CYBLE®

REPORT

U.S. Threat Landscape Report:

A Time of Growing Peril

Table of **Contents**

Overview: A Time of Growing Peril

Perhaps the most noteworthy development in the cyber threat intelligence landscape in October 2024 was the brazen interference in the U.S. presidential election by Russia, China and Iran, as nation-state actors linked to those countries all but abandoned attempts to disguise their influence and cyber operations as the election entered its final days.

The response by the incoming Trump Administration will be important for all organizations.

With the sophistication of financially motivated threat actors increasingly approaching that of nation-state actors, due in part to the misuse of AI and the availability of exploits on the dark web, security teams and the CISOs who lead them have never been more under siege, or more in need of comprehensive cybersecurity.

Here are some of the major trends to watch before we delve into the specifics of the changing threat landscape.

Disinformation – particularly by Russia-linked actors – escalated significantly in the final weeks of the U.S. election and was likely a factor in persuading a large share of pro-Palestinian voters to abandon the Democratic party. The main foreign actors involved in influence campaigns – notably Russia, China and Iran – will likely continue efforts to amplify divisive content after witnessing recent successes undermining faith in democratic systems in the U.S. and elsewhere.

Nation-State Threats reached a new level of concern when China-linked threat actors successfully infiltrated U.S. telecom systems to access wiretap data and the phone data of top U.S. officials. As China is believed to have significantly infiltrated critical infrastructure in the U.S. and elsewhere, national cyber agencies must do more to detect and remove these threats.

AI in Social Engineering has reached a point of sophistication where Cyble has added AI deepfake detection and takedown to its threat intelligence suite. The proliferation of AI technology is enhancing the effectiveness of social engineering attacks, enabling more personalized and convincing tactics that have scammed average citizens as well as multi-national corporations.

Dark Web and Cybercrime activity remains a major threat, as exploits are under discussion on dark web forums within hours after vulnerabilities are publicly revealed, and zero-day vulnerabilities can frequently be found for sale on these forums.

Healthcare remains a prime target, particularly for ransomware groups, while **OT/ICS environments** continue to be heavily targeted by threat actors, with Manufacturing, Energy, Oil and Gas, and Building Automation the leading targets detected by Cyble.

Ransomware remains a scourge, but data exfiltration is increasingly a goal of ransomware groups.

Infostealers continue to grow in frequency and sophistication, threatening the accounts and credentials of both enterprises and consumers.

This report covers the most active threat and hacktivist groups and malware families in October 2024, Dark Web and cybercrime trends, the most exploited IT and critical infrastructure vulnerabilities, notable cyber incidents shaping the threat landscape, and recommendations for security teams.

The Most Active Threat Groups in October

Cyble threat intelligence data identified these 14 threat groups as the most active in October. Ransomware groups were the most active during the month, followed by cybercrime groups, but nation-state groups and hacktivists were active in threat campaigns too.

Name	Aliases	Categories	Used Malware Families
RansomHub	Water Bakunawa	Ransomware Group	RansomHub
DragonForce		Ransomware Group	
LockBit Gang	Bitwise Spider	Ransomware Group	3AM, CrackMapExec, EmpireProject, LockBit, Mimikatz, PsExec
Storm-0501		Ransomware Group	BlackCat, LockBit, Cobalt Strike, Embargo
UNC5812		APT	
Cicada3301		Ransomware Group	
Cyber Operation Alliance	C.O.A Agency , COA	Hacktivist Group	
Dark Angels		Ransomware Group	Babuk, RTM Locker, RagnarLocker
0xy0um0m	Nick Diesel	Cybercriminal Group	
ZeroSevenGroup	ZeroSevenG	Cybercriminal Group	
Water Makra		Cybercriminal Group	Astaroth
Awaken Likho	Core Werewolf	APT	
Storm-1567	Akira, GOLD SAHARA, PUNK SPIDER	Ransomware Group, APT	Akira, PsExec, Mimikatz, AdFind, SharpHound, SoftPerfect Network Scanner, AnyDesk, RustDesk, Impacket, Ngrok, FileZilla, WinSCP
Key Group		Hacktivist, Ransomware	Xorist, Chaos, RURansom, Slam, njRAT

Note: The appendix includes a table detailing the 52 most active malware families in October.

Notable Cyber Attacks

Here are ten notable cyber attacks and campaigns that occurred in October; we cover more in the Ransomware section below.

