CYBLE®

APT Threat Landscape Report: H1-2024

→

CONTENT

EXECUTIVE SUMMARY

During the first half of 2024, **Cyble Research & Intelligence Labs** observed notable advancements in the tactics, techniques, and procedures (TTPs) employed by Advanced Persistent Threat (APT) groups. This report aims to provide a comprehensive overview of significant incidents, emerging patterns, and the evolution in the strategies of these APT groups between January and June 2024.

KEY FINDINGS

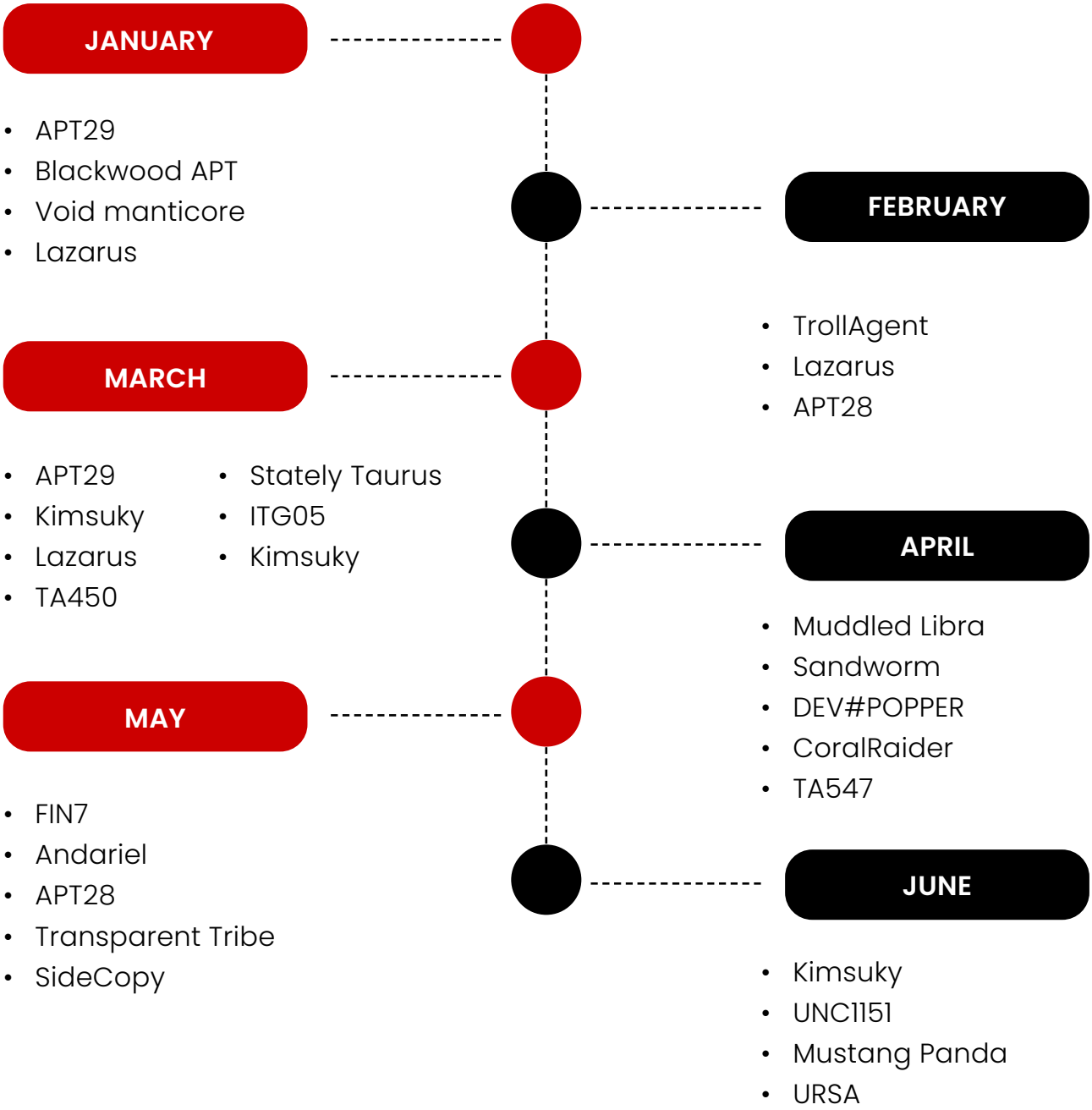
1. **Attack Techniques continue to evolve:**
   APT groups continue to evolve their techniques for initial compromise, utilizing phishing and malicious software and exploiting vulnerabilities to gain access. Persistence strategies have similarly been upgraded to include malware deployment, scheduled tasks, and backdoors.
2. **Command and Control communications go dark:**
   C&C communications and infrastructure are increasingly difficult to detect as they are now carried out using HTTPS encryption and RSA/AES and even leveraging platforms like Telegram.
3. **Critical Infrastructure and Government in the crosshairs:**
   Critical infrastructure, financial institutions, government agencies, and technology sectors were observed to be primary targets for APT groups in H1-2024.
4. **Geopolitical Flashpoints draw APT groups' attention:**
   Due to ongoing geopolitical tensions, APT activity increased in global flashpoints such as Ukraine and Israel. Other frequently targeted countries included the United States, the United Kingdom, Germany, and South Korea.
5. **Vulnerability Exploits remain a key vector for attack:**
   In H1-2024, key vulnerabilities were aggressively targeted by APTs either as a direct exploit or for initial access.
6. **APT Groups' Arsenal diversifies:**
   To achieve their intended purpose, whether it be initial access, remote access, lateral movement, or even credential theft, APT groups are using a wider range of diverse malware families such as WINELOADER, Cobalt Strike, NetSupport RAT, and more.

