Ontinue

JANUARY – JUNE 2024

1H 2024 Threat Intelligence Report

Executive Summary

In the 1H 2024 Threat Intelligence Report, Ontinue's Advanced Threat Operations (ATO) team provides analysis of the evolving cyber threat landscape, emphasizing proactive threat identification, analysis, and mitigation strategies that empower our customers to build resilience against emerging threats.

The report found that despite patches being available, older vulnerabilities remain heavily exploited, with 50% of the top 10 trending vulnerabilities in early 2024 originating in 2023. Lockbit remains the most active ransomware group, while new players like Hunters International pose significant threats. The Manufacturing & Industrial sector has seen a surge in attacks, while the Technology/IT services sector has experienced a decline due to improved cyber defenses.

The ATO also spotlights the rise of sophisticated phishing techniques using Microsoft-owned domains, the ongoing threat of Infostealers, and the persistent danger of the PlugX RAT, particularly in government agencies. Additionally, Chinese state-sponsored cyber operations are intensifying, with a focus on information control and the use of zero-day exploits. Ontinue emphasizes the importance of proactive measures, such as staying informed through advisories and enhancing cybersecurity maturity through best practices.

1H 2024 THREAT INTELLIGENCE REPORT

Cyber Trends to Watch

Most Exploited Vulnerabilities

Top 10 Trending Vulnerabilities Since January 2024

In Q1 alone, there were 8,967 published CVE records, with over 13,400 more awaiting publication. However, the most widely published vulnerabilities aren't always the ones most exploited.

Of the top 10 trending vulnerabilities, 5 originated in 2023, even though patches were available at the time of their disclosure. Threat actors **continue to target these vulnerabilities because they know many organizations are not consistently applying patches**.

At the start of 2024, we witnessed a surge in zero-day vulnerabilities affecting Ivanti products, with 3 of them still actively exploited today. This highlights the critical importance for organizations to stay aware of the software and hardware they use, ensure timely patching, and subscribe to vendor security bulletins. Patching once a month or quarter is no longer sufficient to maintain adequate security.

1. **CVE-2023-36025**
   Windows SmartScreen Security Feature Bypass Vulnerability
2. **CVE-2024-21887**
   Command injection vulnerability in Ivanti Connect Secure and Policy Secure
3. **CVE-2024-3400**
   Command injection vulnerability in Palo Alto Networks PAN-OS software
4. **CVE-2023-6295**
   Exploited vulnerability with unknown parties in real-world attacks
5. **CVE-2023-51281**
   Cross-Site Scripting vulnerability in Customer Support System 1.0
6. **CVE-2023-31036**
   Directory Traversal vulnerability in NVIDIA Triton Inference Server
7. **CVE-2024-21412**
   Security feature bypass vulnerability in Microsoft Defender SmartScreen
8. **CVE-2023-7024**
   Zero-day vulnerability actively exploited in the wild
9. **CVE-2024-1709**
   Vulnerability being actively exploited in Ivanti Connect Secure
10. **CVE-2024-1708**
    Vulnerability being actively exploited in Ivanti Connect Secure.

