nuspire

Q3 2023
Threat Landscape Report

Botnets Soar, Malware Dips, Top Ransomware Operators Unveiled

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

What's in the Report

nuspire

Introduction:
Q3 Saw Evolving Cyber Threats: Botnet Expansion and Ransomware Highlights

In today's rapidly evolving digital landscape, cybersecurity is not just an IT concern but an essential aspect of safeguarding industries and their patrons across the globe. The cyber realm's undercurrents have become intricate and ubiquitous, from ransomware gangs like ALPHV exploiting advanced tactics to the alarming rise of botnets like Torpig Mebroot. Quarter three of 2023 alone witnessed a staggering 67.51% increase in botnet activity, and major attacks on the hospitality industry were discovered. This activity, while significant, only hints at the vast cyber ecosystem that lurks beneath the surface.

As you delve into this comprehensive report, you'll uncover insights into the tactics and techniques of renowned ransomware groups, the dynamics of zero-day vulnerabilities, and the industries most targeted by cyber adversaries. Join us on this enlightening journey as we decode the intricacies of the cyber world, highlighting the urgent need for proactive cybersecurity measures and showcasing how to navigate these digital waters.

MALWARE

BOTNET

EXPLOIT

Summary of Findings

-5.94%
decrease in total activity from Q2

1,722,909 total
Q3 Malware Events

76,631,396 total
Q3 Exploitation Events

-35.92%
decrease in total activity from Q2

67.51%
increase in total activity from Q2

2,274,028 total
Q3 Botnet Events

How We Crunch the Numbers

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

GATHER

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

1

PROCESS

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

2

DETECT

Using Nuspire's cloud-based SIEM, log data is ingested and 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 and the community through the creation of detection rules, briefs and presentations.

5

Q3'S Top Threat Events

July 7

CISA Releases Joint Advisory on TrueBot Malware

July 11

Microsoft Announces Unpatched Zero-Day Affecting Office Products

July 12

Fortinet released Patches for Critical Vulnerability in FortiOS and FortiProxy

July 12

Popular Open-Source PDF Library GhostScript Announces Critical RCE

July 13

Microsoft's July 2023 Patch Tuesday Addresses 6 Zero-Days, 132 Vulnerabilities

July 18

Citrix Discloses Actively-Exploited Critical Vulnerability

August 8

PaperCut Discloses New High-Level Vulnerability

August 9

Microsoft's August 2023 Patch Tuesday Addresses 2 Zero-Days, 87 Vulnerabilities

August 16

Racoon Stealer Returns with New Version

August 30

Qakbot Malware Disrupted in Multinational Cyber Takedown

September 13

Microsoft's September 2023 Patch Tuesday Addresses 2 Zero-Days, 59 Vulnerabilities

September 19

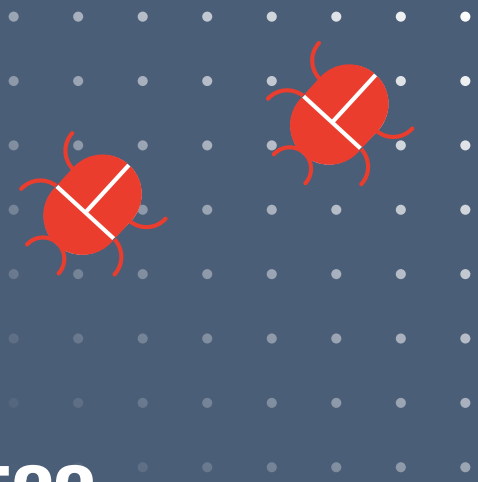
Critical Unauthenticated Juniper RCE Vulnerability Affects Estimated 12,000 Devices

September 27

Google Reclassifies libwebp Vulnerability Exploited in Attacks to Critical

September 29

Critical RCE Vulnerability Disclosed for Progress WS_FTP



Q3 2023

Malware Events
1,722,909 total

522

unique variants detected

143,575

detections per week

20,510

detections per day

-5.94%

decrease in total activity from Q2

Malware –

Two New Ransomware Groups Emerge As Top Offenders

Figure 1 shows the average Q3 malware activity in a dashed trend line. The solid line shows the true weekly numbers to help identify spikes and abnormal activity. Overall, malware detections remained relatively stable, with only a slight 5.94% decrease across the quarter. As the quarter concluded, activity appeared to be on the rise again leading into Q4.

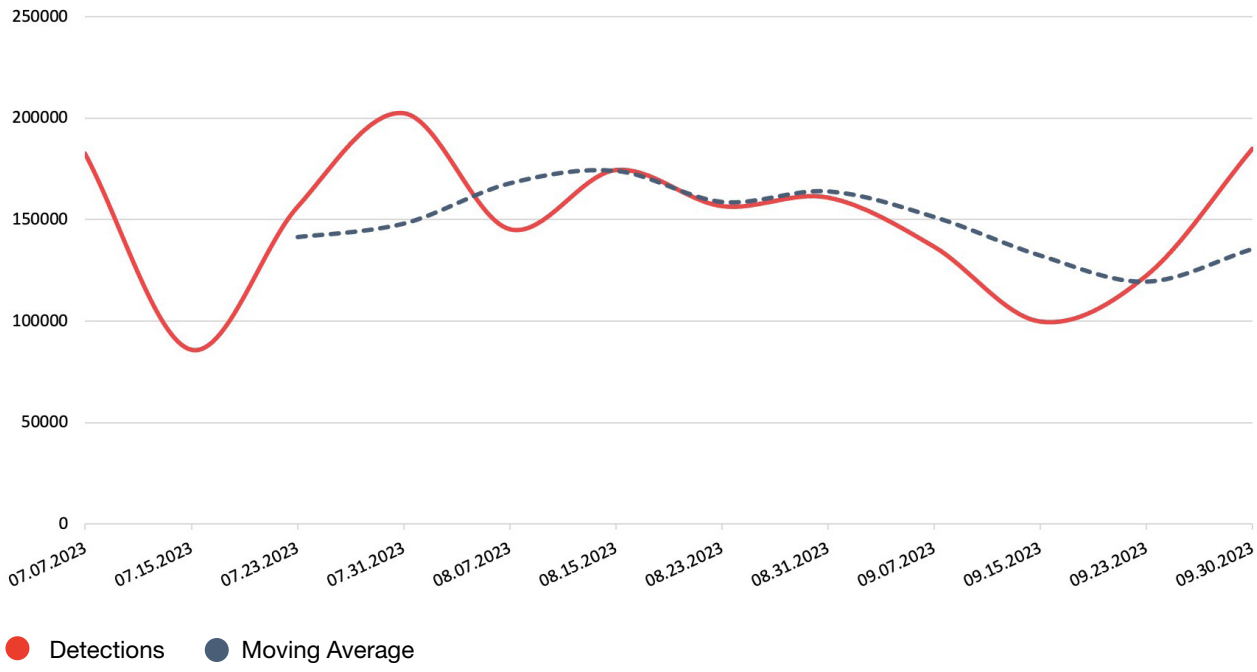
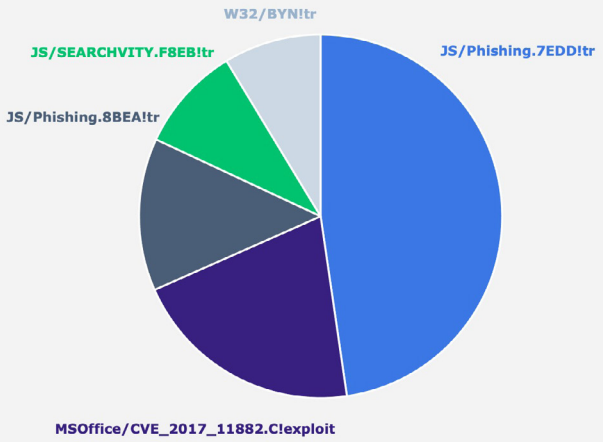


FIGURE 1. MALWARE DETECTIONS | NUSPIRE, Q3 2023



As shown in Figure 2, the top five malware variants witnessed throughout Q2 were mostly JavaScript phishing variants. Phishing remains one of the top methods threat actors and ransomware gangs use to gain access to organizations.

