Q3 2024 Threat Landscape Report

nuspire

Rising Ransomware, Dark Web Trends and Exploit Surges

nuspire.com

This report is sourced from over a trillion traffic logs ingested from Nuspire client sites and associated with thousands of devices around the globe.

nuspire

nuspire

What's in the Report

Introduction:

Inside Q3's Threats: The Rise of Ransomware Extortions and Targeted VPN Exploits

As we wrap up the third quarter of the year, Nuspire has witnessed shifting trends in the ransomware, dark web and exploit sections of our report. Our research revealed that ransomware extortion publications increased by **8%**, Lumma Stealer fiercely reclaimed its top spot as the leading infostealer, and threat actors are focusing heavily on exploiting VPN technology.

Our report is divided into three key sections, each tackling some of the most pressing threats organizations face today: Ransomware, the Dark Web and Exploits. In each section, we highlight the most critical data points, uncover emerging trends and offer actionable recommendations to help you stay ahead of these evolving threats. As always, we're thrilled to share our insights, giving you a clear view of the cyber threat landscape through the lens of Nuspire's expertise and data.

Ransomware Publications

Dark Web Listings

Exploits

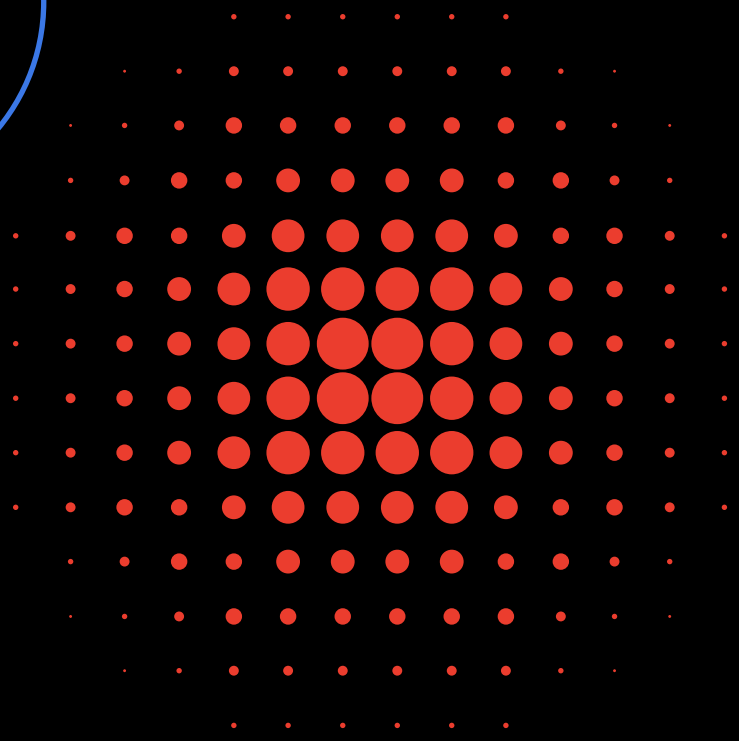
Q3 Ransomware Publications

1,542 total ransomware publications

129 publications averaged per week

18 publications averaged per day

8.06% increase in publications from Q2



Q3 Dark Web Market Activity

28,512
listings of stolen accounts for sale

695,709
listings of credit cards for sale

3,244,066
total marketplace listings

1,972,372
listings of stolen browser data

86,325
listings of email account access for sale

27,748
listings of shell access for sale

40,029
listings of RDP access for sale

42,559
listings of social security numbers for sale

-5.41%
decrease in total listings from Q2

Q3 Exploitation Events

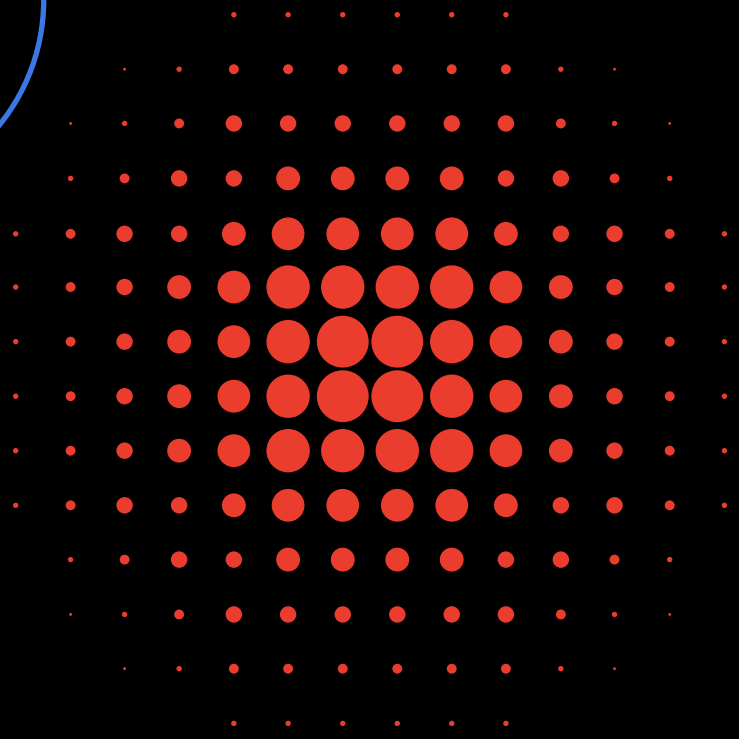
16,964,624
total

50.96%
increase in total activity from Q2

1,413,718
exploit attempts detected per week

1,192
unique exploits detected

201,959
exploit attempts detected per day



How We Crunch the Numbers

Nuspire's Threat Intelligence Team follows a five-step data analysis methodology.

GATHER

Sources threat intelligence and data from global sources, client devices and reputable third parties.

1

PROCESS

Data is analyzed using a combination of machine learning, algorithm scoring and anomaly detection.

2

DETECT

Log data is ingested using Nuspire's cloud-based SIEM, which alerts the security operations center (SOC). The SOC then notifies the client and works with them to remediate the threat.

3

EVALUATE

Analysts further scrutinize the research, scoring and tracking of existing and new threats.

4

DISSEMINATE

Analysts leverage the insights to constantly improve the SOC, alerting the community through the creation of detection rules, briefs and presentations.

5

Q3's Top Threat Events

July 1
Critical Out-of-Cycle Patch Released for Juniper Devices

July 1
OpenSSH Vulnerability "regreSSHion" allows root access

July 9
Critical Vulnerability "Blast-Radius" affecting RADIUS Protocol Announced

July 10
Microsoft's July 2024 Patch Tuesday Addressed 4 Zero-Days, 142 Vulnerabilities

July 19
Worldwide BSOD Outage on Microsoft Windows Caused by EDR Update

July 19
CISA Warns of Actively Exploited RCE Vulnerability in GeoServer GeoTools Software

July 25
CISA Warns BIND 9 Users to Address New DNS Exploits

August 1
CISA Warns Users of VMware ESXi Vulnerability Exploited in Ransomware Attacks

August 9
North Korean Attackers Exploit VPN Update Flaw to Deploy Malware

August 13
Cisco Warns of Critical RCE Zero-Day in End-of-Life IP Phones

August 14
Microsoft's August Patch Tuesday Addresses 10 Zero-Days, 6 Exploited

August 21
CISA Warns of Critical SolarWinds RCE Vulnerability Exploited in Attacks

August 22
CISA Warns of Critical Jenkins Vulnerability Exploited in Ransomware Attacks

