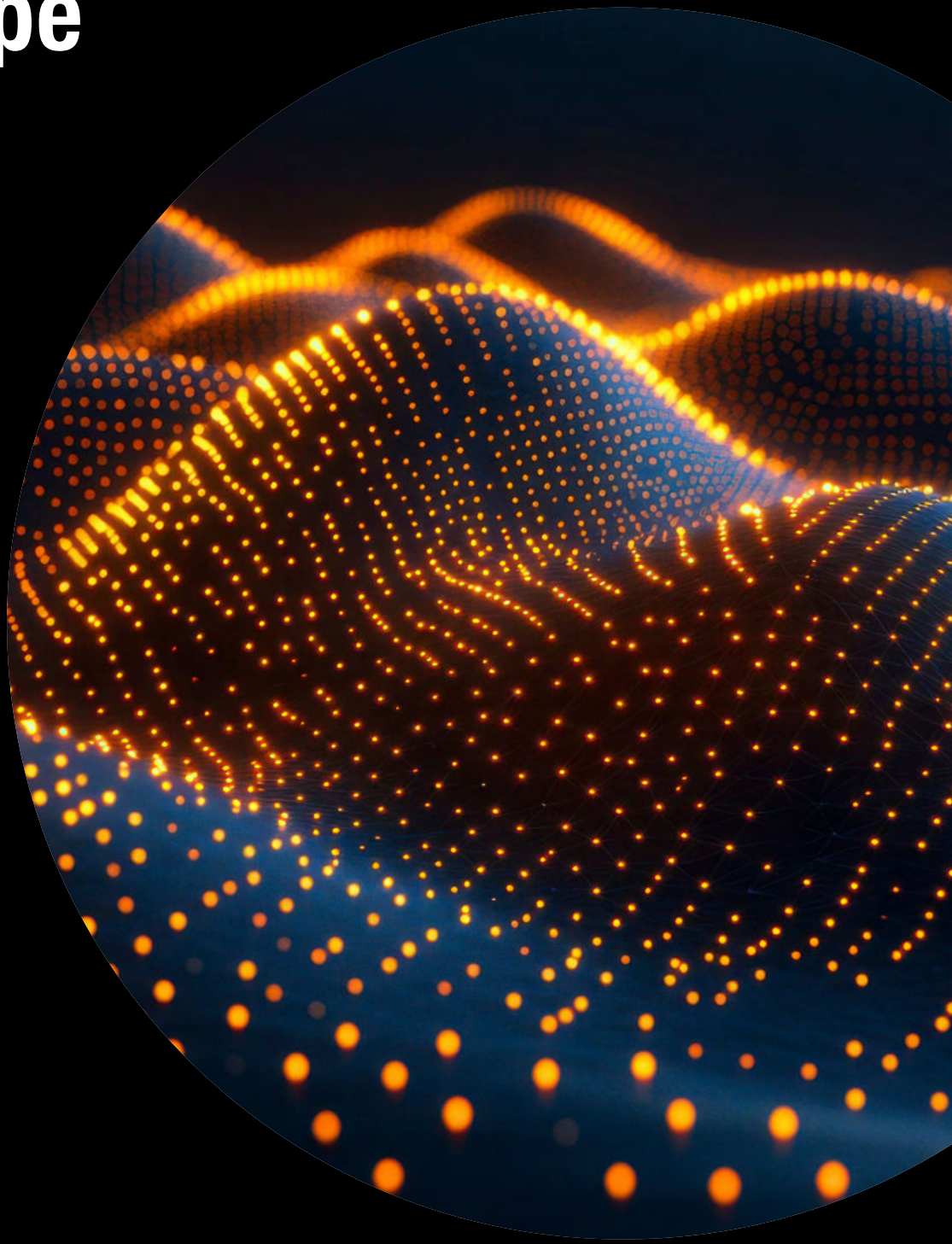
Q4 and Full-Year 2024 Threat Landscape

nuspire



Ransomware and Exploit Activities Increase While Dark Web Market Trends Shift

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:

Q4 and 2024 Year-in-Review

With Q4 and 2024 behind us, now is the perfect time to reflect on the evolving cyber threat landscape and the key trends we've observed. This past year brought significant increases in ransomware and exploitation activity, alongside shifts within dark web markets and the threat actors who leverage them. The rapid disclosure of numerous critical vulnerabilities and the speed at which attackers exploited them emphasized the urgency for proactive cybersecurity measures.

Q4 alone saw major surges in ransomware and exploitation events, with threat actors increasingly targeting vulnerabilities in firewalls, VPNs, and other critical systems. Meanwhile, dark web activity shifted as some marketplaces saw declines, while others adapted to newer, more covert methods of operation. This report delves into these developments, offering actionable insights and strategies that your organization can use to mitigate risks and strengthen its defenses in the ever-evolving threat landscape.

In early 2025, Nuspire will become **PDI Security and Network Solutions**, marking an exciting transformation for our organization and the industry as a whole. By combining 25 years of cybersecurity expertise with PDI's renowned industry leadership, we're enhancing our ability to deliver world-class security solutions. This integration will enable us to provide:

- Industry-leading managed security services protecting 2,500+ businesses
- Quarterly processing of 1+ trillion logs for comprehensive threat detection
- Management of 3,600+ firewalls and 150,000+ endpoints
- Advanced AI-powered security features through the PDI Cybersecurity Platform
- A 97% client retention rate that reflects our unwavering commitment to excellence

We are proud to continue serving as a trusted partner for organizations navigating the complexities of today's cybersecurity landscape.