The non-profit Internet Archive and Open Library was hit by multiple cyber attacks by different actors, including DDoS, website defacement, data breach and exfiltration. While the non-profit clearly had inadequate security, the threat actors in this case were criticized apparently even within their own channels for attacking a group whose purpose is to provide "universal access to all knowledge."

The Boston Children's Health Network suffered a data breach and exfiltration attack by the BianLian threat group. It's not clear if ransomware was involved, but the attack occurred via an IT vendor's systems and compromised sensitive data of patients, employees and guarantors.

Cyble researchers identified a sophisticated cyberespionage campaign dubbed "HeptaX" that uses a multi-stage attack that leverages LNK files, RDP and PowerShell and BAT scripts. Cyble also identified a threat campaign that uses Visual Studio Code (VSCode) to gain unauthorized remote access, and a sophisticated loader and obfuscation tool.

ADT, a prominent security system provider for homes and small businesses, suffered its second cyber attack in as many months.

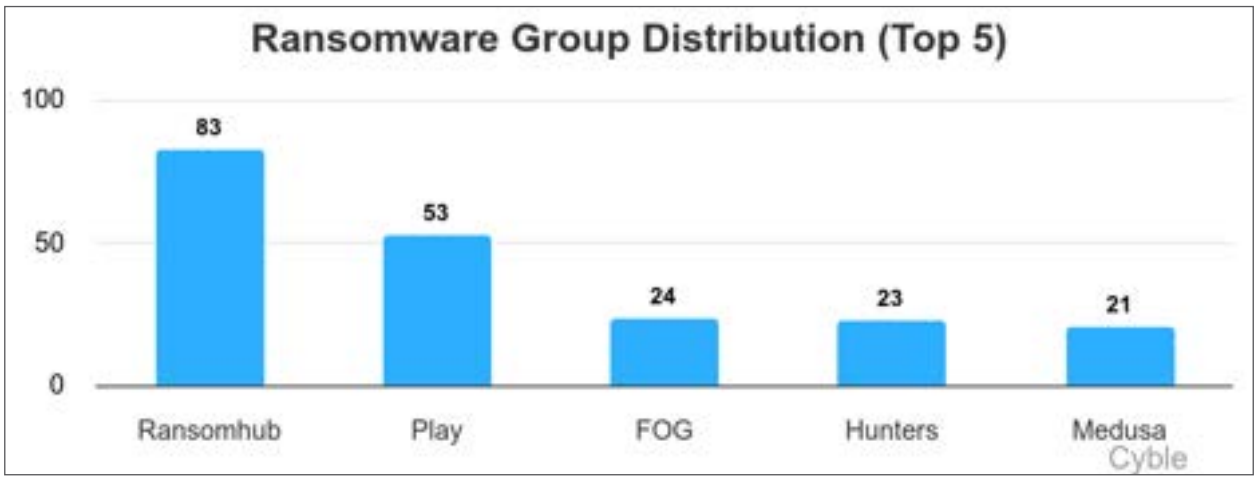
American Water Works was hit by a cyber attack that fortunately did not reach OT systems.

Cryptocurrency remains a popular target for hackers, with EigenLayer and Radiant Capital suffering huge losses.

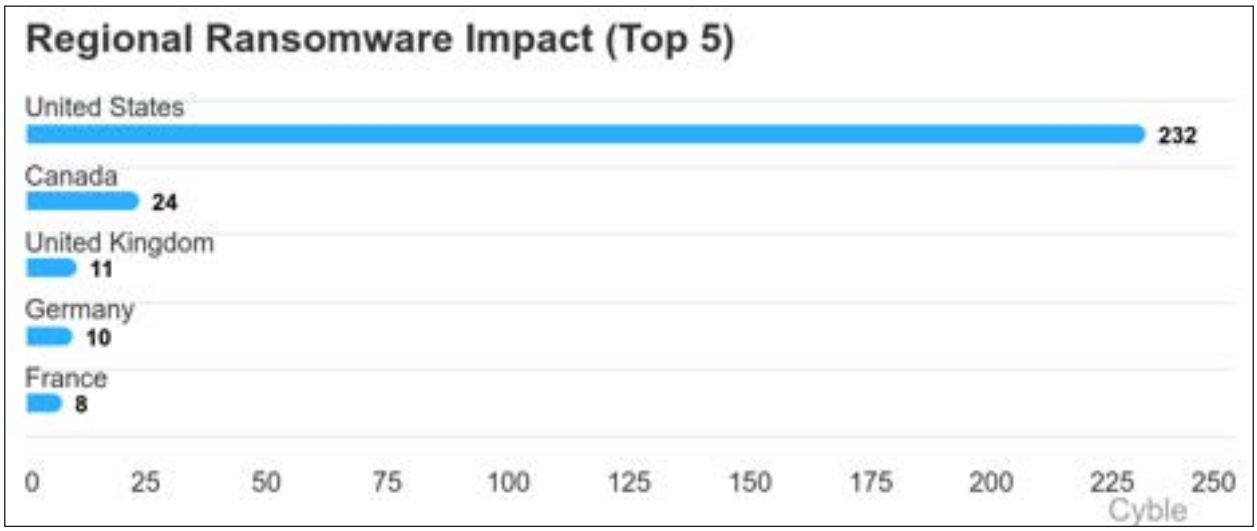
And a long-running data breach that affected some of Italy's top politicians and leaders became public in a massive scandal.

