CYBLE®

REPORT

Threat Landscape

SEPTEMBER 2024

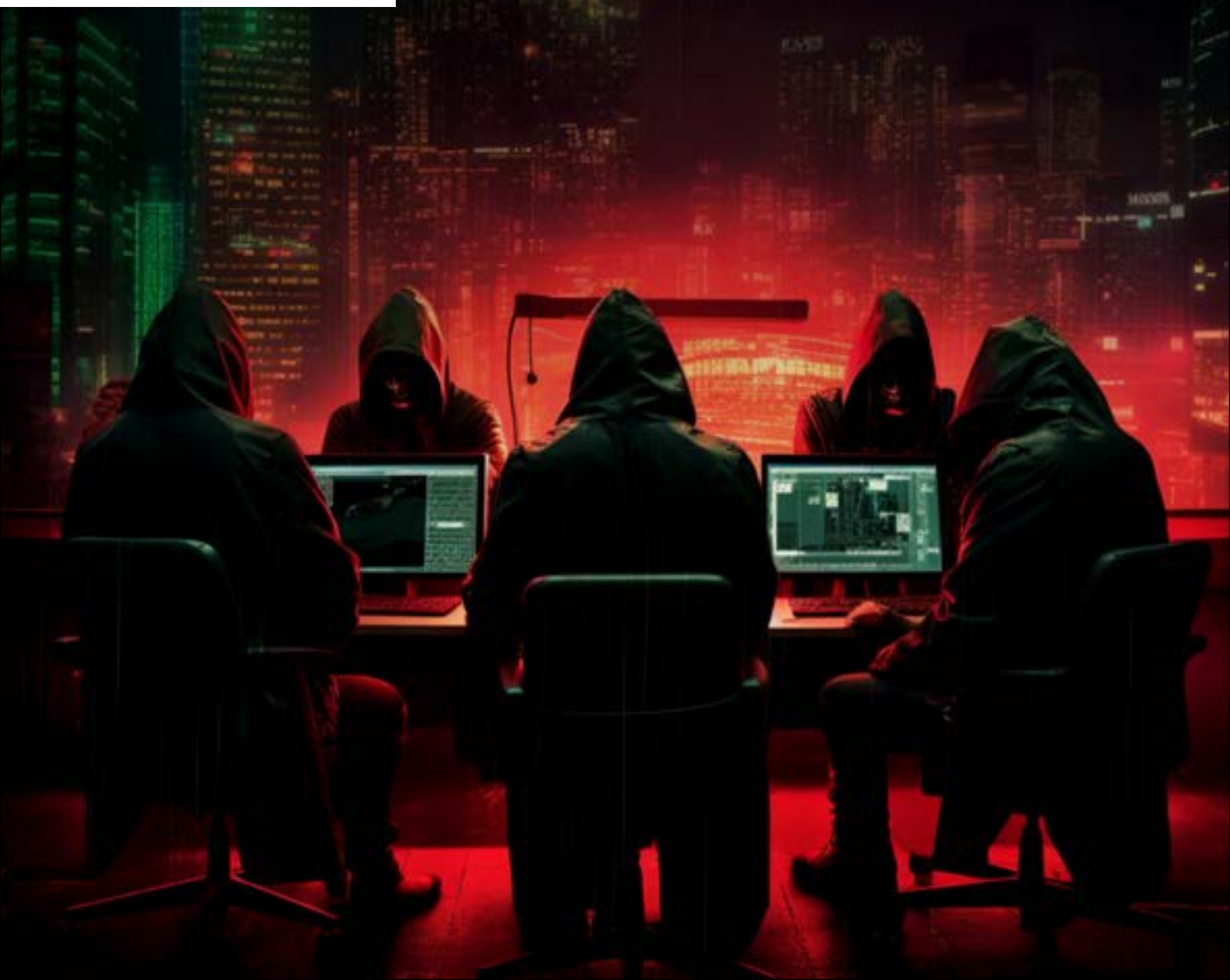


Table of **Contents**

EXECUTIVE SUMMARY

Of the billions of data points collected and analyzed by Cyble's AI-powered threat intelligence systems in September 2024, one stands out above all others: Dark Web data exposures increased by 80% from August 2024 to 79 million in September, an astonishing increase that shows that threat actors (TAs) are meeting with increasing success.

IT security teams must respond with equal urgency, and assisting in that response is a major goal of this report: To give security teams guidance on where to target defensive efforts while also introducing readers to the breadth and depth of Cyble's threat intelligence offerings.

Here are some of the major trends Cyble's Vulnerability Intelligence and Dark Web research units observed in September 2024.

EXECUTIVE SUMMARY

THREAT LANDSCAPE OVERVIEW

ICS-Specific Exploits: A surge in the trade of Industrial Control System (ICS) exploits on Dark Web forums is expected due to an increase in vulnerabilities within ICS assets, threatening already vulnerable critical infrastructure sectors.

Disinformation Campaigns: The spread of disinformation and fake news is becoming a significant cybersecurity concern as the U.S. election approaches, potentially eroding public trust and impacting cybersecurity resilience. The role of nation-state actors in spreading disinformation was one focus of a recent Cyble special report that also examined the role of the dark web in this election.

AI in Social Engineering: The proliferation of AI technology is enhancing the effectiveness of social engineering attacks, enabling more personalized and convincing tactics.