Ransomware Publications

Dark Web Listings

Exploits

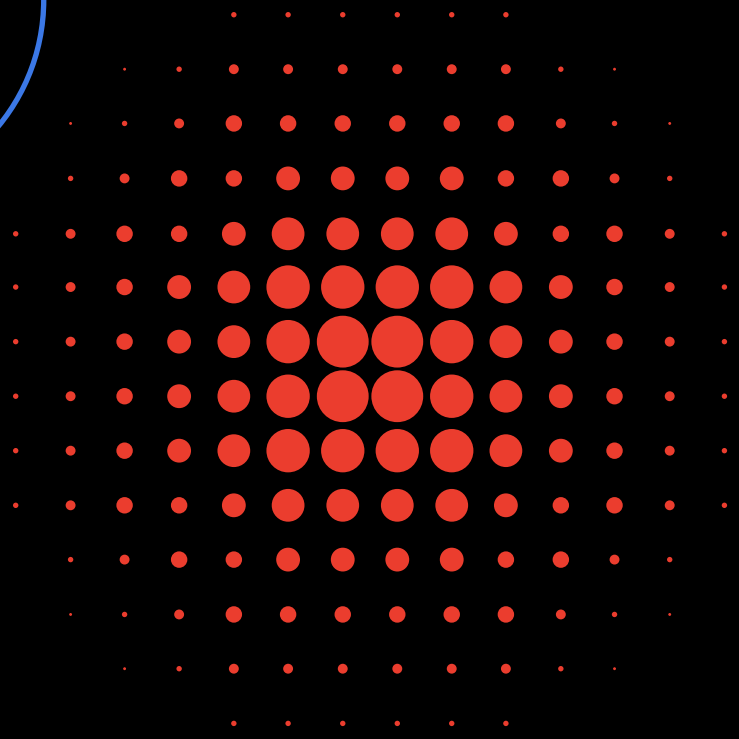
Q4 Ransomware Publications

2,247 total ransomware publications

187 publications averaged per week

26 publications averaged per day

46% increase in publications from Q3

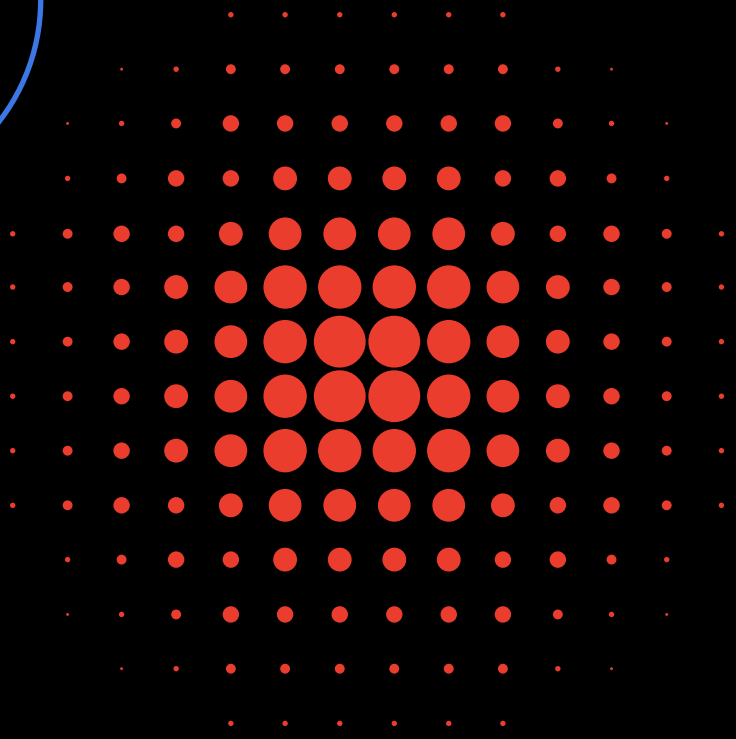


2024 Ransomware Publications

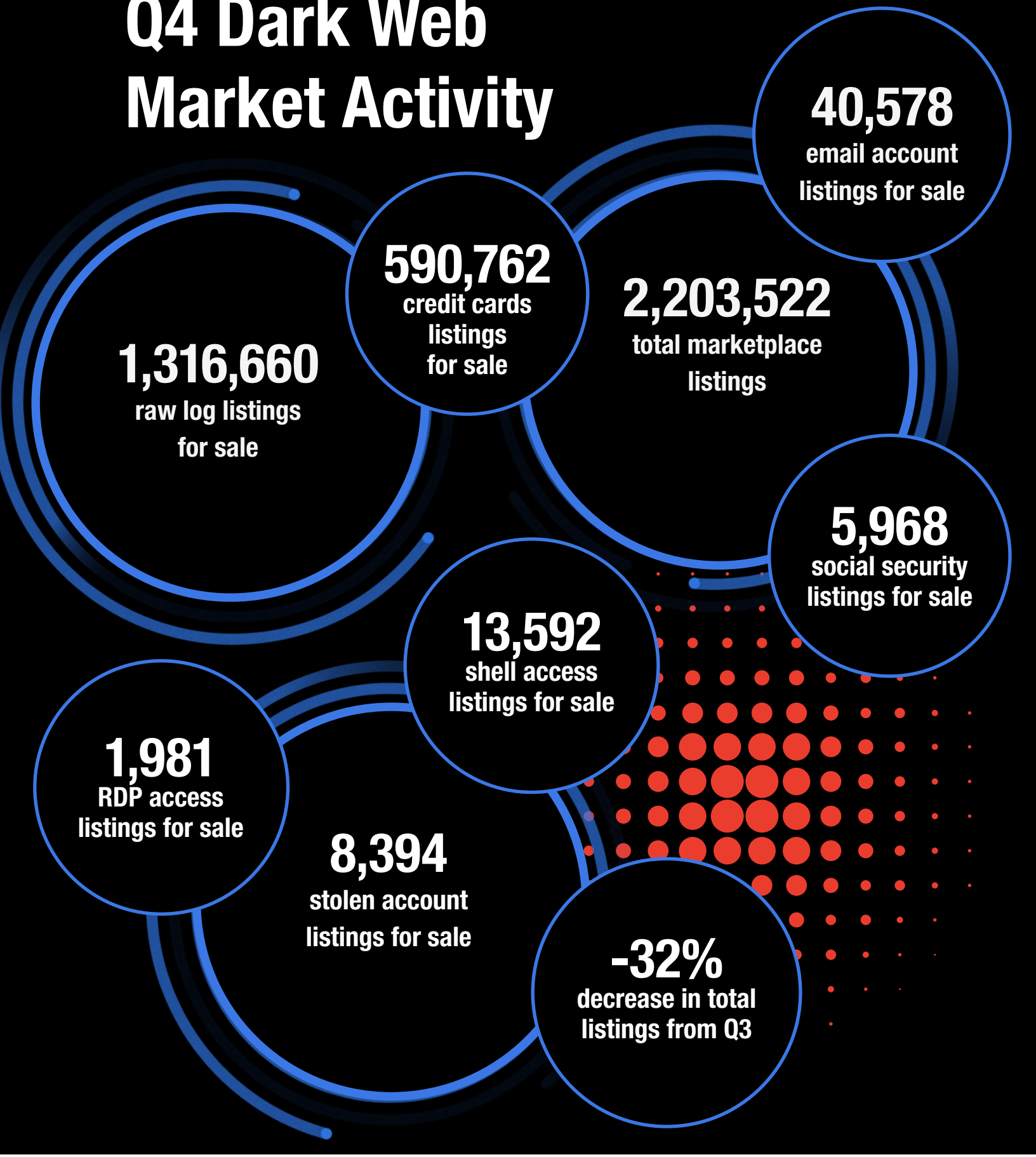
8,156 total ransomware publications

679 publications averaged per month

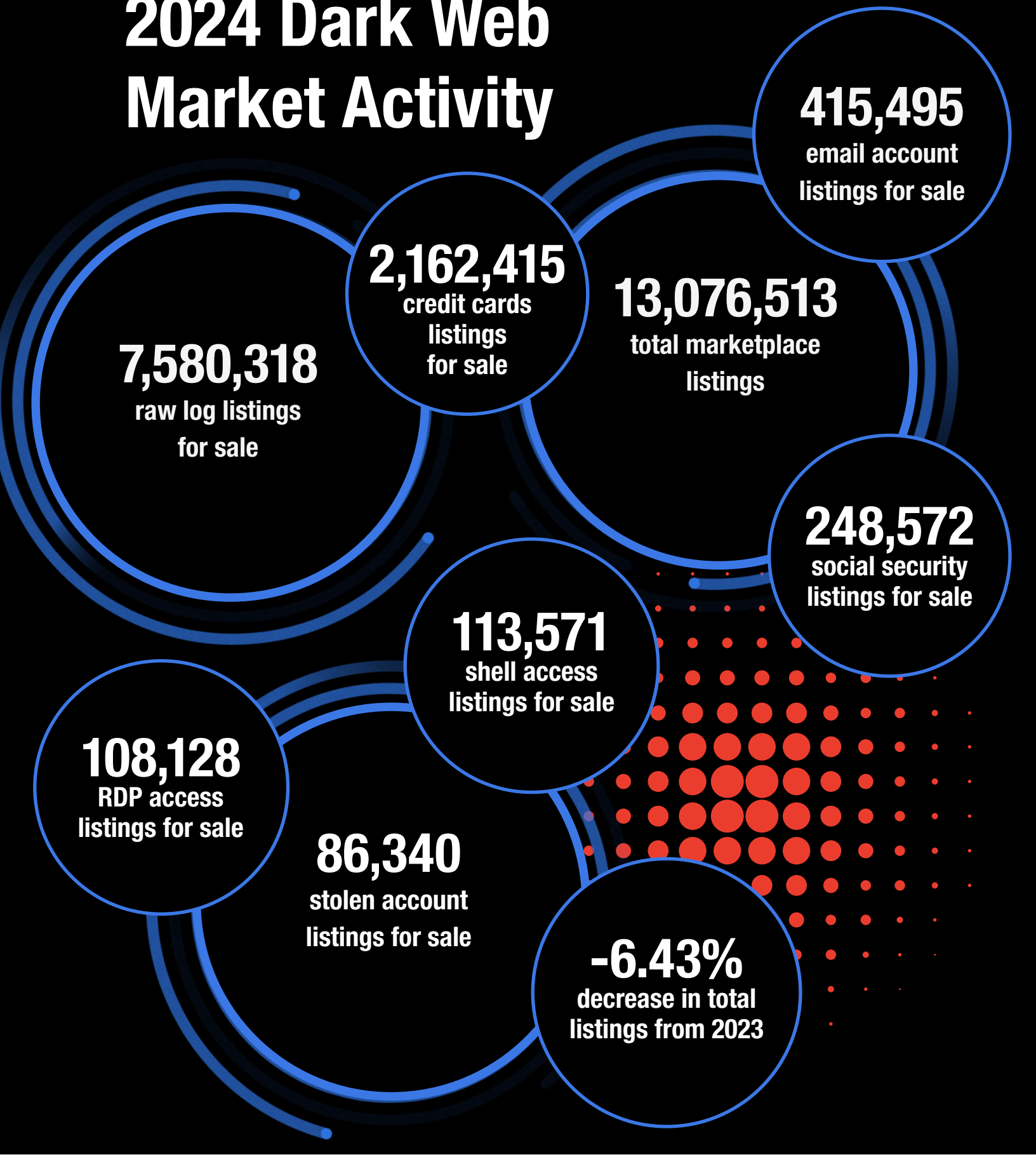
5% increase in publications from 2023



Q4 Dark Web Market Activity



2024 Dark Web Market Activity



Q4 Exploitation Events

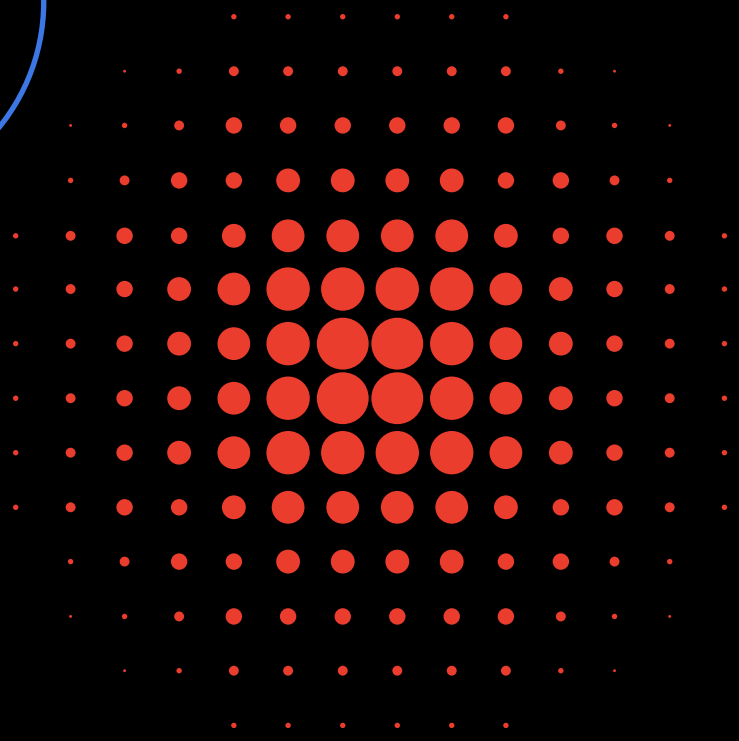
2,431,730
exploit attempts detected per week

29,180,763
total

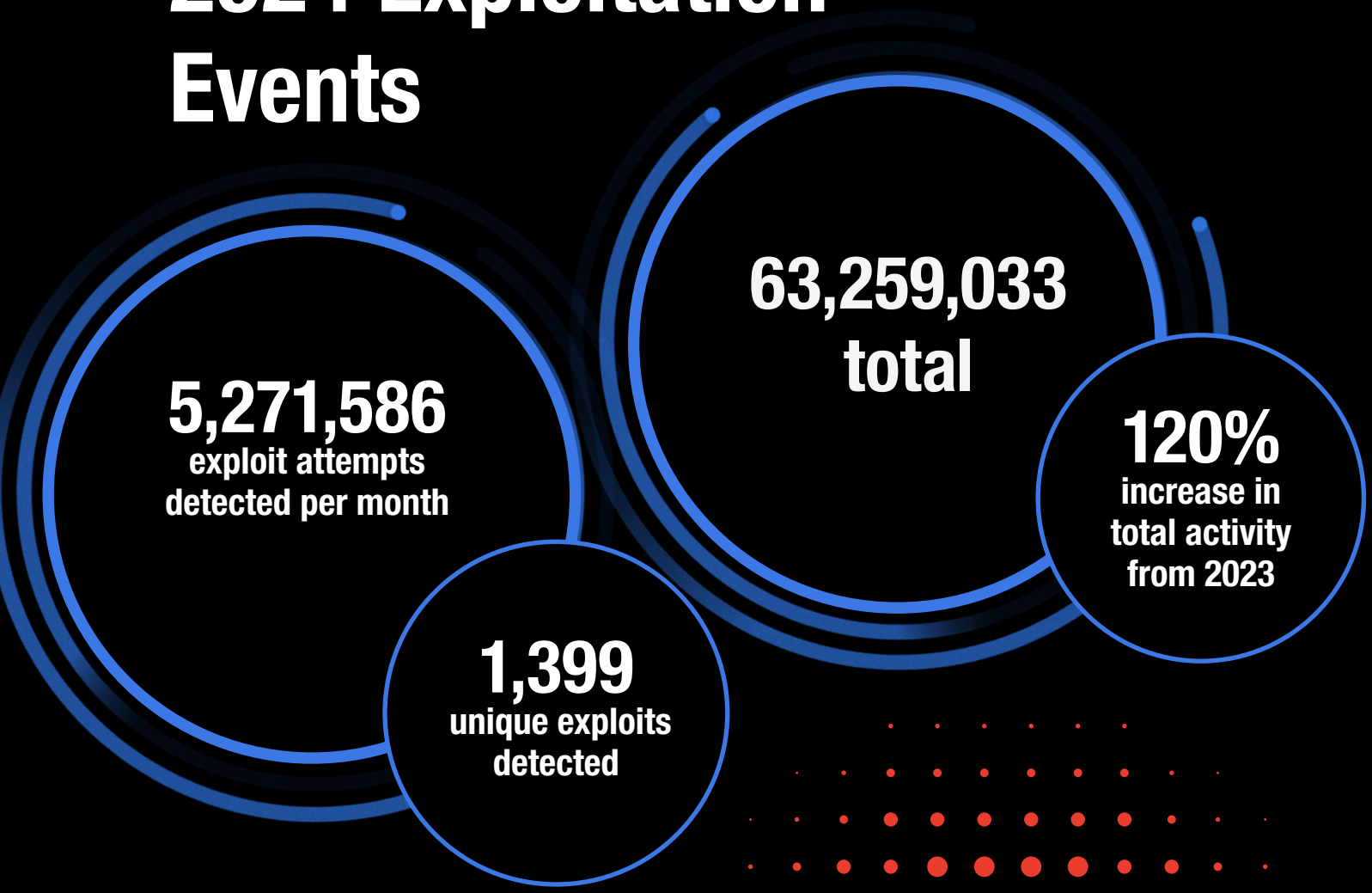
72%
increase in total activity from Q3

601
unique exploits detected

347,390
exploits detected per day



2024 Exploitation Events



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

Q4's Most Significant Threat Events

October 9
Microsoft's October Patch Tuesday Addresses 5 Zero-Days, 118 Vulnerabilities

October 11
CISA Warns of Attacks Exploiting Critical Fortinet RCE Vulnerability

October 15
CISA Warns of Threat Actors Exploiting F5 BIG-IP Cookies for Network Reconnaissance

