



QUARTERLY

Threat Landscape Report

Q4 2020 AND 2020 YEAR IN REVIEW

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	4
Summary of Findings	6
Methodology and Overview	7
Malware	9
Botnets	16
Exploits	23
Targeted Ransomware Campaign	30
Conclusion and Recommendations	34

Introduction

In Q4 2020, we came to the end of what proved to be a volatile year that shifted the threat landscape and changed the way organizations perform business operations. COVID-19 taught us that regardless of what is happening around us, some security tools are not optional — specifically incident response testing and endpoint protection. The supply-chain attack against SolarWinds in Q4 incited organizations to evaluate if they were affected, while government organizations moved swiftly to isolate and patch critical national infrastructure.

“The volume of sophisticated attacks seen throughout 2020 highlight the criticality of business intelligence and cybersecurity detection and response to improving organizational cyber readiness,” said Craig Robinson, Program Director, Security Services at IDC. “Nuspire’s latest report puts into perspective the changing nature of cyberattacks. Security leaders must be ready for unexpected situations, consistently revisiting and revamping their cybersecurity strategies.”

In this report, Nuspire summarizes Q4 and 2020 activity. A Q4 timeline of significant events sets the stage for sections on malware, botnets

and exploits. Highlights of each section include:

- Activity statistics
- The top five variants
- Need-to-know information about high-priority threats
- Expert recommendations to detect and mitigate attacks

The report closes with a spotlight on a key industry with close attention to Q4 and 2020 year in review with recommendations and 2021 predictions.

Summary of Findings

⬆️ **57.93%**
increase in total activity from Q3

5,758,721
MALWARE
EVENTS

51,159,641
EXPLOITATION
EVENTS

⬆️ **67.84%**
increase in total
activity from Q3

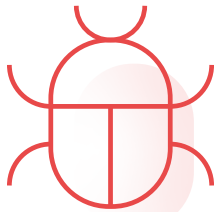
⬆️ **-19.85%**
decrease in total
activity from Q3

1,218,224
BOTNET
EVENTS

Methodology and Overview

Nuspire Threat Intelligence Team adheres to 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

 Election-based Phishing Scams on the Rise


OCTOBER 15

 Ransomware Activity Targets the Healthcare and Public Health Sectors


OCTOBER 29

 Maze Ransomware Gang Announces Closing of Maze Project


NOVEMBER 3

 Holiday Shopping Phishing Scams on the Rise

NOVEMBER 18

 APT's Target Fortinet SSL-VPN (CVE-2018-13379)

DECEMBER 4


 CISA Releases Emergency Directive Regarding Active Exploitation of SolarWinds Orion Software

DECEMBER 14


OCTOBER 21

Egregor Ransomware Samples Shared on Social Media 

NOVEMBER 2

At least 12 Hospitals and Healthcare Agencies Targeted in Coordinated Ransomware Attack 


NOVEMBER 5

Google Drive Notifications Abused in New Phishing Campaign 


NOVEMBER 25

Threat Actor Posts Exploits for More Than 49,000 Vulnerable Fortinet Devices 

DECEMBER 8

NSA Advisory Indicates Russian Threat Actors Are Exploiting VMWare Vulnerability 

DECEMBER 18

Dridex Malware Utilizes Amazon Gift Card Lures in New Phishing Campaign 

Malware



Malware Events

5,758,721

TOTAL MALWARE EVENTS

57.93%



INCREASE IN TOTAL ACTIVITY FROM Q3

1,030

UNIQUE VARIANTS DETECTED

68,556

VARIANTS DETECTED PER DAY

479,893

VARIANTS DETECTED PER WEEK

Malware Detection

In Figure 1, average Q4 malware activity is represented in a dashed trend line. The solid line shows the true weekly numbers to help identify spikes and abnormal activity. Across Nuspire managed devices, there was a 57.93% increase in total malware activity in comparison to Q3.

From start to finish during Q4, malware activity peaked during week three and began to trail off until

the end of the year with activity decreasing by 30.7%. This could be a result of the holiday season as end users took vacation time, reducing the number of users interacting with malware. Additionally, threat actors may have used the slower periods to retool and shift tactics before launching additional attacks in 2021.

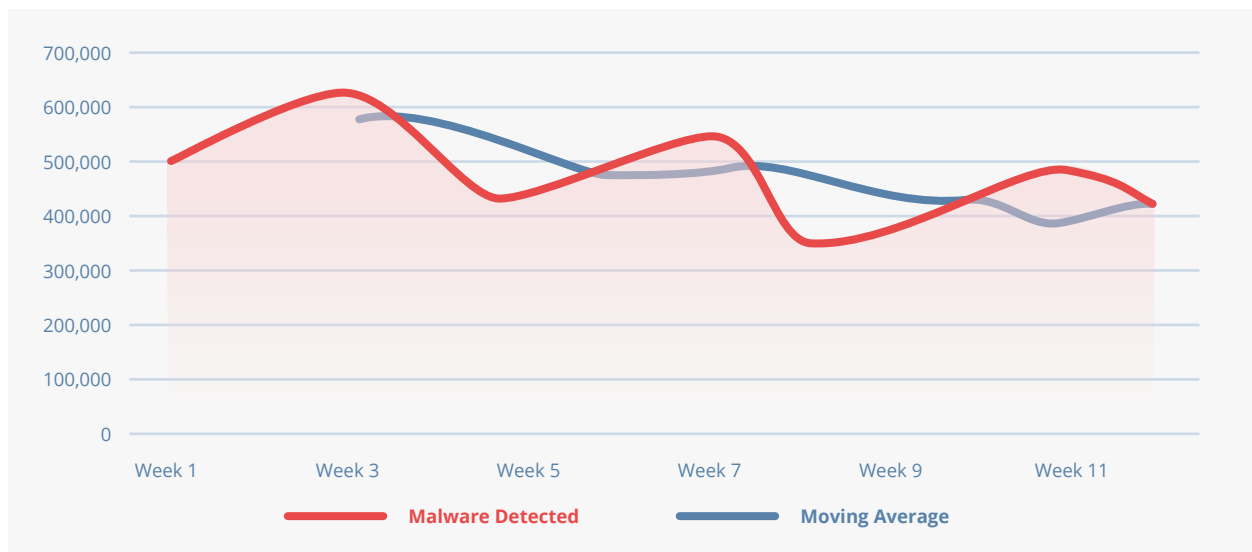


Figure 1. Malware detection, Nuspire, Q4 2020

As shown in Figure 2, the top five malware variants we witnessed over Q4 were Visual Basic for Applications (VBA) trojans, Emotet, Heodo, multi-compressed ZIP/GZIP files and Executable Linkable Format (ELF) trojans. VBA trojans dominated the observed malware and consisted of more than 95% of all observed malware detected on managed devices. As these are often the first stage of infection, Nuspire expects to see VBA agent activity continue to overshadow other variants.