Cybercrime Forum Activities: Mass exploitation of vulnerabilities will continue, as Cyble Dark Web monitoring indicates that exploits of major vulnerabilities are actively discussed within hours of them becoming public, if not minutes, and the markets for Proofs of Concept (PoC) and zero-day vulnerabilities are active and lucrative.

Geopolitical Impacts: Ongoing regional conflicts and an increase in cyber espionage and politically motivated hacktivism have significantly increased cyber threats for all entities.

SECTOR-SPECIFIC INSIGHTS

Targeted Sectors: IT & ITES, Healthcare, Pharmaceutical & Biotechnology, Energy & Utilities, Government, Transportation & Logistics, and BFSI sectors have seen higher attack rates.

Ransomware Focus: Healthcare, Pharmaceutical, Energy & Utilities, and Telecommunications sectors have been particularly targeted by ransomware groups, with significant downtime and data loss reported.

This report covers the most active threat and hacktivist groups and malware families in September 2024, emerging threat actors and hacktivist groups, Dark Web and cybercrime forum trends, the most exploited IT and critical infrastructure vulnerabilities, and notable cyber incidents shaping the threat landscape.

THE MOST ACTIVE THREAT GROUPS IN SEPTEMBER

Cyble threat intelligence data identified these nine threat groups as the most active in September. Ransomware groups were by far the most active during the month, but nation-state groups and hacktivists were active in threat campaigns too.

Name	Aliases	Categories	Malware & Tools
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
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 Group, Ransomware Group	Xorist, Chaos, RURansom, Slam, njRAT
Sniper Dz		Cybercriminal Group	
TWELVE		Hacktivist Group	Mimikatz, Cobalt Strike, Chisel, BloodHound, PowerView, CrackMapExec, PsExec

Note: The appendix includes a table detailing the 50 most active malware families in September.

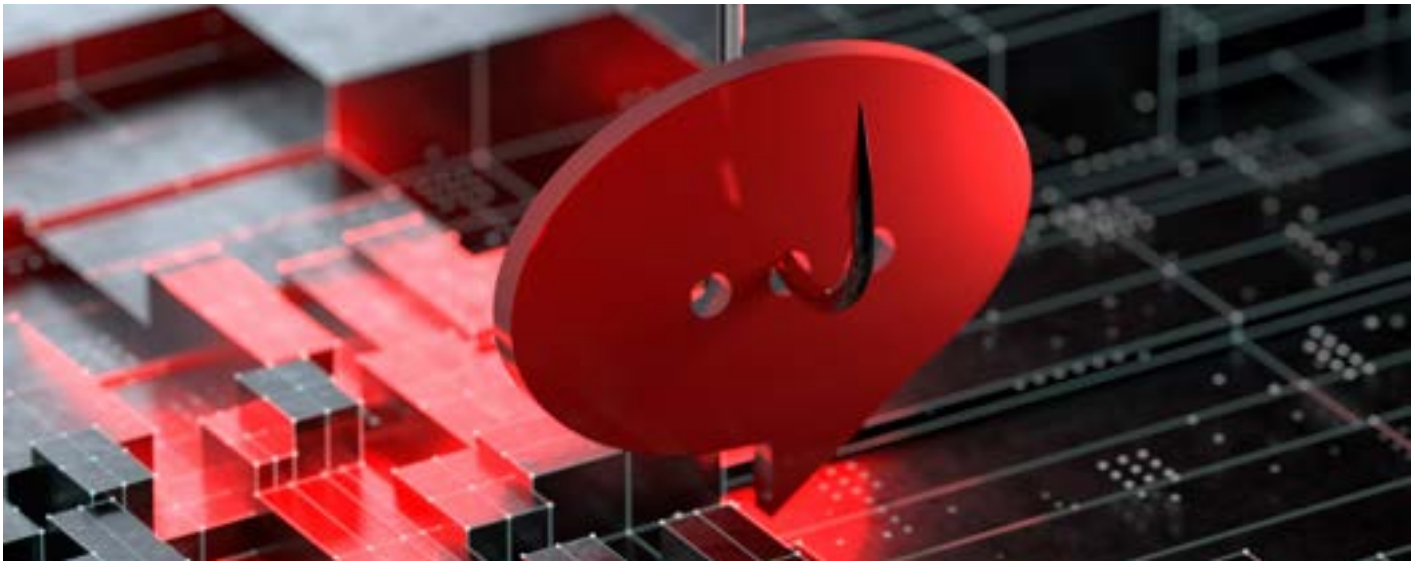
EMERGING THREAT AND HACKTIVIST GROUPS

Cyble advisories alerted clients to numerous emerging threat actors (TAs) and hacktivist groups in the month of September. Here are six that are particularly noteworthy.

Hacktivist Vanguard: First identified by Cyble in 2023, Hacktivist Vanguard primarily focuses on targeting educational institutions and government entities in Pakistan, Indonesia, Bangladesh and Malaysia. Their attacks are mostly in retaliation to hacktivist groups sympathizing with the above-mentioned countries and attacking Indian entities. However, they expanded their operations with cyberattacks on Algerian systems in mid-July 2024 (#PawnAlgeria) and launched several attacks on Egyptian government websites under the banner of #OPERATION_Egypt in September 2024. The group claimed the attacks on Egypt were in response to Egyptian hacktivist attacks on Indian sites.

DeathNote Hackers: Formed in 2016, this Philippines-based collective joined BreachForums in June 2024 and began releasing leaked documents and data from China.