October 22
VMware Release New Patch to Fix Critical vCenter RCE Vulnerability

October 23
Fortinet Announces Critical FortiManager Zero-Day Vulnerability

October 31
Black Basta Ransomware Uses Microsoft Teams to Breach Networks

October 31
Redline and Meta Stealers Seized by Global Operation

November 7
CISA Warns of Large-Scale Spearphishing Campaign Using RDP Files

November 8
Cisco Patches Critical Vulnerability Affected URWB Access Points

November 13
Microsoft's November Patch Tuesday Addresses 4 Zero-Days, 91 Vulnerabilities

November 19
Critical VMware vCenter Vulnerabilities Exploited in Attacks

November 26
Exploited Zero-Days Compromise Over 2000 Palo Alto Firewalls

December 4
LogoFail Exploited to Deploy Bootkitty to Infect Linux Systems

December 5
Chinese-Backed Threat Groups Target Major U.S. Telecommunications Stealing Data

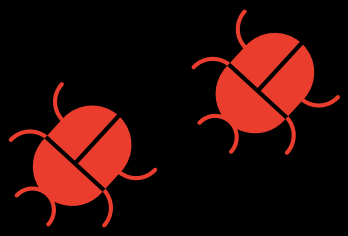
December 9
Active Exploitation of Cleo Products for Previously Patched Vulnerability

December 11
Microsoft's December Patch Tuesday Addresses 1 Zero-Day, 72 Vulnerabilities

December 12
New Patches Released for Actively Exploited Cleo Products

December 17
Critical BeyondTrust Vulnerability Receives Patches

Q4 Ransomware Extortion Publications



2,247 Total Ransomware Publications

187
publications averaged per week

26
publications averaged per day

46%
increase in publications from Q2

Ransomware

Clop Ransomware Activity Surges After Abuse of Cleo Products Zero-Day

Figure 1 shows the average Q4 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. In comparison to the third quarter, publications on ransomware extortion have risen by 46%, indicating that despite law enforcement operations, ransomware operators continue to successfully target organizations.

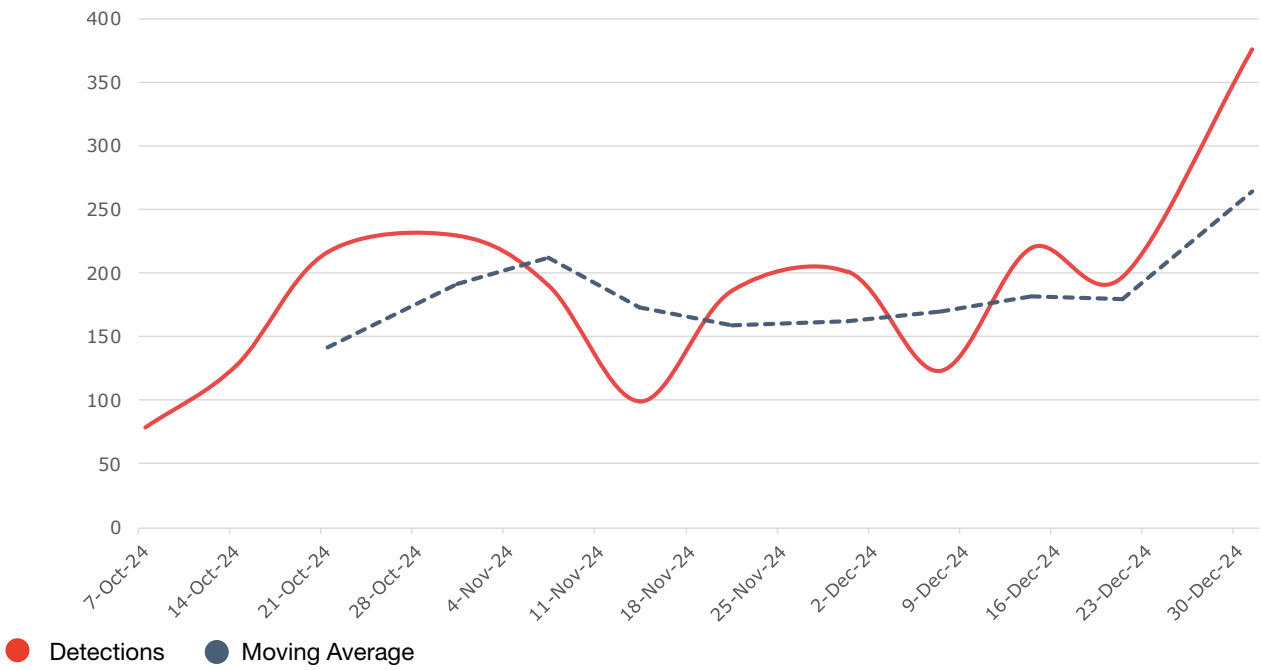
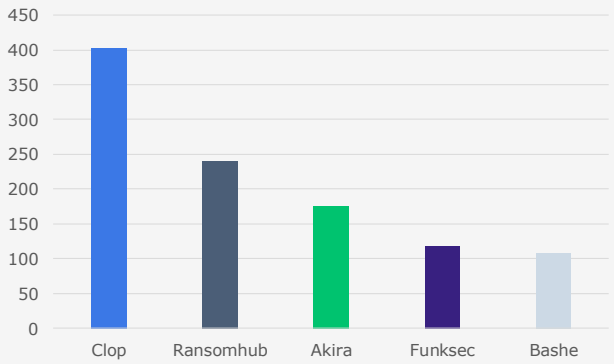


FIGURE 1. RANSOMWARE EXTORTION PUBLICATIONS | NUSPIRE, Q4 2024



As shown in Figure 2, the most active ransomware operators have shifted when compared against Q3 with Clop ransomware now taking the leading spot over Ransomhub. Meow, Play, and Qilin groups have fallen out of the most active 5, replaced by Akira, Funksec, and Bashe. As reported by Corvus Insurance, cybersecurity ransomware policy claims against these groups surged, especially in the month of November.

FIGURE 2. FIVE MOST ACTIVE RANSOMWARE OPERATORS NUSPIRE, Q4 2024

Ransomware

Clop Ransomware Surges to Lead Operator Abusing Cleo Products Zero-Day

Clop ransomware, first identified in 2019, remains a significant threat to organizations worldwide. Originating as a variant of CryptoMix ransomware, Clop encrypts files and demands substantial ransoms, often targeting high-value organizations. In addition to encryption, Clop is notorious for its "double extortion" tactic: threatening to leak stolen data if demands are unmet. This quarter, Clop demonstrated its continued evolution and sophistication by exploiting multiple zero-day vulnerabilities, underscoring its status as a significant ransomware threat.

The Clop ransomware gang has focused on exploiting vulnerabilities in managed file transfer (MFT) platforms, a tactic that has proven highly effective in breaching organizations. In Q4 2024, the group leveraged two zero-day vulnerabilities—CVE-2024-50623 and CVE-2024-55956—in Cleo's Harmony, VLTrader, and LexiCom platforms. These flaws enabled unauthorized file uploads and remote code execution, allowing Clop to establish backdoors and exfiltrate sensitive data. Despite vendor patches, researchers noted that initial fixes were inadequate, highlighting the challenge of defending against rapidly evolving threats.

The latest campaign compromised numerous organizations, with Clop using its dark web portal to publicly pressure victims into negotiations. The gang listed 66 partial company names and issued ultimatums, threatening full exposure if demands were ignored. This aggressive public shaming strategy is consistent with Clop's history of targeting prominent organizations, demanding ransoms as high as $20 million, and leveraging leaked data as proof of compromise.

Clop has increasingly relied on zero-day vulnerabilities as a primary attack vector. Their previous campaigns included exploiting vulnerabilities in Accellion FTA, SolarWinds Serv-U FTP, GoAnywhere MFT, and MOVEit Transfer platforms, affecting thousands of organizations globally. This specialization allows Clop to bypass traditional defenses and gain initial access to networks with minimal resistance. The group's use of vulnerabilities in widely deployed platforms amplifies the scale and impact of their operations, making them a persistent and formidable adversary.

The U.S. State Department's Rewards for Justice program currently has a $10 million bounty for information linking the Clop ransomware attacks to a foreign government.

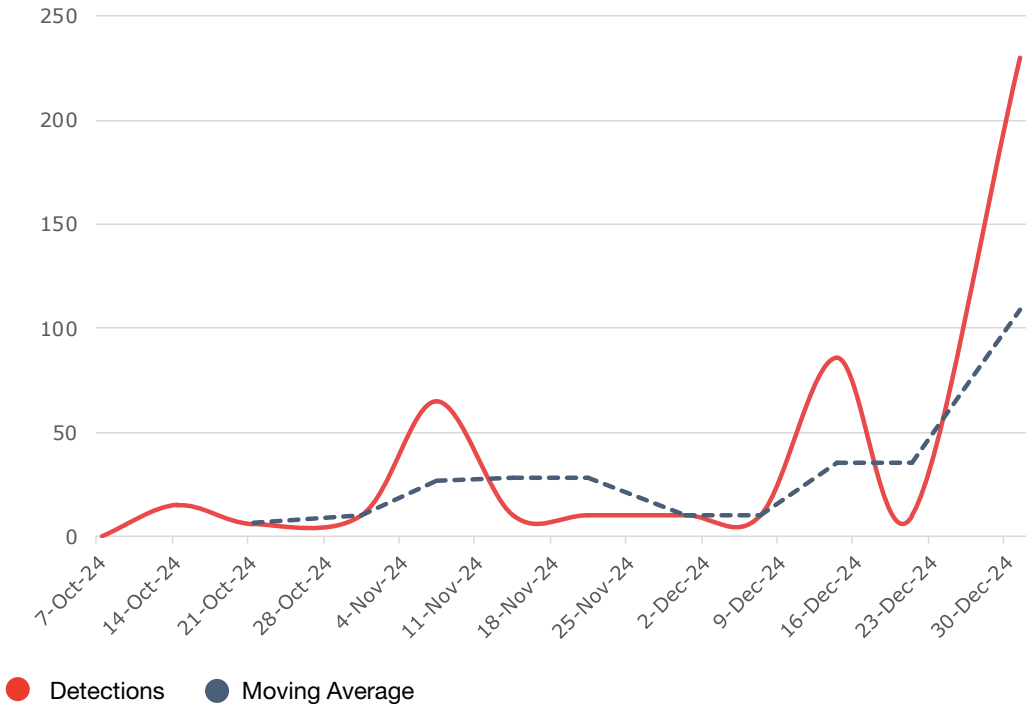


FIGURE 3. CLOP RANSOMWARE PUBLICATION ACTIVITY | NUSPIRE, Q4 2024

Ransomware

Commonly Abused Vulnerabilities

CVE-2024-50623 – Cleo Harmony & LexiCom RCE

CVE-2024-55956 – Cleo Harmon & LexiCom RCE

CVE-2023-34362 – MOVEit Transfer SQL Injection

CVE-2023-35036 – MOVEit Transfer SQL Injection

CVE-2023-35708 – MOVEit Transfer SQL Injection

CVE-2023-0669 – GoAnywhere MFT Command Injection

CVE-2021-35211 – SolarWinds RCE

CVE-2021-27101 – Accellion SQL Injection

CVE-2021-27102 – Accellion OS Command Execution

CVE-2021-27103 – Accellion SSRF Vulnerability

CVE-2021-27104 – Accellion OS Command Execution

Common Tactics, Techniques & Procedures (TTPs) for Clop Ransomware

INITIAL ACCESS	
Exploit Public-Facing Application	T1190
Phishing	T1566
EXECUTION	
Command and Scripting Interpreter: PowerShell	T1059.001
Exploitation for Client Execution	T1203
PERSISTENCE	
Account Manipulation	T1098
Create or Modify System Process: Windows Service	T1543.003
PRIVILEGE ESCALATION	
Abuse Elevation Control Mechanism	T1548
DEFENSE EVASION	
Obfuscated Files or Information	T1027
System Binary Proxy Execution	T1218
CREDENTIAL ACCESS	
OS Credential Dumping	T1003
OS Credential Dumping: LSASS Memory	T1003.001
LATERAL MOVEMENT	
Remote Services: Server Message Block (SMB)/Admin Windows Shares	T1021.002
COLLECTION	
Data from Local System	T1005
Data from Network Shared Drive	T1039
EXFILTRATION	
Exfiltration Over Web Service	T1567
Automated Exfiltration	T1020
IMPACT	
Data Destruction	T1485
Data Encrypted for Impact	T1486
Data Manipulation	T1565