Ransomware Actors and Targets

RansomHub was again the top ransomware group, as LockBit continues to regroup following recent international enforcement actions. Here were the top five ransomware groups in October:



The U.S. remains overwhelmingly the top target for ransomware attacks, with attack volumes ten to twenty times greater than the next countries on the list:



Some notable organizations hit by ransomware groups in October include:

- Volkswagen Group
- Texas Tech Health Sciences Center
- Aspen Healthcare Services
- Boston Children's Health Physicians

Hacktivism

Hacktivist activity remained strong in advance of the U.S. election, as Cyble detected more than 14,000 records and 700 site defacements related to hacktivism in October. Global hotspots and the U.S. were the most frequently cited regions, with Israel taking the top spot:

Region and number of hacktivist mentions

Hacktivism activity ranged from cyber attacks and site defacements to advocacy and propaganda. These groups may target many of the same known web vulnerabilities as other hackers. Notable actors include:

XYZ/Alpha Wolf
Key Group
NoName
Cyber Operation Alliance
Anon Black Flag
Tiger
Fatality
!Y4n
K3T0PR4K
Ethersec Team Cyber
Zalcyber/Eagle Error System
Inside Alone7
Ghost Princess

Dark Web and Cybercrime Forum Activity

The dark web has become something of a democratizing force in the world of cybercrime, giving less experienced threat actors and hacktivists access to more sophisticated exploits, in addition to leaked files, credentials, stolen credit cards, compromised endpoints, and more.

Cyble dark web researchers typically see ten or more vulnerability exploits discussed each week on cybercrime forums, many with available proof of concept (PoC) exploits that can be easily deployed. Many of those are the basis for the next section of this report on IT vulnerabilities.

Below are the dark web data points detected by Cyble for October, including 1.5 million data exposures, 48,000 compromised endpoints, and 178,000 leaked credentials, all widely available for a price.

There was a great deal of discussion of the U.S. election on Telegram and other dark web forums, much of it focused on perceived election fraud in the U.S. leading up to the election – largely echoing Trump's own rhetoric – and preparing for the possibility of violence.

The Most Exploited IT Vulnerabilities in October

Here are 34 of the most exploited and at-risk IT vulnerabilities for the month of October, as assessed by Cyble vulnerability intelligence researchers.

CVE-2024-40766 is a 9.8-severity improper access control vulnerability in the administrative interface and controls in the SonicOS operating system used for managing SonicWall's network security appliances and firewalls.

Fortinet environments were under attack from threat actors exploiting a pair of 9.8-severity vulnerabilities: **CVE-2024-47575**, also known as "FortiJump," is a vulnerability in Fortinet FortiManager that allows an attacker to execute arbitrary code or commands via specially crafted requests; and **CVE-2024-23113** is a critical vulnerability in multiple versions of FortiOS, FortiProxy, FortiPAM, and FortiSwitchManager that allows remote, unauthenticated attackers to execute arbitrary code through specially crafted requests.

CVE-2024-44000 is an Insufficiently Protected Credentials vulnerability in LiteSpeed Cache that allows Authentication Bypass and could potentially lead to account takeover. The issue affects versions of the WordPress site performance and optimization plugin before 6.5.0.1.

