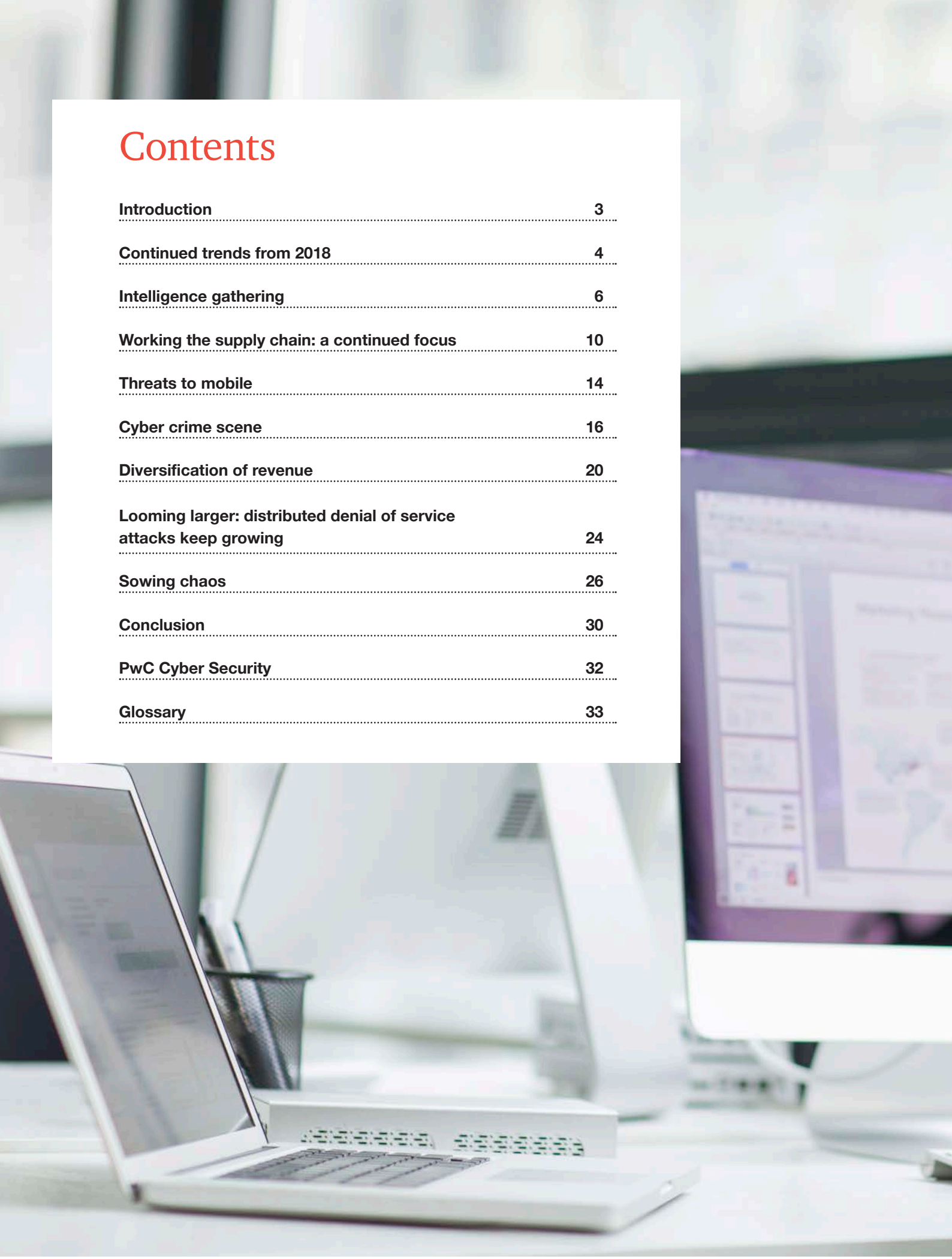
Cyber Threats 2019: A Year in Retrospect

Cyber Threat Operations
February 2020

pwc

Contents



Introduction

In 2019, the cyber threat landscape became increasingly complex to navigate: with the proliferation of financially motivated cyber activity, intelligence operations navigating the currents of powerful interests and international politics, and information operations attempting to manipulate the narrative.

2018 marked a year of audacity, with nation states becoming more brazen in their attacks and intelligence agencies around the world calling out other governments' cyber activity. While in 2019 PwC did not observe a radical shift in cyber activity, there was a continuation of the same brazenness and even an uptick in operational tempo from several threat actors, including financially motivated and espionage-focused threat actors. Several trends observed in 2018 continued to dominate the landscape throughout 2019, with business email compromise (BEC) attacks growing ever more sophisticated, threat actors continuing to manipulate living-off-the-land techniques to disguise activity, and an overall overt alignment between the cyber threat landscape, the geopolitical landscape, and real-world events.

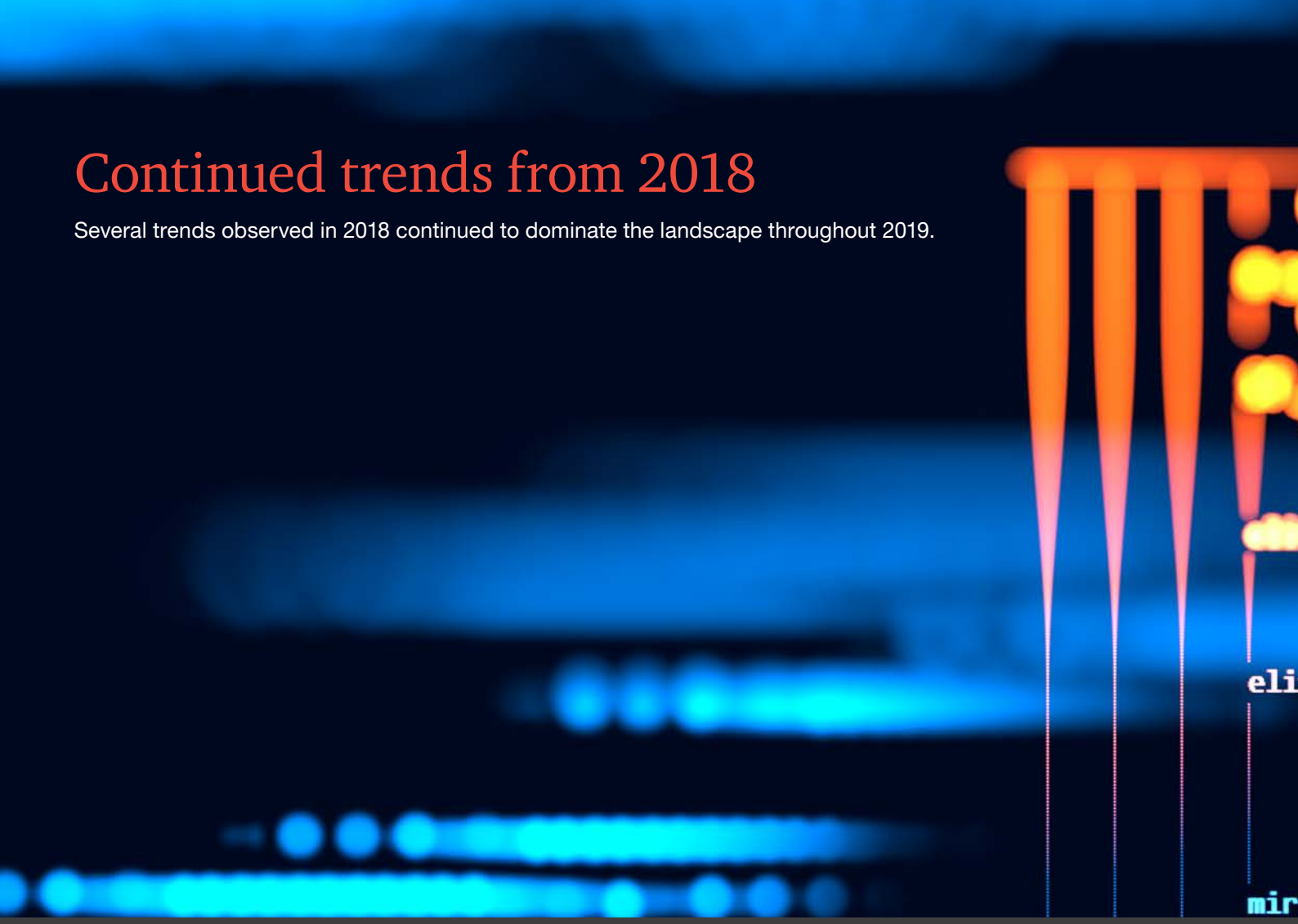
2019 also saw the continued proliferation of ransomware, and further criminal threat actors diversify their operations to incorporate ransomware. In 2019, cyber criminal activity remained an extremely significant threat to commercial organisations. While PwC saw new threat actors rise to prominence in the cyber criminal space, overall, the cyber criminal market effectively consolidated around large, established players that maintained, managed, and updated some of the largest cyber criminal operations. This report considers the incumbent leaders on the cyber crime scene, as well as the new players and diversification of revenue.

In terms of sabotage attacks, the end of 2019 saw a new form of wiper named ZeroCleare – with links to Shamoon malware – target organisations in the Middle East. Throughout 2019, DDoS attacks remained a steady trend in the background of other cyber operations. Election interference via information operations is an increasingly well-documented phenomena, and 2019 saw the same information operation principles used for other nefarious activities.

This report analyses the overarching and thematic trends from 2019, including mapping tools, techniques, and procedures to the cyber-attack landscape. Our analysis is based on our in-house intelligence datasets on cyber attacks and targeting from a variety of threat actors, intelligence gleaned from our incident response engagements around the world, our Managed Cyber Defence service, as well as publicly available information from the cyber security community. This report intends to highlight the most prolific trends PwC observed throughout 2019 and explore their wider impact.

Continued trends from 2018

Several trends observed in 2018 continued to dominate the landscape throughout 2019.



Increasing sophistication of business email compromise attacks

Our 2018: A Year in Retrospect report illustrated the rising trend of BEC attacks, where a threat actor either hijacks or closely imitates ('spoofs') a legitimate email account in order to more effectively socially engineer individuals. The targeted individuals receive spear-phishing emails from the attacker, often masquerading as someone known to the target. In 2019, BEC attacks remained prevalent across all industry sectors and business sizes, and there was a rise in targeted attacks with more sophisticated social engineering as a result of extensive preparatory reconnaissance. This highlights the importance of security awareness training for employees, as detection of this type of scam typically relies on employees being able to identify suspicious emails and being empowered to verbally query the (usually internal) sender. In one case investigated by the PwC Incident Response team, the threat actor created a sophisticated web of impersonated individuals at every level in the email chain, and used phone calls to reiterate claims from the phishing emails.

From useful to dangerous: living-off-the-land techniques

Another theme that has endured throughout 2019 is the use of legitimate tools and processes, often already installed on a victim's device, to reduce the chance of an attack being detected. This method is referred to as living-off-the-land – attempting to hide in plain sight. Fileless persistence techniques or memory-only tools are common living-off-the-land techniques. Indeed, many threat actors include or download legitimate tools as part of the infection process; the remote execution tool PsExec is a legitimate tool that is commonly used in this way.

In September 2019, PwC analysed an unusual form of fileless malware, dubbed Nodersok, which installs several legitimate tools such as Node.exe to proxy traffic.[1] Node.js is a JavaScript Runtime environment that is not usually associated with malware and potentially less likely to be detected as a result.

In June 2019, PwC reported on a sophisticated espionage campaign targeting a police force in the Indian subcontinent which relied on living-off-the-land techniques to evade detection.[2] The threat actor, Orange Chandi (**a.k.a.** Sidewinder), masqueraded as a senior superintendent in the police force in a phishing email that contained a malicious file disguised as a compliance document. In the chain of events following the malicious document's execution, the threat actor took advantage of standard Windows features to achieve its goal, rather than creating bespoke malware.

[1] 'Threat Vector Bulletin', PwC Threat Intelligence, CTO-TVB-20191010-01A

[2] 'Punjab Police in the crosshair of Sidewinder', PwC Threat Intelligence, CTO-TIB-20190620-01A

Continued geopolitical alignment

Throughout 2018, PwC intelligence reporting regularly documented a more overt alignment between the cyber threat landscape and the geopolitical landscape. This trend continued in 2019, with further attacks in response to sanctions, diplomatic tensions, and trade deals. This report considers multiple examples of this parallel, from:

- Repeated cases of threat actors incorporating timely real-world events into crafting convincing lures; to,
- Pakistan-based and India-based threat actors engaging in ripostes to one another's cyber operations, and even copying techniques used by other threat actors; and,
- Information operations in the lead up to national elections.

As with 2018, PwC assesses it likely that the alignment between cyber attacks and geopolitics will continue to be prominent through 2020.

Intelligence gathering

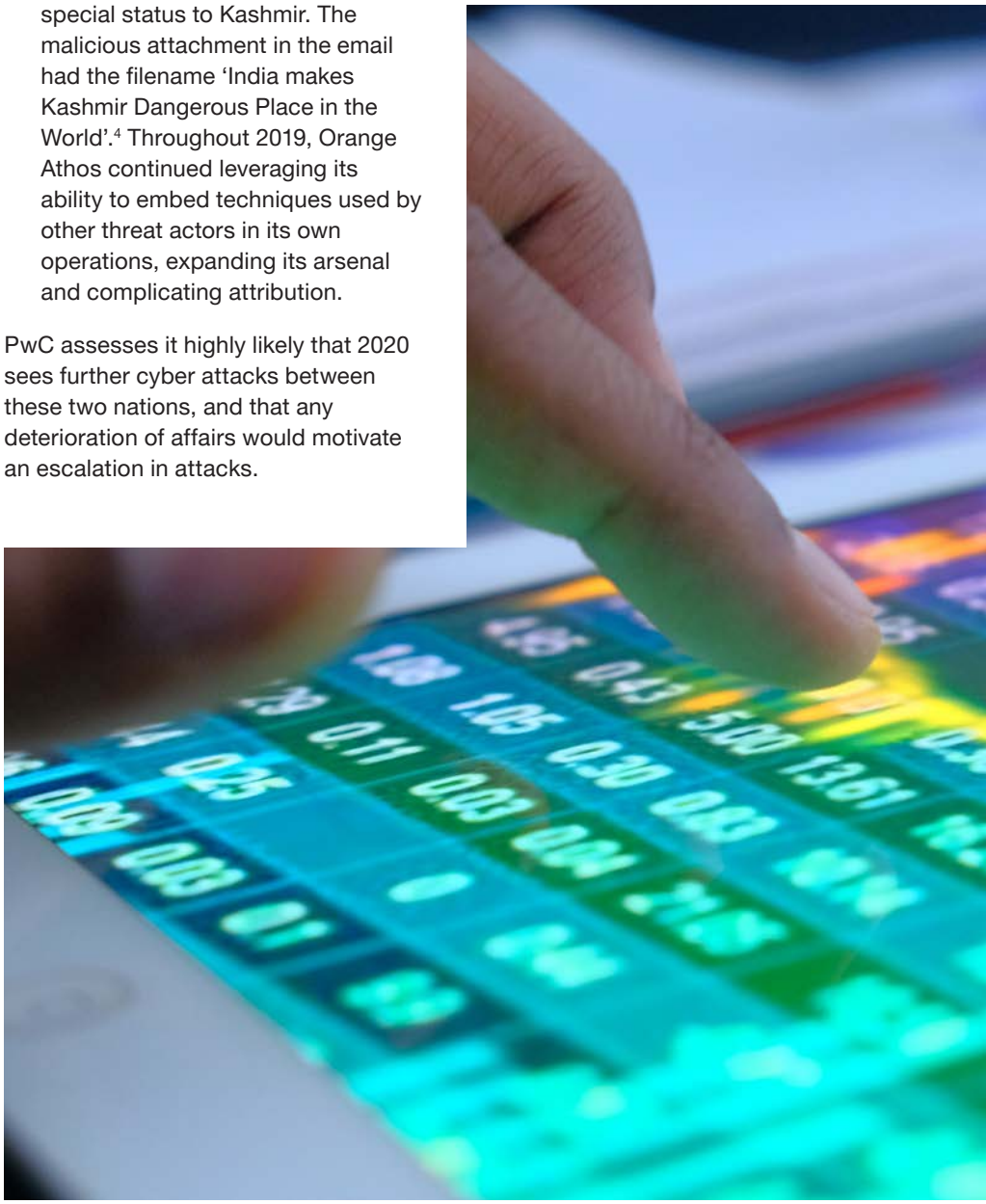
Action and reaction

2019 was a tense year for India-Pakistan relations, with numerous instances of posturing, heated and inflammatory rhetoric, and the occasional spill-over into physical conflict. This volatile set of circumstances also led to a spate of tit-for-tat cyber attacks, with threat actors based in both countries conducting intelligence-gathering campaigns amongst the political chaos. The attacks exploited the state of heightened alert, weaponising news pieces into malicious documents to socially engineer targets.

In particular, in 2019, PwC observed Pakistan-based and India-based threat actors engaging in timely ripostes to one another's cyber operations, with cases of threat actors borrowing and incorporating their adversaries' techniques.