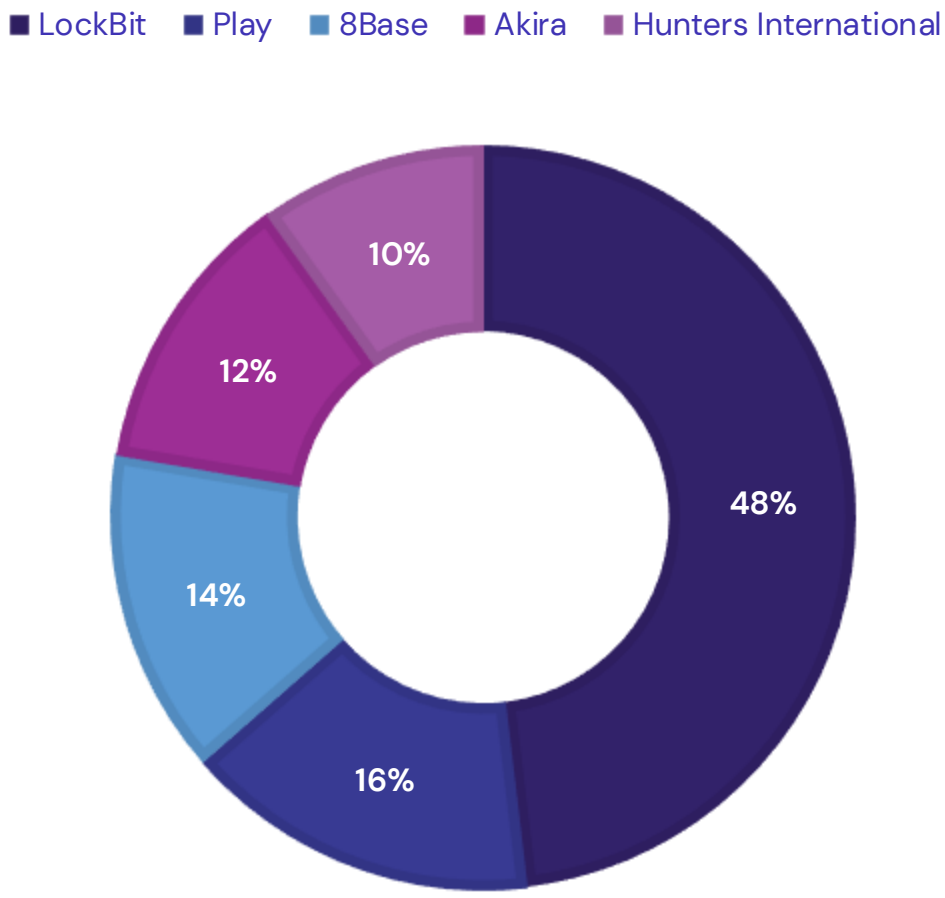
Source: Recorded Future

Most Active Ransomware Groups

Lockbit continues to dominate as the most active ransomware in 2024. Clop and AlphV have fallen from the top spots, replaced with Akira and newcomers Hunters International.

In the 2023 Ontinue Threat Intelligence Report, LockBit emerged as the most active ransomware group, engaging in numerous high-profile attacks throughout the year. With its "name and shame" technique, LockBit threatened to leak stolen data from its victims if the ransom demands were not met. Despite efforts from law enforcement and cybersecurity firms, LockBit maintains its position as one of the most active and dangerous ransomware groups.

It is expected that we will see the return of Clop in Q4 of 2024, fitting their pattern of working in bursts. Their last major success involved exploiting zero-day vulnerabilities in MOVEit, GoAnywhere, and Accellion file transfer software between July and November 2023.



Source: https://cybernews.com/ransomlooker/

Ransomware Group Profile

Hunters International

Origin

Domain registration for a Data Leak site, email and IP tracking points to the name OYEWOLE LAWRENCE and suggests Nigeria.

Industries Targeted

Global, healthcare, automotive, manufacturing, logistics, financial, educational, and food sectors, indicating a non-discriminatory approach aimed at exploiting any vulnerable entity

Motivators

Financial. Wide-ranging victimology underscores the group's opportunistic nature and its capacity to adapt and penetrate various sectors, posing a significant threat to organisations of all sizes and functions globally

Hunters International, a Ransomware-as-a-Service (RaaS) operation, emerged in late 2023 following the disruption of the HIVE ransomware group by law enforcement. It is speculated that this new operation may be run by the same individuals, **potentially making Hunters International a rebranded version of HIVE**.

An analysis of the malware revealed that the Hunters International encryptor shares 60% of its code with the HIVE version 6 ransomware strain. Despite this, Hunters International claims to be a new entity in the RaaS market, stating they purchased HIVE encryptors before HIVE's shutdown.

If a connection to HIVE exists, it is cause for concern. HIVE successfully extorted over 1,300 organizations and collected around $100 million in ransom payments.

Ransomware Profile: Hunters International

Detected Activity

Tactic	Technique
Execution	Native API (T1106), Shared Modules (T1129)
Persistence	Boot or Logon Autostart Execution (T1547.001)
Defence Evasion	Obfuscated Files or Information (T1027), Impair Defenses (T1562.001)
Discovery	Process Discovery (T1057), System Information Discovery (T1082), File and Directory Discovery (T1083)
Command and Control	Application Layer Protocol (T1071), Specifically Web Protocols (T1071.001)
Impact	Data Encrypted for Impact (T1486)

Detection of this ransomware activity is not limited to the ransomware itself. As defenders, we look to detect and prevent the precursors to a ransomware deployment. The following are a few detection and prevention rules in place for Hunters International related activity.

- Backdoor:Win32/SuspAadInternalsUsage
- Behavior:Win32/CobaltStrike
- Backdoor:Win64/CobaltStrike
- HackTool:Win64/CobaltStrike
- Trojan:Win32/Gozi
- Microsoft Defender Antivirus detects multiple variants of IcedID..
- Behavior:Win32/BlackCatExec
- Ransom:Win32/Blackcat
- DDoS:Win32/Blackcat
- TrojanDropper:Win32/Blackcat
- Ransom:Linux/BlackCat
- Behavior:Win32/BlackCat
- Ransom:Win64/BlackCat
- Behavior:Win64/Hunters
- Behavior:Win32/RansomHalt