The GutenKit Page Builder Blocks, Patterns, and Templates for Gutenberg Block Editor plugin for WordPress is vulnerable to **CVE-2024-9234**, with arbitrary file uploads possible due to a missing capability check.

CVE-2024-9264 is a 9.4-severity vulnerability in the SQL Expressions experimental feature of Grafana, an open-source analytics and monitoring platform developed by Grafana Labs.

CVE-2024-51567 and **CVE-2024-51568** are critical vulnerabilities in CyberPanel, an open-source web hosting control panel designed to simplify server management, particularly for those using the LiteSpeed web server.

CVE-2024-46483 is a critical integer overflow vulnerability in Xlight FTP Server, a high-performance file transfer server for Windows designed to facilitate secure and efficient FTP and SFTP (SSH2) file transfers.

CVE-2024-9463, CVE-2024-9464, CVE-2024-9465, CVE-2024-9466, CVE-2024-9467: These vulnerabilities – the first of which carries a 9.9 severity rating – impact Palo Alto Networks Expedition, a migration tool designed to facilitate the transition of network configurations from various vendors to Palo Alto Networks PAN-OS. The flaws can be chained to let attackers hijack PAN-OS firewalls and exploits are being discussed on the dark web. CVE-2024-9463 and CVE-2024-9464 are OS command injection vulnerabilities allowing an unauthenticated attacker to run arbitrary OS commands as root in Expedition.

CVE-2024-42640 is a critical vulnerability affecting the angular-base64-upload library, specifically in versions prior to v0.1.21. This vulnerability allows remote code execution (RCE) through the demo/server.php endpoint, enabling attackers to upload arbitrary files to the server.

CVE-2024-46538 is a critical cross-site scripting (XSS) vulnerability in pfSense version 2.5.2 allows attackers to execute arbitrary web scripts or HTML by injecting a 'crafted payload' into the $pconfig variable, specifically through the 'interfaces_groups_edit.php' file.

CVE-2024-8963 is a critical admin bypass vulnerability in Ivanti Cloud Services Appliance (CSA), and could be exploited by chaining CVE-2024-8963 with CVE-2024-8190 to bypass admin authentication and execute arbitrary commands on unpatched appliances. Cyble researchers also issued a separate advisory on a vulnerability (CVE-2024-7593) in Ivanti's Virtual Traffic Manager (VTM).

Microsoft's October 2024 Patch Tuesday included security updates for 118 flaws, including five publicly disclosed zero-days, two of which are being actively exploited: **CVE-2024-43572**, a Remote Code Execution vulnerability in Windows Management Console, and **CVE-2024-43573**, a spoofing vulnerability in the Windows MSHTML Platform.

CVE-2024-30088 is a high-severity privilege escalation vulnerability in Windows that enables attackers to escalate their privileges to the SYSTEM level, giving them significant control over compromised devices.

CVE-2024-38178 is a high-severity type confusion vulnerability that impacts Internet Explorer and is being used by threat actors to perform zero-click malware infections.

CVE-2024-30052 is a remote code execution (RCE) vulnerability affecting Microsoft Visual Studio, particularly versions 2022 prior to 17.8.11 and certain configurations of Visual Studio 2019.

CVE-2024-7479 and **CVE-2024-7481** are critical vulnerabilities affecting TeamViewer's Remote Client and Remote Host products for Windows and arise from improper verification of cryptographic signatures, allowing for privilege escalation and arbitrary code execution.

CVE-2024-6769 affects multiple versions of Microsoft Windows, including Windows 10, Windows 11, and various Windows Server editions. It exploits a combination of DLL Hijacking and Activation Cache Poisoning, allowing an attacker to elevate privileges from a medium to a high-integrity process without triggering a User Account Control (UAC) prompt.

CVE-2024-45409 is a critical SAML authentication bypass vulnerability impacting self-managed installations of the GitLab Community Edition (CE) and Enterprise Edition (EE).

CVE-2024-9164 is a critical vulnerability in GitLab Enterprise Edition (EE) that allows unauthorized users to trigger Continuous Integration/Continuous Delivery (CI/CD) pipelines on any branch of a repository.

CVE-2024-7490 is a critical improper input validation vulnerability in Microchip Technology Advanced Software Framework, a comprehensive library designed for microcontrollers, facilitating various stages of product development, including evaluation, prototyping, design, and production. The vulnerability can cause remote code execution through a buffer overflow.

