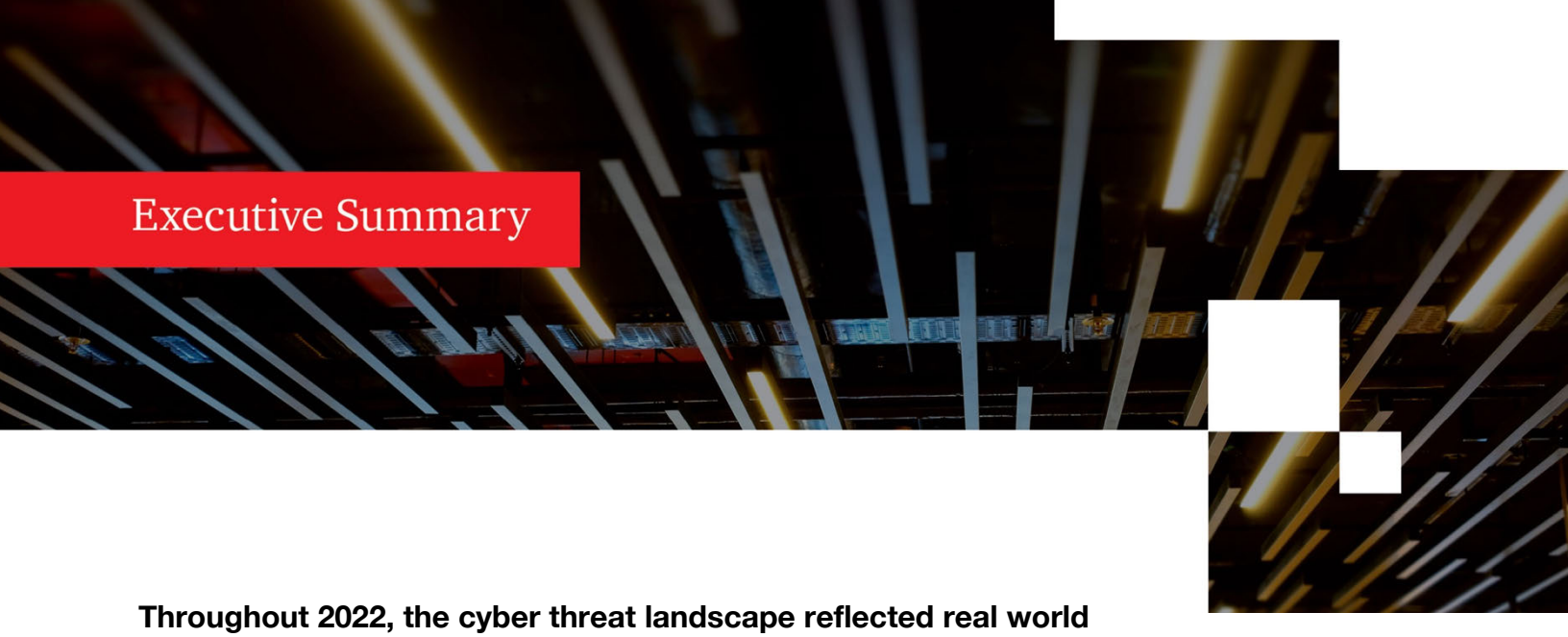
pwc

Cyber Threats 2022: A Year in Retrospect



Executive Summary

Throughout 2022, the cyber threat landscape reflected real world events and geopolitical tensions, with much of the year impacted by the Russian invasion of Ukraine. Log4Shell ushered in a chaotic start to 2022 and highlighted the positive impact of industry collaboration, as well as the criticality of patching and understanding the footprint of widely used software in environments.

Log4Shell was an edge case in terms of vulnerabilities disclosed in 2022, as threat actors continued to make use of known vulnerabilities, exploits and tools (e.g. Cobalt Strike) when conducting their attacks. However, throughout 2022 we also saw threat actors ranging in motivation and sophistication employing enhanced tooling and frameworks, as well as modifying their behaviours to outmanoeuvre security practices implemented by defenders. Further, threat actors increasingly targeted cloud environments as well as identity and privileged access capabilities in 2022.

As the Russian invasion escalated into full scale war, Ukraine along with other governments and cyber security organisations around the world tracked and responded to a series of sabotage efforts by Russia-based threat actors deploying multiple variants of wiperware.[1, 2, 3] These sabotage attacks were largely contained within the immediate conflict zone, i.e. within Ukraine and territories annexed by Russia, and did not have the same level of impact as seen in 2015 and 2016 when Russia-based threat actors targeted Ukraine's energy grid. Whilst multiple espionage motivated threat actors reacted and aligned to this world-changing event, as seen through notable shifts in phishing and targeting operations, the war prompted some cyber criminal threat actors and hacktivists (e.g. Blue Kurama a.k.a. Killnet) to react and respond in their operations and public statements, such as by declaring

[1] 'ESET Research jointly presents Industroyer2 at Black Hat USA with Ukrainian government representative', ESET, https://www.eset.com/int/about/newsroom/press-releases/events/eset-research-jointly-presents-industroyer2-at-black-hat-usa-with-ukrainian-government-representativ/ (25th August 2022)
[2] 'NCSC advises organisations to act following Russia's attack on Ukraine', UK National Cyber Security Centre (NCSC), https://www.ncsc.gov.uk/news/organisations-urged-to-bolster-defences (18th March 2022)
[3] 'Alert AA22-110A - Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure', US Cybersecurity & Infrastructure Agency (CISA), https://www.cisa.gov/uscert/ncas/alerts/aa22-110a (20th April 2022)

pro-Ukraine or pro-Russia stances and targeting government and private sector entities perceived as opposition in the context of the war.

In addition to the Russian war in Ukraine, the cyber threat landscape in 2022 saw a continued optimisation and sophistication of China-based threat actor operations, although the targets of these operations did not significantly change from those seen in prior years. These threat actors increasingly employed obfuscation-as-a-service capabilities, including proxy networks (e.g. RedRelay) and shared malware, exploits and toolsets (e.g. ShadowPad and ScanBox). The most prominent and prolific threat actor using these capabilities was Red Scylla (a.k.a. CHROMIUM, ControlX, Earth Lusca, Aquatic Panda), which targeted at least 70 organisations around the world. Other threat actors flexed sophisticated operations impacting numerous regions, with some threat actors continuing their focus on the telecommunications sector.

Iran-based threat actors continued to make headlines in 2022 for their involvement in sabotage attacks against the Albanian government, their targeting of protesters and dissidents and sectoral targeting against organisations largely in the Middle East, Europe and the United States - activities which often aligned with priorities of the Iranian regime. North Korea-based threat actors doubled down on financial theft through their continued targeting of financial services, cryptocurrency and decentralised finance (DeFi) organisations.

Overall, the advanced persistent threats (APTs) we analysed in 2022 appeared to largely conform to previously observed targeting patterns despite continued efforts within corners of the international community to economically isolate their respective countries, although some threat actors made significant advancements in their operations. Whilst we presume Western-based actions occurred in 2022, we did not identify adequate evidence of these activities, and therefore they are not covered extensively in this report.

The cyber criminal ecosystem also demonstrated operational enhancements in some cases, as well as new developments which challenged organisations around the world throughout 2022. Whilst ransomware remained the top concern for many, we did see indications of a potential regroup or recalibration among some of the more prolific and prominent ransomware threat actors, and 2022 ended with a nearly identical number of leak site victims compared to 2021.

One of the most concerning threat actors with high profile victims in 2022 was White Dev 111 (a.k.a. LAPSUS$ Group), which engaged in a string of “smash-and-grab” and “hack-and-leak” operations against their targets. Many of these attacks used social engineering and other tactics to exhaust security measures and users employed by victim organisations. Cyber-enabled fraud was also rampant throughout 2022, further underscoring the trend of threat actors commoditising access, exploits and tooling and lowering the barrier to entry for a wider range of cyber criminals.

About us

PwC serves more than 200,000 clients in 152 countries, and we use our vantage point as one of the largest international professional services networks to provide global threat intelligence services, tailored and delivered locally to our clients. Our research underpins our security services and is used by public and private sector organisations around the world to protect networks, provide situational awareness and inform strategy.

PwC Threat Intelligence combines our detection capabilities with threat-focused research as well as our proactive efforts to recognise emerging issues, building opportunities to identify and counter gaps in our detection of malicious activity, enrich our threat knowledge and integrate actionable intelligence into our reporting. Our Threat Intelligence team is comprised of members spanning the globe, including Australia, Germany, Italy, the Netherlands, Norway, Sweden, the United Kingdom and the United States. In this report, we provide numerous detection examples[4] that have fueled our threat intelligence and informed resilient cyber strategies.

[4] Please see *Appendix D - Defender index* for a quick guide to all detection content in this report.

Table of Contents


Detection Content


Incident response insights


More information available


Insights from specific PwC firms


Key takeaways


Threat insights

Key Events in 2022

Some of the events from 2022 detailed in this report:

JANUARY

Log4Shell fallout continues after December 2021 disclosure
(pg. 6)

FEBRUARY

Russian invasion of Ukraine begins

(pg. 8)

MARCH

Leaks of Blue Cronus (a.k.a. Conti) internal chats

(pg. 45)

APRIL

White Dev 115 (a.k.a. BlackBasta) emerges, later linked to Blue Cronus
(pg. 46)

MAY

ScanBox targeting with Australian election-themed lures
(pg. 25)

JUNE

Red Dev 32 shifts from PlugX to ShadowPad, joining other threat actors
(pg. 22)

JULY

Brute Ratel red teaming tool gains traction in cyber criminal forums
(pg. 53)

AUGUST

Black Alicanto diversifies lures using Microsoft Software Installers
(pg. 32)

SEPTEMBER

Notable spike in ransomware leak site victims for 2022

(pg. 42)

OCTOBER

Yellow Dev 32 deploys mobile malware against protesters in Iran
(pg. 29)

NOVEMBER

Decline in ransomware leaks, contrary to this time in prior years
(pg. 42)

DECEMBER

Blue Callisto phishes more organisations supporting Ukraine
(pg. 15)

Fallout of Log4Shell

Publicly disclosed in December 2021, the critical vulnerability known as Log4Shell (`CVE-2021-44228`), present within certain versions[5] of Apache Log4j software, initiated a chaotic start to 2022 for organisations around the world.[6] The ubiquitous nature of Apache Log4j software meant entities across sectors and countries needed to respond to the Log4Shell vulnerability disclosure. This urgency was further exacerbated by a proof of concept freely available soon after the disclosure, providing instructions for exploiting this vulnerability and allowing for any type of attacker to remotely execute code on an impacted system. Organisations scrambled to discover Log4j instances within their environments and Apache worked to develop a patch whilst threat actors began exploiting this opportunity within hours of the disclosure.[7]

Detecting Log4Shell exploitation

A simple, and broad, network detection option is to inspect all inbound traffic to exposed servers for the string `${jndi:` - or to account for some common evasion techniques by looking for `${` followed shortly by `jndi`.

By the end of December 2021, Apache released numerous updates to address Log4Shell. The international security community and various government agencies also provided information regarding which versions of the popular software contained security fixes, as well as which software still required attention.[8, 9] This collective effort likely made a difference in quelling the chaos; however, threat actors still managed to exploit Log4Shell throughout 2022, as well as the associated Log4j vulnerabilities `CVE-2021-45046` and `CVE-2021-45105`, discovered after initial remediation attempts were made.

Since the Log4Shell disclosure, dozens of espionage and financially motivated threat actors have exploited this vulnerability across a variety of sectors.[10] In one example from 2022, eight months after the Log4Shell disclosure, Yellow Nix (a.k.a. MuddyWater, MERCURY)[11]

---

[5] *Note:* When originally discovered, Log4Shell impacted Apache Log4j versions 2.0-beta9 to 2.14.1, and subsequent releases spawned additional vulnerabilities, remediated by version 2.17.0. *Source:* 'Alert AA21-356A - Mitigating Log4Shell and Other Log4j-Related Vulnerabilities', CISA, https://www.cisa.gov/uscert/ncas/alerts/aa21-356a (23rd December 2021)
[6] *CTO-QRT-20211210-01A - Active scanning of CVE-2021-44228*
[7] 'Guidance for preventing, detecting, and hunting for CVE-2021-44228 Log4j 2 exploitation', Microsoft, https://www.microsoft.com/security/blog/2021/12/11/guidance-for-preventing-detecting-and-hunting-for-cve-2021-44228-log4j-2-exploitation/ (11th December 2021)
[8] 'Apache Log4j Vulnerability Guidance', CISA, https://www.cisa.gov/uscert/apache-log4j-vulnerability-guidance (December 2021)
[9] 'Alert: Apache Log4j vulnerabilities', NCSC, https://www.ncsc.gov.uk/news/apache-log4j-vulnerability (10th December 2021)
[10] 'Guidance for preventing, detecting, and hunting for CVE-2021-44228 Log4j 2 exploitation', Microsoft, https://www.microsoft.com/security/blog/2021/12/11/guidance-for-preventing-detecting-and-hunting-for-cve-2021-44228-log4j-2-exploitation/ (11th December 2021)
[11] *Note:* We documented one such example in *CTO-TIB-20221007-01A - Yellow Nix with a new access trick, alongside PowerShell scripts*.

exploited the vulnerability in SysAid, an IT support and management product, to gain access to organisations in Israel, according to a Microsoft report.[12] Whilst instances of unmitigated Log4j are still being exploited in the wild, routine exploitation of Log4Shell is likely as prevalent as other well known vulnerabilities[13] from 2022, including `CVE-2022-41040` and `CVE-2022-41082`, collectively known as ProxyNotShell.[14]

Whilst numerous vulnerabilities were disclosed in 2022, Log4Shell reached peak criticality due to the ubiquitous nature of Apache Log4j software, challenges in identifying impacted systems and threat actor persistence in scanning for vulnerable systems and exploiting those not updated or patched. The impact of Log4Shell would likely have been far worse were it not for the impressive response of defenders and the collective efforts of the international security community.

[12] 'MERCURY leveraging Log4j 2 vulnerabilities in unpatched systems to target Israeli organizations', Microsoft, https://www.microsoft.com/security/blog/2022/08/25/mercury-leveraging-log4j-2-vulnerabilities-in-unpatched-systems-to-target-israeli-organizations/ (25th August 2022)
[13] 'Alert AA22-117A - 2021 Top Routinely Exploited Vulnerabilities', CISA, https://www.cisa.gov/uscert/ncas/alerts/aa22-117a (27th April 2022)
[14] *CTO-QRT-20221003-01A - ProxyNotShell*

Russian invasion of Ukraine

On 24th February 2022, Russia invaded Ukraine and attacked Ukrainian infrastructure with air and missile strikes.[15] This invasion followed months of increasingly aggressive rhetoric from the Russian government and years of Ukraine's territorial integrity being violated, including Russia's 2014 annexation of the Crimean peninsula and the de facto separation of the self-proclaimed, Moscow-backed Luhansk and Donetsk People's Republic (L/DPR) regions in eastern Ukraine. The invasion also set the stage for broader geopolitical implications throughout 2022, such as additional countries requesting to join the North Atlantic Treaty Organisation (NATO).[16]

Ukraine has been a persistent target for Russia-based threat actors throughout the past decade, including numerous cyber attacks against the Ukrainian power grid in 2015 and 2016.[17] Blue Echidna's (a.k.a. Sandworm) NotPetya attacks were initially thought to be ransomware deployed against a Ukrainian finance management application; however, NotPetya turned out to be destructive wiperware with devastating consequences for companies beyond Ukraine's borders that used the targeted software.

Memories of NotPetya weighed heavily as Russian wipers began propagating amongst Ukrainian targets in January 2022 and continued during the initial months of the invasion, although the impact of these was contained and much more limited than expected due to the efforts of Ukraine, other governments and security industry partners.[18] In particular, Russia-based threat actors focused on the Ukrainian Defence Ministry and PrivatBank, Ukraine's largest commercial bank, in the first days of the invasion.[19] Whilst many around the world feared a major spillover of cyber activity outside of the conflict zone, as seen with NotPetya, this did not materialise by the end of 2022.

[15] *CTO-SIB-20220224-01A - Tensions escalate into invasion*
[16] *CTO-SIB-20221102-01A - NATO expansion - Finland and Sweden's changing cyber threat landscape*
[17] *CTO-SIB-20220127-01A - Russia and Ukraine: on the brink*
[18] 'ESET Research jointly presents Industroyer2 at Black Hat USA with Ukrainian government representative', ESET, https://www.eset.com/int/about/newsroom/press-releases/events/eset-research-jointly-presents-industroyer2-at-black-hat-usa-with-ukrainian-government-representativ/ (25th August 2022)
[19] 'Ukraine defence ministry website, banks, knocked offline', Reuters, https://www.reuters.com/world/europe/ukraine-reports-cyber-attack-defence-ministry-website-banks-tass-2022-02-15/ (15th February 2022)

JANUARY 2022

Russia arrests 14 individuals associated with White Ursia (pg. 16)

Analysis of WhisperGate wiper, which we associate with Blue Dev 7 (pg. 12)

Analysis of Blue Otso phishing activities (pg. 16)

Blue Kurama emerges as DDoS-for-hire (pg. 19)

Analysis of bomb threat emails sent to Ukraine's security services (pg. 11)

FEBRUARY 2022

Russia's invasion of Ukraine begins (pg. 8)

Attack on Viasat satellite network (pg. 11)

Analysis of Hermetic wiper (pg. 12)

Cyber criminals take sides or project neutrality (pg. 16)

Sanctions against Russia, select Russian financial institutions excluded from SWIFT (pg. 10)

MARCH 2022

Analysis of CaddyWiper and ControlZero wiper (pg. 12-13)

Analysis of Blue Callisto and Blue Dev 4 phishing operations (pg. 15-16)

Leaks of Blue Cronus internal chats (pg. 17, 45)

APRIL 2022

Analysis of StarWiper (pg. 13)

Disclosure of Industroyer variant used alongside CaddyWiper by Blue Echidna and CaddyWiper variants executed by Blue Athena (pg. 11)

Analysis of Blue Callisto infrastructure (pg. 15)

MID-2022

Analysis of Dark Crystal RAT (pg. 18)

Blue Kurama continues DDoS attacks (pg. 19)

Blue Kurama purportedly attacked by Grey Ares (pg. 19)

END OF 2022

Blue Kurama continues DDoS attacks (pg. 19)

Blue Otso phishing continues (pg. 16)

Blue Lelantos operations remained shut down (pg. 17)

Overall, we observed Russia-based threat actors focusing their sabotage operations on the immediate conflict zone, with few exceptions impacting entities outside of Ukraine; however, broader phishing activities by Russia-based threat actors targeted an array of countries and organisations around the world, and in some cases used Ukraine-themed lures.

In the following sections, we detail notable events and trends related to cyber threat actors and their activities leading up to and during the war, such as sabotage operations, phishing operations and intersections with cyber criminal threat actors and techniques.

The impact of threat actor operations had been anticipated, with numerous government agencies publishing mitigation advice that broadly countered the key tools, techniques and procedures (TTPs) of threat actors like Blue Athena (a.k.a. APT28, FANCY BEAR) and Blue

Kitsune (a.k.a. APT29, COZY BEAR), as well as provided threat actor indicators.[20, 21] The private sector also contributed to these efforts, with examples from Mandiant[22] and Dragos[23] demonstrating the collective support to defenders in exposing destructive capabilities targeting operational technology (OT) systems.

Sanctions and responses from the West

Western responses to Russia's invasion of Ukraine included a series of sanctions and widespread public condemnation. These sanctions have resulted in significant economic repercussions for Russia, with a variety of sanctions being imposed on organisations and individuals, such as Russian President Vladimir Putin and other high ranking politicians and officials. Immediately following the initial invasion, select Russian financial institutions were excluded from the SWIFT network, the main global payment messaging system.[24, 25] European Union member countries, the United Kingdom, the United States and other countries further sanctioned Russia in the form of supply chain restrictions and other actions, whilst numerous foreign brands elected to pause or withdraw Russian operations due to ethical considerations and public sentiment.[26]

For some strategic sectors, these restrictions have impacted Russia's ability to access key components and technologies, and Russia has since begun investigating alternatives, such as replacement components and illicit supply chains. As Russia protracts its war and becomes increasingly isolated, we assess Russia-based, espionage motivated threat actors will likely pivot targeting objectives to support Russia's domestic production capabilities through economic espionage, as well as to retaliate against organisations and countries which expressed solidarity with Ukraine.[27]

In our Looking ahead section later in this report, we explore how these scenarios may materialise and the implications for specific sectors and countries.

[20] 'NCSC advises organisations to act following Russia's attack on Ukraine', NCSC, https://www.ncsc.gov.uk/news/organisations-urged-to-bolster-defences (18th March 2022)
[21] 'Alert AA22-110A - Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure', CISA, https://www.cisa.gov/uscert/ncas/alerts/aa22-110a (20th April 2022)
[22] 'INCONTROLLER: New State-Sponsored Cyber Attack Tools Target Multiple Industrial Control Systems', Mandiant, https://www.mandiant.com/resources/blog/incontroller-state-sponsored-ics-tool (13th April 2022)
[23] 'PIPEDREAM: CHERNOVITE's Emerging Malware Targeting Industrial Control Systems', Dragos, https://hub.dragos.com/whitepaper/chernovite-pipedream (13th April 2022)
[24] 'Joint Statement on Further Restrictive Economic Measures', The White House, https://www.whitehouse.gov/briefing-room/statements- releases/2022/02/26/joint-statement-on-further-restrictive-economic-measures/ (26th February 2022)
[25] *CTO-SIB-20220228-01A - Implications of isolation*
[26] *CTO-SIB-20220825-01A - Sanctions and sectoral impact*
[27] *CTO-SIB-20220825-01A - Sanctions and sectoral impact*

Sabotage operations and overlaps

Sabotage operations have been observed throughout the Russian war in Ukraine, ranging from information operations to destructive operations intended to degrade Ukrainian communications and systems. The attack on the Viasat satellite network in February 2022, attributed to Russia-based activity and coinciding with the onset of the Russian offensive, is a notable example of cyber threat actors tactically supporting kinetic operations with longer term strategic implications.[28, 29, 30, 31]

Leading up to the invasion, in late January and February 2022, we analysed samples of bomb threat emails to Ukraine's security services, which we assess were likely from Russia-based threat actors intending to disrupt everyday activities in Ukraine.[32] Since late February 2022, these information operations have extended more broadly to promote both pro-Russia and pro-Ukraine narratives in a variety of channels, as seen prominently on social media.[33] Since the invasion, cyber-enabled information operations and other online activities coincided with a resurgence in hacktivism.

Wipers

Numerous Russia-based threat actors deployed destructive malware against Ukraine-based entities as the invasion persisted.[34] Through our analysis of available samples and research published by others in the security industry, we found examples of code overlaps and potential indicators of sharing across multiple Russia-based threat actors. For example, in April 2022, researchers identified activity attributed to the threat actor we track as Blue Echidna, which showed an Industroyer variant being used alongside a CaddyWiper sample to target a Ukrainian energy organisation,[35, 36] and Mandiant researchers indicated the threat actor we track as Blue Athena had executed CaddyWiper variants against Ukrainian organisations.[37] Given that the Russian government's strategic priorities have centred on its offensive into Ukraine, the potential for Russia-based threat actors to share or crosspollinate malware and capabilities with each other is unsurprising, despite intergroup competition and historical conflicts among security and intelligence services.

