nuspire

QUARTERLY

Threat Landscape Report

Q2 2020

NUSPIRE.COM

THIS REPORT IS SOURCED FROM

90 BILLION TRAFFIC LOGS

INGESTED FROM NUSPIRE CLIENT SITES

AND ASSOCIATED WITH THOUSANDS

OF DEVICES AROUND THE GLOBE.

Contents

Introduction

At the beginning of Q2, the world was experiencing the widespread effects of the COVID-19 pandemic. Organizations scrambled to shift to—and protect—work from home (WFH) environments.

In a recent IDC survey, the total of organizations with more than seven breaches is 58% over the past 12-24 months.[1] So it's no wonder why security leaders have become increasingly concerned with protecting their business operations and IT environments. According to recent research from IDC, the top five greatest concerns are:[2]

1. Data Breaches
2. Malware
3. Target attacks
4. System vulnerabilities
5. Denial of Service (DoS)

In instances where operations may have remained steady in the WFH shift, new attack vectors and challenges for network administrators were created, including:

- VPN usage
- Home network security issues
- Personal device usage for business purposes
- Auditability of network traffic

[1] IDC, Most Organizations Have Experienced a Breach in the Past One to Two Years, Doc # US46774820, August 2020

[2] Forthcoming doc #US46762320

These new attack vectors make securing a virtual organization even more challenging. Not only do they create more opportunity for threat actors to gain a foothold, they make it harder for security teams to quickly detect and respond to threats with limited resources and bandwidth. A recent IDC managed detection and response (MDR) survey found that nearly 40% of participants noted the need to engage security service providers to reduce mean-time-to-detect (MTTD) as well as the equally important mean-time-to-respond (MTTR) KPIs.[3]

"Understanding the current threat landscape and your environment is crucial to improving your overall cybersecurity posture, said Craig Robinson, Program Director, Security Services at IDC. "Partnering with a managed security services provider (MSSP) like Nuspire enables organizations to understand current threats and engage in proactive threat hunting to identify threats before they impact the business."

This report explores recent cybersecurity challenges and presents our findings and analysis. Aggregated and correlated data from our enterprise and mid-market client datasets provide a unique vantage point.

We begin with an overview of the most prevalent cybersecurity headlines throughout the second quarter of 2020. Reported breach headlines play a crucial role in trend identification, as evidenced by findings highlighted throughout this report.

The report concludes with recommendations to secure your organization from these threats and to improve cyber hygiene that may have fallen by the wayside as security budgets declined due to the pandemic.

[3] IDC, MDR: The Next Generation of Managed Security Services, Doc # US46427920, June 2020

Summary of Findings

12%
decrease in total activity from Q1

1,597,858
MALWARE EVENTS

26,156,165
EXPLOITATION EVENTS

12.8%
increase in total activity from Q1

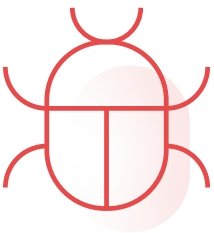
29%
increase in total activity from Q1

1,620,910
BOTNET EVENTS

Methodology and Overview

Nuspire's Security Intelligence and Analytics (SIA) team follows the following five step data analysis methodology.

1. **Acquisition.** Sources threat intelligence and data from global sources, client devices and reputable third parties.
2. **Analytics.** Data is analyzed by a combination of machine learning, algorithm scoring and anomaly detection.
3. **Analysis.** Analysts further scrutinize the research, scoring and tracking of existing and new threats.
4. **Alerting.** 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.
5. **Action.** Analysts leverage the insights to constantly improve the threat intelligence Improvements are gained from continuously reviewing processes, evaluation methods, and disseminating knowledge via sandboxing, malware analysis, honeypot activity, and alert creation.



MALWARE

BOTNET

EXPLOIT

Quarter in Review

APRIL 1 — Targeted Phishing Campaigns Against Zoom Meetings

APRIL 16 — Google Witnesses Over 18 Million Daily Malware and Phishing Emails Related to COVID-19

MAY 6 — APT Groups Targeting Healthcare and Essential Services

MAY 11 — Thunderbolt Vulnerability affects all devices manufactured in 2019 and earlier

MAY 22 — Two new massive COVID-19 Phishing campaigns identified

MAY 28 — Michigan State University falls victim to NetWalker Ransomware

JUNE 1 — BazarBackdoor Malware targeting remote employees

JUNE 3 — Revil Ransomware Group starts an Auction site to sell stolen data

JUNE 5 — Unpatched Microsoft Systems vulnerable to CVE-2020-0796

JUNE 9 — Honda Investigates Network Outage due to Ransomware attack

JUNE 11 — Black Lives Matter Voting Campaign Used to Spread TrickBot Trojan

JUNE 12 — FBI Warns that Cybercriminals are increasingly targeting mobile banking apps

JUNE 15 — New Black Kingdom Ransomware Exploits Pulse Secure VPN Flaw to Target Enterprise Networks

JUNE 29 — Trickbot Delivered Via 'Black Lives Matter' Themed Malspam

JUNE 30 — Multiple Netgear Router Vulnerabilities Announced

Malware

Malware Events

1,597,858
TOTAL MALWARE EVENTS

12%
DECREASE IN TOTAL ACTIVITY FROM Q1

1149
UNIQUE VARIANTS DETECTED

4.4%
DECREASE IN UNIQUE VARIANTS DETECTED FROM Q1

133,154
VARIANTS DETECTED PER WEEK

38%
DECREASE IN WEEKLY DETECTIONS FROM Q1

17,753
VARIANTS DETECTED PER DAY

37%
DECREASE IN DAILY DETECTIONS FROM Q1

Malware Detection

In Figure 1, average Q2 malware activity is represented in a dashed trend line. The solid line shows the true weekly numbers to help identify spikes and abnormal activity. Looking across Nuspire devices, there was a 12% decrease in total malware activity in comparison to Q1 numbers, and a 4.4% decrease in unique variants. From start to finish of Q2, activity remained consistent with no major anomalies, resulting in an overall 8% increase.