CVE-2024-46740 is a high-severity Use-After-Free (UAF) vulnerability in the Linux Kernel. It is specifically related to the binder subsystem.

CVE-2024-40711 is a critical deserialization of untrusted data vulnerability in Veeam Backup & Replication (VBR) that can lead to unauthenticated remote code execution (RCE). Akira and Fog ransomware groups are exploiting the vulnerability to gain RCE on vulnerable servers.

CVE-2024-20439 is a critical security vulnerability affecting the Cisco Smart Licensing Utility, which could allow unauthenticated, remote attackers to gain administrative access to the system.

CVE-2024-20353 is a critical vulnerability identified in Cisco's Adaptive Security Appliance (ASA) and Firepower Threat Defense (FTD) software that allows for a Denial-of-Service (DoS) attack.

CVE-2024-28987 affects the SolarWinds Web Help Desk (WHD) software, specifically version 12.8.3 HF1 and all earlier versions. This vulnerability is classified as critical, with a CVSS score of 9.1. It allows remote, unauthenticated users to access internal functionalities and modify data due to hardcoded credentials in the software.

CVE-2024-38816 is a high-severity Path Traversal vulnerability in the popular Spring Java framework. Applications serving static resources through the functional web frameworks WebMvc.fn or WebFlux.fn are vulnerable to path traversal attacks.

The Most Exploited ICS Vulnerabilities

Cyble identified a number of high-risk vulnerabilities in industrial control systems (ICS) that security teams in those environments should prioritize.

CVE-2024-7587 is an incorrect default permissions vulnerability in the ICONICS Suite, including products like GENESIS64 and Hyper Historian, that poses a high-severity risk to control systems such as DCS, SCADA, and BMS.

CVE-2024-9692 is an improper access control vulnerability in the Blue Plus Transmitter from VIMESA impacting communication units and transmitters.

CVE-2024-10313 is a path traversal vulnerability in the SpiderControl HMI Editor from iniNet Solutions. The vulnerability is classified as high severity and affects human-machine interface systems.

CVE-2024-5947 is a missing authentication vulnerability affecting DSE855 communications devices from Deep Sea Electronics.

CVE-2024-3506 is a classic buffer overflow vulnerability in Siemens' Siveillance Video Camera, with all versions prior to V13.2 vulnerable, impacting physical access control systems and CCTV.

CVE-2023-8531 is a high-severity improper verification of cryptographic signatures vulnerability in Schneider Electric's Data Center Expert, specifically versions 8.1.1.3 and prior, affecting control systems such as DCS, SCADA, and BMS.

CVE-2024-49396 and **CVE-2024-49398** are insufficiently protected credentials and unrestricted upload of files with dangerous types vulnerabilities in Elvaco's CMe3100, version 1.12.1, posing risks to gateway and remote access systems.

CVE-2024-41717 is a critical path traversal vulnerability in Kieback&Peter's DDC4002 and related versions, impacting field controllers and IoT devices.

CVE-2024-41987 and **CVE-2024-41988** are missing authentication for critical function and cross-site request forgery (CSRF) vulnerabilities in Opera Plus FM Family Transmitters.

CVE-2024-0727 is a NULL pointer dereference vulnerability in Mitsubishi Electric's MELSEC iQ-F FX5-OPC communication units that could be used by malicious actors to create denial-of-service (DoS) conditions by getting a legitimate user to import a specially crafted PKCS#12 format certificate. The issue is caused by an OpenSSL vulnerability.

CVE-2024-43699 and **CVE-2024-42417** are SQL injection vulnerabilities in Delta Electronics' DIAEnergie industrial energy management system that could allow an unauthenticated attacker to obtain records contained in the targeted product.

CVE-2024-41981 and **CVE-2024-47046**, found in multiple versions of Siemens' Simcenter Nastran software, are heap-based buffer overflow and improper memory buffer operations vulnerabilities with a high severity rating.

CVE-2024-41798 is a critical improper authentication vulnerability in Siemens' SENTRON 7KM PAC3200.

CVE-2024-47553 is a critical argument injection risk vulnerability in the SINEC Security Monitor from Siemens.

CVE-2024-7952 is a high-severity vulnerability in the Rockwell Automation DataMosaix Private Cloud that could lead to sensitive information exposure.

CVE-2024-47962 is a stack-based buffer overflow in Delta Electronics' CNCSoft-G2 software, classified as high severity.