Our report aims to expand on these key findings with detailed observations, timelines, mitigation strategies, and recommendations for our readers on how they can secure themselves from APT attacks.

TIMELINE

The attack timeline highlights significant cyber incidents and trends from January to June 2024, showcasing how APTs evolved their tactics. The figure below shows the timeline of APT attacks from January 2024 to June 2024.

APT ATTACKS



TARGETED SECTORS

APTs primarily target critical infrastructure, financial institutions, government agencies, and technology sectors. Their goal is to gain prolonged access to these systems, steal sensitive data, and disrupt operations through sophisticated, persistent attacks. The following are the sectors targeted by the APTs since January 2024:

- Government & LEA
- IT & ITES
- Telecommunications
- Aviation
- NGOs
- Manufacturing
- Construction
- Political Parties
- Education & Academia
- Multinational Organizations

TARGETED COUNTRIES

APTs typically target nations with advanced economies and critical infrastructure, with common targets being the United States, the United Kingdom, Germany, and South Korea. Due to current geopolitical tensions, there is a notable rise in APT activities targeting Ukraine and Israel. These Threat Actors (TAs) aim to access sensitive data, disrupt operations, and conduct espionage activities.

COUNTRIES TARGETED BY APTS

Figure 1 - Countries Targeted by APTs Since January 2024

COUNTRIES OF ORIGIN

Since January 2024, Russia, China, North Korea, and Iran-based threat groups have primarily targeted other countries in their cyberattacks, aiming to access sensitive data, disrupt operations, and carry out cyber espionage.

COUNTRIES OF ORIGIN APTS

Figure 2 - Countries of Origin APTs Since January 2024

- Russia
- China
- Iran
- North Korea
- Pakistan

TARGETED CVEs

Vulnerable applications are prime targets for APTs in 2024 to conduct various malicious activities.

The table below outlines the key vulnerabilities exploited by APTs, along with their descriptions.

CVE ID	Threat Actor	Vulnerability Description
CVE-2024-21412 CVE-2024-21351	Water Hydra	Microsoft Windows SmartScreen Security Feature Bypass Vulnerability
CVE-2024-21887 CVE-2023-46805	UNC5221	Ivanti Connect Secure and Policy Secure Command Injection Vulnerability
CVE-2024-3400	UTA0218	Palo Alto Networks PAN-OS Command Injection Vulnerability
CVE-2024-24919	UNC2452, APT29 and BITWISE SPIDER	Check Point Quantum Security Gateways Information Disclosure Vulnerability
CVE-2024-23917 CVE-2024-27199	APT29, APT28	Authentication Bypass Using an Alternate Path or Channel and Relative Path Traversal
CVE-2023-34048	UNC3886	VMware vCenter Server Out-of-Bounds Write Vulnerability
CVE-2023-29300	Flax Typhoon	Adobe ColdFusion Deserialization of Untrusted Data Vulnerability
CVE-2023-46747	UNC5174	F5 BIG-IP Configuration Utility Authentication Bypass Vulnerability
CVE-2022-38028	APT28	Microsoft Windows Print Spooler Privilege Escalation Vulnerability
CVE-2021-40539 CVE-2021-27860	Volt Typhoon	Zoho ManageEngine ADSelfService Plus Authentication Bypass Vulnerability and FatPipe WARP, IPVPN, and MPVPN Configuration Upload exploit
CVE-2019-1653 CVE-2019-1652	Volt Typhoon	Cisco Small Business RV320 and RV325 Routers Information Disclosure Vulnerability and Cisco Small Business Routers Improper Input Validation Vulnerability

MALWARE FAMILIES EMPLOYED

APTs in 2024 employ a range of malware to execute various malicious operations such as credential theft, remote access, lateral movement, etc. The table below highlights the malware used by APTs, along with their descriptions.