FIGURE 2. TOP FIVE MALWARE VARIANTS | NUSPIRE, Q3 2023

Microsoft Office RCE (CVE-2017-11882)

Even though Microsoft's CVE-2017-11882 has offered patches for over 5 years, threat actors are still trying to exploit it. Why? They're likely continuing to find success.

Exploiting this vulnerability involves crafting malicious files and emailing them to potential victims. If opened and successfully exploited, attackers can execute code with the permissions assigned to the victim opening it. This could allow an attacker to install additional payloads, delete or modify data, and create new accounts.

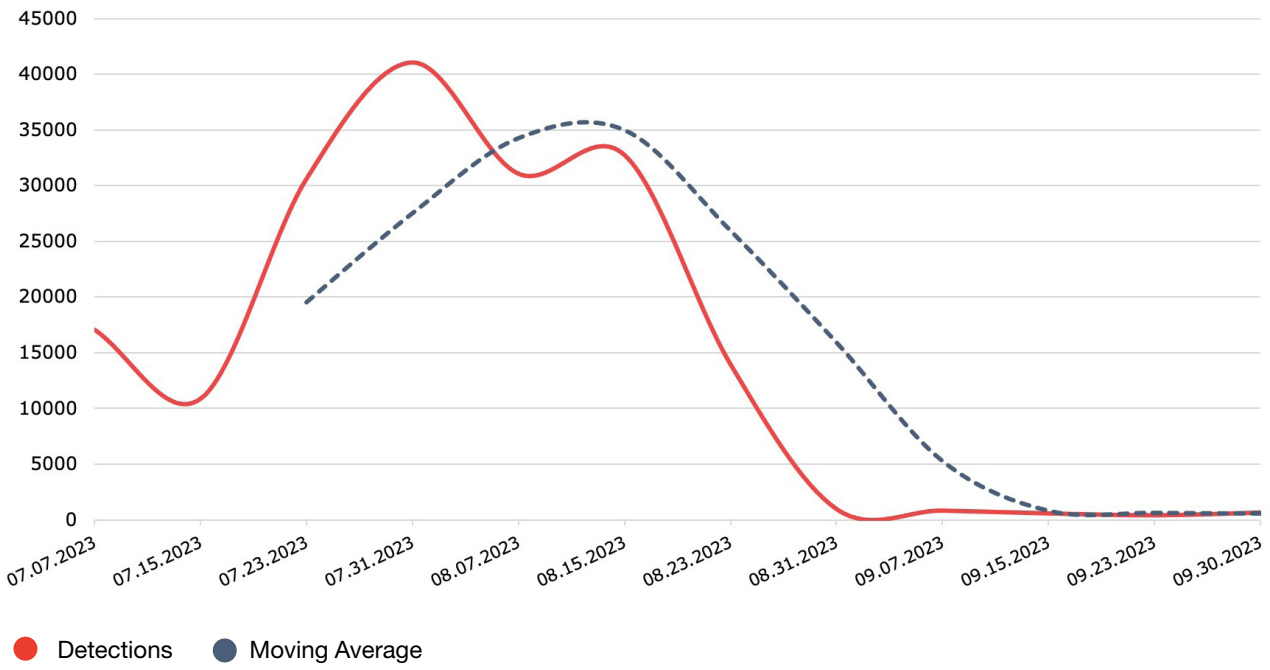


FIGURE 3. MICROSOFT OFFICE RCE (CVE-2017-11882) | NUSPIRE, Q3 2023

Nuspire witnessed significant activity attempting to exploit this vulnerability using malicious files throughout July and August. The amount of activity generated pushed this variant to the second most witnessed malicious file type in Q3; if activity hadn't fallen off in September, the vulnerability likely would have finished as most actively witnessed. While not as popular in Q3, Nuspire saw similar malicious files crafted to exploit CVE-2018-0798, another remote code execution (RCE) vulnerability.

Organizations should ensure they're patching Microsoft products as soon as possible. Especially those being actively exploited and involve RCE.

Ransomware Activity

During Q3, ransomware extortion publications remained relatively stable, with a 1.38% decrease in extortion publications compared to Q2. LockBit persists as the dominant ransomware gang, although its published extortions dropped by 7.27% compared to Q2.

CL0P Ransomware Gang, known for quickly abusing newly announced vulnerabilities, continued its high levels of activity, especially when considering the group's activity increased by 65% from Q1 to Q2. BianLian and BlackBasta Ransomware families fell out of the top 5 in Q3, while 8Base and Akira ransomware stepped in to fill their spots. Remaining in the middle of the pack is ALPHV, also known as BlackCat, which has taken credit for the massive and disruptive attack against MGM (more about that cyberattack later).

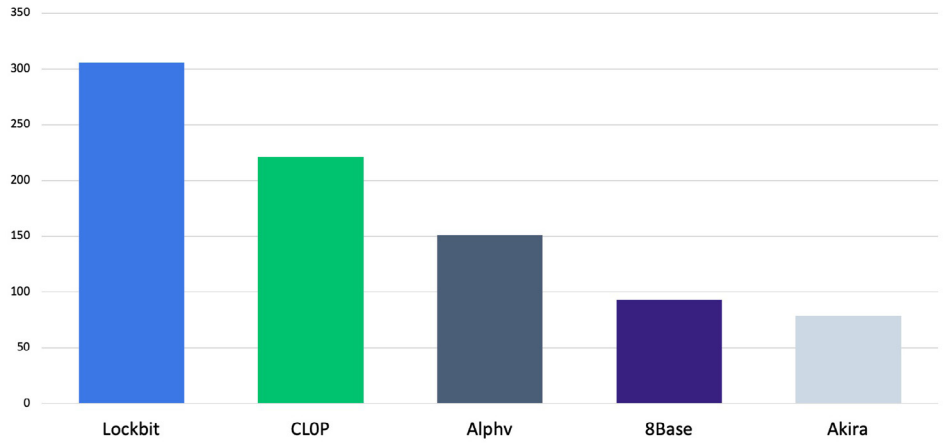


FIGURE 4. TOP RANSOMWARE GANGS Q3 (BY EXTORTION PUBLICATIONS) | NUSPIRE, Q3 2023

During Q3, 8Base showed the most significant levels of growth, almost tripling their activity levels, publishing a 165.71% increase in extortions on their dark website compared to Q2. The group is relatively new to the scene, emerging in early 2023, and has similarities to other ransomware like RansomHouse, Hive and Phobos, but no formal connections have been identified. Currently, its targeted industries include healthcare, information technology, finance and manufacturing, mainly within the United States.

