APT28, THE LONG HAND OF RUSSIAN INTERESTS

Disclaimer

This report was developed by the cybersecurity company Maverits with the help of Institute of Cyber Warfare Research and Women Leadership and Strategic Initiatives Foundation at the request and with the assistance of the National Security and Defense Council of Ukraine and the National Cybersecurity Coordination Center.

This report is intended for informational purposes only and is based on publicly available information, expert analysis, and credible third-party sources. While every effort has been made to ensure the accuracy and reliability of the information presented, the dynamic nature of cyber threats and evolving geopolitical landscapes means that some details may become outdated or subject to change.

The analysis and conclusions drawn in this report do not represent an endorsement or condemnation of any nation, organization, or entity. The report aims to provide a factual and objective review of observed activities attributed to APT28.

Readers are advised to use this report as a reference and complement it with additional research and consultation with cybersecurity professionals. The authors and publishers of this report disclaim any liability for actions taken based on the content herein.

This Special Report covers the period 2022-2024 and represents the status as of 31 December 2024.

Contents

1 **Executive Summary** 3

2 **Countries** 4

3 **Industries** 5

4 **Malware Campaigns** 7

Jaguar Tooth 8

Moobot 9

CredoMap 10

Headlace 11

Steal-It 13

MASEPIE, OCEANMAP, STEELHOOK 14

HATVIBE and CHERRYSPY 15

5 **LOLBINs** 16

6 **Vulnerabilities** 18

7 **Phishing Campaigns** 20

8 **Legitimate Internet Services** 22

9 **Network Infrastructure** 24

10 **Espionage** 25

11 **Influence** 26

12 **Conclusion** 28

+ **Endnotes** 30

1 Executive Summary

In this report we examine the activities of APT28 since the start of the war in 2022, providing an analysis of their major campaigns, evolving tactics, and strategic objectives. By focusing on APT28, a group affiliated with Russia’s GRU Military Unit 26165, we wanted to depict Russia’s broader geopolitical and military aims.

Since the onset of the war, APT28 has shifted its focus, adapting to the changing geopolitical situation. The group has been evolving its tactics and tools to achieve its strategic aims, with a significant change in targeted countries and industries.

Ukraine has become a main target, accounting for 37% of the group’s attacks. This focus indicates a high priority on gathering intelligence and potentially disrupting operations in the region. Similarly, in past conflicts such as the 2008 war in Georgia, the group targeted government entities to gather intelligence on security and diplomatic strategies, and this trend is continuing with the targeting of government and diplomatic institutions, and military and defense sectors in Ukraine.

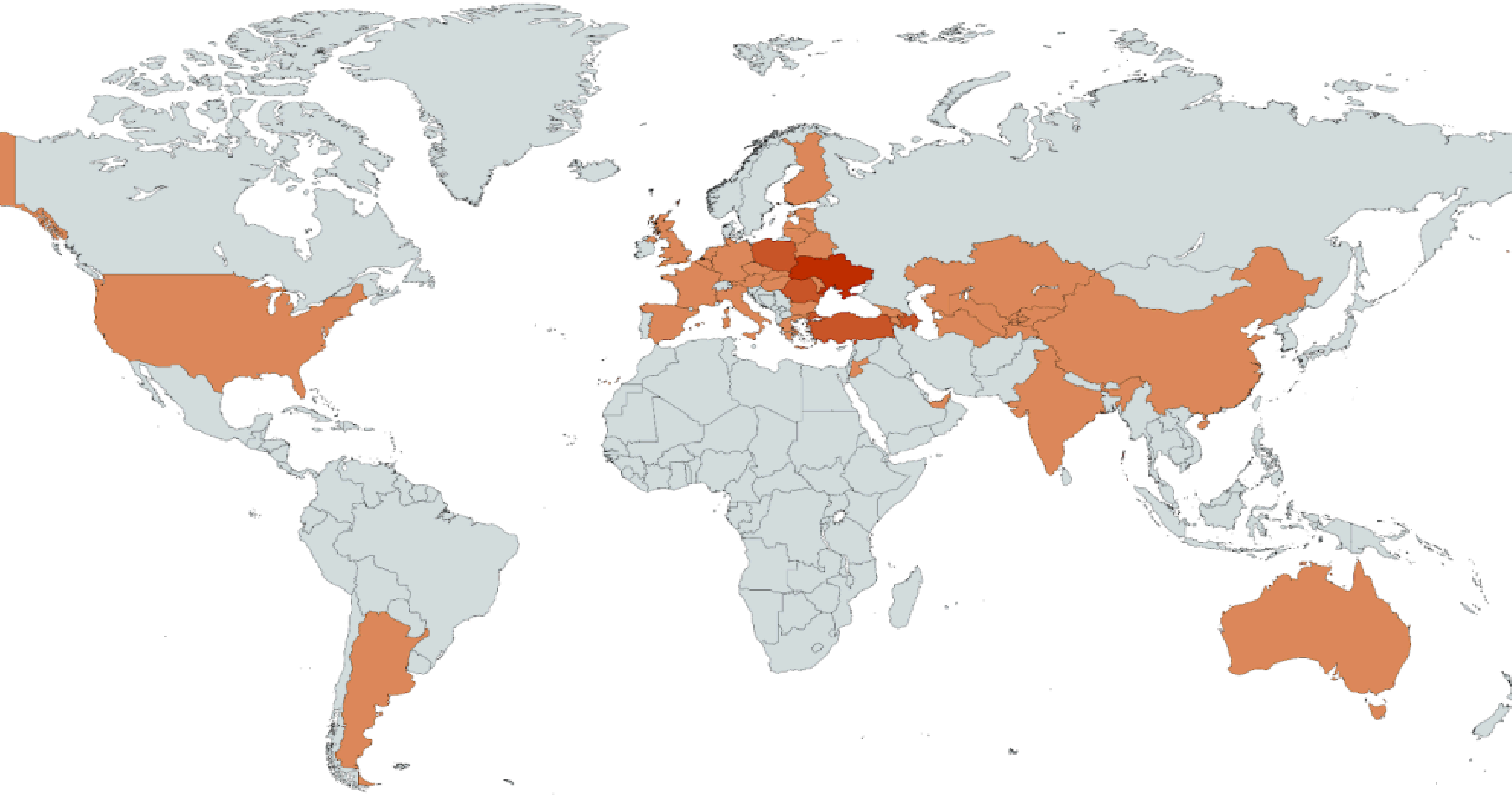
In terms of tactics, APT28 continues its tendency of exploiting both zero-day vulnerabilities and publicly known flaws while developing specialized backdoors and infostealers tailored to their espionage goals. Furthermore, recent campaigns highlight a shift towards using legitimate internet services, living-off-the-land binaries (LOLBINs), and exploiting network devices to evade detection and maintain under the radar. These innovations are complemented by large-scale phishing campaigns that employ novel techniques to enhance their effectiveness.

While APT28’s activities remain rooted in espionage, the group has adapted their methods and objectives to align with the evolving geopolitical landscape and is shifting the focus to the new targets.