- In late February 2019, Pakistan-based threat actor Green Havildar (**a.k.a.** Gorgon Group) used a lure related to airstrikes conducted by the Indian military within Pakistani airspace, allegedly targeting a Jaish-e-Mohammad training camp.[3] The lure document delivered a CrimsonRAT payload to victims.
- Similarly, India-based threat actor Orange Athos (**a.k.a.** Patchwork) used a politicised lure encouraging Pakistani targets to open a malicious attachment, in the wake of the Indian government's decision to revoke an article in the constitution providing special status to Kashmir. The malicious attachment in the email had the filename 'India makes Kashmir Dangerous Place in the World'.[4] Throughout 2019, Orange Athos continued leveraging its ability to embed techniques used by other threat actors in its own operations, expanding its arsenal and complicating attribution.

PwC assesses it highly likely that 2020 sees further cyber attacks between these two nations, and that any deterioration of affairs would motivate an escalation in attacks.



[3] 'Green Havildar on Jaish Camp', PwC Threat Intelligence, CTO-QRT-20190304-01A

[4] 'Orange Athos pushes BADNEWS on Kashmir', PwC Threat Intelligence, CTO-QRT-20190822-01A

Espionage attacks target the nuclear sector

Nuclear energy continues to be the crux of much international tension. Following the US withdrawal from the Joint Comprehensive Plan of Action in 2018, Iran announced at multiple times throughout 2019 that it had resumed its nuclear enrichment programme – which it had previously stopped in order to relieve international sanctions imposed on oil exports. Throughout the year, the US were also engaged in sustained talks with the North Korean government about a proposed nuclear energy agreement, with a view to halt or delay North Korea's nuclear program in exchange for the lifting of currently-imposed export sanctions. Meanwhile, the Indian subcontinent is also witnessing a race between the two main nuclear players in the region, India and Pakistan.

In 2019, PwC observed intense targeting of the nuclear energy space by multiple threat actors, with a strong concentration of activity by Asia-based threat actors. At the very beginning of 2019, PwC identified a fake webmail login page pretending to belong to the Pakistan Atomic Energy Commission (PAEC), and which looked like an exact copy of the legitimate PAEC equivalent. The fake webpage was configured by an IP address controlled by the India-based threat actor that PwC tracks internally as Orange Berserker (**a.k.a.** Viceroy Tiger). Around the same time, the Orange Berserker-controlled IP also set up domains spoofing the Pakistan Navy webmail login.[5] Later in the year, PwC also observed a further campaign delivering a malicious document titled 'PAEC_Security_Advisory.doc',[6] which was concerned with the reported compromise of a large set of Pakistani social media by 'our adversaries'. The malicious document used macros to deliver a malware family that PwC internally named RaveRAT, and which bears some similarities to CrimsonRAT as well as PeppyRAT.

One of the most notable campaigns targeting the nuclear sector in 2019 compromised the Kudankulam Nuclear Power Plant (KKNPP) in Tamil Nadu, a joint venture between India and Russia.[7] PwC analysts were able to independently verify that the malware assessed to have infected KKNPP's networks was a highly tailored sample of a backdoor known in open source as DTrack and Preft.[8] PwC assesses that DTrack, and the customised DTrack sample involved in the KKNPP incident, are tied to North Korea-based threat actor Black Artemis, widely known in open source as Lazarus. The malware had been configured with specific knowledge of the KKNPP internal network, and used a further compromised host on the network as a traffic proxy, implying that the threat actor had compromised and reconnoitered KKNPP prior to the deployment of the customised DTrack payload. Analysing the sample, PwC analysts did not find evidence of destructive capability in the malware, rather, it appeared more oriented towards information theft. This is not the first time that North Korea-based threat actors had targeted, and successfully compromised, nuclear plants or organisations in the nuclear sector. In 2014, for example, Black Banshee had breached the Korea Hydro & Nuclear Power (KHNP) Corporation,[9] leaking stolen confidential documents as well as attempting sabotage wiper attacks against victim machines.

The targeting of nuclear organisations that PwC observed in 2019 broadly aligns with individual states' national interests and strategic objectives, it also reflects at a higher-level the current geopolitical balances and international relations. PwC expects the nuclear sector to continue drawing cyber targeting, especially by espionage motivated threat actors, throughout 2020.

---

[5] 'An atomic phish', PwC Threat Intelligence, CTO-QRT-20190102-01A

[6] 'Recycling and renewal chez Green Havildar', PwC Threat Intelligence, CTO-TIB-20190403-01A

[7] 'An Indian nuclear power plant suffered a cyberattack. Here's what you need to know', The Washington Post, https://www.washingtonpost.com/politics/2019/11/04/an-indian-nuclear-power-plant-suffered-cyberattack-heres-what-you-need-know/ (4th November 2019)

[8] 'Hello! My name is Dtrack', Kaspersky, https://securelist.com/my-name-is-dtrack/93338/ (23rd September 2019)

[9] 'South Korea blames North Korea for December hack on nuclear operator', Reuters, https://www.reuters.com/article/us-nuclear-southkorea-northkorea/south-korea-blames-north-korea-for-december-hack-on-nuclear-operator-idUSKBN0MD0GR20150317 (17th March 2015)

In the Python's coils

Throughout 2019, PwC analysts tracked sustained activity assessed to be conducted by the Russia-based espionage threat actor Blue Python (**a.k.a.** Turla or Snake). Blue Python consistently targeted Central and Eastern European countries, including Austria, Czech Republic, Moldova, Ukraine and Armenia. The threat actor continued to focus on compromising government ministries (with special attention on the Ministries of Foreign Affairs and Ministries of the Interior) as well as other government entities and government organisations, with some targeting of NGOs involved in business and defence.

The threat actor continues to rely on a wide toolset consisting of multiple downloader, dropper, and backdoor malware families. In 2019, PwC analysts observed Blue Python adding new malware to its arsenal, including the Topinambour downloader,[10] but also continuing to develop existing tools, with updated variants of the Kazuar backdoor used to target the Czech Republic.[11] In that instance, the threat actor leveraged compromised WordPress sites for command and control infrastructure. In July 2019, Blue Python compromised the websites of legitimate organisations in the Armenian NGO sector to act as watering holes for further victims. The compromised websites delivered the Blue Python implant known as Skipper – a first-stage profiling tool used to deploy other, more powerful backdoors to victims of special interest.

In summer 2019, PwC detected samples of Skipper used in a multi-stage infection chain targeting a private sector entity that deviated from Blue Python's typical victimology: an Asian shipbuilding company, active in the production of Arctic-capable vessels.[12] The downloader for the sample contained unobfuscated macros; this is uncharacteristic of Blue Python's well-designed decoys and might indicate that the particular document chain used in the attack was still under development at the time it was deployed. Moreover, analysing the metadata of the malicious document and comparing with the date a sample was uploaded to an online multi-antivirus scanner indicates that the threat actor began targeting potential victims less than a week after creating the malicious document. The Arctic is a strategically sensitive region due to its access to natural resources and the opening up of transport routes, and the Arctic Shipping Route has been a crucial element in cooperation between South Korea and Russia. In light of this, the targeting of the Asian shipbuilding company operating in the Arctic would align with Russian strategic economic interests and intelligence requirements.[13]

Blue Python continues to conduct government espionage and intelligence gathering operations; in October 2019, the UK National Cyber Security Centre (NCSC) and the US National Security Agency (NSA) publicly assessed that Blue Python gained access to assets including malware and cryptographic keys belonging to an Iran-based threat actor – which a linked open-source report indicates is Yellow Maero (**a.k.a.** OilRig).[14] Blue Python was then able to deploy malware using Yellow Maero's own infrastructure, and to exploit Yellow Maero's established access to compromised victims for its own intelligence collection purposes against targets in the Middle East. The NCSC's and NSA's description of this activity reinforces the assessment of Blue Python as a highly sophisticated and well-resourced threat actor, able to experiment with new tools and even repurpose complex tools developed by other foreign actors. PwC assesses it is likely Blue Python will continue with sophisticated campaigns going into 2020, with government entities and the defence sector particularly at risk.

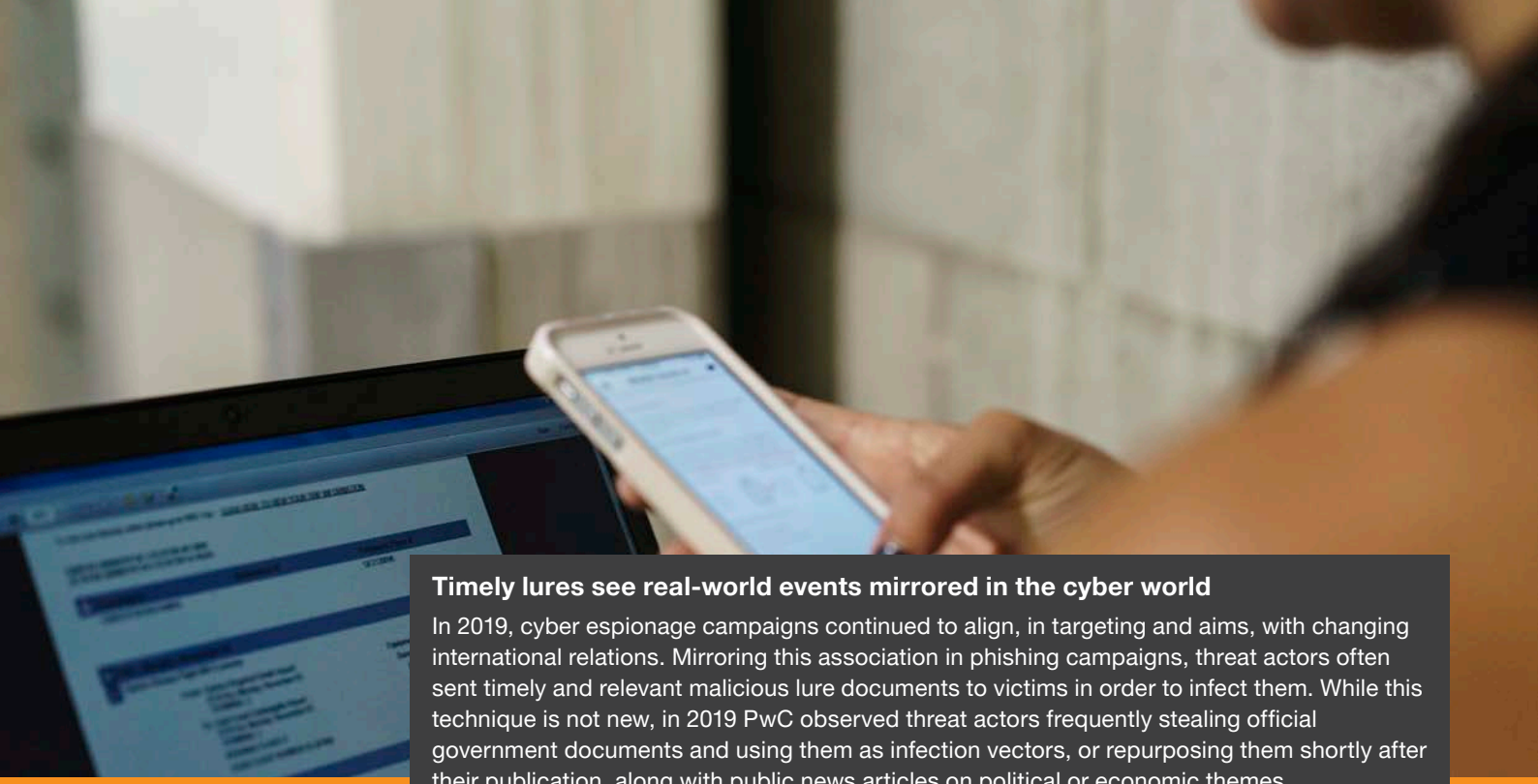
[10] 'Taste of Topinambour: Turla hacking group hides malware in anti-internet censorship software', Kaspersky, https://www.kaspersky.com/about/press-releases/2019_taste-of-topinambour (15th July 2019)

[11] 'Kazuar in Flight', PwC Threat Intelligence, CTO-QRT-20190205-01A

[12] 'The Skipper's New Ships', PwC Threat Intelligence, CTO-TIB-20190624-01

[13] 'PolarBear: cyber espionage in the Arctic', PwC Threat Intelligence, CTO-SIB-20190703-01A

[14] 'Advisory: Turla group exploits Iranian APT to expand coverage of victims. A joint report from the NCSC and NSA highlighting Turla activity', NCSC, NSA, https://www.ncsc.gov.uk/news/turla-group-exploits-iran-apt-to-expand-coverage-of-victims (21st October 2019)



Timely lures see real-world events mirrored in the cyber world

In 2019, cyber espionage campaigns continued to align, in targeting and aims, with changing international relations. Mirroring this association in phishing campaigns, threat actors often sent timely and relevant malicious lure documents to victims in order to infect them. While this technique is not new, in 2019 PwC observed threat actors frequently stealing official government documents and using them as infection vectors, or repurposing them shortly after their publication, along with public news articles on political or economic themes.

Case study – Phishing emails exploit article hours after its release

In late October 2019, PwC tracked the espionage threat actor Red Lich (**a.k.a.** Mustang Panda) as it used a lure document themed around a visit made to Tibet by the US ambassador for International Religious Freedom. The threat actor crafted the malicious payload by taking material from a news article published just hours earlier, as well as pictures from the Central Tibetan Administration's website.[15] The timeliness of the lure was likely intended to make the document appear to be a legitimate news item, enticing victims to open the malicious attachment. Red Lich has used similar types of lure documents, as well as fake CVs, to compromise victims since at least 2017.[16,17] The threat actor has historically targeted non-governmental organisations (NGOs), pro-democracy activists and minority rights groups across Asia, as well as international policy think tanks.

Case study – Summits and anniversaries exploited

In mid-April 2019, PwC analysts detected a sample of the NOKKI backdoor, which is attributed to North Korea-based espionage threat actor Black Shoggoth (**a.k.a.** APT37).[18] In that instance, NOKKI was delivered to targets via a .exe file masquerading as a PDF document with the filename 'Kim, Putin have high hopes for their 1st one-on-one meeting.exe'. The executable would install NOKKI on victim systems while displaying to the user a benign Associated Press article about the Kim-Putin summit of that same month.[19]

PwC identified another NOKKI sample created on the same day as the sample described above. This sample likely targeted individuals involved in diplomatic relations between Norway and South Korea, as the backdoor was laced with an RSVP for a May 2019 reception in South Korea for the 'Constitution Day of the Kingdom of Norway and the 60th anniversary of the diplomatic relations'.[18]

Case study – Invitations used to lure victims

In summer 2019, PwC discovered that Green Havildar had been targeting individuals associated with the Indian military, sending them an invitation to a formal event allegedly to be held in November 2019 at the Indian National Defence College.[20] The threat actor highly tailored the lures to masquerade as the targets' wives.

Case study – Military conferences high on White Ioke's agenda

Espionage threat actor White Ioke (**a.k.a.** OceanLotus) timed its phishing documents around real-world events of interest to its targets. In April 2019, PwC observed the threat actor delivering a malicious document titled 'Form_ Provisional Agenda of the ASEAN Senior Officials Preparatory Meeting.doc'.[21] Interestingly, an ASEAN Senior Officials' Meeting was scheduled to take place in Thailand on 28th May 2019. White Ioke has used lure documents about military and ASEAN-themed conferences before, for example '2018 Cambodia Outlook Conference.doc'. Many of the threat actor's lures were written in Vietnamese, Khmer, or Mandarin, reflecting White Ioke's known targeting.

---

[15] 'Red Lich slight TTP shift', PwC Threat Intelligence, CTO-QRT-20191101-01A

[16] 'Meet CrowdStrike's Adversary of the Month for June: MUSTANG PANDA', CrowdStrike, https://www.crowdstrike.com/blog/meet-crowdstrikes-adversary-of-the-month-for-june-mustang-panda/ (15th June 2018)

[17] '2018 Global Threat Report', CrowdStrike, https://go.crowdstrike.com/rs/281-OBQ-266/images/Report2018GlobalThreatReport.pdf

[18] 'NOKKI against Norway', PwC Threat Intelligence, CTO-QRT-20190424-01A

[19] 'Threats under the Spotlight', PwC Threat Intelligence, CTO-TUS-20190528-01A

[20] 'Green Havildar Malicious Event Invitation', PwC Threat Intelligence, CTO-QRT-20190731-01A

[21] 'White Ioke ASEAN intentions', PwC Threat Intelligence, CTO-TIB-20190417-01A

Working the supply chain: a continued focus

Since at least 2017, a significant trend for sophisticated threat actors has been their targeting of third parties in order to reach their customers. Threat actors will mask backdoors with legitimate digital certificates, direct malicious traffic through trusted companies (as compromised command and control servers (C2s)), and use established organisations to spread malware, in order to gain access to victims and avoid detection.

In particular, China-based threat actors had an increased focus on exploiting the trust and privileged access afforded to third-party suppliers.

Case study – Compromised software updates

ASUS Live Update is a utility that is pre-installed on Asus products, and is required to provide real-time updates to core software components such as a machine's BIOS. In 2019, it was discovered that ASUS pushed compromised software updates for several months in the latter half of 2018 in an operation called ShadowHammer.[22] Threat actors compromised ASUS and manipulated Live Update in order to install a backdoor on victim machines without end users' knowledge. Although it is estimated that the number of compromised victims may be in the hundreds of thousands, it is likely that only a few hundred of these were the ultimate victims of Operation ShadowHammer, which is assessed to be a highly targeted operation despite its blanket-attack tactic for delivery of the malware.