Akira also showed levels of growth, increasing its ransomware extortion publications (when gangs are actively extorting a victim) by 12.86% compared to Q2. The group is another quickly growing ransomware family that emerged in March 2023 and has shown it is experienced and sophisticated. Akira has been targeting U.S.-based and Canadian companies, indiscriminate of industry vertical. The U.S. Department of Health and Human Services Health Sector Cybersecurity Coordination Center (HC3) has **released security advisories** regarding Akira ransomware attacks. Most notably, the group has been seen exploiting the recent Cisco ASA Zero-Day, tracked as **CVE-2023-20269**.

8Base and Akira are ransomware families to watch, and unless intervention comes through law enforcement action, they are likely to continue to grow and make headlines with their attacks.

Ransomware Activity, Cont.

ALPHV (or BlackCat) is a sophisticated ransomware cartel that operates using a "Ransomware-as-a-Service" model and multiple extortion techniques. Most notably, it has claimed credit for the widely publicized ransomware attack on MGM Resorts, which was estimated to cost over $100M in damages in September. The group's payload has a suite of advanced features that can affect numerous environments. The gang is suspected of operating out of Russia and Eastern Europe, and it typically interviews potential affiliates multiple times before providing them access to its toolset. If an affiliate launches a successful attack, it can keep up to 90% of the ransom paid out while providing the rest of the payback to the ransomware operator.

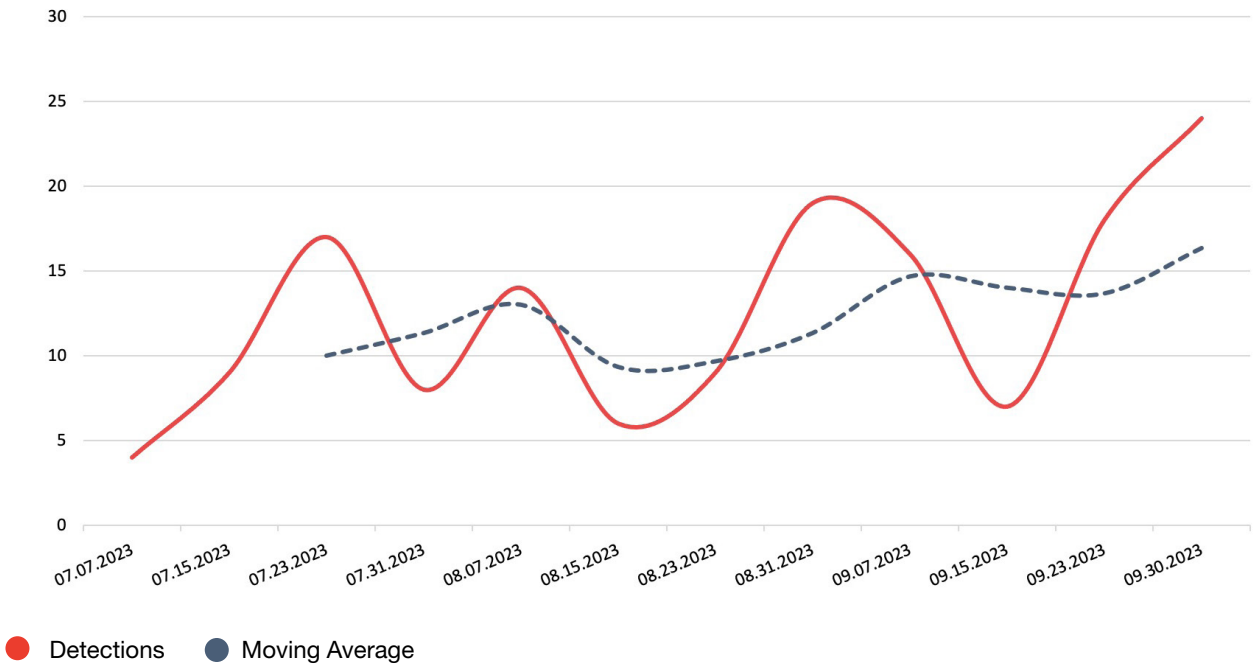


FIGURE 5. ALPHV RANSOMWARE ACTIVITY (BY EXTORTION PUBLICATIONS) | NUSPIRE, Q3 2023

ALPHV has been witnessed exploiting public-facing applications on vulnerable versions and taking advantage of valid accounts for which they can get legitimate credentials. Compared to Q2, this gang's activity is up 4.86% and will likely continue to trend upwards unless direct law enforcement action is taken against their infrastructure.

MITRE ATT&CK Techniques Utilized by ALPHV Ransomware Gang

TECHNIQUE	ID
INITIAL ACCESS	
Exploit Public-Facing Application	T1190
Valid Accounts	T1078
EXECUTION	
Command and Scripting Interpreter: PowerShell	T1059.001
Command and Scripting Interpreter: Windows Command Shell	T1059.003
PERSISTENCE	
Valid Accounts	T1078
PRIVILEGE ESCALATION	
Valid Accounts	T1078
Exploitation for Privilege Escalation	T1068
DEFENSE EVASION	
Valid Accounts	T1078
Impair Defenses: Disable or Modify Tools	T1562.001
Impair Defenses: Safe Mode Boot	T1562.009
Indicator Removal: Clear Windows Event Logs	T1070.001
CREDENTIAL ACCESS	
OS Credential Dumping: LSASS Memory	T1003.001
DISCOVERY	
Account Discovery	T1087
File and Directory Discovery	T1083
Network Share Discovery	T1135
Permissions Groups Discovery	T1069
Process Discovery	T1057
Remote System Discovery	T1018
System Network Configuration Discovery	T1016
LATERAL MOVEMENT	
Remote Services: SMB/Windows Admin Shares	T1021.002
Remote Services Session Hijacking: RDP Hijacking	T1563.002
EXFILTRATION	
Exfiltration Over Alternative Protocol	T1048
Exfiltration Over Web Service	T1567
IMPACT	
Data Encrypted for Impact	T1486
Defacement: Internal Defacement	T1491.001
Inhibit System Recovery	T1490
Service Stop	T1489

FIGURE 6. ALPHV MITRE ATT&CK TECHNIQUES | NUSPIRE, Q3 2023

Ways to Combat These Threats

Malware can take the form of viruses, worms, spyware and ransomware, and is often transmitted via phishing.

Comprehensive Security with Endpoint Protection Platforms (EPP)

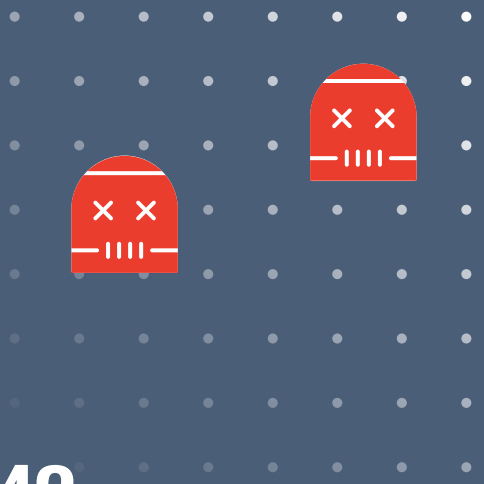
Implement an all-encompassing security approach that incorporates advanced, next-generation antivirus (NGAV) solutions. NGAV can detect and obstruct malicious software not just via signatures, but also by employing heuristics and behavioral analysis that identify and halt irregular activities. This goes beyond traditional antivirus tools, which rely primarily on signature-based detection.