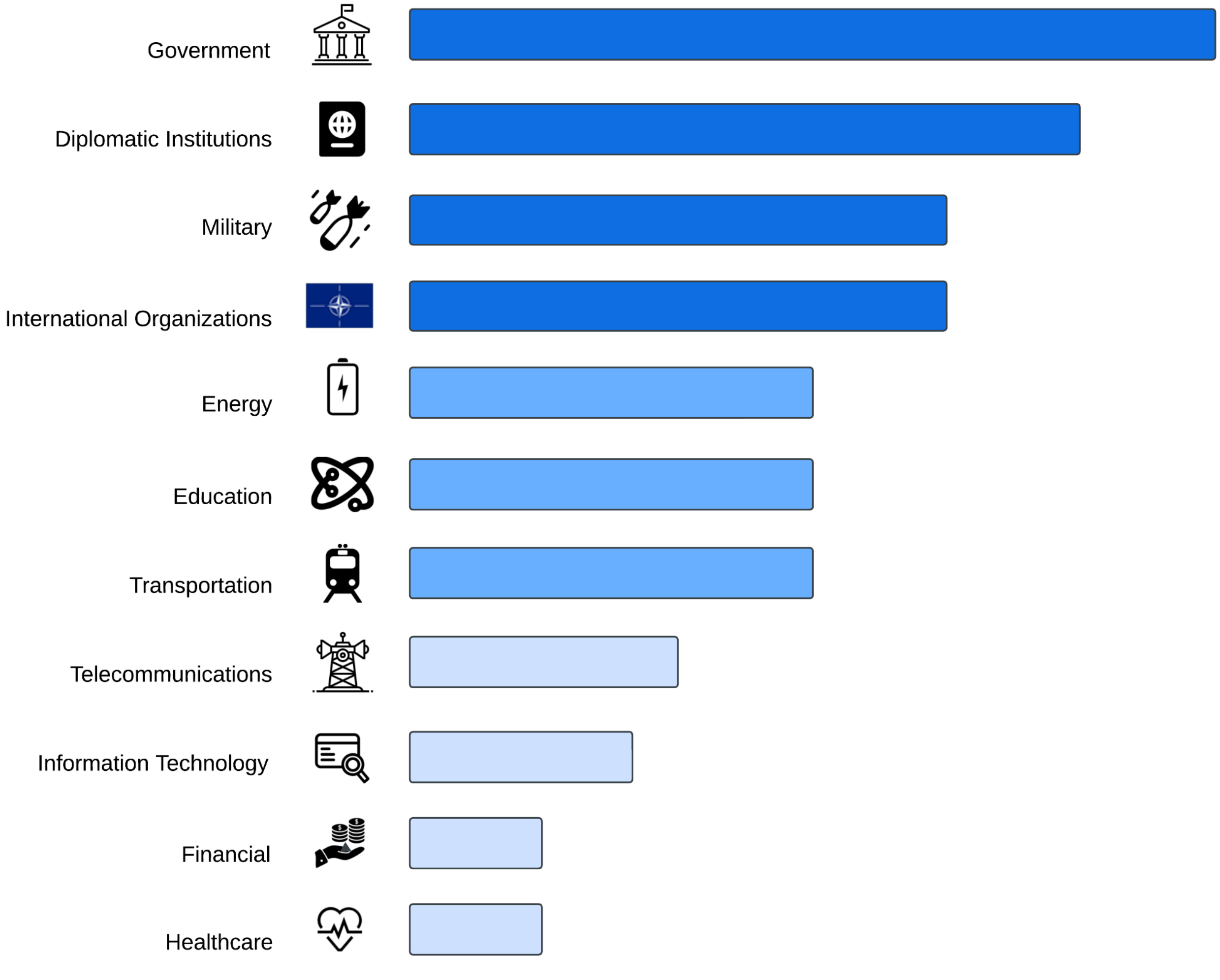
2 Countries

Since the start of the war in 2022, APT28 has significantly shifted its focus, targeting a wide range of European countries. While Eastern Europe remains a key area of interest, nearly every European nation has been a target over the last three years. Ukraine has been the primary focus of APT28's activities, accounting for approximately 37% of the group's operations. These campaigns often involve targeting government and military networks to gather intelligence. Poland follows as a major target, representing 18% of APT28's activity, largely due to its strategic role in supporting Ukraine and hosting NATO operations.

In addition to its European campaigns, APT28 has expanded its operations to include select Asian countries in recent years. This geographic diversification aligns with Russia's broader geopolitical interests, targeting nations with strategic resources or alliances.



3 Industries



APT28 has maintained a consistent focus on targeting government and diplomatic institutions. These sectors are among the most frequently attacked, as the group aims to gather intelligence on geopolitical strategies and foreign policies. By compromising these entities, APT28 seeks to gain insights into decision-making processes and influence international relations.

Military and defense organizations remain another key focus area for APT28. The group's activities in this sector aim to uncover sensitive information related to security measures, military operations, and defense technologies. Such attacks often target NATO and its affiliated entities, underlining the group's strategic interest in undermining Western military alliances and preparedness.

APT28's operations have extended to a wide array of supranational organizations, including the European Commission, United Nations agencies (such as UNHCR and UNICEF), the World Bank, and the World Health Organization's European Region.

These attacks highlight their interest in exploiting global institutions to disrupt international cooperation and extract valuable intelligence. Think tanks, such as the Razumkov Centre in Ukraine and the Azerbaijan Center for Economic and Social Development, have also been targeted, likely for their role in shaping regional strategic policies.

Additionally, private security companies have become a target for APT28, as the group seeks to steal information related to weapons systems and strategic plans. These efforts demonstrate their intent to compromise both public and private entities.

4 Malware Campaigns

The group is known for its use of custom backdoors and stealers, which are systematically developed to evade detection and meet specific operational needs. These tools are tailored to the group's targets, ensuring effectiveness in espionage and data exfiltration campaigns. The hypothesis of a dedicated development pipeline suggests a high degree of organization and long-term planning.

APT28 frequently updates and evolves its malware samples to ensure continued usability, often modifying them to bypass new security measures. The group's campaigns have included exploiting both zero-day vulnerabilities and publicly known flaws. This tactic enables them to gain initial access and maintain persistence in targeted networks. Additionally, APT28's use of living-off-the-land binaries (LOLBINs) and legitimate internet services helps them operate under the radar, minimizing forensic evidence and complicating detection. They persist in their established practice of exploiting zero-day vulnerabilities and focusing on webmail services as key targets.

A significant question surrounding APT28's operations is how they obtain zero-day vulnerabilities. While direct evidence is limited, their consistent exploitation of such vulnerabilities suggests access to advanced research capabilities or external suppliers.

This chapter reviews the main campaigns and malware employed by APT28 since the start of the war in 2022, highlighting their strategic use of custom tools, exploitation of vulnerabilities, and innovative techniques to achieve operational goals.

Jaguar Tooth

The Jaguar Tooth malware campaign targets Cisco IOS routers by exploiting the Simple Network Management Protocol (SNMP) vulnerability CVE-2017-6742. This vulnerability, which allows for remote code execution and write access to the target operating system, is triggered by a stack-based buffer overflow in the Cisco IOS's AirLine Protocol Support (ALPS) function. Specifically, the malware is deployed by sending a crafted SNMP Object Identifier (OID), 1.3.6.1.4.1.9.9.95.1.2.4.1.3, which corresponds to alpsRemPeerConnLocalPort. The attacker uses Return Oriented Programming (ROP) techniques to overwrite memory and deploy the malware code incrementally.

The exploit works by first writing a small piece of helper shellcode into memory that can write an arbitrary 4-byte value to a specific address. This shellcode is then used repeatedly to incrementally write the main Jaguar Tooth payload into memory. Once the main payload is written, its execution is triggered by overflowing the return address of the vulnerable function with the memory location of the payload.

The malware is capable of collecting and exfiltrating sensitive information from the infected device. It creates a new process that automatically gathers device information, including the running configuration, firmware version, directory listing of flash memory, network information, interfaces, and other connected routers. This information is collected using various Cisco IOS CLI commands and exfiltrated via Trivial File Transfer Protocol (TFTP) to a specified IP address and URL. Importantly, Jaguar Tooth patches two Cisco IOS authentication functions, askpassword and ask_md5secret, to grant unauthenticated access to local accounts via Telnet and physical sessions.

The vulnerability CVE-2017-6742 was announced by Cisco on June 29, 2017, so the campaign is believed to have occurred sometime after this date. The malware itself is non-persistent, however the unauthenticated backdoor access that it provides might lead to further compromise of the device and network if not remediated.