August 27
SonicWall Releases Patches for Critical Access Control Vulnerability

August 29
CISA Releases Advisory on Iran-Based Threat Actors Enabling Ransomware Attack

September 5
VMware ESXi Servers Targeted by a New Cicada Ransomware Variant

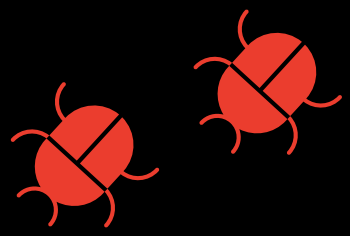
September 11
Microsoft's September 2024 Patch Tuesday Addresses 4 Zero-Days, 79 Vulnerabilities

September 12
Critical SonicWall SSL-VPN Access Control Vulnerability Exploited in Ransomware Attacks

September 18
CISA Warns of Recently Patched Windows Vulnerability Exploited in Infostealer Attacks

September 30
CISA Warns of Critical Ivanti vTM Auth Bypass Vulnerability Exploited in Attacks

Q3 2024 Ransomware Extortion Publications



1,542 Total Ransomware Publications

129

publications averaged per week

18

publications averaged per day

8.06%

increase in publications from Q2

Ransomware

Ransomware Power Shift: RansomHub Dethrones LockBit in Extortion Publications

Figure 1 shows the average Q3 ransomware extortion publication activity in a dashed trend line. Nuspire monitors known ransomware operators' extortion sites where, following a successful attack, these gangs will attempt to extort the victim into paying their ransom by threatening to release stolen data if not paid.

The solid line shows the true weekly numbers to help identify spikes and abnormal activity. Compared to the second quarter, publications on ransomware extortion have increased by **8.06%**, with the most active period at the beginning of September.

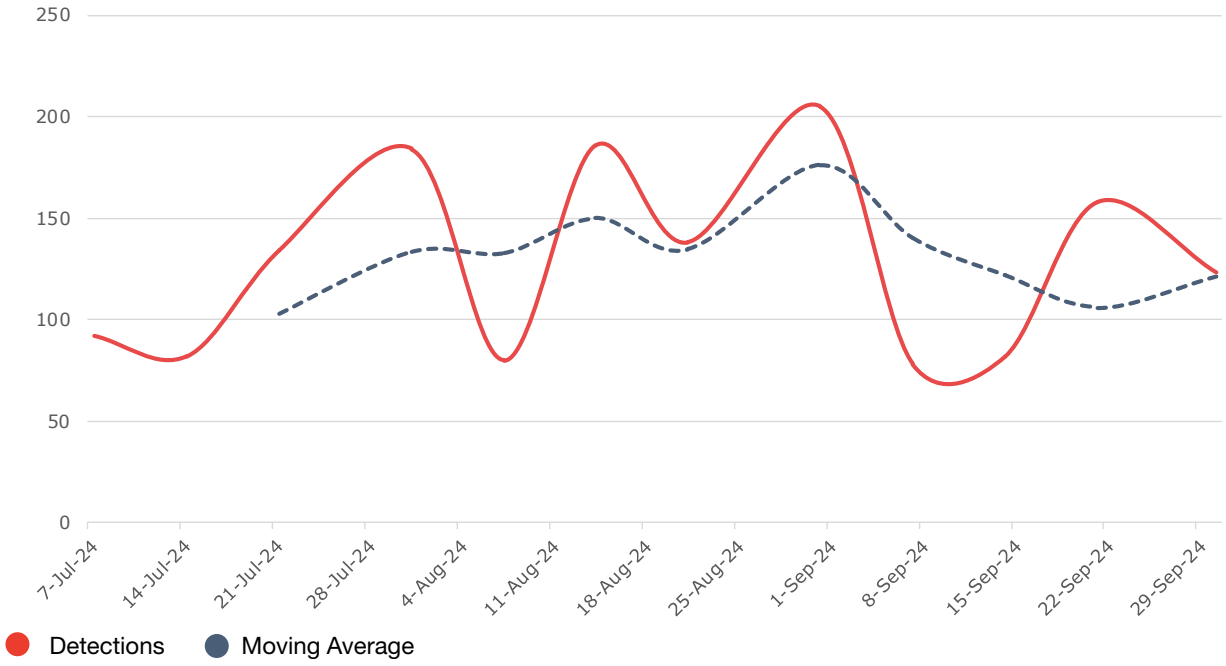
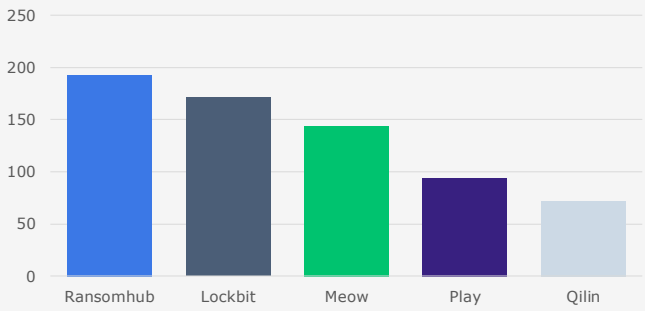


FIGURE 1. RANSOMWARE EXTORTION PUBLICATIONS | NUSPIRE, Q3 2024



In Q3, LockBit saw a sharp decline in extortion activity, dropping by **51.97%**, which allowed RansomHub to interrupt LockBit's long-standing dominance and claim the top spot. Ransomware group Meow has made its debut in the top 5. Although suspected to have been active since 2022, Meow dramatically increased its attack success in Q3 2024 compared to Q2, when it published no extortions on its site.

FIGURE 2. TOP FIVE RANSOMWARE OPERATORS
NUSPIRE, Q3 2024

Ransomware

RansomHub Ransomware

RansomHub Ransomware emerged in February 2024, operating as a Ransomware-as-a-Service (RaaS) platform. It develops the ransomware and provides access to affiliates, taking a percentage of the ransom collected. Since its launch, these affiliates have successfully attacked, encrypted and extorted data from hundreds of victims across various industries, including critical infrastructure, healthcare, information technology, government services, food and agriculture, financial services, manufacturing, logistics and communications. It's clear the group's affiliates target organizations indiscriminately, focusing more on opportunistic strikes than on specific demographics.

Affiliates employ a double-extortion model, encrypting systems while exfiltrating data to pressure victims into paying—a tactic commonly used by many ransomware groups. Attack vectors and exfiltration methods can vary between affiliates, making it challenging to pinpoint specific attack techniques. After a successful breach, a ransom note is left on the affected machines, containing a client ID and a unique .onion URL for the victim to access through the TOR browser. While timelines can differ depending on the affiliate, victims typically have 90 days to pay the ransom before their stolen data is publicly posted on the group's leak site.