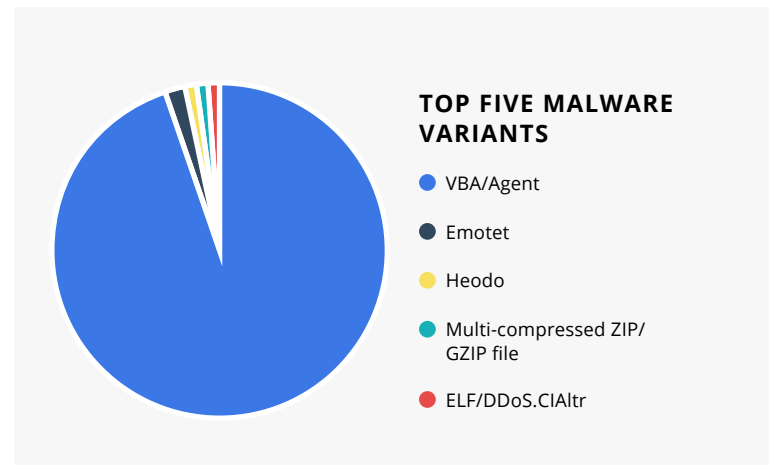


Figure 2. Top five malware variants, Nuspire, Q4 2020

VBA Agents Activity

VBA Agent activity dominated all other witnessed malware activity in Q3, and this trend continued in Q4. Activity spiked in week three as the U.S. election day approached. Attackers utilized the election as a lure, and then again activity spiked near the holiday season. Attackers were witnessed utilizing voter registration, polling information, and other election-related materials to lure end users into interacting with their malicious documents.

As the holiday season approached, false shipping notifications impersonating carriers, shopping deals, gift card registrations and more were used by attackers in an attempt to compromise

a system. After the holiday season, activity continued to trail off into the end of the year as threat actors were likely retheming their payloads for the start of 2021.

The VBA trojans often come through as Microsoft Word or Excel files with a lure attempting to trick the end user into enabling macros. If enabled, the macros activate a malicious script that reaches out to the command-and-control (C2) server to download a payload on the victim machine. Numerous malware families utilize this tactic to spread ransomware and other malware like Emotet.

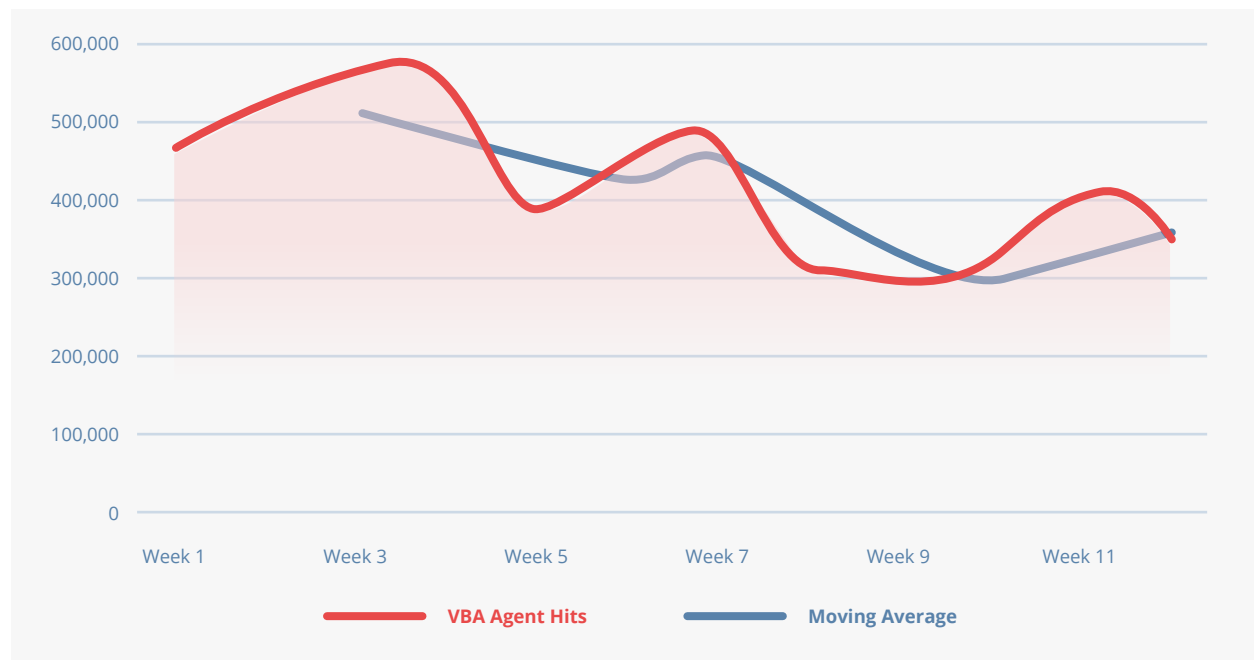


Figure 3. VBA Agent Activity, Nuspire, Q4 2020

Recorded Future®

Recorded Future identified a shift among the botnets distributing Word- or Excel-based lures in Q4. In October 2020, the Trickbot botnet was such a significant threat that a coalition of cybersecurity firms led by Microsoft orchestrated a global takedown of 94% of Trickbot's C2 infrastructure. While Trickbot rebuilt its infrastructure and infected organizations such as Subway UK and Mattel since the takedown, there was a surge in infections linked to QakBot, sometimes referred to as Qbot. Emotet remained a prominent player in first-stage distribution despite taking another hiatus during Q4. The botnet and loader economy will continue to use the most reliable and effective distributors at any given time, with users and affiliates quickly shifting to competitors when larger operations are inactive or ineffective.

Emotet

Emotet continued to appear within the top five variants of malware witnessed at Nuspire, and this is likely due to its ease of use and access for malicious actors. It is extremely customizable and easily widespread through malicious spam campaigns. Emotet can be deployed utilizing the VBA agents mentioned above and also can be used to deploy additional payloads.

Emotet is a wormable malware that spreads to other network-connected devices, and it can load additional malware, such as ransomware on infected machines. Near the end of Q4, [Emotet campaigns targeted Lithuania's National Center for Public Health \(NVSC\)](#), which fell victim to phishing emails. After becoming infected, the

devices began to download additional files, send fake emails and engage in other types of malicious activity. In this particular campaign, the Emotet emails were sent using password-protected archive files as attachments in which the password was included within the body of the email. Additionally, Emotet launched a holiday-themed campaign with various holiday-themed lures, all containing malicious macro-embedded documents and Excel files.