Network Segregation

Devices associated with the Internet of Things (IoT), if exposed to the internet, can potentially escalate your network's vulnerability to attacks. To mitigate the risk of an attacker's lateral movements or the propagation of ransomware following an infection, segregate these devices within a DMZ (Demilitarized Zone).

Cybersecurity Awareness

Regular cybersecurity awareness training is a vital yet frequently overlooked component of a robust security program. Training the organization's personnel to identify phishing attempts and suspicious attachments, and to promptly report such incidents within the company significantly lowers the chances of malware infection or a ransomware attack.



Q3 2023

Botnet Events 2,274,028 total

42

unique variants detected

189,502

detections per week

27,071

detections per day

67.51%

increase in total activity from Q2

Botnets –

Botnets Skyrocket Nearly 70% Over Q2 2023

A dotted line in Figure 7 graphically represents the moving average of botnet operations during the second quarter, while a solid line is used to depict actual weekly figures, facilitating the detection of unusual patterns and sudden increases. Nuspire observed a **67.51% increase in activity** compared to the second quarter. Most of this increase was driven by the Torpig Mebroot Botnet and trailed off by the end of Q3.

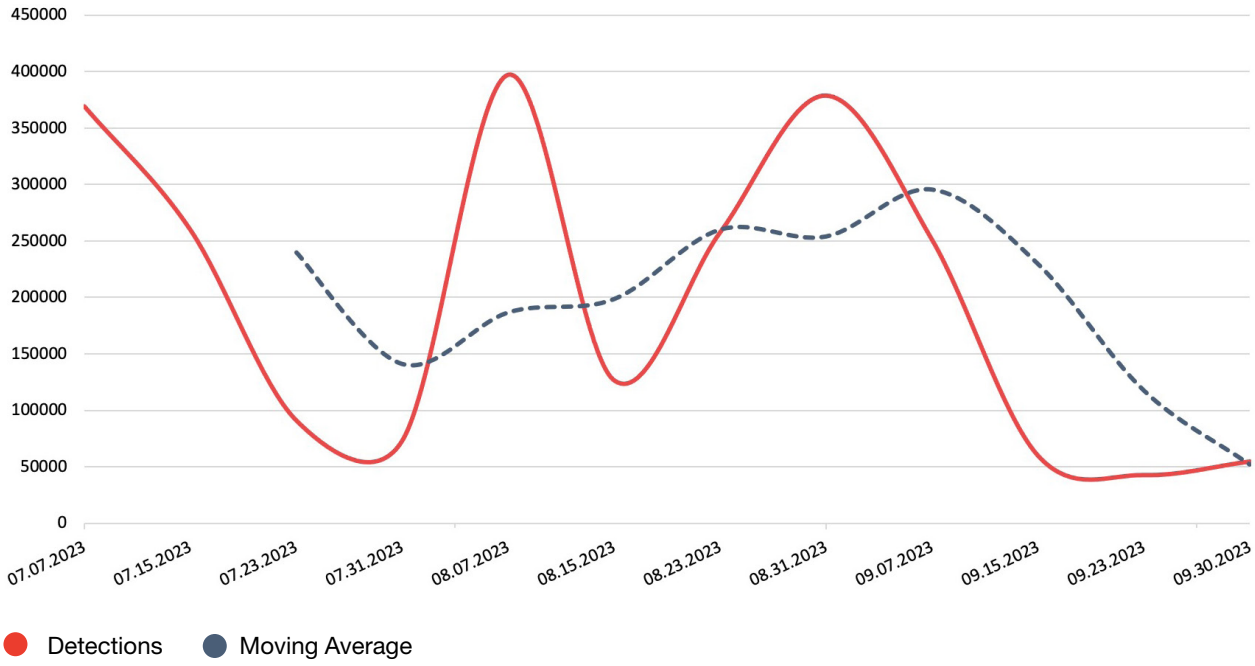


FIGURE 7. BOTNET ACTIVITY Q3 | NUSPIRE, Q3 2023

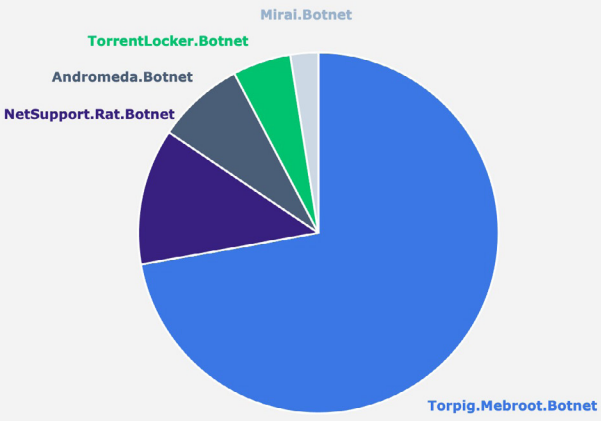


Figure 8 displays the botnets with the highest activity during the third quarter. Torpig Mebroot led the way, accounting for **over 69% of all botnet activities** observed in Q3. Meanwhile, NetSupport, Andromeda and Mirai made a return. Notably, the newly detected TorrentLocker has surpassed FatalRAT, placing it outside the top 5.

FIGURE 8. TOP FIVE BOTNETS | NUSPIRE, Q3 2023

Torpig Mebroot Botnet

Nuspire's examination reveals that Torpig Mebroot consistently holds its position as the top-ranking botnet. Its activities, marked by sporadic spikes, manifest a steady pattern when evaluated based on detection metrics. Notably, the activity growth from Q2 to Q3 was substantial, standing at an estimated **92.53%**. Thus, while Torpig's dominance remains largely unchanged, it has seen a notable escalation.

Torpig Mebroot, often termed Sinowal, represents a refined malware variant traced back to around 2007. This malware is structured around two primary elements: "Mebroot," a discreet rootkit platform, and "Torpig," a Trojan distinguished by its premier data pilfering capabilities. Torpig's expertise lies in gathering an expansive range of data, spanning credit card details to access credentials, leveraging tools such as keylogging, screenshot capture and form extraction.