The decrease in malware activity may be misleading as numerous employees moved to a WFH environment. With this shift, end users' network connections may not be routing through their enterprise device—making them vulnerable to undetected infections.

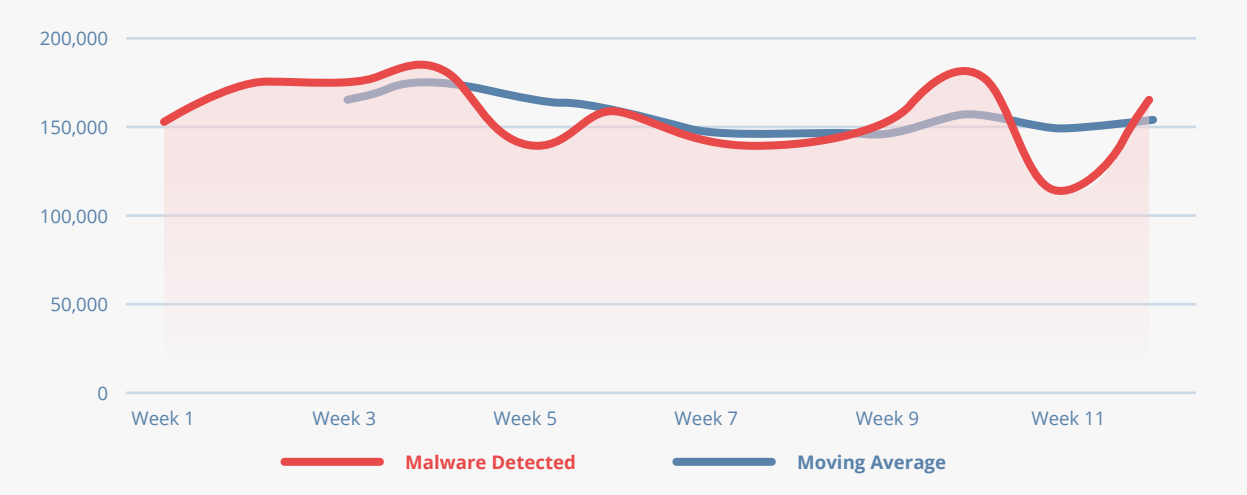


Figure 1. Malware detection, Nuspire, Q2 2020

Emotet

Emotet has consistently been the top offender in Nuspire threat reports, and only seems to be growing in popularity. Due to its ease of use and access for malicious actors, it is extremely customizable and easily widespread through malspam campaigns. During Q2, COVID-19 themed malware became a very popular wrapping due to the chaos the pandemic has caused. Google reported that they were blocking more than 100 million phishing emails a day and almost a fifth of those were COVID-19 themed.[4] Nuspire has also witnessed samples of Emotet with COVID-19 theming in our mail quarantines.

Emotet can be a challenge as it is a wormable malware that spreads to other network connected devices to load additional malware, such as ransomware on infected machines. During Q2, Emotet was seen paired with TrickBot to help deliver the ransomware Ryuk.

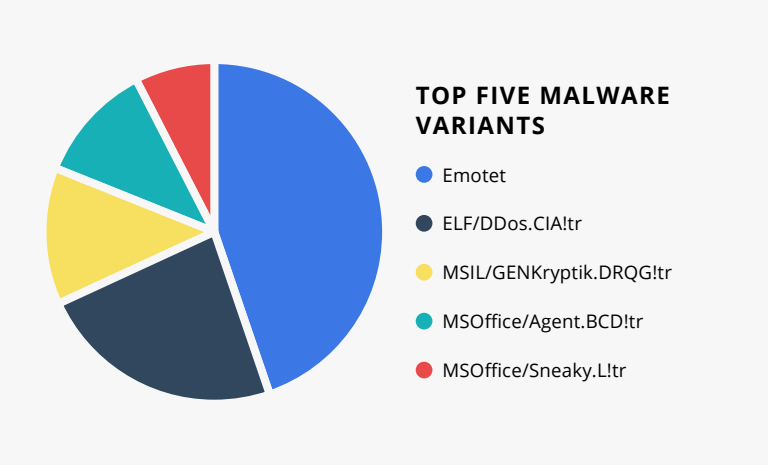


Figure 2. Top five malware variants, Nuspire, Q2 2020

Figure 3 shows witnessed Emotet activity across Q2. From the start of the quarter, to its finish, there was a 6.21% decrease in activity. Overall, activity was fairly consistent with no major variances. The popularity of Emotet activity is expected to remain steady, if not grow, except in moments of retooling or retheming of campaigns. Further research and threat intelligence have shown the majority of Emotet controller internet protocols (IPs) resolve in Latin America.

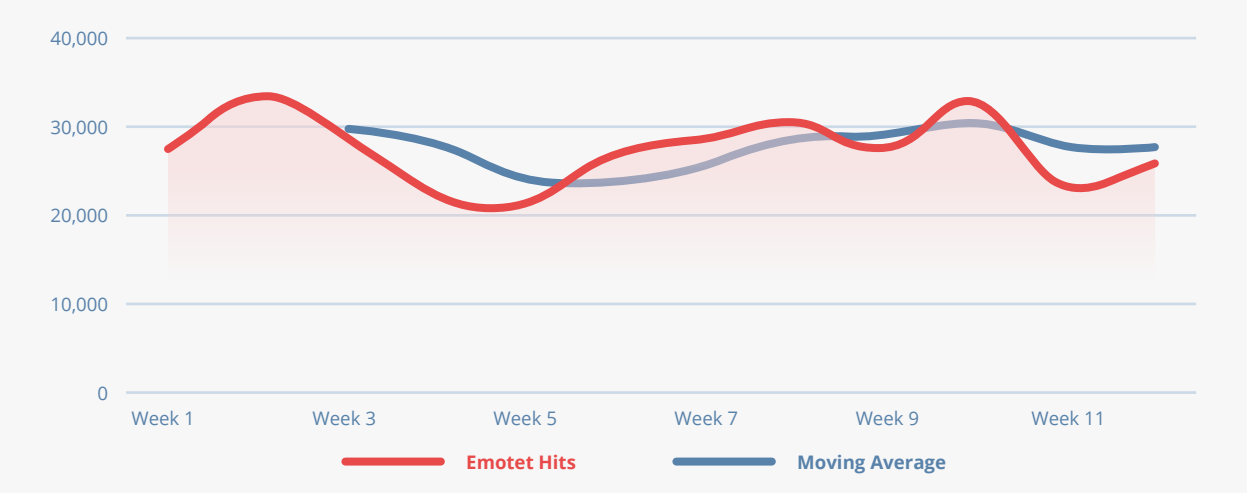


Figure 3. Emotenet activity, Nuspire, Q2 2020

[4] Google, Protecting Businesses Against Cyber Threats During COIVD-19 and Beyond, April 16, 2020