Newly observed Emotet indicators of compromise (IOCs) and those gathered from our threat intelligence partner Recorded Future during Q4 can be found in the [appendix](#).

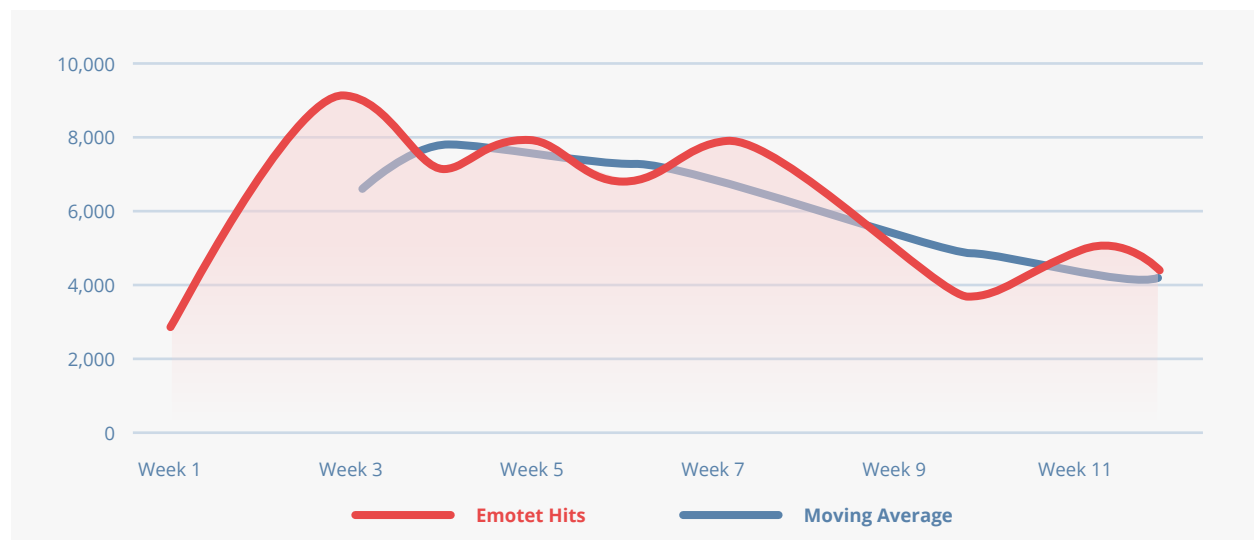


Figure 4. Emotet Activity, Nuspire, Q4 2020

2020 Malware in Review

Malware activity began with a slow decline in the beginning of the year and bottomed in July before sharply rising by 467% in September. This was due to a massive spike in VBA agent activity, suggesting either the launching of numerous malspam campaigns or one large-scale campaign by unknown operators. The malspam emails contained themes witnessed throughout the year such as COVID-19, the U.S. election, invoices,

shipping/package details, legal documents and more.

Activity trailed off slightly towards the end of the year. The lull in activity before September could be explained by threat actors experiencing disruptions and having to adjust as the world reacted to COVID-19 in early 2020 — a situation faced by many organizations.

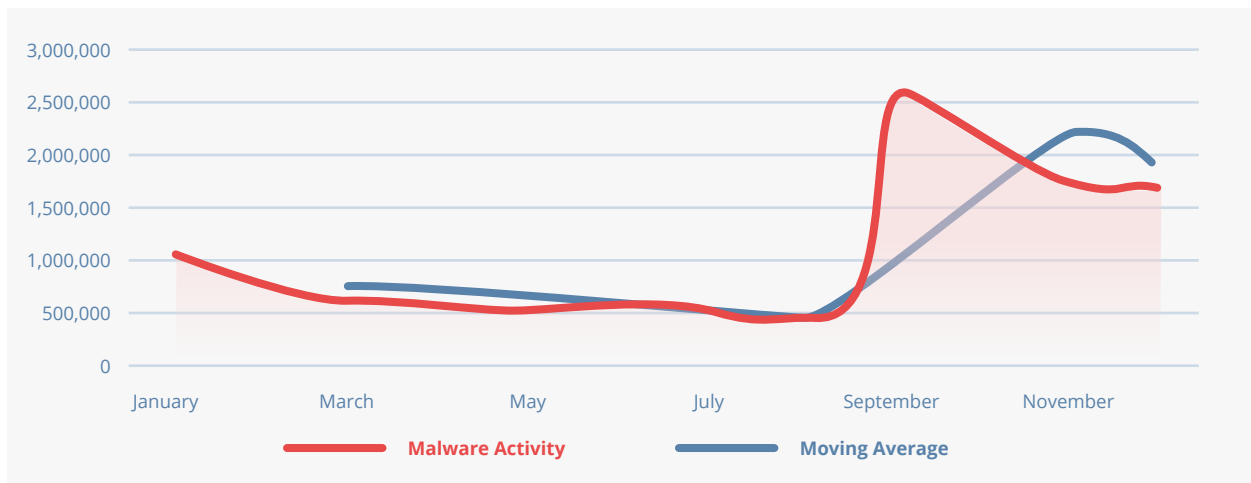


Figure 5. Malware activity, Nuspire, 2020

As shown in figure 6, VBA agents dramatically overshadowed any other variant witnessed. This is not surprising as these are commonly used to deploy multiple variants of malware as the first level of infection. This stresses to the cybersecurity community and organizational administrators the importance of end-user awareness training with a focus on phishing and malicious attachments, establishment of known reporting procedures, next-generation endpoint protection and an in-place incident response plan.

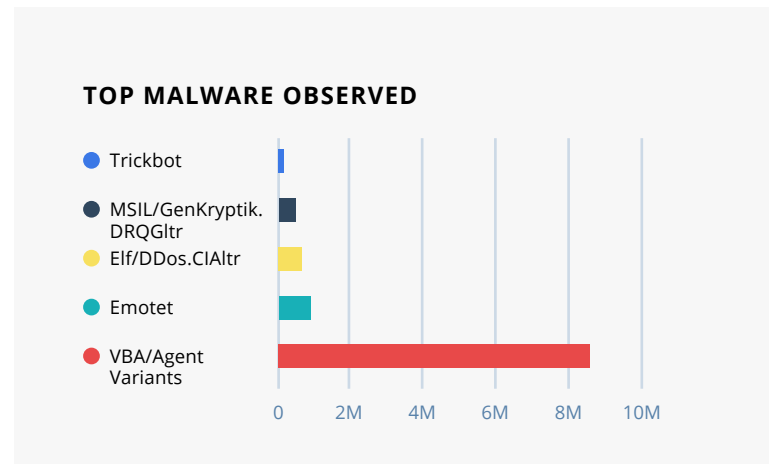


Figure 6. Top Malware Observed Nuspire, 2020

How to Combat

PROACTIVE DETECTION AND MITIGATION MEASURES



Endpoint Protection Platforms (EPP). Legacy antivirus (AV) is strictly signature-based detection capable only of detecting already known variants of malware. Instead, implement security in-depth by utilizing advanced, next-generation antivirus (NGAV). NGAV detects malicious software not only through signatures but also through heuristics and behavior.