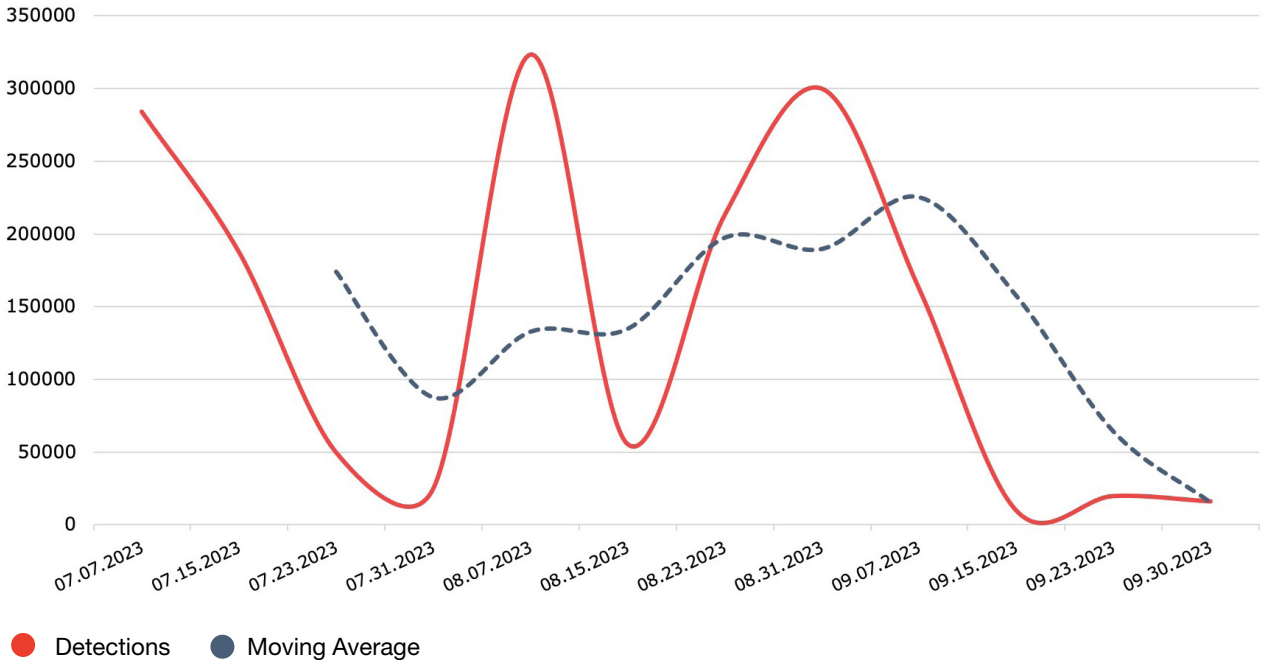


FIGURE 9. TORPIG MEBROOT ACTIVITY | NUSPIRE, Q3 2023

Typically, the botnet penetrates systems via methods like drive-by downloads, deceptive email attachments or phishing schemes. Unsuspecting users accessing compromised web portals frequently become its victims. Once entrenched in a system, the Mebroot facet of the botnet ensures the malicious presence is deeply anchored, making detection a formidable challenge.

As soon as it gains access to the host, Torpig establishes contact with its central servers. This liaison permits the receipt of fresh updates and directives while also facilitating the forwarding of pilfered data. Torpig's dominion over the compromised machine also empowers it to integrate into an extensive botnet array, a conglomerate of tainted devices primed for large operations, encompassing tasks such as distributed denial-of-service (DDoS) onslaughts.

TorrentLocker Botnet

An older botnet, TorrentLocker, re-emerged in Q3, clocking a spike in activity from the end of August to the beginning of September, as witnessed by Nuspire analysts.

Discovered in early 2014, TorrentLocker surfaced as a formidable ransomware. To the unsuspecting eye, it often masquerades as the infamous CryptoLocker or CryptoWall, as it borrows elements from both, but blends them together to create a uniquely supported ransomware entity. While most ransomware attacks utilize the RSA-2048 algorithm, TorrentLocker uses the Rijndael algorithm for encryption.

TorrentLocker is primarily delivered through phishing emails, enticing victims with unpaid invoices, undelivered packages or unpaid fines. The botnet has been known to quickly adapt to security researcher findings. The initial version of TorrentLocker was discovered to have a vulnerability that allowed self-decryption by victims. Once published publicly by security researchers, TorrentLocker quickly released a patch preventing this self-decryption by victims.

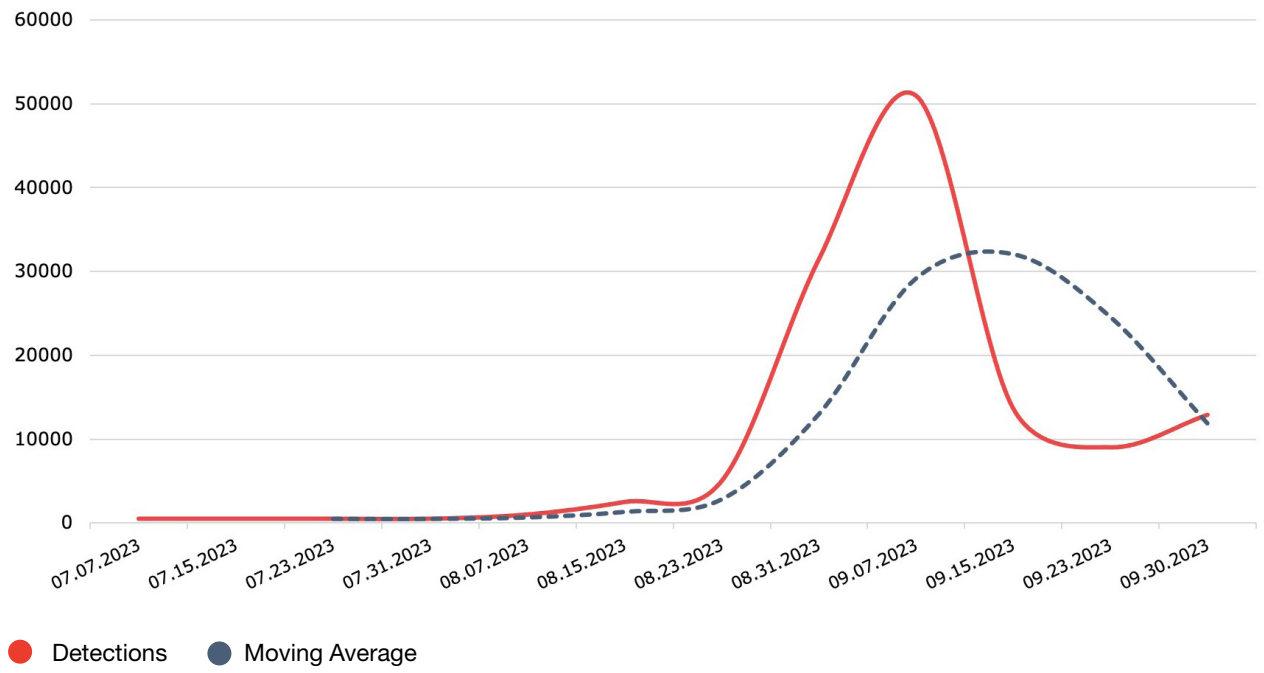


FIGURE 10. TORRENTLOCKER BOTNET ACTIVITY | NUSPIRE, Q3 2023

Ways to Combat These Threats

Botnet activity is typically identified following an infection, which is commonly propagated through phishing.

Employ Threat Intelligence

This provides vital data about botnet command-and-control architectures, alerting your organization to any communication with unauthorized parties. As botnet interactions occur post-infection, when the compromised device tries to connect, being cognizant of network traffic moving toward harmful destinations allows for suitable countermeasures.

Adopt Next-Generation Antivirus

Given that botnet interactions transpire after infection, the optimal approach is to thwart infection at the onset. Next-generation antivirus, using behavioral analysis, outperforms the conventional signature-based antivirus by detecting malicious activities on your devices.