Malware	APT	Details
WINELOADER	APT29	Likely a variant of the non-public BURNTBATTER and MUSKYBEAT code families.
ROOTSAW	APT29	Dropper
NetSupport RAT	Fin7	Legitimate remote access tool misused by malicious actors to gain unauthorized access, observed in phishing campaigns since 2018.
SUBTLE-PAWS PowerShell Backdoor	Gamaredon	A stealthy PowerShell-based backdoor spreading via USB drives to evade detection.
No-Justic	Homeland Justice	Data wiper malware.
BABYSHARK	Kimsuky	VB script-based malware was first seen in November 2018.
TODDLERSHARK	Kimsuky	Similar to BABYSHARK.
TrollAgent	Kimsuky	Steals information from infected systems, including SSH keys, browser data, and system information, sending it to a C&C server.
Endoor	Kimsuky	Golang-based backdoor.
Nikidoor	Kimsuky	A sophisticated backdoor.
ComeBacker	Lazarus	Found in a backdoored Visual Studio project targeting security researchers in late 2020 and early 2021.
Dora RAT	Andariel	Go-based malware strain used by the Andariel Group.
QUEUESEED/IcyWell/ Kapeka	Sandworm	C++ backdoor for Windows collects system information and executes remote commands.
BIASBOAT	Sandworm	Linux variant of QUEUESEED, disguised as an encrypted file server.
LOADGRIP	Sandworm	Linux variant of QUEUESEED, injects payloads into processes using the ptrace API.

MALWARE FAMILIES EMPLOYED

GOSSIPFLOW	Sandworm	Go-based malware for Windows sets up tunneling using the Yamux multiplexer library, providing SOCKS5 proxy functionality.
Cobalt Strike	Multiple APT groups	Paid penetration testing tool used by attackers to deploy 'Beacon' agents on victim machines.
MASEPIE	APT28	Python malware downloader establishes persistence by modifying the Windows Registry.
STEELHOOK	APT28	PowerShell scripts stealing data from Chrome-based browsers, targeting passwords, cookies, and browsing history.
OCEANMAP	APT28	C# backdoor executing base64-encoded commands via cmd.exe.
Cryptbot	UNC2452	Infostealer obtaining browser credentials, crypto wallets, cookies, credit cards, and screenshots, bundling stolen data into a zip-file for C&C upload.
LummaC2	FIN7	Information stealer written in C, available through Malware-as-a-Service on Russian-speaking forums since August 2022.
Rhadamanthys	FIN7	Stealer malware designed to extract data from infected machines.
Xworm	FIN7	Malware with capabilities ranging from RAT to ransomware.
AndarLoader	Andariel	Malware used by the Andariel Group in their latest campaign
MeshAgent	Andariel	Collects system information for remote management, including features like power and account management, file transfers, and command execution.
ModeLoader	Andariel	Long-used JavaScript malware by the Andariel Group.

CYBLE RESEARCH & INTELLIGENCE LABS' FINDINGS

Cyble Research and Intelligence Labs (CRIL) has identified various APT attacks since the start of 2024, documented in our blog posts. UAC-0184 targeted Ukrainian entities in Finland, utilizing the Remcos RAT. Their latest campaign suggests a focus on Ukraine, using disguised lure documents to distribute the XWorm RAT. Mustang Panda, a China-affiliated group, conducted two campaigns targeting Vietnam, using tax compliance and education-related lures.

UNC1151, originating from Belarus, seems to be targeting Ukraine's Ministry of Defence with specific lure documents. The Turla campaign uses human rights seminar invitations and public advisories as lures, embedding malicious PDFs and MSBuild project files within .LNK files.

Since 2019, the SideCopy group has targeted South Asian nations, particularly India. They have recently targeted university students, indicating a coordinated effort. Transparent Tribe, known for targeting universities, suggests a potential intersection with SideCopy's activities.