Network Segregation. Segregate high-risk devices like Internet of Things (IoT) devices from the organization's internal network. This minimizes the attacker's ability to laterally move throughout a network and minimize spread of wormable malware.



Cybersecurity Awareness Training. 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. Reporting policies should be established if they don't already exist within organizations, and security leaders need to ensure everyone in the organization is comfortable using them.



Botnets



Botnet Events

1,218,224

TOTAL BOTNET EVENTS

-19.85% 

DECREASE IN TOTAL ACTIVITY FROM Q3

39

UNIQUE BOTNETS DETECTED

14,502

INFECTIONS PER DAY

101,518

INFECTIONS PER WEEK

Botnet Detection

Figure 7 shows a moving average of botnet activity throughout Q4 as a dashed line. The solid line illustrates the true weekly numbers to help identify spikes and abnormal activity.

Throughout Q4, botnet activity steadily declined with a small spike in week 11. This spike is attributed to activity related to the Torpig Mebroot botnet.

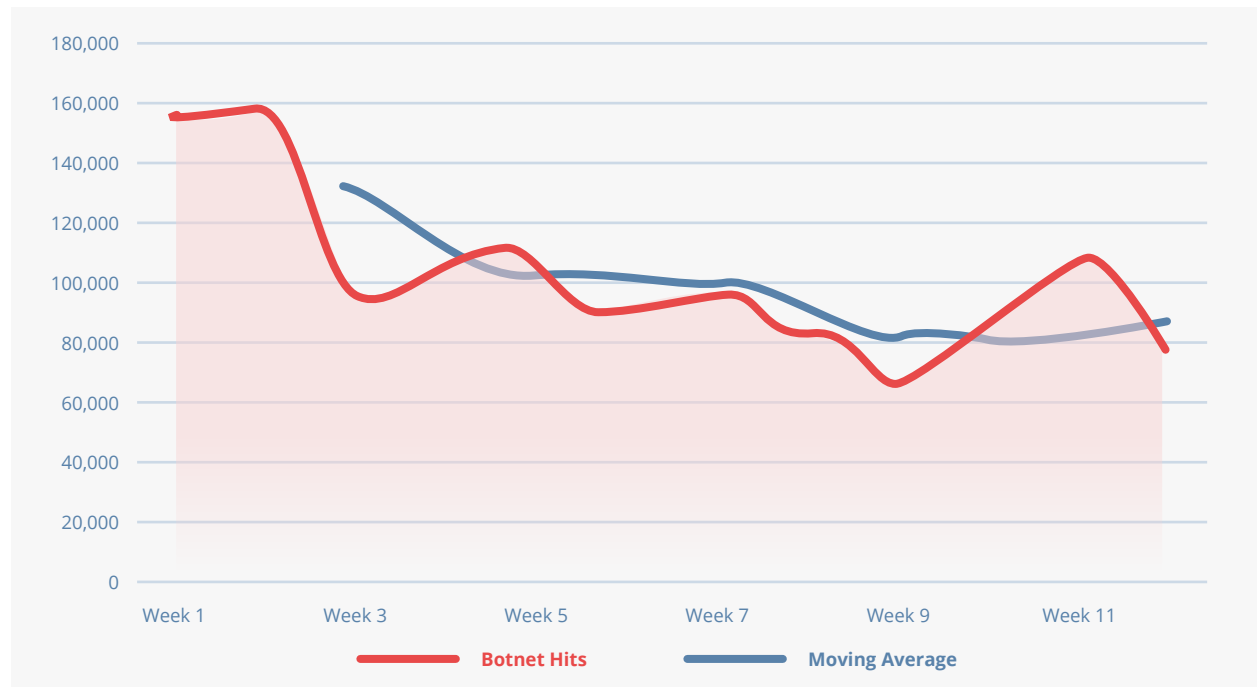


Figure 7. Botnet infections, Nuspire, Q4 2020

Figure 8 shows the top observed botnets during Q4 2020.

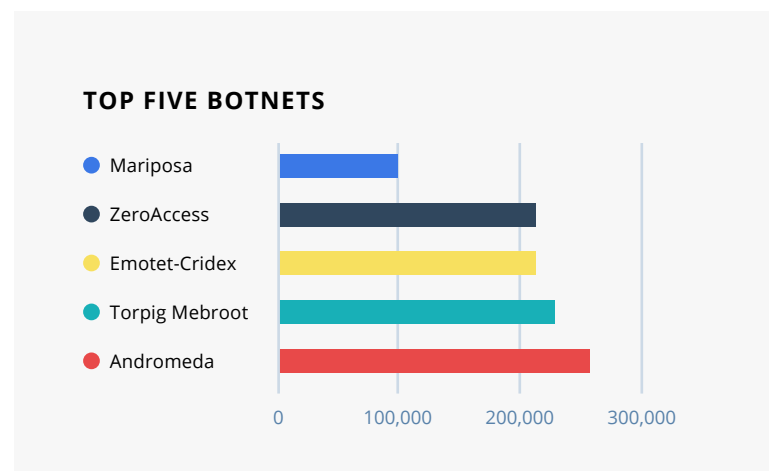


Figure 8. Top Five Botnets, Nuspire, Q4 2020

Andromeda

Andromeda botnet activity, which was in a steady decline during Q3, resurfaced in Q4. Activity rose 172% from the lowest activity to the peak in week 4 of Q4. It is the botnet with the most activity witnessed during Q4.

Andromeda is one of the oldest and largest botnets, and it has been known to distribute multiple malware families. It is unknown as of this writing which actors are utilizing the botnet

as the botnet was sinkholed in 2017 by Microsoft and authorities. During that disruption, [Microsoft announced](#) that the botnet had been associated with more than 80 malware families. It has been seen distributing Gamarue malware, ransomware, spambots and information-stealing malware such as Ursnif. Nuspire has seen Andromeda activity vary throughout the year, and the ancient botnet remains prevalent today.