---

[28] *CTO-WTU-20220513-01A - Ukraine Weekly Report*
[29] 'Russian cyber operations against Ukraine: Declaration by the High Representative on behalf of the European Union', European Council, https://www.consilium.europa.eu/en/press/press-releases/2022/05/10/russian-cyber-operations-against-ukraine-declaration-by-the-high- representative-on-behalf-of-the-european-union/ (10th May 2022)
[30] 'Russia behind cyber-attack with Europe-wide impact an hour before Ukraine invasion', UK Government, https://www.gov.uk/government/news/russia-behind-cyber-attack-with-europe-wide-impact-an-hour-before-ukraine-invasion (10th May 2022)
[31] 'Attribution of Russia's Malicious Cyber Activity Against Ukraine', US Department of State, https://www.state.gov/attribution-of-russias- malicious-cyber-activity-against-ukraine/ (10th May 2022)
[32] *CTO-QRT-20220224-01A - Wiping and disruption in Ukraine*
[33] *CTO-WTU-20220311-01A - Ukraine Weekly Report*
[34] 'Wipermania: An All You Can Wipe Buffet', Trellix, https://www.trellix.com/en-us/about/newsroom/stories/research/wipermania-an-all-you-can-wipe-buffet.html (15th November 2022)
[35] 'Industroyer2: Industroyer reloaded', ESET, https://www.welivesecurity.com/2022/04/12/industroyer2-industroyer-reloaded/ (12th April 2022)
[36] *CTO-WTU-20220414-01A - Ukraine Weekly Report*
[37] 'GRU: Rise of the (Telegram) Mini0ns', Mandiant, https://www.mandiant.com/resources/blog/gru-rise-telegram-minions (23rd September 2022)

Based on our visibility and collection, we analysed the following wipers:

WhisperGate wiper

Prior to the invasion, Microsoft released a report on 15th January 2022 concerning a destructive malware family it tracks as WhisperGate,[38] which we associate with Blue Dev 7. WhisperGate combines several attack stages consisting of a Master Boot Record (MBR) overwrite and a file corruption stage.[39] When WhisperGate was first discovered, its behaviour and design initially suggested ransomware; however, unlike conventional financially motivated ransomware, WhisperGate's corruption process is irreversible, indicating a sabotage intention rather than extortion. Further, the primary targets of WhisperGate were Ukrainian government organisations, as well as at least one technology firm known to provide services to the Ukrainian government.

Hermetic wiper

Coinciding with Russia's invasion, we analysed Hermetic wiper following initial public reporting, and this wiper attempted to execute on Ukrainian infrastructure and, if successful, would wipe partitions of infected machines, rendering them inoperable. The binary drops an EaseUS Partition file to conduct wiping activities but can also wipe files using the Windows application programming interface (API).[40]

CaddyWiper

In mid-March 2022, security researchers discovered CaddyWiper executing on environments in Ukraine.[41] The wiper contained functionality to wipe files and eventually the physical drive of all the drives mapped on the victim system if it was not the primary domain controller. We assess the threat actor behind CaddyWiper likely manipulated the rich header to cover up its original development fingerprint.[42] Other security researchers linked CaddyWiper to the threat actor we track as Blue Echidna, known for manipulating rich Portable Executable (PE) headers, for example in Olympic Destroyer.[43]

---

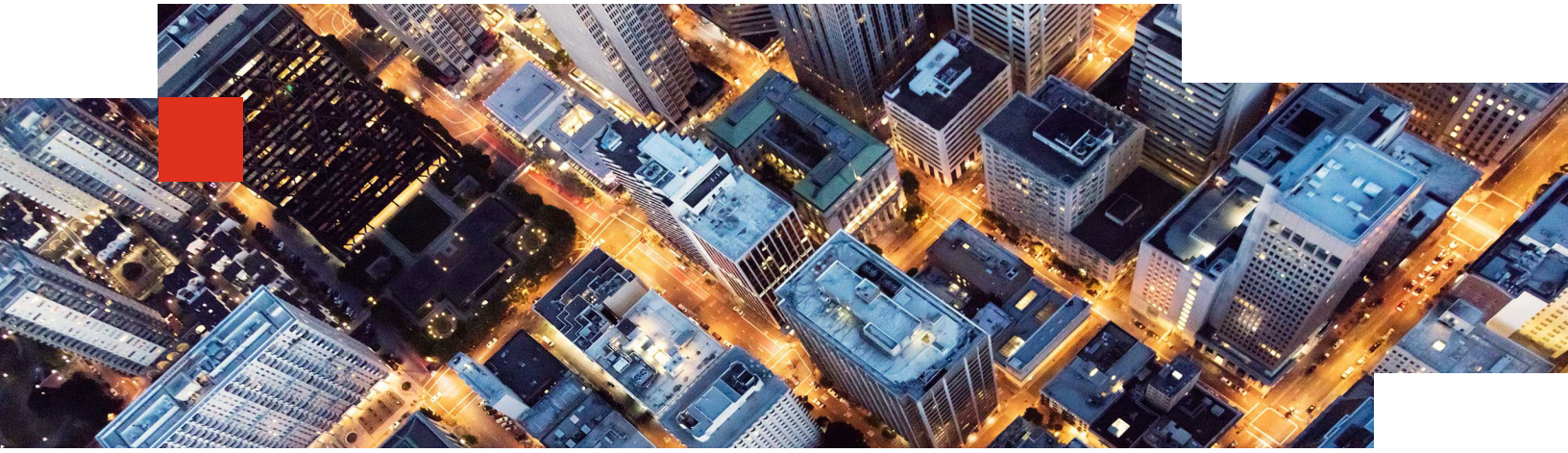
[38] 'Destructive malware targeting Ukrainian organizations', Microsoft, https://www.microsoft.com/security/blog/2022/01/15/destructive-malware-targeting-ukrainian-organizations/ (15th January 2022)
[39] *CTO-TIB-20220121-01A - The WhisperGate Wiper*
[40] *CTO-QRT-20220224-01A - Wiping and disruption in Ukraine*
[41] @ESETResearch, Twitter, https://twitter.com/esetresearch/status/1503436420886712321 (14th March 2022)
[42] *CTO-QRT-20220315-03A - CaddyWiper hits Ukraine*
[43] 'The devil's in the rich header', Kaspersky, https://securelist.com/the-devils-in-the-rich-header/84348/ (8th March 2018)

ControlZero wiper

In mid-March 2022, we named a fourth wiper ControlZero (a.k.a. DoubleZero)[44] for its use of the API call NtFsControlFile to wipe files, and assessed the wiper was likely used for disruption events on Ukrainian networks. In our analysis, we observed ControlZero removing registry keys from the affected system, and the system eventually prompted a restart due to important system resources being modified.[45] From our observations, ControlZero was the first wiper in 2022 to remove registry keys to cause further disruption.

StarWiper

In April 2022, we analysed another wiper we refer to as StarWiper (a.k.a. ACIDRAIN),[46] which appeared to target embedded devices rather than desktop devices due to its microprocessor without interlocked pipelined stages (MIPS) architecture. We connected this wiper with low confidence to Russia's invasion of Ukraine, due to its usage of a filename referencing a Russian language slur against ethnic Ukrainians. If StarWiper was indeed from the arsenal of wipers deployed by Russia-based threat actors against Ukraine, StarWiper represented a shift in destructive malware, targeting embedded devices rather than those previously observed targeting desktop devices.[47]



[44] 'CERT-UA#4243 - Кібератака на українські підприємства з використанням програми-деструктора DoubleZero', Computer Emergency Response Team of Ukraine (CERT-UA), https://cert.gov.ua/article/38088 (22nd March 2022)
[45] *CTO-QRT-20220222-02A - ControlZero added to the wiper list*
[46] 'AcidRain | A Modern Wiper Rains Down on Europe', Sentinel One, https://www.sentinelone.com/labs/acidrain-a-modem-wiper-rains-down-on-europe/ (31st March 2022)
[47] *CTO-TIB-20220405-01A - StarWiper*

Wipers we analysed (MITRE ATT&CK)

During our analysis of the five wipers we observed related to the Russian invasion of Ukraine–WhisperGate wiper , Hermetic wiper, CaddyWiper, ControlZero wiper and StarWiper–we mapped out the tactics (inner circle) and techniques (outer circle) employed by these wipers to the MITRE ATT&CK framework.

In the below wheel, we visualise our detection coverage of these tactics and techniques–addressed through our threat intelligence reporting as well as our detection rules. Each colour represents a different tactic and respective techniques, and next to each label indicates the number of relevant detection rules and/or reports in our holdings. The five techniques that are coloured dark grey below indicate where we do not have relevant coverage. Mapping the tactics and techniques used by threats, however visualised, can help defenders identify gaps and weaknesses in coverage. This then can be used along with the organisation's risk assessment to prioritise the detection backlog.

Phishing operations

Russia-based threat actors employed a broad range of phishing operations to target Ukrainian organisations and other entities leading up to and during the war. Whilst these activities focused on Ukrainian government and military targets, Russia-based threat actors also exhibited broader targeting in relation to their operations, some of which were exposed via public disclosures. Russia-based threat actors rapidly responded to public disclosures of their activities, demonstrating their ability to adapt and continue effective operations despite being actively pursued by both commercial and government security organisations. For example, one day after the early March 2022 Google TAG[48] disclosure of infrastructure associated with the threat actor we track as Blue Athena, the threat actor created new phishing domains, reusing code copied from its previous phishing sites.[49]

In another example of Russia-based threat actor phishing operations, Blue Callisto (a.k.a. Callisto Group) targeted a Ukrainian logistics and courier company, which had been delivering humanitarian aid to Ukraine in addition to its commercial operations. Blue Callisto also conducted credential harvesting campaigns against organisations in Europe and the United States, underscoring the threat actor's dynamic operational portfolio likely at the behest of the Russian government.[50] In December 2022, we identified evidence of Blue Callisto targeting other organisations supporting Ukraine, ranging from providing humanitarian aid to Ukraine to investigating Russia's actions in Ukraine.[51]

Tracking Blue Callisto infrastructure

In April 2022, we analysed Blue Callisto (a.k.a. Callisto Group) domains and found a common infrastructure pattern, further revealing a sprawling network of Blue Callisto infrastructure. We assess the threat actor was likely using this infrastructure to conduct a Ukrainian military-themed phishing campaign.[52] In September 2022, we identified further tracking techniques for Blue Callisto and its interest in US-based laboratories.[53]

Read more about Blue Callisto in one of our blog posts from 2022

In the course of our analysis into Blue Dev 4 (a.k.a. Ghostwriter, UNC1151), we identified a Word document which we assess to be likely associated with the threat actor due to its filename including a Ghostwriter reference. The document contained a list of names and emails of specific individuals and organisations linked to the Ukrainian military, and we assess this list likely contained targets of interest to Blue Dev 4. The list included a website

[48] 'An update on the threat landscape', Google TAG, https://blog.google/threat-analysis-group/update-threat-landscape-ukraine/ (7th March 2022)
[49] *CTO-TIB-20220411-01A - Blue Athena 2022 phishing part 2*
[50] *CTO-SIB-20220908-01A - Ukraine Threat Update - August 2022*
[51] *CTO-SRT-20221213-01A - Blue Callisto targets Ukraine-linked organisations*
[52] *CTO-TIB-20220511-01A - Tracking Callisto infrastructure*
[53] *CTO-TIB-20220913-02A - Blue Callisto still phishing*

owner for a Ukrainian military uniform, equipment and accessories store; Military Unit A1965, Ukrainian Naval forces based in the Zaporizhzhia region; several researchers affiliated with Ukrainian defence institutes; and, a Ukrainian reservist based in the Vinnytsia region.[54] Targeting we attributed to Blue Dev 4 revealed a combination of approaches, from widespread and opportunistic targeting of varieties of victims to persistent, ongoing efforts to compromise specific targets of interest.

We also analysed Blue Otso (a.k.a. Gamaredon Group) phishing activities seen in January 2022. As tensions escalated between Russia and Ukraine leading up to the invasion, Blue Otso used Sievierodonetsk- and Crimea-themed lures in weaponised documents in its spear phishing operations, leading to self-extracting archives and UltraVNC binaries. Both Sievierodonetsk and Crimea hold geopolitical significance, as the former is a city strategically located in Luhansk outside what had been Russia-backed separatist LPR territory, and the latter has been under Russian annexation since 2014.[55] In late 2022, Blue Otso reverted to registering domains using an email we first attributed with its operations in 2020, and the registered domains were themed toward Ukraine's State Special Communications Service; however, the domains were in a different format when compared to previous Blue Otso activity. Throughout 2022, Blue Otso registered domains likely through an automated process using wordlists with no particular theme.[56] It is also likely Blue Otso maintained separate clusters of activity controlled manually as well as automated. Blue Otso's infrastructure management diversified in 2022 and became more dynamic than seen in prior years, and its command and control (C2) domains changed daily to resolve to new IP addresses.

Circling the cyber crime wagons

The Russian war in Ukraine shone an additional spotlight on Eastern European cyber criminals and how they would respond to the war, particularly where they would align their allegiance. Prior to the invasion, in mid-January 2022 the Russian government announced its arrests of 14 individuals allegedly associated with White Ursia, the threat actor in control of the ransomware affiliate programme known as REvil or Sodinokibi. This announcement prompted some cyber criminals to reconsider their targeting, as at least one of those arrested was noted as also being responsible for the May 2021 ransomware attack on US-based Colonial Pipeline, attributed to White Apep (a.k.a. DarkSide, BlackMatter).[57] Following Russia's offensive into Ukraine in February 2022, cyber criminals grew more concerned about sanctions impacting their ability to extort, launder and cash out funds from their illicit activities,[58] but in general cyber crime continued as normal.

[54] *CTO-QRT-20220303-01A - Blue Dev 4 phishing operations in 2022*
[55] *CTO-TIB-20220203-01A - Blue Otso retains Ukraine interest*
[56] 'ACTNIUM targets Ukrainian organizations', Microsoft, https://www.microsoft.com/en-us/security/blog/2022/02/04/actinium-targets-ukrainian-organizations/ (4th February 2022)
[57] *CTO-SIB-20220211-01A - White Ursia, from Unknown to under the bus*
[58] *CTO-SIB-20220915-02A - Tales from the crypto*

Sanctions effectively curtailing high profile cyber criminal organisations

In 2021, Blue Lelantos (a.k.a. Evil Corp), the threat actor responsible for the Dridex banking trojan and the ransomware systems BitPaymer, DoppelPaymer, Grief and Wasted Locker, went through multiple attempts to rebrand its ransomware operations, having been "blacklisted" by insurers and specialist ransomware negotiators in response to US sanctions imposed on the threat actor. With Blue Lelantos being forced to make more radical changes to its operations in 2022, we assess these rebrand efforts likely failed, based on the following observations:

- Once a mainstay of Evil Corp's arsenal, Dridex activity dwindled;
- We did not observe new rebrands of existing Blue Lelantos ransomware variants in 2022; and,
- Other security researchers reported efforts by elements of Blue Lelantos to enrol in rival ransomware schemes.[59]

Once a notorious cyber crime syndicate, the sustained shutdown in 2022 of Blue Lelantos operations demonstrated that, in this case at least, sanctions and takedowns[60] are effective tools to significantly disrupt high profile cyber criminal operations.

In February 2022, the Conti ransomware brand, operated by Blue Cronus, declared its support for the Russian invasion of Ukraine and threatened to target critical infrastructure of countries targeting Russia via threats posted directly on its leak site. Other cyber criminal threat actors, namely White Janus (a.k.a. LockBit) and White Dev 101 (a.k.a. ALPHV-ng, BlackCat), stressed their motivations were purely financial and expressed a degree of neutrality concerning the war.[61] Regardless of their ideological stances, we assess Russia-based ransomware threat actors are likely in the position to be co-opted or coerced by the Russian government to conduct operations in support of Russia.

[59] 'To HADES and Back: UNC2165 Shifts to LOCKBIT to Evade Sanctions', Mandiant, https://www.mandiant.com/resources/blog/unc2165-shifts-to-evade-sanctions (June 2022)
[60] 'Cyber Threats 2021: A Year in Retrospect', PwC Threat Intelligence https://www.pwc.com/gx/en/issues/cybersecurity/cyber-threat-intelligence/cyber-year-in-retrospect/yir-cyber-threats-report-download.pdf (28th April 2022)
[61] *CTO-SIB-20220301-01A - Cyber criminal and hacktivist response*

Dark Crystal RAT activity in Ukraine

Since Russia's invasion of Ukraine, a variety of financially and espionage motivated threat actors have exploited the war as a theme to gain a foothold into victim environments. One particular attack resulted in the execution of Dark Crystal RAT, a remote access trojan (RAT) typically observed in financially motivated operations. We assess the associated malicious Excel file, which contained macros and information related to the State Emergency Service of Ukraine, was likely used for targeting an entity related to the Ukrainian government.[62] The threat actor that deployed Dark Crystal RAT later returned with another Ukrainian-themed lure related to Russian collaborators, and the weaponised lure executed WarZone RAT, another malware variant often associated with financially motivated threat actors.

Detecting Dark Crystal RAT

Universal Resource Identifiers (URIs)

```
\.php\?type=__ds_setdata&__ds_setdata_user=[a-f0-9]{40}&__ds_setdata_ext=[a-f0-9]{32}&__ds_setdata_data=

\.php\?type=__ds_getdata&__ds_getdata_user=[a-f0-9]{40}&__ds_getdata_ext=[a-f0-9]{32}&__ds_getdata_key=[a-f0-9]{32}$
```

COMSurrogate

Dark Crystal RAT launches the task COMSurrogate when the user logs on with escalated privileges (MITRE ATT&CK T1053.005 - Scheduled Task/Job: Scheduled Task).[63]

It will also execute a b64 encoded powershell command, which will trigger the following detections (MITRE ATT&CK T1140 - Deobfuscate/Decode Files or Information and T1059.001 - Command and Scripting Interpreter: PowerShell):

```
[0934]-[evasion]-[m]-powershell_executing_base64_encoded_commands
[0942]-[execution]-[m]-powershell_with_abbreviated_noprofile_switch
[0931]-[execution]-[m]-powershell_with_abbreviated_executionpolicy_bypass_switch
```

As financially motivated threat actors waded into or avoided narratives involving the war, hacktivism-inspired threat actors and interlocutors surfaced, adding further complexity to pro-Russia and pro-Ukraine information operations. This included appearances by self-identified, pro-Ukraine hacktivist accounts attaching themselves to the Anonymous

[62] *CTO-TIB-20220616-01A - Opaque Dark Crystal RAT activity in Ukraine*
[63] *CTO-TIB-20220616-01A - Opaque Dark Crystal RAT activity in Ukraine*

collective, which we track as Grey Ares, as well as the IT Army of Ukraine[64] and Network Battalion 65 (a.k.a. NB65).[65] Killnet, the pro-Russia hacktivist collective that we track as Blue Kurama,[66] gained notoriety for its multiple distributed denial of service (DDoS) attacks against critical infrastructure in Lithuania, high profile public and private institutions in Norway,[67] Latvia's Parliament and Estonian public websites.[68] Blue Kurama's operations were notable in 2022, as their DDoS targets included public and private organisations critical of Russia's actions and located outside of the immediate conflict zone; however, we found the effectiveness of Blue Kurama's campaigns, whilst widely publicised, were usually low impact compared to other types of cyber attacks.[69]

The bluster of Blue Kurama

Blue Kurama (a.k.a. Killnet) is just one example of "patriotic hacking groups" that emerged during the war in Ukraine and which supported either pro-Russia or pro-Ukraine interests. Blue Kurama specifically aligned its support to Russia.[70] The threat actor primarily engaged in DDoS attacks against Ukrainian targets and public and private organisations, especially those tied to critical infrastructure and defence, from countries considered acting against Russian interests (e.g. Romania,[71] Italy,[72] Lithuania, Norway[73] and the United States[74]). Blue Kurama initially formed as a DDoS-for-hire capability in January 2022 and was founded by an individual with the online moniker `Killmilk`, who claimed to be a Russian national based in Russia. As Blue Kurama transitioned from its for-hire model to conducting attacks, the threat actor facilitated its operations and recruitment primarily through Russian language Telegram channels. On a number of public forums, it was reported Blue Kurama conducted DDoS attacks using Mirai botnets in 2022. In May 2022, Blue Kurama found itself on the receiving end of purported attacks launched by Grey Ares (a.k.a. Anonymous).[75]

Overall, Blue Kurama's attacks, if successful, were largely short lived and did not result in significant or sustained impact. However, the potentially disruptive and destructive nature of the threat actor's attacks and intentions serves as a cautionary tale of a proliferation trend in hacktivism that may increase as the war continues, or as other conflicts arise.

[64] *CTO-SIB-20220301-01A - Cyber criminal and hacktivist response*
[65] *CTO-SIB-202220707-01A - Ukraine Threat Update - June 2022*
[66] *CTO-TIB-20221208-02A - Not cool Killnet*
[67] *CTO-SIB-202220707-01A - Ukraine Threat Update - June 2022*
[68] *CTO-SIB-20220908-01A - Ukraine Threat Update - August 2022*
[69] *CTO-TIB-20221208-02A - Not cool Killnet*
[70] *CTO-TIB-20221208-02A - Not cool Killnet*
[71] *CTO-WTU-20220505-01A - Ukraine Weekly Report*
[72] *CTO-WTU-20220513-01A - Ukraine Weekly Report*
[73] *CTO-SIB-20220707-01A - Ukraine Threat Update - June 2022*
[74] *CTO-SIB-20220804-01A - Ukraine Threat Update - July 2022*
[75] *CTO-WTU-20220526-01A - Ukraine Weekly Report*

China-based threat actors optimising operations

Throughout the year, threat actors continued to coalesce around shared networks, infrastructure and capabilities, often resulting in arguably more streamlined, expansive and technically sophisticated operations than those observed in previous years. Whilst this is a trend we have been analysing for several years,[76, 77] in 2022 there was an observed spike in shared exploits and tools, including obfuscation-as-a-service proxy networks. Our analysis of threat actor targeting patterns further revealed country-specific targeting operations, as well as a continued focus on digital supply chain and high technology compromises, notably organisations within the telecommunications sector.

Whilst these targets are not novel, China-based threat actors are increasingly optimising their operations and leveraging shared proxy resources, challenging conventional methods for attribution, incident response and damage assessments.

Additionally, starting in late 2021, we identified numerous instances involving multiple threat actors obfuscating implant payloads, highly likely employed to avoid detection and thwart analysis. Significantly, Red Lich (a.k.a. Mustang Panda, Temp.Hex, TA416) used LLVM-based obfuscation of both its loader and inner PlugX payload during campaigns targeting entities in Europe. Whilst the usage of LLVM and other obfuscation techniques is not new, this has usually only been applied on the loader components and not the payload itself.

This evolution further challenges attempts to identify and reverse engineer new and unknown payloads that would otherwise be detectable through YARA signatures, or through manual review using static and dynamic tools. By adding this extra layer of protection to custom and bespoke tooling, attackers increase the longevity of their campaigns in the face of improvements on the defensive side.