Ransomware by Industry

Q4 2024

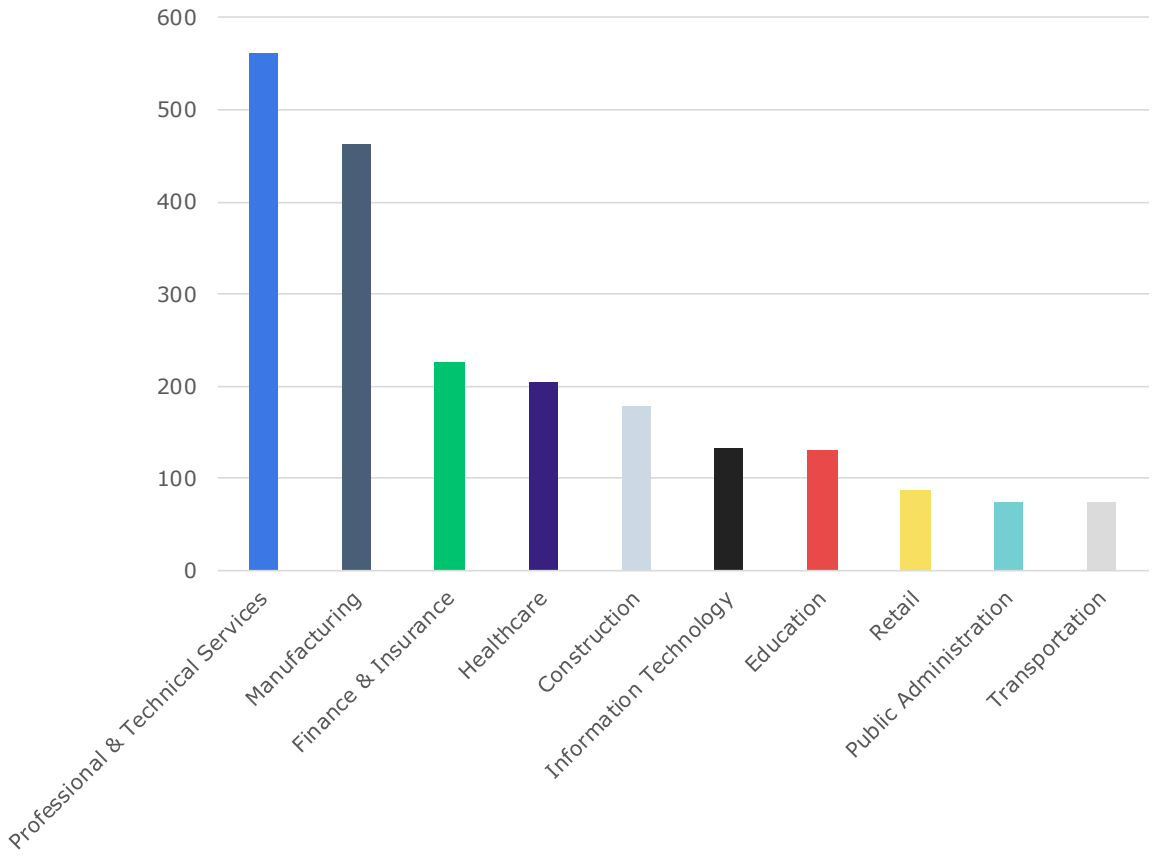


FIGURE 4. RANSOMWARE EXTORTION PUBLICATIONS BY INDUSTRY | NUSPIRE, Q4 2024

Maintaining the shift witnessed in Q3, Professional & Technical Services remained the most extorted industry vertical in Q4. Notably, all of the industries shown faced an increase in extortion publications when compared against Q3 with Finance & Insurance seeing the most dramatic increase. This surge in successful attacks pushed the industry from the 5th spot in Q3 to the 3rd spot in Q4.

INDUSTRY	PERCENTAGE CHANGE COMPARED TO Q3
Professional & Technical Services	+58.31%
Manufacturing	+51.97%
Finance & Insurance	+183.75%
Healthcare	+54.96%
Construction	+57.52%
Information Technology	+112.9%
Education	+92.65%
Retail	+67.31%
Public Administration	+54.17%
Transportation	+51.02%

Ransomware by Industry

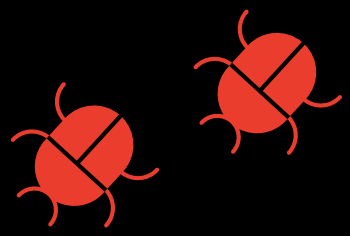
Q4 2024

The Finance & Insurance industry faces significant challenges in combating ransomware attacks due to its high-value data, complex systems, and stringent regulatory requirements, which can create process complexities. Financial institutions are prime targets for attackers seeking large payouts or access to sensitive customer information such as PII and financial records. Threat actors often use techniques like double extortion, encrypting data while threatening to leak it publicly. Additionally, ransomware attacks can severely disrupt critical operations such as payment processing and customer account management, leading to costly downtime and reputational damage.

The industry also grapples with outdated legacy systems, interconnected networks, and supply chain vulnerabilities, which increase the risk of ransomware propagation. Regulatory compliance further complicates recovery, as organizations must navigate data breach disclosure laws and potential penalties. Recovery costs, including ransom payments, system restoration, and forensic investigations, can be enormous, while the loss of customer trust and public scrutiny increases the impact of such incidents.

To address these challenges, financial institutions must adopt proactive defenses, including endpoint detection and zero-trust architectures, alongside robust employee training to mitigate social engineering risks. Regularly testing air-gapped backups, strengthening vendor management, and aligning with evolving regulatory requirements are critical strategies to minimize vulnerabilities and ensure resilience against ransomware threats.

2024 Ransomware Extortion Publications



8,156 total ransomware publications

679
publications averaged per month

5%
increase in publications from 2023

Ransomware Year-In-Review 2024

Ransomware activity increased by 5% from 2023 to 2024, driven by threat actors exploiting newly announced vulnerabilities, zero-day flaws, and supply chain weaknesses through evolving tactics. Among the key developments, Ransomhub emerged as the largest ransomware operator, overtaking LockBit, which was the most prominent operator in 2023. LockBit's decline in dominance can be attributed to mounting law enforcement pressure, which disrupted its operations and diminished its overall activity. In contrast, Ransomhub capitalized on this shift, significantly increasing its share of ransomware extortion publications on leak sites and cementing itself as a major threat actor.

Ransomhub's tactics reflected broader trends in ransomware activity. The group frequently exploited newly disclosed vulnerabilities to target organizations before patches could be implemented, as well as leveraged zero-day vulnerabilities to bypass existing defenses. Additionally, supply chain attacks became a hallmark of their strategy, enabling them to breach multiple victims through compromised vendors or software providers. These developments highlight the growing scale and coordination of ransomware operations and underscore the need for organizations to enhance their security posture with real-time threat intelligence, rigorous patch management, and proactive defense mechanisms to counter the evolving threat landscape.

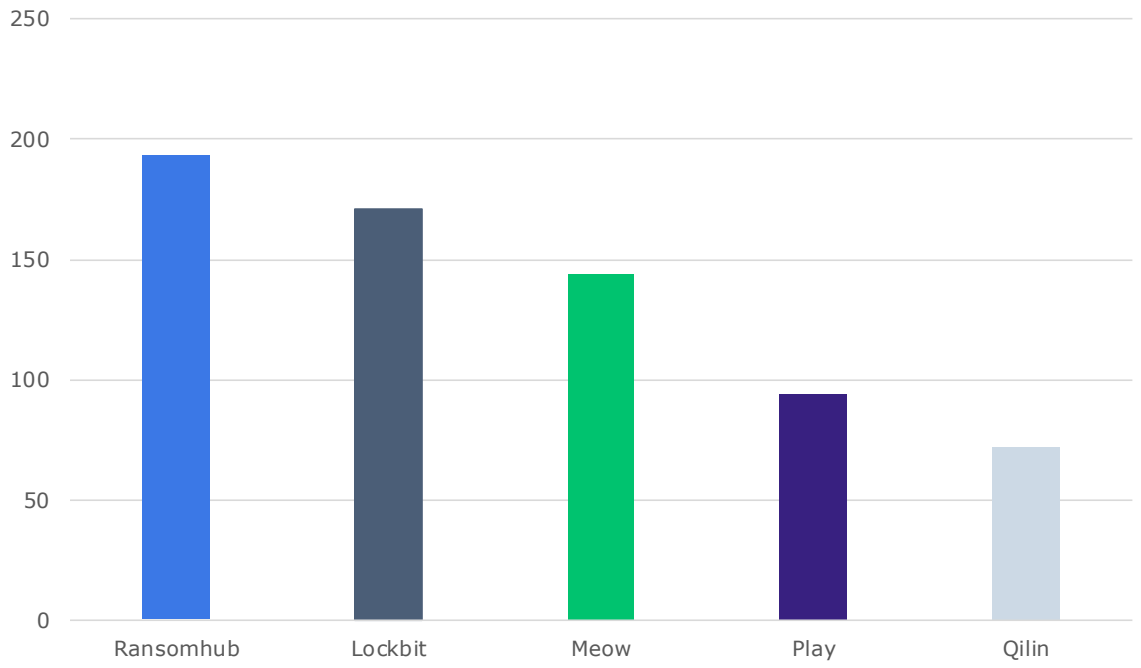


FIGURE 5. RANSOMWARE EXTORTION PUBLICATIONS BY INDUSTRY | NUSPIRE, 2024

Ransomware Year-In-Review 2024

In 2024, March and December were the most active months of ransomware publications. Several groups exploited specific vulnerabilities in March, among them, LockBit alone breached the defenses of 54 organizations. They, along with groups like Black Basta and Bl00dy were observed exploiting vulnerabilities in ConnectWise ScreenConnect (CVE-2024-1709) which exposed servers to unauthorized control. Additionally, BianLian and Jasmin ransomware targeted a critical authentication bypass vulnerability in JetBrains TeamCity (CVE-2024-27198). This allowed attackers to gain access to development pipelines, posing significant risks to software supply chains.