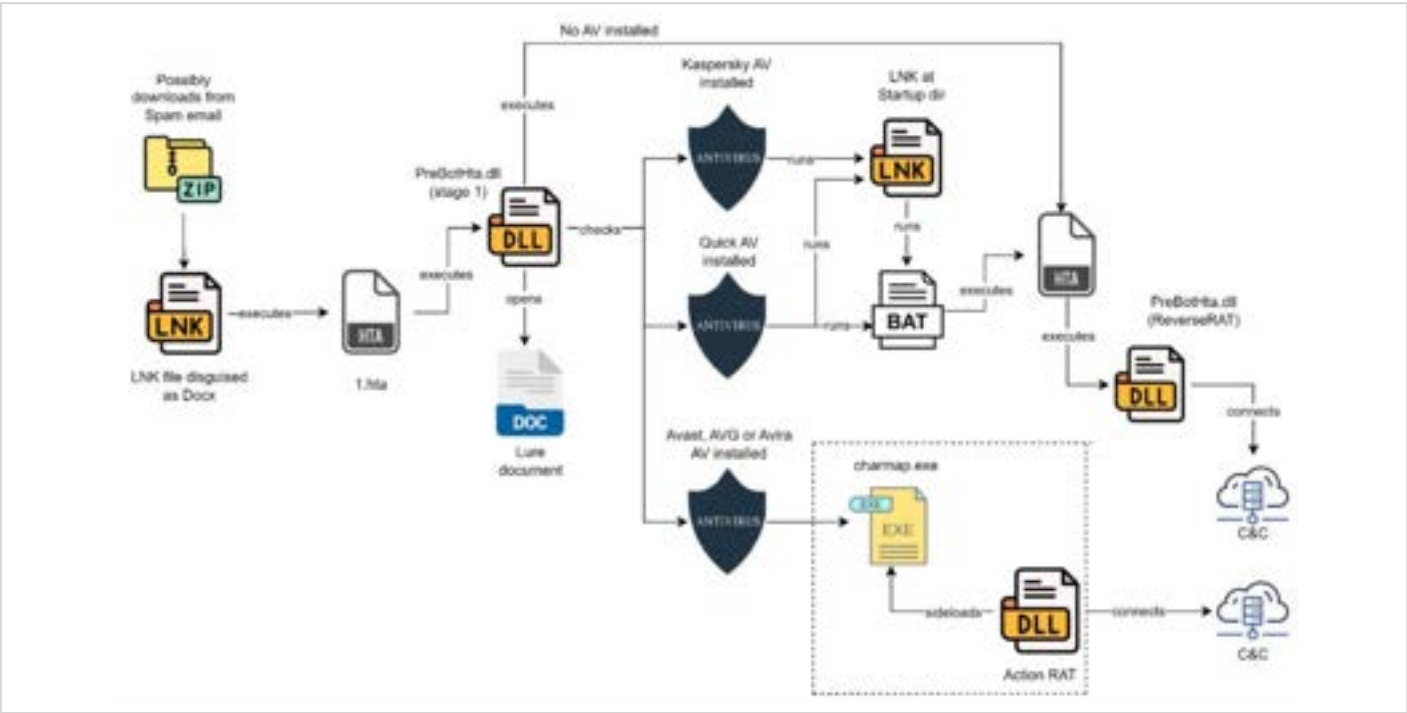


Figure 3 - SideCopy Infection Chain Identified by CRIL

TACTICS, TECHNIQUES, & PROCEDURES (TTPs)

RECONNAISSANCE

Muddled Libra deliberately targets administrative users during their social engineering attacks since those users have elevated permissions within identity providers, SaaS applications, and organizations' various CSP environments.

INITIAL ACCESS

TAs primarily used phishing emails for initial access, exploiting contemporary geopolitical events with malicious documents or compressed files containing shortcut link files. They also employed password spray attacks, using a single password across multiple accounts. They also crafted malicious websites impersonating brands like AnyDesk, WinSCP, BlackRock, Asana, Concur, The Wall Street Journal, Workable, and Google Meet.

They also exploited two critical vulnerabilities in ConnectWise (CVE-2024-1708 and CVE-2024-1709). Software supply chain attacks were also prevalent, with TAs leveraging malicious Python packages for initial access. Other techniques included watering hole attacks and exploiting other application software vulnerabilities.