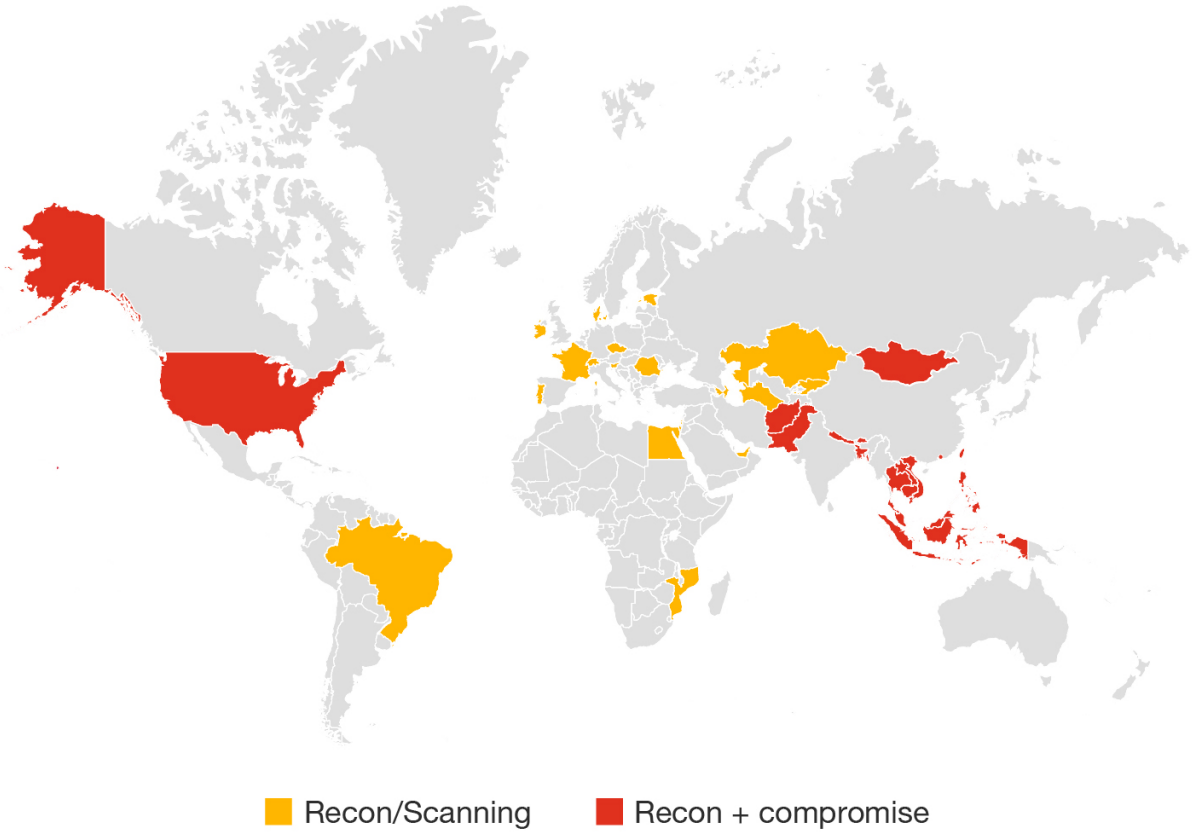
We expect to see the trend of obfuscation and the protection of payloads continue and to improve at the operational level—where individual threat actors are employing obfuscation on custom implants, as well as at the developer level—where malware provided to threat actors is readily packaged or obfuscated by a quartermaster.

[76] 'Cyber Threats 2020: A Year in Retrospect', PwC Threat Intelligence, https://www.pwc.co.uk/cyber-security/pdf/pwc-cyber-threats-2020-a-year-in-retrospect.pdf (17th December 2020)
[77] 'Cyber Threats 2021: A Year in Retrospect', PwC Threat Intelligence https://www.pwc.com/gx/en/issues/cybersecurity/cyber-threat-intelligence/cyber-year-in-retrospect/yir-cyber-threats-report-download.pdf (28th April 2022)

Red Scylla, a Winnti-linked global threat

In August 2022, we assigned Red Scylla (a.k.a. CHROMIUM, ControlX, Earth Lusca, Aquatic Panda) to the activity we previously tracked as Red Dev 10,[78] largely due to our identification of a distinctive set of infrastructure and techniques.[79] Red Scylla was arguably the most prominent and prolific China-based threat actor in 2022, and given its global targeting remit, optimised operational tempo and sophistication, we view Red Scylla as the most active threat actor emanating from China.

Red Scylla targeting in 2022



We observed Red Scylla scanning for vulnerabilities, using the open source tool Acunetix[80] and deploying a wide ranging post-compromise toolset which included both custom backdoors and tools commonly shared among these threat actors, such as ShadowPad and PlugX. Since 2021, we have tracked Red Scylla as a ShadowPad[81] user, primarily

[78] Please see *Appendix B – Threat actor reference* for more information about our naming convention.
[79] *CTO-TIB-20220825-01A - Red Scylla: A Winnti-Linked Global Threat*
[80] *CTO-TIB-20220621-01A - Red Dev 10 - Acunetix Scanning*
[81] 'Chasing Shadows: A deep dive into the latest obfuscation methods being used by ShadowPad', PwC Threat Intelligence, https://www.pwc.co.uk/issues/cyber-security-services/research/chasing-shadows.html (8th December 2021)

through a custom obfuscation method we dubbed ScatterBee,[82] which uses control flow obfuscation, execution guardrails and runtime patching to obstruct forensic analysis. Red Scylla targeted organisations from a global range of sectors, rapidly progressing from reconnaissance activities, gaining access to victim networks and deploying malware early in intrusions in a likely attempt to widen its foothold in victim environments.

Red Scylla has not been the only threat actor deploying ShadowPad in the last year. Throughout 2022, ShadowPad was used among threat actors we already associated with this malware family, as well as newly identified clusters of activity. During our tracking of ShadowPad C2 infrastructure, we identified a new cluster based on associated infrastructure management, which we now track as Red Dev 32.[83] We assess this threat actor likely shifted from PlugX to ShadowPad in June 2022, administering infrastructure that served fake Microsoft Secure Sockets Layer (SSL) certificates. Later in 2022, we identified evidence of overlaps between Red Dev 32 and Red Scylla, such as Red Scylla operational relay boxes (ORBs) being used for testing activity with a Red Dev 32 ShadowPad C2. We assess it is highly likely these two threat actors share some form of organisational relationship. In October 2022, we further linked ShadowPad infrastructure to Red Dev 14, where multiple ShadowPad C2 hosts were serving a stolen, self-signed certificate originally belonging to a Middle Eastern government entity.[84]

Defending against these TTP commonalities

Given these TTP commonalities among China-based threat actors, defenders would be well advised to monitor for LNK files with archive file targets and supplementary command lines (MITRE ATT&CK T1204.002 - User Execution: Malicious File). Additionally, though the hijacked applications vary, dynamic link library (DLL) side-loading (T1574.002 - Hijack Execution Flow: DLL Side-Loading) remains a consistent technique seen across the infection chains for these threat actors.

RedRelay, a shared proxy network

Throughout 2022, we continued research into a proxy network, used by multiple threat actors, which we identified in 2021 and refer to as RedRelay. These threat actors had begun moving to shared proxy networks over the past several years, and we assess these ostensibly covert networks are likely operated in a quartermastering arrangement, through which tools are provisioned, sold and shared by a public or private entity. Proxy network characteristics, such as multihop proxying and facilitating communications over encrypted channels, challenge traditional research methods for analysis and attribution. Proxy networks are also built using a combination of hundreds of threat actor-operated virtual private servers (VPS) and compromised devices.

[82] *CTO-TIB-20211021-01A - Chasing shadows*
[83] *CTO-TIB-20220913-01A - Red Dev 32*
[84] *CTO-TIB-20221005-01A - Not to worry; I have a certificate of authority*

In one example, we analysed the use of RedRelay by Red Vulture (a.k.a. APT15, APT25, Ke3chang). Red Vulture used a specific cluster of RedRelay infrastructure throughout 2021 and into early 2022. In March 2022, Red Vulture decommissioned and rebuilt this cluster before resuming its reconnaissance and exploitation activities against European governments, pan-European institutions and international organisations. This change demonstrated Red Vulture's proactive operational security (OPSEC) measures and mirrored wider shifts in RedRelay infrastructure management methods, which we observed in February 2022.[85]

Country-specific targeting

In January 2022, we analysed malware communicating with C2 domains we attribute to Red Orthrus (a.k.a. Keyboy, TA428, Tropic Trooper), with this specific malware variant being a 64-bit version of the RAT known in open source as nccTrojan.[86] The lure themes of the C2 domains present in these nccTrojan samples appeared to spoof organisations within the Russian defence and manufacturing sectors; further, additional pivoting from infrastructure known to be hosting nccTrojan domains revealed additional crossover between Russian-themed domains and Red Orthrus infrastructure. At some stage, all of these domains were hosted on a Russia-based IP address, and we assess the threat actor likely structured this intentionally to make the C2 traffic appear innocuous to the target.[87] We assess these activities were likely indicative of intelligence collection as Russian forces mobilised ahead of the invasion into Ukraine.

Red Phoenix (a.k.a. APT27, Emissary Panda, LuckyMouse) remained an ever-present and active threat throughout 2022. In January 2022, Germany's Federal Office for the Protection of the Constitution (BfV) released a public blog[88] providing technical details into the operations of this threat actor, as well as Red Phoenix's targeting of German businesses. In tracking infrastructure and malware associated with the longstanding, custom malware families HyperBro and FOCUSFJORD[89] attributed to Red Phoenix, we found the vast majority of operations in 2022 targeted organisations based in the South China Sea region.

[85] *CTO-TIB-20220523-02A - Rampant Reconnaissance Redux*
[86] 'China-linked TA428 Continues to Target Russia and Mongolia IT Companies', Recorded Future, https://www.recordedfuture.com/china-linked-ta428-threat-group (17th March 2021)
[87] *CTO-QRT-20220315-01A - Red Orthrus targets Russia*
[88] 'Cyber attack campaign against German commercial companies', BfV, https://www.verfassungsschutz.de/SharedDocs/kurzmeldungen/DE/2022/2022-01-26-cyberbrief.html (26th January 2022)
[89] 'Cyber Threats 2020: A Year in Retrospect', PwC Threat Intelligence, https://www.pwc.co.uk/cyber-security/pdf/pwc-cyber-threats-2020-a-year-in-retrospect.pdf (17th December 2020)

Red Phoenix, hyped and focused

HyperBro

The HyperBro backdoor has long been associated with Red Phoenix (a.k.a. APT27, Emissary Panda, LuckyMouse). The threat actor uses legitimate binaries to side-load malicious DLLs and drop HyperBro onto victim machines, a technique Red Phoenix has employed since 2015. One indicator of HyperBro malware is the presence of a signing certificate belonging to Cheetah Mobile Inc. - a China-based mobile internet company. As well as eliciting a consistent response, the C2 infrastructure also invariably hosts an SSL certificate of SHA-1 hash `44b9d089cf734d2478165a8539b23aed51887f7d` on port 443. Historic online port scanning data suggests that active HyperBro servers have shared these characteristics since at least June 2019.[90]

FOCUSFJORD

Several new FOCUSFJORD samples were identified in 2022 containing the expected unique Shikata Ga Nai obfuscation code, where the compilation timestamps are from June 2022 onwards. All of the C2 domains associated with these recent samples followed the trend of containing the top-level domain (TLD) `.me`.

Further Tooling

In addition to the above, open source reporting in August 2022 detailed how MiMi, a Chinese instant messaging application, was used to retrieve ELF and Mac variants of the rshell backdoor, along with links to Red Phoenix.[91] We have since identified further rshell malware samples, where we assess, in some cases, Red Phoenix likely managed the associated infrastructure based on overlaps with known HyperBro C2 infrastructure.[92] During our research, we also found a HyperBro C2 server concurrently hosting a Cobalt Strike certificate, whilst a separate HyperBro server concurrently hosted Fast Reverse Proxy (FRP).[93]

Also in January 2022, we began tracking a significant regional targeting shift concerning a campaign we assess is highly likely attributed to Red Lich (a.k.a. Mustang Panda, Temp.Hex, TA416). This particular campaign focused on European government and diplomatic entities, whereas since 2020, Red Lich employed a broad targeting remit against victims ranging from nongovernmental organisations (NGOs) to government entities across South and East Asia specifically, as well as internationally. In the first phase of this Europe-focused campaign, beginning in at least January 2022 to late March 2022, Red Lich used RAR or ZIP archives, the titles of which used themes relevant to European affairs, specific Central European countries and the Russian war in Ukraine.

[90] *CTO-TIB-20221102-01A - Rising from the hashes*
[91] 'LuckyMouse uses a backdoored Electron app to target MacOS', Sekoia, https://blog.sekoia.io/luckymouse-uses-a-backdoored-electron-app-to-target-macos/ (12th August 2022)
[92] *CTO-TIB-20221102-01A - Rising from the hashes*
[93] *CTO-TIB-20221102-01A - Rising from the hashes*

These archives contained a legitimate executable, which would download a decoy document to show the victim, as well as the Trident loader for PlugX, a benign executable, a malicious DLL to be side-loaded and an encoded PlugX sample in a DAT resource.[94] Between late March 2022 and late October 2022, Red Lich updated its TTPs in the context of its targeting of European entities, likely in an attempt to avoid detection, and possibly in response to public disclosure of the campaign.[95] The threat actor pivoted to using compressed archives with malicious LNK files that would launch the Trident loader to run PlugX on victim machines. In the second phase of this campaign, Red Lich added further obfuscation and anti-analysis measures to its malware - including LLVM control flow flattening. Throughout this campaign, Red Lich primarily targeted Eastern and Central European government entities involved in foreign affairs, as well as embassies and supranational entities based in Belgium.

In yet another example of a capability shared among threat actors and being used in high profile operations, we along with Proofpoint[96] analysed an espionage motivated ScanBox campaign running from April 2022 through June 2022. ScanBox is a web reconnaissance and exploitation framework shared uniquely among China-based threat actors, and it has been in use sporadically since at least 2014. The 2022 campaign had an international reach but with a specific focus against organisations in the Asia Pacific region, Australian government and media entities and companies and countries with equities in the South China Sea, including global heavy industrial manufacturers. We attributed this specific campaign to Red Ladon (a.k.a. TA423, APT40, Leviathan). Red Ladon had previously used ScanBox in 2018; in both the 2018 and 2022 campaigns, the threat actor crafted lures around national elections and established news-themed malicious websites to draw in targets. In the 2022 campaign, Red Ladon transposed verbatim headlines concerning the May 2022 Australian election from a UK-based news organisation onto a Red Ladon-controlled website impersonating an Australian news media outlet.[97]

Learn more about a related threat, Red Dev 26, in our talk at Virus Bulletin 2022

[94] *CTO-QRT-20220302-01A - Red Lich eyes Europe*
[95] 'Mustang Panda's Hodur: Old tricks, new Korplug variant', ESET, https://www.welivesecurity.com/2022/03/23/mustang-panda-hodur-old-tricks-new-korplug-variant/ (23rd March 2022)
[96] 'Rising Tide: Chasing the Currents of Espionage in the South China Sea', Proofpoint, https://www.proofpoint.com/us/blog/threat-insight/chasing-currents-espionage-south-china-sea (30th August 2022)
[97] *CTO-TIB-20220829-01A - Rising Tide*

Persistent focus on telecommunications

Whilst we have identified instances of threat actors targeting telecommunications providers for a number of years, our research into 2022 activities against this sector revealed further optimisation efforts undertaken by several threat actors.[98]

The implications for intrusions into telecommunications providers cannot be overstated: these activities undermine secure communications crossing countries, businesses and governments and threaten diplomatic, societal and business norms around the world.

In August 2022, we assigned Red Moros to the threat actor we previously tracked as Red Dev 4 (a.k.a. GALLIUM) after our identification of the threat actor's distinct TTPs, reconnaissance activities and C2 infrastructure and communications. Throughout 2022, Red Moros aggressively targeted telecommunications providers and government entities around the world, as well as a number of academic institutions. Our visibility into Red Moros' activities revealed the threat actor using open source SoftEther virtual private network (VPN) software, both offensively and as part of its infrastructure setup. We also identified variants of a malware family known in open source as PingPull, which we assess is likely an evolved version of China Chopper malware.[99]

First introduced in 2021,[100] Red Menshen remained active in 2022 targeting the telecommunications and logistics sectors. Despite public disclosure of one of its most commonly used malware families, BPFDoor, and a seemingly coordinated removal of a number of long running BPFDoor infections in August 2022, we have continued to observe Red Menshen accessing systems at previous victims as well as new targets.[101]

Read more about these threats in our TROOPERS22 talk synopsis

[98] 'U/OO/160405-22: People's Republic of China State-Sponsored Cyber Actors Exploit Network Providers and Devices', US government, https://media.defense.gov/2022/Jun/07/2003013376/-1/-1/0/CSA_PRC_SPONSORED_CYBER_ACTORS_EXPLOIT_NETWORK_PROVIDERS_DEVICES_TLPWHITE.PDF (7th June 2022)
[99] *CTO-TIB-20220823-02A - Red Moros' Reconnaissance*
[100] 'Cyber Threats 2021: A Year in Retrospect', PwC Threat Intelligence https://www.pwc.com/gx/en/issues/cybersecurity/cyber-threat-intelligence/cyber-year-in-retrospect/yir-cyber-threats-report-download.pdf (28th April 2022)
[101] 'Tinker Telco Soldier Spy', PwC Threat Intelligence, https://troopers.de/troopers22/talks/7cv8pz/ (29th June 2022)

Iran's internal and external challenges

Throughout 2022, Iran-based threat actors continued to conduct espionage motivated attacks against victims in the Middle East, Europe and North America, and in some cases doubled down on destructive attacks that included wipers, ransomware and "hack-and-leak" attacks.

We also observed a focus expansion for Iran-based threat actors involving more domestic and regional targets, likely stemming from counterintelligence failures, domestic unrest and a perceived need for retaliatory operations.

Sanctions and enablers of cyber operations

Much of the Western response to Iran's transgressions in 2022 involved additional sanctions imposed on the regime. Iran was confronted with US sanctions[102] for its illicit activities in four key areas: its involvement in sanction evasion networks to promote its petrochemicals sales; sales of unmanned aerial vehicles (UAVs) and weapons to Russia for use in Ukraine; crackdowns on protesters and political dissidents, internet censorship and human rights abuses; and, offensive cyber operations. As Iran wrestled with continuing economic and diplomatic isolation, Iran-based threat actors targeted sectors and regions with direct and tangential connections to sanctions and formal rebukes of the regime. In some cases, our analysis of Iranian offensive cyber operations in 2022 was supported by US sanctions being levied against the same entities we analysed, such as Najee Technology and Ravin Academy.

In September 2022, SECNERD, formally known as Najee Technology, was included in a list of Iran's Islamic Revolutionary Guard Corps (IRGC)-affiliated entities sanctioned by the US government for their roles in ransomware activities.[103] Earlier in the year, we had begun tracking infrastructure associated with SECNERD, a Farsi-language website purporting to provide cyber security resources.[104] We identified direct infrastructure overlaps between SECNERD and Yellow Dev 24 (a.k.a. DEV-0270, Nemesis Kitten). We then tracked a corporate trail connecting entities behind SECNERD, indicating associations with Iranian government entities such as the IRGC, the Execution of Imam Khomeini's Order (EIKO) and other sanctioned entities.[105]

In October 2022, the US government responded to Iran's cyber operations and crackdown on protesters by sanctioning several Iranian individuals, intelligence agencies and

[102] 'Iran Sanctions', US Department of State, https://www.state.gov/iran-sanctions/ (23rd November 2022)
[103] 'Treasury Sanctions IRGC-Affiliated Cyber Actors for Roles in Ransomware Activity', US Department of the Treasury, https://home.treasury.gov/news/press-releases/jy0948 (14th September 2022)
[104] http://secnerd[.]ir, WayBackMachine (Archive), https://web.archive.org/web/20220223151704/http://secnerd.ir (6th April 2022)
[105] *CTO-TIB-20220517-01A - Get some better OPSEC nerd*

ostensibly NGOs, such as Ravin Academy.[106] Ravin Academy was founded in November 2019, shortly after a series of leaks exposed its co-founders' affiliation with Iran's Ministry of Intelligence and Security (MOIS). Our analysis into Ravin Academy further revealed links to Yellow Nix, as well as professional links between Ravin Academy and Yellow Maero (a.k.a. APT34).[107]

Read more about Yellow Nix in one our blog posts from 2022

Sabotage attacks

In July 2022, several MOIS-aligned threat actors were identified conducting sabotage attacks on Albanian government systems,[108] which involved reconnaissance and prepositioning before their deployment of wipers and ransomware.[109] We assess the attacks were almost certainly motivated by Albania hosting the Mujahedin-e-Khalq (MEK). The diplomatic fallout between Albania and Iran following these attacks was significant, with Albania formally cutting ties with Iran. The Albanian government further considered calling for Article Five of the NATO treaty, but ultimately decided to not escalate its conflict with Iran any further. We found parallels between these attacks and those in January 2022 against a US-based organisation for its connection to the MEK,[110] carried out by the IRGC-aligned threat actor we track as Yellow Dev 19 (a.k.a. Emennet Pasargad).[111]

In their attacks on Albania, Iran-based threat actors[112] remained on Albanian government systems for as long as 14 months, indicative of extensive prepositioning before conducting destructive effects. This overall operation demonstrated threat actor persistence and highlighted the trend of Iran-based threat actors employing both espionage and sabotage

[106] 'Treasury Sanctions Iranian Officials and Entities Responsible for Ongoing Crackdown on Protests and Internet Censorship', US Department of the Treasury, https://home.treasury.gov/news/press-releases/jy1048 (26th October 2022)
[107] *CTO-SIB-20220121-01A - Advanced persistent teacher*
[108] *Note:* Microsoft assesses multiple Iranian threat actors participated in this attack under four different clusters of activity which we associate with Yellow Maero (a.k.a. APT34), Yellow Dev 9 (a.k.a. Lyceum, Hexane) and Yellow Dev 31 (a.k.a. DEV-0842). *Source:* 'Microsoft investigates Iranian attacks against the Albanian government', Microsoft, https://www.microsoft.com/en-us/security/blog/2022/09/08/microsoft-investigates-iranian-attacks-against-the-albanian-government/ (8th September 2022)
[109] 'Alert AA22-264A - Iranian State Actors Conduct Cyber Operations Against the Government of Albania', US Cybersecurity & Infrastructure Security Agency, https://www.cisa.gov/uscert/ncas/alerts/aa22-264a (21st September 2022)
[110] 'PIN 20221020-001 - Iranian Cyber Group Emennet Pasargad Conducting Hack-and-Leak Operations Using False-Flag Persons', US Federal Bureau of Investigation (FBI), https://www.ic3.gov/Media/News/2022/221020.pdf (20th October 2022)
[111] 'Cyber Threats 2021: A Year in Retrospect', PwC Threat Intelligence https://www.pwc.com/gx/en/issues/cybersecurity/cyber-threat-intelligence/cyber-year-in-retrospect/yir-cyber-threats-report-download.pdf (28th April 2022)
[112] *Note:* Microsoft assesses multiple Iranian threat actors participated in this attack under four different clusters of activity which we associate with Yellow Maero (a.k.a. APT34), Yellow Dev 9 (a.k.a. Lyceum, Hexane) and Yellow Dev 31 (a.k.a. DEV-0842). *Source:* 'Microsoft investigates Iranian attacks against the Albanian government', Microsoft, https://www.microsoft.com/en-us/security/blog/2022/09/08/microsoft-investigates-iranian-attacks-against-the-albanian-government/ (8th September 2022)

attacks against targets. The threat actors gained initial access by exploiting an unpatched SharePoint server, dropped webshells, moved laterally with AnyDesk remote desktop and escalated privileges using built-in role groups for Microsoft Exchange. The threat actors then leveraged those role permissions to exfiltrate emails using a bespoke tool just before disabling endpoint defences and deploying both wipers and ransomware.[113]