MSOffice/Sneaky.L!tr

A signature that specifically identified “sneaky” Microsoft Office documents, and are classified as Trojans, was introduced near the end of May. These documents do not contain any specific variant of malware. Instead, they contain malicious macros that reach out to command and control servers to download whatever variant of malware the campaign author is spreading. Malicious actors have taken this route in an attempt to avoid filtering controls. Very few organizations can afford to block Microsoft Office file attachment types. These documents are typically portrayed as legal documents, invoices or other important documents inferring a sense of urgency. They contain images to coerce the user into enabling macros as shown in Figure 4.

This signature is not tied to a specific malware type; therefore, wide variances are expected as campaigns spin up and wind down. Nuspire expects to see this signature place very high in our Q3 data, possibly usurping Emotet as the top threat. This signature demonstrates to administrators the importance of social engineering and phishing awareness training for their end users.

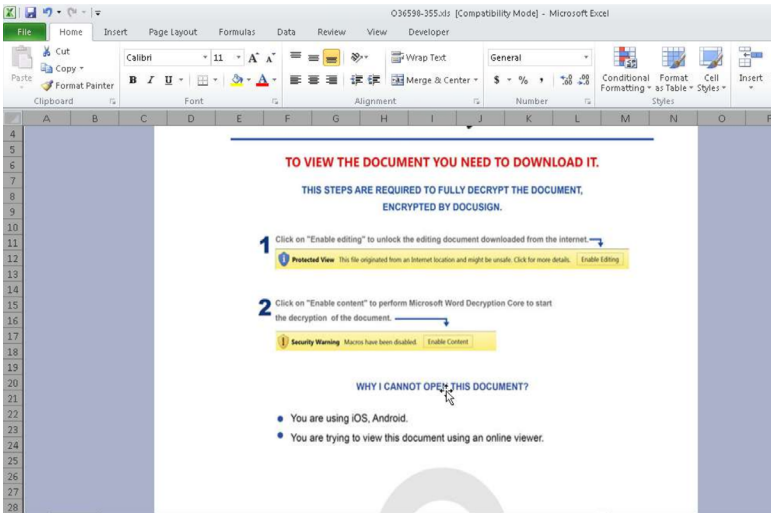


Figure 4. Example of MSOffice/Sneaky.L!tr, Nuspire, Q2 2020

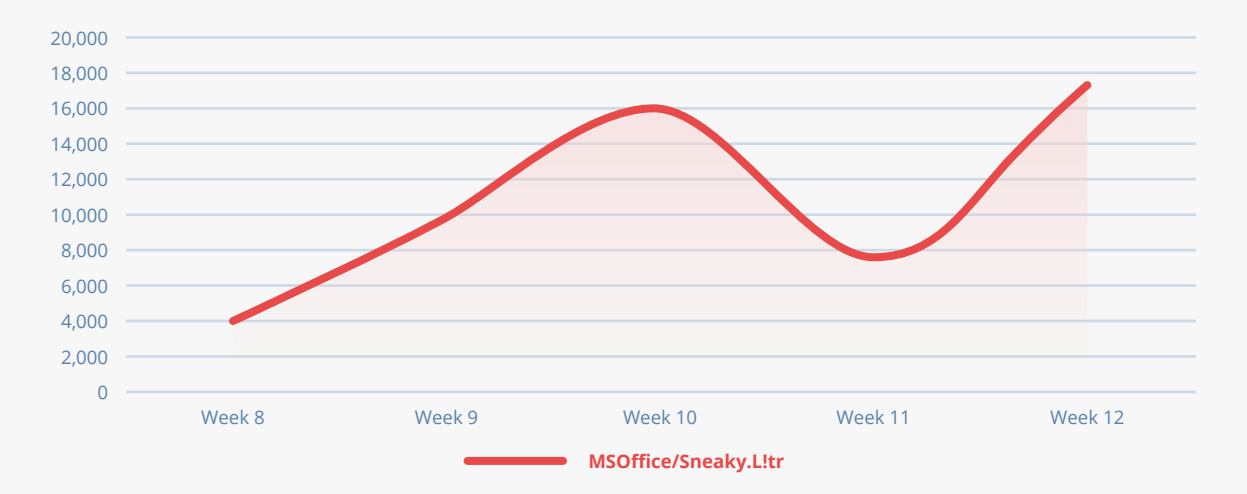


Figure 5. MSOffice/Sneaky.L!tr Activity, Nuspire, Q2 2020

How to Combat

PROACTIVE DETECTION AND MITIGATION MEASURES

Endpoint Protection Platforms (EPP). Implement security in-depth while utilizing advanced, next-generation antivirus (NGAV). NGAV will detect malicious software not only through signatures, but through heuristics and behavior. Legacy AV is strictly signature based and can only detect already known variants of malware.

Network Segregation. Segregate higher risk devices from the organization's internal network, like IoT devices. This will minimize the attacker's ability to laterally move throughout a network.

User Awareness. Cybersecurity awareness training is a critical part of any security program as most infections start through email and interaction with a malicious attachment. Administrators should block email attachments that are commonly associated with malware such as .dll and .exe extensions to prevent these from reaching their end users.