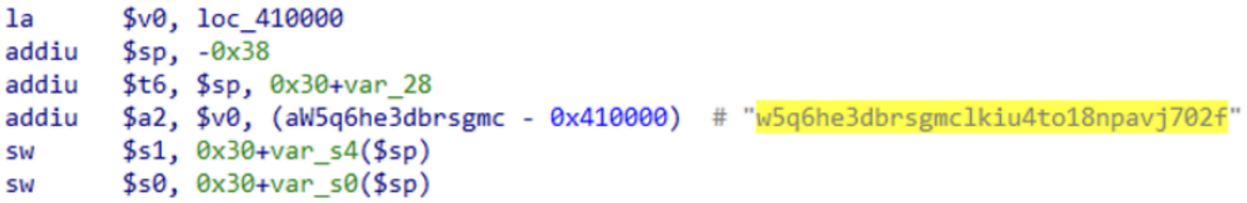
Moobot

Moobot is a botnet, specifically a variant of the Mirai botnet, that is known for targeting exposed networking devices. The malware is used to take control of compromised endpoints and then launch further attacks, such as distributed DDoS attacks.

A distinctive feature of Moobot is its use of a specific seed, "w5q6he3dbrsgmclkiu4to18npavj702f," within a function designed to generate random strings. This method of using a unique seed for random string generation is employed by the malware as a means to obfuscate its activities and avoid detection.

Moobot spreads by exploiting vulnerabilities found in Cacti and Realtek software. Once devices are compromised, they are incorporated into the botnet and can be used in DDoS attacks or other malicious activities. The botnet has also been repurposed by threat actors for cyber espionage.

APT28, for instance, did not develop the Moobot malware, but rather used it to install their own scripts and files. Specifically, they repurposed the botnet, provided by **cybercriminals**, to create a global cyber espionage platform from a network of compromised small office/home office (SOHO) routers, particularly Ubiquiti Edge OS routers. APT28 exploited publicly known default administrator passwords on Ubiquiti Edge OS routers to gain access. This network was then used to conduct spearphishing and credential harvesting campaigns against targets of intelligence interest including foreign governments, as well as military, security, and corporate organizations.



```
la      $v0, loc_410000
addiu   $sp, -0x38
addiu   $t6, $sp, 0x30+var_28
addiu   $a2, $v0, (aW5q6he3dbrsgmc - 0x410000)  # "w5q6he3dbrsgmclkiu4to18npavj702f"
sw      $s1, 0x30+var_s4($sp)
sw      $s0, 0x30+var_s0($sp)
```

Figure 6. *Random string-generating function*

CredoMap

CredoMap is a stealer malware that was developed to target users in Ukraine during the ongoing war. The malware is distributed through weaponized documents that exploit the Follina vulnerability (CVE-2022-30190). This exploit is used to download an HTML file, which in turn executes JavaScript code that downloads and launches a .NET stealer. The malicious document used to spread CredoMap was first observed in June 2022.

The primary function of CredoMap is to steal credentials and cookies from various web browsers. It specifically targets Google Chrome, Mozilla Firefox, and Microsoft Edge. For Chrome, the malware copies the "Cookies" and "Login Data" files from the user's data directory.

CredoMap specifically targeted users in Ukraine. After collecting the data, CredoMap exfiltrates the stolen information using the IMAP email protocol.

Headlace

HeadLace is a modular malware that is used in stage-based loading to compromise systems and steal credentials. HeadLace infection typically starts with a phishing email containing a malicious URL. These phishing emails often use lures related to current events or attractive offers, such as an event ticket or a car for sale advertisement, to entice victims to click on the link.

The URLs often lead to legitimate web services like Webhook.site, which have been weaponized to host malicious scripts. These scripts use techniques such as the search-ms protocol and manipulation of browser history to trick users into thinking they are interacting with legitimate Windows functionality. They may also use browser checks and geolocation verification to ensure that the payload is delivered only to targets in specific countries.

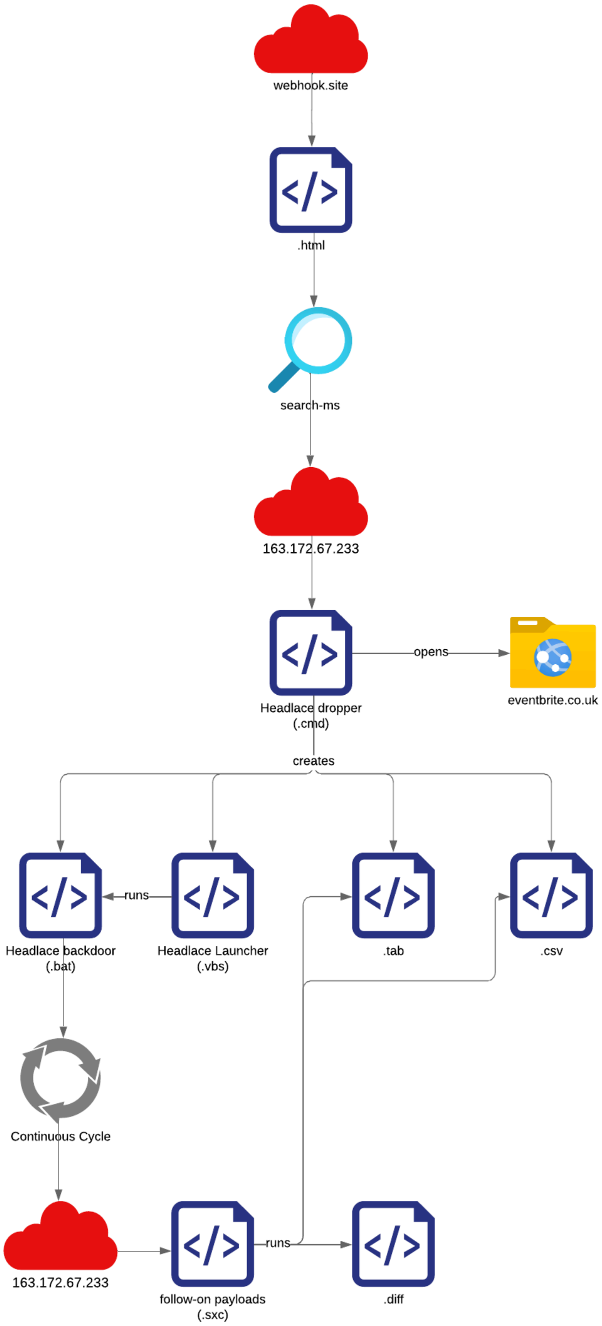
The initial script then downloads a ZIP archive containing the HeadLace dropper, which is disguised with a double file extension to trick users into thinking it is a benign file. This dropper can be executed in several ways:

- Exploiting the CVE-2023-38831 WinRAR vulnerability: This vulnerability allows the dropper to run silently when a user opens a malicious archive with a vulnerable version of WinRAR.
- DLL hijacking: The dropper is packaged with a legitimate executable that is susceptible to DLL hijacking. When the executable is run, it loads a malicious DLL that executes the dropper.
- Direct execution: The dropper may be disguised as a Windows update script and executed directly by the user.

The HeadLace dropper writes and executes a series of files that perform malicious operations on the target system. It is designed to be stealthy, using self-deleting mechanisms to remove traces of its presence. The main components include:
.CMD dropper: This component writes the launcher and backdoor files to the %programdata% directory and then executes the launcher.
.VBS launcher: This component is responsible for silently executing the backdoor.
.BAT backdoor: This component sets up a continuous loop to execute malicious actions.