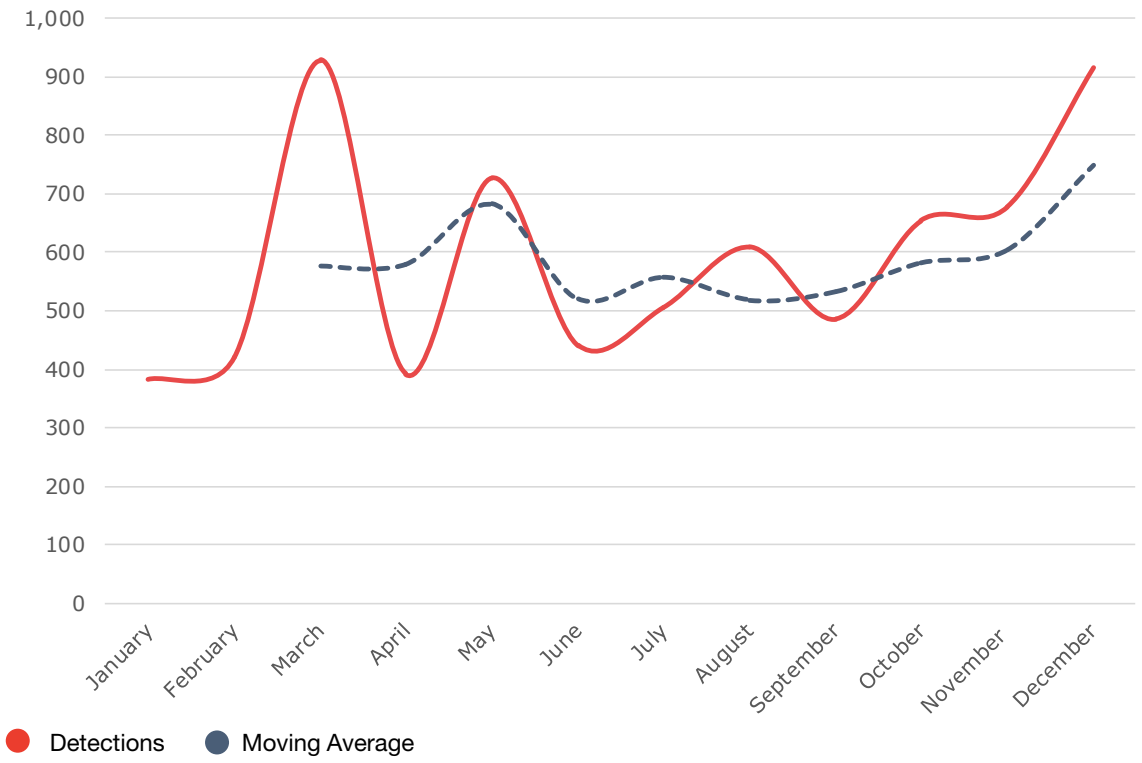


FIGURE 6. RANSOMWARE EXTORTION PUBLICATIONS BY MONTH 2024 | NUSPIRE, 2024

Also, in December 2024, ransomware activity spiked significantly with the Clop ransomware group playing a leading role. Clop exploited a critical zero-day vulnerability, CVE-2024-50623, in Cleo's Secure File Transfer products, including Harmony, VLTrader, and LexiCom. This vulnerability allowed unauthenticated attackers to upload malicious files, resulting in remote code execution. Clop leveraged this flaw to breach at least 66 organizations, primarily targeting organizations dependent on Cleo for secure data transfer.

The surge also saw other vulnerabilities exploited, such as CVE-2023-46604 in Apache ActiveMQ servers and CVE-2024-11667 in Zyxel firewalls, but the Clop group's campaign stood out due to its scale and focus on widely-used enterprise software. These incidents highlight the evolving tactics and increasing coordination of ransomware actors, who continue to prioritize supply chain attacks to maximize impact. The exploitation of Cleo's products underlines the critical need for organizations to maintain rigorous patch management, monitor third-party software, and implement robust security controls to mitigate the growing threat posed by ransomware groups like Clop.

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.

Q4 Dark Web Market Activity

2,203,522 Total Marketplace Listings

1,316,660
raw log listings for sale

590,762
credit cards listings for sale

40,578
email account listings for sale

5,968
social security listings for sale

13,592
shell access listings for sale

1,981
RDP access listings for sale

8,394
stolen account listings for sale

-32%
decrease in total listings from Q3

Dark Web

Lumma Activity Slumps Causing Decrease in Dark Web Market Listings

Nuspire regularly monitors dark web marketplaces, a type of online forum or platform that operates on a part of the internet that is not indexed by traditional search engines or are invitation only. These marketplaces require special configurations and often special authorization to access. By monitoring this activity, Nuspire can determine trends in marketplace sales and what type of information-stealing malware (infostealers) are most commonly used by threat actors.

The dotted line in Figure 7 graphically represents the moving average of dark web marketplace postings for sale during Q4 quarter. It should be noted that a single posting may contain multiple entities and may not fully capture the depth of the data sold while instead showing how active the marketplaces are.

In Q4, Nuspire witnessed a lull in Lumma Stealer activity in December which is likely responsible for the decline in Dark Web Market listings. Additionally, some actors may be retreating from market forums and utilizing other technologies such as Telegram for private groups.

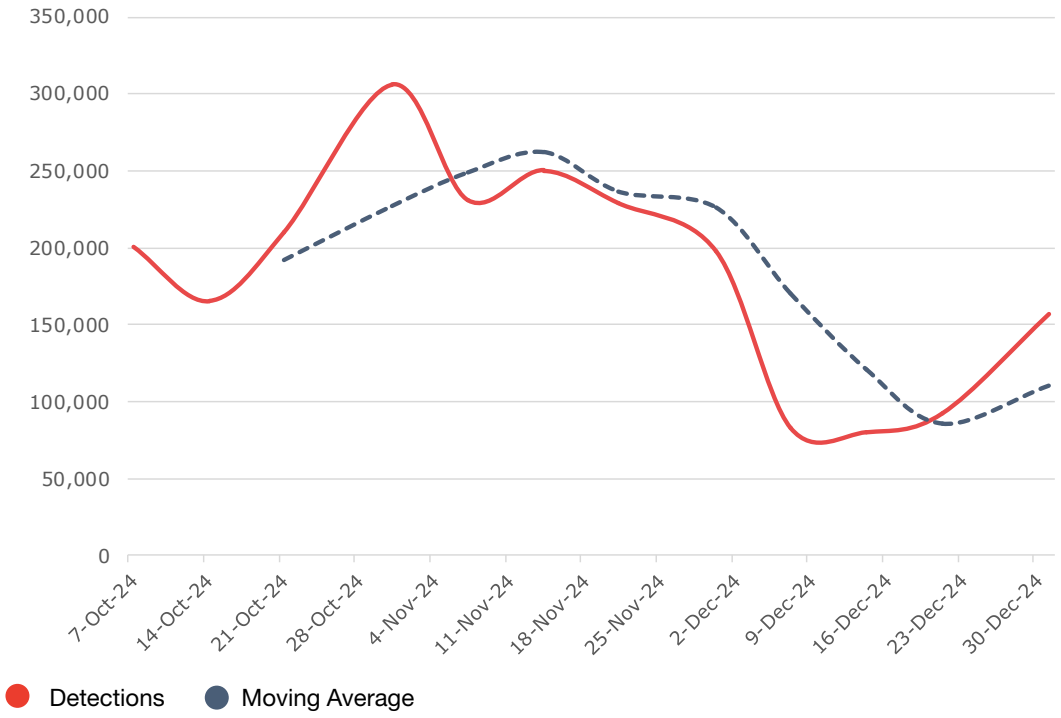
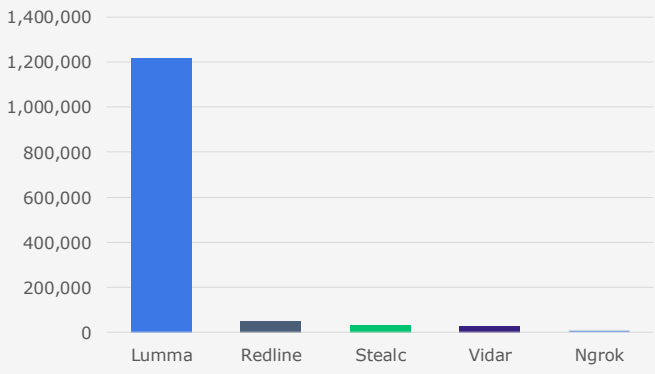


FIGURE 7. DARK WEB MARKETPLACE ACTIVITY Q4 | NUSPIRE, Q4 2024



Data on dark web marketplaces often comes from data breaches or infostealer malware. Figure 8 shows the five most active infostealers that harvest data from victim machines according to their marketplace listings. This information can help guide threat hunting activities and identify common deployment techniques that can be used in cybersecurity awareness training.

FIGURE 8. FIVE MOST ACTIVE INFOSTEALERS | NUSPIRE, Q4 2024

Dark Web

Lumma Stealer

Lumma Stealer, also known as LummaC2, is a sophisticated information-stealing malware that has been active since 2022. Operating under a Malware-as-a-Service (MaaS) model, it is openly sold on dark web forums and Telegram channels, making it accessible to a wide range of cybercriminals. Lumma targets devices running Windows operating systems from Windows 7 up to Windows 11, aiming to exfiltrate sensitive information such as browser credentials, cryptocurrency wallet data, and password manager archives.