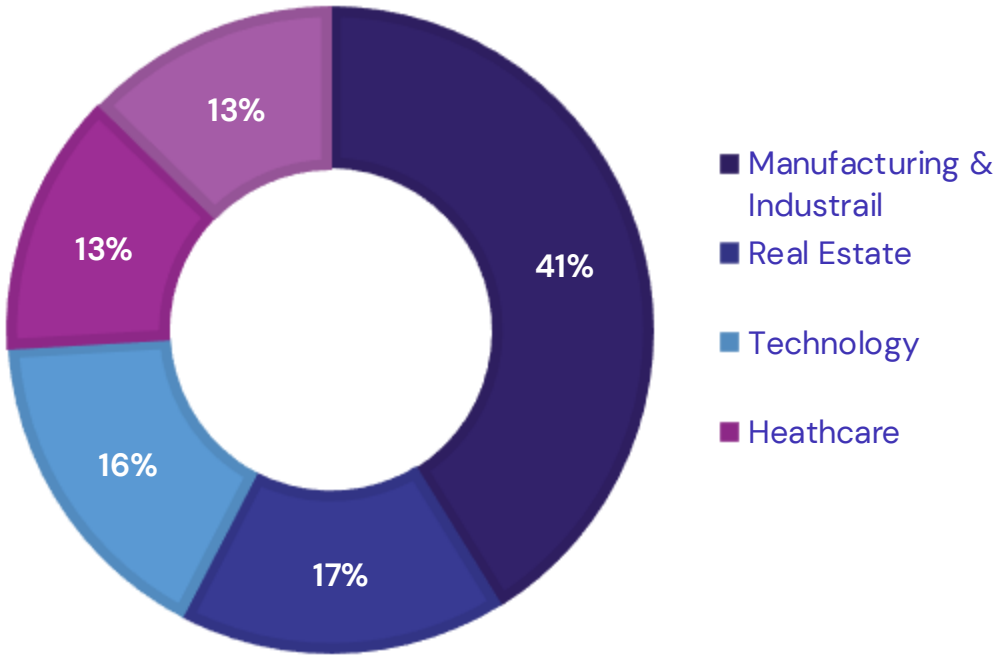
Note that some of these alerts have the names of other Threat groups, like Blackcat, as there is a lot of crossover for threat group TTPs.

Industries Most Targeted by Cyber Attacks

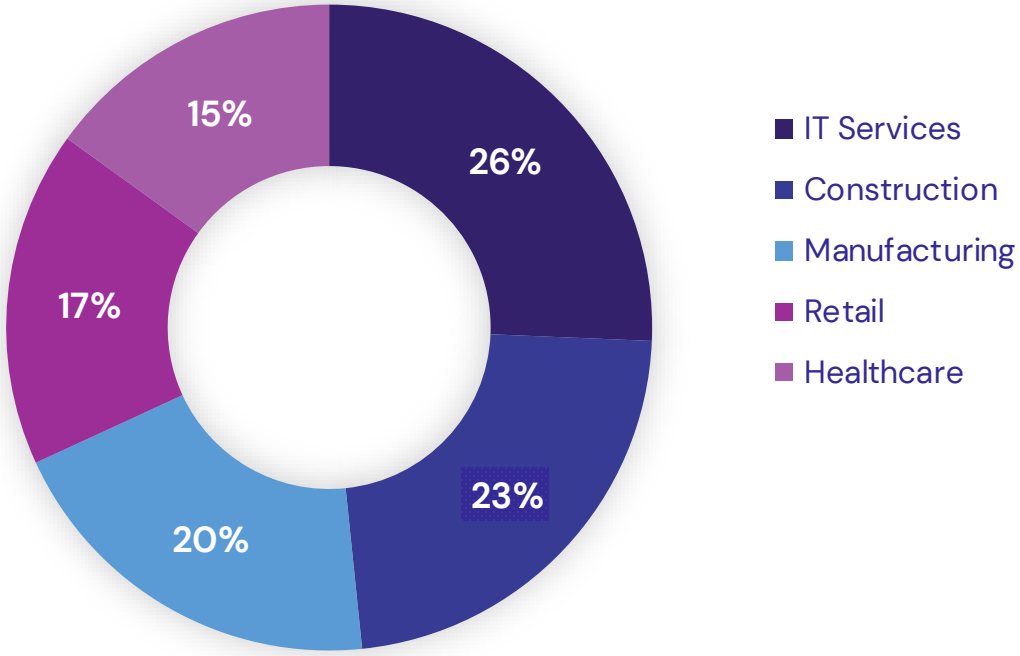
In 2024, the **Manufacturing & Industrial sector has emerged as the most targeted** industry, with its share of attacks rising from 20% in 2023 to 41% this year.

Interestingly, Technology/IT services have experienced a decline in attack volume. This decrease is likely due to IT organizations adopting more proactive approaches to patch management and cybersecurity defenses, resulting in a higher level of cyber maturity compared to other industries