The backdoor leverages Microsoft Edge in headless mode (without a user interface) to fetch and execute additional payloads from a remote server. This allows the script to run undetected by the user. It facilitates data exfiltration by collecting information from the user’s system, including the contents of specific directories, and transmitting it to a remote server controlled by the attacker. To maintain its foothold on the compromised system, HeadLace operates in a continuous execution loop, repeatedly downloading and executing additional malicious code to guarantee its persistence. Moreover, the backdoor incorporates self-cleaning mechanisms, methodically removing temporary files and other artifacts to minimize its forensic footprint and evade detection by security tools and analysts.

Notably, one campaign, which likely targeted diplomats, involved a fake advertisement for an Audi Q7 Quattro SUV, titled "Diplomatic Car For Sale". This advertisement included vehicle images and contact details to enhance credibility. This specific tactic is not unique to APT28, as APT29 has also previously used similar methods, repurposing a BMW advertisement to target diplomatic missions.

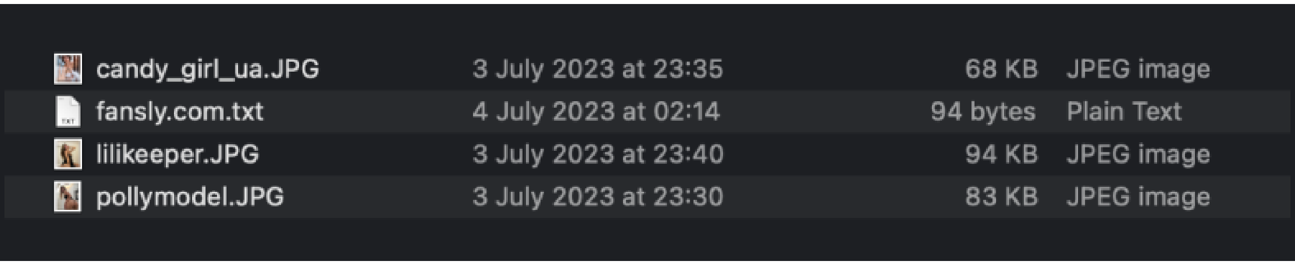


Steal-It

The "Steal-It" campaign is a cyber espionage operation designed to steal and exfiltrate NTLMv2 hashes and system information. The threat actors utilize customized PowerShell scripts, system commands, and the Mockbin API platform to achieve their objectives. This campaign employs a geofencing strategy to target specific regions including Australia, Poland, and Belgium. The initial infection vector involves LNK files concealed in zip archives, and persistence is established through the use of the StartUp folder.

The campaign's infection chains include several variations:

- NTLMv2 Hash Stealing Infection Chain: This chain uses a modified version of Nishang’s Start-CaptureServer PowerShell script to capture NTLMv2 hashes. The captured hashes are then exfiltrated via a GET request to a Mockbin URL using the Net.WebClient.DownloadString() function.
- SystemInfo Stealing Infection Chain: This chain uses the OnlyFans brand as a lure to trick users into downloading malicious files. The infection starts with a malicious LNK file that redirects to a Mocky URL through JavaScript. The JavaScript verifies if the user is on a Windows system and located in Australia. If those conditions are met, another malicious LNK file is downloaded that collects and exfiltrates system information to a Mockbin URL.
- Fansly Whoami Exfil Infection Chain: This chain uses explicit images of models from the Fansly platform to entice users into downloading malicious files. The chain uses JavaScript to verify the operating system, the country code, and the IP address version. If all conditions are satisfied, it downloads a malicious batch file, which eventually executes the "whoami" command and sends the output to a Mockbin URL.
- Windows Update Exfil Infection Chain: This chain begins with a malicious LNK file disguised as a Windows update inside a zip archive. It uses a fake "Windows Update" title to trick users in Belgium into executing multiple stages of a PowerShell script. This script downloads additional scripts from Mocky URLs. The final script in this chain executes commands like tasklist and systeminfo and exfiltrates the output using WebClient.UploadString() to a Mockbin URL.



candy_girl_ua.JPG	3 July 2023 at 23:35	68 KB	JPEG image
fansly.com.txt	4 July 2023 at 02:14	94 bytes	Plain Text
lilikeeper.JPG	3 July 2023 at 23:40	94 KB	JPEG image
pollymodel.JPG	3 July 2023 at 23:30	83 KB	JPEG image

MASEPIE, OCEANMAP, STEELHOOK

APT28 uses a suite of malware including MASEPIE, OCEANMAP, and STEELHOOK, which are linked through their coordinated use in cyberattacks and their evolution from older malware (CREDOMAP).

After gaining initial access through malicious links in emails, attackers deploy MASEPIE to establish a foothold and execute further payload. OCEANMAP maintains control and executes commands via cmd.exe, while STEELHOOK steals sensitive browser data. These malware variants work in concert as part of a coordinated cyberattack to establish persistence, steal data, and enable further network reconnaissance and lateral movement.

It was first reported in late December 2023 by CERT-UA. It is used in phishing campaigns impersonating government and non-governmental organizations (NGOs) in Europe, the South Caucasus, Central Asia, and North and South America. The lures include topics such as finance, critical infrastructure, executive engagements, cybersecurity, maritime security, healthcare, business, and defense industrial production.

MASEPIE is a Python-based backdoor that facilitates follow-on actions by communicating with its command and control (C2) server . It can upload and download files, as well as execute commands using the TCP protocol. It is delivered using the “search-ms” protocol and WebDAV servers.

OCEANMAP is another backdoor, but it's developed using the C# programming language. It is a more capable version of CREDOMAP, a previous stealer used by the group. Its main functionality is to execute commands using cmd.exe, and it uses the IMAP protocol as a control channel. OCEANMAP achieves persistence by creating a .URL file 'VMSearch.url' in the autorun directory.

STEELHOOK is a PowerShell script designed to steal Internet browser data, specifically from Chrome and Edge. It exfiltrates data such as "Login Data", "Local State", and the DPAPI master key by sending it to the management server using an HTTP POST request in base64-encoded form. STEELHOOK likely took over the data-stealing role previously held by CREDOMAP.

HATVIBE and CHERRYSPY

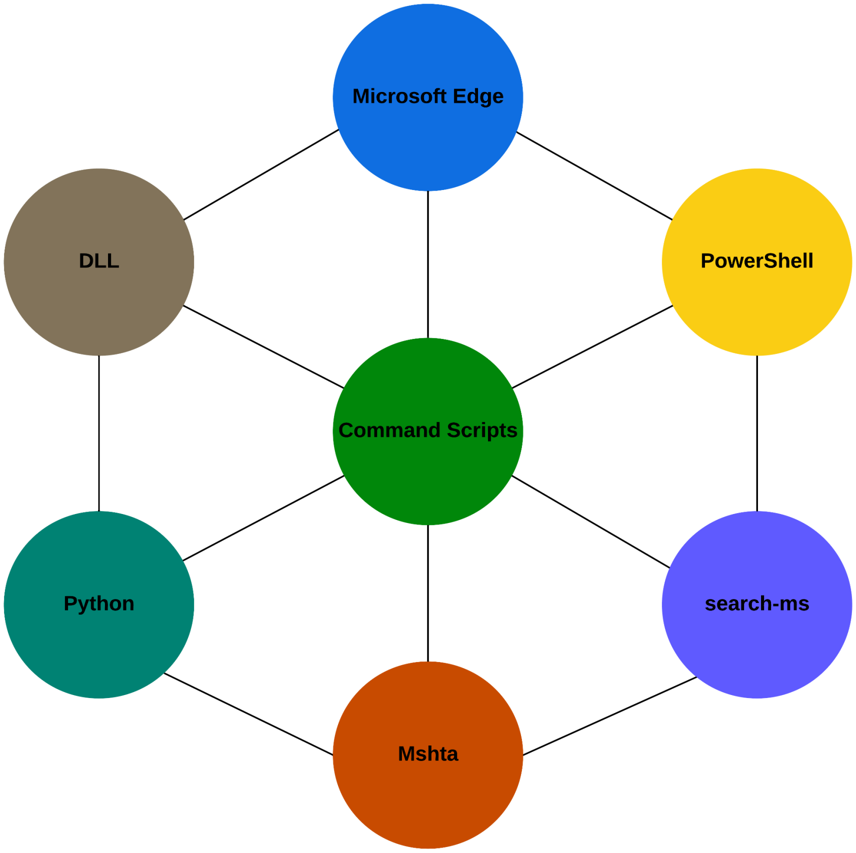
The malware campaign involving HATVIBE and CHERRYSPY represents a significant threat, particularly in the realm of cyber espionage. First observed in April 2023, the campaign has since expanded its reach, with victims identified across eleven countries by July 2024, predominantly in Central Asia, but also extending to East Asia and Europe. The targets of this campaign are primarily government entities, human rights organizations, educational institutions, and private security companies.