Perform Proactive Threat Hunting

New command-and-control structures are established daily, and some might not be publicly recognized. Actively look for irregular activities within your environment. Scrutinize the motives behind system actions and ascertain their legitimacy. If suspicious, delve further to determine if the activities are malicious.

Q3 2023

Exploit Events
78,631,396 total

317

unique variants detected

6,385,949

detections per week

912,278

detections per day

-35.92%

decrease in total activity from Q2

Exploits –

Eight New Zero-Day Vulnerabilities Found in Microsoft Products

Figure 11 provides a visual representation of the trends in exploit 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.

Analyzing the raw data between Q2 and Q3 2023, there's a noticeable decline of **32.92%** in the overall activity. Although, it's essential to recognize that exploit activity has hit record numbers in 2023, so while we witnessed a decline, the volume of exploit activity is still exceedingly high.

Starting in early September, we observed an uptick in activity. Nuspire can attribute this increase primarily to a renewed wave of brute force attacks aimed at the Secure Shell (SSH) and Server Message Block (SMB) protocols.

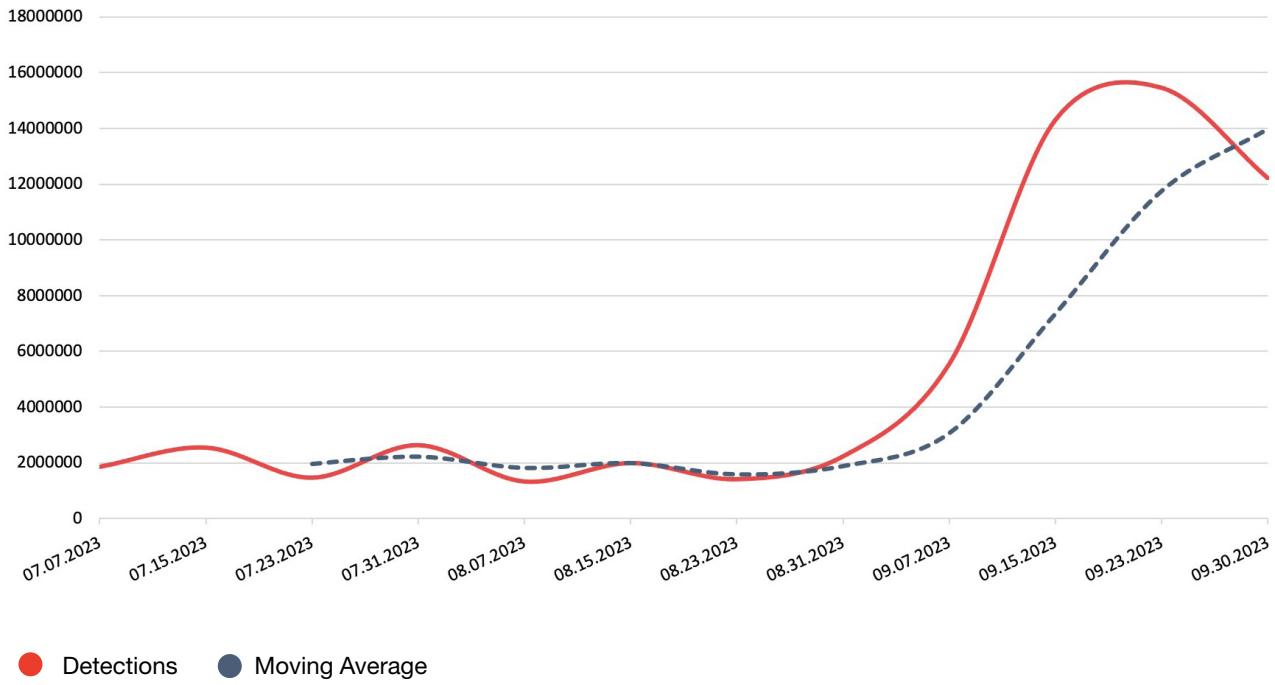


FIGURE 11. Q3 EXPLOIT ACTIVITY | NUSPIRE, Q3 2023

Top 5 Exploits

Figure 11 highlights the prevalent exploit attempts witnessed during the third quarter, setting aside brute force attacks because their sheer volume could eclipse other exploit types. Apache Log4j exploits remain a favorite for cyber adversaries when sidestepping brute force methods, as revealed in Figure 12.

Following closely is the HTTP Server Authorization Buffer Overflow, a formidable exploit targeting potential flaws in server authorization mechanisms, enabling threat actors to run arbitrary code on affected systems. Web Server Password File Access occupies the third spot, focusing on extracting vital data from safeguarded files. Bash Function Definitions Remote Code Execution takes the fourth position. Lastly, the fifth most observed exploit is the HTTP Request URI Directory Traversal, which facilitates unauthorized access beyond the designated web directory.

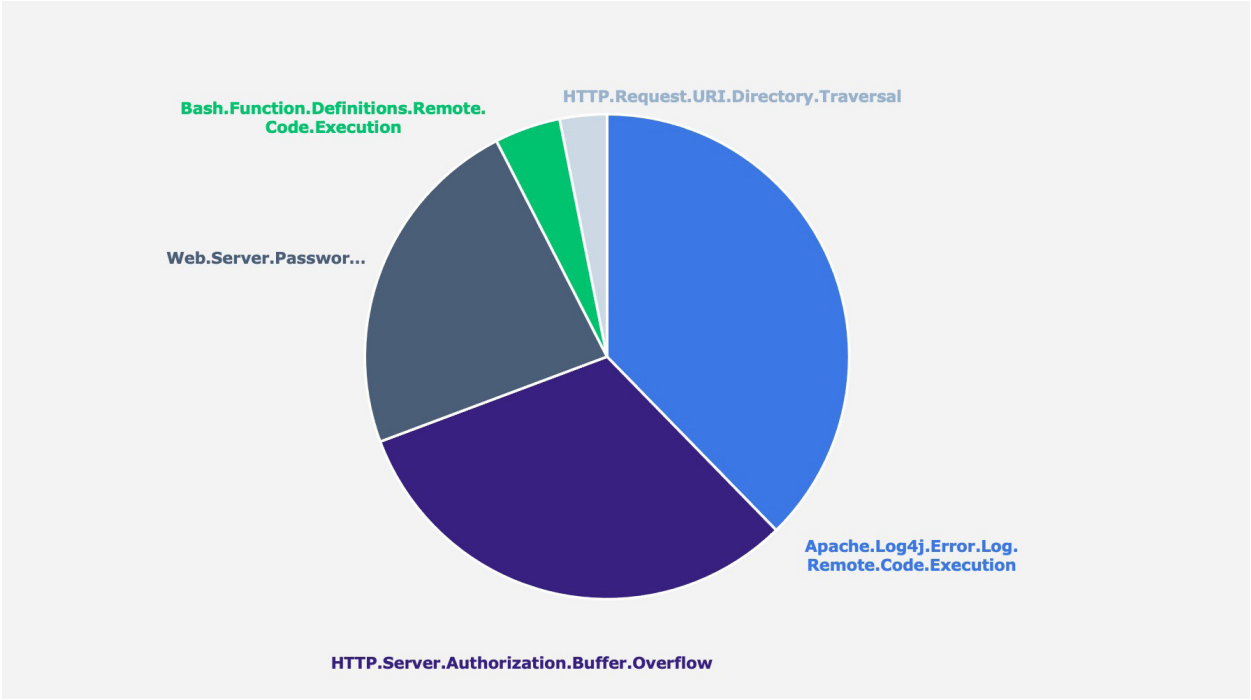


FIGURE 12. Q3 TOP WITNESSED EXPLOITS | NUSPIRE, Q3 2023

Microsoft CVE-2023-36884 RCE

CVE-2023-36884 is a significant zero-day vulnerability related to Microsoft Office and Windows HTML. This flaw, characterized by Microsoft as a remote code execution vulnerability with a CVSS score of 8.3, allows attackers to gain remote access through "specially crafted" Microsoft Office documents. To exploit it, attackers merely have to deceive victims into opening these malicious documents, leading to potential remote code execution in the context of the unsuspecting individual.