JAN – JUN 2024



2023



Source: https://cybernews.com/ransomlooker/

Top observed MITRE ATT&CK techniques

True Positive detections in the ION platform

Honeytoken Authentication Activity	**Detection Type:** Triggered when a honeytoken, a decoy item placed in the system to detect unauthorized access, is accessed.
	MITRE ATT&CK Technique: T1589 - **Gather Victim Identity Information**. Honeytokens can detect when attackers are attempting to gather identity information.
User Accessed Link in ZAP-Quarantined Email	**Detection Type:** Raised when a user interacts with a link in an email that has been quarantined by the Zero-hour Auto Purge (ZAP) system.
	MITRE ATT&CK Technique: T1566.002 - **Spearphishing Link**. Clicking on malicious links in emails is a common phishing tactic.
A Suspicious File Was Observed	**Detection Type:** Identified when a file is suspicious based on unusual characteristics or behavior.
	MITRE ATT&CK Technique: T1203 - **Exploitation for Client Execution**. Suspicious files often exploit vulnerabilities to execute malicious code.
Possible PlugX Activity	**Detection Type:** Triggered by potential PlugX malware activity, used for data exfiltration and remote control.
	MITRE ATT&CK Technique: T1219 - **Remote Access Software**. PlugX is a type of remote access tool.
Connection to Adversary-in-the-Middle (AiTM) Phishing Site	**Detection Type:** Indicates a connection to a phishing site designed to intercept communications.
	MITRE ATT&CK Technique: T1557.002 - **Adversary-in-the-Middle**. Phishing sites can perform man-in-the-middle attacks.
Unfamiliar Sign-in Properties	**Detection Type:** Generated when sign-in attempts have properties not matching the user's typical behavior.
	MITRE ATT&CK Technique: T1078 - **Valid Accounts**. Unusual sign-in properties may indicate misuse of valid accounts.
AO-INA-AADIP-03: Correlate Unfamiliar Sign-in Properties and Atypical Travel Alerts	**Detection Type:** Correlation alert combining unfamiliar sign-in properties with atypical travel alerts.
	MITRE ATT&CK Technique: T1078 - **Valid Accounts**. This technique correlates to detecting misuse of valid accounts across different locations.
AO-INA-MDO-AADIP-01: Correlate Potentially Malicious URL Click and AADIP Alerts	**Detection Type:** Correlation alert linking malicious URL clicks with Azure Active Directory Identity Protection (AADIP) alerts.
	MITRE ATT&CK Technique: T1566.002 - **Spearphishing Link**. Clicking malicious URLs often precedes other malicious actions.
EX-INA-AAD-02: Possible AiTM Phishing Attempt Against Microsoft Entra ID	**Detection Type:** Indicates a possible adversary-in-the-middle phishing attempt targeting Microsoft Entra ID.
	MITRE ATT&CK Technique: T1557.002 - **Adversary-in-the-Middle**. Such phishing attempts aim to intercept authentication tokens.
Suspicious URL Clicked	**Detection Type:** Raised when a user clicks on a suspicious URL, indicating a potential phishing or malicious site visit.
	MITRE ATT&CK Technique: T1566.002 - **Spearphishing Link**. Clicking on suspicious URLs is a primary vector for spearphishing attacks.

1H 2024 THREAT INTELLIGENCE REPORT

Threat Spotlights

Threat Spotlight: LOLSites

Signed Microsoft Domains for Malicious Use

There has been a recent increase in the use of Microsoft-owned domains to bypass traditional security controls. This involves the use of powerappsportals[.]com, which hold a valid certificate, and allows an 'attacker-in-the-middle' techniques to steal users MFA codes.

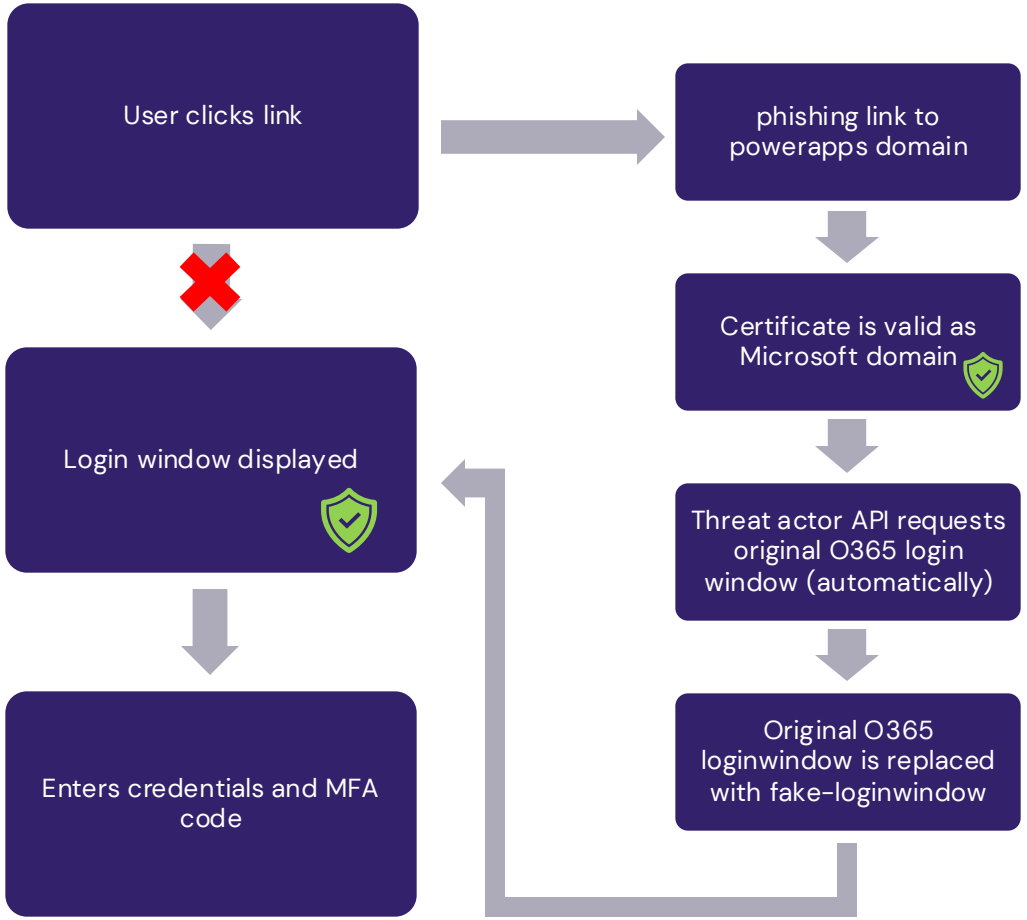
How does this work?