Iran-based threat actors also continued their "hack-and-leak" or "lock-and-leak" operations against other organisations, seen previously in 2021 when the threat actor commonly referred to as Moses Staff conducted "lock-and-leak" operations over a diverse range of sectors in Israel.[114] In the second half of 2022, a very similar threat actor emerged named Abraham's Ax, which claimed to have gained access to Saudi Ministry of Interior systems and posted both anti-West and anti-Israel messages on social media.[115] The modus operandi between Moses Staff and Abraham's Ax are nearly identical, and we identified network infrastructure overlaps indicating the two threat actors are closely aligned.[116]

Domestic and dissident targeting

Our analysis throughout the year indicated a continued trend of Iran-based threat actors, such as Yellow Garuda (a.k.a. Charming Kitten, APT42, PHOSPHORUS), focused on domestic and dissident targets. Yellow Garuda targeted Farsi speakers, likely within Iran but also possibly abroad, with a special focus on students, activists and purported militants. We analysed overlaps of activity occurring between September 2021 and June 2022, with Yellow Garuda weaponising Microsoft documents using `CVE-2021-40444` and `CVE-2022-30190`. Based on compile times, Yellow Garuda was able to operationalise these exploits within one week after their public disclosure, providing a narrow window for defenders to create effective detection and mitigation measures.[117]

Amidst the protest activity in Iran in 2022 sparked by the September 2022 death of Mahsa Amini, a Kurdish Iranian woman arrested for violating hijab laws,[118] Iran-based threat actor targeting continued to focus on a domestic audience, such as activists, dissidents and protesters. Even with the breakout of widespread protests, Iran-based threat actors also maintained their focus on standing priorities for the Iranian regime, which included organisations within the government, defence, telecommunications and energy sectors.[119] Simultaneously, Iran's domestic surveillance apparatus continued its inward targeting, including through third party enablers and malware deployed against civilian mobile

[113] *CTO-TIB-20220916-01A – Iran-based APTs attack Albania*
[114] 'Cyber Threats 2021: A Year in Retrospect', PwC Threat Intelligence https://www.pwc.com/gx/en/issues/cybersecurity/cyber-threat-intelligence/cyber-year-in-retrospect/yir-cyber-threats-report-download.pdf (28th April 2022)
[115] 'Abraham's Ax Likely Linked to Moses Staff', Secureworks, https://www.secureworks.com/blog/abrahams-ax-likely-linked-to-moses-staff (26th January 2023)
[116] 'Iranian Hacking Group Abraham's Ax claims hack on Saudi Ministry of Interior', Cyberwarzone, https://cyberwarzone.com/abraham-ax-saudi-ministry-interior-cyberattack/ (November 2022)
[117] *CTO-TIB-20220728-01A - Bye Follina*
[118] 'UN rights chief says 'full-fledged' crisis underway in Iran amid crackdown on protesters', CNN, https://www.cnn.com/2022/11/24/middleeast/iran-protests-un-human-rights-council-intl/index.html (24th November 2022)
[119] 'Alert AA22-055A - Iranian Government-Sponsored Actors Conduct Cyber Operations Against Global Government and Commercial Networks', CISA, https://www.cisa.gov/uscert/ncas/alerts/aa22-055a (24th February 2022)

devices.[120] Yellow Dev 32 was one group focused on internal targets by deploying Android malware called L3MON on protestors' phones in October 2022.[121]

Sector and regional targeting trends

Another trend concerning Iran-based threat actors seen across 2022 was their heavy targeting of sectors in relation to shipping, logistics, maritime and critical infrastructure in Europe and the Middle East. Since at least May 2022, Yellow Liderc (a.k.a. Tortoiseshell, CURIUM) embedded JavaScript on legitimate websites that operate in the maritime, shipping and logistics sectors.[122] The script fingerprints website visitors by capturing user location, device information and timestamps of visits. Simultaneously, the threat actor registered typosquatted domains masquerading as websites infected with malicious scripts. We assess Yellow Liderc likely used these typosquatted domains in conjunction with user fingerprint data to launch tailored spear phishing attacks. Part of this activity aligned with similar targeting reported in open source, which detailed how the threat actor targeted shipping organisations in Israel between 2020 and 2022.[123] We further assess much of this activity likely related to the seizures of tankers flagged for carrying Iranian crude oil, such as the vessel seized in the Mediterranean at the request of the US government in May 2022.[124]

In early 2022, we identified instances of Yellow Garuda leveraging lures covering a variety of themes, including Turkey's nuclear ambitions and US shipping ports. We considered the possibility that Yellow Garuda crafted the lures for targets in the wider Middle East, and that the activity may not have been indicative of a campaign targeting energy sector organisations specifically. At least one US port-related lure document was likely targeted since its format consisted of a letter with a named recipient.[125]

We also continued to observe Yellow Garuda targeting journalists, think tanks and researchers using similar TTPs first seen in 2019, through our analysis of associated infrastructure publicly disclosed in open source in January 2022.[126] We attributed the infrastructure to Yellow Garuda and identified domains spoofing media organisations and think tanks based in the United States, Israel and the United Arab Emirates. Upon further analysis, we identified the think tanks and journalists targeted as being notable experts of, or typically involved in, Middle East foreign policy, nuclear negotiations and other strategic interests relevant to the Iranian regime. We also identified domains spoofing Google and Microsoft accounts, along with more domestic focused targets aligning with typical Yellow Garuda victimology.[127]

---

[120] *CTO-TIB-20221206-01A - A sour L3MON and a FurBall*
[121] *CTO-TIB-20221206-01A - A sour L3MON and a FurBall*
[122] *CTO-TIB-20221208-01A - Yellow Liderc ships its scripts*
[123] 'Suspected Iranian Actor Targeting Israeli Shipping, Healthcare, Government and Energy Sectors', Mandiant, https://www.mandiant.com/resources/blog/suspected-iranian-actor-targeting-israeli-shipping (17th August 2022)
[124] 'Iranian oil tanker's cargo seized in Greece after US request', AP News, https://apnews.com/article/russia-ukraine-politics-united-states-68af0db11c5c03e89049da0629ef4d85 (26th May 2022)
[125] *CTO-TIB-20220308-01A - Charming Kitten's Turkish delight*
[126] 'Shady Network of Fake Mossad Job Sites Targets Iranian Spies', The Daily Beast, https://www.thedailybeast.com/shady-network-of-fake- mossad-job-sites-target-iranian-spies (24th January 2022)
[127] *CTO-TIB-20220302-01A - A busy bird that Yellow Garuda*

Read more about Yellow Garuda in one of our blog posts from 2022

In 2022, Iran-based threat actors continued to target Israel-based organisations. In one example, we analysed a GitHub account associated with Yellow Nix, and subsequently identified a script within the account's repository containing a C2 IP address. We attributed the infrastructure to Yellow Nix and assessed it was highly likely used to target Israeli and Turkish organisations.[128] In another example, Yellow Nix targeted multiple Israeli insurance companies in November 2022 by leveraging a commercial remote administration tool called Syncro.[129]

Incident response case involving Yellow Liderc

Early in 2022, we supported broader PwC incident response efforts involving a European engineering and manufacturing organisation targeted by Yellow Liderc (a.k.a. Tortoiseshell, TA456). Through our analysis of the sample executables provided by the victim, we found the threat actor employing evolved tools and tradecraft, and we assess these shifts are likely indicative of Yellow Liderc attempting to enhance its operational security to evade detection and maintain persistence in victim networks.

We analysed the functionality of three Python scripts obfuscated with PyArmor, a tool available in open source for that exact purpose, as well as network traffic between the victim and the Yellow Liderc server. We found C2 communications beginning as early as January 2022 and continuing for a period of at least four months. The highly obfuscated samples communicated over a secure messaging protocol to dedicated mailboxes, all of which serve as an indicator of Yellow Liderc enhancing its operational security.[130]

Whilst we often discover Iran-based threat actors through their poor operational security and use of known infrastructure and tools, this incident highlights the importance of not underestimating motivated threat actors and their ability to evolve outside of assessed behaviours and boundaries. Our deep knowledge of threat actor motivations and TTPs allowed us to prioritise incident response efforts and provide substantive context to the victim for future planning.

[128] *CTO-TIB-20220210-01A - Smooth Operator*
[129] *CTO-TIB-20221206-02A - Let's Syncro up with Yellow Nix*
[130] *CTO-TIB-20220628-02A - Three varieties of Liderc*

Other regional case studies

In this section, we provide a sampling of other threat actors ranging in sophistication and motivation.

As in previous years, threat actor activities in 2022 aligned with real world events and reflected geopolitical circumstances, which in many cases appeared connected to political and national strategic objectives and priorities.

Black bag operations for the money

Our research into activities concerning North Korea-based threat actors throughout 2022 primarily reinforced known trends, TTPs and victimology we had seen in previous years, such as the targeting of organisations within the financial services sector and cryptocurrency-affiliated companies,[131] as well as financially motivated attacks across numerous other sectors. Based on targeting patterns we observed in 2022, we assess North Korea-based threat actors are highly likely continuing to respond to financial theft tasking on behalf of the government.

We continued to observe a high operational tempo attributed to financially motivated Black Alicanto (a.k.a. COPERNICIUM, DangerousPassword, CryptoMimic, CryptoCore, Operation SnatchCrypto) and Black Dev 2 (a.k.a. Operation Gold Hunting, Operation SnatchCrypto), which targeted cryptocurrency as well as venture capital and startup organisations in 2022. We assess Black Dev 2 is likely linked to Black Alicanto, and since 2021, the two have targeted victims with job-themed lures, as well as around opportunities for raising venture capital in the cryptocurrency space.[132] Black Alicanto used Microsoft Software Installers (MSIs) in mid-to-late 2022 to achieve initial access and installation on victim systems, as opposed to its traditional use of malicious LNK files.

Black Artemis (a.k.a. Lazarus Group, Hidden Cobra, ZINC) remained very active, running multiple campaigns throughout 2022. The threat actor continued its campaign known in open source as “Operation Dream Job” and “Operation Interception” and which we track as ShowState, using the malware family known in open source as BLINDINGCAN.[133] Black Artemis’ continued use of malware implants like BLINDINGCAN and DTrack, deployed since at least 2018 and 2014 respectively, demonstrates the threat actor’s proclivity to develop its existing codebase rather than abandoning it, in addition to adding new tools to its arsenal.

[131] *CTO-SIB-20220915-02A - Tales from the crypto*
[132] *CTO-TUS-20220616-01A - Threats under the Spotlight - May 2022*
[133] *CTO-TIB-20220812-01A - Black Artemis’ dream job hunt*

Black Artemis also continued to conduct espionage motivated targeting against defence and military entities, developing significant additions to its toolset and introducing malware families like YamaBot and MagicRAT. Industry reporting concerning the threat actor's targeting of energy sector organisations[134, 135] has been particularly noteworthy and complemented our visibility into other aspects of Black Artemis activity.

Insights from PwC South Korea

In the second half of 2022, PwC South Korea was alerted to the ransomware threat actor self-branded as GWISIN, meaning ghost in Korean, targeting organisations strictly within South Korea. The threat actor appears to have thorough knowledge of the Korean environment, such as widely used local security systems, as well as Korean security certifications and law enforcement. The threat actor employed defensive evasion techniques, true to its name, in combination with web vulnerabilities and web shells used to send commands and exfiltrate data from victims.

Seeing static Orange

Throughout 2022, India-based threat actors maintained their relatively high operational tempo, employing known TTPs from 2021. Whilst we have observed heavy targeting of Pakistan-based government and defence entities with malware similar to those used in previous years by India-based threat actors, we identified several notable new targets and TTPs. Several threat actors, such as Orange Yali (a.k.a. BITTER)[136] and Orange Kala (a.k.a. DONOT), seemingly broadened their targeting to include organisations based in other countries in the region, whilst Orange Chandi (a.k.a. SideWinder) changed its attack process from its longstanding TTPs used across 2020 and 2021.

Whilst 2022 provided evidence of new targeting aligning with political events in the region,[137] India-based threat actors have primarily altered tooling within their attack processes instead of implementing more sophisticated techniques. In several instances, as previously seen in 2021,[138] India-based threat actors continued to make use of commodity RATs in their campaigns.

[134] 'Stonefly: North Korea-linked Spying Operation Continues to Hit High-value Targets', Symantec, https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/stonefly-north-korea-espionage (27th April 2022)
[135] 'DTrack activity targeting Europe and Latin America', Kaspersky, https://securelist.com/dtrack-targeting-europe-latin-america/107798/ (15th November 2022)
[136] *CTO-TUS-20221027-01A - Threats under the Spotlight - September 2022*
[137] *CTO-SIB-20220915-01A - APAC-origin forecast - Q2 2022 developments*
[138] *CTO-TIB-20210112-01A - Orange Kala enters the Warzone*

Talent Need Not Apply: Advanced Persistent Threats using job-themed lures

As the COVID-19 pandemic led a significant number of workers to rethink their careers, threat actors exploited the opportunity throughout 2022 to fulfil strategic objectives for both financial and espionage motivations. North Korea- and Iran-based threat actors were particularly brazen in their attempts to target employees at high profile companies, using social engineering to approach employees over email and social media to build rapport before attempting to gain initial access into company networks.[139]

- **North Korea-based threat actors and financially motivated campaigns**
  Job recruitment is a long running pretext for North Korea-based threat actors. During one such campaign in 2022, Black Artemis (a.k.a. Lazarus Group, Hidden Cobra, ZINC) established a variety of social media personas, including posing as recruitment professionals and human resources contacts at high profile companies, to socially engineer targets. Black Artemis also set up websites, impersonating well known job search companies, weaponised with browser exploits to deploy malware on the targets' machines.

  In another method, after contacting individuals on LinkedIn, WhatsApp or via email, the threat actor attempted to coax targets into opening malicious documents from systems they used for work. Once opened, the remote template injection or malicious macros would download malware implants on the organisations' networks. Since at least July 2022, Black Artemis pivoted to having targets open EXE files[140] or ISO files[141] contained in compressed archives, under the pretence of job descriptions for open roles at high profile technology companies or candidate assessments. In another example, since at least August 2022, Black Alicanto (a.k.a. COPERNICIUM, DangerousPassword, CryptoMimic, CryptoCore, Operation SnatchCrypto) experimented with MSI files as malicious lures in similar campaigns, likely in an attempt to diversify initial access techniques.

- **Iran-based threat actor employing an espionage motivated campaign**
  Yellow Dev 13 (a.k.a. BOHRIUM, TA455) also posed as recruiters for real or fictitious companies across a variety of social media, including LinkedIn, Facebook, Instagram and Twitter, despite takedowns by Meta[142] and Microsoft.[143] Yellow Dev 13 used a variety of artificial intelligence (AI)-generated photographs for its personas and impersonated at least one real individual for its operations.

[139] 'Talent Need Not Apply Tradecraft and Objectives of Job-themed APT Social Engineering', PwC Threat Intelligence, https://i.blackhat.com/USA-22/Thursday/US-22-Wikoff-Talent-Need-Not-Apply.pdf (11th August 2022)
[140] *CTO-TIB-20220812-01A - Black Artemis' dream job hunt*
[141] 'It's Time to PuTTY! DPRK Job Opportunity Phishing via WhatsApp', Mandiant, https://www.mandiant.com/resources/blog/dprk-whatsapp-phishing (14th September 2022)
[142] 'Meta Quarterly Adversarial Threat Report: Q1 2022', Meta, https://about.fb.com/wp-content/uploads/2022/04/Meta-Quarterly-Adversarial-Threat-Report_Q1-2022.pdf (April 2022)
[143] 'Microsoft Corporation, A Washington corporation, Plaintiff, v. John Does 1-2, Controlling a computer network and thereby injuring plaintiff and its customers: Ex Parte temporary restraining order and order to show cause re preliminary injunction', Microsoft, https://news.microsoft.com/wp-content/uploads/prod/sites/358/2022/06/Doc.-No.-16-Ex-parte-TRO-SEALED.pdf (27th May 2022)

Yellow Dev 13 also ran at least two websites for fake recruitment companies named ApplyTalents and CareersFinders,[144] which shared the same fake team and contact addresses purporting to be UK-based recruitment companies. In at least one case, the threat actor built a malicious executable simulating an entire assessment platform for job candidates, including aptitude tests and a live chat support function, that would connect back to the ApplyTalents domain in the background. Whilst the platform required users to input credentials likely supplied by the threat actor to avoid analysis by researchers, we assess Yellow Dev 13 was likely attempting to compromise individuals or organisations for espionage purposes.

Learn more in our Talent Need Not Apply talk at BlackHat USA 2022

WIRTING about White Dev 21

In 2022, White Dev 21 (a.k.a. WIRTE) continued to target a variety of victims throughout the Middle East, including Jordan, Palestine, Syria and Lebanon. A particular cluster of activity in September 2022 revealed that White Dev 21 relied heavily on geopolitical lures, leveraging themes relating to the Gulf Cooperation Council and information about Arab financial services and government organisations. The threat actor demonstrated a persistent ability to target key sectors and entities in the region.[145]

An in-Tur-esting development

In January 2022, we released a public blog concerning the threat actor we track as White Tur, which targeted organisations within the Balkans region from at least 2017 through 2021. Following our disclosure,[146] the threat actor remained active and continued to target organisations within the Balkans region with themes related to Bosnia-Herzegovina and Serbia. We further identified a series of HTML Application (HTA) scripts which were created between January 2022 and April 2022 and indicative of a shift in White Tur's TTPs. In this series of HTA scripts, the threat actor used the WebDAV protocol to transfer a malicious payload to the victim's machine.[147]

Learn more about White Tur in one our blog posts from 2022 and our Threat Actor of in-Turest talk at SANS CTI Summit 2022

[144] *CTO-TIB-20220121-02A - Talent need not apply to this career finder*
[145] *CTO-TUS-20221027-01A - Threats under the Spotlight - September 2022*
[146] 'Threat actor of in-Tur-est', PwC Threat Intelligence, https://www.pwc.com/gx/en/issues/cybersecurity/cyber-threat-intelligence/threat-actor-of-in-tur-est.html (27th January 2022)
[147] *CTO-TIB-20221012-03A - White Tur's WebDAV adventures*

More about White Tur TTPs

HTA files are interpreted by `mshta.exe`, a well known live-off-the-land binary (a.k.a. LOLBin) that is frequently abused by threat actors. As HTA files present an opportunity to launch scripts in HTML without many of the restrictions of a browser, they are abused by attackers to proxy execution of malicious JavaScript or VBScript, for example. Detection controls should be focused around the `mshta.exe` process, for example detecting mshta.exe calling an HTA file from a remote location or writing files with certain extensions to disk.

As White Tur copied executables to disk using the WebDAV protocol, they were placed in the Startup folder to ensure their persistent execution. Monitoring all files written to the Startup folder in an enterprise environment is challenging, but given the frequency of its abuse by threat actors, detection controls need to be in place to identify suspicious file creations. Detection logic based on anomalous activity or globally unique files in this directory is likely to surface this type of activity, although this type of analysis is not available for all detection tooling. A good starting point is to monitor for LOLBins, or commonly abused executables writing files to this location.

What's up with White Dev 140?

One of our research projects in 2022 resulted in a perplexing pattern of behaviour which we attribute to White Dev 140. The threat actor's interest included Ukrainian entities in 2022, similar to targeting we have seen from Russia-based threat actors, but White Dev 140 also had a diverse set of other interests outside of Ukraine which have confounded our initial assessments of the threat actor's motivations. These interests included:[148]

- Food exporters, supermarkets and retailers;
- Regional governmental organisations, such as the Dnipro government and Piatykhatky District;
- Energoatom, Ukraine's nuclear agency;
- A gas company;
- Factories manufacturing metals and electronic devices; and,
- Logistics companies and private couriers.

Sample indicators of White Dev 140 activities we identified in 2022:

```
https[:]//product808[.]godaddysites[.]com/purchase-order
https[:]//support-domaill[.]godaddysites[.]com/ukr
https[:]//shipping8[.]godaddysites[.]com/dhl
https[:]//servicesagreement[.]godaddysites[.]com/update
https[:]//support-ukr[.]godaddysites[.]com/log-in
```

[148] *CTO-TIB-20221209-02A - Phishing trips to Ukraine*

We first identified White Dev 140 spear phishing activity in May 2022, with the threat actor targeting a Ukraine-based software reseller that also supplies licences to the Ukrainian government.[149] The spear phishing email contained a `UKR[.]net` theme, a popular internet portal used in Ukraine for email. The email contained a PDF attachment with the following message in Ukrainian, which has been roughly translated:

```
Dear User
This message was sent with high importance. Our record shows that your
account has not been updated Note: if you do not verify your account,
it will be deactivated shortly

This update is required immediately after receiving this message
Sincerely
@UKR mail team
```

The TTPs from the spear phishing activity at the time were similar to those used by Blue Athena, which had been conducting a broad phishing campaign, including:[150, 151]

- PDF attachment containing the phishing link and using `UKR[.]net` themes;
- Utilisation of free hosting providers;
- Targeting; and,
- Email contents.

The spear phishing emails contained a PDF attachment with a phishing link to the URL:

```
https[:]//ukrverifikaciyaakkaunta[.]godaddysites[.]com/privacy-policy
```

In October 2022, another White Dev 140 spear phishing email targeted a Ukrainian domain, and the email used DHL themes but with a Deutsche Post URL used for the phishing link. The phishing URL was:

```
https[:]//deutschepost[.]godaddysites[.]com/login
```

When analysing the technical data associated with the spear phishing email, we discovered similarities with the May 2022 and October 2022 phishing pages we previously analysed.

---

[149] *CTO-QRT-20220601-01A - More phishing attempts against Ukraine*
[150] *CTO-QRT-20220326-01A - Blue Athena Phishing Part 1*
[151] 'Update on cyber activity in Eastern Europe', Google, https://blog.google/threat-analysis-group/update-on-cyber-activity-in-eastern-europe/
(3rd May 2022)

From the additional sample, we found a consistent pattern allowing us to identify further phishing pages.

A tailored response?

In September 2022, China's National Computer Virus Emergency Response Center (CVERC) reported the US National Security Agency (NSA), specifically its Tailored Access Operations (TAO), had launched attacks against a Chinese university using a suite of tools,[152] some of which shared names with tool names previously leaked separately by both an individual and a group known as the Shadow Brokers.[153] The September 2022 report did not include indicators, timeframes or other characteristics of the alleged activities.

Insights from PwC Brazil

In 2022, PwC Brazil analysed Brazil-based threat actors utilising a commercialised web interface known as "Data Broker Panels", which has been in existence for at least five years and allows for the searching of sensitive information concerning Brazilian citizens. The threat actors were able to sell subscription access to the panels, typically in monthly plans, enabling cyber criminals to exploit the information for social engineering attacks and fraud.