Botnets

Botnet Events

1,620,910
TOTAL BOTNET EVENTS

29%
INCREASE IN TOTAL ACTIVITY FROM Q1

46
UNIQUE BOTNETS DETECTED

0%
CHANGE IN UNIQUE BOTNETS DETECTED FROM Q1

135,075
INFECTIONS PER WEEK

18.69%
INCREASE IN WEEKLY DETECTIONS FROM Q1

18,010
INFECTIONS PER DAY

13.33%
INCREASE IN DAILY DETECTIONS FROM Q1

Botnet Detection

Compared against Q1's data, botnet activity increase by 29% with a large spike in week eight attributing to most of the data. The majority of week eight data was associated with the ZeroAccess botnet. From the beginning of Q2, to peak activity in week eight, there was a 733% increase that declined back by the end of the quarter.

Figure 6 below shows a moving average of botnet activity throughout Q2 as a dashed line, whereas the solid line illustrates the true weekly numbers to help identify spikes and abnormal activity.

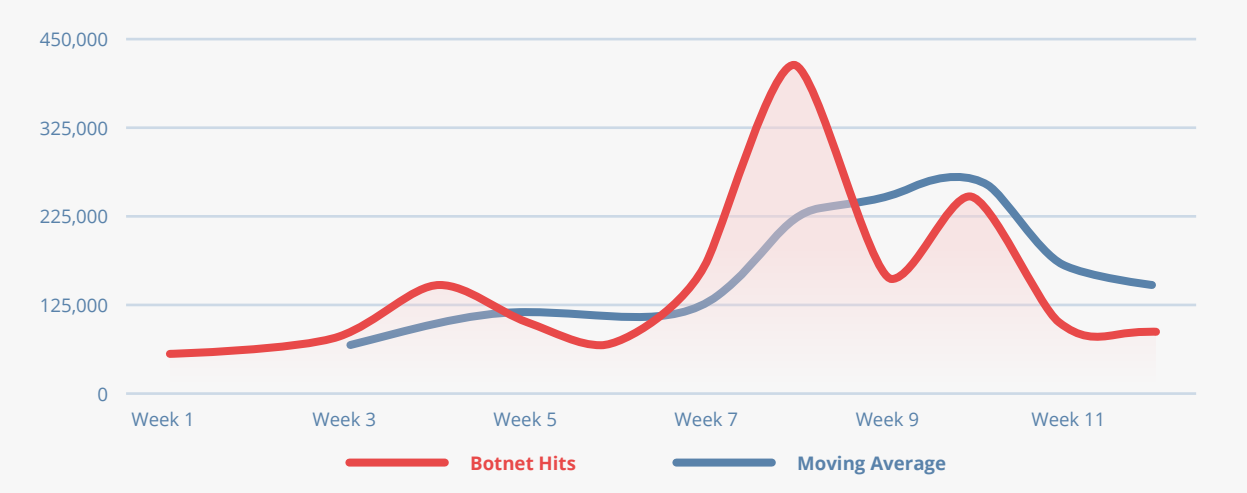


Figure 6. Botnet infections, Nuspire, Q2 2020

As predicted in Q1, the Andromeda botnet traffic declined and fell out of the top five observed botnets. As the botnet has been shut down, numbers are expected to continue to decrease until all infections are cleaned up. The ZeroAccess botnet took the top of the list closely followed by the Cidox botnet in Q2.

Figure 7, right, shows the top five botnets witnessed in Q2.

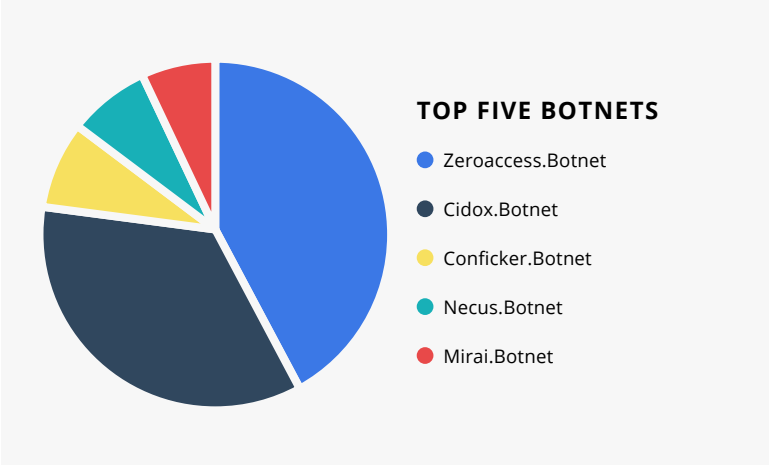


Figure 7. Top Five Botnets, Nuspire, Q2 2020

ZeroAccess

The ZeroAccess botnet debuted in 2009 and saw its peak in 2013. During that peak, it was estimated that 1.9 million PCs were infected. The botnet focused mostly on financial organization with click fraud and bitcoin mining. In December of 2013, Microsoft and law enforcement partners worked together to disrupt ZeroAccess and effectively shut the botnet down. In 2014 and in 2015 the botnet was reactivated by the botnet owners and began attacking organizations again. The ZeroAccess botnet's source code has since been leaked, allowing attackers to take that code and create their own versions of it. Many variants of the ZeroAccess botnet have appeared in the wild since which may attribute to it triggering signatures of the botnet.

In reviewing the ZeroAccess data in figure 8 below, it appears a large wave of hits began around week eight of Q2 and then began to trail off. This wave of hits may be due to a campaign using ZeroAccess' source code or the botnet owners may have reactivated the botnet again—initiating a resurgence. We plan to review Q3's dataset to determine if the botnet is still relevant to gain insight into operations.