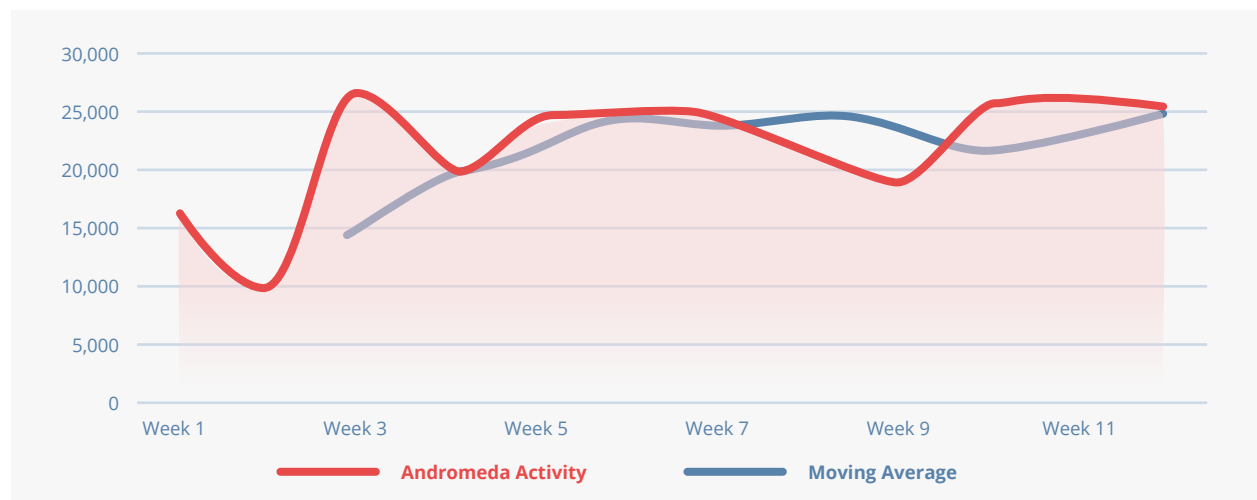


Figure 9. Andromeda activity, Nuspire, Q4 2020

·||· Recorded Future®

In addition to Andromeda, Recorded Future identified a continuation of Emotet activity. Similar to previous quarters, Emotet was a persistent threat to organizations. The operators demonstrated use of large-scale infrastructure, including [using](#) nearly six million parked domains to redirect victims to malicious or unwanted landing pages. In addition, we [continued](#) to see Emotet used to drop Trickbot on infected systems. There was a decrease in Emotet activity in November, although the operators quickly [resumed](#) operations in December by targeting users in Italy and Japan, which then quickly expanded into a global effort. On December 30, 2020, a new Emotet malware campaign was observed [targeting](#) the internal networks of Lithuania's National Center for Public Health (NVSC). Based on telemetry data of Lithuania's National Cyber Security Center, a large number of trojanized emails were observed targeting several state institutions, as part of the Emotet malware campaign. According to a report [released](#) by Check Point, in December 2020, researchers considered Emotet to be the "Most Wanted Malware", impacting 7% of organizations globally following a campaign which targeted over 100,000 users per day during the holiday season.

Torpig Mebroot

Torpig is another botnet that has been in existence for years. It produced a lot of activity during Q4, finishing as the second-highest observed botnet.

Figure 10 shows the Torpig botnet activity witnessed throughout Q4 with the largest spike in activity during week 11 of the quarter in which it increased by 1,453% from the lowest witnessed activity in week four. Activity spiked in week five close to the U.S. election and again during week 11 at its peak during the holiday season. This indicates

the botnet may have attempted to use theming related to the election and holidays to lure victims into interacting with the payloads.

The Torpig botnet utilizes backdoor trojans and is capable of installing fraudulent certificates that lead victims to believe they are visiting a secured website. The primary focus of the botnet is capturing valuable banking credentials, but it also can intercept API calls and steal usernames and passwords.

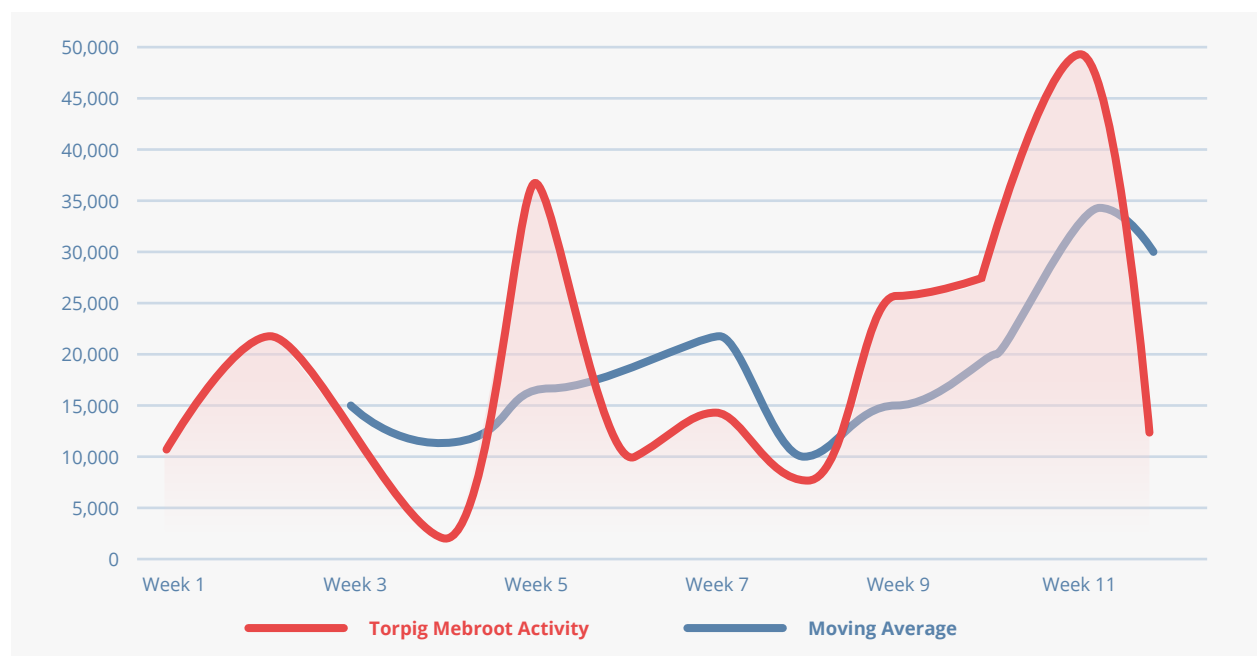


Figure 10. Torpig botnet activity, Nuspire, Q4 2020

2020 Botnet in Review

As shown in Figure 11, botnet activity remained fairly consistent with an exception in the month of May in which activity increased by 48% from beginning-of-year activity. After the spike, activity continued to decline to beginning-of-year levels. The spike in May is attributed to a large increase in

activity from the ZeroAccess botnet as discussed in the Q2 Nuspire Threat Report. The activity in May contributed heavily to ZeroAccess being the top-witnessed botnet by Nuspire during 2020. Figure 12 shows the top five most active botnets as observed by Nuspire.