Patchwork APT: Cyble Research and Intelligence Labs (CRIL) encountered an ongoing campaign associated with the Patchwork APT group that is likely aimed at Chinese entities, in keeping with previous targets in China and Bhutan. The TAs have utilized a malicious LNK file, likely originating from a phishing email, as the initial infection vector. This file executes a PowerShell script that downloads two files: a seemingly innocuous PDF intended to lure the user and a malicious Dynamic Link Library (DLL). CRIL researchers have named the malware "Nexe Backdoor" after a string found in the binary used for command and control (C&C) communication.

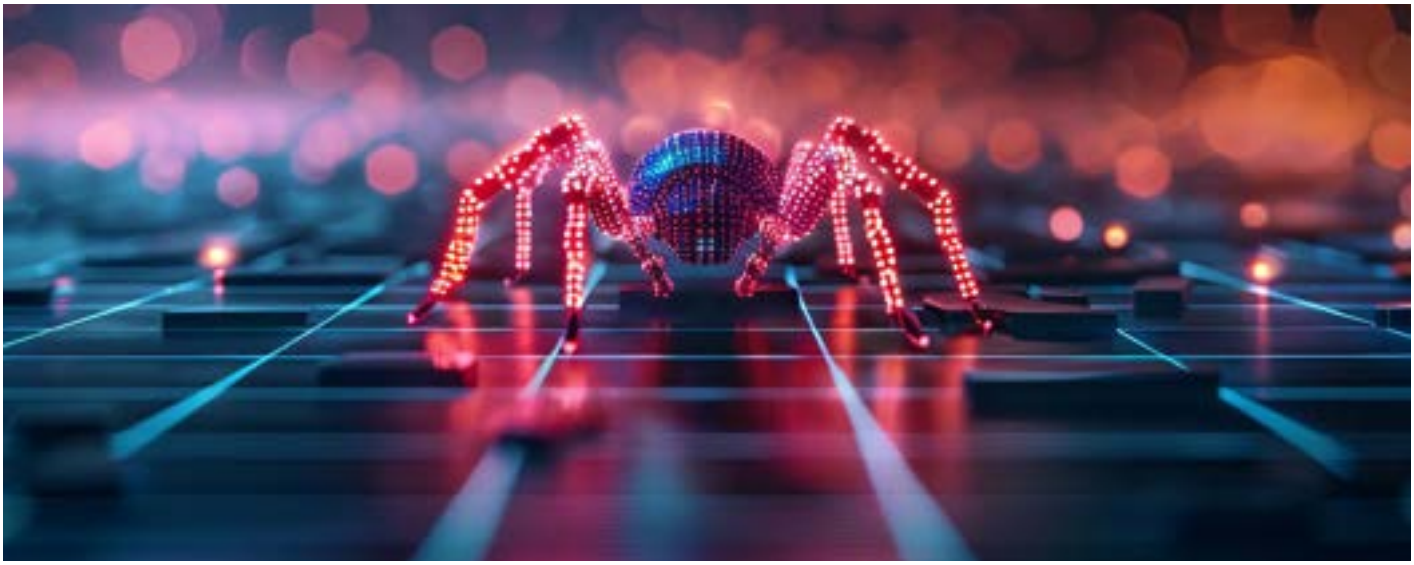


EMERGING THREAT AND HACKTIVIST GROUPS

RipperSec: A hacktivist group known for its anti-Israel and anti-India stance and frequent Distributed Denial of Service (DDoS) attacks, RipperSec recently diversified its attack methods to include more sophisticated cyber activities, such as database leaks and unauthorized access to admin panels. RipperSec is also constantly involved in spreading malicious tools aimed at attacking Israeli targets, with active promotions of these tools on their Telegram platform. On July 4, 2024 the group announced the death of its leader, reportedly from a car crash. Despite this, RipperSec continued its operations without significant interruption, suggesting a decentralized or resilient internal structure. Rippersec group has collaborated numerous times with pro-Russian hacktivists such as NoName057(16) and People's Cyber Army in targeting Ukrainian public and private entities.

Radar/Dispossessor: Despite a coordinated global law enforcement action in August to dismantle this ransomware group's online infrastructure, Radar/Dispossessor has remained active and was actively seeking new victims in September.

RADNET64: This professed Anti-Zionist group only appeared on the radar in March 2024, but has been very active since. The group primarily targets India, especially Indian government agencies, transporters, banks and telecom companies. However, at various times, the group has carried out attacks on France, Israel, Saudi Arabia, United States, and Nepal. Recent attacks include a late August DDOS attack on the French airport system, and early September DDoS attacks on Harcobank and the Nuclear Power Corporation of India Limited.



NOTABLE SEPTEMBER 2024 CYBER INCIDENTS

Here are seven noteworthy incidents that occurred in September – five cyber attacks and two incidents that raised broader concerns.

1. **Money transfer service MoneyGram** was knocked offline for days by a cyberattack that resulted in the theft of sensitive customer and transaction data. The Dallas-based company initially called it a network issue, then two days later said it was a cybersecurity issue.

2. **The German Air Traffic Control (ATC) system,** managed by Deutsche Flugsicherung (DFS), faced a significant cyberattack that underscored the vulnerabilities of critical infrastructure in aviation. The air traffic control cyberattack impacted DFS's administrative IT systems, disrupting office communications, but it did not affect air traffic operations. The air traffic control cyberattack incident is suspected to be the work of the notorious APT28 group.

3. **Public Wi-Fi services at 19 major railway stations across Britain** were taken offline, disrupting internet access for thousands of commuters and travelers. Users attempting to log in were confronted with disturbing messages that included references to terror attacks in Europe, raising widespread concern over the security of public Wi-Fi networks in the UK.