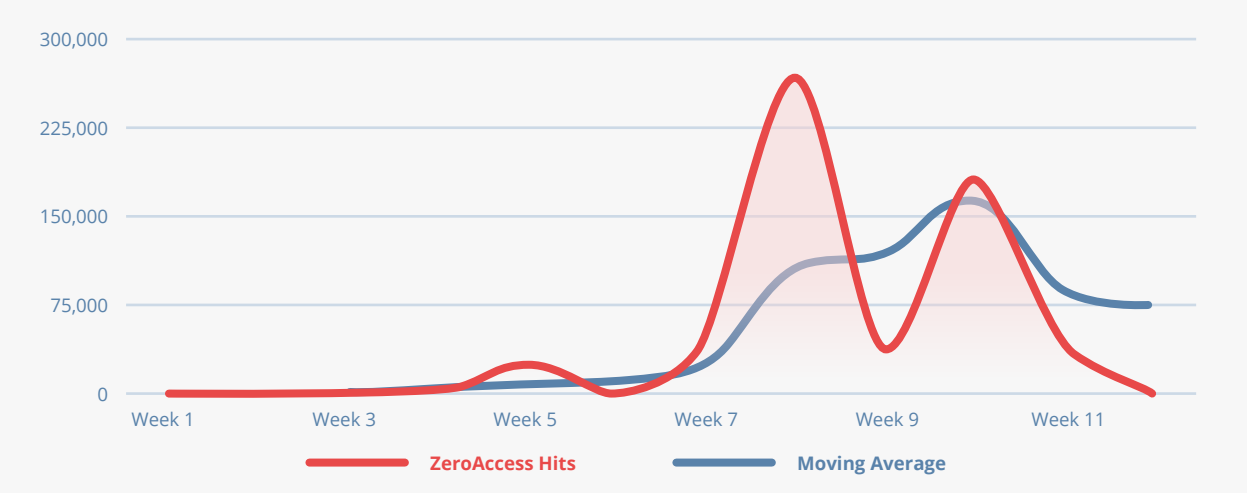


Figure 8. ZeroAccess botnet activity, Nuspire, Q2 2020

Cidox

Cidox is a botnet that is spread via a rootkit that targets Microsoft Windows users and injects itself into running processes like Internet Explorer, svchost and Google Chrome. Once hooked into the process, it will redirect the user to unwanted links and gathers host information to transfer back to the command and control servers. Cidox has been consistently seen across quarters at Nuspire, but had some spikes suggesting campaigns involving the rootkit may have been run during week four and week eight of Q2.

Since the beginning of the quarter, there has been a 201% surge in Cidox activity in week four and a 241% surge in week eight. Activity declined to a 12% increase from start of quarter to end as shown in figure 9.

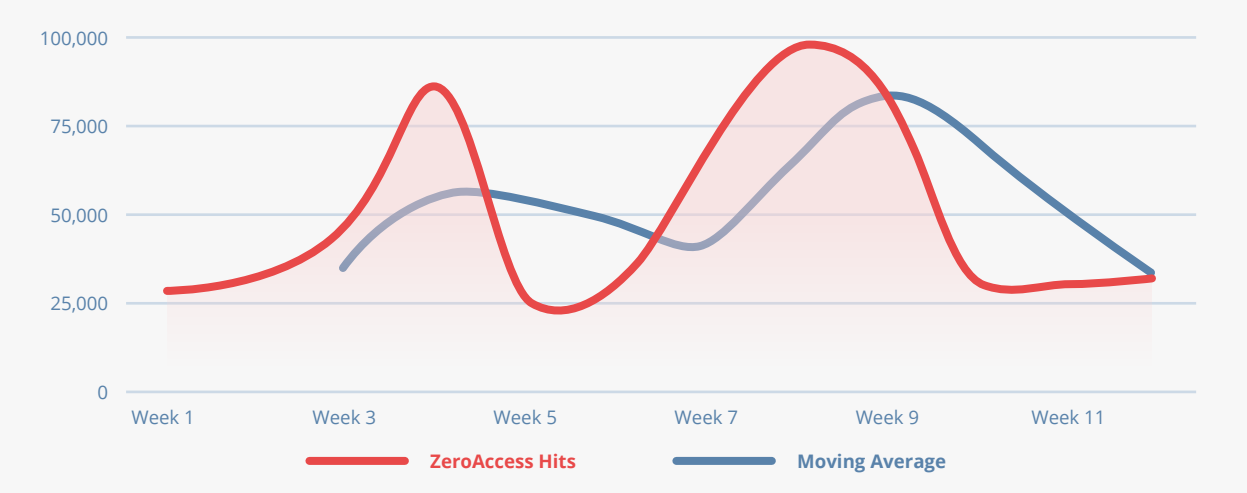


Figure 9. Cidox botnet activity, Nuspire, Q2 2020

How to Combat

PROACTIVE DETECTION AND MITIGATION MEASURES

Botnet activity is typically detected post-infection and is often spread via phishing.

Leverage Threat Intelligence. Threat intelligence helps organizations identify if devices are reaching out to known malicious hosts with C2 communication. C2 communications can contain commands or could be used to download additional malware. Correlation of networking logs and threat intelligence is critical to identify when this is happening to allow administrators to block malicious traffic and remediate infected machines.

Use Next Generation Antivirus. Botnet traffic is detected post-infection and if your antivirus is not capable to detect malicious behavior, you may be missing malicious programs without a known signature. A solution such as endpoint protection and response (EPR) can assist with detection as well as provide endpoint log visibility to detect malicious traffic.

Threat Hunt. Threat intelligence isn't perfect. New malicious C2 servers are found every day. Organizations should audit their network data for abnormal traffic and react if found. Should your server be reaching out to that foreign IP address?

Exploits

Exploit Events

26,156,165
TOTAL EVENTS

13.72%
INCREASE IN TOTAL ACTIVITY FROM Q1

359
UNIQUE EXPLOITS

11.14%
DECREASE IN UNIQUE EXPLOITS DETECTED FROM Q1

2,179,680
EXPLOITS DETECTED PER WEEK

13.04%
INCREASE IN WEEKLY DETECTIONS FROM Q1

290,624
EXPLOITS DETECTED PER DAY

3.24%
INCREASE IN DAILY DETECTIONS FROM Q1

Exploit Detection

In Q2, there was an increase in exploit activity by 13.72%, with an 11% decrease in unique variants when compared against Q1's data.

Figure 10 below shows a moving average of exploit activity throughout Q2 as a dashed line, the solid line shows the true weekly numbers to help identify spikes and abnormal activity along with the top protocol's exploits were attempted against.