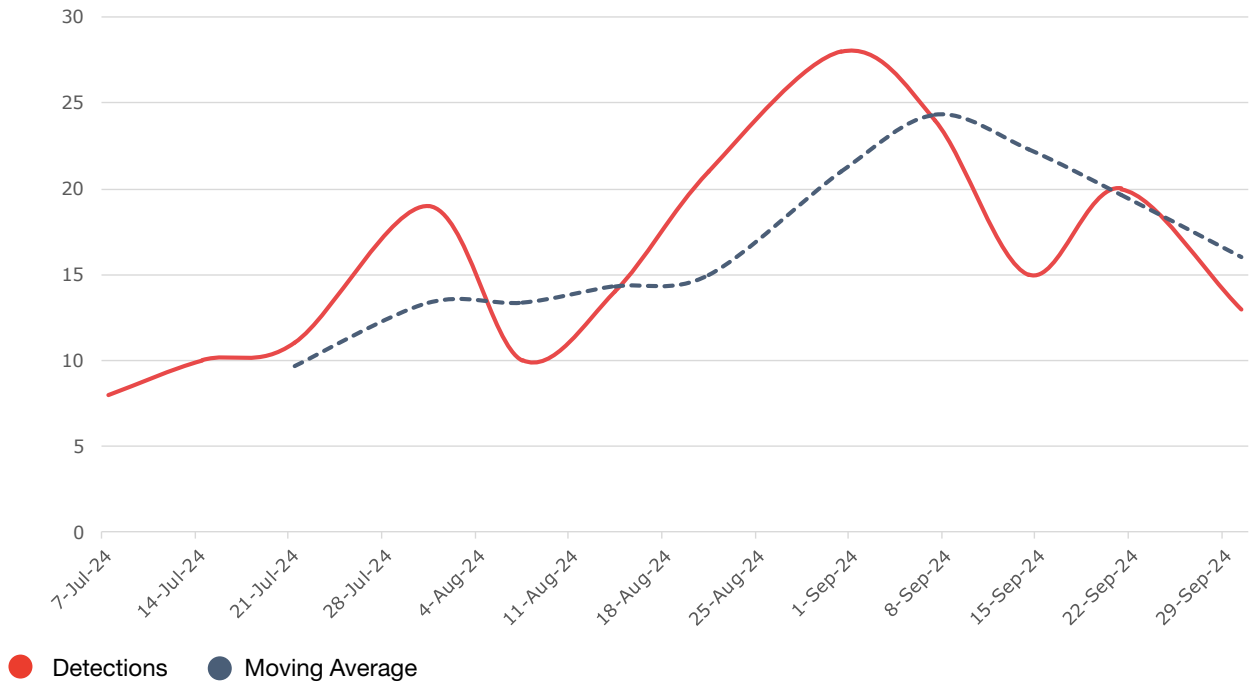


FIGURE 3. RANSOMHUB EXTORTION PUBLICATION ACTIVITY | NUSPIRE, Q3 2024

Ransomware

RansomHub Ransomware

The Cybersecurity and Infrastructure Security Agency (CISA) released an advisory regarding RansomHub, which includes technical details and mitigation options.

RansomHub affiliates have been witnessed using multiple methods of initial access. While these techniques aren't new, they remain effective because they continue to exploit common vulnerabilities across organizations. Tactics include phishing emails [T1566], exploitation of known vulnerabilities [T1190], and the use of database breaches to password spray compromised credentials [T1110.003].

Affiliates have abused multiple vulnerabilities, some over five years old, to gain initial access. Below is a list of known exploited vulnerabilities targeted by their campaigns:

CVE-2023-3519 – Citrix ADC (NetScaler) Remote Code Execution

CVE-2023-27997 – FortiOS Heap-Based Buffer Overflow

CVE-2023-46604 – Java OpenWire Protocol Remote Code Execution

CVE-2023-22515 – Confluence Data Center and Server Creation of Accounts

CVE-2023-46747 – BIG-IP Authentication Bypass

CVE-2023-48788 – Fortinet FortiClientEMS SQL Injection

CVE-2017-0144 – Windows SMBv1 Remote Code Execution

CVE-2020-1472 – Netlogon Remote Protocol Privilege Escalation

CVE-2020-0787 – Zerologon Privilege Escalation

Once the threat actor gains access to the network, they use various tools for reconnaissance, persistence, lateral movement and exfiltration. A list of known tools used by the group can be found below:

- BITSAdmin
- Cobalt Strike
- Mimikatz
- PSExec
- PowerShell
- RClone
- Sliver
- SMBExec
- WinSCP
- CrackMapExec
- Kerberoast
- AngryIPScanner

Below is a comprehensive list of known tactics, techniques and procedures (TTPs) used by RansomHub affiliates. It's important to note that since affiliates purchase access to RansomHub, their operations can vary, and they often adapt their tactics based on what proves most successful for them.

Common Tactics, Techniques & Procedures (TTPs) for RansomHub

RESOURCE DEVELOPMENT	
Obtain Capabilities: Exploits	T1588.005
INITIAL ACCESS	
Exploit Public-Facing Application	T1190
Phishing	T1566
Valid Accounts	T1078
EXECUTION	
Command and Scripting Interpreter: PowerShell	T1059.001
Windows Management Instrumentation	T1047
PERSISTENCE	
Command and Scripting Interpreter: PowerShell	T1059.001
Create Account	T1136
PRIVILEGE ESCALATION	
Account Manipulation	T1098
Remote Services: Remote Desktop Protocol	T1021.001
DEFENSE EVASION	
Masquerading	T1036
Impair Defenses: Disable or Modify Tools	T1562.001
Indicator Removal on Host	T1070
CREDENTIAL ACCESS	
Brute Force: Password Spraying	T1110.003
OS Credential Dumping	T1003
DISCOVERY	
Network Service Discovery	T1046
Remote System Discovery	T1018
LATERAL MOVEMENT	
Remote Services: Remote Desktop Protocol	T1021.001
Exploitation of Remote Services	T1210
COMMAND & CONTROL	
Remote Access Software	T1219
EXFILTRATION	
Exfiltration Over Alternative Protocol: Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	T1048.002
Transfer Data to Cloud Account	T1537
Exfiltration Over Alternate Protocol: Exfiltration Over Asymmetric Unencrypted Non-C2 Protocol	T1048.003
IMPACT	
Data Encrypted for Impact	T1486
Inhibit System Recovery	T1490

FIGURE 4. COMMON RANSOMHUB RANSOMWARE TTPS | NUSPIRE, Q3 2024

Ransomware

Professional & Technical Services Overtakes Manufacturing as Top Targeted Industry

The Professional & Technical Services industry, which comprises organizations such as law firms, accounting firms, consulting agencies, human resources firms and marketing firms, has overtaken the manufacturing industry as the top ransomware target in Q3.

These firms handle highly sensitive client data, such as financial records, legal documents and business strategies, making them prime targets for ransomware operators. The rise of double-extortion tactics heightens the pressure, as the exposure of this confidential information can cause severe reputational damage, prompting victims to pay to keep it from going public.