1. User receives phishing email with attachment
2. Attachment contains URL (powerappsportal) to imitation Microsoft login
3. Certificate is confirmed as legitimate (avoiding detection)
4. User enters username & password
5. MFA input is intercepted by threat actor
6. Threat actor now has all credentials harvested

Unlike a proxy variant, where the victim's MFA input is redirected or intercepted to an external server to harvest. Although the address bar contains the correct URL, the victim communicates with the wrong server (proxy), which inevitably leads to a certificate error and a possible alert or prevention.

Recommended actions

- Never enter a password or credit card number on a page you reached via a link in a message. It is most likely a phishing attempt.
- Check any website requesting your login credentials very carefully. Two-factor authentication does not protect you from real-time phishing.



Threat Spotlight: Phishing Via SharePoint

Using Compromised Accounts and SharePoint for Onward Phishing

Continuing the Microsoft Phishing trend, SharePoint has frequently been observed being used to redirect users to AiTM sites.

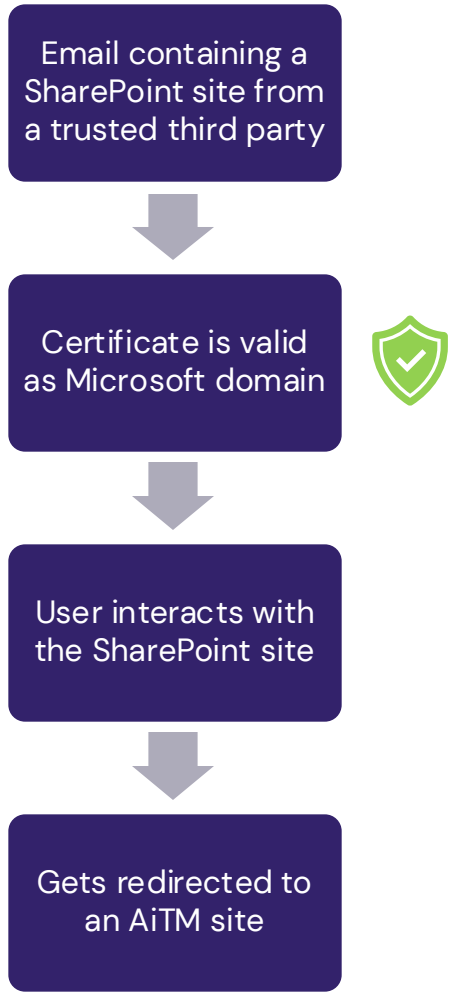
How does this work?

1. User is compromised from a previous AiTM attack
2. The actors create a SharePoint site using the compromised user which poses as a file sharing page which redirects to a credential harvester
3. The compromised user forwards the SharePoint site onto both internal and external users

This technique is highly effective because email defense mechanisms are less likely to flag SharePoint sites as suspicious, and users are more likely to trust the associated compromised sender. This increases the likelihood of interacting with the credential harvesting page.

Recommended actions

- Always treat SharePoint sites as suspicious even if they come from internal or trusted external users
- Don't hesitate to temporarily block senders and purge emails from trusted third parties should they be suspected of onward phishing your users



Threat Spotlight: Infostealers

Malware-as-a-Service (MaaS)

Infostealers are a type of malware commonly used by cybercriminals to gather credentials, financial data, or personal information. Often delivered via malvertising, phishing and droppers, the stolen data will then be exfiltrated to a C2 server. The MaaS model allows for their ease of distribution and use by a wide range of cybercriminals.

For example, Raccoon Stealer, sold on a subscription basis. Steals data including browser autofill passwords, history, and cookies, usernames, passwords, credit cards, and cryptocurrency wallets. This can be rented on underground forums for an average price of $75 per week.