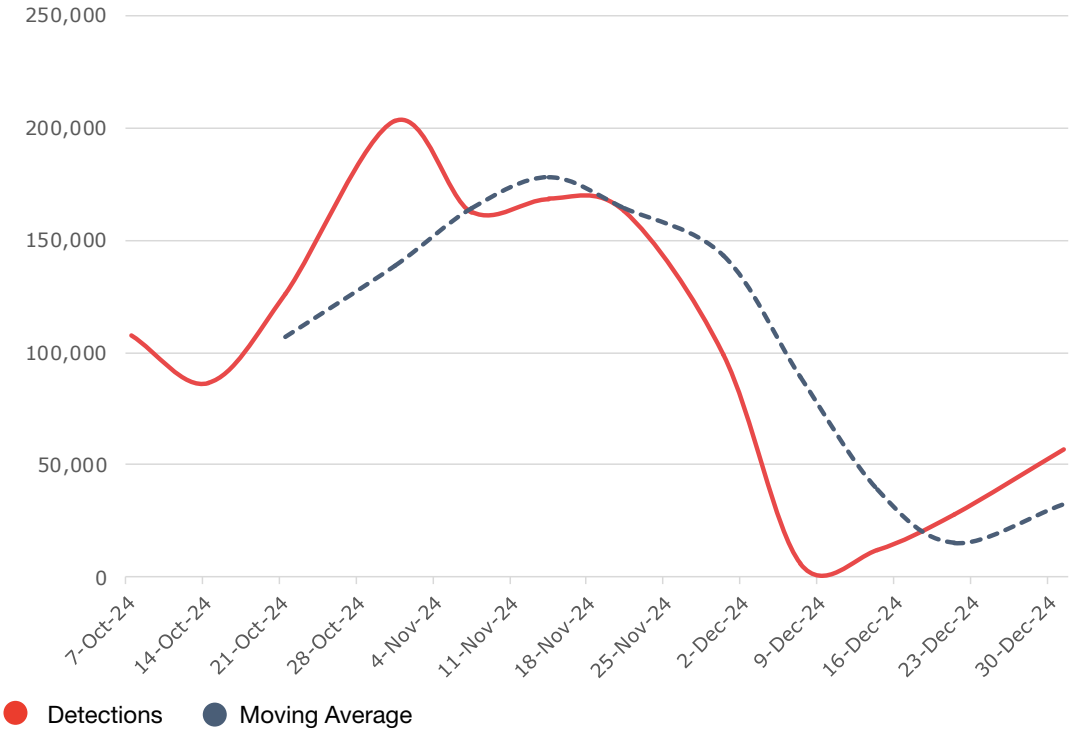


FIGURE 9. LUMMA STEALER ACTIVITY | NUSPIRE, Q4 2024

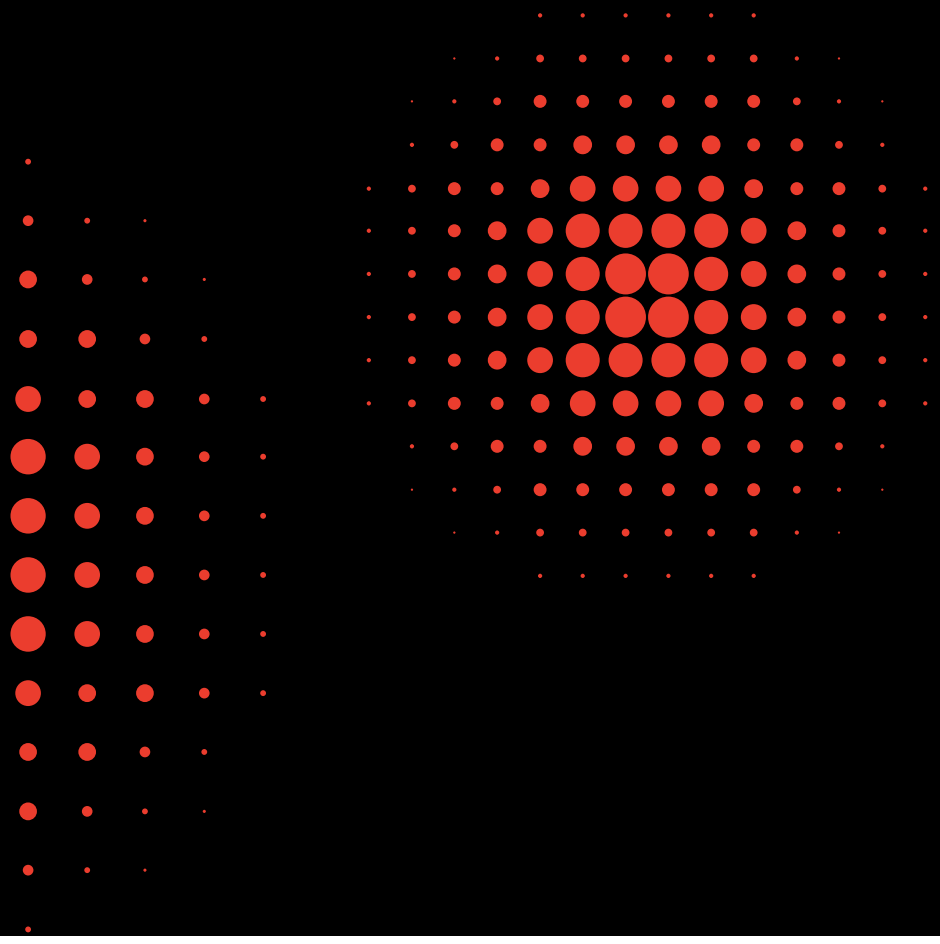
The malware is commonly distributed through deceptive methods, including phishing emails, fake software downloads, and malicious CAPTCHA verification pages. In some campaigns, attackers create convincing phishing sites featuring fake CAPTCHA verification pages; when users interact with these pages by clicking "I'm not a robot," malicious code is automatically copied to their clipboard. Users are then socially engineered to paste this code into the Windows Run dialog, triggering PowerShell commands that download and execute the Lumma Stealer payload.

Once installed, Lumma employs anti-sandbox techniques to evade detection and establishes a connection to its command-and-control server. It then scans the system for valuable data, including cryptocurrency wallets, browser profiles, persistent cookies, and extensions, exfiltrating any found information to the command-and-control server. Notably, Lumma has been observed working in conjunction with other malware families, such as the Amadey botnet, expanding its reach and capabilities.

While Dark Web listings utilizing Lumma slumped during December, this InfoStealer is still the dominant force, dwarfing listing using other stealers. Security teams are advised to adopt continuous monitoring and adaptation strategies, regularly updating detection rules, indicators of compromise, and security controls to effectively combat this evolving malware.

2024 Dark Web Market Activity

13,076,513 total marketplace listings



7,580,318
raw log listings for sale

2,162,415
credit cards listings for sale

415,495
email account listings for sale

248,572
social security listings for sale

113,571
shell access listings for sale

108,128
RDP access listings for sale

86,340
stolen account listings for sale

-6.43%
decrease in total listings from 2023

Dark Web Activity Year-In-Review 2024

In 2024, Nuspire witnessed a slight decrease of –6.43% in Dark Web Market listings when compared to 2023. While this appears to be a decrease in activity, it more likely reflects a shift in how and where threat actors operate, favoring more covert and decentralized platforms. The Nuspire Threat Intelligence Team believes that threat actors are beginning to shift away from Dark Web Marketplace forums and instead migrating to private chat servers and groups hosted on technology such as Telegram and Discord.

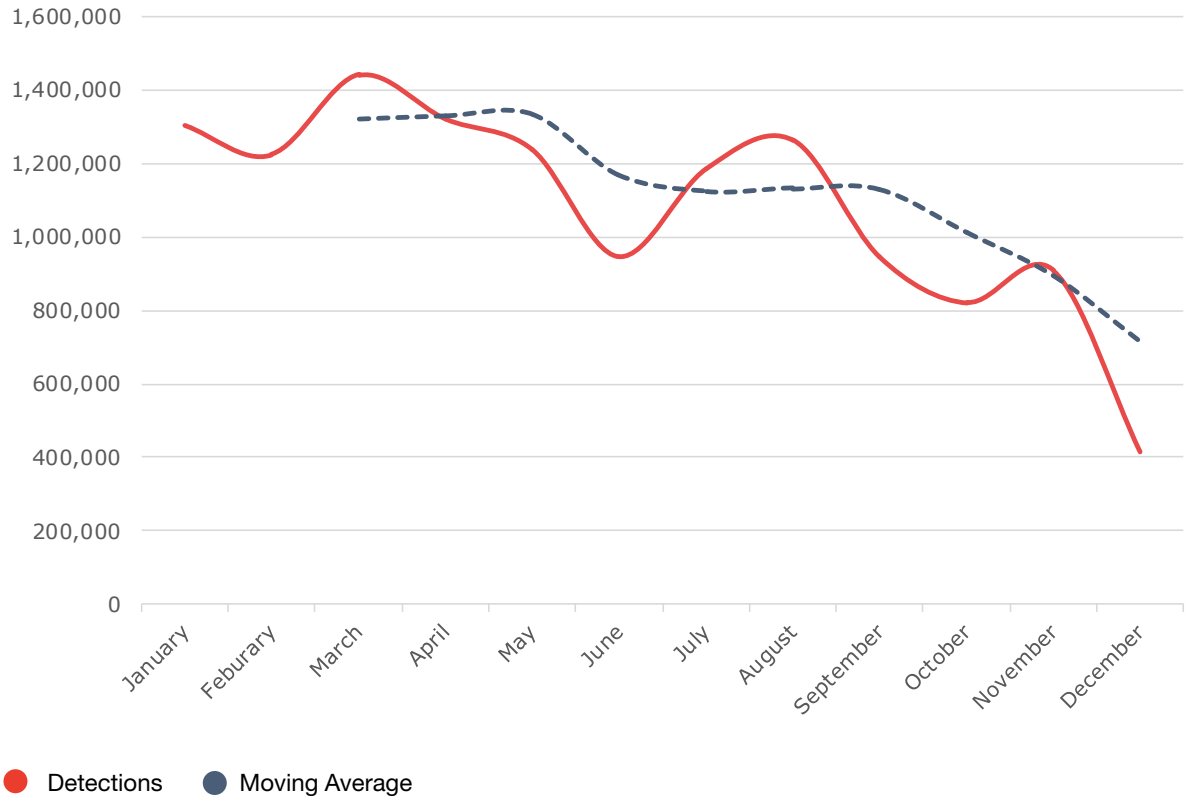


FIGURE 10. DARK WEB MARKET ACTIVITY - 2024 | NUSPIRE, Q4 2024

Dark Web Activity Year-In-Review 2024

Marketplace Distribution Methods Shifting

Cybercrime is constantly evolving. As law enforcement increases pressure on traditional dark web marketplaces like Russian Market, threat actors are shifting to private and decentralized platforms such as Telegram and Discord. These platforms provide Initial Access Brokers (IABs), who specialize in obtaining credentials and unauthorized network access, and illicit data brokers, who sell stolen data, with more covert, exclusive, and unmonitored environments to connect with interested parties.

Invite-only groups on these platforms reduce visibility to law enforcement and cybersecurity teams, while features like end-to-end encryption make monitoring and interception more difficult. Additionally, these platforms facilitate real-time interactions, enabling threat actors to conduct negotiations, exchange illicit resources, and coordinate attacks with minimal detection.

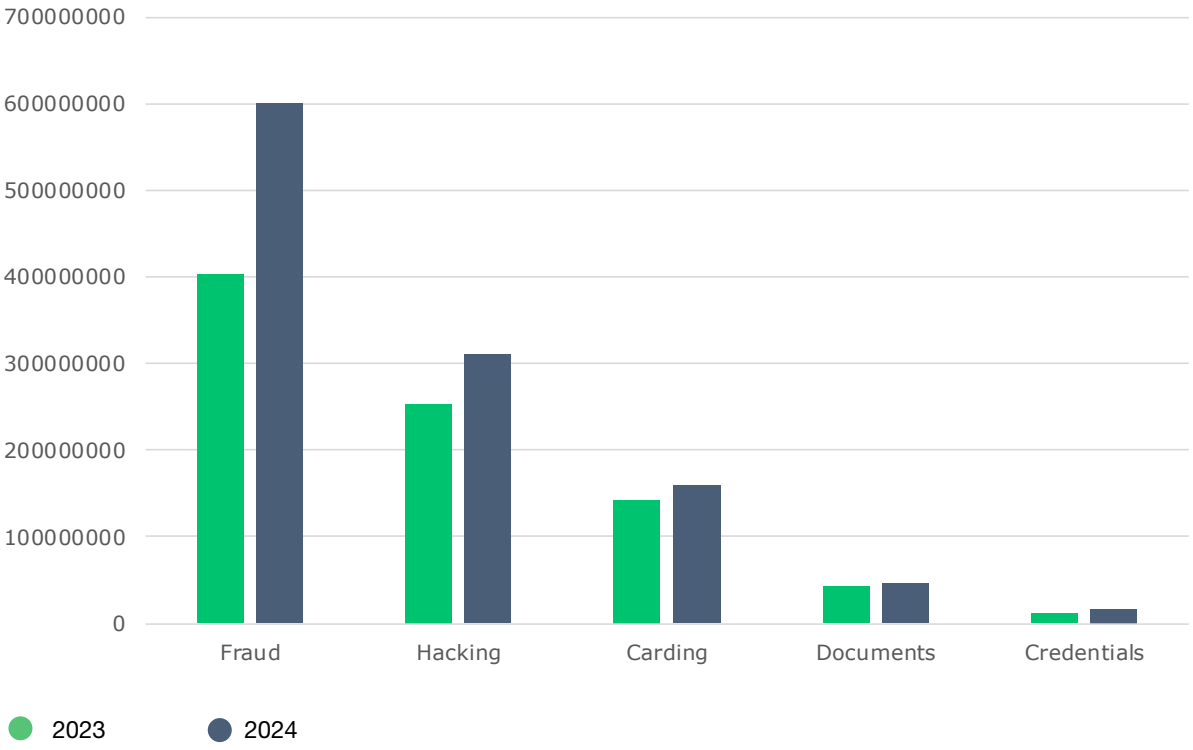


FIGURE 11. UNDERGROUND COMMUNICATION ACTIVITY - 2024 | NUSPIRE, Q4 2024

On underground communication channels visible to Nuspire, Discussions about malicious activity have increased significantly across several topics using platforms such as Telegram and Discord when compared to 2023.

Fraud-related topics, including guides, success stories, and other resources, saw a 49% increase. Hacking discussions, encompassing attack coordination, malware/exploit sales, and walkthroughs, rose by 22%. Chats related to carding—the unauthorized use of stolen credit card information obtained through phishing, data breaches, skimming devices, or trading of these items—grew by 11%. Conversations about stolen or forged documents increased by 8%, while discussions involving stolen credentials surged by 38%.