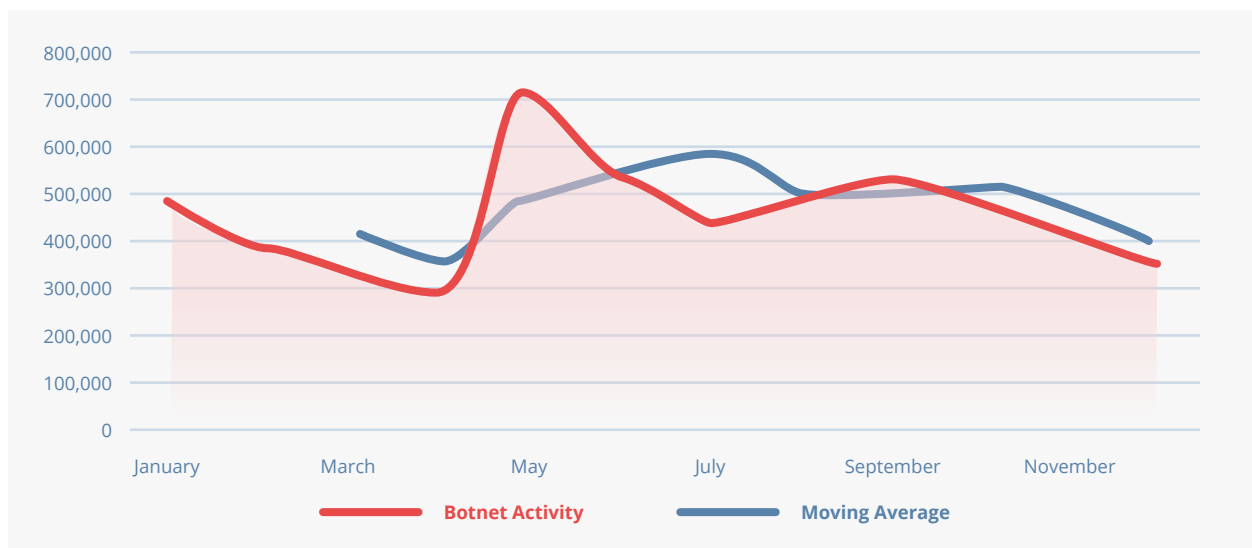


Figure 11. Botnet activity, Nuspire, 2020

TOP BOTNETS OBSERVED

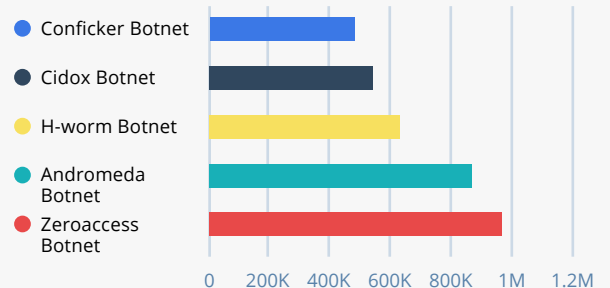


Figure 12. Top Botnets Observed Nuspire, 2020

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 devices that are reaching out to known malicious hosts with C2 communication. Communication with malicious servers could allow attackers to drop additional payloads or exfiltrate sensitive data. The ability to correlate network traffic logs with threat intelligence to identify malicious communications is critical to identifying botnets.



User Awareness Training. Infection often begins via phishing with malicious attachments. Ensure your organization knows how to identify suspicious emails and processes and implement procedures for reporting and review.



Use Next Generation Antivirus. If your antivirus software is not capable of detecting malicious behavior, you may be missing malicious programs without a known signature. Next-generation endpoint protection can detect malicious activities and quarantine devices to minimize spread through the network and allow responders to take action.



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 it's found. Should your server be reaching out to a foreign IP address? Utilize a SIEM to review traffic and help make sense of network communications.

Exploits



Exploit Events

51,159,641

TOTAL EVENTS

67.84% 

INCREASE IN TOTAL ACTIVITY FROM Q3

326

UNIQUE EXPLOITS

609,043

EXPLOITS DETECTED PER DAY

4,263,303

EXPLOITS DETECTED PER WEEK

Exploit Detection

Figure 13 shows a moving average of exploit activity throughout Q4 as a dashed line. The solid line illustrates the true weekly numbers to help identify spikes and abnormal activity. Exploit activity at the beginning of Q4 capped the peak of witnessed activity with spikes in week seven and week nine of Q4 with some lulls in between.

This activity syncs closely with the release of known vulnerable Fortinet devices on the dark web and APT groups that also targeted the SSL-VPN Vulnerability ([CVE-2018-13379](#)) along with a massive increase of SMB Login brute force attempts.