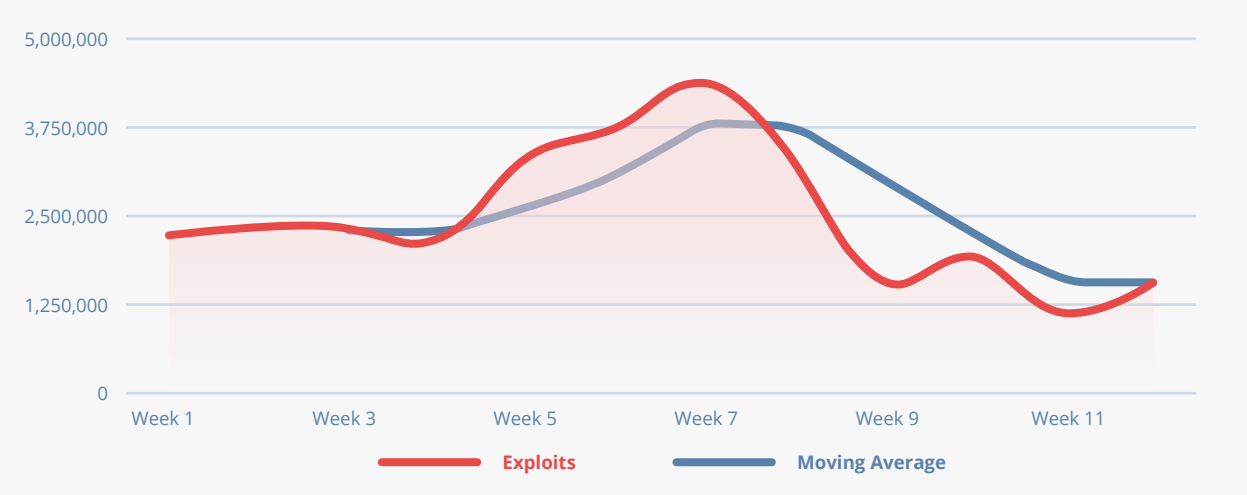


Figure 10. Exploits detected, Nuspire, Q2 2020

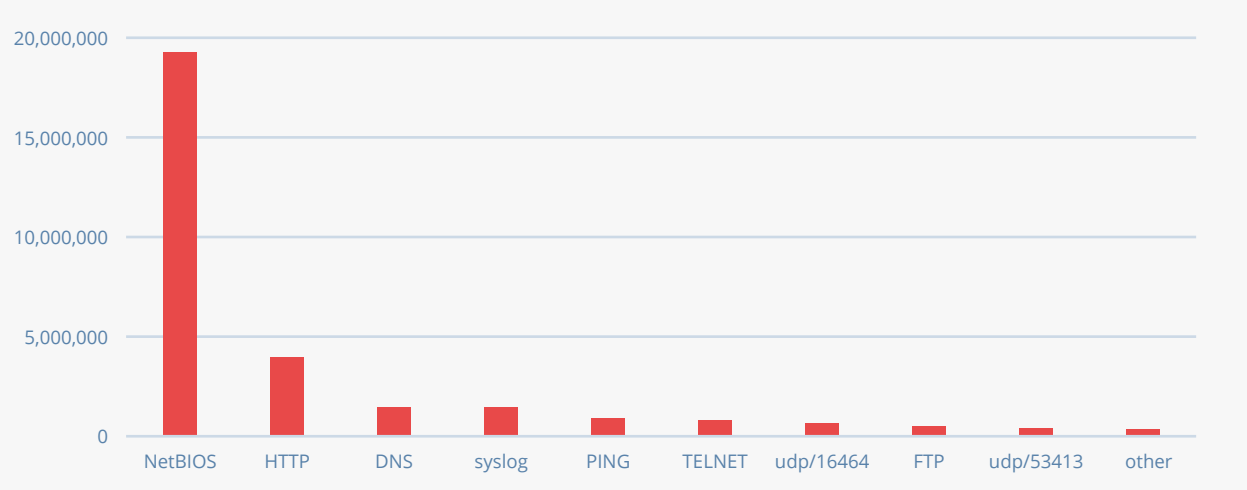


Figure 11. Protocols Exploited, Nuspire, Q2 2020

Q2 saw a negative 28% decrease in activity from the beginning of quarter to the end. DoublePulsar continues to dominate the exploit chart, as it has in previous quarters, comprising 72% of all exploit attempts witnessed by Nuspire.

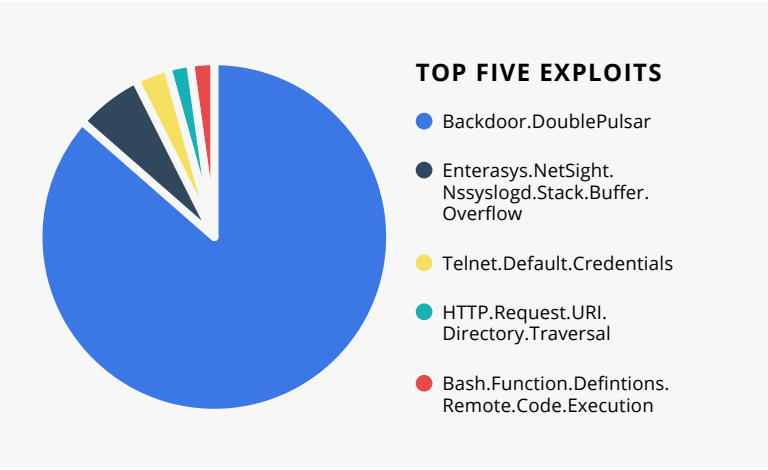


Figure 12. Top Five Exploits, Nuspire, Q2 2020

DoublePulsar

In Q2 the top exploit continues to be DoublePulsar. This exploit was leaked by the ShadowBrokers group in 2017 through an exploitation framework called FuzzBunch. DoublePulsar is most infamous in the deployment of the WannaCry ransomware and Nyeta worms and is an extremely sophisticated payload that is said to have originated with the National Security Agency (NSA). Once a device is infected, it opens a backdoor to allow additional malware to be loaded—further infecting its target.

Every server message block (SMB) and remote desktop protocol (RDP) exploit within FuzzBunch uses DoublePulsar as the primary payload.