Dark Web Activity Year-In-Review 2024

Marketplace Distribution Methods Shifting

The rise in underground chatter highlights a growing trend in the accessibility and dissemination of resources for conducting cybercrime and embracing decentralized platforms. The sharp increases in discussions about fraud, hacking, and stolen credentials signal that threat actors are sharing techniques, tools, and success stories in these platforms at a growing rate, fueling the expansion of criminal activity.

For security teams, the uptick in malware, exploits, and stolen credential discussions is particularly concerning. These activities often serve as entry points for more significant attacks, such as ransomware or network intrusions. Organizations should prioritize implementing multi-factor authentication (MFA), monitoring for unusual login behavior, and regularly updating detection rules for compromised credentials. Additionally, the increased availability of walkthroughs involving fraud emphasizes the need for ongoing security awareness training to better equip employees against phishing and social engineering tactics.

To counteract these evolving methods, organizations must adopt a proactive threat intelligence strategy. This includes monitoring underground forums and communication channels for relevant indicators of compromise (IOCs) and leaked or stolen credentials, maintaining up-to-date threat models, and fostering collaboration between intelligence teams, security operations centers (SOCs), and incident response teams. The evolving cybercrime landscape requires a multifaceted defense approach that combines advanced technical controls with continuous education and adaptation to stay ahead of emerging threats.

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

A dark web monitoring program can inform your organization when threat actors possess sensitive data about your organization and are trading it. This allows the discovering of proprietary code, discussions about your organization, and leaked credentials providing insight and quick action such as rotating passwords making them useless to attackers.

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.

Q4 Exploitation Events

29,180,763 Total

601

unique exploits detected

2,431,730

exploits detected per week

347,390

exploits detected per day

72%

increase in total activity from Q3

Exploits

Exploit Attempts Continue to Grow Against Firewalls and VPNs

Figure 12 provides a visual representation of the trends in exploitation activity throughout the fourth 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 Q3 to Q4, Nuspire observed a substantial increase in activity, spurred mainly by massive increases in attempts against vulnerabilities like Hikivision's camera systems, Apache's Log4j, and Firewall technologies. This uptick in activity led to an increase of 72% in total activity.

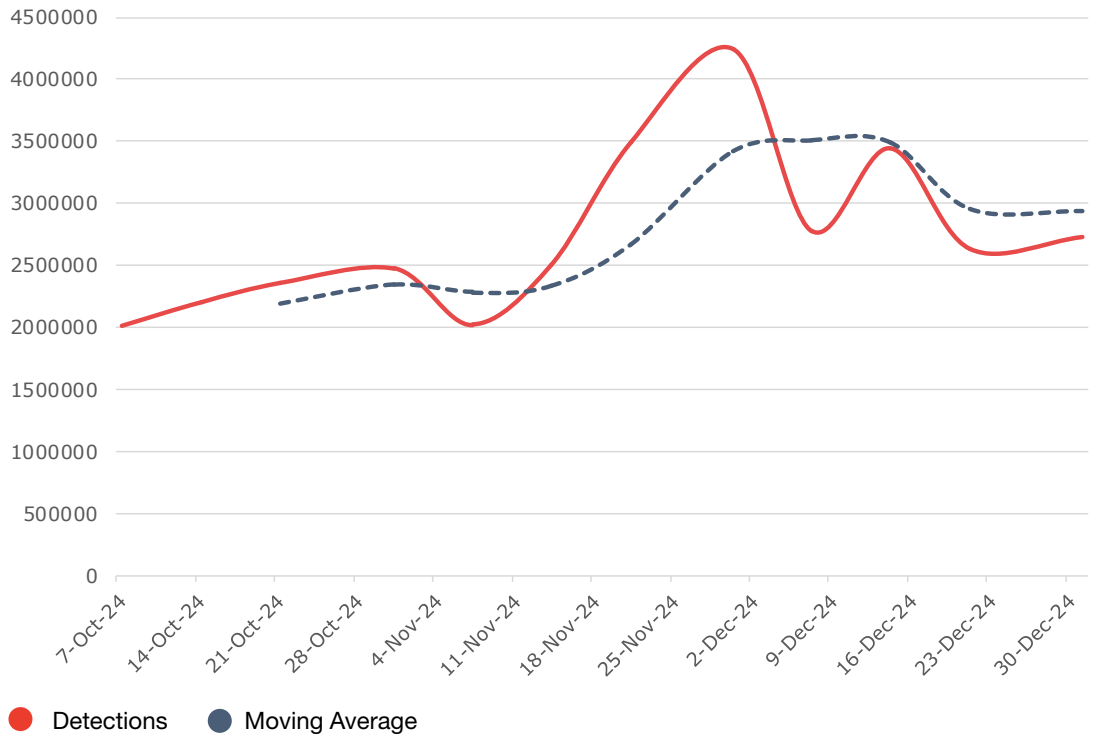


FIGURE 12. Q4 EXPLOIT ACTIVITY | NUSPIRE, Q4 2024

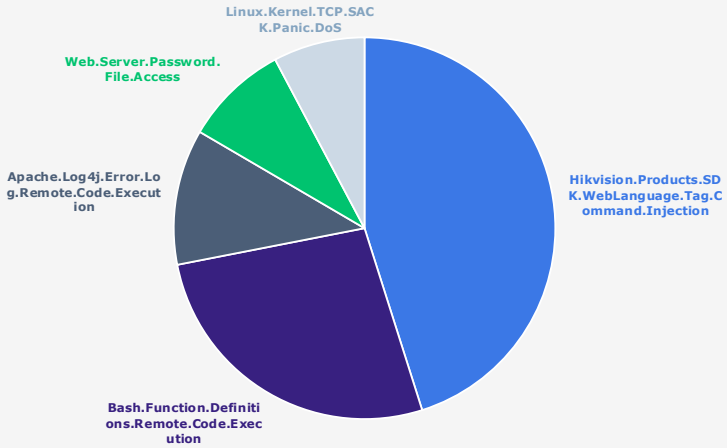


Figure 13 illustrates the most frequent exploit attempts observed in Q4. Exploit attempts against Hikvision Camera Products (CVE-2021-36260) dominated the quarter and a renewed focus in attempts on abusing vulnerabilities in Bash (CVE-2014-6271), a free command-line shell scripting language that is the default shell for most Linux distributions, drove a significant amount of Q4's activity. When compared against Q3, activity against Hikivision increased by 56% and Bash by 77%.

FIGURE 13. Q4 TOP WITNESSED EXPLOITS | NUSPIRE, Q4 2024

Exploits

Firewall & VPN Technologies

Firewall and VPN technologies are critical components of an organization's cybersecurity infrastructure, acting as the first line of defense against external threats and enabling secure remote access to internal resources. Threat actors prioritize targeting these technologies because they serve as gatekeepers to an organization's network. Successfully exploiting a firewall or VPN not only provides attackers with a foothold but often grants direct access to sensitive data, internal systems, and potentially even administrative controls. This level of access makes them high-value targets for cybercriminals, nation-state actors, and other advanced threat groups.

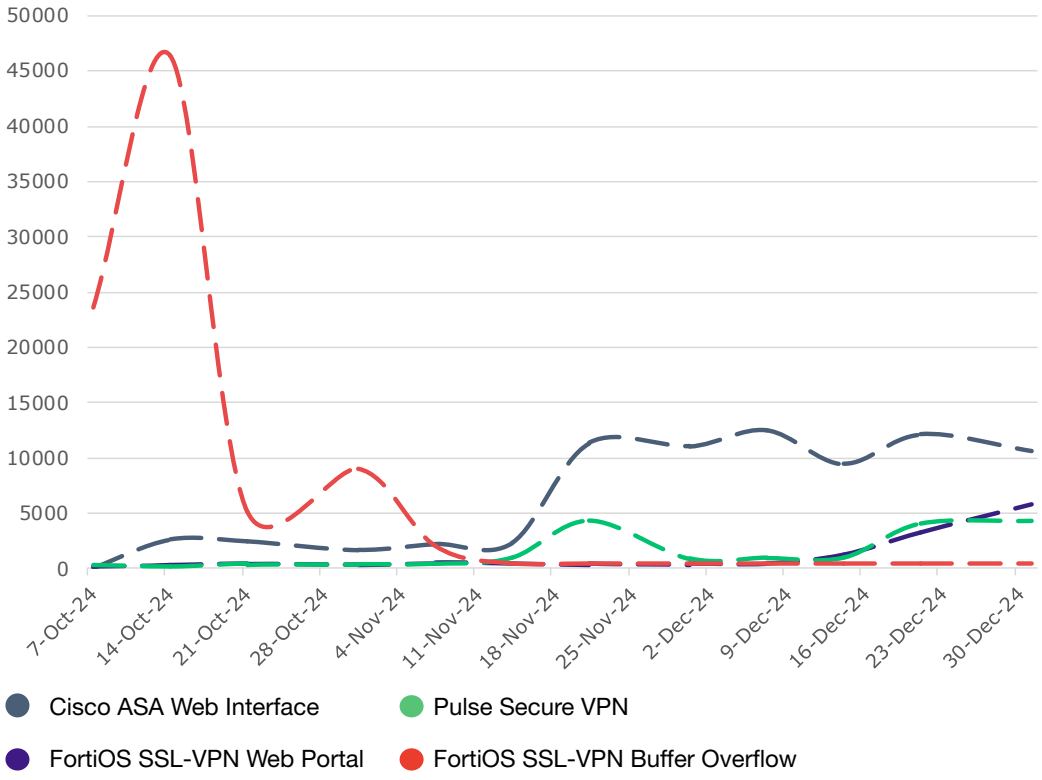


FIGURE 14. Q4 FIREWALL & VPN TECHNOLOGY EXPLOIT ATTEMPTS | NUSPIRE, Q4 2024

During Q4, Nuspire witnessed activity against numerous Firewall and VPN technology exploits and newer critical ones were announced. Older Fortinet FortiOS SSL-VPN Heap-Based Buffer Overflow (CVE-2022-42475) saw the most activity at the beginning of the quarter before attempts trailed off into the end of the year. A steady increase of exploitation attempts against Cisco ASA's abusing a directory traversal vulnerability (CVE-2020-3187) was seen. While activity initially started low, Fortinet's SSL-VPN was increasingly targeted through an older flaw in the web portal, specifically CVE-2018-13379. Additionally, attempts increased against Pulse Secure VPNs in an information disclosure attack (CVE-2019-11510) into the end of the year.

Numerous critical vulnerabilities affecting Firewall and VPN products were also announced or updated during Q4. The Cybersecurity & Infrastructure Security Agency released an advisory in October stating that threat actors were actively targeting Fortinet's critical vulnerability (CVE-2024-23113) affecting the 'FGFM' daemon, which allows remote code execution. They then added it to their Known Exploited Vulnerabilities Catalog and ordered federal agencies to patch within three weeks.

Exploits

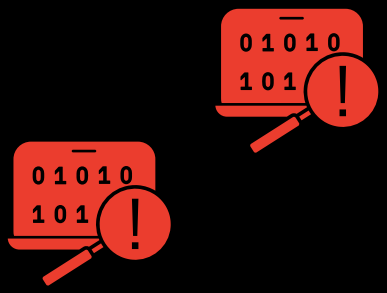
Firewall & VPN Technologies

Fortinet's FortiManager, a tool used to centrally manage Fortinet devices, also was victim of a critical zero-day vulnerability (CVE-2024-47575) during Q4. If abused, threat actors could execute arbitrary code or commands putting managed devices at risk.