HATVIBE, a custom HTML Application (HTA) loader, serves as the initial entry point for the malware. It is designed to deliver and execute other malicious payloads, most notably the CHERRYSPY backdoor. To ensure persistence on a compromised system, HATVIBE creates a scheduled task that executes the HTA file using mshta.exe. Communication with its command-and-control (C2) server is achieved through an HTTP PUT request, with the request body containing sensitive information such as the username, computer name, and the XOR key used for payload decryption.

CHERRYSPY, the second component of the attack, is a custom Python backdoor used for espionage activities. Similar to HATVIBE, CHERRYSPY achieves persistence through a scheduled task, which executes the .pyd file using a Python interpreter. To ensure secure communication with its C2 server, CHERRYSPY employs a combination of asymmetric (RSA) and symmetric (AES) encryption algorithms, allowing for secure key exchange and confidential data transmission. The sophistication of these tools, along with the careful selection of targets, underscores the advanced nature of this campaign.

5 LOLBINs

APT28 uses Living-Off-the-Land Binaries (LOLBINs) in their cyber operations to execute malicious activities while remaining covert. By leveraging legitimate, pre-installed tools and services within the Windows operating system, they can perform tasks such as command execution, data exfiltration, or lateral movement under the radar. This approach allows APT28 to blend seamlessly into normal system operations, making their actions appear as routine administrative tasks. The use of LOLBINs not only helps them bypass traditional security mechanisms, such as antivirus software, but also significantly reduces forensic evidence, as these tools are trusted and often excluded from scrutiny.



These techniques have been actively used in APT28 operations for the last 3 years.

- mshta.exe: This is a legitimate Microsoft utility mshta.exe that is used to execute malware. The threat actor use mshta.exe to execute the HATVIBE HTA file, achieving persistence on the compromised system through a scheduled task

- Command scripts: The group made use of command scripts (.cmd), batch files (.bat), and Visual Basic scripts (.vbs) to execute commands and perform malicious operations on the target system.

- Microsoft Edge in Headless Mode: The group leveraged Microsoft Edge in headless mode to fetch and execute additional payloads from remote servers. This allowed them to perform malicious activities without a visible browser window, making their actions more covert.

- PowerShell: In the initial campaigns, APT28 used PowerShell to execute malicious code.

- search-ms URI handler: APT28 uses the "search-ms" URI handler to download malware hosted on actor-controlled servers. This involves a malicious link embedded in a lure document that, when clicked, uses the Windows search protocol to download and execute a malicious file. The "search-ms" protocol is used to locate a Saved Search XML file (.search-ms), which then points to a malicious .LNK file on the attacker's server. The display name parameter was used to set a custom display name for the search results to make them appear related to a specific target (like "diplomat.va"), which could deceive users into trusting the results. More about this technique in our report.

- DLL Execution: This action results in the execution of a malicious DLL.

- Python: APT28 uses a Python interpreter to execute malicious scripts. This shows that they use python.exe as a LOLBIN to execute their malware.

6 Vulnerabilities

APT28 employs a wide array of vulnerabilities to focus on strategic targets, including defense sector and government entities. By leveraging these vulnerabilities, the group gains access to systems, escalates privileges, and deploys malware. Their approach is both diverse and adaptable, utilizing zero-day exploits, publicly disclosed vulnerabilities, and custom tools such as CredoMap and HATVIBE to achieve their objectives.

Exploitation of Windows Print Spooler Vulnerability (CVE-2022-38028) via GooseEgg.
One of the most significant methods employed by APT28 is the use of the GooseEgg tool to exploit the Windows Print Spooler vulnerability (CVE-2022-38028). This vulnerability enables privilege escalation by manipulating a JavaScript constraints file, which is then executed with SYSTEM-level permissions. The attack sequence involves redirecting the C: drive symbolic link, which forces the Print Spooler to load a malicious JavaScript file from an attacker-controlled directory. This leads to the execution of a malicious DLL, named wayzgoose.dll, with elevated privileges.

Zero-Day Exploitation of Microsoft Outlook Vulnerability (CVE-2023-23397).
APT28 has demonstrated the ability to leverage zero-day vulnerabilities, such as the CVE-2023-23397 vulnerability in Microsoft Outlook, to gain unauthorized network access. This vulnerability allows for Net-NTLMv2 hash leaks and requires no user interaction to be exploited. APT28 began exploiting this vulnerability in March 2022, prior to its public disclosure, and continued its use even after the vulnerability was patched. This demonstrates the group's dedication to intelligence gathering, outweighing the risk of exposure. This exploit has been used in numerous campaigns targeting over 30 organizations in 14 nations, with a primary focus on NATO members.

Exploitation of WinRAR Vulnerability (CVE-2023-38831).
APT28 exploited a vulnerability in WinRAR versions prior to 6.23, identified as CVE-2023-38831. This vulnerability allows attackers to execute arbitrary code via specially crafted ZIP archives. When a user attempts to open a benign file within a malicious archive, which also contains a folder with a matching name concealing executable content, it results in the execution of the malicious code. This vulnerability was used to deliver the Headlace malware.

Weaponized Documents and the Follina Vulnerability (CVE-2022-30190).
APT28 has utilized weaponized documents to deliver malware through the exploitation of the Follina vulnerability (CVE-2022-30190) in their CredoMap campaigns. They used a malicious RTF document designed to exploit

this vulnerability. Opening this document leads to the download of an HTML file and the execution of JavaScript code, which leverages the vulnerability to execute code by exploiting a flaw in the Microsoft Support Diagnostic Tool (MSDT). The JavaScript code subsequently downloads and launches the CredoMap malware.

SNMP Vulnerability (CVE-2017-6742) in the Jaguar Tooth Campaign.
The SNMP vulnerability (CVE-2017-6742) was exploited in the Jaguar Tooth Campaign to gain initial access and deploy itself. This vulnerability enables remote code execution and write access to the target operating system. The vulnerability is triggered by a specially crafted SNMP Object Identifier (OID) that causes a stack-based buffer overflow.

Roundcube Webmail Vulnerabilities.
APT28 has exploited several vulnerabilities in Roundcube Webmail to conduct reconnaissance, exfiltrate data, and redirect emails:

- CVE-2020-35730: A cross-site scripting (XSS) vulnerability, enabling attackers to send emails with embedded JavaScript in a link reference.
- CVE-2021-44026: A SQL injection (SQLi) vulnerability, allowing attackers to exfiltrate Roundcube database information.
- CVE-2020-12641: A vulnerability exploited to conduct reconnaissance and exfiltrate data from victim's Roundcube server.
- CVE-2020-13965: Another XSS vulnerability that allows for XSS when previewing XML attachments.