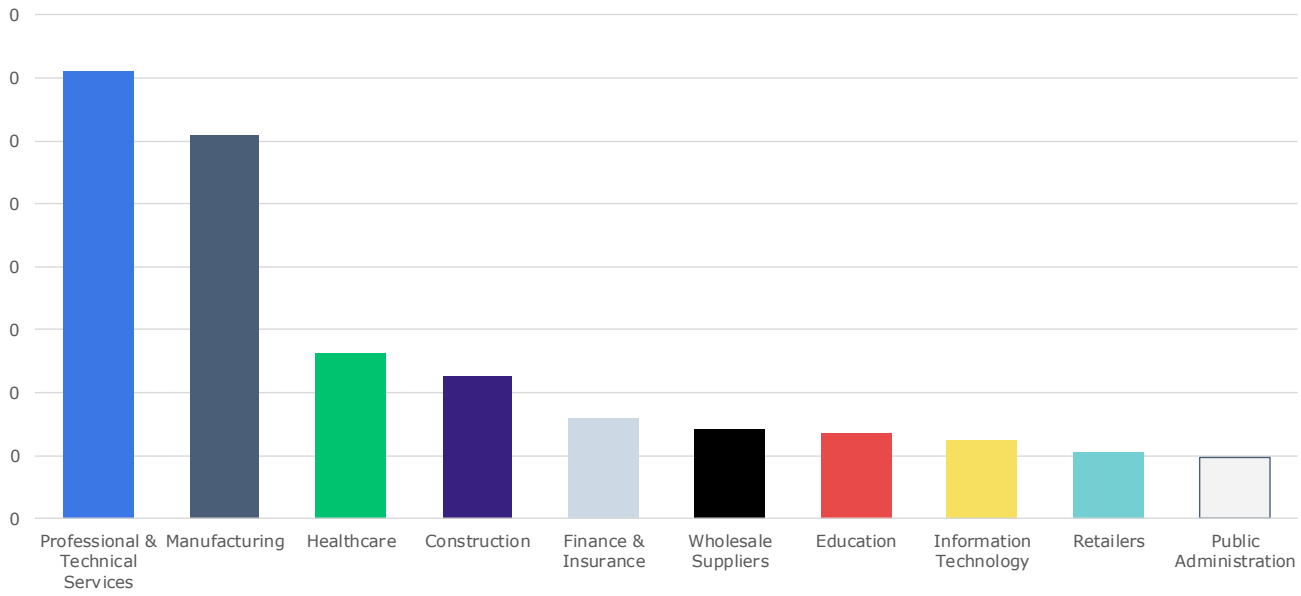


FIGURE 5. RANSOMWARE EXTORTION PUBLICATIONS BY INDUSTRY | NUSPIRE, Q3 2024

Many of these organizations fall under the small-or medium-sized business category, and often lack the robust cybersecurity investments seen in larger enterprises. This underinvestment, coupled with outdated technology, weaker policies and slower adoption of advanced security tools, leaves them more vulnerable to attacks. Ransomware operators typically go after easy targets, using proven methods that still yield high returns with minimal effort.

With ransom demands **averaging around $2.5 million** for law firms, ransomware operators will continue to target this industry as long as the potential rewards outweigh the effort.

Ways to Combat These Threats

Ransomware threats are constantly evolving, using various tactics like phishing to exploit vulnerable systems. Addressing these threats necessitates a strategic approach focused on preemptive measures, advanced technological defenses and informed human behavior.

Endpoint detection and response (EDR)

EDR systems not only help prevent malware attacks through advanced threat detection mechanisms, but also offer detailed forensic capabilities and automated response actions to isolate infected endpoints and prevent the spread of ransomware. This approach ensures prevention as well as effective management of threats that penetrate the initial defenses.

Data backup and recovery plan

Organizations should implement robust, regularly updated and securely stored backups. This practice enables organizations to recover critical data without paying the ransom in the event of an attack. Backups should be encrypted, stored off-site or stored in a cloud service that is not directly accessible from the network to protect them from being compromised.

Cybersecurity awareness

Regular, engaging and comprehensive cybersecurity awareness training is essential for all employees. It should include simulated phishing exercises, updates on the latest cyber threat tactics and clear instructions on what to do if a potential security threat is detected. It is crucial that a security-focused culture is created within your organization.

Q3 2024 Dark Web Events

3,244,066 Total Marketplace Listings

1,972,372

listings of stolen browser data

695,709

listings of credit cards for sale

86,325

listings of email account access for sale

42,559

listings of social security numbers for sale

27,748

listings of shell access for sale

40,029

listings of RDP access for sale

28,512

listings of stolen accounts for sale

-5.41%

decrease in total listings from Q2

Dark Web

Dark Web Marketplaces See Lumma Stealer Rise Again as Top Infostealer

Nuspire regularly monitors dark web marketplaces, which are online forums or platforms operating on parts of the internet not indexed by traditional search engines. These marketplaces require special configurations and sometimes authorization to access. By monitoring this activity, Nuspire can identify trends in marketplace sales and the types of information-stealing malware (infostealers) commonly used by threat actors.

The dotted line in Figure 6 shows the moving average of dark web marketplace listings for sale throughout the third quarter. It's important to recognize that a single listing may include multiple data sets, meaning it doesn't fully reflect the extent of data being sold, but it does provide a clear indicator of marketplace activity levels.

Compared to Q2, marketplace listings dropped by **5.41%**, largely due to a decline in postings offering scraped browser data for sale.

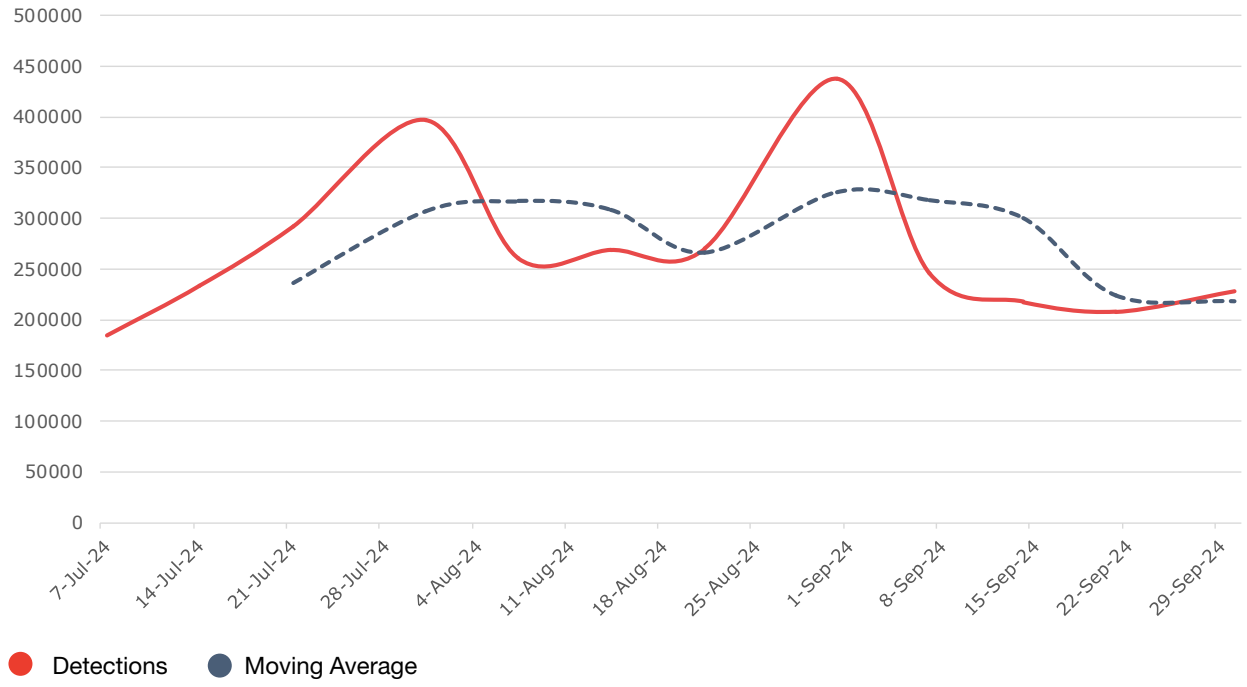
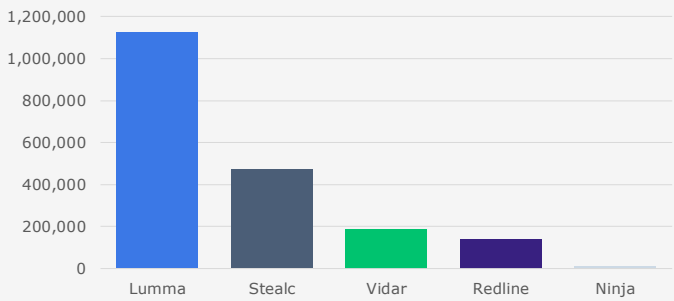


FIGURE 6. DARK WEB MARKETPLACE ACTIVITY Q3 | NUSPIRE, Q3 2024



Data on dark web marketplaces frequently originates from data breaches or infostealer malware. Figure 7 analyzes marketplace listings to highlight the top five infostealers that collect data from compromised machines. This insight can help inform threat hunting efforts and pinpoint common deployment methods, which can be incorporated into cybersecurity awareness training.