[152] 'Chinese reports uncover details of cyber attacks by U.S. security agency', Xinhua, https://english.news.cn/20220913/71f9b72993614795b4d8ff554c99ef9b/c.html (13th September 2022)
[153] 'Shadow Brokers leaks show U.S. spies successfully hacked Russian, Iranian targets', CyberScoop, https://www.cyberscoop.com/nsa-shadow-brokers-leaks-iran-russia-optimusprime-stoicsurgeon/ (18th April 2017)

Cyber criminal ecosystem shifts

Notable developments of the overall cyber criminal ecosystem emerged in 2022, such as threat actors engaging in "hack-and-leak" operations resembling the digital equivalent of "smash-and-grab" sprees combined with "big game hunting", i.e. selecting high profile or perceived high value targets whilst chasing headlines and notoriety.

However, cyber criminal ecosystem shifts were largely supported by a continued undercurrent of financially motivated threat actors capitalising on opportunistic and exploitative attacks involving theft, extortion and fraud, with ransomware attacks dominating the market.

Ransomware threat actors were more brazen in their attempts to pressure extortion victims and recruit insiders in 2022, and we assess this trend will likely grow more prominent in the coming year as threat actors further fracture ransomware brands, compete for resources and respond to increased defences and resiliency across organisations. Given the intersections of cyber crime and threat actors based in Eastern Europe, we addressed specific developments related to the Russian war in Ukraine earlier in this report - Russian invasion of Ukraine: Circling the cyber crime wagons.

Ransomware developments

Once considered a disrupter to the cyber crime threat landscape, over the past several years ransomware has become a consistently dominant threat to organisations. Ransomware's continued prevalence has been largely due to Ransomware-as-a-Service (RaaS) operations, the perpetuating model we detailed in our **Cyber Threats 2021: A Year in Retrospect** report.[154]

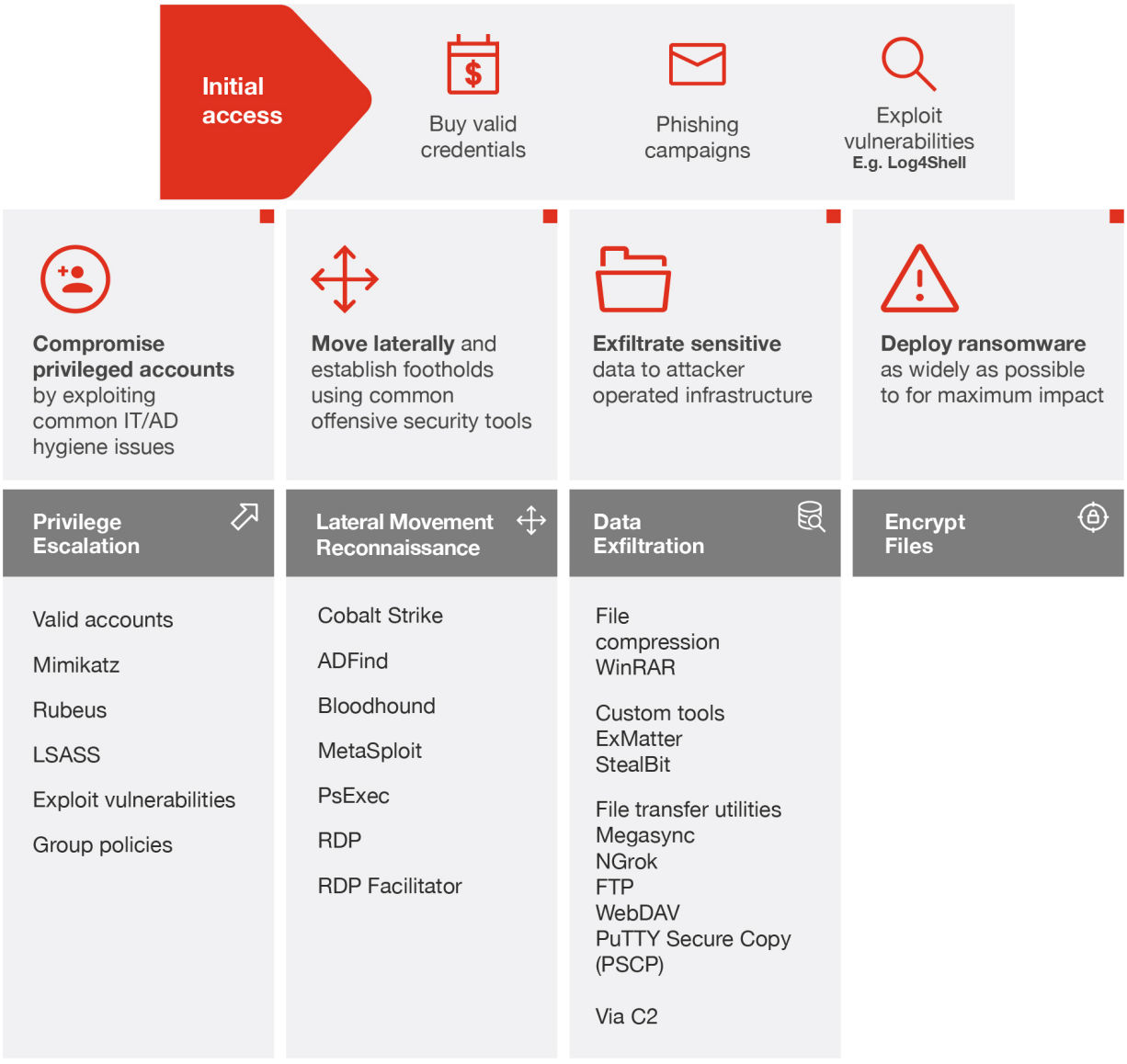
In 2022, the ransomware threat landscape saw a levelling off of leak site victims comparable to 2021 trends. We assess this level of leak site activity is likely to remain consistent in 2023; however, the number of distinct ransomware brands is unlikely to be a

[154] 'Cyber Threats 2021: A Year in Retrospect', PwC Threat Intelligence https://www.pwc.com/gx/en/issues/cybersecurity/cyber-threat-intelligence/cyber-year-in-retrospect/yir-cyber-threats-report-download.pdf (28th April 2022)

relevant indicator of the threat landscape, as it has been common practice for groups to rapidly shift and rebrand.

Moving forward, we judge the more relevant data points to track atmospherics across ransomware activity will be seen in the overlapping TTPs of ransomware threat actors.

TTPs observed in a typical Ransomware-as-a-Service (RaaS) operation



Leak site analysis

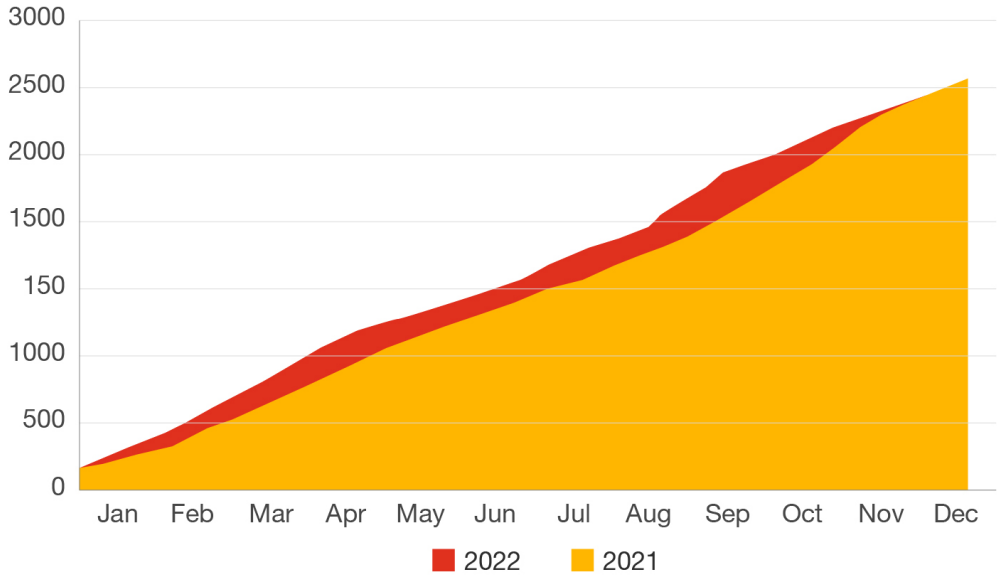
In 2022, there were 2,462 total victims posted to ransomware leak sites we tracked, slightly fewer (within 1%) compared to the 2,471 posted in 2021 and almost doubling the 1,330 posted in 2020. Whilst there was a progressive increase in ransomware leak site victims from 2020 to 2021, the total number of leak site victims appeared to plateau between 2021 and 2022.

We therefore assess the number of leak site victims for 2021 and 2022 likely represents a "high water" mark for this activity, with 2022 having posed significant challenges to the ransomware ecosystem, such as the Russian war in Ukraine, law enforcement actions against ransomware threat actors, cryptocurrency volatility and internal leaks and conflicts fracturing prominent ransomware groups.[155]

Leak site activity vs. broader ransomware threat activities

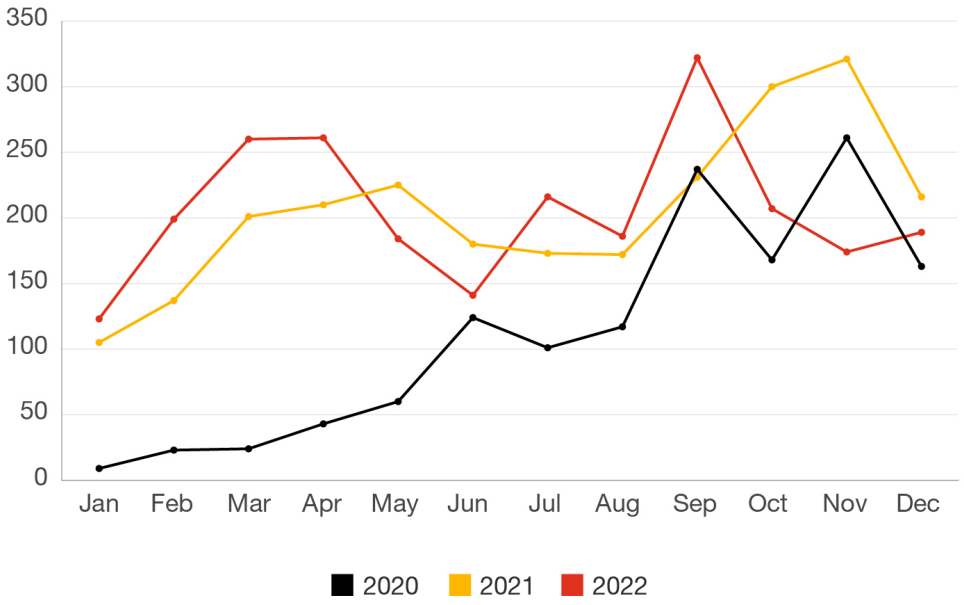
Tracking leak site activity provides specific visibility into the ransomware threat landscape; however, we continue to pursue other avenues of analysis as leak sites do not provide a complete picture of ransomware activities, particularly concerning threat actors operating without leak sites and victims that are not posted to leak sites or otherwise publicly disclosed.

Number of leak site victims posted throughout year (2021 – 2022)



[155] *CTO-SRT-20230118-01A - Ransomware report for December 2022*

Number of leak site victims posted each month (2020 – 2022)



We classify ransomware attacks as opportunistic and enabled by widespread and indiscriminate infection operations, but we did observe several sectors having more leak site victims than others in 2022. Notably, the top five sectors with victims posted to ransomware leak sites in 2022 were manufacturing (15%), construction (10%), professional services (9%), technology (8%) and retail (8%).

Possible explanations include the perceived high cost of operational downtime for these sectors, as well as the comparatively lower level of information security regulations imposed on these sectors. In addition to these trends, ransomware attacks significantly impacted organisations affiliated with other sectors in 2022, including government, telecommunications, transportation, energy and education.

White Janus with the lion's share

In our analysis of leak site activity in 2022, White Janus (a.k.a. LockBit) dominated in numbers throughout the year and quickly overtook the 2021 pace of Blue Cronus, which led the ransomware pack in leak site activity in 2021. In June 2022, White Janus announced its LockBit 3.0 RaaS programme, which further powered its operations and leak tempo in the second half of 2022. We assess White Janus likely spent much of June 2022 beta testing LockBit 3.0, coinciding with a pronounced decline in victims posted to its leak site when compared to the threat actor's leak site activity in the first half of 2022.[156] By the end of December 2022, White Janus posted 907 victims to its leak site in total for all of 2022, compared to 460 victims the threat actor posted in 2021.[157]

[156] *CTO-QRT-20220804-03A - White Janus changes the Locks*
[157] *CTO-SRT-20230118-01A - Ransomware report for December 2022*

When LockBit 3.0 was first released in June 2022, we identified codebase overlaps with malware previously used as the main ransomware binary in the now defunct BlackMatter RaaS operation. We analysed these overlaps - found initially in the opening functions - and determined LockBit 3.0 was nearly identical to BlackMatter, such as language checks for specific country codes, encryption implementation and anti-analysis techniques.[158] The technical overlaps were substantial enough that we, alongside other researchers, assessed the similarity is likely a result of White Janus' procurement of the BlackMatter codebase.[159] This was confirmed by the White Janus spokesperson in an interview reported in July 2022.[160]

Seeing BlackMatter in BlackCat

White Janus (a.k.a. LockBit) was not the only threat actor with capabilities overlapping with BlackMatter in 2022. In December 2021, the ransomware threat actor ALPHV-ng emerged, with its logo prompting many in open source to label the brand BlackCat. We began tracking this threat actor as White Dev 101 and quickly identified connections to BlackMatter.[161] Based on significant code overlaps between BlackMatter and White Dev 101 binaries, we assess BlackMatter developers highly likely evolved their operations to establish the ALPHV-ng brand following BlackMatter operations shutting down in November 2021.[162]

Whilst White Janus dominated ransomware leak site activity with an inordinately higher number of leak victims throughout 2022 with 907 victims, White Dev 101 leaked the second largest number with 228, followed by Blue Cronus (a.k.a. Conti) with 177 and White Dev 115 (a.k.a. BlackBasta) with 139.[163]

Learn more about our research into ransomware in our The R Word: Retelling the Recent Rise and Resurgence of Resilient RaaS Operators talk at SANS Ransomware Summit 2022

[158] *CTO-TIB-20220916-02A - LockBit evolves…sort of*
[159] 'LockBit Ransomware Group Augments Its Latest Variant, LockBit 3.0, With BlackMatter Capabilities', Trend Micro, https://www.trendmicro.com/en_us/research/22/g/lockbit-ransomware-group-augments-its-latest-variant--lockbit-3-.html (25th July 2022)
[160] 'RHC interviews LockBit 3.0. "The main thing is not to start a nuclear war"', Red Hot Cyber, https://www.redhotcyber.com/en/post/rhc-interviews-lockbit-3-0-the-main-thing-is-not-to-start-a-nuclear-war/ (26th July 2022)
[161] *CTO-TIB-20220121-03A - White Dev 101 does not Rust on its laurels*
[162] 'The R Word: Retelling the Recent Rise and Resurgence of Resilient Ransomware-as-a-Service Operators', PwC Threat Intelligence, https://www.youtube.com/watch?v=pZ3tyhL61rI (2nd August 2022)
[163] *CTO-SRT-20230118-01A - Ransomware report for December 2022*

Following the release of LockBit 3.0, in September 2022, White Janus experienced its own compromise involving an "allegedly disgruntled insider" who leaked the builder for LockBit Black, White Janus' 3.0 encrypter.[164] We tested the builder independently and confirmed it generated working LockBit 3.0 binaries and valid decrypters, and the binaries triggered our detection rules for both LockBit 3.0 and BlackMatter.[165] The availability of the LockBit 3.0 builder has almost certainly reduced barriers to entry for less sophisticated threat actors breaking into ransomware, or threat actors more broadly seeking to avoid attribution. Starting in October 2022, we saw a decline in the tempo of White Janus operations, which we assess to be a likely consequence of the LockBit 3.0 builder leak.

In 2022, we saw also a pattern of successful, skilled and experienced individuals shifting from dissolving RaaS operations to other opportunities within the cyber criminal ecosystem.

The maturation of this space over the past several years has resulted in the development of an enterprise-like model, wherein individuals have taken their knowledge and expertise with them as they shift across RaaS operations, and their influence has been apparent as ransomware groups emerged, fractured and rebranded. The launch of LockBit 3.0 did not conform to this pattern, which we assess is likely indicative of an emerging shift in the RaaS model, through which technology and codebases are repurposed or acquired outright.[166]

Effective defence against constantly evolving ransomware threats requires a two pronged approach. Organisations should make use of ransomware readiness frameworks to build a strategy that is agnostic of specific threats. At the same time, organisations should build an understanding of the underlying precursors and codebases powering known threats, creating opportunities to streamline detection and mitigation.

An unwelcome professionalisation of RaaS programmes

Several ransomware threat actors further professionalised their RaaS programmes in 2022, indicating the oversaturated threat landscape has prompted threat actors to employ new tactics to outmanoeuvre competitors whilst finding new ways to coerce and extort victims, who are increasingly enhancing their security measures and responses.

[164] 'LockBit ransomware builder leaked online by "angry developer"', Bleeping Computer, https://www.bleepingcomputer.com/news/security/lockbit-ransomware-builder-leaked-online-by-angry-developer-/ (21st September 2022)
[165] *CTO-SRT-20221019-01A - Ransomware report for September 2022*
[166] *CTO-TIB-20220916-02A - LockBit evolves…sort of*

Bug bounty programme and searchable databases

In September 2022, White Janus (a.k.a. LockBit) announced its first payout for its bug bounty programme, allegedly worth USD 50,000. The bug discovered would have allowed for the decryption of files encrypted by the threat actor's ransomware.[167] By the middle of 2022, both White Janus and White Dev 101 (a.k.a. ALPHV-ng, BlackCat) added search functionality to their leak sites, allowing for visitors to search victim data.[168]

High pressure tactics in ransomware negotiations

Our analysis of the leaked communications attributed to the Conti brand revealed high pressure yet mature operations where the threat actor capitalised on direct communications with victims or their representatives in negotiations. These leaks also informed our understanding of the stable of ransomware operations attributed to the threat actor we track as Blue Cronus, including Conti and Emotet. From our analysis, we identified tactics used against ransomware victims, including:

- Conti brand employees frequently referencing countdown timers associated with the scheduled release of victim data;
- Demonstrating "proof" of compromises through hidden blog posts containing victim data and file directory settings;
- Promoting discounts to victims who paid ransoms quickly and without negotiation;
- Estimating the value of stolen data and remediation costs in comparison to paying ransoms, and sharing this comparison with victims; and,
- Threatening to contact the victims' clients, partners and investors.[169]

Blue Cronus operations and updates

On 25th February 2022, a day after Russia invaded Ukraine, Blue Cronus, the threat actor behind the Conti ransomware group and which we previously tracked as White Onibi, released public statements supporting Russia's actions. Subsequently, between 27th February 2022 and 2nd March 2022, a Twitter account released a series of internal data associated with Blue Cronus operations, revealing unprecedented details and internal machinations via more than 100,000 archived instant messenger communications dating back to June 2020. Upon examination of the communications and analysis of the threat actor's operations, we ascertained the threat actors White Magician (a.k.a. TrickBot, Bazar, Anchor), White Onibi (a.k.a. Conti, Ryuk) and White Taranis (a.k.a. Emotet) were essentially component parts of the same criminal organisation, which we designated as Blue Cronus in March 2022.[170]

[167] *CTO-SRT-20221019-01A - Ransomware report for September 2022*
[168] 'Experts concerned about ransomware groups creating searchable databases of victim data', Recorded Future, https://therecord.media/experts-concerned-about-ransomware-groups-creating-searchable-databases-of-victim-data/ (14th July 2022)
[169] *CTO-SIB-20220324-01A - Negotiation tactics and internal dynamics*
[170] *CTO-QRT-2022-20220315-02A - In the leak midwinter*

These disclosures and subsequent assessments about Blue Cronus operations did not slow down the threat actor, despite an apparent phasing out and dissolution of the Conti brand. In April 2022, BlackBasta, the ransomware threat actor we track as White Dev 115, commenced operations with posts on the Russian language, cyber criminal forums Exploit and XSS. In addition to Blue Cronus using Qakbot as a delivery mechanism, White Dev 115 also consistently used Qakbot to gain initial access into victim networks. We have since assessed White Dev 115 to be highly likely part of the Blue Cronus portfolio of ransomware variants.[171]

Sizing up the precursors

Cyber criminals continued to be some of the most agile and forward-evolving threat actors, especially when responding to enhanced security practices implemented across industry, and this is reflected in precursor activity seen in 2022.

One trend of note from the past year can be seen in the response some cyber criminals had to the July 2022 implementation of Microsoft's policy to block macros by default on Microsoft Office documents downloaded from the Internet,[172] which we detail later in this report – Attack insights and trends: No macros, no problem? The threat actors behind Bumblebee (i.e. Blue Cronus), IcedID (i.e. White Khione) and Qakbot (i.e. White Horoja) developed workarounds in 2022 to counter the changes implemented by Microsoft, resulting in more bespoke and altogether more sophisticated attack processes. These processes involve multiple stages which make use of a combination of ISO and LNK files to drop and execute their malware loaders on victim machines.[173]

Bumblebee

In the first half of 2022, the initial stage malware loader known as Bumblebee emerged, developed by Blue Cronus to replace TrickBot and BazarLoader. Bumblebee quickly became a prolific capability used in ransomware attacks, with embedded advanced anti-virtualisation techniques and the ability to deliver post exploitation kits such as Metasploit or Cobalt Strike. Bumblebee is delivered almost exclusively through phishing attacks, quite often in hijacked threads to appear more legitimate to victims, and masquerading as invoices, meeting agendas and other documentation intended to elicit responses from victims. The emails also contain "personal passwords" for victims, further luring them into opening a password protected malicious ZIP archive or ISO file. Once the victim opens the malicious file, Bumblebee is loaded onto the victim machine through an LNK file.[174]

[171] *CTO-SIB-20221222-01A - Blue Cronus and Black Basta*
[172] 'Macros from the internet will be blocked by default in Office', Microsoft, https://learn.microsoft.com/en-us/deployoffice/security/internet-macros-blocked (11 October 2022)
[173] *CTO-TIB-20221014-01A - ISO-lemnly swear, that we are up to no good*
[174] *CTO-TIB-20220729-02A - New Queen of the APIary*

IcedID

IcedID is a banking trojan turned malware delivery system we attribute to White Khione, and it is used by a number of threat actors as an initial entry point into a victim system or network. In 2022, following the implementation of macro default disabling by Microsoft, White Khione updated IcedID to move away from the use of malicious Excel spreadsheets with macros in favour of ISO files. These files were coupled with White Khione's popular "Fake Legal Threat" phishing campaign, which it has consistently used to deliver its payloads.