Palo Alto devices utilizing PAN-OS software also fell victim to critical zero-day vulnerabilities (CVE-2024-0012 & CVE-2024-9474) allowing authentication bypass and privilege escalation. Abusing these allows successful attackers to perform actions on the firewall with root privileges. This vulnerability compromised thousands of devices.

The increasing adoption of remote work and cloud-based services has further elevated the importance, and the risks associated with these technologies. Misconfigurations, unpatched vulnerabilities, and zero-day exploits in firewalls and VPNs present opportunities for attackers to bypass perimeter defenses undetected. As a result, threat actors continually refine their techniques to exploit these vulnerabilities, aiming to breach high-value systems and bypass traditional security measures. This persistent targeting underscores the importance of regular updates, following vendor best-practice guides, and proactive threat intelligence to mitigate the evolving risks to firewall and VPN technologies.

2024 Exploitation Events



63,259,033 total

1,399
unique exploits detected

5,271,586
exploits detected per month

120%
increase in total activity from 2023

2024 Exploits Year-In-Review

Throughout 2024, Nuspire saw a steady increase of exploit attempts, driving activity up 120% when compared to 2023. In 2023, 502 unique exploits were attempted, whereas in 2024 that number surged to almost 1,400. Threat actors continue expanding their arsenal of available exploits, relying on older critical vulnerabilities and adding newly announced ones to their kit every day. In 2024, most exploit activity targeted Hikvision Command Injection, Apache Log4j RCE, and Bash RCE—patterns that remained consistent throughout the year. This activity seems to be highly automated by threat actors looking for legacy devices hosting unpatched technology to slip into organizational networks.

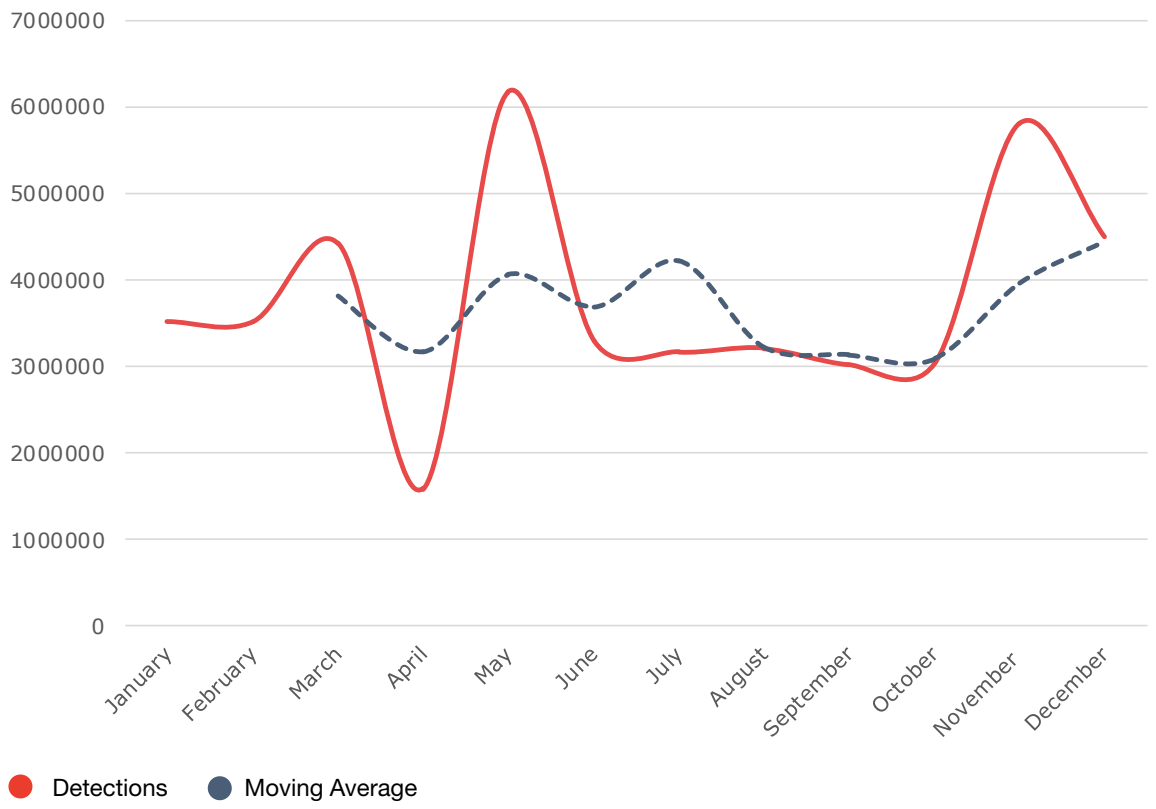


FIGURE 15, EXPLOIT ACTIVITY 2024 | NUSPIRE, Q4 2024

2024 Exploits Year-In-Review

While threat actors may come from all over the world, most of their attacks originate from the U.S. IP space. With platforms like Amazon Web Service (AWS), Google Cloud Platform (GCP), Microsoft Azure, and smaller hosting providers threat actors can quickly spin up infrastructure for an attack and rent these services with minimal or no verification of who or where they are. In circumstances of stricter verification, stolen or false identities are used to bypass this minor hurdle.

Using U.S. IP based infrastructure provides numerous advantages for the attackers. IP addresses sourced from the U.S. are less likely to be flagged as suspicious compared to countries known for malicious activity. This allows them to blend into the background of legitimate internet traffic, increasing their chances of bypassing security features like geofencing or IP-based blocklists. Organizations should still consider applying geofencing and utilize IP-based blocklists but understand that it is a part of a layered defense and not a single solution.

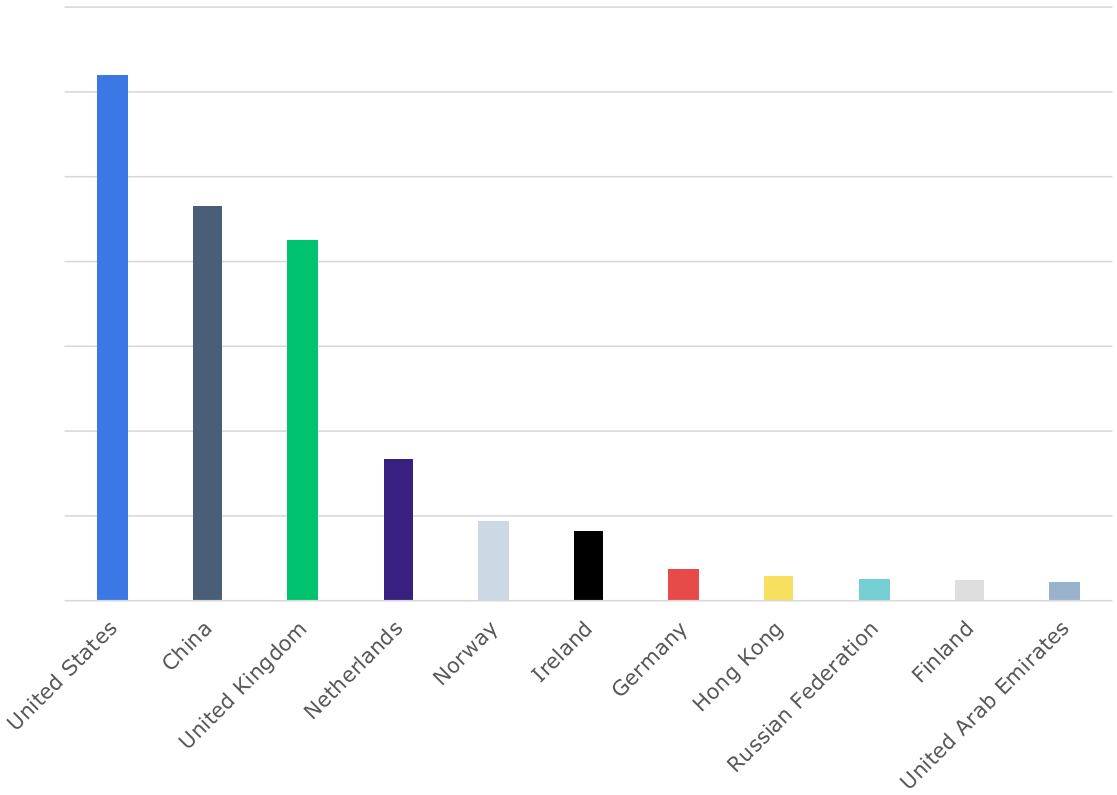


FIGURE 16, EXPLOIT ATTEMPTS SOURCED BY COUNTRY 2024 | NUSPIRE, Q4 2024

Ways to Combat These Threats

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

Prioritize patching and vulnerability management

Threat actors are constantly on the lookout for organizations that have not kept their systems and technologies up to date with the latest security patches. This makes it crucial for organizations to have a clear understanding of their technology stack and to ensure that patches or mitigations are applied without delay. Special attention should be directed toward addressing high and critical vulnerabilities, particularly those involving remote access, as these are often the most attractive targets for attackers.

Utilize Firewalls with Intrusion Prevention Systems (IPS):

Implement a firewall with an integrated intrusion prevention system (IPS) to bolster network security by detecting and blocking exploit attempts. Regularly update the signatures provided by your security vendor to stay protected against the latest attack methods.

Stay updated by following security news and subscribing to 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.

Follow vendor “best practice” guides for configuration

Disable any unnecessary services to minimize the risk of introducing additional vulnerabilities. Organizations should also have a clear understanding of which services are exposed to the internet and secure them appropriately, such as by using VPN technology. Additionally, following vendor best practice guides for configurations is crucial to ensure services are set up securely and optimized to reduce potential attack surfaces.

Cyber Resilience: Anticipating Tomorrow's Threats

With the ongoing advancement in cyber threats and techniques, attacks are progressively growing more complex and can cause extensive damage at a rapid pace. The silver lining is that cyberattacks can often be anticipated. Companies with internet connectivity or the possibility of internet connections must know they are potential targets. Consequently, these organizations should familiarize themselves with the most prevalent threats and evaluate their digital boundaries to determine the necessary steps for risk reduction.

Learn about the **transformative impact of Managed Detection and Response (MDR)** on your organization's ability to predict and respond to cyber incidents.

Discover the benefits of incorporating **dark web monitoring** into your security posture to prevent identity theft and data breaches.

Fortify Your Defenses with Additional Resources from Nuspire

Escalating threat activity demands vigilant defense strategies.

Don’t know where to start? Take these five simple actions to safeguard your 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.

Buying 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, perform threat modeling on your organization to determine how Advanced Persistent Threat groups are targeting your industry vertical, and implement dark web monitoring to quickly discover credential leaks and sensitive data exposure.

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

Nuspire, a leading managed security services provider (MSSP) with 25 years of experience, is revolutionizing the cybersecurity experience by taking an optimistic and people-first approach. Our deep bench of cybersecurity experts, world-class threat intelligence, and 24x7 security operations centers (SOCs) detect, respond to, and remediate advanced cyber threats. We offer comprehensive services that combine award-winning threat detection with superior response capabilities to provide end-to-end protection across the gateway, network, and endpoint ecosystem.

In early 2025, Nuspire will transition to **PDI Security and Network Solutions**, combining our legacy of cybersecurity excellence with PDI's industry leadership. This integration creates a powerhouse of capabilities, including advanced AI-powered security features, the management of thousands of endpoints and firewalls, and an unwavering commitment to client satisfaction—demonstrated by our 97% client retention rate.

Our client base spans thousands of enterprises of all sizes and industries, achieving the greatest risk reduction per cyber-dollar spent. As PDI Security and Network Solutions, we remain laser-focused on delivering an extraordinary cybersecurity experience that exceeds expectations. For more information, visit www.nuspire.com and follow @NuspireNetworks on Twitter.

nuspire.com
LinkedIn @Nuspire
X/Twitter @NuspireNetworks