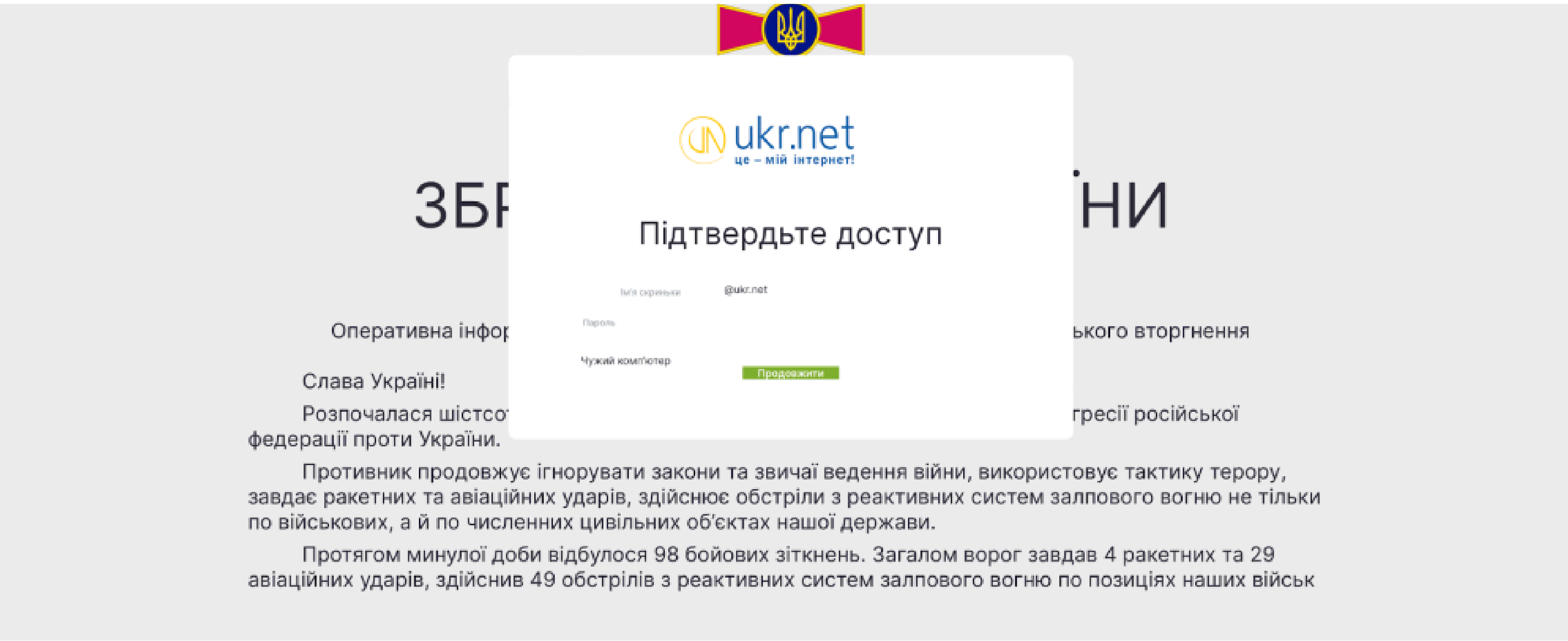
These vulnerabilities were exploited using malicious JavaScript files to redirect emails, perform reconnaissance on the target Roundcube server, and exfiltrate data including session cookies, address books, and database information.

HTTP File Server Vulnerability (CVE-2024-23692).
APT28 exploited a Template Injection flaw, CVE-2024-23692, found in the HTTP File Server (HFS) software. This vulnerability allows unauthenticated users to execute arbitrary commands through specially crafted HTTP requests. APT28 used this vulnerability to gain initial access to systems and deliver the HATVIBE malware. The attackers likely exploited this vulnerability to execute code or drop malicious files onto the targeted system, thus initiating the infection chain.

7 Phishing Campaigns

APT28 employs a variety of phishing techniques to infiltrate targeted systems and networks, primarily focusing on credential harvesting. Their phishing campaigns are designed to steal user credentials, often bypassing standard security measures like two-factor authentication (2FA) and CAPTCHA. These techniques are not only technically advanced but also contextually relevant to the threat actor's objectives, which include intelligence gathering.

The group's operations often begin by targeting webmail service users, particularly those using Yahoo and Ukr.net. To enhance their effectiveness, APT28 uses compromised Ubiquiti routers, hosting scripts that defeat 2FA measures. This allows them to relay requests between legitimate services and the compromised routers, successfully bypassing security protocols. They also leverage free API and hosting services for page and code hosting, credential capture, and data exfiltration, streamlining their operations and avoiding the need for their own infrastructure.



Підтвердьте доступ

Оперативна інфор … ького вторгнення

Слава Україні!

Розпочалася шістсо … гресії російської федерації проти України.

Противник продовжує ігнорувати закони та звичаї ведення війни, використовує тактику терору, завдає ракетних та авіаційних ударів, здійснює обстріли з реактивних систем залпового вогню не тільки по військових, а й по численних цивільних об'єктах нашої держави.

Протягом минулої доби відбулося 98 бойових зіткнень. Загалом ворог завдав 4 ракетних та 29 авіаційних ударів, здійснив 49 обстрілів з реактивних систем залпового вогню по позиціях наших військ

One notable technique is the "man-in-the-browser" attack, where an HTML attachment with a fake login window is used. The fake login page is embedded in an iframe, tricking users into entering their credentials, which are then stolen by the attackers. APT28 also uses public HTTP debugging/webhook services to retrieve stolen credentials, setting up webhook pages on services like PipeDream.com and Webhook.site. This method allows them to receive credentials sent by the victim, marking a significant shift for a state-sponsored threat actor to use such services for phishing operations.

For accounts secured with 2FA, APT28 utilizes dedicated webpages hosted on *.frge.io domains, which interact with a Python script running on compromised Ubiquiti routers. These scripts communicate with the Ukr.net API to authenticate users and bypass 2FA, while the anti-captcha.com service is used to bypass RecaptchaV2 during the authentication process. In addition to these technical tactics, APT28 targets specific military interests, imitating military operational information in their phishing pages and mimicking services like Ukr.net. They also employ "browser in browser" attacks by embedding fake login pages within iframes.

Furthermore, APT28 has been seen utilizing fake reCAPTCHA mechanisms in their phishing campaigns. They send emails with links that imitate Google Sheets, and when a user clicks on these links, a fake reCAPTCHA appears. If the user interacts with the fake reCAPTCHA by clicking the "I am not a robot" checkbox, a PowerShell command is copied to the clipboard. Once executed by the user, this command downloads and runs an HTA file and a PowerShell script, which then establishes an SSH tunnel, steals browser data, and downloads the METASPLOIT tool. This multi-stage approach demonstrates the group's comprehensive and adaptable methods in cyber operations.

8 Legitimate Internet Services

The Russian threat actor has been observed using legitimate internet services to conduct malicious activities while evading detection. These services, which are typically used by developers and organizations for testing, debugging, and automation, include platforms like Webhook.site, Pipedream.com, Mocky.io, Mockbin.org, Forge (getforge.com). By leveraging these tools, APT28 can effectively disguise their operations within normal web traffic, which makes it more difficult for security professionals to identify and attribute their actions.

One of the key purposes for using these legitimate services is to exfiltrate stolen data. These platforms provide attackers with a seamless way to collect intelligence in real-time, without the need to host their own infrastructure, and because these services are widely used, connections to them are often overlooked.

APT28 also utilizes trusted platforms like Mocky, Mockbin, and Forge to embed malicious payloads, host phishing portals, or create fake API endpoints that appear legitimate. This tactic not only increases the believability of their operations to victims but also enables them to bypass traditional security measures like firewalls and intrusion detection systems. By using public services, APT28 avoids the risk of their infrastructure being identified, blacklisted, or traced back to them, which complicates attribution.