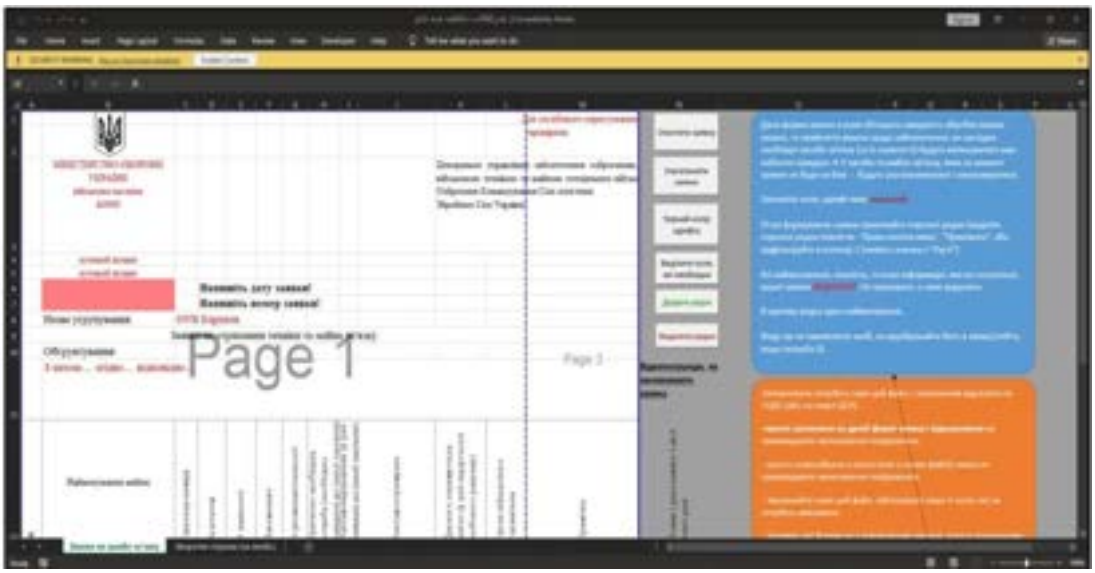


Figure 4 – UNC1151 Using Lure Excel Document

TACTICS, TECHNIQUES, & PROCEDURES (TTPs)

PERSISTENCE

To achieve persistence on affected systems, Threat Actors are leveraging a mixed bag of techniques to ensure stealthy operation, persistence, and redundancies. In H1-2024, these included dropping malware and creating scheduled tasks, placing backdoors in the startup folder, and using legitimate executables paired with malicious DLLs for DLL sideloading. Additionally, they added executables to the autorun registry entry, ensuring the malicious processes would run automatically upon system startup.

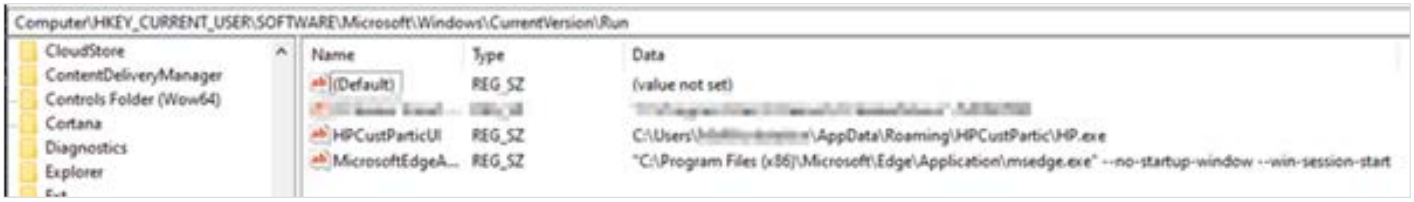


Figure 5 – Mustang Panda Creating Persistence Using Registry Entry

TACTICS, TECHNIQUES, & PROCEDURES (TTPs)

PRIVILEGE ESCALATION

For privilege escalation, attackers bypassed IAM restrictions and modified user permission sets to increase access. They also leveraged GUID creation to facilitate their attacks, ensuring they could manipulate system permissions and maintain elevated privileges. Additionally, the APTs also used process Injection to high-privilege process for privilege escalation.