4. **Arkansas City, Kansas** encountered a cybersecurity issue early Sunday morning, September 22, 2024, involving its Water Treatment Facility. Out of caution, the Facility was switched to manual operations while the situation was resolved. It was believed to be a ransomware attack.

5. **The University Medical Center Health System in Lubbock, Texas –** the only Level 1 trauma center within 400 miles – confirmed that IT outages were caused by a ransomware incident. The hospital system stated that the attack led to "temporarily diverting incoming emergency and non-emergency patients via ambulance to nearby health facilities until access to our systems is restored."

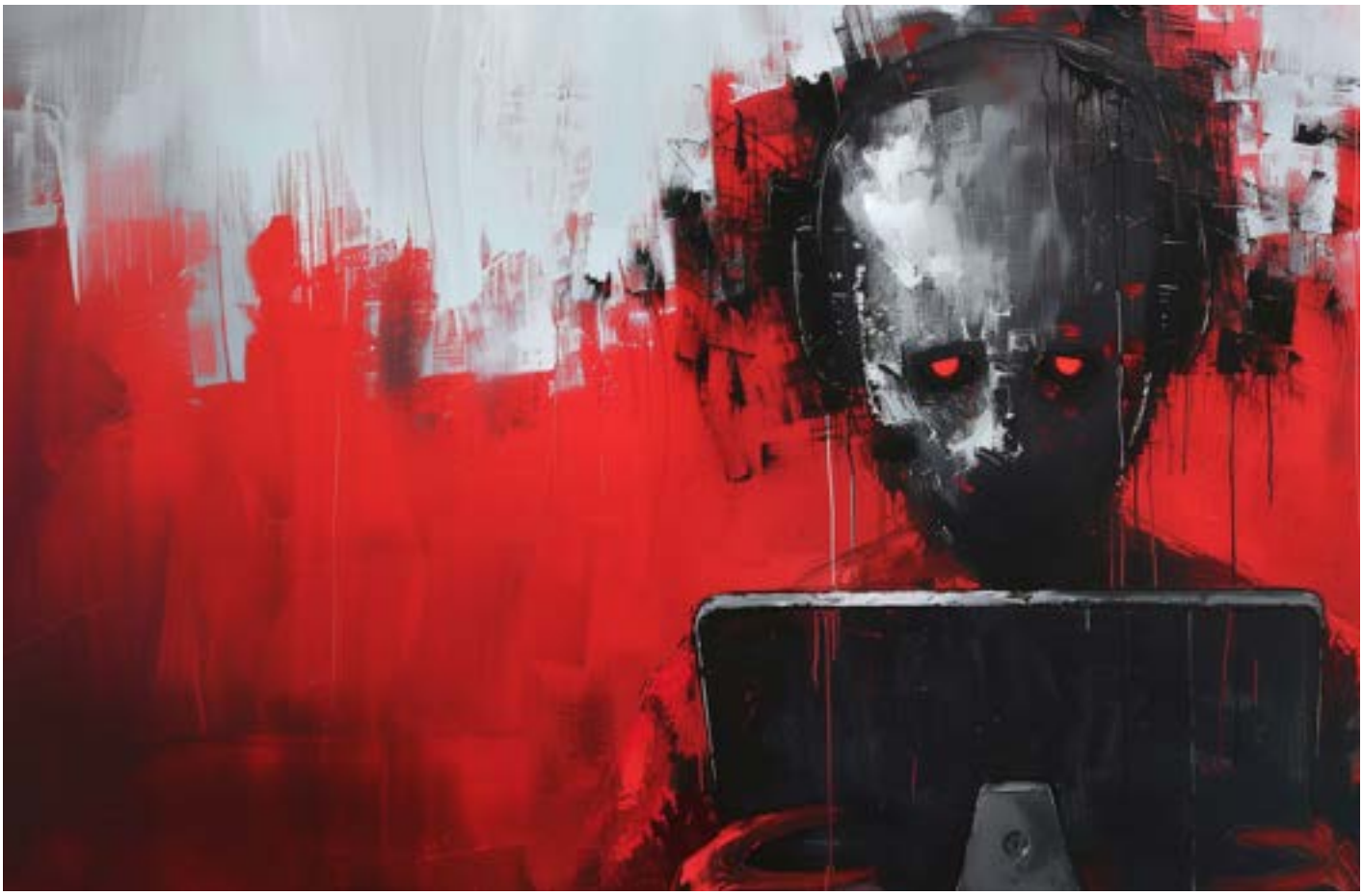
NOTABLE SEPTEMBER 2024 CYBER INCIDENTS

6

Russia pivoted its disinformation efforts to focus on Democratic presidential candidate Kamala Harris with the U.S. election approaching, releasing several fake, widely-seen videos designed to harm her campaign. Microsoft published a new report warning that two Russian groups have used X (formerly Twitter), Telegram and several fake news websites to disseminate controversial and fictitious videos about Harris.

7

Russian cybersecurity company Kaspersky, facing a U.S. ban imposed by President Biden, deleted its anti-malware software from customers' computers across the United States and automatically replaced it with UltraAV's antivirus solution. This came after Kaspersky decided to shut down its U.S. operations and lay off U.S.-based employees. Kaspersky's ability to install a program with kernel-level access that users hadn't approved heightened concerns about security tool kernel access that began when CrowdStrike crashed 8.5 million Windows machines worldwide after a faulty update in July.