DoublePulsar is expected to continue to dominate the charts as a highly used exploit due to its sophistication and ease of use with FuzzBunch. Administrators should ensure that they are using updated intrusion prevention signatures that can detect this exploit attempt.

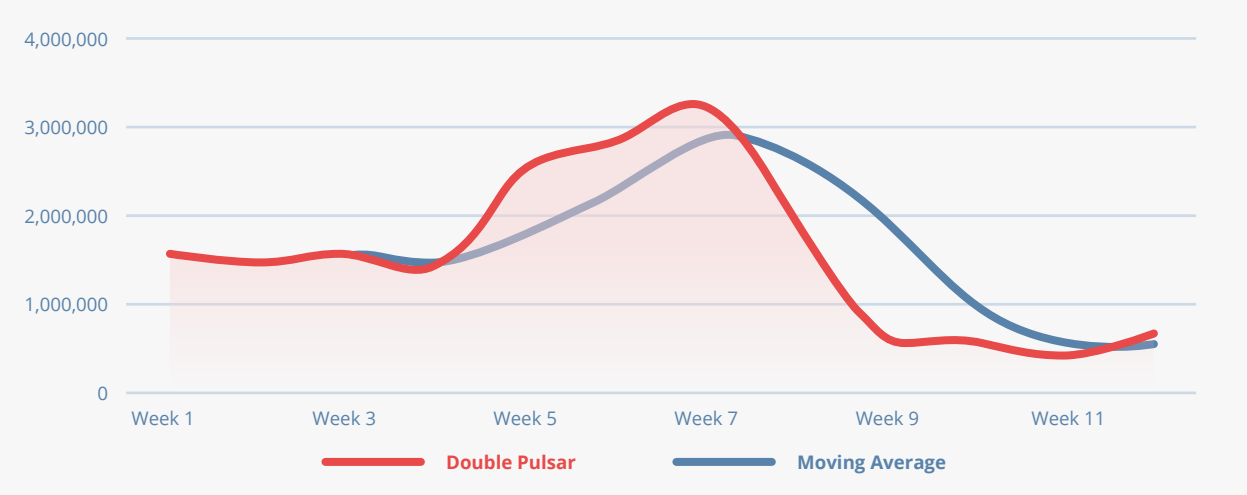


Figure 13. DoublePulsar Activity, Nuspire, Q2 2020

As shown in the figure 13 above, DoublePulsar activity peaked in week seven—increasing by 105% from the beginning of the quarter. This suggests a campaign may have been launched during that timeframe, possibly targeting remote desktop protocol (RDP) connections. Attackers are often looking for low hanging fruit, out of date and internet exposed versions of RDP, to resell connections or to launch an additional attack. Compromised RDP connections can sell for up to $15 each and attackers can use tools like Shodan to scout out potential targets. Once they gather enough compromised RDP connections, they will sell them in bulk on dark web forums and websites to collect their bounty. One threat actor, streetskip, has been observed selling compromised RDP connections from organizations on dark web forums.

By the end of the quarter, activity had decreased from its peak by 79%. This indicates that attackers may be regrouping and plotting their next campaign. DoublePulsar activity is expected to continue in Q3 and continue to be the most attempted exploit.

Bash Remote Code Execution (RCE) "Shellshock"

During Q2, Nuspire witnessed a significant spike in exploit attempts against CVE-2014-6271—also known as Shellshock. Multiple malware families such as C99Shell, p0wnedShell, JSShell and more utilize this vulnerability to launch an attack. Shellshock is found in numerous penetration testing tool suites like Metasploit, which makes it easily accessible by attackers. Unfortunately, the Unix Bash Shell where the vulnerability resides can be found on the majority of Unix based web servers and network devices.

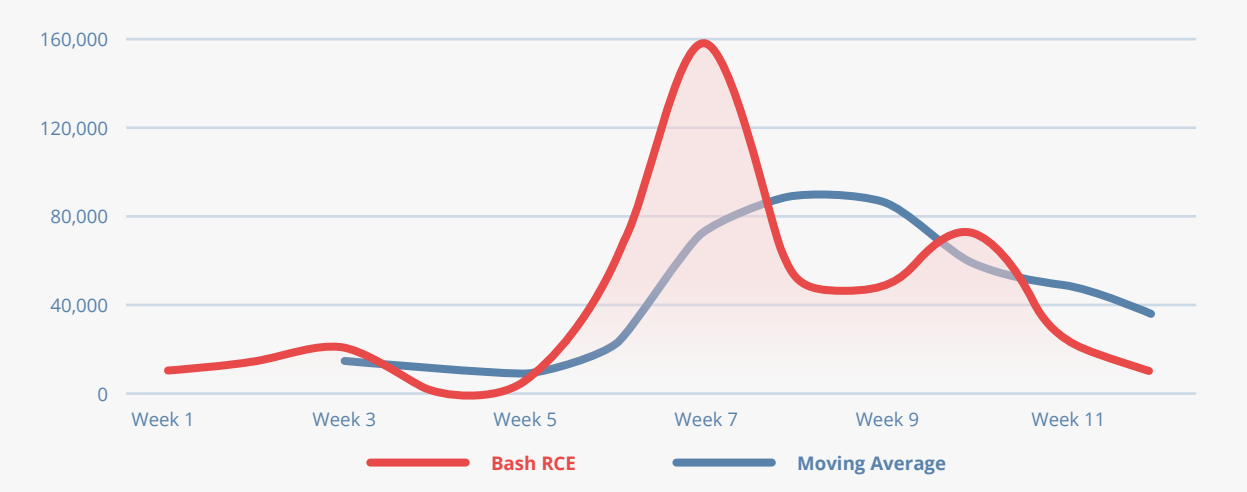


Figure 14. Bash Remote Code Execution, Nuspire, Q2 2020

The figure above shows that Bash Remote Code activity spiked over 1,310% from the beginning of the quarter. It then declined back to beginning of quarter's average attempts. It appears in week seven a large-scale campaign was attempted against this vulnerability. This demonstrates that even though the vulnerability was discovered in 2014, attackers will attempt old vulnerabilities to attempt to catch administrators with unpatched systems. This is a great example of why it is critical to continuously patch systems.