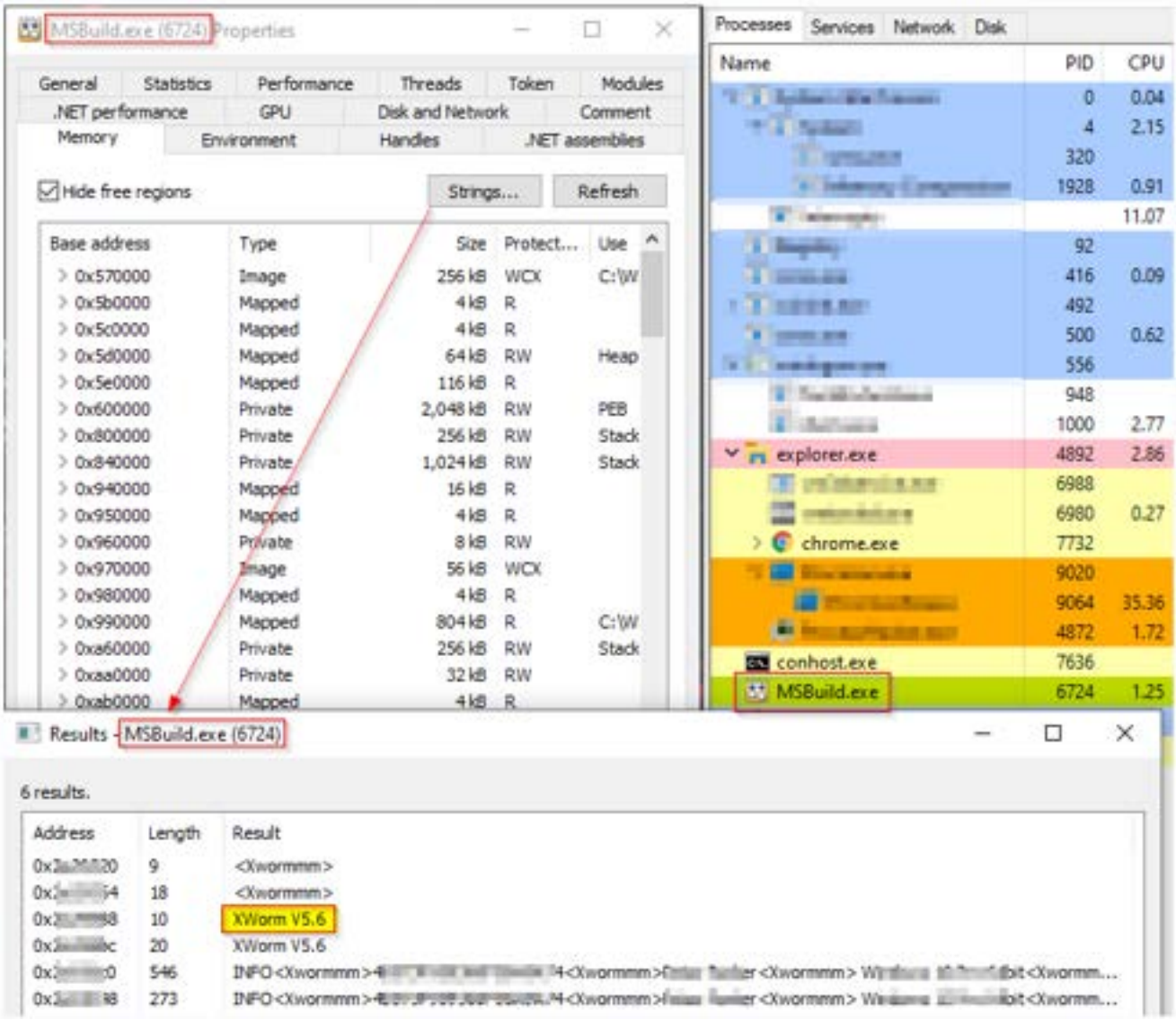


Figure 6 – UAC-0184 Performing Process Injection for Privilege Escalation

TACTICS, TECHNIQUES, & PROCEDURES (TTPs)

DEFENCE EVASION

Evading detection is crucial for stealthy operations, and APTs employed multiple methods to achieve this. They used obfuscated scripts and valid stolen certificates to bypass anti-malware detection. The malware checked for processes related to analysis applications and terminated itself if any were detected.

Instead of their own domains, TAs used commonly recognized services, significantly reducing the detection of malicious links and lowering operational costs. Russian military hackers leveraged compromised Ubiquiti EdgeRouters to evade detection. Additionally, to increase file size and avoid detection, ingeniously embedded partial lure documents within malicious LNK files.

Figure 7 – Mustang Panda Appending Partial Lure to Increase File size

TACTICS, TECHNIQUES, & PROCEDURES (TTPs)

LATERAL MOVEMENT

TAs employed various techniques to explore infected networks, identify vulnerabilities, escalate access privileges, and reach their targets. TAs targeted Secrets Manager to access stored sensitive information. The STEADY#URSA campaign relied exclusively on USB drives to deliver and spread malware within air-gapped network systems. Starting with Innorix Agent, Kimsuky has consistently exploited Korean asset management solutions to distribute malware during lateral movements. Additionally, Sandworm combined previously documented malware with new malicious tools like BIASBOAT and LOADGRIP for Linux to gain access and move laterally within networks.

COMMAND AND CONTROL

APTs strive to keep their command and control (C&C) communications as stealthy as possible. FIN7 uses an interesting ccTLD and name structure (alphabetic string + numeric string + .space) similar to cdn46[.]space. In various campaigns, backdoor malware establishes C&C communication through DNS queries and HTTP requests to dynamic IP addresses via Telegram. In some campaigns communications are secured with HTTPS, with data encrypted using RSA and AES. Sharp Dragon has shifted from dedicated servers to compromised ones, exploiting the CVE-2023-0669 vulnerability in the GoAnywhere platform for pre-authentication command injection. The OCEANMAP backdoor achieves persistence by dropping "EdgeContext.url" into the Windows Startup directory, then logs into the IMAP server for C&C and sends emails containing command results and other identifying parameters.