HACKTIVISM TRENDS AND ACTIVE GROUPS

The following trends and groups were notably active in the realm of hacktivism:

1. **Increased Geopolitical Retaliation:** Hacktivist activities have increasingly become a form of geopolitical retaliation, with groups targeting nations as a form of protest against political decisions, military actions, or international agreements.
2. **Targeting of Critical Infrastructure:** There's a noticeable trend towards targeting Industrial Control Systems (ICS) and Supervisory Control and Data Acquisition (SCADA) systems, crucial for national economies, defense, public health, and energy sectors.
3. **Evolution into Across-the-Border Crime:** Hacktivism has evolved from a means of promoting social and political change to a tool for furthering ideological agendas, disrupting governments and businesses, and creating social disharmony.
4. **State-Sponsored and Destructive Hacktivism:** The emergence of state-sponsored hacktivism indicates a shift towards more organized and potentially destructive cyber operations, blurring the lines between hacktivism and cyber warfare.

Active Groups:

1. **THE NIGHT HUNTERS:** Active in Southeast Asia, particularly targeting Cambodia, Indonesia, Malaysia, and Bangladesh through website defacements, data leaks, and unauthorized access to critical sectors like government, education, healthcare, food commodity, and finance. Shares similar regions and targets as KINGSMAN.
2. **Mysterious Team Bangladesh:** Engaged in operations against the Australian government and banking sectors as a response to cultural provocations.
3. **GhostClan:** Reacted to the Japan-Israel cybersecurity cooperation agreement by targeting Japanese websites.
4. **NoName:** A pro-Russian group that targeted Japanese organizations in retaliation for sanctions against Russia.
5. **SiegedSec:** Participated in operations against Colombian entities following the arrest of a notable hacker, indicating a trend of hacktivist groups defending their members.

Hacktivism in 2024 continues to be a significant cybersecurity concern, with groups leveraging sophisticated cyber tactics for ideological, political, or retaliatory purposes. The evolution of hacktivism into a tool for across-the-border crime and the involvement of state-sponsored activities suggest a complex and escalating threat landscape.

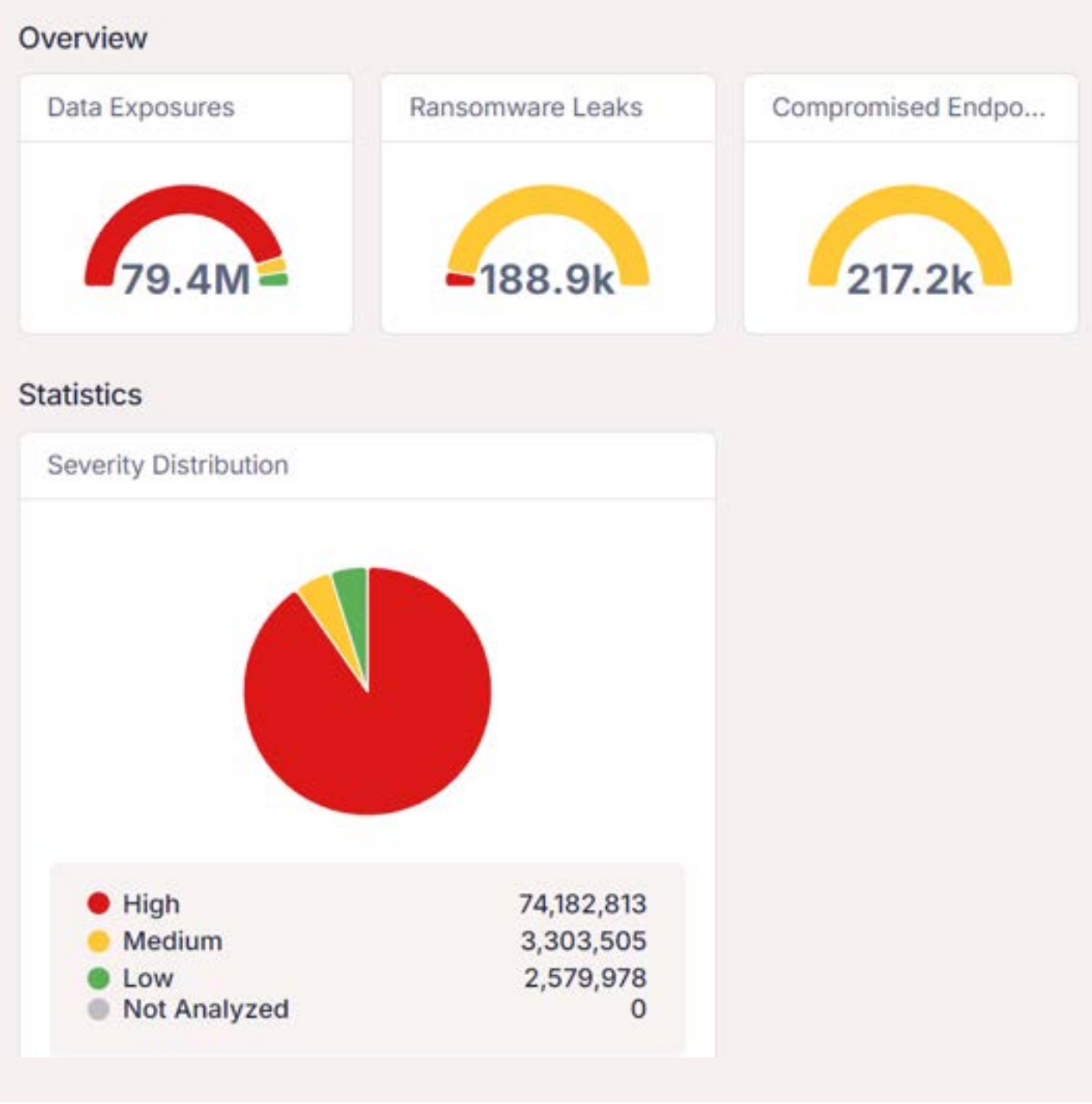
THE MOST ATTACKED CVES IN SEPTEMBER

Cyble's Vulnerability Intelligence and Dark Web research units highlighted a number of vulnerabilities meriting high-priority attention by security teams because of their criticality or exploitation activities. Here are 21 vulnerabilities that Cyble warned clients about in September:

1. **CVE-2024-27348**
   Apache HugeGraph-Server Improper Access Control Vulnerability - **Critical**
2. **CVE-2024-7490**
   Microchip Technology Advanced Software Framework Improper Input Validation Vulnerability - **Critical**
3. **CVE-2024-45409**
   GitLab Community Edition (CE) and Enterprise Edition (EE) Authentication Bypass Vulnerability - **Critical**
4. **CVE-2024-23692**
   Rejetto HTTP File Server Template Injection Vulnerability - **Critical**
5. **CVE-2024-8190**
   Ivanti Cloud Services Appliance OS Command Injection Vulnerability - **High**
6. **CVE-2024-40766**
   SonicWall SonicOS Improper Access Control Vulnerability - **Critical**
7. **CVE-2024-41869**
   Adobe Acrobat and Reader Use After Free Vulnerability - **High**
8. **CVE-2024-7591**
   Progress LoadMaster Improper Input Validation Vulnerability - **Critical**
9. **CVE-2024-45195**
   Apache OFBiz Direct Request ('Forced Browsing') Vulnerability - **High**
10. **CVE-2024-40711**
    Veeam Backup & Replication (VBR) Remote Code Execution (RCE) Vulnerability - **Critical**
11. **CVE-2024-20469**
    Cisco Identity Services Engine (ISE) Command Injection Vulnerability - **Medium**
12. **CVE-2024-24401**
    Nagios XI SQL Injection Vulnerability - **Critical**
13. **CVE-2024-20017**
    MediaTek Chipsets Remote Code Execution (RCE) Vulnerability - **Critical**
14. **CVE-2022-40684**
    Fortinet FortiOS and FortiProxy Authentication Bypass Vulnerability - **Critical**
15. **CVE-2024-38063**
    Microsoft Windows TCP/IP Remote Code Execution (RCE) Vulnerability - **Critical**
16. **CVE-2024-36974**
    Splunk Enterprise on Windows Path Traversal Vulnerability - **High**
17. **CVE-2024-5274**
    Google Chrome Type Confusion - **High**
18. **CVE-2024-7262**
    Kingsoft WPS Office Path Traversal Vulnerability - **High**
19. **CVE-2024-7263**
    OpenSSH server (SSHD) on glibc-based Linux systems Remote Code Execution (RCE) – **High**
20. **CVE-2024-29847**
    Ivanti Endpoint Manager Deserialization of Untrusted Data vulnerability - **Critical**
21. **CVE-2024-38812**
    VMware vCenter Server Heap-based Buffer Overflow vulnerability - **Critical**

DARK WEB AND CYBERCRIME FORUM ACTIVITIES

Cyble detected more than 79 million data exposures in September (up nearly 80% from 44 million in August), 189,000 ransomware leaks, and 217,000 compromised endpoints. A summary of those findings and trends follows the graphic below.



DARK WEB AND CYBERCRIME FORUM ACTIVITIES

- **Increased Discussions on Exploit Kits:** There was a notable rise in discussions around new exploit kits targeting recent vulnerabilities in web browsers and document readers. These discussions often included technical breakdowns of the exploits and potential countermeasures.
- **Sale of Access Credentials:** Forums saw a surge in the sale of access credentials to compromised systems, particularly those belonging to organizations in the healthcare and financial sectors. Prices varied based on the perceived value of the access.
- **Ransomware-as-a-Service (RaaS) Updates:** Several posts were observed where RaaS operators provided updates on their encryption algorithms and negotiation services. This indicates an ongoing evolution and professionalization of ransomware operations.
- **Leak of Government Data:** A significant leak was discussed extensively, involving sensitive data from a government entity. The data was purportedly obtained through a sophisticated phishing campaign.
- **Botnet Recruitment:** There was an uptick in posts related to the recruitment of compromised machines into botnets. The focus was primarily on devices that could be used for large-scale DDoS attacks.
- **Software Vulnerability Auctions:** Cybercriminals were seen auctioning off information about unpatched software vulnerabilities, with a particular emphasis on operating systems and widely used enterprise software. These auctions attracted significant attention, highlighting the high demand for such vulnerabilities.

KEY TAKEAWAYS

1. Cybercrime forums are active hubs for the exchange of information, tools, and services related to cybercrime.
2. There is a clear trend towards the commercialization of cybercrime, with structured services like RaaS becoming more sophisticated.
3. The sale and auction of access credentials and software vulnerabilities remain a critical threat, underlining the importance of robust cybersecurity measures and vulnerability management programs.