Qakbot

Qakbot (a.k.a. Qbot, Pinkslipbot) is controlled by the threat actor we track as White Horoja and has been in operation since 2007. Originating as a banking trojan, in 2021 Qakbot began evolving into a fully modular malware toolkit, boasting loader capabilities, a custom packer, anti-sandbox failsafes and anti-debug techniques. Whilst Qakbot is still delivered via phishing attacks leveraging lures of all kinds, in 2022 it moved away from its use of macro-enabled Office files to instead being embedded inside malicious MSIs and packaged within password protected ZIP archives.[175]

White Taranis' reactivation by Blue Cronus

White Taranis (a.k.a. Emotet) re-emerged in late 2021 upon reactivation by Blue Cronus. Throughout the first half of 2022, White Taranis operations proceeded at a steady pace, with brief pauses to implement upgrades to its C2 infrastructure, spam engine and system reconnaissance capabilities.[176] Blue Cronus also revived some older functionality, including its payment card credential stealer.[177] Like other members of the Blue Cronus "stable", the shutdown of the Conti ransomware operation had no immediate impact on White Taranis campaigns; however, by mid-July 2022, White Taranis operations had come to an abrupt halt and remained dormant until early November 2022. Spam campaigns resumed in earnest in November 2022, with payloads consisting of malicious Microsoft documents containing macros to download and execute a White Taranis binary on victim machines.

After Microsoft changed its default for macros, Blue Cronus sought to bypass this protection by instructing recipients to copy malicious attachments to their Templates folder and open the document from that location. This action removed the Mark of the Web (MotW) flag from the malicious document, and once opened, the file would no longer open in Protected View, enabling the macros to execute and install the Emotet binary.[178] It remains to be seen if the threat actor persists with this technique, or switches to methods used by Blue Cronus for Bumblebee and IcedID delivery.

[175] *CTO-TIB-20220525-01A - Duck, Duck, Bot: Qakbot evolves!*
[176] *CTO-TIB-20221104-01A - More modules, More Problems*
[177] *CTO-QRT-20220728-01A - You can't keep a good botnet down*
[178] *CTO-QRT-20221103-01A - Emotet resumes operations*

Detection methods for common techniques seen in Bumblebee, Qakbot and IceID campaigns

In delivering these loaders, threat actors have converged on an effective attack path which presents itself with slight variations for each campaign. Regardless of these variations, these attack paths have intersecting nodes. These nodes are where we can build detections and pinpoint evidence of possible malicious activity.

Threat actors have been observed delivering links to Microsoft OneDrive or Google Drive to entice a user to download an archive file. This is effective because these domains are allowlisted by most organisations. Alternatively, threat actors use a technique called HTML smuggling, where a malicious HTML file is delivered to a user with a prompt to open the file. The HTML file contains an embedded and obfuscated payload, and using JavaScript, the browser assembles and writes it to the user's machine. With a log of a user receiving an email attachment of a single HTML file, a chained detection can be built upon the subsequent execution of an HTML file by a browser, where the file originates from the user's downloads directory.

As mentioned, password protected archives are popular with threat actors. If an organisation analyses its archive tooling and extracts the command line parameters associated with decryption, informational detections can be built for a user unpacking an encrypted archive to disk. Such archives will often contain an ISO file, which once mounted presents a shortcut file with launch arguments that engage the execution of the payload. The use of DLL payloads has also grown in popularity, and therefore threat actors look to abuse system binaries such as `rundll32.exe` for payload execution. Detections looking for `rundll32.exe` launching a DLL on a non C:\ drive are generally robust, so attackers attempt to ship a legitimate copy of `rundll32.exe` to perform the same action. To detect this, organisations can look for its execution outside of the System32 directory, or in case it has been renamed, build detections for command line arguments that are unique to the binary with the absence of its process name.

Upon execution, we have observed payloads rapidly attempting to disable features of Windows Defender and add exclusions for themselves. In response to these behaviour patterns, we signatured the registry changes that payloads make to enforce these configuration changes.

Hackers, fraudsters and stealers

Whilst cyber criminals demonstrated quick shifts to counter Microsoft's default macro settings in 2022, other threat actors also remained agile in their tactics for evading multifactor authentication (MFA). With threat actors increasingly encountering MFA protections, the demand has risen for MFA bypass capabilities, such as MFA fatigue tactics, modified credential stealers and enhanced Phishing-as-a-Service (PHaaS) offerings.

Threat actors motivated by other reasons also attempted to evade MFA, which we detail later in this report – Attack insights and trends: More MFA, more evasion.

LAPSUS$ in judgement

The data stealing extortion group we track as White Dev 111 (a.k.a. LAPSUS$ Group) gained international notoriety in 2022 for several high profile attacks on large organisations, including Samsung, NVIDIA and Microsoft, as well as its claims of breaches into Okta, Uber and Rockstar. White Dev 111 used social engineering, MFA fatigue and other attacks preying on the human element of security and employing "smash and grab" tactics to target high profile organisations.[179] White Dev 111 first appeared in December 2021 after the threat actor successfully compromised Brazil's Ministry of Health,[180] claiming to have stolen 50 TB of data. White Dev 111 advertised its victims on a Telegram channel, which it also used to post recruitment adverts for "Employees/Insiders" at several major technology, gaming and telecommunications organisations requesting access to company "VPN or Citrix" logins.[181]

Whilst numerous countries have arrested teenagers allegedly affiliated with White Dev 111 (a.k.a. LAPSUS$ Group) operations,[182, 183, 184] the threat actor's TTPs and motivations nonetheless remain of concern to organisations around the world.

Liars, cheats and thieving raccoons

Credential stealing malware thrived in the underground economy in 2022, with systems like RedLine,[185] Raccoon[186] and Vidar[187] dominating the market for compromised credentials. This was largely because the developers of these information stealers (a.k.a. infostealers) adjusted their tooling amidst a surge in organisations implementing MFA to protect their environments.

[179] *CTO-QRT-20220920-01A - Uber and Rockstar breaches*
[180] 'Brazil health ministry website hit by hackers, vaccination data targets', Reuters, https://www.reuters.com/technology/brazils-health-ministry-website-hit-by-hacker-attack-systems-down-2021-12-10/ (10th December 2022)
[181] *CTO-TIB-20220406-01A - LAPSUS$ Group has entered the chat*
[182] 'Lapsus$: Oxford teen accused of being multi-millionaire cyber-criminal', BBC News, https://www.bbc.com/news/technology-60864283 (24th March 2022)
[183] 'UK police arrest teenager suspected of Uber, GTA 6 hacks', TechCrunch, https://techcrunch.com/2022/09/26/london-police-arrest-uber-rockstar/ (26th September 2022)
[184] 'PF prende brasileiro suspeito de integrar organização criminosa internacional', Brazilian Ministry of Justice and Public Security, https://www.gov.br/pf/pt-br/assuntos/noticias/2022/10/pf-prende-brasileiro-suspeito-de-integrar-organizacao-criminosa-internacional (19th October 2022)
[185] *CTO-TIB-20220209-01A - The Rise of RedLine*
[186] *CTO-TIB-20220914-02A - Raccoon Stealer 2.0*
[187] *CTO-TIB-20230113-01A - Vidar Stealer*

Throughout 2022, more and more developers of credential stealing malware added or enhanced capabilities to syphon session cookies, which in certain circumstances facilitated MFA bypassing.

In March 2022, Raccoon Stealer suddenly ceased operations after the malware developers reported their lead was killed in Ukraine during the Russian invasion.[188] By mid-2022, Raccoon Stealer developers assured their criminal customer base that despite the major setback, they would continue the development of a new version of Raccoon Stealer boasting enhanced capabilities; however, in October 2022, the US government announced the lead developer, a Ukrainian national, was not killed in Ukraine but was instead arrested by Dutch police in March 2022, and Raccoon Stealer infrastructure was subsequently dismantled in a joint effort by international law enforcement agencies, forcing the developers to restart and relaunch operations.[189]

Phishing with dynamite

In 2022, cyber criminals continued to rely on tried-and-true phishing tactics, which consisted of clever messaging and a reliance on single factor authentication. When forced to adapt, numerous threat actors took advantage of free-to-use services largely intended for security practitioners, such as Glitch and Gophish, which provide both infrastructure and tooling to create and distribute phishing emails and develop phishing landing pages. Threat actors engaging in phishing attacks also continued to demonstrate little reservation in masquerading as government or law enforcement agencies. One threat actor went as far as using the arrest of another well known scammer, Ramon Abbas (a.k.a. `HushPuppi`), to impersonate the US Department of Justice's Office of Victims of Crime in further attempts to victimise targets and steal their private financial information.[190]

Not just a Glitch

Creating and maintaining infrastructure to conduct phishing attacks is an expensive and labour-intensive operation, and it can be especially frustrating for threat actors when their infrastructure is taken down by hosting providers or blocked by web browsers. For this reason, threat actors seek free and easy-to-use platforms and services for their phishing operations. Glitch was one such free-to-use, cloud-based software development platform used by West Africa-based business email compromise (BEC) threat actors for this purpose. The Glitch platform has a free tier which allows users to quickly deploy public webapps with a Glitch-provided hostname. The threat actors combined Glitch with an older phishing kit known as LogoKit to create fake webmail

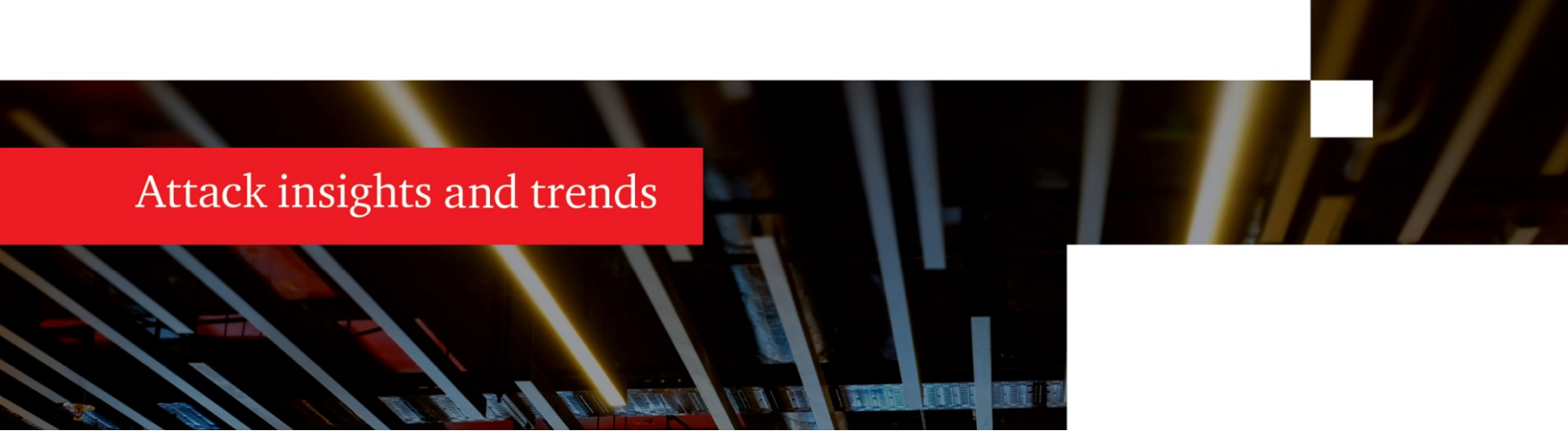
[188] *CTO-TIB-20220914-02A - Raccoon Stealer Returns*
[189] 'United States of America v. Mark Sokolovsky', US Department of Justice, https://www.justice.gov/usao-wdtx/page/file/1546626/download (26th September 2022)
[190] 'Nigerian Man Sentenced to Over 11 Years in Federal Prison for Conspiring to Launder Tens of Millions of Dollars from Online Scams', US Department of Justice, https://www.justice.gov/usao-cdca/pr/nigerian-man-sentenced-over-11-years-federal-prison-conspiring-launder-tens-millions (7th November 2022)

login pages and capture user credentials, which were then used to gain access into victim networks.[191]

Whilst not particularly new, PHaaS remains a viable model and resource for cyber criminals, with 2022 seeing several new providers offering in-demand features and functionality, including the EvilProxy, Caffeine and Robin Banks toolkits. EvilProxy emerged in mid-2022, operating as an adversary-in-the-middle (AitM) between phishing victims and enterprise login portals, and providing cyber criminals a graphical user interface (GUI) to customise and automate phishing campaign deliveries, all for a low use fee. EvilProxy facilitates both credential and cookie stealing capabilities for bypassing MFA and has advertised its ability to compromise sign-on portals for large enterprises, such as Google, Microsoft and LinkedIn, as well as other services.

The point-and-click nature of EvilProxy is one product in a growing market within the cyber criminal ecosystem, encouraging the development of on-demand and fee-based capabilities and further lowering the barrier to entry for a wide range of threat actors to engage in attacks.

[191] *CTO-SIB-20220811-01A - A glitch in the BEC system*



Attack insights and trends

Throughout 2022, new technologies and common vulnerabilities permeated the dynamic between attackers and defenders, with each seeking an advantage and highlighting the need for defence in depth. Threat actors increasingly leveraged enhanced tooling and frameworks in their attacks, as well as modified their TTPs to outmanoeuvre security practices implemented by defenders. Threat actors paired these shifts with their continued use of tried-and-true methods, such as exploiting exposed instances of remote desktop protocol (RDP) and systems not yet secured with MFA.

Tooling and frameworks

Throughout 2022, numerous examples of tooling and frameworks were discussed and tracked across industry, and we observed a greater awareness of how these are used by legitimate red teams and abused by malicious attackers.

As a defender, these frameworks bring challenges due to their rapid evolution; however, they also bring detection opportunities. In some cases, once a defender detects the use of a particular framework, other frameworks could be detected as well with the same or similar approach.

Although some frameworks gained notoriety across industry in 2022, Cobalt Strike remained the most abused post exploitation framework, used by a wide range of threat actors. Detecting the use of a particular framework in isolation is likely to remain a challenge for defenders and will likely become more difficult in the coming years.

Detecting Cobalt Strike

The default configurations of Cobalt Strike are well known and straightforward to detect, for example the default DNS C2 using .stage. in the domain name. The following network detection rule looks for the standard format, which typically begins with a query for aaa.stage.*

Network

```
alert dns any any -> any any (msg:"[PwC] Generic - CobaltStrike - DNS query for
.stage."; \
    dns_query; content:".stage."; \
    pcre:"/^[a-z]{3}\.stage\.[0-9]+\.(?:[a-z0-9-]+\.)+[a-z]{2,4}$/"; \
    classtype:domain-c2; \
    metadata:copyright,Copyright PwC Threat Intelligence 2017; metadata:tlp green; \
    metadata:confidence Medium; metadata:efficacy Medium; \
    metadata:mitre,T1071/004; \
    metadata:author RM; metadata:created 2020-07-07; \
    sid:200100001; rev:2020070701;)
```

Brute Ratel

Brute Ratel is a commercial C2 framework that became more well known as 2022 progressed due to its use by several threat actors.[192] Various versions of Brute Ratel were leaked and cracked in the past year, and the framework can be customised and extended with ease. By default, Brute Ratel boasts a variety of features which can be used to evade detection, such as unhooking Endpoint Detection and Response (EDR)/antivirus (AV), a variety of C2 mechanisms and indirect execution of APIs.

[192] 'When Pentest Tools Go Brutal: Red-Teaming Tool Being Abused by Malicious Actors', Palo Alto Unit 42, https://unit42.paloaltonetworks.com/brute-ratel-c4-tool/ (5th July 2022)

Detecting Brute Ratel

As a defender, there are various defaults allowing for the detection of Brute Ratel, whether in memory/on-disk - for example using YARA - or network traffic that features the default SSL certificate or domain.

YARA

```
rule Brute_Ratel_PE_Badger_API_Loading_Routine : Heuristic_and_General
{
    meta:
        description = "Detects Brute Ratel Badger payloads (PE and DLL) based on a
unique routine used to dynamically load APIs"
        TLP = "AMBER"
        author = "PwC Threat Intelligence"
        copyright = "Copyright PwCIL 2022 (C)"
        created_date = "2022-09-29"
        modified_date = "2022-09-29"
        revision = "0"
        hash = "4de333f164d70b59849c3aa12a9c95cdcbecae3023386ee08c15b38874260941"
        hash = "dc71c5721fa6b3148a3a0564931dc063d03694ca57aa61e8c2532b5a565b2548"
        hash = "ef803ea871c974623ceb678548c938826b683c857adc85a6bf8af34c8b61fc52"

    strings:
        // 8B5324        MOV EDX,DWORD PTR [RBX+24]
        // 4D01DB        ADD R11,R11
        // 8B431C        MOV EAX,DWORD PTR [RBX+1C]
        // 4D01D3        ADD R11,R10
        // 410FB71413    MOVZX EDX,WORD PTR [R11+RDX]
        // 498D1492      LEA RDX,[R10+RDX*4]
        // 8B0402        MOV EAX,DWORD PTR [RDX+RAX]
        // 4C01D0        ADD RAX,R10
        $ = {8B53244D01DB8B431C4D01D3410FB71413498D14928B04024C01D0}

    condition:
        all of them
}
```

Network

```
alert dns any any -> any any (msg:"[PwC] Generic - Brute Ratel - C2 node
evasionlabs[.]com in DNS query"; \
    dns.query; \
    content:".evasionlabs.com"; endswith; \
    threshold: type limit, track by_src, count 1, seconds 3600; \
    classtype:domain-c2; \
    metadata:copyright,Copyright PwC Threat Intelligence 2022; \
    metadata:tlp green; metadata:confidence High; metadata:efficacy Low; \
    metadata:mitre,T1071/004; \
    metadata:author RM; metadata:created 2022-09-29; \
    sid:222092910; rev:2022092901;)
```

Sliver

Unlike Brute Ratel, Sliver is an open source framework, allowing those using it to more easily customise the framework in use. Sliver supports a range of C2 mechanisms, including mutual Transport Layer Security (mTLS) and Wireguard, and supports beacon object files (BOFs), making it possible to reuse Cobalt Strike plugins.

Detecting Sliver

The mTLS configuration is hard coded and the JARM fingerprint is consistent (`28d28d28d00028d00043d28d28d43d47390d982d099a542ccbc90628951062`); if a defender is able to inspect HTTPS traffic, then the server response headers are consistent, as are the format of the HTTP requests. Wireguard traffic is also very signaturable and easy to detect in network traffic.

YARA

```
rule Sliver_Protobuf_Symbol : Heuristic_and_General
{
    meta:
        description = "Detects symbol in Sliver implants (PE, ELF, Mach-O and
shellcode) referencing a custom protobuf module"
        TLP = "AMBER"
        author = "PwC Threat Intelligence"
        copyright = "Copyright PwCIL 2022 (C)"
        created_date = "2022-10-18"
        modified_date = "2022-10-18"
        revision = "0"
        hash = "41cf473fe535b932c68e9f295680fe228cde0094a8bac70ccb68c21aaff22188"
        hash = "c12c33111b41bf2be458004d532f1255fd734057d2c7bf59e0877e31dbedfd4e"
        hash = "3b4c57e04422825609bc70dfa5bf741cded6961df87369b530c45720eee828fd"
        hash = "4c668595d6767e9cdb68f875aab9d4d39ae0ff94d94e76dc301eb336f1d74096"
        reference = "https://github.com/BishopFox/sliver"

    strings:
        $ = ".sliverpb."

    condition:
        // Note, you can remove these file signature checks to wider the rule further
        (
            // PE
            uint16(0) == 0x5A4D or
            // Shellcode
            uint32be(0) == 0x4883e4f0 or
            // Mach-O
            uint32be(0) == 0xcffaedfe or
            // ELF
            uint32be(0) == 0x7f454c46
        ) and
        any of them
}
```

Network

```
alert udp any any -> any any (msg:"[PwC] Policy - Tunnelling - Wireguard VPN client
handshake"; flow:from_client; dsize:148; \
    content:"|01 00 00 00|"; startswith; \
    content:"|00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00|"; endswith; \
    flowbits:set,PwC.Policy.Tunnelling.Wireguard; target:src_ip; \
    reference:md5,b82a587befc34c0db00eed5c4117d88d343b8b895f03fc409a55d9240cf9fde1; \
    classtype:pup-activity; \
    metadata:copyright,Copyright PwC Threat Intelligence 2022; metadata:tlp green; \
    metadata:confidence High; metadata:efficacy Low; \
    metadata:mitre,T1133; \
    metadata:author RM; metadata:created 2022-05-04; \
    sid:222050432; rev:2022050401;)
```

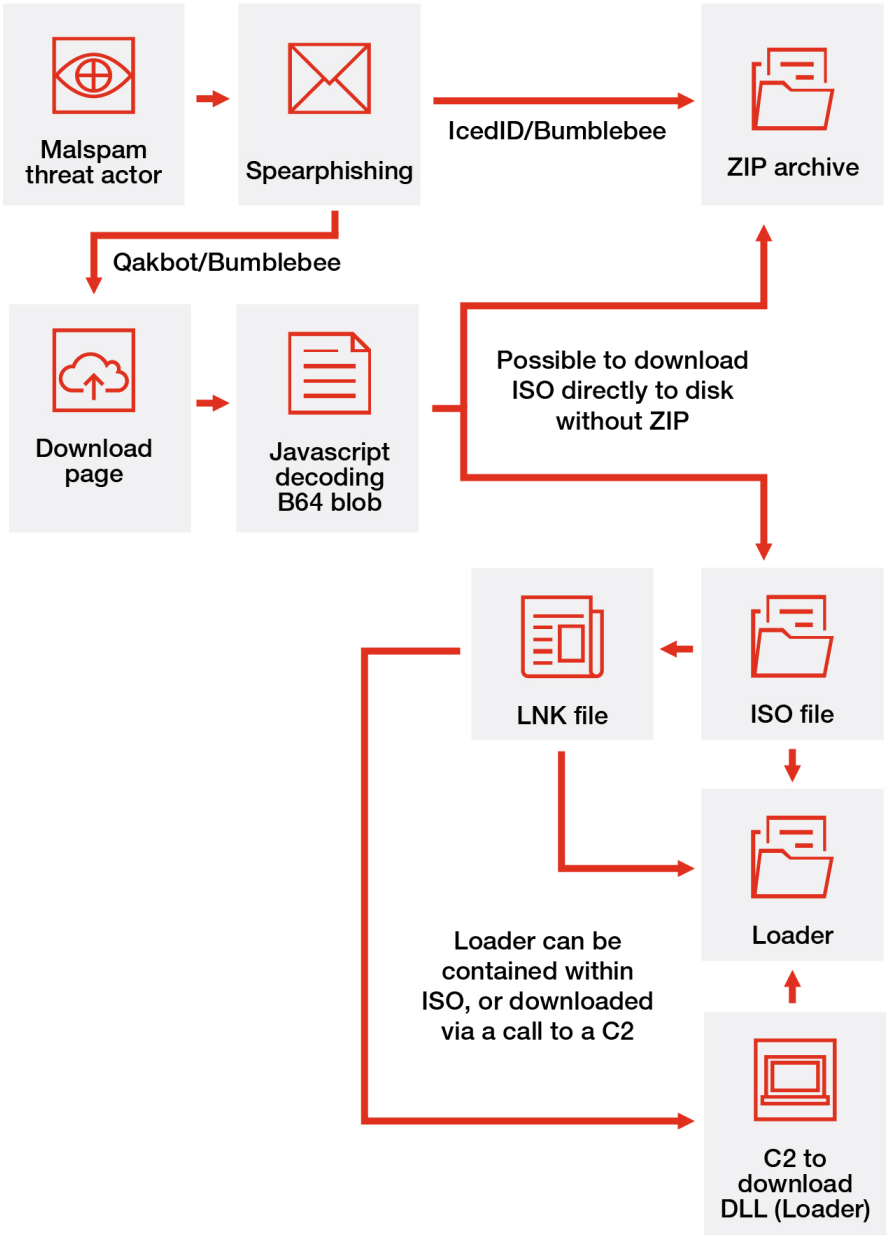
No macros, no problem?