These services are often used to establish temporary or disposable infrastructure for single-use phishing campaigns or short-lived command-and-control (C2) servers. Platforms like Mockbin and Mocky offer easy-to-configure endpoints for hosting data or redirecting victims to malicious resources, reducing the operational burden on the attackers and making their operations cost effective as there is no need for the group to maintain dedicated servers. Additionally, traffic to these internet services blends in with normal operations, making detection difficult for security teams. Because enterprises often whitelist or permit access to these platforms, APT28 can use this trust to mask malicious communications within legitimate-looking traffic, avoiding security monitoring.

Service Name	Domain	Official Use	APT28 Misuse
Webhook	webhook[.]site	Generally used by developers to test and debug webhooks, which are automated messages sent between applications when an event occurs.	Used by APT28 to collect exfiltrated data, such as credentials and session cookies, from victims.
Pipedream	pipedream[.]com	A platform for integrating different applications and services, allowing developers to build and automate workflows by connecting various APIs.	Used to receive stolen data from phishing victims, enabling covert collection of intelligence.
Mocky	mocky[.]io	Designed for creating mock APIs for development purposes. Lets developers simulate the behavior of an actual API for front-end development and testing.	Used to embed malicious payloads, host phishing portals, and create fake API endpoints. Provides easy-to-configure endpoints for hosting data.
Mockbin	mockbin[.]org	Helps developers test and debug HTTP requests and responses by creating mock endpoints.	Used to host malicious content, set up phishing sites, and create fake APIs. Provides endpoints for redirecting victims to malicious resources and is also used for short-lived C2 servers.
Forge	getforge[.]com	A platform that helps developers deploy and manage web applications.	Used to embed malicious payloads, host phishing portals, or create fake API endpoints.

9 Network Infrastructure

APT28 demonstrates a notable preference for compromising edge infrastructure, such as routers and other internet-connected devices. This tactic allows them to maintain access to targeted organizations, even if direct access to endpoints is lost. Their operations are characterized by a combination of exploiting vulnerabilities in commonly used devices and using various anonymization techniques.

One significant aspect of their strategy involves the exploitation of Ubiquiti EdgeRouters, which are popular due to their user-friendly, Linux-based operating system. However, these routers often come with default credentials and lack firewall protection, making them easy targets for APT28. The group uses these compromised routers to collect credentials, proxy network traffic, host spear-phishing pages, and deploy custom tools. Additionally, they've been known to collect NTLMv2 digests and execute NTLM relay attacks using compromised EdgeRouters. The root access they gain allows them to install tools and obfuscate their activities. These routers also serve as command-and-control infrastructure for MASEPIE backdoors, although the malware isn't directly deployed on the routers. Often, the compromise of EdgeRouters is facilitated by the Moobot botnet, which installs OpenSSH trojans. The use of compromised EdgeOS routers appears to blend cybercriminal activities, providing an additional anonymization layer.

APT28 also exploits Cisco IOS routers through the Jaguar Tooth malware, which is a sophisticated attack vector that takes advantage of vulnerabilities in network infrastructure. The group leverages the CVE-2017-6742 vulnerability, a weakness in the Simple Network Management Protocol (SNMP) of Cisco IOS routers. This vulnerability allows for remote code execution and write access to the target operating system, which is critical for the malware's deployment.

To further hide their tracks, APT28 employs various anonymization techniques. They use numerous VPN services, over a dozen different services have been observed in use. Additionally, they use the Tor network, and data center IP addresses to obscure the origin of their attacks. They also use compromised email accounts to launch spear-phishing campaigns, and employ free services like URL shorteners, file hosting services, and email services.

10 Espionage

Since the start of the war in early 2022, APT28's activities have shown a continued and consistent focus on espionage, with a clear objective of data theft. Their campaigns have targeted a variety of sectors and geographical regions, with a notable emphasis on critical infrastructure. A key area of focus for APT28 has been critical government and military networks, highlighting their ongoing pursuit of sensitive state secrets and military intelligence. Furthermore, APT28's espionage activities have also targeted diplomatic institutions, an area that sometimes overlaps with the actions of APT29.

Just before the Russian invasion of Ukraine in early February 2022 the group employs in espionage efforts a novel approach to compromising Wi-Fi networks, the Nearest Neighbor Attack This sophisticated tactic involves compromising multiple organizations in close proximity to the intended target to gain access to their Wi-Fi networks. The goal of this specific attack was to collect data from individuals with expertise and projects related to Ukraine. Right after the outbreak of the war, the group exploits the 0-day vulnerability CVE-2023-23397 to infiltrate organizations with ties to Ukraine.

Later, APT28 launches attacks with custom backdoors against Ukrainian organizations and massive phishing campaigns using Ukr.net themes, also targeting the Ukrainian military. These actions indicate an attempt to gain access to sensitive military and government communications, potentially aimed at disrupting operations or gathering intelligence on defense strategies. The group's activities also extend beyond Ukraine, with campaigns targeting government agencies not only in Ukraine but also in Europe and NATO countries. NATO and other human rights-related organizations are also among their targets, indicating an intention to monitor or potentially undermine the activities and interests of these organizations. There have been cases where political parties have been targeted, in Poland, the Czech Republic and Germany, with the potential to influence democratic processes in these countries.

Recently, the group has become interested in the Caucasus and Central Asia. APT28 has shown a clear interest in gathering information on regional strategic policies and developments, as evidenced by its choice of think tanks in the Caucasus and Central Asia.

11 Influence

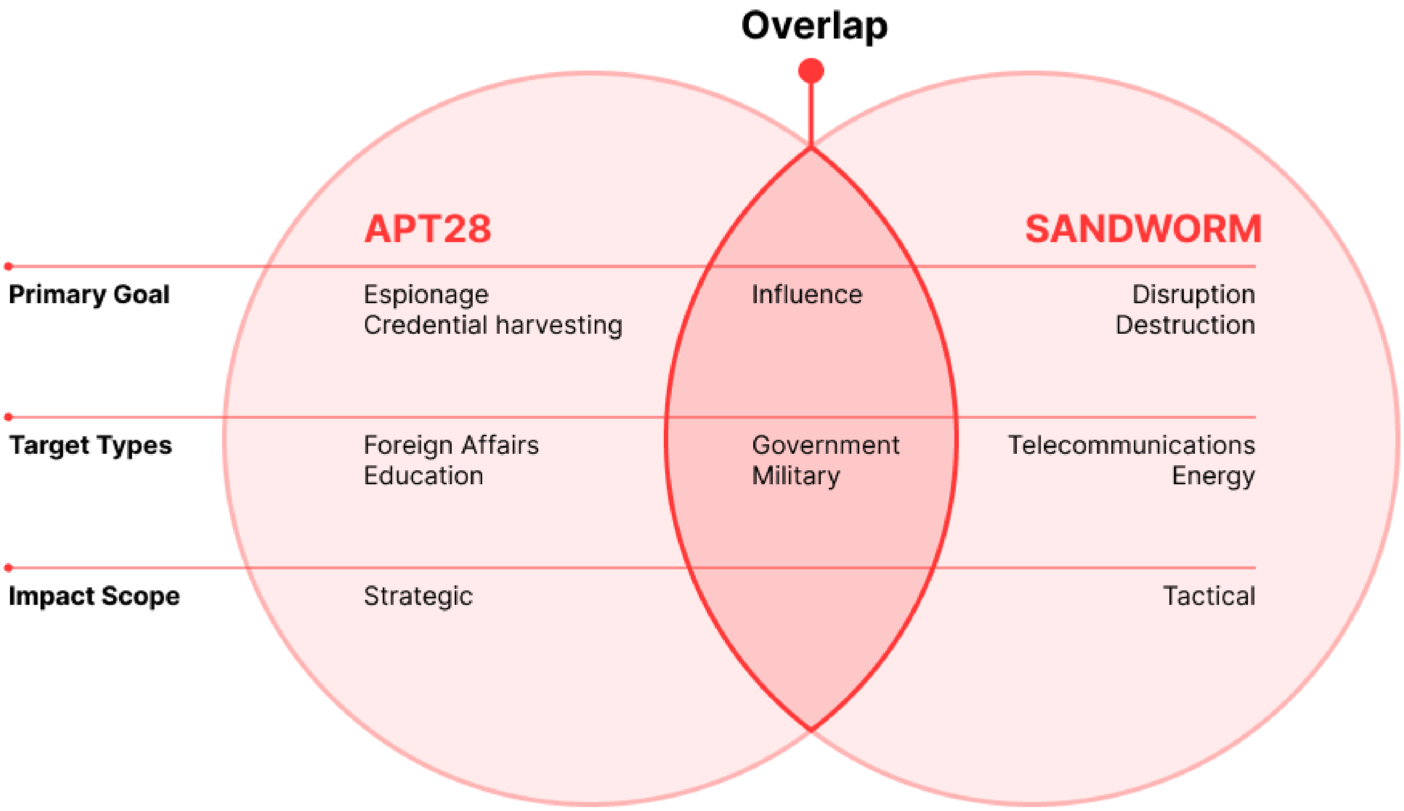
APT28's operations increasingly align with Russian military and geopolitical strategies, although their primary focus remains espionage. Unlike Sandworm, which is associated with deploying destructive malware such as Industroyer2 and HermeticWiper, APT28 has not been definitively linked to wiper usage or explicitly destructive campaigns. However, there has been a discernible shift in their activities toward influence-driven objectives alongside their traditional intelligence-gathering efforts.