FIGURE 7. TOP FIVE INFOSTEALERS | NUSPIRE, Q3 2024

Dark Web

Lumma Stealer

Infostealers remain popular among threat actors due to their ability to harvest sensitive information from victim devices, especially stored credentials and financial information. This stolen information creates a lucrative opportunity for threat actors, allowing them to quickly profit by selling the data to others while avoiding the increased risk and complexity of carrying out a more in-depth attack themselves. These sellers, known as initial access brokers, gain access to user or organizational credentials and post them for sale. Once purchased, other threat actors can swiftly exploit this information to achieve their objectives, often resulting in ransomware attacks and data exfiltration.

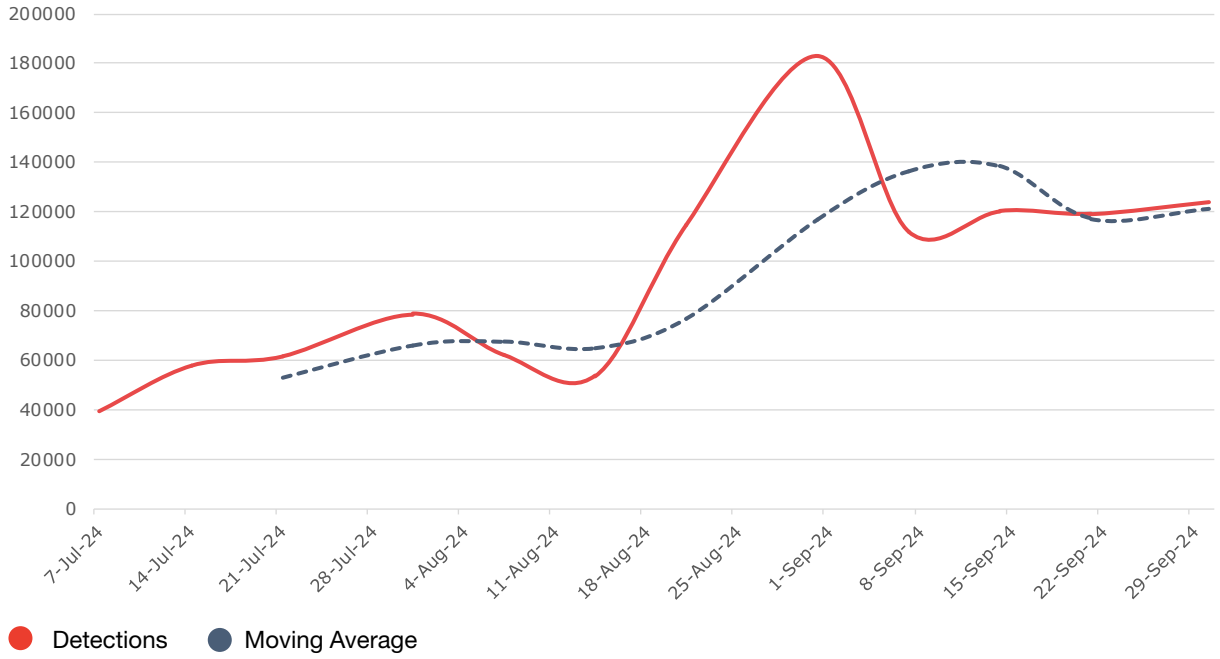


FIGURE 8. LUMMA STEALER ACTIVITY | NUSPIRE, Q3 2024

Lumma, a once-popular infostealer variant that remained unusually quiet during Q2, made a powerful comeback in Q3, overshadowing its competitors.

Lumma is primarily delivered through phishing emails, malicious downloads disguised as legitimate software, or pirated software. In 2024, campaigns targeting the transportation and logistics industries were observed using malicious Google Drive URLs embedded directly in email messages to deliver Lumma payloads. Once executed, the malware connects to a remote server, downloads Lumma and installs it on the victim's device. Nearly all of the stolen data associated with Lumma ends up for sale on Russian Market.

Russian Market is a threat actor-driven platform that offers vast amounts of stolen data for sale, accessible through both the clear web and dark web. New users must deposit cryptocurrency before gaining access to the listings, but once inside, they can purchase credentials, credit card details, organizational access and various hacking tools. Some credentials are priced as low as $10, making it an accessible marketplace for a range of cybercriminals.

Organizations can leverage dark web monitoring services to receive alerts when their domains, credentials or sensitive information appear in underground marketplaces. This proactive approach provides valuable time to respond to emerging threats and detect data transfers before they escalate.

Ways to Combat These Threats

Data sales on the dark web and the threat of infostealer malware require proactive and robust security measures.

Implement comprehensive cybersecurity measures

Strengthen your defenses against infostealer malware by employing a layered cybersecurity strategy. This should include the use of advanced antivirus solutions that utilize machine learning and behavioral analysis to detect and block malware before it can exfiltrate data. Employ firewalls, secure web gateways and email security solutions to filter out malicious traffic and phishing attempts. Regularly update and patch all software to close vulnerabilities that attackers could exploit.

Enhance data protection and privacy

To prevent sensitive information from being sold on the dark web, it's crucial to minimize the amount of data shared online and ensure that the data is encrypted. Use end-to-end encrypted messaging services for sensitive communications and enable encryption on all devices. Additionally, employ strong, unique passwords for all accounts, complemented by multi-factor authentication (MFA), to add an extra layer of security. Consider using a reputable password manager to securely store and manage your passwords.

Implement Dark Web monitoring and threat intelligence

Regularly monitor dark web marketplaces to gain insights into emerging threats and the sale of stolen data. By doing so, organizations can avoid potential risks and implement timely preventive measures. Integrate threat intelligence platforms to correlate dark web findings with internal network activity, identifying possible compromises early on. This proactive approach enhances incident response capabilities and helps identify vulnerabilities before they can be exploited by cybercriminals.

Educate and train on phishing and social engineering attacks

Since many infostealer malware infections originate from phishing or social engineering tactics, educating yourself and your organization's users about recognizing and responding to these threats is vital. Conduct regular training sessions that include the latest phishing techniques and provide clear guidelines on what to do if a suspicious email or message is received. Simulated phishing exercises can also help users practice their response to attempted attacks, thereby reducing the likelihood of successful infections.

Q3 2024 Exploitation Events

16,964,624 Total

1,192

unique exploits detected

1,413,718

exploit attempts detected per week

201,959

exploit attempts detected per day

50.96%

increase in total activity from Q2

Exploits

VPN Technology Hit Hard as Exploit Attempts Climb by Over 50%

Figure 9 provides a visual representation of the trends in exploitation activity throughout the third quarter. The dashed line shows the moving average of this activity, while the solid line shows the actual weekly figures, highlighting any unusual spikes in the data.

When comparing Q2 to Q3, Nuspire witnessed another quarter of growing exploit activity, increasing by over **50%**. Of particular note, Nuspire saw a surge of activity against VPN-based vulnerabilities, dwarfing previous detections.