Threat actors have historically relied on macros to execute malware they deliver to victims, such as through malicious documents attached to phishing emails. Without malicious files having the ability to execute macros automatically without victim intervention, threat actors have been forced to rely on other self-executing methods, avoiding as much victim interaction and system interdiction as possible. With Microsoft's 2022 update to disable Mark of the Web (MotW) by default,[193] we observed threat actors having to adapt their targeting of organisations with malicious documents relying on the execution of macros. Further, threat actors ranging in resources, sophistication and motivation have sought alternative ways to gain initial access to targets, as seen in an infection vector revolving around using:

- ISO files (which effectively act as archive files) to deliver malicious payloads; and,
- LNK (shortcut) files to masquerade as legitimate documents, but in reality execute malicious payloads.

[193] 'Macros from the internet will be blocked by default in Office', Microsoft, https://learn.microsoft.com/en-us/deployoffice/security/internet-macros-blocked (11th October 2022)

Example infection chain using ISO + LNK files



Detecting potentially malicious ISO and LNK files

ISO files serve the legitimate purpose of replicating a physical disk image. To detect ISO files containing malware, we must consider the profile of a legitimate ISO file and look for deviations from this baseline. For example, in an enterprise environment, ISO files may be handled by administrative accounts for large software installation operations. With this in mind, detections can be built for ISO file creations under standard user accounts, or ISO files of a small size. We can also signature commonly abused applications writing ISO files to disk. Particularly noteworthy applications to signature for this behaviour include email clients and web browsers, as those tend to be the primary avenue for phishing.

When an ISO file is opened from within an archive, temporary files are created on disk which indicate this, and hence alerts from these file creation events can help us detect the early stages of an attack. This same mechanism can be used to detect LNK files within archives. For many organisations, a LNK file in an archive may occur with some frequency, so alerts must be correlated with other behaviours to warrant incidents, but for some organisations this in itself is worth further analysis given its popularity with threat actors.

More MFA, more evasion

As more organisations adopt MFA protections for privileged access and identity access management (IAM), threat actors have shifted to evasion techniques ranging from social engineering, as seen in the case of White Dev 111 employing MFA fatigue attacks against its victims, to technical bypass techniques, such as those integrated into malware commonly used by cyber criminals as well as more sophisticated threat actors.

One such threat actor is Blue Dev 5 (a.k.a. NOBELIUM), which we analysed in 2022 during an incident response case and found the threat actor had evaded MFA protections by exploiting a dormant account to gain access to the victim's Microsoft Azure Active Directory (AD) environment. Blue Dev 5 authenticated to the account using valid credentials, with the dormant account having been established before the victim implemented MFA. Blue Dev 5 then enrolled a new MFA method, a software OATH token, using the compromised account.[194]

[194] *CTO-QRT-20220720-01A - Blue Dev 5 - MFA Evasion using dormant accounts*

Lessons from the Blue Dev 5 (a.k.a. NOBELIUM) MFA evasion incident

Our analysis of this incident included the following Blue Dev 5-associated indicator of compromise (IoC) seen in July 2022, which can be queried in historical logs and added to detection alerts:

- `198.244.224[.]89`[195]

We recommend configuring detections for MFA enrolments for users which have not logged in for at least 14 days. Doing so would detect activity similar to that described in this incident.

Further, we recommend enforcing MFA in Microsoft cloud environments with a secure authentication method, such as number matching, and proactively identifying accounts which do not currently have MFA enrolled, such as using the following command provided by the Microsoft Azure AD Incident Response PowerShell Module:

- `Get-AzureADIRMfaAuthMethodAnalysis`[196]

Targeting the clouds

More threat actors are targeting cloud environments to compromise victims, likely in response to organisations increasingly integrating the technology, with threat actors preying on vulnerabilities or misconfigurations to unlock troves of data. Earlier in 2022, we responded to a separate Blue Dev 5-related incident, which involved the threat actor gaining initial access into the victim's cloud environment through the compromise of its Cloud Service Provider (CSP).[197] The CSP had Delegated Administrator[198] permissions for the victim's Microsoft Azure AD and O365 tenant, effectively providing the threat actor with administrative access to the victim's Microsoft cloud environment.

Using this access, Blue Dev 5 added a password credential to an Azure AD Service Principal[199] used by a backup application, allowing the threat actor to then log into the victim environment with the same permissions as those available to the legitimate backup application. Blue Dev 5 then used these credentials to authenticate as the backup application and make Exchange Web Service (EWS)[200] cloud API calls to Exchange Online (O365), with the backup application privileges opening the possibility for Blue Dev 5 to access and exfiltrate the emails of all of the victim's O365 user accounts. Blue Dev 5

[195] *CTO-QRT-20220720-01A - Blue Dev 5 - MFA Evasion using dormant accounts*
[196] 'Azure AD Incident Response PowerShell Module', Microsoft, https://github.com/AzureAD/Azure-AD-Incident-Response-PowerShell-Module
[197] 'What is a cloud service provider', Microsoft, https://azure.microsoft.com/en-us/resources/cloud-computing-dictionary/what-is-a-cloud-provider/
[198] 'Delegated admin privileges in Azure AD', Microsoft, https://learn.microsoft.com/en-us/azure/active-directory/enterprise-users/directory-delegated-administration-primer (12th March 2023)
[199] 'Application and service principal objects in Azure Active Directory', Microsoft, https://learn.microsoft.com/en-us/azure/active-directory/develop/app-objects-and-service-principals (15th December 2022)
[200] 'Explore the EWS Managed API, EWS, and web services in Exchange', Microsoft, https://learn.microsoft.com/en-us/exchange/client-developer/exchange-web-services/explore-the-ews-managed-api-ews-and-web-services-in-exchange (13th June 2022)

mirrored these methods in a subsequent period of activity against the same victim, compromising a separate CSP.[201]

Lessons from the Blue Dev 5 (a.k.a. NOBELIUM) CSP compromise incident

Whilst we assess the following IoCs analysed in this incident are no longer in use, we supply them nonetheless to assist in the querying of historical logs and alerting:

- `193.8.172[.]208` - Seen July 2021 through August 2021
- `18.130.157[.]66` - Seen in July 2021
- `18.169.208[.]15` - Seen January 2022 through February 2022
- `79.143.87[.]14` - Seen in March 2022[202]

Further, this case enabled us to develop a series of recommendations for hardening Microsoft Azure AD and O365 environments against Blue Dev 5 and other threat actors utilising similar TTPs, such as:

- Remove Delegated Administrator permissions from partner relationships with managed service providers (MSPs) and other third parties, or use Granular Delegated Administrator Privileges[203] to only allow third parties time-bound administrative access where strictly required;
- Configure strong methods of MFA for all users (e.g. push notifications with number matching);[204]
- Onboard logs from Azure AD and O365 to an existing SIEM or new Microsoft Sentinel deployment;
- Configure detection rules for techniques commonly used to compromise Azure AD and O365;
- Audit and secure the use of privileged accounts in Azure AD and O365;
- Audit Azure AD Service Principals and applications for credentials and sensitive permissions, and monitor their ongoing use; and,
- Secure Service Principals by using Conditional Access rules[205] to restrict logins to sensitive Service Principals to an allowlist of IP addresses.[206]

Additional insights from our incident response cases

In addition to the incident response cases already highlighted in this report, we analysed our broader dataset for additional trends and insights. In 2022, 63% of the incident response cases we analysed resulted from attacks by financially motivated threat actors,

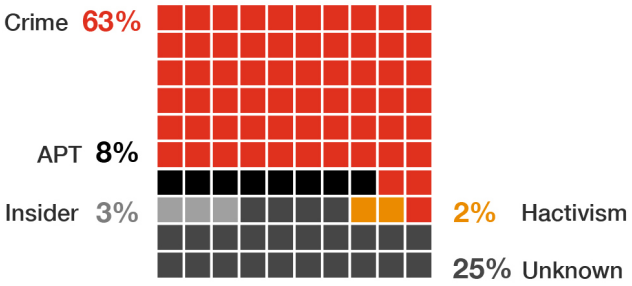
[201] *CTO-TIB-20220429-01A - Bearing down on the Clouds*
[202] *CTO-TIB-20220429-01A - Bearing down on the Clouds*
[203] 'Introduction to granular delegated admin privileges (GDAP)', Microsoft, https://docs.microsoft.com/en-us/partner-center/gdap-introduction (8th August 2022)
[204] 'How to use number matching in multifactor authentication (MFA) notifications (Preview) - Authentication Methods Policy', Microsoft, https://docs.microsoft.com/en-us/azure/active-directory/authentication/how-to-mfa-number-match (30th November 2022)
[205] 'Conditional Access for workload identities preview', Microsoft, https://docs.microsoft.com/en-us/azure/active-directory/conditionalaccess/workload-identity (21st November 2022)
[206] *CTO-TIB-20220429-01A - Bearing down on the Clouds*

and nearly half of these cases involved ransomware attacks. Of the ransomware cases we analysed in 2022, the top three sectors impacted were manufacturing, construction and retail, aligning to broader trends we observed from ransomware leak site data over the course of 2022.

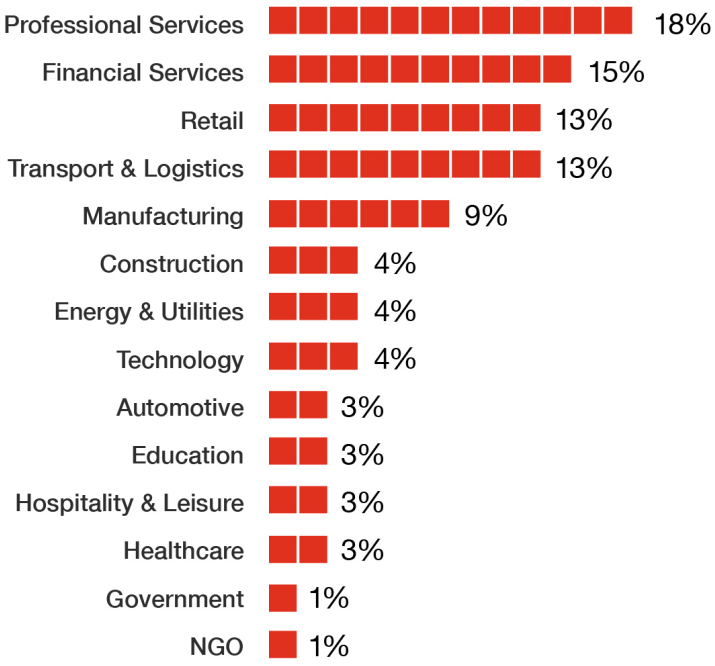
Of all the incident response cases we analysed in 2022, the top five sectors impacted were professional services, financial services, transport and logistics, retail and manufacturing.

We could not ascertain a motivation for about a quarter of all of the cases we analysed in 2022, which was higher than the 7.5% of cases we categorised in this manner in 2021. This is likely due to detection and response efforts occurring earlier in the intrusion lifecycle, but possibly also related to the trend we saw across threat actors increasingly using shared capabilities and tooling and enhancing their TTPs in 2022.

Incident response cases we analysed by threat actor category in 2022



Incident response cases we analysed by sector in 2022

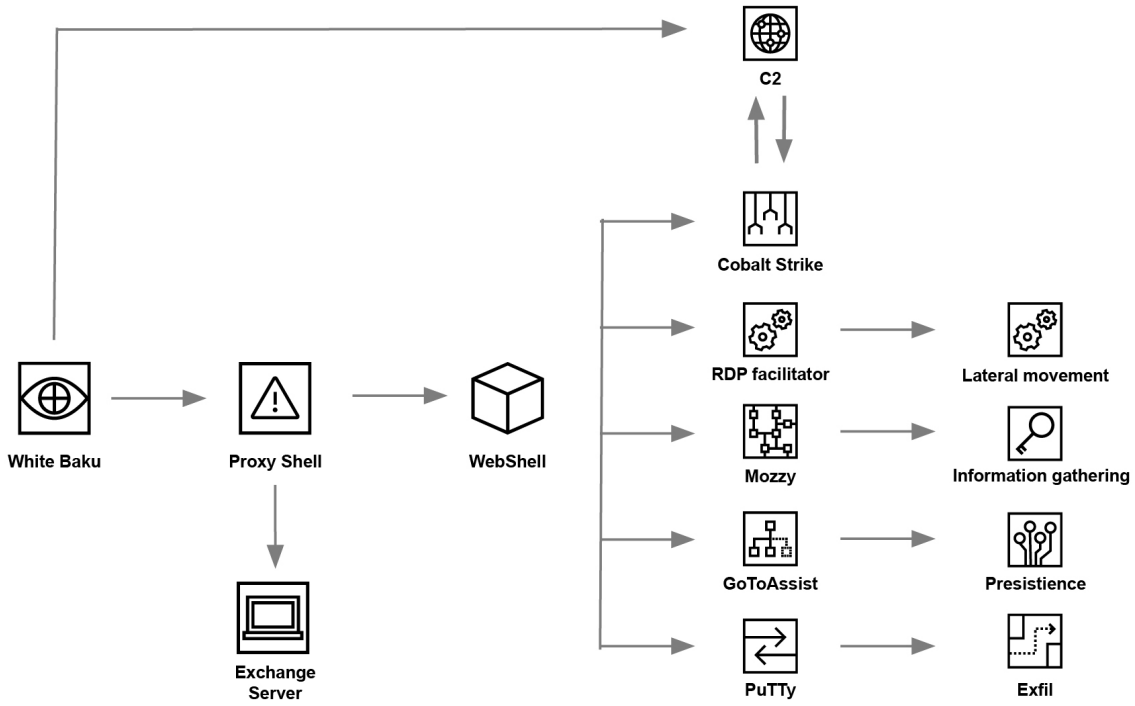


It is imperative for organisations to record and maintain as much telemetry as possible from the entire security stack, as being able to review historical network metadata, or host activity, will assist incident responders with understanding the impact of an attack not detected at the time. The data volumes for key log and telemetry types are relatively low and are well suited to long term, archival-type storage.

White Baku case study

In March 2022, we responded to an incident involving White Baku, the threat actor behind Cuba ransomware.[207] White Baku gained initial access to the victim by exploiting ProxyShell vulnerabilities to drop webshells on Microsoft Exchange servers, which aligned with other publicly reported ransomware incidents attributed to this threat actor. White Baku then leveraged Cobalt Strike for C2 and lateral movement, deploying Mozzy, a custom piece of malware designed to gather information about the victim's EDR, and RDP Facilitator, a piece of malware used to configure backdoors to facilitate RDP. To reinforce its foothold in the victim's network, White Baku installed the GoToAssist remote support tool. For collection and exfiltration, White Baku installed WinRAR to compress files and PuTTY Secure Copy (PSCP) for file transfer and data exfiltration, enabling White Baku to steal files from the victim before encrypting the system. Finally, White Baku used PsExec for the final ransomware deployment.

White Baku intrusion chain



[207] *CTO-TIB-20220608-01A - White Baku grabs a foothold*

Lessons from the White Baku (a.k.a. Cuba) incident involving ProxyShell

We drew insights from several aspects of this White Baku incident, spanning through several stages of its attack chain and potential detection and mitigation strategies.

- *Initial access:* Detecting unusual processes spawning from web server processes, such as ProxyShell, or unusual file writes originating from web server processes is a key strategy to identify web shell activity in general. This is frequently an attacker's first point of access into the network, and followed by learning more about the victim's environment. Defenders can search for child processes and commands associated with network discovery which can surface such suspicious activity on a web server.
  MITRE ATT&CK T1505.003 - Server Software Component: Web Shell

- *Persistence:* It is critical to monitor for the installation of remote access tooling (e.g. GoToAssist), not only because of the simple detections that can be implemented, but also because remote desktop tooling is usually deployed in the early stages of an attack. With an understanding of the remote administrative tooling that is approved by policy in allowlists, detection rules can be created to look for common remote administrative tools that fall outside of this policy. Should a savvy attacker install approved remote administrative tooling, then detections can be built to identify anomalous installations, such as userland installations or installations conducted by unexpected accounts. In addition to monitoring for installation, defenders can also look for specific command lines of the installation process, as some tools leverage installers with specific command line flags which should raise suspicions. Examples are a silent flag (i.e. no install user interface (UI)), which prevents user visibility of the installation taking place, or flags that add the utility to Startup, which is also unusual for remote support tooling.
  MITRE ATT&CK T1219 - Remote Access Software

- *Lateral Movement:* PsExec is a highly popular tool amongst ransomware actors. Intended for remote administration, PsExec's ability to execute code on remote systems over Server Message Block (SMB) is ideal for ransomware propagation. If PsExec is not an authorised administrative tool, defenders can monitor for any executions of PsExec. Users performing legitimate executions can simply be guided to alternative means of remote management. PsExec is frequently renamed by adversaries, so looking for its bespoke command-line parameters or the registry artefact associated with the acceptance of its end-user licence agreement (EULA) in the absence of its standard process name is usually a clear sign of an adversary trying to avoid detection. If PsExec is widely used by administrators on the network, then more complex logic will need to be deployed to identify suspicious PsExec activity. PsExec is also built as a lateral movement feature of post exploitation tools such as Metasploit and Cobalt Strike, each of which have implemented PsExec in slightly different ways. Detections must be built to monitor for the remote service processes that are executed by each post exploitation tool. Defenders should use regular expressions to capture the randomness that these tools attempt to inject into the operation. MITRE ATT&CK T1021.002 - Remote Services: SMB/Windows Admin Shares

- *Collection:* Once more, it's important to stress that whilst compression tools like WinRAR and others are perfectly legitimate, they are also used by cyber criminal threat actors and advanced persistent threats alike. Detecting when such tools are downloaded from the Internet, or installed in specific folders, such as %TEMP%, may be a useful heuristic to identify suspicious activity that can be flagged for review.
  MITRE ATT&CK T1560.001: Archive Collected Data: Archive via Utility

- *Exfiltration:* Similar to the compression tools utilised for collection as described above, actors facilitating data exfiltration via legitimate file transfer tools, such as PuTTY Secure Copy (PSCP), can often blend in with legitimate activity. To differentiate such exfiltration activity from legitimate file transfer activity, it may be useful to specifically alert on origins, destinations and volumes of outgoing data transfers that are unusual for the environment. Additionally, endpoint signatures may be created to detect file transfer tools that are not in line with the organisation's policy. Similarly, processes which exhibit behaviour identical to that of known benign file transfer tools, but are using unusual process names, may be alerted on through endpoint signatures.
  MITRE ATT&CK T1048.002 - Exfiltration Over Alternative Protocol: Exfiltration Over Asymmetric Encrypted Non-C2 Protocol

Black Artemis case study

In late 2022, we responded to a long term, persistent intrusion against an organisation in the chemicals sector by the North Korea-based threat actor Andariel (a.k.a. Stonefly, Silent Chollima), which we track internally as a subgroup of Black Artemis. The threat actor achieved persistent access to the victim's environment and returned to the network to perform further activity at least once, occurring two months after the initial compromise. Given the nature of the victim organisation, its subject matter expertise and the evidence found during our incident response engagement, we assess this intrusion was highly likely motivated by espionage and targeting intellectual property and unique knowledge belonging to the victim organisation.

Our review of surviving evidence led us to assess the initial compromise into the victim's environment was likely facilitated by Andariel's exploitation of an Internet-facing server vulnerable to Log4Shell. Following initial access into the network, Andariel deployed executable loaders for the DTrack backdoor[208] on multiple hosts and established persistence through a variety of methods, including setting Autorun keys and creating Startup services, whilst the backdoor itself was exclusively run in memory.

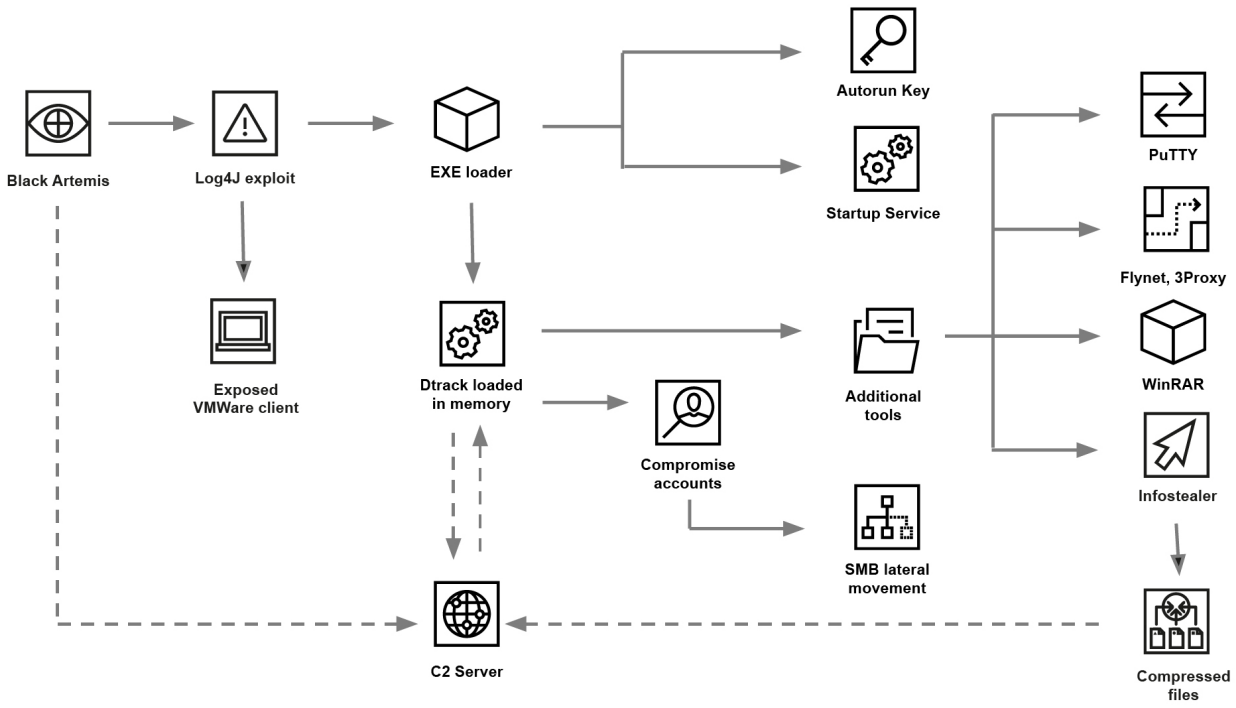
[208] 'Dtrack activity targeting Europe and Latin America', Kaspersky, https://securelist.com/dtrack-targeting-europe-latin-america/107798/ (15th November 2022)

Andariel then dropped additional tools to disk:

- Legitimate PuTTY clients;
- A custom build of a specific, older version of the PuTTY Secure Shell Protocol (SSH)/Telnet client for Windows compiled from source;
- Often in combination with Flynet, an open source Go TCP/UDP proxying tool for Windows; and,
- In at least one case, Andariel also dropped 3Proxy, an open source proxying utility.