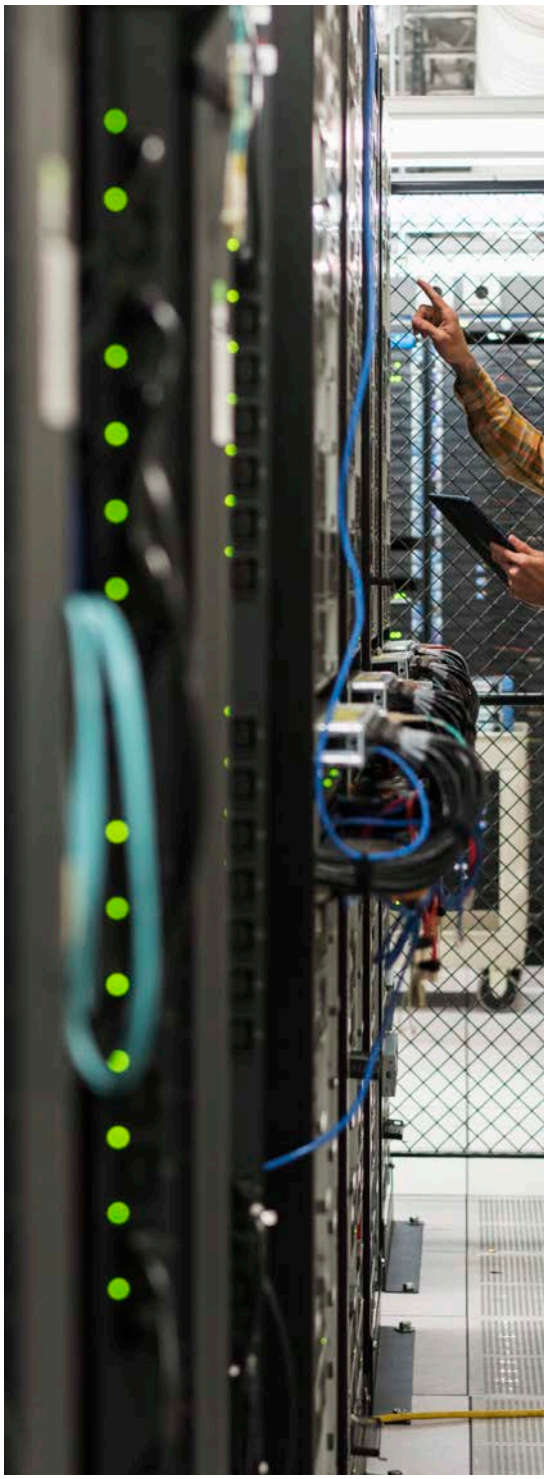
Winnti collective exploits the supply chain

PwC assesses that the users of Winnti encompasses activity by multiple China-based threat actors, which occasionally share infrastructure, techniques, and implants. Most notably, these actors are known for having access to a version of the 'Winnti backdoor'. While the threat actors share tools, techniques, and procedures, they often operate independently with different objectives. This could be attributed to a small number of key developers moving around threat actors, however, PwC assesses it likely that they operate under a digital quartermaster arrangement. The PwC Threat Intelligence team tracks at least five China-based clusters as part of the Winnti collective, although it is notoriously difficult to distinguish among threat actors due to their likely use of a digital quartermaster.

The threat actors PwC tracks as part of the Winnti collective have also been linked to multiple supply chain attacks. Prominent examples include the compromises of CCleaner and NetSarang in 2017,[23, 24, 25] in which the threat actor deployed the ShadowPad backdoor, developed by one of the core threat actors in the Winnti collective. In October 2019, open sources reported that the ShadowPad backdoor had been updated, and was being used to target an Asian mobile software and hardware manufacturer, likely as part of a supply chain attack.

Since 2011, the Winnti malware family has been, and continues to be, deployed in targeted intrusions across a range of sectors. PwC research from May 2019 identified more than 150 systems spanning 23 countries and a wide variety of sectors that had been compromised by the Winnti malware.[26]

Victims within the entertainment and media sector include gaming companies, which aligns to the earliest known targeting by a threat actor using the Winnti backdoor.



[22] 'Operation ShadowHammer: a high-profile supply chain attack', Kaspersky, https://securelist.com/operation-shadowhammer-a-high-profile-supply-chain-attack/90380/ (23rd April 2019)

[23] 'Connecting the dots: Exposing the arsenal and methods of the Winnti Group', ESET, https://www.wired.com/story/inside-the-unnerving-supply-chain-attack-that corrupted-ccleaner/ (14th October 2019)

[24] 'ShadowPad in corporate networks', Kaspersky, https://securelist.com/shadowpad-in-corporate-networks/81432/ (15th August 2017)

[25] 'Inside the unnerving supply chain attack that corrupted CCleaner', Wired, https://www.welivesecurity.com/2019/10/14/connecting-dots-exposing-arsenal-methods-winnti/ (17th April 2018)

[26] 'Knock knock who's there?', PwC Threat Intelligence, CTO-TIB-20190514-01A

This graph displays the sectors targeted by the Winnti collective in order of most targeted.

Technology and telecommunications

Religious organisation/Dissident

Manufacturing

Government/public sector

Transport and logistics

Entertainment and media

Education

DNS hijacking

DNS hijacking involves compromising DNS infrastructure providers or related parts of the DNS ecosystem in order to access further victims. Compromising DNS infrastructure providers allows threat actors to modify DNS records and redirect traffic meant for a legitimate server to an attacker-controlled server instead. There were two large-scale DNS hijacking campaigns active during 2019, referred to as DNSpionage and Sea Turtle. DNSpionage was uncovered in November 2018, as a campaign initially targeting Lebanon and the UAE. In April 2019, a state-sponsored attack manipulating DNS systems was disclosed and named Sea Turtle.

- The two campaigns use different person-in-the-middle technologies, different proxies, and different infrastructure, yet both targeted DNS infrastructure providers and government entities.
- The Iran-based threat actor behind DNSpionage compromised the name servers of legitimate public sector websites in Lebanon and the UAE.[27] This allowed the threat actor to change DNS records for victim websites and, as a result, users attempting to reach the legitimate websites were unwittingly redirected to rogue IP addresses instead. Websites including ministries, airlines, and public domains in the Middle East were impacted.
- Teal Kurma – the Turkey-based threat actors behind Sea Turtle – used various methods to carry out DNS hijacking attacks.[28] They compromised organisations, pivoting through networks searching for credentials that would allow them to change DNS records. They also compromised DNS registrars. DNS registrars sell domain names and manage the DNS records on behalf of the customers. By compromising the registrars, the threat actor could change the registrars' customers' DNS records. Open-source reporting alleges that the Sea Turtle threat actor compromised at least one DNS registry. Registries manage top level domains, such as .com and .co.uk; compromising a DNS registry would allow the threat actor to alter a much greater number of DNS records.

A concern for the near future is that other threat actors will follow Sea Turtle's success and also attack the global DNS system – attacks that ultimately undermine the trust users have in the internet itself.

[27] 'DNSpionage campaign targets Middle East', Cisco Talos, https://blog.talosintelligence.com/2018/11/dnspionage-campaign-targets-middle-east.html (27th November 2018)

[28] 'Exclusive: Hackers acting in Turkey's interests believed to be behind recent cyber attacks – sources', Reuters, https://uk.reuters.com/article/uk-cyber-attack-hijack-exclusive/exclusive-hackers-acting-in-turkeys-interests-believed-to-be-behind-recent-cyberattacks-sources-idUKKBN1ZQ10S (27th January 2020)

Certified!

North Korea-based threat actor Black Artemis is known for its abuse of valid code-signing certificates to exploit trust and pass antivirus checks.[29] In June 2019, PwC analysts detected Black Artemis activity resembling the tradecraft displayed in an earlier intrusion against a Chilean bank.[30] The threat actor was using a valid digital certificate, issued by a global security company to a UK-based private limited company, to sign a GUI application mimicking a recruitment form, but actually downloading a malicious payload in the background. PwC assesses it is highly likely that the threat actor, or a cyber crime signing service in its supply chain, impersonated the UK-based company to obtain a valid certificate, rather than compromising the legitimate company, and that it is unlikely that the threat actor was trying to phish victims by posing as such a company.

What was notable in this campaign was that the threat actor employed a sophisticated process in order to obtain the certificate. Firstly, it likely conducted reconnaissance of vendors based in the UK with some software development capability, then, the threat actor directly contacted the certificate issuer masquerading as a legitimate company. The certificate issuer likely verified the legitimate company's identity based on the spoofed email address and other reputation-based services – which means that to succeed in spoofing the UK-based company, the threat actor had to socially engineer a reputation-based service, requesting an update of the contact details for the legitimate company and providing a spoofed email address instead. The same certificate was then used to sign a code injector utility utilised in a different campaign.[31]

Threat actor Andariel, which PwC tracks as a sub-group of Black Artemis, also abused valid digital certificates in the summer of 2019.[32] The threat actor exploited a certificate issued by a South Korean software security company to sign binaries of a new reloaded version of its historic tool Rifdoor in an espionage campaign PwC tracked as ANONYBR.

No Mr. Bond, I expect to read all your texts

In 2019, PwC analysed a malicious implant targeting mobile telecommunications infrastructure,[33] later called 'MESSAGETAP' in open-source reporting.[34] The implant runs at root level, which requires a threat actor to have already compromised a target in the telecommunications sector before deploying this tool. The malware is specifically designed to target Short Message Service (SMS) Centres and is able to monitor SMS messages in real time and extract their content and metadata. Given the features and capabilities of the malware, PwC assesses it is likely that the threat actor behind MESSAGETAP compromised telecommunications infrastructure used for SMS, and exploited the knowledge gained for cyber espionage activities. MESSAGETAP has the ability to target specific phone and International Mobile Subscriber Identity (IMSI) numbers, and even specific keywords contained in messages. PwC saw evidence suggesting that the malware was in development around May 2018, and that particular countries were being specifically targeted.

Similar tools were previously reported as being operated by intelligence agencies. It will be crucial to continue monitoring the evolution of this tool and activity associated with it, as the ability for a threat actor to deploy MESSAGETAP implies a capability to conduct both mass-scale as well as precise surveillance on targets.

---

[29] 'Exploiting inherent trust in certificates', PwC Threat Intelligence, CTO-SIB-20190312-01A

[30] 'Bluenoroff's recruitment drive', PwC Threat Intelligence, CTO-TIB-20190605-01A

[31] 'Lazarus is Watching', PwC Threat Intelligence, CTO-TIB-20190621-01A

[32] 'Rifdoor reloaded The ANONYBR campaign', PwC Threat Intelligence, CTO-TIB-20190905-02A

[33] 'Nono Mr Bond I expect to read all your texts', PwC Threat Intelligence, CTO-TIB-20191030-01A

[34] 'MESSAGETAP: Who is reading your text messages?', FireEye, http://www.fireeye.com/blog/threat-research/2019/10/messagetap-who-is-reading-your-text-messages.html (31st October 2019)

Threats to mobile

One of the defining trends of 2019 was the growing attention that threat actors turned to mobile malware and trojanised mobile applications, as well as to the exploitation of mobile devices more broadly.

PwC saw numerous threat actors active in this space, either using exploits to directly compromise victim mobile devices, or socially engineering targets into installing malicious applications on their mobile phones. Aside from financially motivated cyber criminal activities, in many of the cases that PwC observed mobile malware, it was used to target specific demographics, groups, or even individuals.

Malware in your pocket: Malicious applications make the rounds

Case study – ROKDROID, DragonMessenger, KevDroid

In August 2019, PwC tracked an espionage campaign by North Korea-based threat actor Black Shoggoth. The threat actor posed as an exponent of a Christian minority within North Korea in need of aid, indicating possible targeting of religious communities or defectors. The threat actor also sent spear-phishing emails mentioning a North Korean uranium mine; with realistic probability, the threat actor was trying to attract interest from the victim given the concurrent escalation of North Korean missile testing. The spear-phishing emails delivered samples of one of Black Shoggoth's main tools, ROKRAT, as well as a malicious Android application that PwC named ROKDROID. The application has in-built malicious functionality, is designed to remain persistent across phone reboots, and starts collecting information as soon as it is installed on a victim device. Its permissions indicate its functionality, which includes accessing the phone's camera and microphone, reading SMS messages, and processing calls. ROKDROID is able to communicate with Yandex or Dropbox C2s, and contains false-flag configuration information as well as anti-analysis measures.

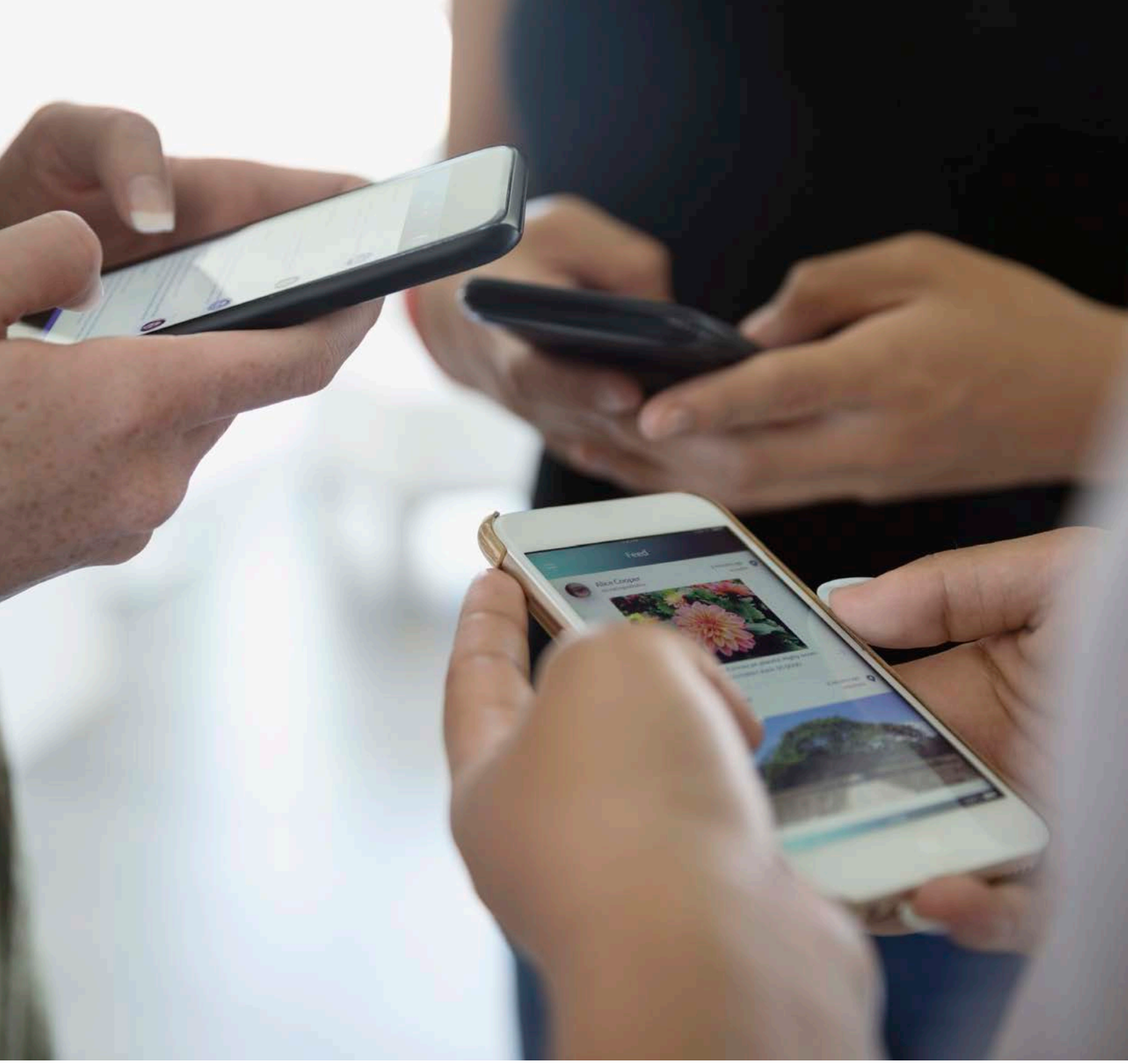
Around the same time as the ROKDROID campaign, Black Shoggoth also developed a malicious Android application known in open source as DragonMessenger, which, according to third-party research, was added to Google Play in October 2019.[35] The application was distributed via a WordPress website posing as a fundraising service for supporting North Korean defectors, and targeted that same demographic for espionage purposes.

This is not the first time that North Korea-based threat actors have experimented with trojanised or malicious applications, suggesting that this will, with realistic probability, continue to be an area of capability for development by the threat actors.

Case study – Fake voices in Kashmir

In July 2019, PwC detected a malicious Android application attempting to impersonate 'Kashmir Voice', a blog containing news about the Kashmir region.[26] Pivoting on the application's metadata, PwC analysts identified multiple related resources: fragments of document exploits, process dumps, network fingerprinting tools and anonymity tools, as well as Android development frameworks. PwC assesses that an individual that operates within a known India-based espionage threat actor likely developed the Android application. The application was highly likely designed for espionage rather than cyber criminal purposes, targeting individuals in Kashmir or with an interest in Kashmir, during a heightened state of geopolitical tension around the region.