Recommended Actions

- Use a Password Manager, but don't keep its password in your browser
- Update your browser regularly to protect against:
  - Java scripts in vulnerable browsers (malvertising) and 0-click infections
  - Unofficial/fake/malicious browser extensions
- Inspect incoming emails for malware and file macros
- Do not download pirated app versions
- Do not open suspicious files or click suspicious links
- Only download software from trusted sources

Threat Spotlight: PlugX

China-based RAT

PlugX remains a persistent threat, spreading through its USB worm variants by using innovative techniques to hide malicious files on infected USB devices, rendering them invisible to Windows-based systems. It creates a hidden directory named “RECYCLER BIN” to store stolen files before exfiltrating them via command and control (C2) channels. These C2 channels can also be utilized to execute commands remotely on an infected host. Additionally, once PlugX is active on a network, it continuously scans for more USB devices to infect, further propagating its presence.

Government agencies are the most common victims of PlugX attacks, with threat actors demonstrating a particular interest in military information, intelligence on foreign affairs and diplomatic activities.

Corporations in the private sector should still consider PlugX as an active threat.

Recommended actions

- Hash based blocking continues to be a great method of preventing PlugX from further spreading in environments due to its inability to create new files and therefore unique hashes. We have observed single block indicators preventing hundreds of further infections in customer environments.
- Build user awareness around the usage of USBs. Ideally, they shouldn't be used at all. Encourage users to share files using platforms like SharePoint, OneDrive or even via Teams and Outlook

1H 2024 THREAT INTELLIGENCE REPORT

Noteworthy News & Rising Threats

Noteworthy News: Disruption to Threat Groups

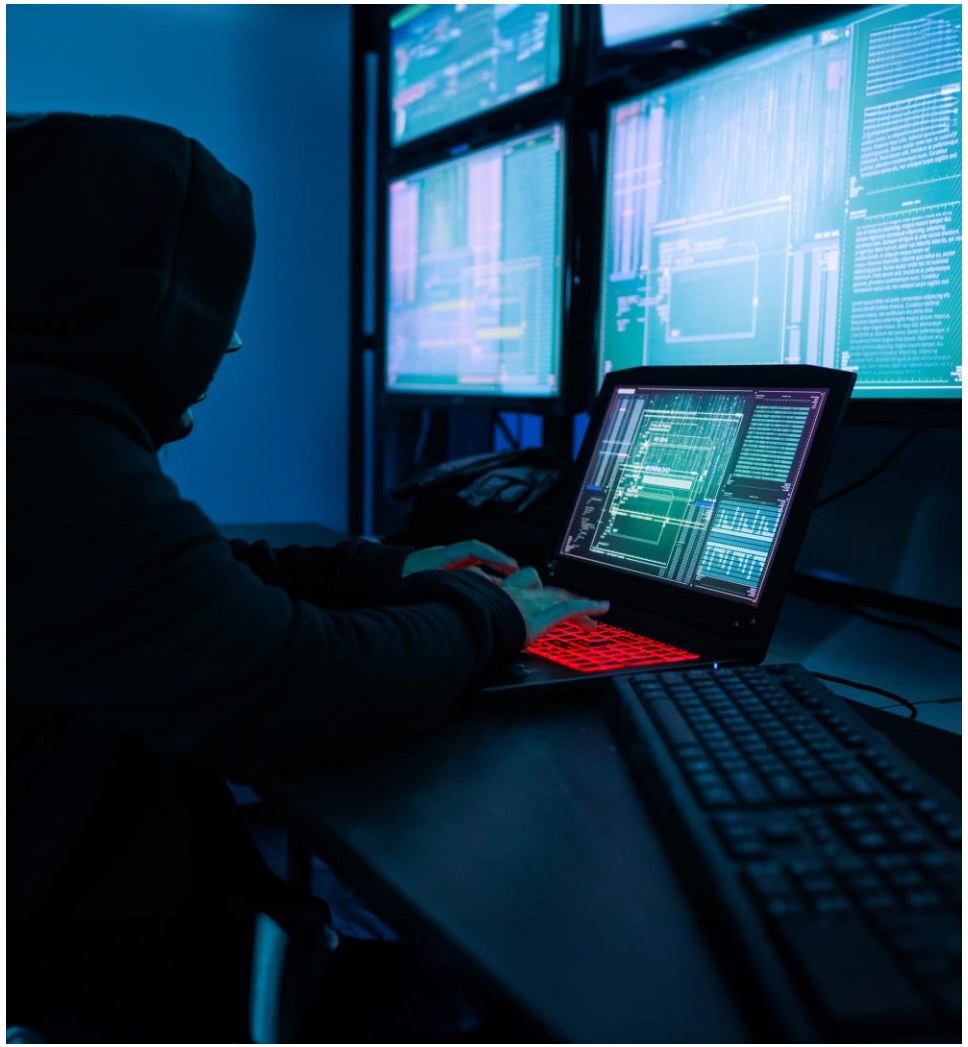
Lockbit Ransomware Group targeted by law enforcement

Recent operations by international law enforcement agencies have successfully disrupted the notorious LockBit ransomware group, one of the most active ransomware operators globally. This effort, led by the UK's National Crime Agency (NCA), the FBI, Europol, and various other international police agencies, was part of "Operation Cronos.". The takedown involved seizing LockBit's servers, arresting key members, and obtaining decryption keys to help victims recover their data without paying ransoms.