These tools were given filenames that allowed them to masquerade as being related to the antivirus present in the victim's environment. We assess Andariel used these tools likely to proxy traffic in and out of the victim's network. This is consistent with other Andariel activity encountered by Cisco Talos during incident response cases on the networks of other victims,[209] suggesting the threat actor has a very defined and consistent playbook across intrusions.

Black Artemis intrusion chain



[209] 'Lazarus and the tale of three RATs', Cisco Talos, https://blog.talosintelligence.com/lazarus-three-rats/ (8th September 2022)

Andariel additionally compromised several accounts ranging from Local Administrators to Domain Administrators, and we observed evidence of the threat actor moving laterally across the network, including by likely jumping hosts through SMB connections. The threat actor dropped a specific version of WinRAR on multiple hosts, which was used to unpack compressed archives containing DTrack loaders to be executed, and with realistic probability to compress files for exfiltration. We also found evidence suggesting Andariel used a custom infostealer matching the description provided by Symantec in a blog on DTrack activity, which it deployed specifically on file servers.[210]

Lessons from the Andariel incident involving DTrack

There are several possibilities for detection and mitigation opportunities across the intrusion chain performed by Andariel which we observed in this incident. When comparing this case to the White Baku case described above, it is important to consider similarities in some of the attack stages, further reinforcing the importance of defending against techniques widely used across threat actors.

- *Initial access:* Please see this section in the White Baku case study above.
  MITRE ATT&CK T1505.003 - Server Software Component: Web Shell.

- *Persistence:* Threat actors continued to use well known persistence mechanisms such as Registry Keys and services. Whilst these are easy to establish for threat actors, they are also simple to detect and monitor, and can be identified both at creation time as well as during routine security hygiene checks for the environment. Whilst items like Registry Keys and services are a legitimate and normal part of organisation environments, and can be set up by threat actors to blend in among expected software and tasks, detection rules can be created to monitor for creation or modification of Autorun methods. MITRE ATT&CK T1547.001 - Boot or Logon Autostart Execution: Registry Run Keys/Startup Folder, T1543.003 - Create or Modify System Process: Windows Service

- *Lateral Movement:* Please see this section in the White Baku case study above.
  MITRE ATT&CK T1021.002 - Remote Services: SMB/Windows Admin Shares

- *Collection:* Once more, it's important to stress that whilst compression tools like WinRAR and others are perfectly legitimate, they are also used by cyber criminals and advanced persistent threats alike. Detecting when such tools are downloaded from the Internet, or installed in specific folders, such as %TEMP%, may be a useful heuristic to identify suspicious activity that can be flagged for review.
  MITRE ATT&CK T1560.001 - Archive Collected Data: Archive via Utility

[210] 'Stonefly: North Korea-linked Spying Operation Continues to Hit High-value Targets', Symantec, https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/stonefly-north-korea-espionage (27th April 2022)

- *Exfiltration:* Like White Baku, Andariel utilised file transfer tools for data exfiltration purposes, the defensive measures for which have been detailed in this case study. Additionally, this threat actor utilised legitimate network proxy tools as well, for which similar points apply, as defenders should be looking for deviations of such activity from the baseline characteristics of the environment. However, legitimate scenarios for proxying of network traffic are typically more limited, which may allow for slightly stricter signatures.
  MITRE ATT&CK T1048.002 - Exfiltration Over Alternative Protocol: Exfiltration Over Asymmetric Encrypted Non-C2 Protocol, T1090.001 - Proxy: Internal Proxy

Looking ahead

In 2023, we anticipate the threat landscape will be dominated by the targeting of identity and privileged access capabilities, as a broad range of threat actors continue to evolve and employ TTPs to bypass security mechanisms. More prolific espionage motivated threat actors will increasingly target digital supply chains and exploit 0-days for access operations.

As threat actors operate through quartermaster arrangements and use commodity or shared tooling, frameworks and malware, we expect the commercial marketplace for these capabilities to evolve and prompt wider adoption. Indicators of this evolution include an increasing market for 0-days and commercial threat actors stockpiling exploits, such as NSO Group (a.k.a. Grey Anqa)[211] and others. This evolution will enable more espionage motivated threat actors to emerge from nascent capabilities that were typically under-resourced or underutilised.

Concerning quartermaster trends specifically, we anticipate espionage motivated threat actors will increase their investments into obfuscation-as-a-service proxy networks, and that vulnerable Internet-of-Things (IoT) and small office/home office (SOHO) devices will continue to be some of the primary targets for exploitation and co-option systems run by the commercial providers of these networks.

Given the saturated market across the cyber criminal ecosystem, we anticipate cyber criminals will continue to adapt in the depth and breadth of monetised criminal services. We anticipate the high profile “smash-and-grab” attacks of 2022 will prompt similar activity in the coming year, for both financially and hacktivism motivated threat actors. Software library vulnerabilities are also likely to be an exploitation focus for threat actors in the year ahead.

Finally, as we research the development and deployment of sabotage capabilities by threat actors such as those based in Iran, we expect a continuation of “hack-and-leak” attacks,

[211] We previously shared information about this threat actor in ‘Cyber Threats 2021: A Year in Retrospect’, PwC Threat Intelligence https://www.pwc.com/gx/en/issues/cybersecurity/cyber-threat-intelligence/cyber-year-in-retrospect/yir-cyber-threats-report-download.pdf (28th April 2022).

use of wipers, pursuit of long-standing destruction operations against industrial control systems (ICS) and evolving techniques that could include data alteration-style attacks.

Threat actor-specific targeting anticipated in 2023

With Russia's protracted war in Ukraine and fallout of diplomatic relations across much of the globe, we anticipate Russia-based threat actors will increasingly target sectors and organisations in retaliation for their perceived or overt support of Ukraine or divestiture from Russia. We also expect Russia-based threat actors to target logistics, transport and manufacturing sectors as the war continues, as well as other sectors in which Russia experiences significant supply chain challenges—akin to industrial espionage targeting. Russia-based threat actors will also continue to show interest in government, defence and related entities as part of longstanding espionage operations.

We expect China-based threat actors to increase their targeting operations against the semiconductor industry and high technology, particularly given US sanctions imposed on China in 2022.[212] Further, we anticipate geopolitical tensions in the region will increase related targeting operations by these threat actors. Given the protest activity that occurred across China in late 2022, how threat actors may respond to support internal surveillance activities will be an area to watch.

Iran-based threat actors will continue targeting sectors relevant to the Iranian regime, as well as sectors related to the development of its strategic interests. We expect Iran-based threat actors to continue targeting Israel-, Saudi Arabia- and US-based entities, whilst also continuing their tempo for inward targeting against domestic targets and dissidents.

We anticipate Western-based actions emanating from countries like the United States will likely remain consistent and reflect geopolitical issues, as seen in the US's admission in 2022 of conducting offensive cyber operations "in support of Ukraine" amidst the Russian war.[213]

[212] *CTO-SIB-20221117-01A - US export controls on semiconductors*
[213] 'US military hackers conducting offensive operations in support of Ukraine, says head of Cyber Command', Sky News, https://news.sky.com/story/us-military-hackers-conducting-offensive-operations-in-support-of-ukraine-says-head-of-cyber-command-12625139 (1st June 2022)

PwC Cybersecurity

If you would like more information about any of the threats detailed in this report, please feel free to get in touch with us at threatintelligence@pwc.com.

PwC is globally recognised by industry analysts as a leader in cybersecurity: as a firm with strong global delivery capabilities and the ability to address the security and risk challenges our clients face.

We underpin our board-level security strategy and advisory consulting services with expertise gleaned from the front lines of cyber defence across our niche technical expertise in services such as managed cyber defence, red teaming, incident response and threat intelligence.

We differentiate ourselves with our ability to combine strategic thinking, strong technical capabilities and complex engagement delivery with client service excellence. Our unique research and security intelligence, technical expertise and understanding of cyber risk help clients get the clarity they need to confidently adapt to new challenges and opportunities.

We bring together a team of specialists with expertise in security management, threat detection and monitoring, threat intelligence, security architecture and consulting, behavioural change and regulatory and legal advice in our efforts to help our clients protect what matters most to them.

We specialise in providing the services required to help clients resist, detect and respond to advanced cyber attacks. This includes crisis events such as data breaches, ransomware attacks, economic espionage and targeted intrusions, including those commonly referred to as APTs. Our threat intelligence research underpins all of our security services and is used by public and private sector organisations around the world to protect networks, provide situational awareness and inform strategy

Appendices

Appendix A - Methodology

Throughout the year, we engage with clients and stakeholders, as well as with experts across the security industry, to validate and refine our intelligence requirements as we transform our unique visibility, bespoke tools, tradecraft and analytic efforts into actionable intelligence for our clients. This report specifically covers a selection of our analysis developed over the course of 2022. In addition to our proprietary capabilities and access to commercial tools and open source, we work closely with PwC Network firms during incident response cases and other engagements. The following PwC firms provided their insights from these engagements to enrich our analysis: Australia, Austria, Brazil, Canada, Czech Republic, Germany, Hong Kong, Indonesia, Italy, Malaysia, Netherlands, New Zealand, South Korea, United Kingdom, United States and Vietnam.

Estimative language

Interpretations of estimative or probabilistic language (e.g. “likely” or “almost certainly”) vary widely, and to avoid misinterpretation we have used the following qualitative terms within this report when referring to the level of confidence we have in our assessments. Unless otherwise stated, our assessments are not based on statistical analysis.

Qualitative term	Associated probability language
Remote or highly unlikely	Less than 10%
Improbably or unlikely	10-25%
Realistic probability	26-50%
Probable or likely	51-75%
Highly probable or highly likely	76-90%
Almost certain	More than 90%

In Appendix B - Threat actor reference, we describe the methodology behind our threat actor naming convention and how we define threat actor motivations and capabilities.

In Appendix D - Defender index, we provide additional definitions and explanations of our detection and mitigation methodology.

Appendix B - Threat actor reference

We track a wide range of threat actors from around the world and apply our naming convention, first consisting of a colour referring to where we assess the threat actor to be based. We designate the colour "White" to threats under assessment, and the below table includes some of our colour mapping. Following the colour, we assign a mythical figure to establish a unique name for the threat actor. If we observe activity that cannot be attributed to a known entity, we refer to the threat actor as a “dev set” to facilitate further development and analysis, and in some cases we will assign a named set to a dev set if our analysis results in an attribution assessment. Where we see overlaps in attribution between our research and other organisations’, we provide the respective threat actor names.

North Korea-based (Black)	Russia-based (Blue)	China-based (Red)	Iran-based (Yellow)
India-based (Orange)	Five Eyes-based (Magenta)	Nigeria-based (Bronze)	Location agnostic or based out of multiple countries (Grey)

Key terms and phrases concerning threat actors

Cyber criminal -as-a-Service offerings: Cyber criminal services which are developed and then advertised for use in exchange for payment, such as the following included in this report:

- Access-as-a-Service (AaaS): The criminal service offering which charges customers for accesses to networks, predominantly corporate.
  This type of offering can be divided into the following two categories:
  - Initial access broker (IAB): A cyber criminal who sells login credentials to exposed Internet-facing infrastructure, such as remote desktop protocol (RDP) and virtual private networks (VPNs), to customers.
  - Malware delivery system: A criminal service which uploads a customer’s malware onto a compromised host as a secondary payload, such as White Taranis via Emotet and White Horoja via Qakbot. - pg. 45-48
- Distributed Denial of Service-for-hire (DDoS-for-hire): The criminal service offering where cyber criminals pay a fee to an illicit capability to conduct DDoS attacks, such as Blue Kurama (a.k.a. Killnet) which started as a DDoS-for-hire capability. - pg. 19

- Phishing-as-a-Service (PHaaS): The criminal service offering where cyber criminals pay a fee to an illicit phishing capability to send phishing emails, such as EvilProxy, Caffeine and Robin Banks toolkits. - pg. 48, 50-51
- Ransomware-as-a-Service (RaaS): The model of ransomware programmes involving operators, who develop the ransomware and the overall brand of operations, and affiliates, or those who use the ransomware in attacks. - pg. 39-46

Data Broker: In the context of this report, an illicit entity that collects, aggregates and sells access to sensitive information stolen from victims. - pg. 38

Espionage motivated threat actors: Often referred to as “Advanced Persistent Threats” (APTs), these threat actors typically seek access and information to address intelligence collection requirements and provide an economic or political advantage to their benefactor. - pg. 61 (high level insights specific to the incident response cases we analysed)

Financially motivated threat actors: These threat actors can be indiscriminate in whom they attack as cyber criminals simply seek to monetise their activities. The range in sophistication of these threat actors is vast and displays a widely different set of TTPs. - pg. 39-51, 61

Hacktivism: Hacktivists conduct attacks to increase their public profile and raise awareness of their cause. This is typically done through the disruption of services, such as denial of service (DoS) attacks, and website defacements. - pg. 1, 11, 18-19, 61, 68

Insider: A current or former employee, contractor or other business partner who has or had authorized access to an organisation's network, system or data and intentionally misused that access to compromise the organisation's data or systems. - pg. 39, 44, 49, 61

Operational Security (OPSEC): The steps taken to secure operations and assets so they cannot be disrupted, pre-empted or attributed. - pg. 23, 31

Proxy network: In the context of this report, an anonymised network or otherwise obfuscated relay system used by threat actors to conduct operations, such as RedRelay. - pg. 2, 20, 22-23, 68

Quartermaster: An entity that enables threat actor operations through the development, provisioning and brokerage of tools, capabilities and frameworks. - pg. 20, 22, 68

Sabotage motivated threat actors: Saboteurs seek to damage, destroy or otherwise subvert the integrity of data and systems. - pg. 1-2, 8, 11-14, 28-29, 68-69

Tools, techniques and procedures (TTPs): TTPs refer to threat actor behaviours, and Appendix D - Defender index provides a quick reference for examples of TTPs cited in this report.

Threat actors included in this report

- Abraham’s Ax - pg. 29
- Andariel (a.k.a. Stonefly, Silent Chollima), a subgroup of Black Artemis - pg. 64-67
- Business email compromise (BEC) threat actors - pg. 50
- Black Alicanto (a.k.a. COPERNICIUM, DangerousPassword, CryptoMimic, CryptoCore, Operation SnatchCrypto) - pg. 32, 34

Appendix C - Executive companion

Cyber security and geopolitical conflict were identified as top tier risks for the next five years by CEOs in PwC's 26th Annual Global CEO Survey. In 2022, cyber threat actors continued to adapt and modify their behaviours to outmanoeuvre security practices against a backdrop of escalating conflict in Ukraine, a sustained yet high tempo in ransomware activity and the use of sabotage to further both political and criminal gains. While the threat landscape evolved and the risks increased, PwC's 2023 Global Digital Trust Insights research highlighted collaboration between CISOs and the C-suite and Board as a critical contributor to cyber security improvements and making the most of sustained, cumulative investments in risk mitigation.

PwC Threat Intelligence identified the following key cyber risks from our threat-focused research in 2022, as well as our proactive efforts to spot and assess emerging cyber issues.

1. **Geopolitics reflected in threat actor activities - pg. 1-2, 68-69**
    - Cyber capabilities were used extensively by threat actors to complement traditional warfare methods observed in the Russian war in Ukraine (pg. 8-19).
    - China-based threat actors advanced their abilities to obfuscate their activities against traditional targets and demonstrated a keen interest in intelligence relating to the war in Ukraine, as well as the response of the international community (pg. 20-26).
    - Iran-based threat actors escalated their targeting of dissidents and demonstrated a willingness to use cyber as a political weapon in the Balkans (pg. 27-31).
    - North Korea-based threat actors continued to target financial services and cryptocurrencies as a way of generating revenue and offsetting the effects of sanctions (pg. 32-34).
    - Many nations escalated the priority of increasing cyber resilience at a national level after cyber authorities like the Cybersecurity and Infrastructure Security Agency (CISA) in the United States and the National Cyber Security Centre (NCSC) in the United Kingdom forewarned of the potential for organisations to become collateral damage in the wake of increased geopolitical tensions (pg. 9-10).

2. **Ransomware's evolution and outlook - pg. 39-48**
    - Ransomware remained the main cyber threat to the majority of organisations across the globe, as threat actors professionalised their business model to 24/7 operations against high value sectors, including manufacturing, construction and retail (pg. 41-42, 44-45).
    - Threat actor interest also extended to small and medium size organisations, including local government, incurring significant costs for

mitigation and remediation and publicising attacks and disruptions on leak sites (pg. 41-42).
- Ransomware groups and key threat actors continued to fracture and rebrand throughout 2022, with Ransomware-as-a-Service (RaaS) proving increasingly popular as a business model (pg. 39-46).

3. **Sabotage operations escalate - pg. 1-2, 68-69**
    - Russia-based threat actors deployed multiple forms of destructive malware against Ukraine-based entities, and we expect the same in 2023 (pg. 1, 11-14).
    - Iran-based threat actors launched sabotage attacks against organisations within the Albanian government. The success of these potentially foreshadows emboldened attempts to exert strategic influence via offensive cyber means in the future by Iran-based threat actors, as well as others with sabotage motivations and capabilities (pg. 2, 28-29, 68-69).

4. **Multifactor Authentication (MFA) bypassing/evasion and fatigue - pg. 49-52, 58-60**
    - Threat actors demonstrated the ability to adapt and bypass enhanced security controls, including some forms of MFA, and tailor social engineering (pg. 49) and credential stealing tools (pg. 49-50) to maximise their ability to gain unfettered access to corporate environments, including cloud-based environments (pg. 58-59).
    - The failure to use MFA in a corporate environment, especially on privileged access accounts, contributed to the success of some ransomware attacks and other cyber criminal compromises observed in 2022. MFA makes it exceptionally difficult for a criminal to access a network remotely, even if they have a legitimate username and password (pg. 50).

5. **Targeting digital identity and privileged access - pg. 1, 58-60, 68**
    - Protecting identity and privileged access is the single highest priority to secure an organisation’s environment and data.
    - Threat actors in 2022 focused extensively on compromising digital identities, often by using sophisticated social engineering, to achieve initial access (pg. 49).
    - Threat actors also used infostealers, which syphon user credentials and other information to gain initial access into networks (pg. 49-51).

6. **Cloud environments in the crosshairs - pg. 59-60**
    - As more organisations moved to the cloud and reaped the benefits of enhanced security afforded by those environments, threat actors worked hard to develop new tools and knowledge to compromise cloud-based services (pg. 58-60).

- Responding to attacks targeting cloud-based environments and services requires different approaches, as threat actors predominantly abuse identities, services and application programming interfaces (APIs) (pg. 59-60). Software library vulnerabilities are also likely to be an exploitation focus in 2023 (pg. 68).
- We developed several recommendations for hardening cloud environments based on incident response cases we supported in 2022 (pg. 59-60).

Looking ahead, cloud service, managed service and identity and access management (IAM) providers with privileged access to client networks will increasingly become targets of choice for the most sophisticated actors – to achieve the scaled access that they need to compromise the targets of their espionage and intellectual property theft operations (pg. 68).

Other appendices within this report provide more information about our methodology, the various threats described and a collated index of information relevant to defenders. This report also contains forward leaning insights in our Looking ahead section, as well as references to incidents impacting the following sectors[214] and industries:

- Automotive - pg. 61
- Chemicals - pg. 64
- Construction - pg. 42, 61
  - Engineering - pg. 31
- Critical infrastructure - pg. 17, 19, 30
- Defence - pg. 8, 19, 23, 29, 33, 69
  - Defence institutes - pg. 16
  - Military - pg. 15, 32
  - Military-themed targeting - pg. 15
  - Research laboratories - pg. 15
  - Supplier - pg. 16
- Dissidents - pg. 27, 29, 69
  - Activists - pg. 29
  - Protesters - pg. 27, 29-30, 69
- Education and research - pg. 42, 61
  - Academia and researchers - pg. 16, 26, 30, 39
  - Students - pg. 29
  - Think tanks - pg. 30
- Energy, utilities and resources - pg. 29-30, 33, 42, 61
  - Nuclear power - pg. 30, 36
  - Oil and gas - pg. 30, 36
  - Power grid - pg. 8
- Entertainment and gaming - pg. 49
- Financial services - pg. 2, 32, 35, 61
  - Cryptocurrency and decentralised finance (DeFi) - pg. 2, 32, 34, 41
  - Commercial banking - pg. 8, 17, 47
  - Financial management software - pg. 8
  - Insurance providers - pg. 17, 31
  - Venture capital - pg. 32
- Food exporters, supermarkets and retailers - pg. 36, 61
- Government - pg. 1-2, 6, 8-19, 22-37, 42, 50, 61, 69
  - Communications services - pg. 11, 16
  - Computer emergency response - pg. 13 (footnote), 38
  - Diplomatic entities - pg. 24-26
  - Election-themed targeting - pg. 25
  - Emergency services - pg. 18
  - Government systems - pg. 28-29
  - Law enforcement and security - pg. 11, 33, 50
  - Parliament - pg. 19

[214] *CTO-SIB-20230223-01A - Sector shifts and insights - 2022*

More from the PwC Threat Intelligence team:

- Read the blog posts we published in 2022
- View our talk at BlackHat USA 2022
- View our talk at SANS CTI Summit 2022
- View our talk at SANS Ransomware Summit 2022
- View our talk at Virus Bulletin 2022

Appendix D - Defender index

To stay ahead of threat actor trends, increase our visibility of threat actor shifts and develop detection and mitigation strategies for our clients, we utilise the following primary pillars, which serve as the foundation of our detection capabilities:

1. **Endpoint:** In today's decentralised, cloud-native environment, having effective detection on the endpoint, whether a virtual or physical server, laptop or mobile device, is one of the most important positions a defender can take.

2. **Network:** Whilst Transport Layer Security (TLS) remains a challenge, almost all malware uses the Internet for C2 communications. Having visibility of all network traffic means that even when an attacker evades detection on the endpoint, or compromises an endpoint that has no detection tooling, the C2 activity can usually be detected. Internal network visibility can also help with detecting and tracking lateral movement.

3. **Security Information and Event Management (SIEM)/Security Orchestration, Automation and Response (SOAR):** Having a central view of all detection events allows a defender to correlate at a higher level and conduct additional detection. It also brings together the wider context of activity in ways that, if done well, help the defender find signal in the noise. SOAR platforms also allow a defender to automate remediation, which is particularly useful when ransomware is in play and time is of the essence.

4. **YARA:** Whilst rarely used for real time detection, YARA is incredibly useful for analysing suspect binaries and for scanning memory. With YARA, rules can be written to assist with the triage of suspicious samples and cluster artefacts as part of intrusion and campaign analysis efforts.

Defence in depth can be further enhanced by developing detection for both specific activity attributed to threat actors with high confidence, as well as the behaviour more generally so that changes in behaviour, minor and otherwise, can be detected.

Read more about the YARA workshop we provided at FIRST22

Common Vulnerabilities and Exposures (CVEs) cited in this report

Key themes and examples of threat actor TTPs

Detection logic and methods

[215] 'Macros from the internet will be blocked by default in Office', Microsoft, https://learn.microsoft.com/en-us/deployoffice/security/internet-macros-blocked (11th October 2022)

Insights from incident responses and other case studies

MITRE ATT&CK References

All references to capabilities and malware

pwc.com/cyber-security