[35] 'Dragon Messenger', ALYac EST Security, https://blog.alyac.co.kr/attachment/cfile1.uf@99A46A405DC8E3031C9E2A.pdf (11th November 2019)



Dangers to two-factor authentication

Cyber criminal threat actors also increasingly targeted mobile devices as a new revenue stream. The techniques and tools used varied from fraudulent banking applications used to capture access credentials, to full-scale malware systems designed to intercept messages and harvest data stored on infected devices.[36] The introduction of the Second European Payment Services Directive (PSD2) in 2019 added Strong Customer Authentication (SCA) to online transactions and contactless payments. Once fully implemented, online transactions will require some form of two-factor authentication (2FA), and many 2FA solutions rely on authentication via SMS or voice messages to confirm transactions. Cyber criminal threat actors have already developed techniques targeting SMS 2FA solutions used for online banking and ecommerce systems. For example, in February 2019, threat actors intercepted text messages containing two-factor authentication codes for customer transactions with a UK-based bank.[37] They exploited flaws in the Signalling System 7 protocol to bypass the two-factor authentication used by the bank, defrauding a small number of customers. In a later case, the threat actors behind the TrickBot malware introduced a new module in July 2019 to capture data required to conduct SIM-swapping attacks, which enables them to port a victim's mobile phone account to a device under criminal control. Once established, the attackers can intercept incoming voice and SMS messages and authorise payments via SMS-based 2FA.[38]

[36] 'McAfee Mobile Threat Report', McAfee, https://www.mcafee.com/enterprise/en-us/assets/reports/rp-mobile-threat-report-2019.pdf

[37] 'Criminals hit Metro Bank with multi-factor authentication bypass SS7 attack', SC Media, https://www.scmagazineuk.com/criminals-hit-metro-bank-multiauthentication-bypass-ss7-attack/article/1524670 (4th February 2019)

[38] 'Analysis of a recent Emotet/Trickbot campaign', PwC Threat Intelligence, CTO-TIB-20191011-01A

Cyber crime scene

Cyber criminal activity continued to be an extremely significant threat to commercial organisations and enterprises. Despite law enforcement crackdowns and temporary lulls in activity, the cyber criminal market effectively consolidated around large, established players behind some of the largest cyber criminal operations. PwC also observed a solid continuation of 2018 trends, including formjacking and Magecart skimmers (which we discuss later in this section), as well as the proliferation of ransomware variants – ranging between spam operations and extremely narrowly targeted attacks.

However, PwC also saw new financially motivated threat actors rise to prominence, such as TA505, known for large scale spam operations, and White Jackalope (**a.k.a.** Silence) with its international targeting of banks. Likewise, the cyber criminal market increasingly sought a diversification of revenue streams; rather than relying on the theft of banking credentials or POS malware, ransomware was often seen as an effective means to this end.

Finally, one of the most interesting observations on the cyber criminal front in 2019 was evidence suggesting that certain threat actors, long considered to be espionage motivated and with objectives aligned to national interests, have been duplicating and dividing their efforts to also perform cyber criminal activities.

Double-down espionage-crime

Historically, criminal threat actors and advanced persistent threats (APTs) acted in strict alignment with their individual aim or tasking, focusing on fulfilling one specific objective – either espionage or financial gain for example. Even in cases where a threat actor would run multiple concurrent campaigns with different victims, these tended to be linked by an overarching purpose such as intellectual property theft, or intelligence collection. In 2019 however, PwC observed a growing trend of threat actors 'doubling-down' their operations: conducting sophisticated and targeted espionage campaigns as well as financially motivated ones, at times even concurrently. In some cases, the financially motivated element of these 'double' operations is run on the side of other tasking by the same operators responsible for espionage campaigns. However, in other cases, this duplication of purpose and targets highly likely stems from direct or indirect state tasking aligning with government strategic objectives.

It's not all games

The threat actor that PwC tracks as Red Kelpie (**a.k.a.** APT41) has been active since at least 2012, and has compromised a significant number of organisations on a global scale and across sectors including technology, telecommunications, and healthcare. In compromising such organisations, Red Kelpie mostly sought to exfiltrate intellectual property, confidential business information, or intelligence to be used for surveillance – but the same threat actor is also known to attack victims for financially motivated reasons.[39, 40] In its continued targeting of the video game industry since 2012, and of cryptocurrency organisations since at least 2019, Red Kelpie used the same toolset for both financially motivated attacks and espionage operations. However, despite overlaps in toolset and infrastructure,[41] the manipulation of in-game currencies as well as attempts to deploy commodity ransomware on certain victims' systems suggest that Red Kelpie runs financially motivated operations that are separate, and very different, from its espionage activity.

Crimson for crime

Another espionage-focused threat actor that also engaged in cyber criminal activity is Green Havildar. Green Havildar has been consistent in its targeting of the Indian government and military, as well as other nations, such as Kazakhstan, since 2016. In this timespan, the threat actor has progressively widened its toolset, automated the building of its main malware tool CrimsonRAT, and taken steps to incrementally improve its anti-detection capabilities as well as operational security.[42] However, in 2018, PwC was able to connect Green Havildar to Gorgon Group, a threat actor engaging in financially motivated cyber criminal activity. At that time, PwC assessed that Gorgon Group at the very least shared access to resources as well as infrastructure with Green Havildar.[32] In the autumn of 2019, PwC tracked a spam campaign by Gorgon Group distributing commodity backdoors as well as CrimsonRAT for cyber criminal purposes, rather than espionage. The use of CrimsonRAT, which so far is uniquely tied to Green Havildar, supports the assessment that Gorgon Group is an integral part of Green Havildar, and that it is able to conduct financially motivated campaigns that are independent of the threat actor's espionage operations.[43]

---

39 'Nono, Mr Bond, I expect to read all your texts', PwC Threat Intelligence, CTO-TIB-2019-10-30-01A

40 'Knock Knock Whos there', PwC Threat Intelligence, CTO-TIB-20190514-01A

41 'Double Dragon: APT41, a dual espionage and cyber crime operation', FireEye, https://content.fireeye.com/apt-41/rpt-apt41/ (7th August 2019)

42 'Unmasking Green Havildar', PwC Threat Intelligence, CTO-20181127-01A

43 'Crimson for Crime', PwC Threat Intelligence, CTO-TIB-20191028-01A

Shoot to the stars (and the crypto)

Continuing on from their 2018 activity, North Korea-based threat actors Black Artemis and Black Banshee aggressively pursued and mixed cyber espionage and financially motivated cyber criminal activity.[44] In 2019, both threat actors had a shared focus on the aerospace and defence sectors from an espionage standpoint, while also showing consistent targeting of financial institutions and organisations in the cryptocurrency space.[45, 46, 47]

Incumbent leaders in cyber crime: Old dogs, new tricks – Part 1

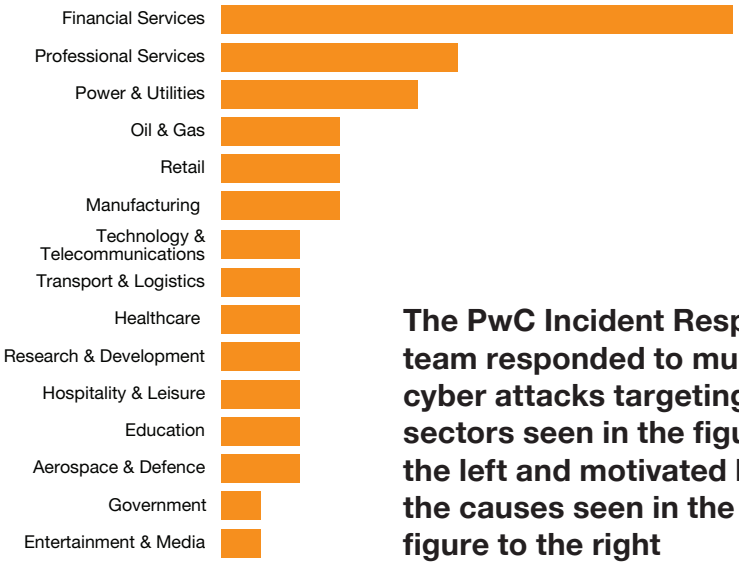
Some of the most prominent criminal threat actors have been active since the early 2000s, often originally as subordinate members or affiliates of now-defunct groups. These groups used to be active on criminal forums, where they recruited affiliates for their own enterprises or hired services from third parties. In 2019, the old guard were far less active in this respect, instead relying on trusted relationships that they built up from years of successful cooperation.

Although identified as an emerging phenomenon in 2018, 2019 has seen a clear convergence in some of the tools, techniques, and procedures (TTPs) employed by a range of established threat actors. Those previously focused on point-of-sale (POS) systems in the retail and hospitality sector broadened their targeting to include online retailers and modified their toolsets as a consequence. Similarly, while threat actors in control of high-profile credential stealing malware, such as TrickBot and Dridex, continued to harvest financial data from consumers, these threat actors increasingly used those systems as a platform from which to launch targeted ransomware attacks against a range of corporate victims. However, targeted ransomware attacks were also carried out by threat actors that had previously been engaged exclusively with POS malware, possibly through cooperation with specialist ransomware actors or by becoming affiliates of ransomware operations.

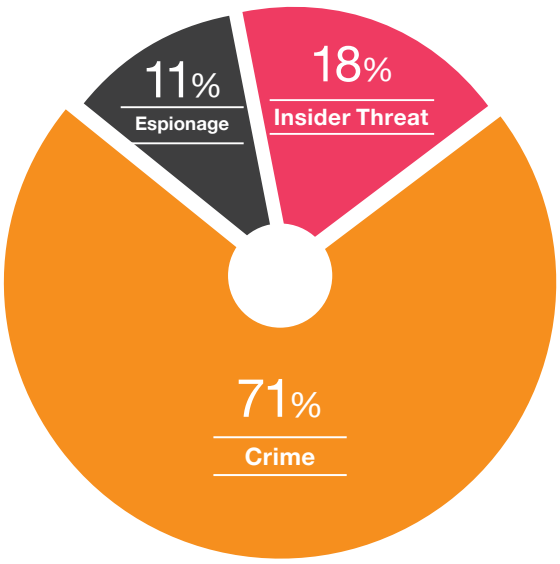
Formjacking frenzy: Magecart

The umbrella term 'Magecart' describes the use of JavaScript-based malware to capture payment card information from compromised online retailers or their third-party ecommerce platforms. The technique is often referred to as 'digital skimming' or 'formjacking' as the malware grabs the data entered by a consumer during the checkout process. Unlike POS malware, Magecart not only captures payment card information, but also the billing address, CVV2 number, and (depending on the data required by the retailer) email and phone number.

Magecart is not a single entity but rather consists of at least 30 different threat actors that possess varying levels of sophistication and employ different TTPs. The most prominent Magecart threat actor is Magecart Group 5, which is associated with the compromise of a major ticket sales and distribution company, and specialises in targeting third-party suppliers to compromise



The PwC Incident Response team responded to multiple cyber attacks targeting the sectors seen in the figure to the left and motivated by the causes seen in the figure to the right



[44] Cyber Threats 2018: A Year in Retrospect
[45] 'A Month of Manuscrypt', PwC Threat Intelligence, CTO-QRT-20190809-01A
[46] 'A Black Banshee goes Wild(Command)', PwC Threat Intelligence', CTOTIB-20190509-02
[47] 'Mixed intentions', PwC Threat Intelligence, CTO-TIB-20191106-01A

multiple ecommerce operators. Magecart Group 6 targets 'household name' companies and was attributed to attacks on an international airline and a major consumer electronics retailer. In October 2019, reports revealed that Magecart Group 6 is likely linked to White Giant (**a.k.a.** FIN6), also responsible for an attack on an ecommerce platform provider that put over 3,000 online retailers at risk.[48]

FINs can only get better?

FIN6, FIN7, and FIN8 are threat actors that specialise in targeting the retail and hospitality sectors, with the primary objective of harvesting payment card information from compromised networks. Their attacks involve either the deployment of malware onto multiple POS devices within a compromised network or attacking the victim's payment processing systems. While all the threat actors share similar TTPs (spear-phishing attacks, living off the land, and penetration testing tools) they all have unique characteristics: FIN6 and FIN8 have their own bespoke POS malware (FrameworkPOS and ShellTea respectively) while FIN7 has developed and deployed a new range of tools in 2019. In most of their attacks, the threat actors attempt to maintain persistence in the compromised network for as long as possible in order to harvest payment card information over an extended period. These intrusions can last for several months and in the past resulted in the compromise of hundreds of thousands, and in some high-profile cases, millions of payment cards.[49, 50] Successful POS malware attacks harvest the data encoded on the magnetic stripe of a payment card when it is swiped through a card reader. This data, known as a 'dump' by criminal actors, is sold on specialist criminal vendor sites, the most prominent of which is Joker's Stash.

In 2019, it was predicted that the cost of counterfeit payment card fraud in the US would drop in line with the growing use of EMV technology in the restaurant, hospitality and retail sectors.[51] Within criminal forums, there was speculation that wider use of EMV in the US would disrupt the market for dumps. However, both the price and supply of dumps appears to have been stable throughout 2019. In August 2019, Joker's Stash announced the sale of 5.3 million dumps in what was advertised as the Solar Energy Breach, although they were careful to release the data in batches rather than flood the market with all 5 million cards in one go. The data appeared to be harvested from a US retailer. In October 2019, Joker's Stash advertised a further 1.3 million dumps, this time originating from India.[52, 53] In view of continued release and sale of dumps data, it is clear that the hoped-for decline in POS malware operations did not materialise in 2019.

Enter the stage: new players in the cyber criminal space

In a Silence way

The financially motivated threat actor White Jackalope (**a.k.a.** Silence) has been active since mid-2016, and was first reported on in open source at the end of 2017.[54, 55] In 2018 and 2019, the activity of the threat actor significantly increased, as well as the scope of its targeting.[56, 57] Originally focusing on the banking sector in Russia, the threat actor expanded its targeting to include Asia, and eventually the rest of Europe.

White Jackalope has evolved its toolset over time, adjusting its initial downloaders and payloads to constantly evade detection. Its ongoing campaign, being conducted across countries in Eastern Europe, uses a technique called 'ATM jackpotting' – compromising ATM systems in order to dispense cash at will, and relying on a network of money mules to physically move and launder the notes.

The cyber criminal threat actor achieved its aims through two alternative paths of intrusion:

- Compromising the bank's internal ATM network (known as a card management system) and enabling a waiting money mule to physically withdraw money using bank-issued credit cards at the victim bank's ATMs; and
- Compromising the card processing system to remove or alter the withdrawal limit (usually USD 1,000) for use in conjunction with stolen cards to yield the greatest amount per stolen card.

In July 2019, the threat actor reportedly cost a targeted bank a total of USD 3 million and leveraged a combination of physical and cyber aspects to enable the theft of money.[58]

The tactics of White Jackalope led us to assess that this cyber criminal threat actor is likely to be sophisticated and continue attempting to remain stealthy (excluding the activities of its mule operators).

---

48 'FIN6 compromised ecommerce platform via Magecart to inject credit card skimmers into thousands of online shops', TrendMicro, https://blog.trendmicro.com/trend-labs-security-intelligence/fin6-compromised-e-commerce-platform-via-magecart-to-inject-credit-card-skimmers-into-thousands-of-online-shops/ (9th October 2019)

49 'Dissecting the activities and operations of FIN6 threat actor group', cyware, https://cyware.com/news/dissecting-the-activities-and-operations-of-fin6-threat-actor-group-ebc7df0a (13th April 2019)

50 'HBC says data breach lasted up to 9 months', CBC, https://www.cbc.ca/news/business/hbc-saks-data-breach-1.4638249 (27th April 2018)

51 'The future of US fraud in a post-EMV environment', Retail Payments Risk Forum, June 2019, https://www.frbatlanta.org/-/media/documents/rprf/publications/2019/06/23/future-of-us-fraud-in-post-emv-environment-king-doug.pdf

52 'Breach at Hy-Vee supermarket chain tied to sale of 5M+ stolen credit, debit cards', KrebsonSecurity, https://krebsonsecurity.com/tag/hy-vee-breach/ (19th August 2019)

53 'Joker's Stash lists 1.3 million stolen Indian payment cards', BankInfoSecurity, https://www.bankinfosecurity.com/jokers-stash-lists-13-million-indian-payment-cards-a-13302 (29th October 2019)

54 'Silence – a new Trojan attacking financial organisations', Kaspersky, https://securelist.com/the-silence/83009/ (1st November 2017)

55 'Silence', PwC Threat Intelligence, CTO-QRT-20171106-01B

56 'Silence: Moving into the darkside', Group-IB, September 2018, https://www.group-ib.com/resources/threat-research/silence_moving-into-the-darkside.pdf

57 'Silence 2.0: Going Global', Group-IB, August 2019, https://www.group-ib.com/resources/threat-research/silence_2.0.going_global.pdf

58 'Silence Groups not-so-silent attack', PwC Threat Intelligence, CTO-QRT-20190719-02A

Spotlight on TA505

TA505 is a cyber criminal threat actor, active since at least 2014, which first came to prominence for large-scale malicious spam operations primarily delivering Dridex. Since then, the group has been associated with numerous spam campaigns delivering a broad range of malicious payloads, including the banking trojans TrickBot and Shifu and the ransomware systems Locky and GlobeImposter.[59] In addition to providing a delivery mechanism for other threat actors, TA505 is associated with the development and deployment of its own bespoke malware, including FlawedAmmyy and FlawedGrace.