Cyble Recommendations

To protect against vulnerabilities and exploits, Cyble recommends that organizations start with the following best practices:

- To mitigate vulnerabilities and protect against exploits, regularly update all software and hardware systems with the latest patches from official vendors.
- Develop a comprehensive patch management strategy that includes inventory management, patch assessment, testing, deployment, and verification. Automate the process where possible to ensure consistency and efficiency.
- Divide your network into distinct segments to isolate critical assets from less secure areas. Use firewalls, VLANs, and access controls to limit access and reduce the attack surface exposed to potential threats.
- Implement immutable, air-gapped, ransomware-resistant backup procedures for sensitive and critical data.
- Create and maintain an incident response plan that outlines procedures for detecting, responding to, and recovering from security incidents. Regularly test and update the plan to ensure its effectiveness and alignment with current threats.
- Implement comprehensive monitoring and logging solutions to detect and analyze suspicious activities. Use SIEM (Security Information and Event Management) systems to aggregate and correlate logs for real-time threat detection and response.
- Subscribe to security advisories and alerts from official vendors, CERTs, and other authoritative sources. Regularly review and assess the impact of these alerts on your systems and take appropriate actions.
- Conduct regular vulnerability assessment and penetration testing (VAPT) exercises to identify and remediate vulnerabilities in your systems. Complement these exercises with periodic security audits to ensure compliance with security policies and standards.

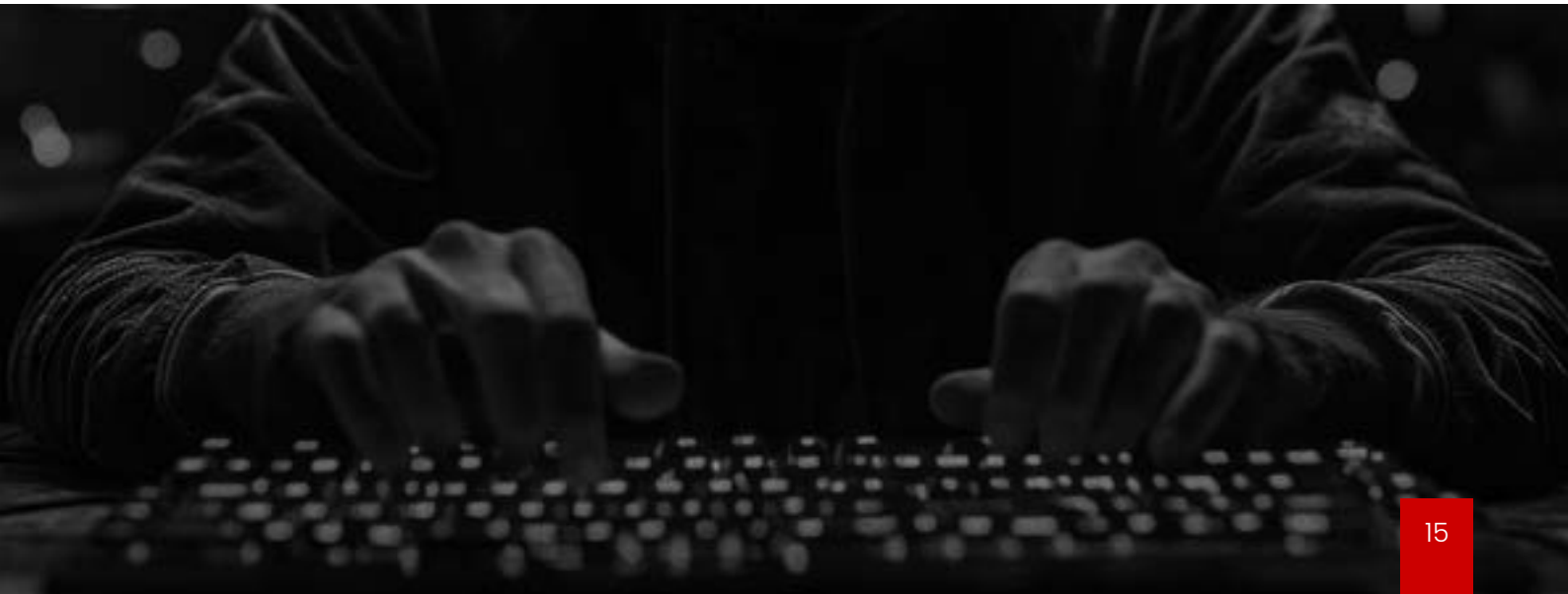
Appendix: Top 52 Malware Families October 2024