LockBit has been responsible for over 2,000 ransomware attacks since its emergence in late 2019, targeting organizations worldwide and extorting over $120 million in ransom payments. The disruption operation included the seizure of 34 servers across multiple countries and the arrest of several key members in Poland and Ukraine. Additionally, over 200 cryptocurrency wallets associated with the group were seized, potentially enabling victims to recover some of their payments.

The Justice Department has emphasized that this disruption is part of a broader strategy to dismantle the ecosystem supporting ransomware operations, prioritizing victim assistance and prevention. As part of these efforts, law enforcement has developed a decryption tool for LockBit 3.0, available through the "No More Ransom" portal, enabling victims to recover their encrypted files for free

This significant operation demonstrates the international commitment to combating ransomware and highlights the ongoing efforts to hold cybercriminals accountable, disrupt their activities, and provide relief to affected organizations



References:

Justice Department

The Record from Recorded Future

BleepingComputer

Noteworthy News: i-Soon leak

The Targeting of Defense Contracts

One of the most intriguing leaks this year has revealed deep affiliations between the i-Soon company and 32 state customers.

The leak sheds light on the potential role and capabilities of private companies in global cyber initiatives, including Advanced Persistent Threat (APT) operations-for-hire targeting both government and private sector entities worldwide. The i-Soon case alone involves approximately 100 alleged victims by name. The leaked information includes internal conversations between 37 users spanning four years.

Despite the mixed sophistication of i-Soon's tools and capabilities, the company has managed to execute large-scale, successful operations. This suggests that the cyber warfare industry is becoming increasingly organized.

Capabilities advertised

- Offensive toolkits against major platforms (MacOS, Win, Linux, Android, iOS)
- Automated Offensive Testing Platform (Vulnerability Scan aggregation)
- Maldoc and malicious payload generation
- Hardware 4G Router for hiding behind relay networks
- Victim e-mail analysis platform with text recognition
- DDoS as a service
- WiFi proximity attack system
- Social Media Monitoring of main platforms
- Public Opinion Guidance and Control System
- Mobile Implants and Hacking platform
- Cloud Intelligence Data Platform aggregating identity, communications, network, location and other data
- Cyber-range for training

The Rising Threat: Chinese State Sponsored Attacks

China has been undergoing its largest military and cyber reorganization, aiming to enhance its cyber military capabilities with a unique approach to cyberspace. Instead of focusing solely on controlling cyberspace, China is now prioritizing the control of information as a strategic focus for capability development. Multiple boutique intelligence firms and government analyses support this shift in direction

Recent changes indicate that China's cyber operations are becoming more prolific, particularly in discovering new vulnerabilities and developing zero-day exploits. The use and redistribution of these zero-days have become more streamlined across different entities for general-purpose use, maximizing their offensive value. Once these exploits are "burned"—discovered by victims and reported publicly—they are often repurposed by various military entities and, it is believed, by offensive contractors as well.

A recent report confirmed a significant shift that complicates attribution, as well as the distribution of Indicators of Compromise (IOCs) and Tactics, Techniques, and Procedures (TTPs). Cyber operations are no longer carried out by single actors using targeted botnets; instead, there are dedicated entities responsible for both managing and compromising or setting up attacker infrastructure. These infrastructures are either provisioned—frequently reused by several APT entities in short, two-week cycles at reputable ISPs and VPS providers globally—or non-provisioned, built on compromised civil infrastructure with a large number of nodes, similar to TOR.

These complex networks, which are rapidly shuffled, make tracking and attribution much more difficult. The multi-layered approach also complicates uncovering adversary-controlled operational servers beyond exit nodes, staging nodes, and relays. Different groups within this framework have specific goals and targets, often leading to a broader wave of exploitation following the initial discovery. This environment elevates the importance of emergency patching as a critical defensive tactic for organizations.

This playbook has been repeatedly observed over the past year, with high volumes of attacks against several brands and network equipment used as initial entry points. Analysts report that attribution becomes increasingly difficult after the initial discovery.

Contractors, many of whom have documented relationships through leaked contracts or marketing materials related to offensive capabilities, are playing a more significant role in various aspects, including malware and exploit development.

Recent scandals have surfaced involving public sector contractors, such as an email and WeChat leak at China Far East International Tendering, which led to the termination of assumed relations with the People's Liberation Army. Another infamous and revealing leak came from i-Soon, providing valuable operational intelligence.

1H 2024 THREAT INTELLIGENCE REPORT

Stay Ahead of Threats

Be Proactive: The Importance of Advisories

Staying Ahead of New and Emerging Threats

Partnering with a managed security provider offers the benefit of expert guidance, advanced threat detection, and 24/7 monitoring, ensuring your organization is equipped to respond swiftly to evolving cyber threats.

At Ontinue, we provide advanced security solutions, as well as the knowledge and tools organizations require to manage their security landscape. By handling day-to-day security operations and providing continuous peace of mind, we allow organizations to focus on driving their business forward and getting more time back in their days.

While we do our part, your organization must also stay proactive. It is crucial to stay informed about emerging threats, read advisories, and implement the necessary protocols and patches.