In 2019, the threat actor redoubled its efforts, introducing multiple new tools and broadening its range of targets. In October 2019, the actor began deploying a new modular malware system known as SDBot after introducing two new downloaders: Andromut and Get2.[60] In November 2019, PwC identified a new high-volume TA505 campaign targeting a wide range of industry sectors and victims,[61] which used several legitimate URL shortening services to direct victims to fake landing pages. These were used to host downloadable versions of the penetration testing tool Cobalt Strike as part of an initial infection process.

ATM cashouts

The first case of ATM jackpotting took place in Mexico in 2013,[62] where threat actors attached a new boot disk that installed malware on the ATMs. Attacks have since become more sophisticated, with prominent campaigns including the following:

- Since at least late 2016, Black Artemis has targeted banks in Africa and Asia in order to gain access to payment switch application servers and enable fraudulent ATM cash withdrawals;[63]
- In late 2018, Black Artemis compromised the corporate network of the Chilean ATM interbank network – while the organisation claims the incident was mitigated before any money was stolen, it is likely the attack was financially motivated;[64] and,
- In 2019, reporting uncovered attacks against banks across Asia that resulted in ATM jackpotting. These are attributed to a criminal threat actor, White Jackalope (**a.k.a.** Silence).[58]

Spotlight on Cobalt Group

The Cobalt Group is a threat actor that has specialised mainly in ATM attacks since it first became active in 2016. Its name is derived from the legitimate penetration testing tool Cobalt Strike: the threat actor was one of the first criminal groups to adopt the use of this tool as part of its standard TTPs. Throughout the year, the threat actor used a combination of third-party tools, including Terraloader (also known as more_eggs) and a malicious document builder for dropping and executing JavaScript. The most distinguishing aspect of its operations was the continued use of its own bespoke malware, CobInt. Cobalt campaigns were almost continuous during 2019, with a variety of phishing lures designed for attacking financial institutions. Many of these were spoofed to appear to be from the European Central Bank, while others purported to contain the outcome of legal or financial arbitration decisions. Based on the language used for its phishing messages, Cobalt was mainly targeting victims in Eastern Europe and Central Asia, with a smaller number of attacks focused on Central America and the Middle East.

---

59 'Threat actor profile: TA505, from Dridex to GlobeImposter', Proofpoint, https://www.proofpoint.com/us/threat-insight/post/threat-actor-profile-ta505-dridex-globeimposter (27th September 2017)

60 'TA505 distributes new SDBbot remote access trojan with Get2 downloader', Proofpoint, https://www.proofpoint.com/us/threat-insight/post/ta505-distributes-new-sdbbot-remote-access-trojan-get2-downloader (16th October 2019)

61 'TA505 ups the ante with fake landing pages', PwC Threat Intelligence, CTO-QRT-20191118-01A

62 'Criminals hit the ATM jackpot', Symantec, https://www.symantec.com/connect/blo gs/criminals-hit-atm-jackpot (11th October 2013)

63 'HIDDEN COBRA – FASTCash campaign', CISA, https://www.us-cert.gov/ncas/alerts/TA18-275A (2nd October 2018)

64 'One unified platform to run your entire business', ZDNet, https://www.zdnet.com/article/north-korean-hackers-infiltrate-chiles-atm-network-after-skype-job-interview/ (16th January 2019)

Diversification of revenue

Emotet resurgent

In the first quarter of 2019, Emotet was one of the most prolific malware delivery systems, accounting for 60% of email traffic containing malicious payloads (attachments and hyperlinks).[65] At the end of May 2019, Emotet suspended operations: its C2 network dropped connections to infected hosts and spam campaigns halted. On 22nd August 2019, Emotet's C2 network reactivated and by 9th September its C2 servers began pushing out new binaries to infected hosts. Spam operations resumed on 16th September and began pushing out new spam campaigns almost daily.[66] The reliance of multiple threat actors on delivery systems such as Emotet saw a continuation of a well-established trend: the use of phishing techniques to deliver weaponised attachments that all but supplanted the use of exploit kits as a means of introducing malware into targeted networks.

In addition to its capacity to deliver high volumes of broadcast spam, increasing use was made of Emotet's spear-phishing capabilities in 2019. The malware harvests the content of email accounts on infected hosts and can insert messages into existing email threads between the infected host and third parties. It is likely that email thread injection attacks are more effective than the bulk delivery of unsolicited messages: a recipient will be less suspicious of an attachment in a message they were expecting to receive from a known contact. Both broadcast and spear-phishing techniques were used as a delivery system by a range of sophisticated cyber crime threat actors, including the Trickbot/Ryuk, Gozi/Ursnif and Qakbot groups. Emotet was also used less frequently for the delivery of Dridex.

Old dogs, new tricks – Part 2

As with all leading credential-stealing malware, systems like TrickBot, Dridex, Ursnif and Ramnit are modular in design and can tailor their functionality based on customer requirements. This is especially the case with inject codes used to capture bank and ecommerce login credentials from infected hosts. For example, TrickBot variants delivered by an Emotet campaign targeting the UK are configured to download inject modules crafted for a range of UK banks and other entities. But TrickBot can do more than just capture banking credentials: in late 2018 TrickBot added a module to identify POS systems, enabling threat actors to conduct POS attacks similar to those employed by FIN6 and FIN7. As noted earlier in this report, in 2019 it added a new inject module to support SIM-swapping attacks. And along with Dridex and possibly Qakbot, TrickBot was increasingly used in targeted ransomware attacks.

The DiabolicalTrinity: Emotet/ TrickBot/Ryuk

2019 saw a succession of high-profile ransomware attacks attributed to Ryuk. The majority of these incidents involved an initial infection via Emotet that carried TrickBot as a secondary payload. The threat actor used TrickBot's worming and lateral movement modules in combination with legitimate penetration testing tools and living-off-the-land techniques to spread through targeted networks, identify key infrastructure and install and execute Ryuk. In many cases, the threat actors spent at least two weeks inside the victim network before deploying Ryuk, mainly because the post-exploitation phase of the attack involved time-consuming, semi-manual processes. The impact of a Ryuk attack means that it was often difficult for incident responders to demonstrate that data was exfiltrated prior to the activation of the ransomware. However, as the primary delivery method for Ryuk is a combination of two powerful credential stealers, which both automatically harvest data, it is likely that some degree of data exfiltration occurred prior to encryption.

Dridex and BitPaymer

Although Dridex threat actors used Emotet as a delivery mechanism in 2019, they did not do so as frequently as TrickBot or Ursnif threat actors. They also used compromised websites as an infection vector, inserting malicious JavaScript into vulnerable websites to display a fake browser update. Clicking on the update would activate the initial malware insertion process. Dridex is almost uniquely associated with its ransomware counterpart, BitPaymer. After the initial Dridex installation process, a BitPaymer incident follows the same pattern described in an Emotet/TrickBot/ Ryuk attack. BitPaymer underwent an upgrade in 2019, and emerged with new network enumeration capabilities in the middle of the year to improve the efficiency of attacks[67] – the upgrade included the use of the address resolution protocol (arp) to identify devices on a victim network to add a degree of automation to the post-exploitation phase of a Dridex/BitPaymer incident.

Follow the cryptocurrency

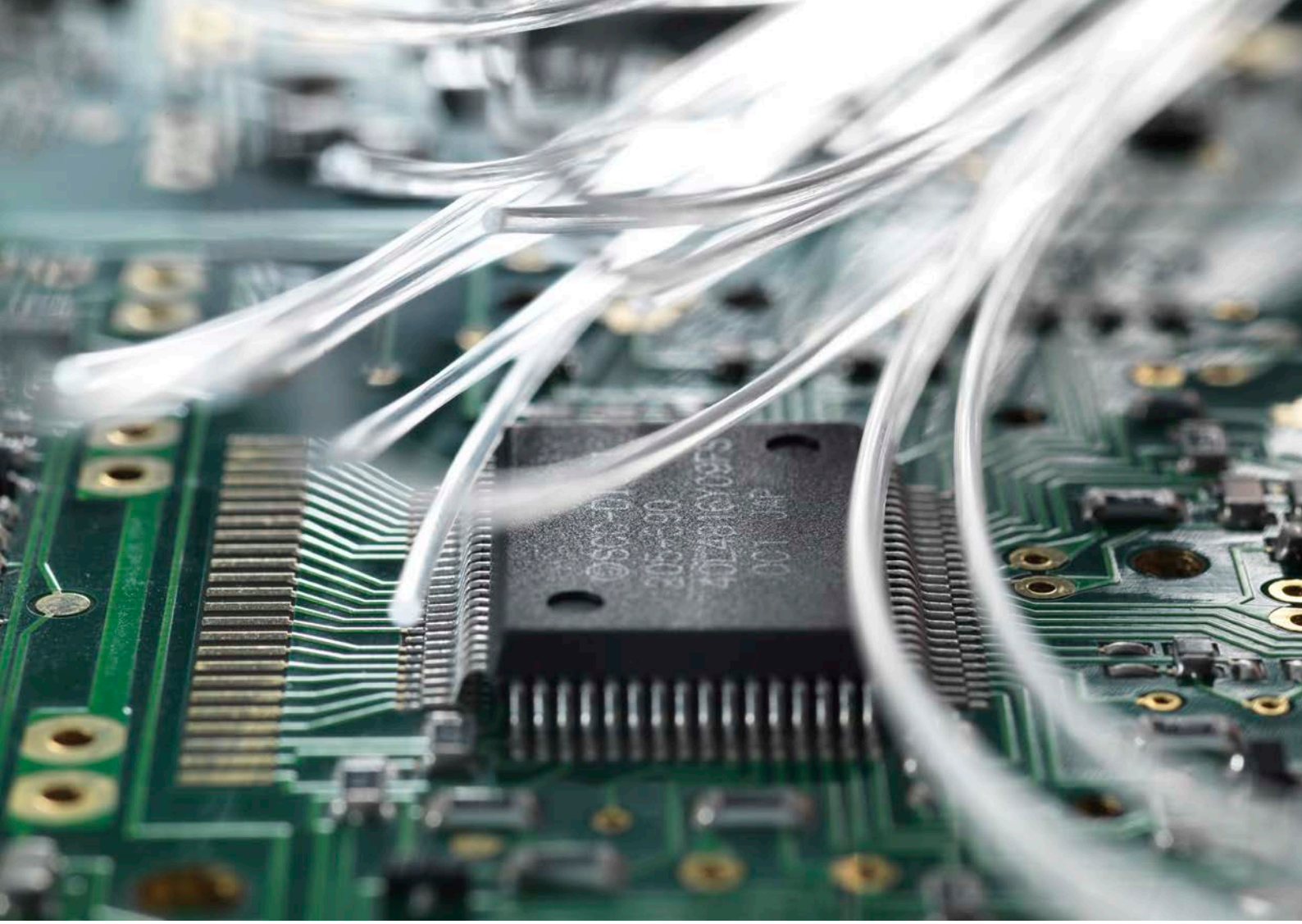
The diversification into ransomware operations was certainly one of the main cyber crime themes of 2019, but it would be incorrect to assume Dridex or TrickBot threat actors abandoned credential theft in favour of ransomware operations. Dridex and TrickBot were originally designed as banking trojans, and along with other threat actors like the Ramnit, Ursnif and Qakbot groups, they still retain this capability and attacks on online banking systems leveraged by

---

65 'Latest Quarterly Threat Report – Q1 2019', Proofpoint, 2019, https://www.proofpoint.com/us/resources/threat-reports/latest-quarterly-threat-research

66 'Analysis of a recent Emotet Trickbot campaign', PwC Threat Intelligence, CTO-TIB-20191011-01A

67 'BitPaymer's recent European sprint', PwC Threat Intelligence, CTO-TIB-20191115-02A



these groups continued throughout 2019. But these 'business-as-usual' activities were overshadowed by the media attention focused on high-profile ransomware attacks that resulted from TrickBot or Dridex infections.

In reality, many of the principal cyber criminal threat actors operated affiliate programmes and leased access to their systems on a fee-paying or profit-sharing basis. In the case of TrickBot, it is likely that only a small number of affiliates had access to Ryuk and that the majority of TrickBot threat actors were focused on traditional, credential-stealing activities. Likewise, only a subset of Dridex actors appeared to have access to BitPaymer. The attraction of ransomware was almost certainly due to its high return on investment compared to online banking attacks:

- The majority of online banking attacks were detected before funds were transferred;[68]
- Even after funds were transferred to a bank account under criminal control (a mule account), in many cases the victim's bank was able to freeze the transfer and prevent the criminals from withdrawing the funds;
- A successful transfer of stolen money required careful coordination with the mule controllers and is labour intensive;
- The threat actors must have paid commission fees to the mule controllers and often received little more than 30-40% of the funds transferred in a successful attack; and
- Threat actors engaged in the transfer and laundering of stolen funds risked detection and prosecution by law enforcement organisations.

By contrast, apart from the overheads associated with managing malware infrastructure, and membership fees for participating in an affiliate programme, ransomware threat actors got to keep the majority of the funds generated from successful attacks, and incurred lower commission fees when they convert cryptocurrency into fiat currency.

Other threat actors, such as FIN6 and FIN7, comprehensively demonstrated their ability to infiltrate and compromise corporate networks. They mostly did so for the purpose of deploying POS malware, which by necessity restricts their range of available targets. Their business model is not fully understood, especially the share of the profits they make from the sale of compromised payment card information. While there is isolated reporting that FIN6 was involved in LockerGoga and possibly Ryuk incidents in early 2019,[69] PwC is not aware that they did so in the second half of the year. However, PwC assesses that threat actors such as FIN6 have the technical capability to conduct further ransomware attacks if they choose.

---

68 'Fraud the facts 2019', UK Finance, 2019, https://www.ukfinance.org.uk/policy-and-guidance/reports-publications/fraud-facts-2019

69 'Pick-Six: Intercepting a FIN6 intrusion, an actor recently tied to Ryuk and LockerGoga ransomware', FireEye, https://www.fireeye.com/blog/threat-research/2019/04/pick-six-intercepting-a-fin6-intrusion.html (5th April 2019)

Resident Evil: The indictment of Maksim Yakubets

From a crime perspective, the highlight of 2019 was the high-profile indictment of members of the Dridex group, self-styled as 'Evil Corp'. Maksim Yakubets, also known by his online identity Aqua, and Igor Turashev, a senior member of the group known online as Nintutu, were both indicted by the US Department of Justice on 5th December 2019. Other members of the group were named (but not indicted) including Denis Gusev, whose businesses were subject to US sanctions imposed by the US Treasury Department. The indictments were the result of years of work by the FBI and the UK's National Crime Agency (NCA), with the latter revealing details of the group's lavish lifestyle. A significant part of the Dridex saga was the revelation that Yakubets had also been working on behalf of the Federal Security Service (FSB)[70, 71] since 2017, in addition to his purely criminal operations. This appears to be the mirror image of state actors either officially or unofficially conducting financially motivated attacks: a long-established criminal actor carrying out undisclosed activities on behalf of the state.[72]

Ransomware threat intensifies in 2019

The last 12 months have seen a succession of high-profile ransomware attacks affecting a broad range of victims and sectors. In 2018, there was a notable change in threat actor behaviour, with an emphasis on targeted attacks in preference to the large-scale distribution of ransomware. In 2019, this trend for 'big game hunting' became firmly established with an increase in the intensity and frequency of attacks, the arrival of new ransomware threat actors and the deployment of ransomware by established crime groups that previously specialised in other types of attack. Businesses in the manufacturing, oil and gas, professional services, healthcare and logistics sectors were all prominent victims in 2019. Local government and the education sector were also hit hard, with the latter experiencing highly damaging attacks timed to coincide with the reopening of schools and colleges in September 2019.

One threat actor known as GandCrab, which ran an affiliate-based, ransomware-as-a-service (RaaS) platform, announced its 'retirement' and ceased operations in June 2019. However, a new ransomware strain known as Sodinokibi or REvil emerged soon afterwards, and given the coding similarities between the two malware families it is likely that Sodinokibi was little more than a rebranding exercise by the GandCrab threat actor and the 'retirement' was merely a smokescreen.[73] Sodinokibi attacks increased in tempo during the fourth quarter of 2019, with a number of high profile incidents reported in the last few weeks of the year.

Case study – Lockergoga

LockerGoga ransomware struck victim organisations of all sizes across multiple continents and industries, yet, in early 2019, a LockerGoga campaign appeared to intentionally target organisations in the manufacturing sector. Norsk Hydro, one of the largest aluminium and renewable energy companies, had systems across 40 countries infected with LockerGoga malware. To carry out this targeted attack, the threat actor likely compromised and studied Norsk Hydro's internal IT architecture prior to deploying the ransomware. Norsk Hydro was forced to resort to manual operations as a result, and the operational downtime and mitigation efforts cost the company more than GBP 47 million in losses.[74]

Case study – BitPaymer strikes professional services

In November 2019, the Spanish professional services company Everis was the victim of a ransomware attack.[75] Initially, there was widespread media speculation that the victim had been targeted by Ryuk – this was partly because multiple Ryuk incidents were underway at the time of the attack, but also possibly because Ryuk had gained such notoriety in the preceding months that it had become almost synonymous with ransomware. In reality, the incident was the result of a BitPaymer attack that had been leveraged through a conventional Dridex campaign.