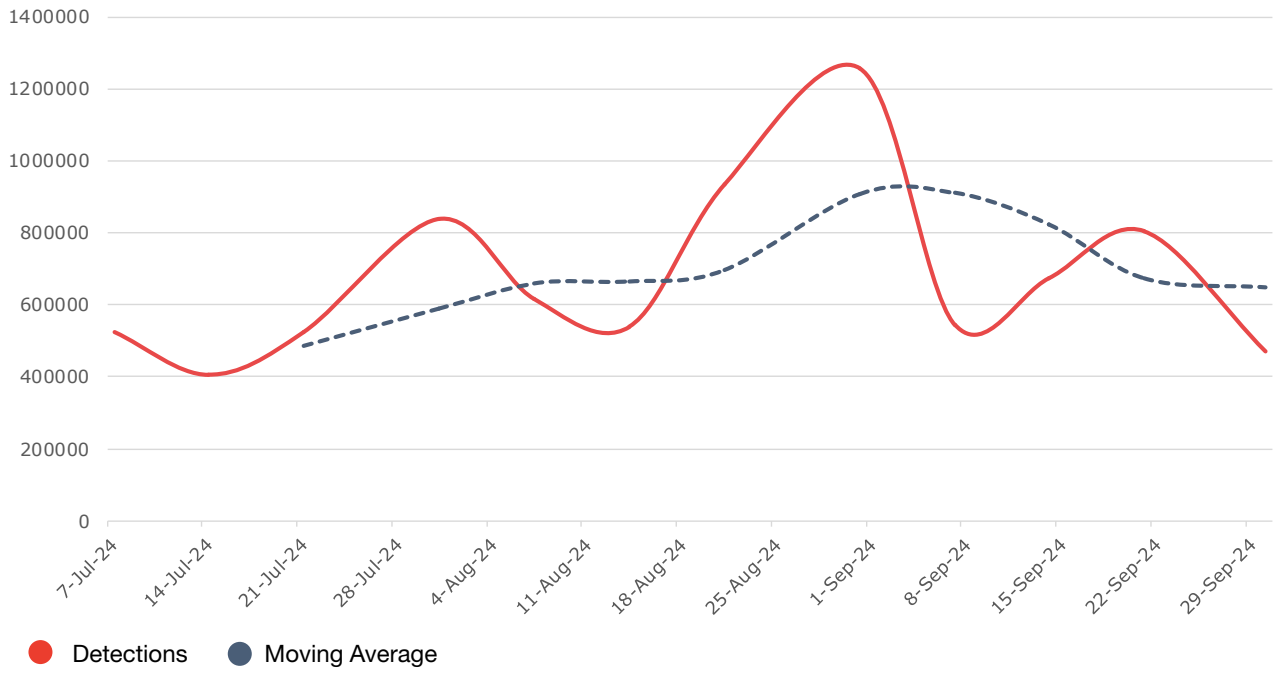


FIGURE 9. Q3 EXPLOIT ACTIVITY | NUSPIRE, Q3 2024

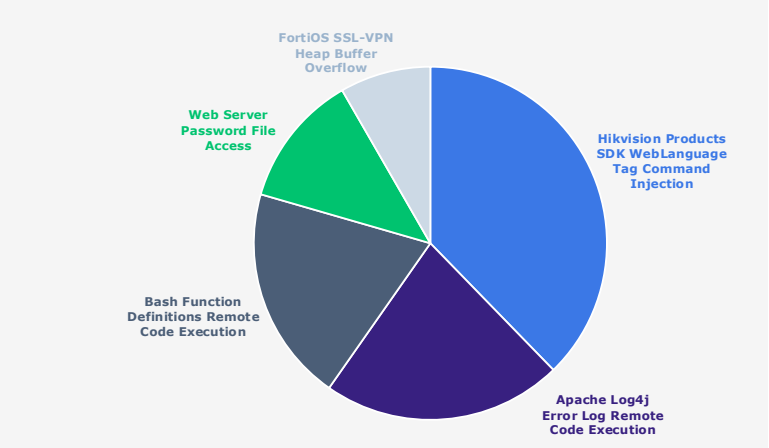


Figure 10 highlights the most frequent exploit attempts observed in Q3. Leading the list is the Hikvision Product SDK WebLanguage Tag Command Injection vulnerability (CVE-2021-36260), signaling a renewed interest in targeting IoT devices. Apache's Log4j, despite being several years old, continues to be a go-to exploit for threat actors. A notable newcomer to the top five is the Fortinet FortiOS SSL-VPN Heap Buffer Overflow vulnerability (CVE-2022-42475), driven by a significant increase in attack attempts compared to Q2. To provide a clearer analysis of the data, the overwhelming number of brute force attacks has been excluded from this report.

FIGURE 10. Q3 TOP WITNESSED EXPLOITS | NUSPIRE, Q3 2024

Exploits

Surge in VPN Vulnerability Attacks

During Q3, Nuspire saw a dramatic uptick in attacks attempted against VPN technologies. The largest waves of attacks targeted CVE-2022-42475. This vulnerability impacts Fortinet's FortiOS SSL-VPN, a widely used technology for secure remote access. It exploits a heap-based buffer overflow, allowing attackers to send malicious requests that overflow the system's memory and alter the software's normal behavior.

In this case, attackers can execute unauthorized commands, giving them control over the device. Once inside, they can pivot within the network, launching further attacks such as installing malware, deploying ransomware, exfiltrating data or disrupting operations.

While this vulnerability was the largest offender, Nuspire also witnessed attempts against other VPN-based vulnerabilities. In total, there was an over **4,000%** increase in attempts to exploit VPN technologies compared to attempts in Q2.