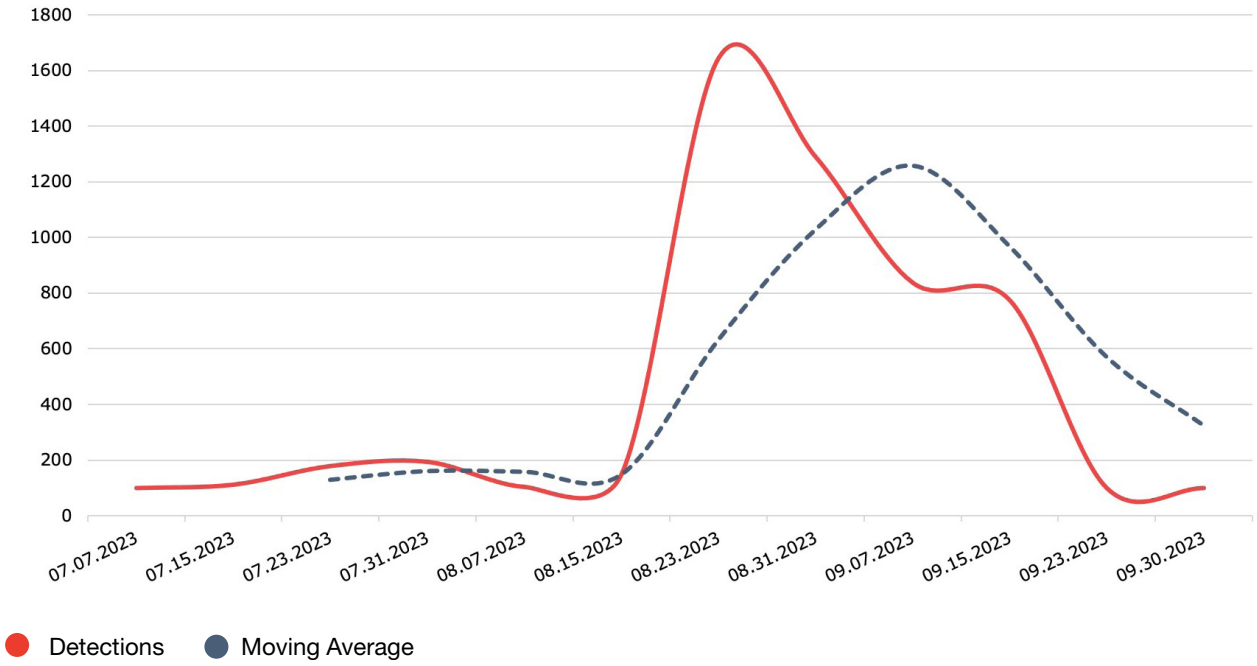


FIGURE 13. Q3 CVE-2023-36884 ACTIVITY | NUSPIRE, Q3 2023

Microsoft observed an alarming exploitation of this vulnerability by a threat actor they track as Storm-0978. In June, this adversary launched a phishing campaign targeting defense and governmental bodies across North America and Europe. The emails linked to Word documents, which, when opened, exploited CVE-2023-36884 to establish backdoors into the victim's systems. While espionage appeared to be a primary motive, Microsoft also detected Storm-0978 leveraging the same vulnerability for separate ransomware attacks, indicating a dual-threat potential.

Shortly after its announcement, Nuspire detected a spike in attempts to exploit CVE-2023-36884, followed by a gradual decline toward the end of the quarter. As this vulnerability is similar to the one previously reported in the malware section, CVE-2017-11882, we expect to see threat actors' continued exploitation of this vulnerability.

Microsoft “Patch Tuesday” Zero-Days Q3 2023

In addition to CVE-2023-36884 mentioned above, Microsoft revealed a total of eight new zero-days in its Q3 “Patch Tuesday” announcements.

DESCRIPTION	CVE	CVSS SCORING
MSHTML Platform Elevation of Privileges	CVE-2023-32046	7.8
SmartScreen Security Bypass	CVE-2023-32049	8.8
Error Reporting Service Elevation of Privileges	CVE-2023-36874	7.8
Office and Windows HTML RCE	CVE-2023-36884	8.8
Outlook Security Feature Bypass	CVE-2023-35311	8.8
Denial Of Service in Visual Studio	CVE-2023-38180	7.5
Streaming Proxy Elevation of Privileges	CVE-2023-36802	7.8
Word Information Disclosure	CVE-2023-36761	5.3

FIGURE 14. Q3 MICROSOFT ZERO-DAYS | NUSPIRE, Q3 2023

Organizations must prioritize patching their systems, especially as many vulnerabilities are actively targeted. Microsoft consistently rolls out patches on "Patch Tuesdays" (the second Tuesday of every month at 1 p.m. EST). Administrators must monitor these updates and be ready to implement patches swiftly. Effective communication within your organization about upcoming patches can make the difference, allowing you to counter threat actors eager to exploit vulnerabilities preemptively.

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

Without awareness of new vulnerabilities, protecting against them is impossible. Most vendors issue security bulletins that organizations can subscribe to, delivering vital information about patching and mitigation. It's crucial to subscribe to these bulletins and monitor updates regularly.

Deactivate unnecessary services

Any unused service should be disabled to avoid introducing extra vulnerabilities. A service shouldn't pose an additional potential attack path if it isn't required. It's also essential for organizations to understand which services are exposed to the internet and ensure their protection through VPN technology.

Industry Spotlight: Hospitality Services

The hospitality industry, encompassing sectors such as hotels, restaurants, travel agencies and cruise lines, has always been an integral part of the global economy, focusing on delivering memorable experiences and unparalleled service to its patrons. This industry, relying heavily on building and maintaining trust, has increasingly integrated technology to enhance customer experiences, streamline operations and offer personalized services. With the proliferation of digital touchpoints, from online reservations to smart room controls, the hospitality sector has transformed into a technologically advanced arena.

However, this digital evolution comes with its own set of challenges, especially in the realm of cybersecurity. As the industry collects vast amounts of personal and financial data from guests, it becomes a lucrative target for cybercriminals. Unfortunately, data breaches, ransomware attacks and phishing schemes have become common occurrences, with both major chains and small establishments falling victim. Additionally, the interconnected nature of the services, from third-party booking sites to in-room IoT devices, expands the potential vulnerabilities that attackers can exploit. As such, cybersecurity has swiftly moved from being an IT concern to a top priority for hospitality leaders worldwide.