How to Combat

PROACTIVE DETECTION AND MITIGATION MEASURES

Exploitation activity is a race against the clock for all parties involved.

Patch your systems ASAP. When you receive notification of a vulnerable system, attackers see those same notifications. Make every effort to get patches applied to your critical systems as soon as you can in an attempt to front-run the malicious parties.

Use a Firewall with IPS. Firewalls with an Intrusion Prevention System will have the ability to block known exploits via signature. It is important to ensure these signatures are also being updated or it may lead to a false sense of security. Utilizing a managed detection and response (MDR) program can assist organizations with this task.

Monitor Security News and Vendor Security Bulletins. If you don't know about an issue, you can't fix it. Subscribe to security news feeds and your tech stack's security bulletins. Often these bulletins include direct links to patching information for administrators.

Pandemic Triggered Threats

COVID-19 introduced new threats as organizations and administrators were forced to protect a sudden and large WFH model. While employees scrambled to build their home offices and get operations back up and running smoothly, attackers did their best to take advantage of the chaos.

Current threat intelligence suggests attackers are starting to shift away from COVID-19 themed attacks and instead utilize other prominent media themes. The upcoming United States presidential election and current Black Lives Matter protests across the United States are two themes they are starting to exploit.

Near the end of the quarter, a new round of Netgear vulnerabilities were publicly disclosed, stating at least 28, and very possibly up to 80, home WiFi router models were vulnerable to attack. Unfortunately, these home routers are often never updated after being taken out of the box and enterprise administrators have no visibility into exploit attempts against them. It is important for administrators to inform their employees, especially those working remote, of common home router vulnerabilities and provide patching direction. Cybersecurity teams should consider collecting the make and model of their remote workers devices to help track vulnerabilities related to them.

Ransomware operators are also evolving. Intelligence released during Q2 suggests that these operators are forming "cartels" where they share resources and tactics to extort their victims. Ransomware operators at Maze created a website in 2019 to release stolen information of victims who did not pay as an extra layer of extortion. What's interesting is that in Q2 they began releasing information from other ransomware operators, particularly from the operators at LockBit. The operators at Maze have stated they intend to absorb and collaborate with more organizations and continue to grow their empire.

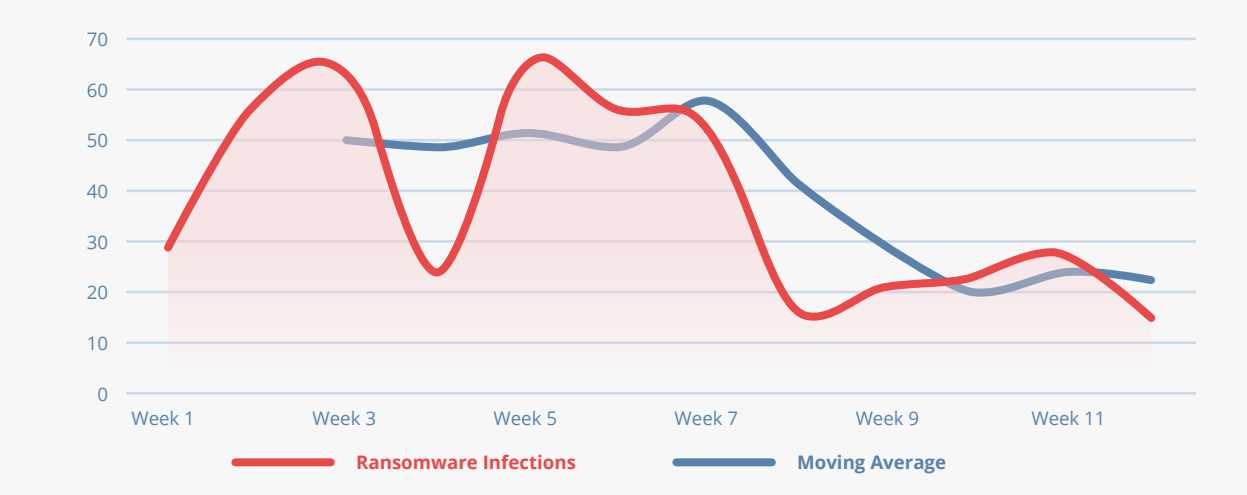


Figure 15. Ransomware infections, Nuspire, Q2 2020

Figure 15 above illustrates detected ransomware infections for each week of Q2. The current decline may be due to the retheming and retooling, as suggested earlier in this section. As new wrappers are created and redistributed, it is expected to see an increase again in Q3.

Since the beginning of Q2, to peak activity in week five, there was a 124% increase in ransomware activity. With regards to the start of Q2 to close, there was an observed 48% decrease.

Conclusion and Recommendations

As cybersecurity threats and tactics continue to evolve, they are becoming increasingly more sophisticated, and have the potential of inflicting more harm faster than ever before. The opportunity is that cyberattacks can be predictable. Organizations that are connected to the internet, or even with potential of internet connections, should know they are a potential target. Which means, organizations can learn what the most active threats are and look at their organization's digital perimeter to assess what actions need to be taken to mitigate risk.

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

Educate all users, often. User awareness is one of the most powerful and cost-effective ways to defend your organization from a cyberattack. Train users on how to identify phishing emails and to have a level of suspicion before opening attachments. 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. Ensuring your organization has all of the necessary security essentials covered will result in stronger security.

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. Integrating defense components counters any gaps in other defenses of security. A strategic security assessment is a great first step to identify and fill any gaps.

Up your malware game. 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 move within a network.

Segregate higher-risk devices from your internal network. IoT devices that are internet facing are targets. Administrators should ensure these devices have default passwords changed as attackers are actively searching for devices that provide them easy access into a network. Adopting a secure device management strategy enables you to harden security, no matter where or how your employees access your network.

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. Adopting cyber hygiene best practices achieves a stable, healthy environment.

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 www.nuspire.com and follow @Nuspire.

GET IN TOUCH →

nuspire