---

70 'Russian contractor document leak', PwC Threat Intelligence, CTO-SIB-20190812-01A

71 'Hackers breach FSB contractor, expose Tor deanonymization project and more', ZDNet, https://www.zdnet.com/article/hackers-breach-fsb-contractor-expose-tordeanonymization-project/ (20th July 2019)

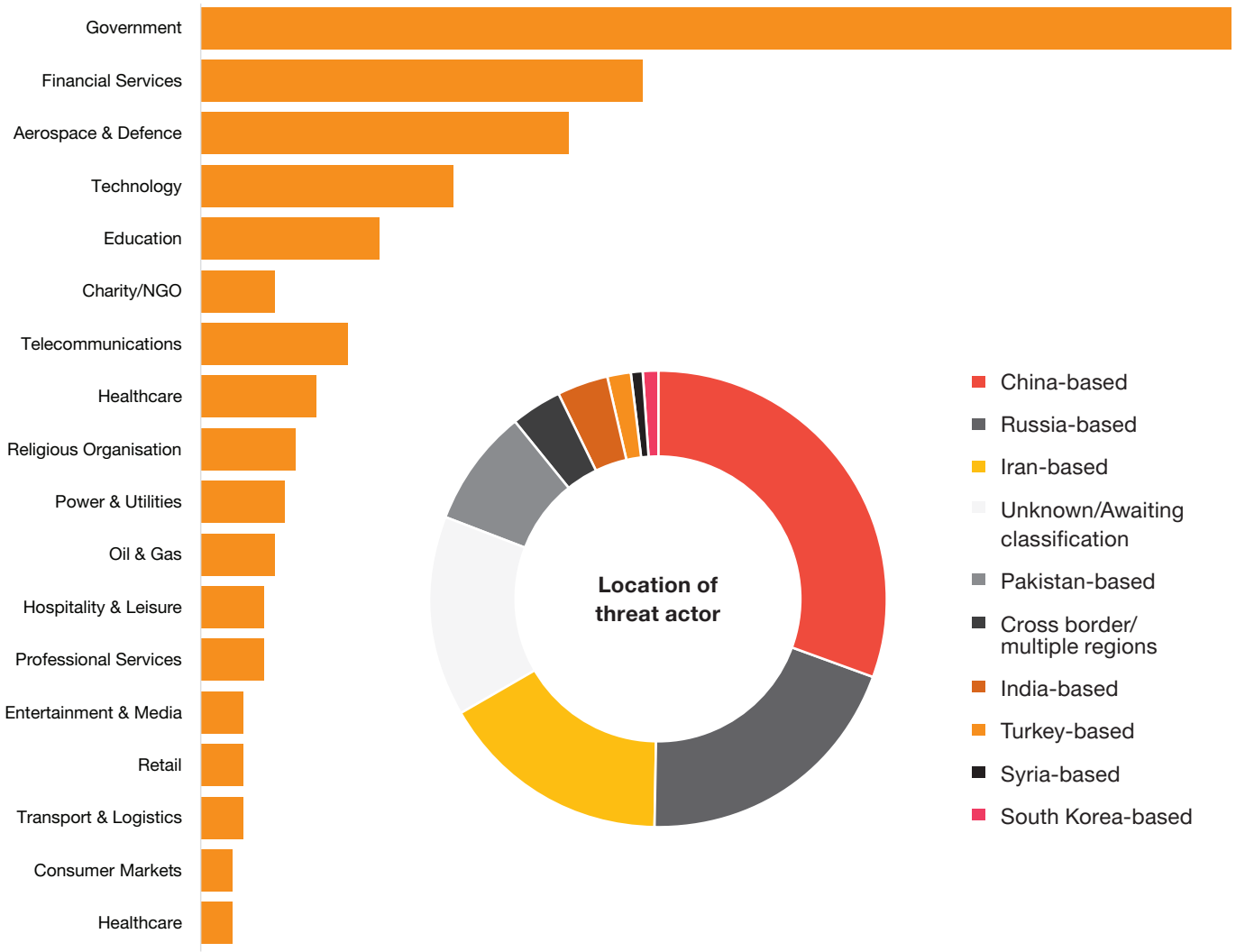
72 'Russian national charged with decade-long series of hacking and bank fraud offenses resulting in tens of millions in losses and second Russian national charged with involvement in deployment of 'Bugat' malware', Department of Justice, https://www.justice.gov/opa/pr/russian-national-charged-decade-long-series-hacking-and-bank-fraud-offenses-resulting-tens (5th December 2019)

73 'Notorious GandCrab hacker group returns from retirement', BBC, https://www.bbc.co.uk/news/technology-49817764 (24th September 2019)

74 'Norsk Hydro reveals initial cyber insurance payout', Insurance Business UK, https://www.insurancebusinessmag.com/uk/news/cyber/norsk-hydroreveals-initial-cyber-insurance-payout-189461.aspx (24th October 2019)

75 'BitPaymers recent European sprint', PwC Threat Intelligence, CTO-TIB-20191115-02A

The PwC Threat Intelligence team issued 221 intelligence reports in 2019 covering a range of sectors and threat actor locations, as seen below.



Looming larger: distributed denial of service attacks keep growing

Throughout 2019, distributed denial of service (DDoS) attacks remained a steady trend in the background of other cyber operations. DDoS attacks rose to prominence many years earlier as one of the preferred tools in the arsenal of hacktivist threat actors as a means to conduct disruptive action. This was partly due to the relatively low barrier to entry for conducting such attacks, and the highly visible nature of their impact (i.e. knocking a website or service offline for a period of time).

As organisations have moved to protect themselves from DDoS attacks, threat actors increasingly sought to launch fewer but more targeted attacks and developed novel techniques to amplify attacks and overcome DDoS mitigations. Furthermore, with the proliferation of connected devices and the growth of the Internet of Things (IoT), more and more exploitation paths and malware families have emerged to compromise these devices and enslave them into botnets. An example from 2019 includes a multi-stage infection chain delivering a BillGates malware variant, which was used to hijack non-updated versions of Elasticsearch databases and coerce their host systems into botnet activity.[76] Just as the creation of these large-scale botnet networks in turn facilitated larger-scale DDoS attacks, the cyber criminal ecosystem also turned to DDoS-as-a-Service and DDoS-for-hire offerings to monetise botnet creation.

Many DDoS-for-hire services are advertised on the darkweb as stresser services. Typically, they purport to be legitimate services for network administrators, providing a resource to test the resilience of a network to a DDoS attack. Pricing for stresser services varies according to duration of attacks, with 'reputable' services offering attacks for USD 10 per hour.[77] Despite prominent law enforcement operations against stresser sites, in 2019 they continued to persist and were frequently advertised within online gaming communities. The attack capabilities of these services varied, and it is likely that in many cases their advertised capability was exaggerated. Academic research suggests that the commissioning of DDoS attacks by juveniles within the online gaming community served as an entry-level cyber crime and some cases led to other cyber offending.[78]

Ransom DDoS

In 2019, cyber criminal threat actors continued targeting businesses with DDoS attacks – even attempting to extort victims for financial gain to refrain from, or cease, targeted DDoS attacks. In some cases, threat actors will send victims a ransom note demanding payment even before an actual attack is performed, promising a 'small attack' as a tester to threaten victims and coerce them into paying attackers to deter them from launching an actual DDoS attack. In one example, a financially motivated threat actor posed as Russia-based espionage threat actor Blue Athena (**a.k.a.** Fancy Bear),[79] to appear more intimidating to victims given Blue Athena's reputation. The threat actor indicated the time when it would start a prospective DDoS against the victim, and requested payment of around USD 15,000 in Bitcoin to desist from the attack.

In other cases, threat actors directly attacked victims with DDoS attacks, only to then send ransom requests. South African financial institutions were one of the primary targets for such attacks in the last quarter of 2019,[80] leading the South African Banking Risk Information Centre (SABRIC) to issue an advisory on the matter. Reportedly, the attacks mainly affected the banks' customer-facing services rather than internal operations. Although these attacks did not cause material impact, the danger posed by DDoS attacks to sectors heavily relying on web portals – finance and retail, for instance – remains significant.

Hacktivists strike back

As organisations continued to improve their cyber defences, and law enforcement increasingly cracked down on individuals and collectives responsible for computer misuse, hacktivist activity has relatively subsided. However, in April 2019, Ecuador came temporarily under siege, as DDoS attacks were directed at websites including those of Ecuador's Foreign Ministry, Presidential office, and Central bank.[81] The attacks against Ecuadorian internet infrastructure allegedly came in retaliation against the Ecuadorian government's decision to

---

76 'Multistage Attack Delivers BillGates/Setag Backdoor, Can Turn Elasticsearch Databases into DDoS Botnet 'Zombies'', TrendMicro, https://blog.trendmicro.com/trendlabs-security-intelligence/multistage-attack-delivers-billgates-setag-backdoor-can-turn-elasticsearch-databases-into-ddosbotnet-zombies/ (23rd July 2019)

77 'Hire a DDoS Service to Take Down Your Enemies', CSO Online, https://www.csoonline.com/article/3180246/hire-a-ddos-service-to-take-down-your-enemies.html (15th March 2017)

78 'Exploring the provision of online booter services', 2015, https://www.repository.cam.ac.uk/bitstream/handle/1810/252340/Hutchings%20&%20Clayton%20 2015%20Deviant%20Behavior.pdf

79 'A DDoS Gang is extorting businesses posing as Russian government hackers', ZDNet, https://www.zdnet.com/article/a-ddos-gang-is-extorting-businesses-posing-as-russian-government-hackers/ (24th October 2019)

80 'Sustained DDoS Attack on South African Banks Accompanied by Ransom Notes', CPO Magazine, https://www.cpomagazine.com/cyber-security/sustained-ddos-attack-on-south-african-banks-accompanied-by-ransom-notes/ (4th November 2019)

81 'Free Julian Assange or 'CHAOS IS COMING!' Anonymous warns as they threaten crime agency', Express, https://www.express.co.uk/news/uk/1114863/julian-assange-news-wikileaks-ecuador-embassy-arrest-twitter-anonymous (16th April 2019)

stop supporting Julian Assange, who had remained in asylum in the Ecuadorian Embassy in London since 2012. In April 2019, Assange was expelled from the embassy and arrested by British authorities. Following this, threat actors self-identifying as Grey Ares – the loosely-tied hacker syndicate collectively known as Anonymous – launched a DDoS attack against the NCA**,** causing intermittent minimal downtime to the NCA's website.

The operations of hacktivist threat actors like Grey Ares can be unpredictable, given that the rationale with which they pick their targets may not always, like in the case above, be immediately apparent. Hacktivist activity involving DDoS can cause disruption when executed at scale but PwC, as well as numerous independent studies, observe that such operations are becoming rarer with time[82, 83] – and that effective preparation can help fend off such attacks.

No news good news: DDoS silencing

The ability of DDoS attacks to overwhelm web servers and take internet infrastructure offline makes it an effective, if temporary, means to disrupt information sources. In late October 2019, Georgia was the target of a wave of cyber attacks bringing excessive traffic to servers and effectively knocking offline about 2,000 websites as well as the national TV station.[84] While thousands of web pages including that of the Georgian President were defaced with warnings of other future cyber attacks, two TV broadcasters were sent offline, with one reportedly having equipment damaged as a consequence of the attacks. Georgia had already been a victim of various DDoS attacks during the Russian-Georgian war, including DDoS attacks directed at the South Ossetian government.

In September 2019, online encyclopedia Wikipedia was also targeted by a large-volume DDoS attack that lasted around nine hours,[85, 86] causing downtime across Europe, Africa, and the Middle East as well as slower connection in the US and Asia. The Wikimedia Foundation characterised the incident as a 'malicious attack' by 'a bad faith actor'.

Earlier in 2019, numerous Philippine alternative media outlets had also come under sustained DDoS attacks that repeatedly knocked the websites offline and made them temporarily inaccessible by visitors as well as administrators.[87] The National Union of Journalists of the Philippines (NUJP) was also targeted numerous times. The DDoS attacks on these media outlets took place around the same time, between December 2018 and February 2019, in the period of the 2019 midterm elections. According to a forensic investigation, the DDoS attacks were performed using a botnet-for-hire service.[88]

As organisations increasingly adopt DDoS mitigation solutions, the scale of DDoS attacks will continue to grow as threat actors find new amplification techniques. Threat actors seeking to launch DDoS attacks are also increasingly reliant on larger botnets to be able to impart significant downtime on victims. This, in turn, is fuelling demand in the cyber criminal marketplace, leading to continued activity aimed at amassing bots for malicious purposes.

---

82 'Return to Normalcy: False Flags and the Decline of International Hacktivism', Recorded Future, 21st August 2019, https://go.recordedfuture.com/hubfs/reports/cta-2019-0821.pdf

83 'The Decline of Hacktivism: Attacks Drop 95 Percent Since 2015', Security Intelligence, https://securityintelligence.com/posts/the-decline-of-hacktivism-attacks-drop-95-percent-since-2015/ (16th May 2019)

84 'Georgia hit by massive cyber-attack', BBC, https://www.bbc.co.uk/news/technology-50207192 (28th October 2019)

85 'Malicious attack on Wikipedia—What we know, and what we're doing', Wikimedia Foundation, https://wikimediafoundation.org/news/2019/09/07/malicious-attack-on-wikipedia-what-we-know-and-what-were-doing/ (7th September 2019)

86 'Analysing the Wikipedia DDoS attack', ThousandEyes: Alex Henthorne-Iwane, https://blog.thousandeyes.com/analyzing-the-wikipedia-ddos-attack/ (9th September 2019)

87 'STATEMENT: DDoS attacks on NUJP, alternative media continue', National Union of Journalists of the Philippines, Minda News, https://www.mindanews.com/statements/2019/02/statement-ddos-attacks-on-nujp-alternative-media-continue/ (11th February 2019)

88 'Attributing the attacks against media and human rights websited in the Philippines', Qurium The Media Foundation, https://www.qurium.org/alerts/philippines/attributing-the-attacks-against-media-human-rigths-philippines/ (29th March 2019)

Sowing chaos

Shamoon arisen

Sabotage attacks rose to prominence in 2011, with the infamous campaign targeting Iran's nuclear programme using destructive malware, dubbed Stuxnet. Since then, the use of destructive malware has evolved to no longer be entirely motivated by sabotage.

StoneDrill is a sophisticated wiper used predominantly to cause destruction to the oil and gas sector in the Middle East, however, StoneDrill also contains espionage tools in its arsenal indicating the destructive malware serves multiple purposes. StoneDrill is attributed in open source to Yellow Garuda (**a.k.a.** APT35 or Charming Kitten),[89] an Iran-based threat actor that has been known to target a wide range of sectors. Recent StoneDrill activity could be linked to a statement by the US Cyber Security and Infrastructure Security Agency (CISA) from June 2019, which reported a rise in malicious cyber security activity directed at US industries and government agencies by Iran-based threat actors – in particular an increase in destructive wiper attacks.[90]

Traditional destructive attacks purely seeking to cause destruction still occur. First observed in 2012, when it wiped the systems of a state-owned oil producer in the Middle East, Shamoon was used to repeatedly target Saudi Arabia and its critical sectors, causing major data and financial losses and disruption. In December 2018, a third wave of Shamoon attacks targeted Italian oil and gas contractor Saipem, as well as two similar organisations from Saudi Arabia and the UAE.

Shamoon malware is inherently destructive, wiping data on victim systems and impeding their reboot. It consists of a tripartite structure, with its dropper, wiper, and reporter functionality contained in three different implants. 10% of Saipem's systems were infected, the vast majority of which were located in the Middle East.

In late 2019, researchers identified a new wiper malware family called ZeroCleare in open-source reporting. Similarly to Shamoon, ZeroCleare was deployed against targets in the Middle East, and exploited a specific unsigned system driver to load wiper code on victim systems.[91]

Information operations

Information operations – i.e. attempts to 'influence, disrupt, corrupt, or usurp the decision making of adversaries and potential adversaries while protecting [its] own'[92] – rose to prominence in 2016 with the infamous case of Russia-based threat actors accused of meddling in the 2016 US presidential election. Election interference via information operations is now a well-documented phenomena, however, 2019 highlighted the use of information operations for other nefarious activities.

Research from 2019 identified 53 cases of foreign influence efforts (FIEs)[93] – coordinated campaigns by one state to impact politics in another state through media channels – in 24 victim countries from 2013 to 2018.[94] Two of the cases were ongoing as of April 2019. In total, 72% of the campaigns were conducted by threat actors based in Russia, with threat actors based in China and Iran accounting for most of the remainder.

While many of the cases sought to shape election outcomes, others focused on discrediting specific political actors, such as a campaign targeting the Syrian Civil Defence Force. In other campaigns, threat actors attempted to shift the political agenda on specific topics, such as from health to security. The proposal of the extradition bill sparked protests in Hong Kong, and disinformation was used in support of both the protestors and the police.[95] Finally, campaigns encouraged political polarisation – Russia-based threat actors simultaneously supported the Black Lives Matter and the White Lives Matter counter-movements. Within Australian, Brazilian, Candian, and South African politics, Russia-based threat actors attempted to polarise the debate.

---

89 'Elfin: Relentless espionage group targets multiple organisations in Saudi Arabia and US', Symantec, https://www.symantec.com/blogs/threat-intelligence/elfin-apt33-espionage (27th March 2019)

90 'US government warns of data wipers used in Iranian cyberattacks', Bleeping Computer, https://www.bleepingcomputer.com/news/security/us-government-warns-of-data-wipers-used-in-iranian-cyberattacks/ (22nd June 2019)

91 'New Destructive Wiper 'ZeroCleare' Targets Energy Sector in the Middle East', IBM Security, https://www.ibm.com/downloads/cas/OAJ4VZNJ (December 2019)

92 'Information operations: Joint Publication 3-13', US Department of Defense, November 2014, https://fas.org/irp/doddir/dod/jp3_13.pdf

93 'Managing and mitigating foreign election interference', Lawfare, https://www.lawfareblog.com/managing-and-mitigating-foreign-election-interference (21st July 2019)

94 In addition, the research identified 40 purely domestic online influence campaigns, in which state actors targeted their own populations in ways designed to mask government involvement.