Threat Groups that Target the Hospitality Industry

Numerous threat groups are known to target the hospitality industry vertical; these are some of the most prevalent:

THREAT GROUP	ALSO KNOWN AS	COUNTRY OF ORIGIN
UNC3944	Scattered Spider	Eastern European
APT28	Fancy Bear	Russia
FIN7	Carbon Spider	Eastern European
APT41	Wicked Panda	China
TrickBot	Wizard Spider	Russia
FIN5	N/A	Eastern European
Carbanak	Carbon Spider	Eastern European
FIN6	Skeleton Spider	Unknown
FIN8	N/A	Eastern European
APT39	Remix Kitten	Iran
Maze Team	Twisted Spider	Eastern European
APT36	Mythic Leopard	Pakistan
APT32	Ocean Buffalo	Vietnam
TA544	Narwhal Spider	Unknown

Some common methods appear when reviewing these groups' tactics, techniques and procedures (TTPs). Below are some of the top TTPs utilized by these groups. Organizations should ensure they can mitigate and detect these types of events.

TECHNIQUE	ID
Phishing	T1566
Valid Accounts	T1078
OS Credential Dumping	T1003
Adversary-in-the-Middle	T1557
External Remote Services	T1133
Brute Force	T1110
Scripting	T1059
Hardware Additions	T1200
Input Capture	T1056
Scheduled Task/Job	T1053
Data Encrypted for Impact	T1486
Supply Chain Compromise	T1195
Exfiltration Over C2 Channel	T1041
User Execution	T1204

How to Combat Common Techniques Used Against the Hospitality Industry

Address the following TTPs with confidence

1. **Spear Phishing (T1566):** Implement a robust security awareness training program for all employees to recognize and report potential phishing attempts. Use email filtering solutions to block malicious emails.
2. **Valid Accounts (T1078):** Ensure strong, unique passwords are used and enforce multi-factor authentication (MFA) wherever feasible. Regularly review and revoke unnecessary user privileges and monitor user logins for any suspicious activity.
3. **OS Credential Dumping (T1003):** Use solutions to detect and prevent unauthorized system and memory access. Implement Credential Guard in Windows environments and regularly monitor for suspicious system access or activity.
4. **Adversary-in-the-Middle (T1557):** Employ strong encryption for both data in transit and at rest. Ensure that all systems use secure and verified certificates. Educate staff and guests about the risks of connecting to unsecured public Wi-Fi.
5. **External Remote Services (T1133):** Limit the number of external-facing systems and ensure they are appropriately hardened. Any remote administration should be conducted over a VPN with MFA enabled.
6. **Brute Force (T1110):** Implement account lockout policies to thwart brute force attempts. Use CAPTCHA and other similar mechanisms on public-facing sites to deter automated bots.
7. **Scripting (T1059):** Control and manage the execution of scripts in your environment by using application allowlisting solutions. Regularly review and monitor scripts running in the environment for unusual or malicious behavior.
8. **Hardware Additions (T1200):** Establish and enforce strict physical security measures for sensitive equipment or information areas. This includes access controls, surveillance and regular audits of access logs.
9. **Input Capture (T1056):** Educate staff about the dangers of suspicious devices like rogue keyboards or keyloggers. Regularly inspect physical connection points (like USB ports) for any unfamiliar devices.
10. **Scheduled Task/Job (T1053):** Monitor and manage all scheduled tasks. Avoid using shared or domain-wide accounts for scheduled tasks, and ensure that only necessary tasks have permission to execute.
11. **Data Encrypted for Impact (T1486):** Regularly back up important data and ensure it can be restored quickly. Keep offline backups and educate employees about ransomware threats. Test restoration capabilities periodically.

12. **Supply Chain Compromise (T1195):** Perform due diligence and risk assessments of all your third-party vendors, suppliers and partners. Clearly outline security expectations in service contracts. Ensure vendors hold relevant security certifications and comply with regulations and industry standards.
13. **Exfiltration Over C2 Channel (T1041):** Implement network segmentation and employ intrusion detection and prevention systems (IDS/IPS) to monitor and block suspicious outbound traffic. Regularly review network logs for data transfer anomalies.
14. **User Execution (T1204):** Implement security awareness training to educate users about the risks of executing unknown or unsolicited files and attachments and falling victim to vishing (voice phishing) attempts. Emphasize the importance of verifying unsolicited communication over the phone, especially requests for sensitive information or actions. Use endpoint protection solutions to detect and block malicious file executions. Set up file reputation services to alert or deny the execution of unknown or suspicious files. Limit the file types that can be received via email or downloaded from the internet to reduce the risk of malicious files reaching end-users.

These recommended mitigations should serve as a foundation for strengthening security postures against the mentioned TTPs. Given the dynamic nature of threats, continuous monitoring and updating of defense strategies are crucial.

MGM Ransomware Attack

MGM Resorts International, a premier hospitality and entertainment entity, faced a debilitating cyberattack that disrupted its operations and resulted in a $100 million setback for its third quarter results. The breach, claimed by ransomware group ALPHV (also known as BlackCat), reportedly involved a collaboration with Scattered Spider. Scattered Spider is a group known for focusing on social engineering tactics to gain initial access into their victims' organizations. The specifics of the attack were notably simple yet devastating. Using vishing, the attackers identified an MGM employee on LinkedIn and posed as that employee to deceive the help desk over the phone, granting them unauthorized system access.

The breach's aftermath exposed a range of customer data, including contact details and more sensitive information like SSNs and passport details. This incident, combined with a similar, costly attack on Caesar's Entertainment, underscores the profound vulnerabilities organizations face when overlooking the human element of security. While MGM managed to contain the breach's ramifications, its share price dropped by 6%, and the trust in its brand was undeniably shaken.

The MGM cyberattack serves as a stark reminder of the importance of robust security protocols and employee training. Despite involving complex hacking groups, many such breaches leverage simple security lapses, like an untrained employee or lax help desk verification processes. Proper employee training regarding phishing and vishing threats, combined with multi-factor authentication and stringent verification procedures, could have potentially averted this breach. By investing proactively in these mitigation strategies, companies like MGM can protect their financial assets and safeguard their brand reputations.

Q3 Threat Landscape Reinforces Need For Advanced Security Defenses

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.

Fortify Your Defenses with Additional Resources from Nuspire

- eBooks
- Blogs
- Videos
- Reports

The following are five simple actions security leaders can take to safeguard their organization and reduce 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 on common theming, including any major events that could be created into a phishing lure. Establish 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. Once an attacker has compromised an email account, they will often 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 single 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.

Devices that are internet-facing 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 into 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 that 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.

Navigating today's digital battlefield can be difficult, but it doesn't have to be.

Contact us for help protecting your organization from these latest threats.

About Nuspire

Nuspire is a leading managed security services provider (MSSP) that 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 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. Our client base spans thousands of enterprises of all sizes, across multiple industries, and achieves the greatest risk reduction per cyber-dollar spent. At Nuspire, we are laser focused on delivering an extraordinary cybersecurity experience that exceeds client expectations.

For more information, visit nuspire.com and follow @NuspireNetworks on Twitter.

nuspire.com
LinkedIn @Nuspire
Twitter @NuspireNetworks