Our team keep customers ahead of new, relevant, high-risk vulnerabilities that might impact their environment by publishing regular Threat Advisories that detail potential risk. In the first half of 2024, our team has published 20 Threat Advisories.

When a new threat is on the horizon, these threat advisories can provide instant and actionable intelligence, helping protect against the next threat or addressing newly discovered vulnerabilities. Below is an example of some of the threat advisories we share, often ahead of publicly available information.

The following is an example of some of the threat advisories we share, often ahead of the publicly available information.

- Regular Monthly Microsoft Patch Tuesday
- VMware ESXi Hypervisor Vulnerability CVE-2024-37085
- OilAlpha Malicious Android Apps Target Humanitarian Aid Groups
- RegreSSHion SSH Vulnerability
- TeamViewer Compromise
- CVE-2024-30103 in Microsoft Outlook
- SessionLifeTimePolicy expiry
- PowerApps Domain AitM
- CVE-2024-3400 Unauthenticated RCE in Palo Alto GlobalProtect
- JetBrains TeamCity - CVE-2024-27198 and CVE-2024-27199
- ConnectWise ScreenConnect Authentication Bypass
- Exploited vulnerabilities Fortinet, Google, Roundcube
- AnyDesk Cyber Attack
- CVE-2023-46805 (Authentication Bypass) & CVE-2024-21887 (Command Injection) for Ivanti Connect Secure and Ivanti Policy Secure Gateways
- Citrix, Chrome, Ivanti, VMware & Laravel actively exploited
- CVE-2024-23897 Critical Jenkins RCE Flaw
- Midnight Blizzard attack on Microsoft corporate systems
- CVE-2023-22527 RCE Vulnerability In Confluence Data Centre and Confluence Server
- Plus, regular updates on actively exploited and Trending Vulnerabilities with reference to CISA KEVC

Be Proactive: Strengthen Your Cyber Posture

Best Practices to Prevent Business Disruption

The following are cybersecurity best practices to help organizations harden their security postures to reduce the risk of cyber threats and data breaches.

1. **Stay Up-to-Date on Patch Management**
   Ensure patches are applied as soon as they are released, especially for critical vulnerabilities. Threat actors are exploiting known vulnerabilities because organizations delay patching.
2. **Implement Multi-Factor Authentication with Caution**
   While MFA is essential, ensure it is properly configured to avoid real-time phishing attacks that intercept MFA codes. Educate users on recognizing legitimate vs. phishing MFA prompts.
3. **Employee Training and Awareness**
   Create a culture where security is top-of-mind. Conduct ongoing training about phishing, social engineering, and safe internet usage. Adopt a secure password manager, ensure browsers are updated, and inspect emails for suspicious files or macros to prevent Infostealer malware infections. Limit or disable USB usage to prevent malware like PlugX from spreading through USB devices. Encourage cloud-based file sharing via platforms such as SharePoint or OneDrive instead.
4. **Strengthen Ransomware Defenses with Regular Backups and Planning**
   Regularly back up critical data, ensuring these backups are offline and not susceptible to ransomware encryption. Isolate critical systems to limit ransomware spread. A breach in one part of the network should not lead to full-scale compromise. Additionally, develop and test an incident response plan specifically for ransomware attacks to minimize downtime.
5. **Network Segmentation**
   Segment your network to isolate critical systems and sensitive data, limiting the potential impact of a security breach. Implement network monitoring tools to detect and respond to suspicious activity in real-time. Monitor network traffic, user behavior, and system logs for signs of unauthorized access or malicious activity.
6. **Develop an Incident Response Plan, Now.**
   Develop and test an incident response plan specifically for ransomware attacks to minimize downtime. Partner with a managed security provider like Ontinue for real-time threat intelligence, advisories, and continuous monitoring. Regularly review threat advisories to adapt defenses as new threats arise, such as the rise of Chinese state-sponsored cyber operations.

References

List of sources etc.

https://www.justice.gov/opa/pr/us-and-uk-disrupt-lockbit-ransomware-variant
The Record from https://therecord.media/lockbit-ransomware-disrupted-international-operation Future
https://www.bleepingcomputer.com/news/security/police-arrest-lockbit-ransomware-members-release-decryptor-in-global-crackdown/
https://cybernews.com/ransomlooker/
https://www.helpnetsecurity.com/2024/03/07/2024-x-force-threat-intelligence-index-video/
https://thehackernews.com/2024/07/microsoft-defender-flaw-exploited-to.html
https://www.japantimes.co.jp/news/2024/04/21/asia-pacific/politics/china-military-reorganization/
https://asia.nikkei.com/Politics/Defense/China-military-s-biggest-shakeup-in-9-years-adds-info-cyber-space-units
https://www.scmp.com/news/china/military/article/3255255/chinas-military-disqualifies-procurement-company-serious-risks-leaked-secrets
https://harfanglab.io/en/insidethelab/isoon-leak-analysis/

Special thanks to William Bailey, ION Senior SOC Analyst, for his contributions


Ontinue
Nonstop SecOps