95 'Chinese covert social media propaganda and disinformation related to Hong Kong', The Jamestown Foundation, https://jamestown.org/program/chinese-covert-social-media-propaganda-and-disinformation-related-to-hong-kong/ (6th September 2019)

Case study – Document leak

A leak of apparent FSB contractor documents made the headlines in July 2019,[96, 97] after a hacktivist group leaked a cache of data pertaining to be from the internal networks of Moscow-based company SyTech. Whilst the documents provide interesting insight into the type of research being conducted – including into Tor deanonymisation, social media tracking and email monitoring – it is important to bear in mind that the cache remains unverified and the authenticity of the documents therefore questionable. The motivation behind this attack is unknown, however, PwC has seen similar hack and leak operations attempting to further the threat actor's cause, as seen in the following example.

Case study – Oil(Rig) leaks expose an information operation

In June 2019, information on tools and infrastructure attributed to Iran-based threat actor, Yellow Maero, were exposed in a series of leaks.[98] PwC assesses it highly likely that this activity forms part of an information operation seeking to disrupt Iran's espionage operations. By promoting the narrative that the Ministry of Intelligence of the Islamic Republic of Iran (MOIS) is sinister and betraying the Iranian people, the threat actor is likely attempting to sow discord within Iran's domestic population.

96 'Russian contractor document leak', PwC Threat Intelligence, CTO-SIB-20190812-01A

97 'Hackers breach FSB contractor, expose Tor deanonymization project and more', ZDNet, https://www.zdnet.com/article/hackers-breach-fsb-contractor-expose-tordeanonymization-project/ (20th July 2019)

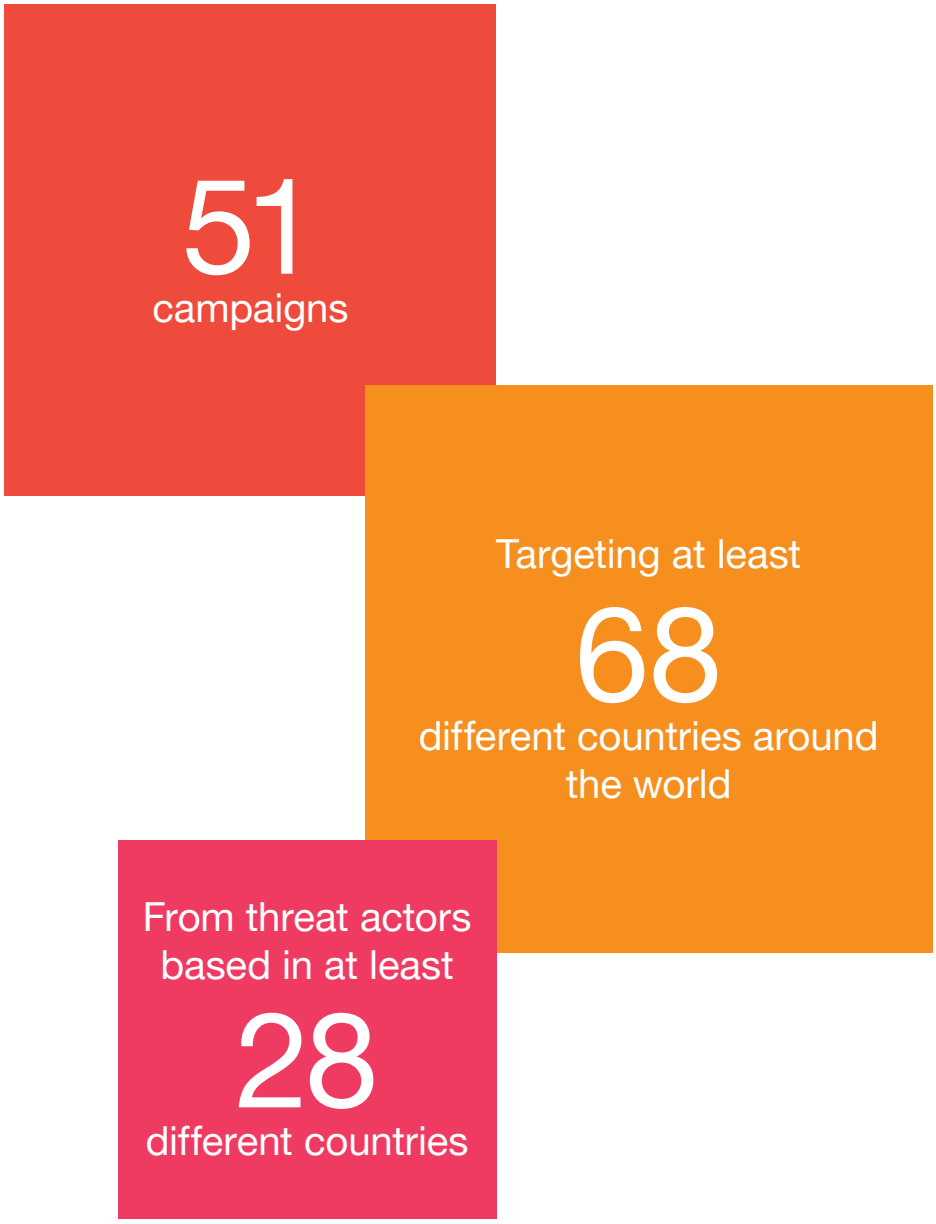
98 'A mystery agent is doxing Iran's hackers and dumping their code', Wired, https://www.wired.com/story/iran-hackers-oilrig-read-my-lips/ (18th April 2019)

Shattering the mirror maze of information operations

In 2016, Russia-based threat actors were accused of interfering in the US presidential election, highlighting how social media can be exploited to promote a political agenda, sow discord, and incite polarisation. Meanwhile, in other cases, information operations aimed to undermine the objective assessment of evidence, providing multiple 'alternative narratives' or promoting falsehoods. In the fallout of 2016, social media companies vowed to step up to identify and combat disinformation on their platforms. The same research that identified 53 cases of foreign influence efforts also concluded that the information operations' preferred social media platforms were Twitter and Facebook, likely due to the scale of their reach.[99, 100]

In 2019, Facebook alongside Twitter and Google continued disabling accounts associated with information operations from around the world. Overall, they disclosed 51 campaigns through 2019, from threat actors based in at least 28 countries and targeting more than 68 countries around the world.

In addition to social media platforms, countries around the world are making changes to protect against information operations. In May 2019, the European Union adopted a new sanctions regime that would impose penalties on individuals, companies, and government organisations that are involved in cyber attacks.[101] The new regime came into effect ahead of the European Union parliament elections, as both a deterrent and a response.

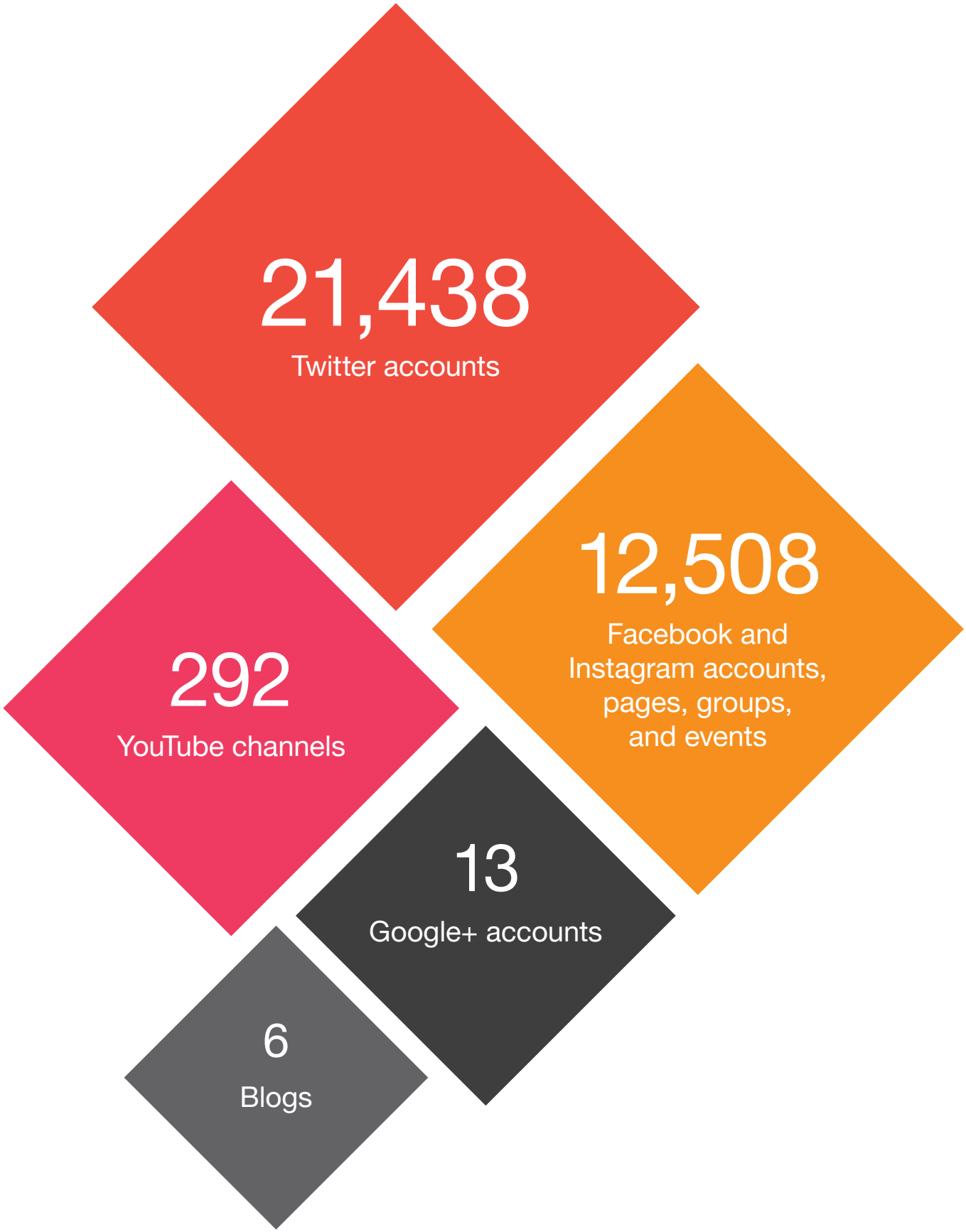


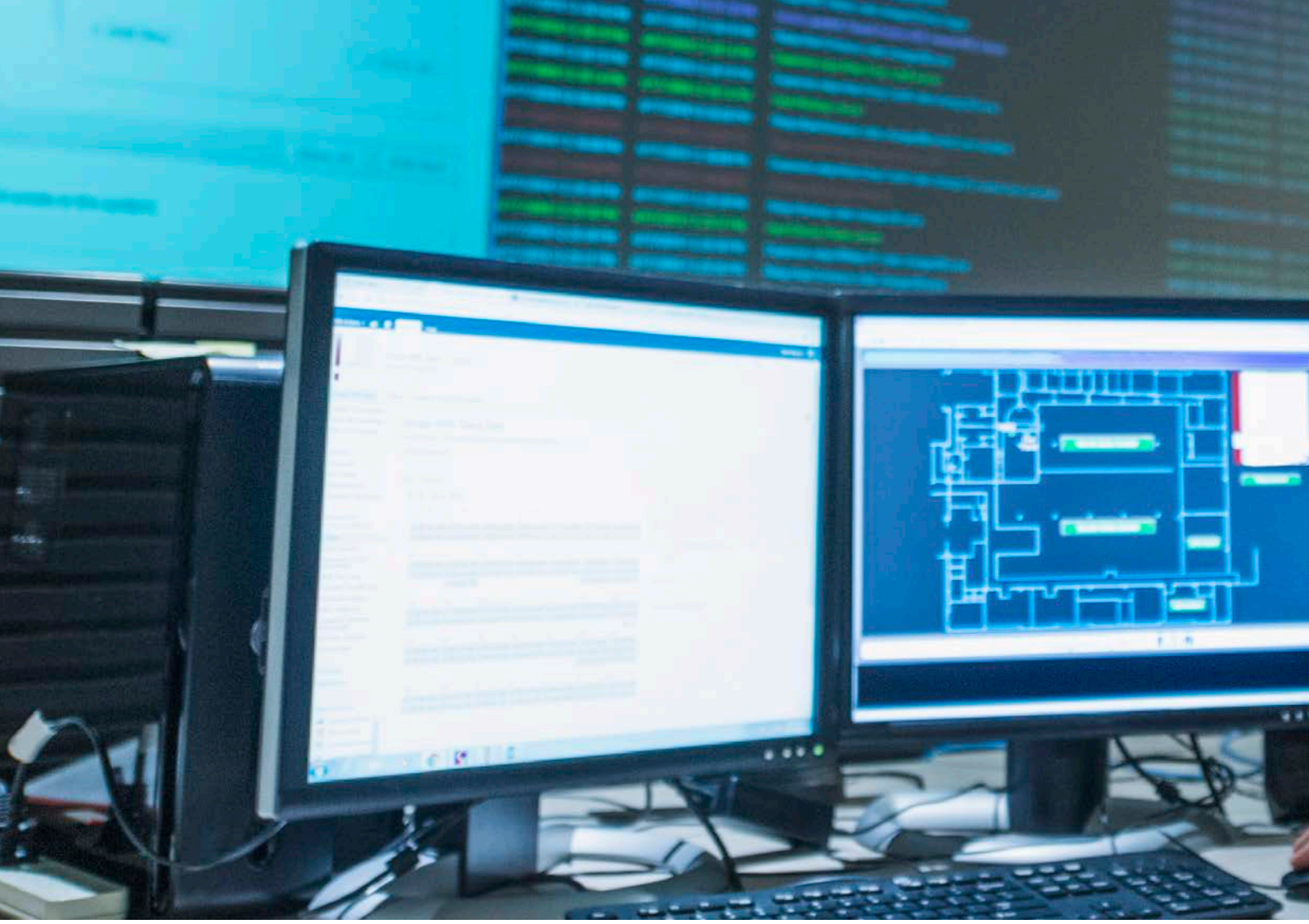
99 83% of the information operations used Twitter, and 50% used Facebook.

100 'Managing and mitigating foreign election interference', Lawfare, https://www.lawfareblog.com/managing-and-mitigating-foreign-election-interference (21st July 2019)

101 'EU approves new cyber-sanctions regime ahead of parliament elections', Radio Free Europe/Radio Liberty, https://www.rferl.org/a/eu-approves-new-cyber-sanctions-regime-ahead-of-parliament-elections/29947704.html (17th May 2019)

The following accounts, pages, groups, channels, events, and blogs were suspended for being associated with information operations.





Conclusion

In 2019, PwC analysts witnessed and documented a convergence of the physical and cyber domains, as campaigns continued to align, in targeting and aims, with international relations. Mirroring this association, in phishing campaigns in particular, threat actors often delivered timely and relevant malicious lure documents to victims in order to infect them, with short turnaround periods between a piece of news being published and its weaponisation in malicious operations. PwC observed tit-for-tat operations alongside longer-term intelligence collection efforts, threat actors' overlapping interests turn into cases of fourth-party collection, as well as an increasing focus on surveillance by espionage motivated threat actors.

Especially – though not exclusively – in relation to surveillance and information collection, one of the defining trends of 2019 was the growing attention threat actors afforded to mobile devices. PwC saw multiple cyber criminal and espionage threat actors either using exploits to directly compromise mobile devices, or socially engineering victims into installing malicious applications on their mobile phones. In many cases, PwC observed mobile malware used to target specific demographics, groups, or even individuals.

Supply chains continued to be a key targeting focus, with sophisticated threat actors (and especially China-based threat actors) going after third parties or acquired companies, or even trusted software providers, in order to reach organisations and their customers – exploiting the trust and privileged access afforded to third-party suppliers.

In 2019, PwC saw evidence suggesting that certain threat actors, long considered to be espionage motivated and with objectives aligned to national interests, have duplicated and divided their efforts to also perform cyber criminal activities.

While PwC saw new threat actors rise to prominence in the cyber criminal space, the cyber criminal market effectively consolidated around large, established players that maintained, managed, and updated some of the largest cyber criminal operations. Many of the principal cyber criminal threat actors – the likes of Emotet, Dridex, as well as FIN threat actors – operated affiliate programmes and leased access to their systems on a fee-paying or profit-sharing basis.

Even in the financially motivated cyber crime space, PwC observed a solid continuation of 2018 trends, including formjacking, Magecart skimmers, theft of banking credentials and POS malware. Yet the diversification into ransomware operations was one of the main cyber crime themes of 2019. The last 12 months, continuing from a trend established in 2018, have seen a succession of high profile ransomware attacks affecting a broad range of victims and sectors. More and more, the affiliate programmes mentioned above also see 'stable' relationships between specific spam operations and ransomware actors – for example the triad Emotet – TrickBot – Ryuk.