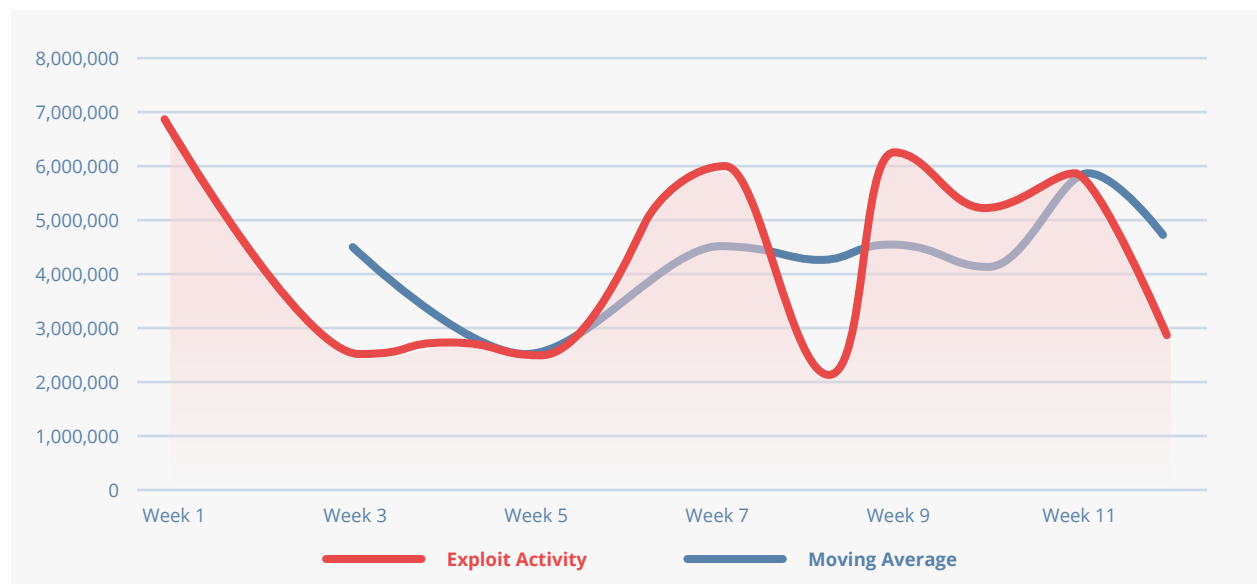


Figure 13. Exploits detected, Nuspire, Q4 2020

Fortinet SSL-VPN (CVE-2018-13379)

During Q4, intelligence indicated that more than 49,000 Fortinet devices vulnerable to CVE-2018-13379 were released on a dark web forum. Fortinet had previously provided firmware version upgrades to mitigate this vulnerability that was from 2019. Unfortunately, some organizations did

not upgrade to non-vulnerable versions. Shortly after this list was released, activity attempting to exploit this vulnerability increased by 4,176% from attempts witnessed at the beginning of Q4. Figure 14 shows this activity.

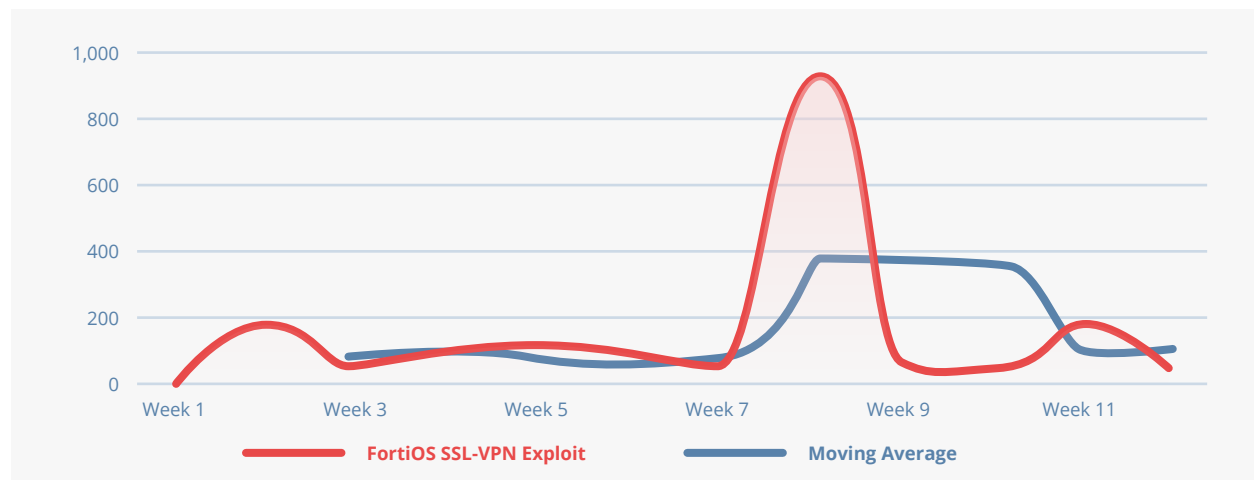


Figure 14. Fortinet CVE-2018-11379 exploit attempt, Nuspire, Q4 2020

Recorded Future®

Recorded Future discovered on November 22, 2020, reports emerged of cybercriminals using public exploits that allow access to the “sslvpn_websession” files from the vulnerable Fortinet VPN devices. CVE-2018-13379 is a path traversal vulnerability that impacts Fortinet FortiOS SSL VPN devices. An unauthenticated remote attacker could exploit this vulnerability by using specially crafted HTTPS requests to access the victims’ system files. A security researcher, who goes by the moniker “Bank_Security,” disclosed a forum thread in which an unspecified threat actor shared a list of the targets that were vulnerable to the exploitation of the CVE. The majority of these targets is reported to be domains belonging to reputable banks, financial organizations and government institutions globally. On November 25, 2020, a user on Raid Forums posted a 6.7GB file that contained plaintext usernames and passwords as well as IP addresses associated with Fortinet VPN devices, which were obtained based on the CVE-2018-13379 exploits reported earlier. This exposure means that organizations that had patched CVE-2018-13379 may still be vulnerable to account compromise from criminals who have accessed the file on Raid Forums. However, it is currently unclear what proportion of these devices remain vulnerable. Given the ease with which CVE-2018-13379 can be exploited, coupled with its history of being used by a range of state-sponsored groups, it is important for system administrators to stay informed about vulnerabilities on their devices and patch those as soon as possible within their environment. Threat actors are consistently on the hunt for low-hanging fruit and exploits regardless of how long ago the vulnerability was disclosed publicly.

SMB Login Brute Force

Nuspire witnessed activity that targeted SMB brute force tactics. Many tools, such as powershell scripts, the commonly used Metasploit Exploitation Framework and many malware variants, exist to perform this attack. These attacks are noisy as they generate numerous failed login attempts. Workforces have moved remote for many organizations, and this provides additional attack vectors for malicious actors to exploit. As of this

writing, Shodan shows more than 1.3 million SMB ports (port 445) exposed to the open internet with the highest amount being in the U.S.

Figure 15 shows these trends during Q4. From lowest to highest points within Q4, activity spiked more than 90,000% in bursts before sharply falling off and cycling. These bursts of activity pushed this exploit to the top-witnessed exploit attempt in Q4.