Name	Aliases & Related Threat Actors	Types
Hydra	BianLian	Ransomware
Lynx		Ransomware, Malware
Nitro	Hydra	Ransomware
RansomHub		Ransomware
Rhysida		Ransomware, Malware
Hellcat Ransomware		Malware, Ransomware
Cactus		Ransomware
Everest		Ransomware, Malware
Medusa	Gorgona	Ransomware
Interlock		Ransomware, Malware
PLAY	PlayCrypt	Ransomware, Malware
HellDown		Ransomware
SteelFox		
winos4		Malware, Info stealer
AgendaCrypt	Agenda, Qilin	Ransomware, Malware
Embargo	Storm-0501	Ransomware, Malware
BianLian Ransomware		Malware, Ransomware
Hunters International		
Pygmy Goat		Malware, Backdoor
BlackSuit		Ransomware
LockBit	ABCD Ransomware, Syrphid, Storm-0501	Ransomware, Malware, Remote command
SYS01		Malware, Credential stealer
Black Basta	no_name_software	Ransomware, Malware
CloudScout	Evasive Panda	Malware, RAT
Clop	Cl0p, Carbanak, FIN11, TA505	Ransomware, Big Game Hunting
SRBMiner		Tools, Miner
Monti		Ransomware
Bear C2		Tools, C2
Gophish		
PowerRAT		Malware, RAT

DarkVision RAT		Malware, Remote command
EDRSilencer		
ErrorFather		Malware, Banking trojan
8Base		Ransomware, Malware
SilentCryptoMiner		Tools, Miner
MisterioLNK		Tools, Loader
PhantomLoader		Tools, Loader
GoldenAce	GoldenJackal	Malware, Info stealer
GoldenBlacklist	GoldenJackal	Malware, Compression
GoldenDealer	GoldenJackal	
GoldenDrive	GoldenJackal	Malware, Exfiltration
GoldenMailer	GoldenJackal	Malware, Exfiltration
GoldenPyBlacklist	GoldenJackal	Malware, Downloader
GoldenUsbCopy	GoldenJackal	Malware, Info stealer
GoldenUsbGo		Malware, Info stealer
Vilsa Stealer		Malware, Info stealer
Prince		Malware, Ransomware
Akira	Akira	Ransomware
Grateful POS	TRINITY, FIN6	Ransomware, POS malware, Info stealer
perfctl		Malware, Rootkit
VeilShell	APT37	Malware, Backdoor
Nexe Backdoor	Patchwork	Malware, Backdoor

How Cyble is Addressing Cybersecurity Challenges in the United States

Cyble offers a robust suite of cybersecurity solutions tailored to meet the unique challenges faced by organizations in the United States. These solutions include Attack Surface Management (ASM), Brand Intelligence, Dark Web Monitoring, Advanced Threat Intelligence, and cutting-edge capabilities in Executive Monitoring, Physical Security Intelligence, Cloud Security Posture Management, and more.



Key Offerings

1. Attack Surface Management (ASM)

Comprehensive Visibility: Cyble's ASM tools identify and mitigate threats across an organization's entire digital footprint, ensuring protection against vulnerabilities.

Proactive Security: Helps organizations uncover hidden risks, providing actionable intelligence to stay ahead of cyber threats.

2. Brand Intelligence

Protect Brand Integrity: Safeguard against impersonation, phishing attacks, and fraudulent domains to maintain trust and credibility in the digital space.

Online Abuse Mitigation: Ensure your brand remains uncompromised across various platforms.

3. Cyber Threat Intelligence

Actionable Insights: Aggregates data from diverse sources, helping organizations detect and mitigate threats in real time.

Enhanced Response Times: Reduces the need for manual monitoring, streamlining threat detection and response.

4. Dark Web Monitoring

Continuous Vigilance: Scans millions of websites, forums, and marketplaces in real time, identifying threats specific to the U.S. market.

Custom Alerts: Set up personalized notifications to enable swift responses to emerging threats.

Safeguarding Stakeholders: Tracks compromised information to minimize the impact of potential breaches.

5. Executive Monitoring

Leadership Protection: Safeguards executives by tracking impersonations, deepfake content, and personally identifiable information (PII) leaks across social media, dark web platforms, and cybercrime forums.