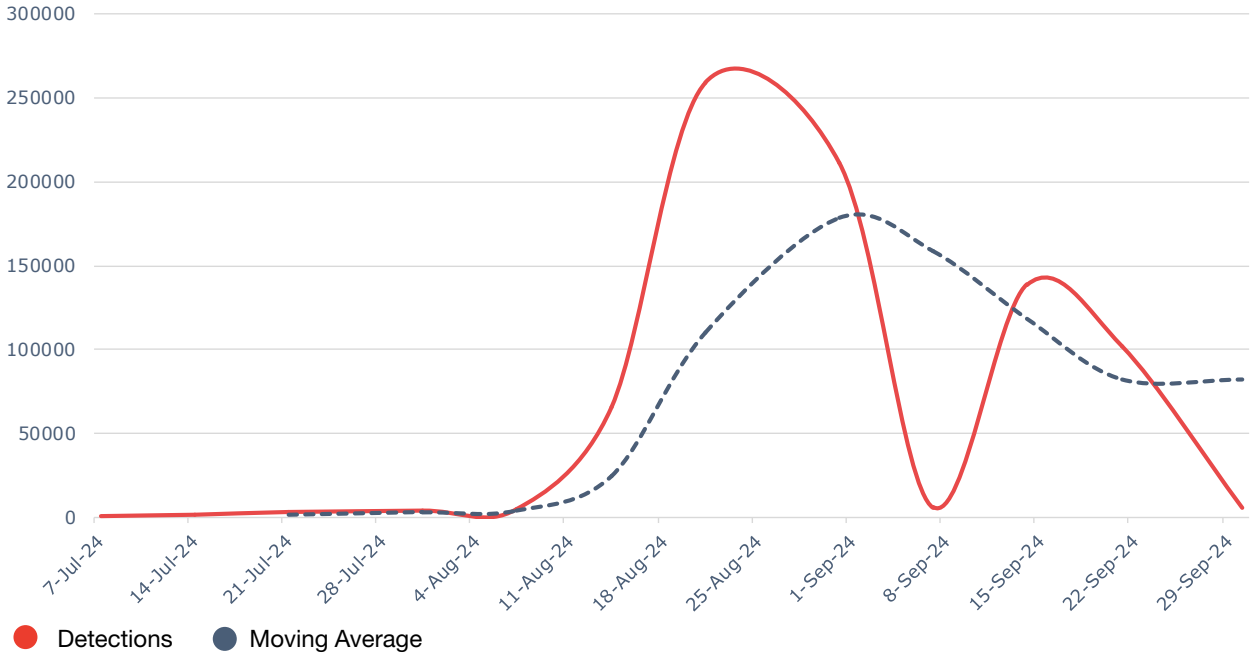


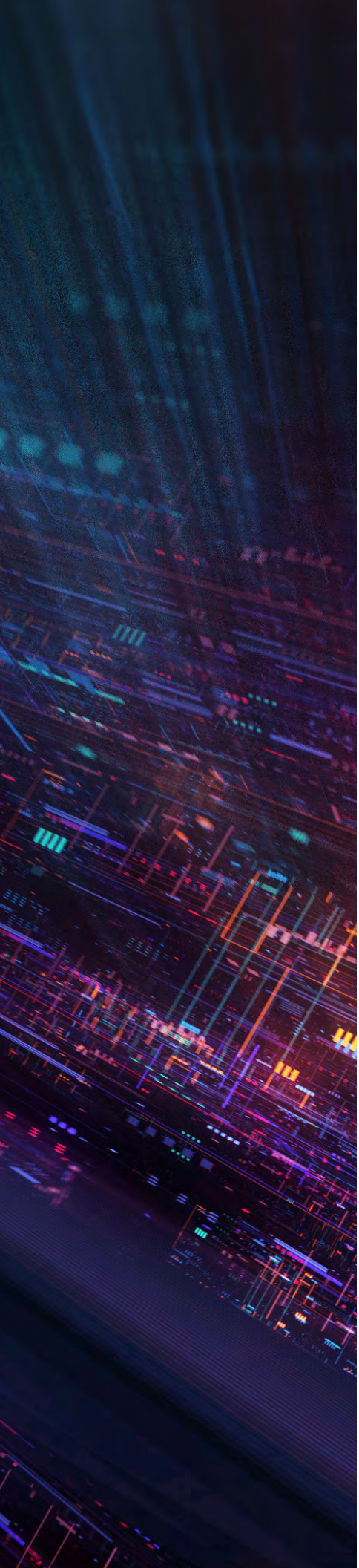
FIGURE 11. Q3 FORTINET FORTIOS SSL-VPN HEAP BUFFER OVERFLOW | NUSPIRE, Q3 2024

Many VPN-based attacks rely on brute force or stolen credentials, but threat actors also understand that exploiting vulnerabilities to gain control of a device offers a direct route into an organization. The challenges of patching these devices, often causing service disruptions, can leave them vulnerable to exploitation—an opportunity attackers are eager to exploit.

Organizations must prioritize patching critical infrastructure, like VPNs, as soon as vulnerabilities are disclosed. Threat actors often exploit delays caused by concerns over service disruptions, waiting to strike vulnerable systems when patching is postponed.

Below is a ranked list of all VPN attacks observed by Nuspire in Q3, organized from the highest to lowest frequency.

ATTACK NAME	ASSOCIATED CVE	VENDOR
SSL-VPN Heap Buffer Overflow	CVE-2022-42475	Fortinet
SSL-VPN Web Portal Information Disclosure	CVE-2018-13379	Fortinet
SSL-VPN HTML5 Information Disclosure	CVE-2019-11510	Ivanti
VPN Directory Traversal	CVE-2019-19781	Citrix
HTTP Server Information Disclosure	CVE-2018-3949	TP-Link



Microsoft Patch Tuesday Q3 2024 Summary

The global prevalence of Microsoft products is well-known, making their platforms a prime target for threat actors. Cybercriminals are quick to exploit any newly announced or discovered vulnerabilities, turning them into valuable tools in their arsenal. Below is the latest list of zero-day vulnerabilities announced by Microsoft in Q3.

DESCRIPTION	CVE	CVSS SCORING
Escalation Privilege in Windows Hyper-V	CVE-2024-38080	7.8
Weakness in MSHTML	CVE-2024-38112	7.5
Windows Kernel Information Disclosure	CVE-2024-37985	5.6
HTTP/3 Vulnerability in .NET and Visual Studio	CVE-2024-35264	8.1
Scripting Engine Memory Corruption	CVE-2024-38178	7.5
Windows Ancillary Function Driver Elevation of Privilege	CVE-2024-38193	7.8
Windows Mark of the Web Bypass	CVE-2024-38213	6.5
Windows Kernel Elevation of Privilege	CVE-2024-38106	7.0
Windows Power Dependency Coordinator Elevation of Privilege	CVE-2024-38107	7.8
Microsoft Project Remote Code Execution	CVE-2024-38189	8.8
Windows Line Printer Daemon Remote Code Execution	CVE-2024-38199	9.8
Windows Secure Kernel Mode Elevation of Privilege	CVE-2024-21302	6.7
Microsoft Office Spoofing Vulnerability	CVE-2024-38200	9.1
Windows Update Stack Elevation of Privilege	CVE-2024-38202	7.3
Windows Installer Elevation of Privilege	CVE-2024-38014	7.8
Windows Mark of the Web Security Feature Bypass	CVE-2024-38217	5.4
Microsoft Publisher Security Feature Bypass	CVE-2024-38226	7.3
Microsoft Windows Update Remote Code Execution	CVE-2024-43491	9.8

FIGURE 11. Q3 MICROSOFT ZERO-DAYS | NUSPIRE, Q3 2024

Considering how often vulnerabilities are exploited, it's crucial for organizations to prioritize timely system updates. Microsoft regularly releases updates, known as Patch Tuesdays, on the second Tuesday of every month at 1 p.m. ET. IT administrators must stay informed about these updates and apply patches without delay. Clear, efficient communication about upcoming updates across the organization is crucial, allowing teams to promptly address vulnerabilities and minimize the risk of attackers exploiting these security gaps.

Microsoft Exchange Autodiscover RCE

(ProxyShell & ProxyNotShell)

During Q3, Nuspire observed significant activity targeting vulnerabilities in Microsoft Exchange Server technologies. A notable portion of the attacks focused on CVE-2022-41040 and CVE-2022-41082, part of the "ProxyNotShell" vulnerabilities. These vulnerabilities, when chained together, allow threat actors to execute remote code on vulnerable Microsoft Exchange servers. CVE-2022-41040 exploits a server-side request forgery (SSRF) flaw, which can then be leveraged to execute malicious PowerShell commands via CVE-2022-41082. This chain of attacks provides an attacker with highly privileged access, allowing them to further compromise the network by installing malware, deploying ransomware or exfiltrating data.

In addition to these newer vulnerabilities, older Exchange vulnerabilities such as CVE-2021-34473 (ProxyShell) continue to be a target for exploitation. This particular vulnerability allows remote code execution without authentication, providing attackers with a direct route into the network.

Threat actors, including ransomware groups like Play, have capitalized on these vulnerabilities, using them to gain initial access to environments where they can move laterally, steal credentials and deploy ransomware. While these attacks require initial access, threat actors often obtain valid credentials through password spraying, phishing or purchasing them via underground markets, which lowers the barrier for exploitation.