In terms of sabotage attacks, throughout 2019, DDoS attacks remained a steady trend in the background of other cyber operations. With the proliferation of connected devices and the growth of the IoT, more and more exploitation paths and malware families are emerging to compromise these devices and enslave them into botnets.

Nevertheless, sabotage operations leveraging malware are increasingly taking on destructive objectives. In 2019, wiper and destructive malware have continued posing a threat to organisations – specifically in the Middle East and United States – between December 2018's third wave of Shamoon attacks and destructive activity using ZeroCleare malware in late December 2019.

Yet also in 2019, sabotage operations exhibited a more subtle, treacherous side that has been on the rise for the past few years: that of causing disruption through information operations. For example, election interference via information operations is now a well-documented phenomena, and in 2019 social media companies have moved to tackle increasing 'inauthentic coordinated behaviour' on their platforms. In the future, PwC assesses it highly likely that novel detection techniques will be required to build confidence assessments on media integrity.

Now at the beginning of 2020, PwC has already seen new aggressive intelligence collection campaigns unfold, all while financially motivated threat actors continue using tried and tested, as well as novel techniques, to exact profit from victims. PwC assesses that this will continue throughout 2020, as cyber espionage and sabotage continue to align with international dynamics.

PwC Cyber Security

If you would like more information on any of the threats discussed in this report please feel free to get in touch at **threatintelligence@uk.pwc.com**.

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

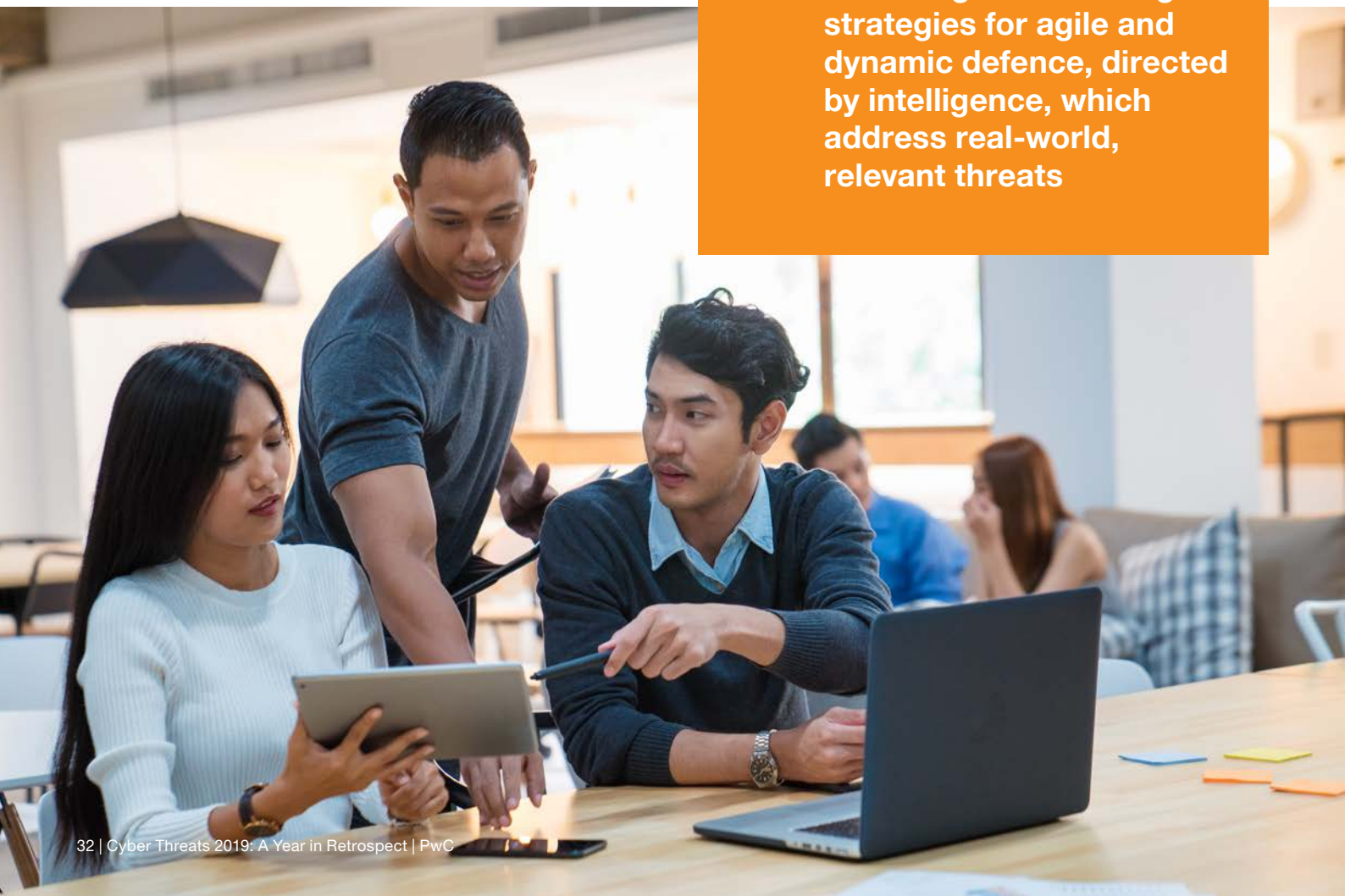
We underpin our board-level security strategy and advisory consulting services with expertise gleaned from the front lines of cyber defence across our niche technical expertise in services such as red teaming, incident response and threat intelligence.

We differentiate ourselves with our ability to combine strategic thinking, strong technical capabilities and complex engagement delivery with client service excellence. Our core focus is delivering pragmatic services to our clients, helping them handle some of their most sensitive business issues.

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, to help our clients protect what matters most to them.

Our rapidly growing threat intelligence team has been described by the Financial Times as one of 'the world's most elite corporate teams of cyber defenders'. 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, economic espionage and targeted intrusions, including those commonly referred to as APTs.

> **"Informing and enabling strategies for agile and dynamic defence, directed by intelligence, which address real-world, relevant threats**



Glossary

Term	Definition
ATM jackpotting	ATM jackpotting involves compromising ATM systems in order to dispense cash.
BabyShark	BabyShark is a piece of malware first seen in November 2018, and attributed to Black Banshee. It involves a multi-stage, script-based delivery and execution chain which refers back to the C2 throughout, and it also sets persistence on victim systems and results in a backdoor payload being installed on infected systems.
BitPaymer	A ransomware family almost always delivered in conjunction with a Dridex infection. BitPaymer, which embeds numerous anti-analysis and UAC bypass techniques, often has individual samples and ransom notes tailored to specific victim environments.
Business Email Compromise (BEC)	A BEC attack involves a threat actor hijacking or closely imitating a legitimate email account in order to more effectively socially engineer individuals.
Cobalt Strike	Cobalt Strike is a commercial penetration testing tool, that is marketed as 'adversary simulation software designed to execute targeted attacks and emulate the post-exploitation actions of advanced threat actors'. Despite its legitimate purposes, CobaltStrike's fully-featured module suite is often used by malicious threat actors (including advanced persistent threats) in their operations.
Code injection	The malicious introduction of code into a running process, to achieve execution of malicious actions without any input validation from the system.
CrimsonRAT	A C#/.Net backdoor implant thought to be unique to Green Havildar, capable of a series of functions including logging keystrokes, capturing audio, and taking screenshots from infected systems.
DNS hijacking	An attack that maliciously alters the correct resolution of queries to the Domain Name System (DNS). Such an attack can lead users to unknowingly be redirected to threat actor-controlled sites, creating the opportunity for traffic interception and installation of malware.
DragonMessenger	A malicious Android application attributed to Black Shoggoth and added to Google Play in October 2019 according to third-party research. It was allegedly distributed via a WordPress website posing as a fundraising service for supporting North Korean defectors, targeting that same demographic for espionage purposes.
Dridex	A banking trojan active since at least 2014, delivered via spearphishing emails, Dridex was used to steal banking credentials and to drop ransomware on victim systems. Despite a takedown in 2015, and the 2019 FBI indictment of one of the individuals behind the management of the malware, Dridex continues operations and remains a substantial threat.

Term	Definition
DTrack	DTrack is a RAT that we assess has likely been used by Black Artemis since at least 2014. It has been used against numerous targets worldwide, including banks and the Kundankulam Nuclear Power Plant.
Dumps	Stolen credit card information – specifically, the raw information stored on a card's magnetic strip. Dumps are mostly collected through skimming of point of sale terminals. Criminals may cash out 'dumps' by embedding them into a fake credit card and physically making a purchase in a store – a process known as 'carding'.
Emotet	Emotet was developed off the Bugat/Cridex/Feodo malware family, and was first observed in 2014 as a banking trojan. Although it retains credential-stealing capabilities, Emotet has been converted into a malware delivery system focused on gaining an initial foothold on victim machines, and is used by a range of sophisticated cyber crime threat actors. PwC assesses it is highly likely that Emotet is run on an affiliate model, whereby Emotet administrators form a core group with multiple affiliates that include Trickbot, Dridex, and IcedID.
Formjacking	Also known as 'digital skimming', formjacking involves the surreptitious injection of malicious JavaScript code into the checkout pages of legitimate websites, to enable the theft of credit card information and other data (such as billing addresses) from payment forms.
GermanWiper	A ransomware variant highly likely linked to another mature ransomware family known as Sodinokibi, based on overlaps in targeting and infrastructure. In a campaign in the summer of 2019, spear-phishing emails targeted German speakers, claiming to be from an individual reaching out to a prospective employer seeking a new professional challenge, with a zip embedding a malicious LNK file.
GlobeImposter	The second most prevalent ransomware family in 2017, GlobeImposter variants abused spear-phishing, exploit kits and RDP bruteforce to gain access to networks and encrypt system files. Recently, we observed GlobeImposter not completely encrypt files, leaving some sections legible, to make file encryption faster (and thus harder to stop).
Hooking	Any technique that alters the behaviour of the operating system (OS) or any program by intercepting a program's execution at a particular point to take another action. Hooking can enable malware to establish persistence, or to load additional malicious code within another process.
Incident response	The organised process of investigating, addressing, and mitigating a cyber security incident or cyber attack. Incident response often involves pre-incident planning, and ties in with other critical business functions, ensuring that an organisation can continue business as usual while countering a threat or recovering from an incident.
Information operations	Information operations are attempts to 'influence, disrupt, corrupt, or usurp the decision making of adversaries and potential adversaries while protecting [its] own'.
Joker's Stash	A criminal marketplace specialised in stolen card data, where data coming from a single breach is often sold in several tranches. Joker's Stash was opened in 2014, and has representation on numerous other cyber criminal and carding forums.

Term	Definition
Kazuar backdoor	A .Net backdoor attributed to Blue Python, consisting of an executable and a loaded DLL. Kazuar supports numerous capabilities, including acting as an HTTP server able to receive commands from a remote attacker.
Living off the land	Using legitimate tools and processes, often already installed on a victim's device, to reduce the chance of an attack being detected.
LookBack	LookBack is a C++ RAT with capabilities that include system, process, and file discovery and manipulation, screen capture as well as remote interaction with the host. The RAT leverages a proxy communication module to create a proxied C2 channel, through which LookBack exfiltrates data from the infected host. LookBack has been observed targeting a few specific sectors, including academia.
Lure document	A document designed to attract the attention of a user – to 'lure' them – while malware is being installed on the victim's machine. The document can be simply a decoy, or weaponised with malicious code.
Magecart	The umbrella term Magecart describes threat actors that use JavaScript-based malware to capture payment card information from compromised online retailers or their third party ecommerce platforms.
MESSAGETAP	A malicious implant targeted at mobile telecommunications infrastructure, that carries out real-time monitoring of SMS services.
Nodersok	A strain of fileless malware, installed via the execution of a HTML Application (HTA) file. Nodersok uses a multi-stage process to download and install several legitimate tools, including Node.exe (the Windows implementation of Node.js), and WinDivert, a packet capture tool. Nodersok then abuses these tools to proxy victims' traffic, in order to intercept personal data and credentials.
NOKKI backdoor	A backdoor attributed to Black Shoggoth, consisting of a main executable and loaded DLL. NOKKI is designed to steal information from victims, and has been deployed against numerous targets, including victims in South Korea and victims speaking Cambodian and Cyrillic.
Owl	The Owl backdoor uses the Windows HTTP API to serve HTTP endpoints, providing command execution on the host and the ability to proxy traffic into an internal network, making an infected webserver a potential pivot point for the threat actor.
POS malware	Malware installed on point of sale terminals used to harvest credit card and debit card information, by intercepting its processing at checkout and forwarding it to attacker-controlled servers. An example of POS malware is FIN6's FrameworkPOS.
Reconnaissance	The process, undertaken by threat actors, of researching available information about a target, including attempting to identify vulnerabilities in target systems or individuals of interest.
Rifdoor	A backdoor attributed to Andariel, a threat actor that PwC tracks as a subset of North Korea-based Black Artemis. Rifdoor has been documented in its basic form since at least 2015; in 2019, PwC observed an updated variant of the malware with added capabilities such as screen capture.

Term	Definition
ROKRAT	One of Black Shoggoth's main tools, ROKRAT is a backdoor using Cloud services for C2 that was first observed in 2016, and has undergone active development at least up until 2018.
ROKROID	A malicious Android application attributed to Black Shoggoth, and delivered to victims via URL shortened links embedded in spear-phishing emails. ROKDROID has a large set of capabilities, including recording calls, exfiltrating call logs, and interacting with a C2 server.
Ryuk	A ransomware family almost always deployed after an initial infection of Emotet has installed TrickBot on victim systems. It has been used in a number of highly targeted attacks against enterprises, with ransom notes unique to compromised victims.
ShadowPad backdoor	A backdoor that was used to trojanise management software: this was the first stage in a complex supply-chain attack aimed at profiling victims to identify interesting targets to compromise further. ShadowPad contains multiple anti-analysis techniques, and is able to set persistence on victim systems and escalate privileges, as well as to send system profiling information back to its C2.
Shamoon	Shamoon is a destructive malware family that was observed in extremely targeted attacks in 2012, 2016, and 2018. Comprising of three components – a dropper, a reporter, and a wiper – Shamoon is engineered to cause the greatest damage possible by spreaing like a worm on a network, completely erasing victims' file and booting systems to render them factually unusable.
Skipper	A Blue Python implant that acts as a first-stage profiling tool to gather victims' information, which is then used to then deploy other, more powerful tools such as the Snake backdoor.
Spoof	To spoof an email account, domain, or entity is to imitate it, with the aim to deceive a victim as to the account, domain, or entity's legitimacy (trustworthiness) and identity.
Stonedrill	A disk wiping malware also called SHAPESHIFT, Stonedrill also contains espionage tools indicating the destructive malware serves multiple purpose.
Supply chain attack	Attacks in which threat actors seek ways to exploit computer networks via the privileged access given to third-party suppliers, using them as entry points into targeted entities. Supply chain attacks can involve compromising software or hardware providers, and creating malicious versions of the products.
Threat actor	A malicious entity responsible for an intrusion attempt (successful or unsuccessful), which can be motivated by factors including a desire to steal confidential data, commit financial fraud, disrupt or destroy a system or cause reputational damage.
Threat intelligence	Threat intelligence consists of the analysis and collection of information pertaining to different malicious cyber threat actors, understanding the techniques they employ and their targets, so as to better protect a specific organisation given the particular threats it faces.

Term	Definition
Topinambour	Blue Python dropper malware written in .Net, used to deliver malware including the KopiLuwak JavaScript backdoor to victims.
TrickBot	First seen in 2016, TrickBot is a modular banking trojan and credential stealer designed to steal banking and other online account details. It is often delivered after an initial Emotet infection. PwC assesses that one core threat actor is in charge of the overall TrickBot system, with sub botnets that are configured to individual requirements for 'clients'.
Trojanised (program)	The term refers to a trusted legitimate program that has been altered or tampered with by a threat actor to hide malware in transit and deliver it to targets, or to perform malicious functionality on victim systems.
UAC	User Account Control (UAC) is a Windows component that makes applications and tasks run in a context with non-administrative privileges on a system. It is meant to prevent inadvertent system changes caused by a standard user, and to impede malware from taking system administrator-level actions.
UAC bypass	The term 'UAC bypass' refers to any measure that leads a program (including, but not exclusively, malware) to elevate its system privileges, and take actions normally reserved for system administrators even if the signed-in user does not have administrator rights.
Vishing	Short for 'voice phishing', it consists of an attacker attenmpting to socially engineer a victim over a phone call, to discover more information about them or convince them to perform certain actions (for example, unwittingly installing malware).
Watering hole	Also referred to as strategic web compromises, a watering hole attack is a method of infiltration. A threat actor will compromise a specific trusted website and use this to infect visitors to the site.
WhiteShadow	A macro-based downloader malware attributed to Green Havildar, that uses SQL queries to download a payload (which can be CrimsonRAT or commodity RATs like AzoRULT) to the infected machine from a remote server.
Winnti backdoor	A backdoor first identified in 2011, Winnti has been used by multiple threat actors collectively known as the 'Winnti' metagroup. Used as a backdoor implant as well as a first pivot point to further compromise victim environments, Winnti has been deployed against numerous targets: from gaming companies and commercial organisations to telecommunication companies and dissident communities.
ZeroCleare	A new wiper malware family disclosed in late 2019, ZeroCleare has links to Shamoon malware and was also deployed against targets in the Middle East.

200124-155742-KW-OS