CONCLUSION

The first half of 2024 saw APT groups significantly augmenting both their attack techniques as well as evasion and persistence strategies, making any intrusion harder to detect and act upon. While the traditional methods of phishing and typosquatting continued to be present, CRIL observed an increase in the exploitation of vulnerabilities to gain initial access. Upon securing access, these APT groups made use of advanced encryption and adaptive network tactics to make their Command & Control communications as stealthy as possible.

The primary targets of these attacks were large in both scope and operation, with Critical Infrastructure, BFSI industries, and Government entities being amongst the most frequently targeted – likely due to APT groups desiring the greatest possible nationwide disruption from a successful attack.

This same philosophy is also apparent in the disproportionally higher targeting of countries with advanced economies, such as the United States, the United Kingdom, Germany, and South Korea, which are frequent targets for APT groups. This is in large part due to APT groups operating in support of countries that have adversarial relations with the aforementioned nations.

Rising global instability and geopolitical conflict also contributed heavily to the scale, timing, and motivation for many notable APT campaigns, particularly those in the Middle East and Ukraine in H1-2024, underscoring the need for nations to preemptively secure their critical infrastructure and organizations from APT groups with real-time, actionable threat intelligence.

MITRE TTPs

Mapping APT campaigns to MITRE ATT&CK tactics, techniques, and procedures (TTPs) involves identifying specific methods used by threat actors and aligning them with the corresponding MITRE ATT&CK framework categories. Here are some examples based on typical APT activities:

1

INITIAL ACCESS

- Phishing: **T1566.001** (Spearphishing Attachment), T1566.002 (Spearphishing Link)
- Exploiting Vulnerabilities: **T1190** (Exploit Public-Facing Application)

2

EXECUTION

- Malicious Scripts: **T1059** (Command and Scripting Interpreter)
- User Execution: **T1204** (User Execution)

3

PERSISTENCE

- Scheduled Tasks: **T1053.005** (Scheduled Task/Job: Scheduled Task)
- Registry Run Keys / Startup Folder: **T1547.001** (Registry Run Keys / Startup Folder)

4

PRIVILEGE ESCALATION

- Exploiting Vulnerabilities: **T1068** (Exploitation for Privilege Escalation)
- Valid Accounts: **T1078** (Valid Accounts)

MITRE TTPs

5

DEFENSE EVASION

- Obfuscated Files or Information: T1027 (Obfuscated Files or Information)
- Deobfuscate/Decode Files or Information: T1140 (Deobfuscate/Decode Files or Information)
- Process Injection: T1055 (Process Injection)

6

CREDENTIAL ACCESS

- Credential Dumping: T1003 (Credential Dumping)
- Brute Force: T1110 (Brute Force)

7

DISCOVERY

- System Network Configuration Discovery: T1016 (System Network Configuration Discovery)
- System Information Discovery: T1082 (System Information Discovery)

8

LATERAL MOVEMENT

- Remote Services: T1021 (Remote Services)
- Windows Admin Shares: T1077 (Windows Admin Shares)

MITRE TTPs

9

COLLECTION

- Data from Local System: **T1005** (Data from Local System)
- Data from Network Shared Drive: **T1039** (Data from Network Shared Drive)

10

EXFILTRATION

- Exfiltration Over C2 Channel: **T1041** (Exfiltration Over C2 Channel)
- Automated Exfiltration: **T1020** (Automated Exfiltration)

11

COMMAND AND CONTROL

- Encrypted Channel: **T1573.002** (Encrypted Channel: Asymmetric Cryptography)
- Web Service: **T1102** (Web Service)

12

IMPACT

- Data Encrypted for Impact: **T1486** (Data Encrypted for Impact)
- Service Stop: **T1489** (Service Stop)

By mapping these techniques, security teams can better understand the attack patterns and prepare defenses accordingly.