Deepfake Detection and Takedown: Utilizes advanced AI technology to identify and remove manipulated media in real-time, protecting the reputation and integrity of key personnel.

6. Physical Security Intelligence

Comprehensive Threat Management: Provides real-time updates to proactively address potential physical threats and ensure the safety of assets and personnel.

Centralized Oversight: Effortlessly manage security across multiple locations, including offices and warehouses, from a unified platform.

7. Cloud Security Posture Management (CSPM)

Cloud Security Enhancement: Offers continuous monitoring of cloud environments, identifying misconfigurations and ensuring compliance with security policies.

8. Takedown and Disruption

Fraud Prevention: A powerful tool for combating online fraud and cybercrime, ensuring malicious content is promptly removed.

9. BotShield

Intelligence on Compromised Hosts: Provides detailed insights into infected devices within your network that communicate with known command-and-control infrastructures.

10. Vulnerability Management

Real-Time Risk Evaluation: Advanced scanning and remediation strategies give organizations a comprehensive view of exploitable vulnerabilities.

11. Third Party Risk Management (TPRM)

Secure Collaborations: Identifies and mitigates risks arising from third-party interactions, ensuring secure business operations.

12. Digital Forensics & Incident Response (DFIR)

Comprehensive Support: Cyble provides digital forensics and incident response services to help businesses manage, mitigate, and recover from cybersecurity incidents.

Timely Remediation: Aids in reducing downtime and ensuring continuity post-incident.

Enhancing Cybersecurity in the United States with Cyble's Advanced Solutions

Cyble offers a suite of cybersecurity products tailored to address the unique challenges faced by organizations in the Australia and New Zealand (ANZ) region:

CYBLE VISION	**Cyble Vision:** Cyble Vision is an award-winning, AI-powered cyber threat intelligence platform that enhances organizational security through real-time intelligence and threat detection. It offers comprehensive features, including Attack Surface Management, Brand Intelligence, Cyber Threat Intelligence, Dark Web Monitoring, Executive Monitoring, Physical Security Intelligence, Cloud Security Posture Management, Takedown and Disruption, BotShield, Vulnerability Management, Third Party Risk Management, and Digital Forensics & Incident Response. These capabilities empower U.S.-based organizations to proactively address emerging threats and safeguard their digital assets in an increasingly complex cyber threat landscape.
CYBLE HAWK	**Cyble Hawk:** A specialized threat detection and intelligence platform designed for federal bodies, law enforcement agencies, and regulatory organizations. Cyble Hawk provides insights into cybercrime activities relevant to national security, detailed information on threat actors targeting critical infrastructure, and immediate notifications of emerging threats.
ODIN by CYBLE	**Odin by Cyble:** An advanced internet-scanning tool offering real-time threat detection and cybersecurity insights. Odin covers over 4 billion IPs to identify vulnerabilities, provides detailed host information—including data on IP addresses, hostnames, and locations—and allows for scanning and examination of digital certificates.
AmIBreached Powered by CYBLE	**AmIBreached:** A dark web search engine that enables consumers and organizations to identify, prioritize, and mitigate dark web risks. AmIBreached accesses over 150 trillion records from various breaches and forums, offers real-time monitoring with immediate alerts on compromised data, and provides a user-friendly interface for easy monitoring and management.
THE CYBER EXPRESS	**The Cyber Express:** A cybersecurity news platform providing current news, in-depth insights, and a wealth of knowledge on cybersecurity matters. The Cyber Express covers a wide range of topics, including cyber threats, vulnerabilities, and data breaches; offers expert analysis from skilled journalists and researchers; and provides educational content on cybersecurity auditing and compliance.

By leveraging these solutions, organizations in the United States can enhance their cybersecurity posture, proactively address emerging threats, and safeguard their digital assets in an increasingly complex cyber threat landscape.

About Cyble

Cyble Inc. is a cybersecurity company specializing in dark web monitoring and threat intelligence services. Cyble leverages proprietary AI-based technology to help enterprises, federal bodies, and individuals stay ahead of cybercriminals. The company is known for its expertise in tracking cyber threats, data breaches, and other malicious activities.

See Cyble in Action

10080 North Wolfe Road, Suite SW3-200, Cupertino, CA 95014 | contact@cyble.com | +1 888 673 2067