ICS AND OT THREATS AND VULNERABILITIES

Industrial control systems (ICS) and operational technology (OT) are crucial components of critical infrastructure – and thus a key target for nation-state threat actors, hacktivists and cybercriminals. The most prominent development in the critical infrastructure threat landscape thus far in 2024 may have been dramatic ransomware attacks on healthcare targets, but there are a number of other noteworthy trends:

1. **Increased Trade of ICS-Specific Exploits on Dark Web Forums:** There has been a surge in the trade of ICS-specific exploits over Dark Web forums due to a substantial uptick in vulnerabilities within ICS-specific assets. This trend suggests a growing interest and capability among cybercriminals in targeting Industrial Control Systems more aggressively.
2. **Ransomware Attacks on Critical Infrastructure (CI):** Ransomware continues to be a core threat to ICS and OT security, with multiple successful campaigns that have crippled operations and caused significant financial losses. This trend is intensifying in 2024, indicating that ransomware attacks on CI are becoming more common and impactful.
3. **Hacktivism Threats to CI Sectors:** Hacktivism poses a significant threat to CI sectors, not only through direct service disruption but also through its potential to cause widespread panic, inspire copycat attacks, and leave the door open for more dangerous actors. A minor disruption in one part of a CI network can have cascading effects on other interconnected systems.
4. **Exposure of Critical Infrastructure Assets:** The exposure of critical infrastructure assets like Human-Machine Interfaces (HMI), Supervisory Control and Data Acquisition (SCADA) systems, and Programmable Logic Controllers (PLC) over the internet has led to disastrous events. Incidents where attackers gained access to these systems highlight the vulnerabilities in CI sectors.
5. **Targeting of Specific ICS Components and Protocols:** Specific ICS components and protocols have been targeted, with Kamstrup_protocol, S7comm, and Guardian AST protocols among the highest-targeted by attackers in 2023 and continuing into 2024, reflecting a strategic focus by cybercriminals on exploiting known vulnerabilities in these areas.

ICS AND OT THREATS AND VULNERABILITIES

6. **Collaboration Among Threat Actors:** There has been a noticeable shift in tactics, with threat actors that were previously acting independently now collaborating with other groups. This collaboration could lead to more sophisticated and coordinated attacks against ICS and OT environments.

These trends underscore the evolving and increasingly sophisticated threat landscape facing OT and ICS environments as of September 2024. Organizations in these sectors must remain vigilant and proactive in their cybersecurity measures to mitigate these growing threats.

ICS AND OT THREATS AND VULNERABILITIES

CRITICAL ICS/OT VULNERABILITIES

Here are 17 ICS and OT vulnerabilities that stood out in Cyble's analysis:

1. **CVE-2024-7847**
   Rockwell Automation's RSLogix 5 and RSLogix 500 software, remote code execution (RCE) vulnerability.
2. **CVE-2024-45824**
   Rockwell Automation FactoryTalk View Site Edition up to version 14.0 - Command injection vulnerability.
3. **CVE-2024-7986, CVE-2024-7987, and CVE-2024-7988**
   Rockwell Automation ThinManager ThinServer, Improper Privilege Management, Incorrect Permission Assignment, and Improper Input Validation vulnerabilities.
4. **CVE-2024-43647**
   Siemens SIMATIC S7-200 SMART CPUs, improper handling of TCP packets with incorrect structures.
5. **CVE-2024-35783**
   Siemens SIMATIC BATCH, SIMATIC Information Server (2020, 2022), SIMATIC PCS 7, SIMATIC Process Historian (2020, 2022), and SIMATIC WinCC (Runtime Professional, SCADA Software), Execution with Unnecessary Privileges vulnerability.
6. **CVE-2023-44373**
   Siemens RUGGEDCOM and SCALANCE M-800/S615 family, Improper Neutralization of Special Elements vulnerability.
7. **CVE-2024-45032**
   Siemens Industrial Edge Management Authorization Bypass vulnerability.
8. **CVE-2023-46850**
   Use After Free OpenVPN vulnerability affecting Siemens products.
9. **CVE-2024-33698**
   Siemens SIMATIC Information Server 2022 and 2024, SIMATIC PCS neo, SINEC NMS, and Totally Integrated Automation Portal, Heap-based Buffer Overflow vulnerability.
10. **CVE-2023-45852 and CVE-2023-5222**
    Viessmann Vitogate 300 firmware, Command Injection and Use of Hardcoded Credentials vulnerabilities.
11. **CVE-2024-39278 and CVE-2024-42495**
    Hughes Network Systems WL3000 Fusion Software, Insufficiently Protected Credentials and Missing Encryption of Sensitive Data vulnerabilities.
12. **CVE-2024-6795 and CVE-2024-6796**
    Baxter Connex Health Portal, SQL Injection and Improper Access Control vulnerabilities.

APPENDIX: MOST ACTIVE MALWARE FAMILIES SEPT. 2024

Name	Types	Platforms	Related Threat Actors
RansomHub	Ransomware	Windows	
BlackSuit	Ransomware	Linux	
Clop	Ransomware,Big Game Hunting	Windows	Carbanak,FIN11,TA505
Medusa	Ransomware	Windows	
Rhysida	Ransomware,Malware	Linux,Windows	
8Base	Ransomware	Windows	
PLAY	Ransomware	Windows	
SilentCryptoMiner	Tools,Miner	Windows	
Cactus	Ransomware	Windows	
Hydra	Ransomware	Linux	
Nitro	Ransomware	Windows	
MisterioLNK	Tools,Loader	Windows	
PhantomLoader	Tools,Loader	Windows	
GoldenAce	Malware,Info stealer	Windows	GoldenJackal
GoldenBlacklist	Malware,Compression	Windows	GoldenJackal
GoldenDealer		Windows	GoldenJackal
GoldenDrive	Malware,Exfiltration	Windows	GoldenJackal
GoldenMailer	Malware,Exfiltration	Windows	GoldenJackal
GoldenPyBlacklist	Malware,Downloader	Windows	GoldenJackal
GoldenUsbCopy	Malware,Info stealer	Windows	GoldenJackal
GoldenUsbGo	Malware,Info stealer	Windows	
LockBit	Ransomware,Big Game Hunting,Remote command	Linux	LockBit Gang,Storm-0501
Vilsa Stealer	Malware,Info stealer	Windows	