APT28 has been involved in manipulation and influence campaigns in the information domain, complementing their cyberattacks. These activities have included phishing attempts targeting political parties and cyberattacks timed around elections globally. Such efforts mirror the group's historical involvement in hack-and-leak campaigns, where stolen emails and documents were publicly released to sway public opinion. These operations often overlap with the activities of pseudo-hacktivist groups like CyberArmyofRussia and NoName057(16), which carry out DDoS attacks on critical online resources during election periods. In parallel, Russian media outlets amplify these efforts through propaganda and disinformation, further shaping public perception.

The group has consistently been employed by Russia to conduct cyber operations against the EU, its member states, and particularly Ukraine. Since 2022, APT28 has focused on espionage campaigns targeting government and military networks. They have also exploited vulnerabilities such as CVE-2017-6742 in Cisco routers, often for reconnaissance purposes. While these activities appear to support intelligence objectives, they could also serve as precursors to potential disruptive operations.

Although APT28 is predominantly centered on espionage, speculation suggests potential collaboration with Sandworm. APT28 may handle initial reconnaissance and access operations, which could then be leveraged by Sandworm for subsequent destructive attacks.

This division of roles reflects the broader structure of Russian cyber forces, where cyber intelligence and cyber influence are distributed between groups like APT28 and Sandworm, each contributing distinct capabilities to a unified strategy.



	APT28	Overlap	SANDWORM
Primary Goal	Espionage Credential harvesting	Influence	Disruption Destruction
Target Types	Foreign Affairs Education	Government Military	Telecommunications Energy
Impact Scope	Strategic		Tactical

12 Conclusion

The cyber espionage group known as APT28 has shown a clear evolution in its methods and objectives, especially after the start of the Russian war in Ukraine. Initially focused on traditional espionage, the group has now blended its activities with active cyber warfare, reflecting a closer alignment with Russia's military and geopolitical goals. The shift indicates a change from simple data theft and influencing narratives to also include attacks on the military, targeting not only Ukraine, but also its allies.

Changes in Tactics

APT28 continues to leverage zero-day vulnerabilities and webmail services as primary attack vectors. Their use of the zero-day vulnerability CVE-2023-23397 at the outset of the war suggests a calculated approach, with preparations likely underway well before the war began. The timing of their operations—starting in earnest only after it became clear that a swift victory in Ukraine would not materialize—indicates strategic patience and adaptability.

Their arsenal has expanded to include custom backdoors and infostealers, alongside scripting languages such as PowerShell, VBScript, and batch files to execute malicious activities. By employing legitimate internet services and LOLBINs, APT28 effectively minimizes detection risks while blending into normal system operations.

APT28 has also demonstrated control over a vast network of compromised devices. This extensive infrastructure supports their cyber espionage and operational needs. A notable case involved cooperation between cybercriminals and APT28. In this instance, cybercriminals deployed Moobot malware on Ubiquiti Edge OS routers. APT28 then repurposed the botnet using bespoke scripts, transforming it into a sophisticated cyber operations platform.

Changes in Objectives

The transition from pre-2022 to post-2022 reflects a shift from traditional espionage to a hybrid of espionage and active cyber warfare. APT28’s focus on government and the extended targeting of Ukraine’s allies aligns closely with Russia’s broader military and geopolitical strategies. While espionage—data theft and influencing narratives—remains at the core of their activities, the scope and scale of their operations have grown.

The group’s geographical focus has broadened from primarily Eastern Europe to include all of Europe, especially Ukraine and Poland, as well as the Caucasus and Central Asia. They target diplomatic institutions and the defense industrial base. Furthermore, campaigns against scientific institutions and think tanks reveal an effort to gather intelligence on regional strategic policies.

The evolution of APT28's operations indicates a strategic shift towards supporting Russia's geopolitical objectives, most notably since the Russian war in Ukraine began. Which demonstrates a clear alignment with Russia's military and geopolitical ambitions.

Endnotes

1. https://go.recordedfuture.com/hubfs/reports/CTA-RU-2024-1121.pdf
2. https://www.ncsc.gov.uk/static-assets/documents/malware-analysis-reports/jaguar-tooth/NCSC-MAR-Jaguar-Tooth.pdf
3. https://www.microsoft.com/en-us/security/blog/2024/04/22/analyzing-forest-blizzards-custom-post-compromise-tool-for-exploiting-cve-2022-38028-to-obtain-credentials/
4. https://securityintelligence.com/x-force/itg05-leverages-malware-arsenal/
5. https://go.recordedfuture.com/hubfs/reports/CTA-RU-2024-0530.pdf
6. https://www.zscaler.com/de/blogs/security-research/steal-it-campaign
7. https://blog.sekoia.io/apt28-leverages-multiple-phishing-techniques-to-target-ukrainian-civil-society/
8. https://go.recordedfuture.com/hubfs/reports/CTA-RU-2024-0530.pdf
9. https://www.volexity.com/blog/2024/11/22/the-nearest-neighbor-attack-how-a-russian-apt-weaponized-nearby-wi-fi-networks-for-covert-access/
10. https://unit42.paloaltonetworks.com/russian-apt-fighting-ursa-exploits-cve-2023-233397/
11. https://cert.gov.ua/article/6276894
12. https://cert.gov.ua/article/40106
13. https://cert.gov.ua/article/6280129
14. https://cert.gov.ua/article/5702579
15. https://www.rnbo.gov.ua/en/Diialnist/6248.html
16. https://services.google.com/fh/files/misc/apt28-window-russia-cyber-espionage-operations.pdf

About Maverits

At Maverits, we are on a mission to reshape the cybersecurity landscape. Headquartered in Ukraine, our company offers a wide range of services, including Threat Intelligence, Incident Response, Consulting & Training. Our mission is to empower organizations with the tools and knowledge they need to defend against cyber threats. We believe that in today’s digital world, security is not a luxury but a necessity. By combining advanced threat intelligence, state-of-the-art technology, and a team of top-tier cybersecurity experts, Maverits helps businesses stay ahead of potential threats and secure their future.

maverits.com