REFERENCES

- https://unit42.paloaltonetworks.com/muddled-libra-evolution-to-cloud/
- https://www.mandiant.com/resources/blog/apt29-wineloader-german-political-parties
- https://msrc.microsoft.com/blog/2024/01/microsoft-actions-following-attack-by-nation-state-actor-midnight-blizzard/
- https://blog.sonicwall.com/en-us/2024/01/blackwood-apt-group-has-a-new-dll-loader/
- https://www.esentire.com/blog/fin7-uses-trusted-brands-and-sponsored-google-ads-to-distribute-msix-payloads
- https://www.securonix.com/blog/security-advisory-steadyursa-attack-campaign-targets-ukraine-military/
- https://therecord.media/albania-parliament-telecoms-airline-cyberattacks-wiper-malware
- https://www.kroll.com/en/insights/publications/cyber/screenconnect-vulnerability-exploited-to-deploy-babyshark
- https://asec.ahnlab.com/en/61934/
- https://asec.ahnlab.com/en/63396/
- https://www.genians.co.kr/blog/threat_intelligence/facebook
- https://asec.ahnlab.com/en/66720/
- https://blogs.jpcert.or.jp/en/2024/02/lazarus_pypi.html
- https://asec.ahnlab.com/en/60792/
- https://asec.ahnlab.com/en/66088/
- https://asec.ahnlab.com/en/63192/
- https://www.proofpoint.com/us/blog/threat-insight/security-brief-ta450-uses-embedded-links-pdf-attachments-latest-campaign
- https://unit42.paloaltonetworks.com/chinese-apts-target-asean-entities/
- https://cyble.com/blog/unc1151-strikes-again-unveiling-their-tactics-against-ukraines-ministry-of-defence/
- https://www.bleepingcomputer.com/news/security/russian-sandworm-hackers-targeted-20-critical-orgs-in-ukraine/
- https://blog.checkpoint.com/research/chinese-espionage-campaign-expands-to-target-africa-and-the-caribbean/
- https://cert.pl/en/posts/2024/05/apt28-campaign/
- https://www.bleepingcomputer.com/news/security/russian-hackers-hijack-ubiquiti-routers-to-launch-stealthy-attacks/
- https://securityintelligence.com/x-force/itg05-leverages-malware-arsenal/

REFERENCES

- https://www.securonix.com/blog/analysis-of-devpopper-new-attack-campaign-targeting-software-developers-likely-associated-with-north-korean-threat-actors/
- https://blog.talosintelligence.com/suspected-coralraider-continues-to-expand-victimology-using-three-information-stealers/
- https://www.proofpoint.com/us/blog/threat-insight/security-brief-ta547-targets-german-organizations-rhadamanthys-stealer
- https://cyble.com/blog/uac-0184-abuses-python-in-dll-sideloading-for-xworm-distribution/
- https://cyble.com/blog/vietnamese-entities-targeted-by-china-linked-mustang-panda-in-cyber-espionage/
- https://www.trendmicro.com/en_us/research/24/b/cve202421412-water-hydra-targets-traders-with-windows-defender-s.html
- https://duo.com/decipher/apt-exploits-microsoft-zero-day-in-malware-attacks
- https://cloud.google.com/blog/topics/threat-intelligence/suspected-apt-targets-ivanti-zero-day/
- https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Cyber-Sicherheitslage/Analysen-und-Prognosen/Threat-Intelligence/Aktive_APT-Gruppen/aktive-apt-gruppen.html
- https://securityaffairs.com/157769/apt/unc3886-exploits-vcenter-server-zero-day-cve-2023-34048.html
- https://australiancybersecuritymagazine.com.au/russian-threat-actor-targeting-windows-print-spooler-vulnerability/
- https://www.tenable.com/blog/cve-2024-3400-zero-day-vulnerability-in-palo-alto-networks-pan-os-globalprotect-gateway
- https://teamt5.org/en/posts/alerts-of-exploiting-adobe-cold-fusion-cve-2023-29300/
- 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/
- https://fortifydata.com/blog/cve-2019-1653-cve-2019-1652-cve-2021-40539-cve-2021-27860-volt-typhoon/
- https://www.mandiant.com/resources/blog/initial-access-brokers-exploit-f5-screenconnect
- https://cybersixgill.com/news/articles/cve-2024-24919-vulnerability
- https://phoenix.security/jet-brain-cicd-vulnerability/

OUR INVESTORS

BLACKBIRD · KING RIVER · Xoogler.co · Singtel innov8 · Aditya Birla Bizlabs · Summit Peak · Y · Spider Capital

CYBLE®

About Cyble

Cyble (YC W21) is a leading global cyber intelligence firm that helps organizations manage cyber risks by utilizing patent-pending AI-powered threat intelligence. With a focus on gathering intelligence from the deep, dark, and surface web, the company has quickly established itself as one of the pioneers in the space. Cyble has received recognition from Forbes and other esteemed organizations for its cutting-edge threat research.

The company is well-known for its contributions to the cybersecurity community and has been recognized by organizations such as Facebook, Cisco, and the US Government. To learn more about Cyble, visit www.cyble.com

contact@cyble.com I +1 888 673 2067

11175 Cicero Drive Suite, 100 Alpharetta, GA 30022, US.