APPENDIX: MOST ACTIVE MALWARE FAMILIES SEPT. 2024

Name	Types	Platforms	Related Threat Actors
Prince	Malware,Ransomware	Windows	
AgendaCrypt	Ransomware,Malware	Windows	
Akira	Ransomware	Linux	Akira
Grateful POS	Ransomware,POS malware,Info stealer		FIN6
perfctl	Malware,Rootkit	Linux	
VeilShell	Malware,Backdoor	Windows	APT37
Nexe Backdoor	Malware,Backdoor	Windows	Patchwork
Embargo	Ransomware,Malware	Windows,Linux	Storm-0501
Lynx	Malware,Ransomware	Windows	
Nitrogen	Malware,Ransomware	Windows	
SnipBot	Malware,RAT	Windows	RomCom
Necro Trojan	Malware,Dropper	Android	
PondRAT	Malware,Backdoor	Linux,MacOS	Lazarus Group
SerpentineRAT	Malware,Backdoor	Windows	
Splinter			
SuperShell	Malware,Backdoor	Linux	
SambaSpy	Malware,Info stealer	Windows	
MISTPEN	Malware,Backdoor	Windows	Lazarus Group
RustDoor	Malware,Backdoor	Windows,MacOS	
Defray777	Ransomware,Big Game Hunting		Sprite Spider
Ajina.Banker	Malware,Banking trojan	Android	
Hadooken	Malware,Dropper	Linux	
Spearal	Malware,Backdoor	Windows	OilRig,APT34
Veaty	Malware,Backdoor	Windows	APT34,OilRig
Vo1d	Malware,Backdoor	Android	
KRANSOM	Malware,Ransomware	Windows	

Industry Recognition

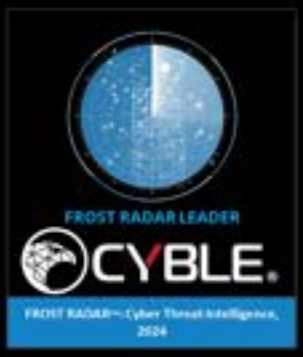
Gartner

Cyble Named a Sample Vendor in Three Gartner® Hype Cycles for Managed IT Services, 2024, Cyber Risk Management, 2024 and Security Operations, 2024

FORRESTER®

Cyble Recognized in Forrester's Attack Surface Management Solutions Landscape Q2-2024 Report

FROST & SULLIVAN



Cyble Named Leader in Frost Radar™ Cyber Threat Intelligence 2024

Gartner Peer Insights.

4.6/5

Ranked among top 5 cyber threat intelligence providers

Named a leader in the G2 Grid for Dark Web Monitoring

Named Editor's Choice for Threat Intelligence by Cyber Defense Magazine

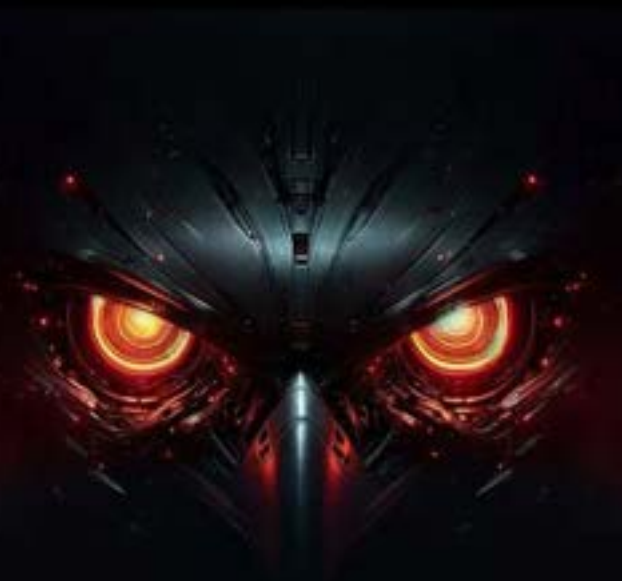
Earned nine awards at the Global InfoSec Awards during RSA

Ranked in Y Combinator's Top 100 AI Startups for 2024

Recognized as one of America's Best Startup Employers by Forbes

CYBLE.

Cyble provides one of the fastest and most comprehensive coverages across adversaries, infrastructure, exposure, weaknesses, and targets by leveraging cutting-edge AI technology and real-time threat intelligence and detection. Through advanced data analysis, expert insights, and automated processes, Cyble facilitates swift detection, prioritization, and remediation of security threats, and enables governments and enterprises to protect their citizens and infrastructure by delivering crucial intelligence promptly. Headquartered in Atlanta, GA, and with employees across 12 countries, Cyble has a global presence. To learn more about Cyble, visit www.cyble.com



11175 Cicero Drive Suite, 100 Alpharetta GA 30022, US. | contact@cyble.com | +1 888 673 2067