Nuspire witnessed an uptick in attempts to exploit these Exchange vulnerabilities throughout Q3, underscoring the critical need for organizations to patch systems promptly. Given the high privilege levels that successful exploitation confers, unpatched Exchange servers remain attractive targets for cybercriminals.

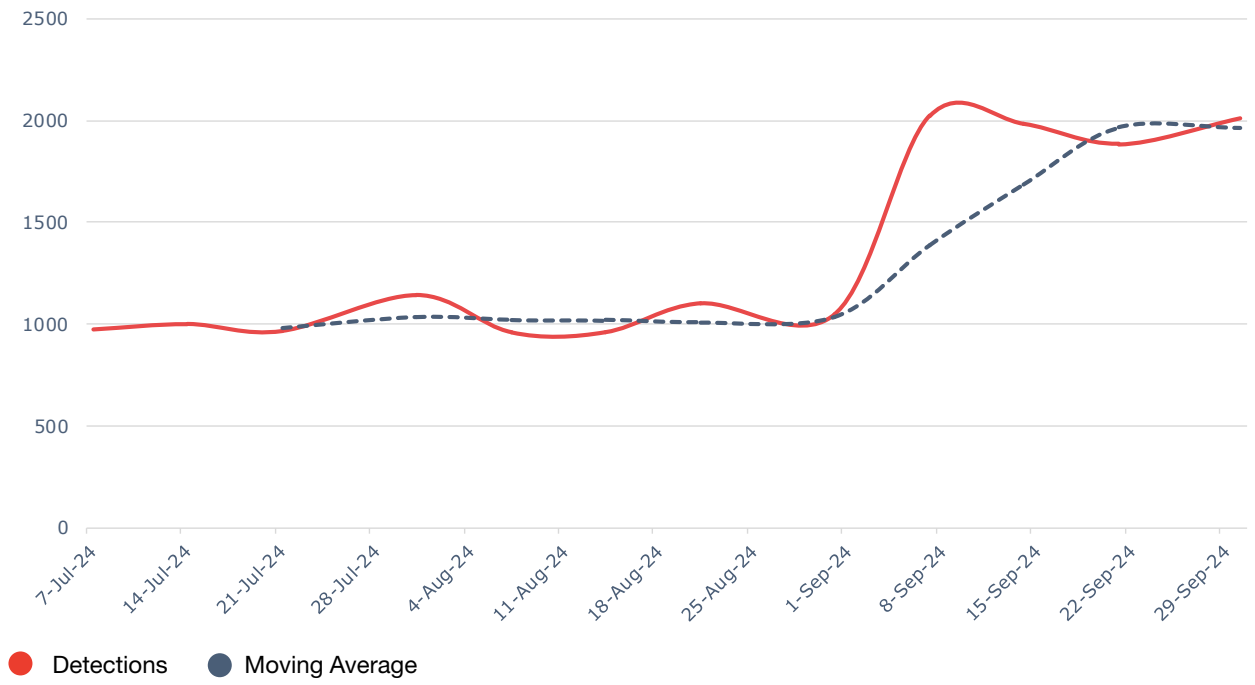


FIGURE 12. Q3 MS EXCHANGE AUTODISCOVER RCE ACTIVITY | NUSPIRE, Q3 2024

Ways to Combat These Threats

In the world of cyber threats, timely action is essential for all involved parties.

Speedy system patching is crucial

Malicious actors continually scan for organizations that haven't updated their systems and technologies with the latest patches. Therefore, it is vital for organizations to comprehend their technology stack thoroughly and promptly apply patches or mitigations as they become available. Particular focus should be given to vulnerabilities rated high or critical, especially those concerning remote access, as these are prime targets for attackers.

Install a firewall equipped with an intrusion prevention system (IPS)

Such a system can enhance network security by identifying and obstructing exploit attempts. Keeping the signature provided by your security vendor updated is essential to defend against the newest forms of attacks.

Stay informed through security news and vendor security bulletins

Protecting against new vulnerabilities is impossible without awareness of them. Organizations should consider enrolling in security bulletin services provided by most vendors, which are essential for receiving updates on patching and mitigation strategies. Regular monitoring of these updates is imperative.

Deactivate unnecessary services

Any unused service should be disabled to avoid introducing extra vulnerabilities. It's also essential for organizations to understand which services are exposed to the internet and ensure their protection through VPN technology.

Bolstering Security Amid Rising Threats and Expanding Attack Tactics

The following are five simple actions security leaders can take to safeguard their organization and reduce the risk of breach.

1. Educate all users, often.

User awareness is one of the most powerful and cost-effective ways to defend your organization from a cyberattack. Educate your end users on how to identify suspicious attachments, social engineering and scams in circulation. Inform them of common theming, including any major events that could be created into a phishing lure. Create procedures to verify sensitive business email requests (especially ones involving financial transactions) with a separate form of authentication in case an email account becomes compromised or is spoofed. Often, once an attacker has compromised an email account, they will use the account as an additional layer of "authenticity" to attack within an organization.

2. Take a layered approach to security.

uying single cybersecurity point products will not secure your business. A comprehensive 'defense in depth' approach with an integrated zero trust cybersecurity program protects businesses by ensuring that every cybersecurity product has a backup. Integrating defense components counters any gaps in other defenses of security. Utilize **vulnerability scanning** to determine your weak spots and build your security around them. Enrich your logs with threat intelligence and perform threat modeling on your organization to determine how APT groups are targeting your industry vertical.

3. Up your malware protection.

Advanced malware detection and protection technology (such as **endpoint protection and response solutions**) can track unknown files, block known malicious files and prevent the execution of malware on endpoints. Network security solutions, such as secure device management, can detect malicious files attempting to enter a network from the internet or laterally moving within a network. This advanced protection can provide threat responders additional tools like quarantining a specific device on the network and deep visibility into events happening on a device during investigations.

4. Segregate higher-risk devices from your internal network.

Internet-facing devices are high-value targets. Administrators should make sure to change the default passwords on these devices, as attackers are actively searching for devices that provide them easy access to a network. IoT devices should be inventoried, and a full understanding of your digital footprint is critical. Network segregation can help limit where an attacker can laterally move within an environment in the event of a breach.

5. Patch, patch and then patch some more.

Administrators should ensure vendor patches are applied as soon as feasible within their environments. These critical patches can secure vulnerabilities from attackers. Administrators need to monitor security bulletins from their technology stack vendors to stay on top of newly discovered vulnerabilities attackers may exploit.

Traversing the complexities of the contemporary digital landscape can pose challenges, but it need not be overwhelming. Reach out to us to secure assistance in safeguarding your organization against these recent threats.

About Nuspire

With over 25 years of expertise, Nuspire, a PDI Technologies company, is redefining cybersecurity through intelligent unification and unparalleled protection. Our company delivers innovative managed security services (MSS), managed detection and response (MDR), endpoint detection and response (EDR) and consulting solutions tailored to clients' needs. Our technology-agnostic platform provides holistic visibility across entire security tech stacks, seamlessly integrating human expertise, advanced AI and cutting-edge technologies. This comprehensive approach offers unprecedented control and predictive intelligence across clients' cybersecurity infrastructure. With features like an AI-powered assistant for streamlined operations and a mobile application for on-the-go threat management, we empower organizations to confidently navigate the evolving threat landscape. Driven by uncompromising excellence, our experts and 24x7 SOCs enable clients to stay ahead of emerging threats while optimizing their security investments.

For more information, visit **https://www.nuspire.com/** and follow the company on **LinkedIn @Nuspire**.

nuspire.com
LinkedIn @Nuspire
X/Twitter @NuspireNetworks