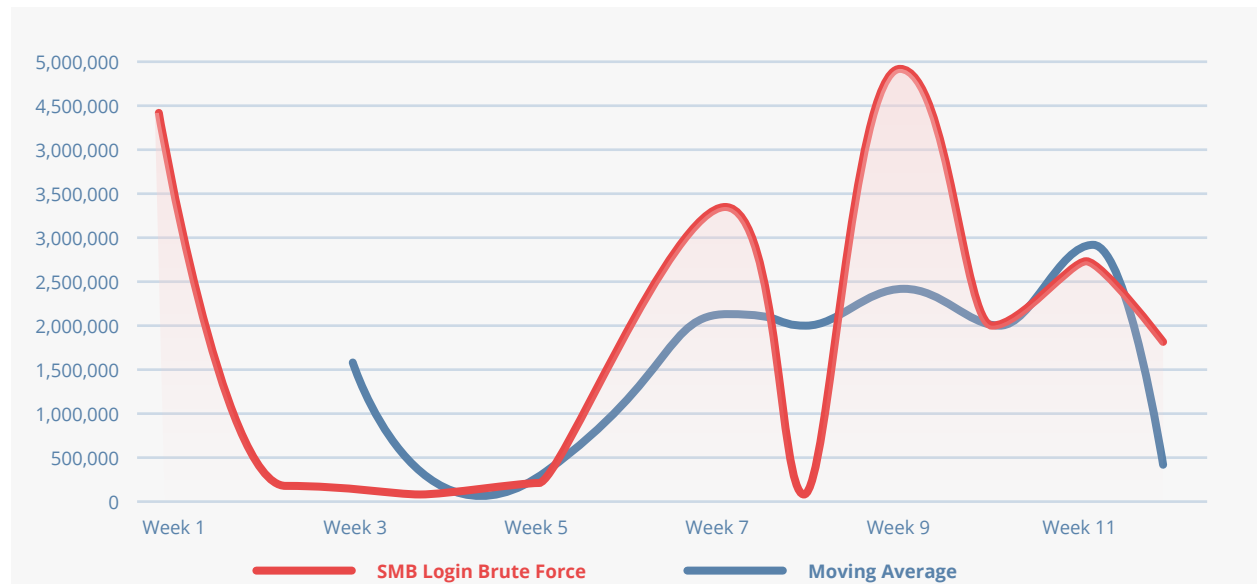


Figure 15. SMB Login brute force activity, Nuspire, Q4 2020

Figure 16 shows the highest witnessed exploit attempts in Q4. Double Pulsar dominated previous Nuspire threat reports and dropped into the third position after being overshadowed by SMB Login brute force attempts and HTTP Server Authorization Buffer Overflow attacks.

TOP 5 EXPLOIT ATTEMPTS Q4

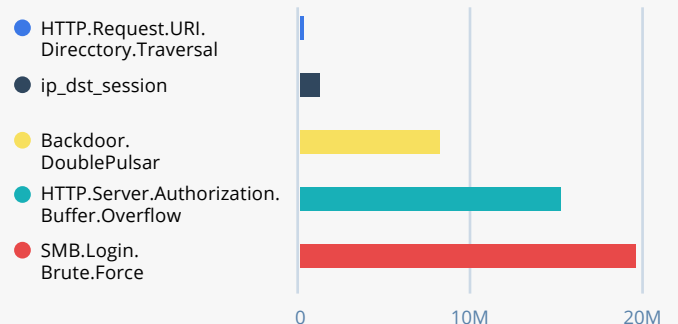


Figure 16. Top 5 Exploit Attempts Q4 Nuspire, Q4 2020

2020 Exploit Review

Throughout 2020, Nuspire observed a consistent increase of exploitation events. December contained the largest volume of activity. From the start to the end of 2020, we witnessed an overall increase of 116%. Figure 17 shows 2020's exploit trend based on Nuspire data. One of the most noteworthy observations is that attackers certainly will attempt to exploit new vulnerabilities as they are disclosed, but they continue to search for organizations that do not maintain good patching procedures. And they will exploit critical

vulnerabilities, growing their arsenal with each new vulnerability while focusing on remote connections.

Figure 18 shows the highest volume of exploit attempts witnessed throughout 2020 with DoublePulsar reigning as the top-utilized technique. As 2021 begins, administrators should be extremely cautious regarding remote access and monitor any disclosed vulnerabilities relating to their technology stack.

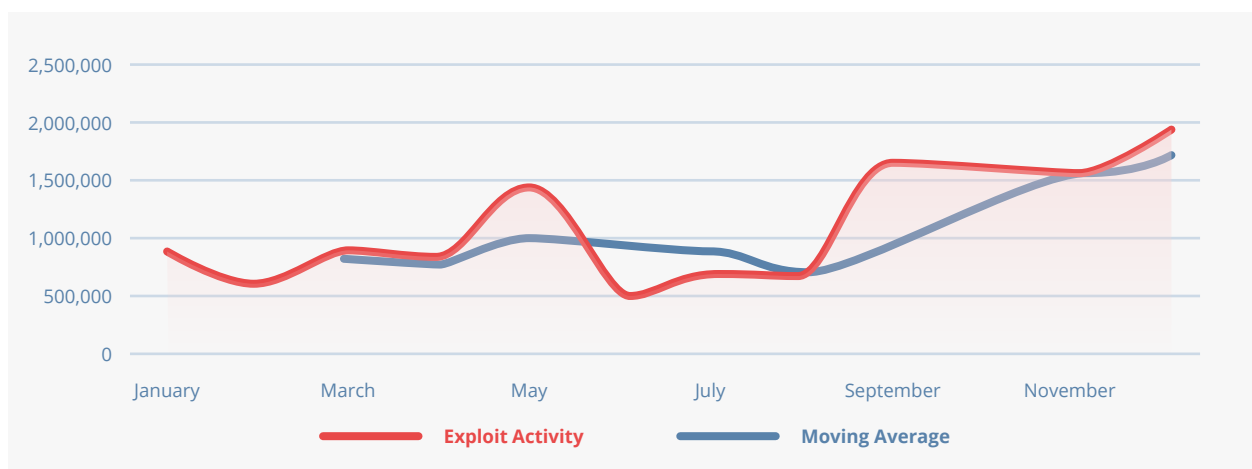


Figure 17. Exploit activity, Nuspire, 2020

TOP 5 EXPLOIT OBSERVED 2020

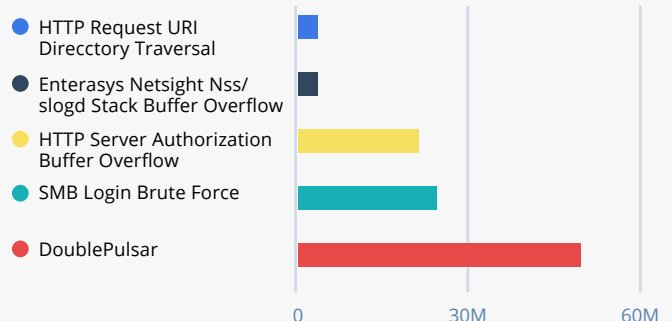


Figure 16. Top 5 Exploit Attempts Q4 Nuspire, Q4 2020

How to Combat

PROACTIVE DETECTION AND MITIGATION MEASURES

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



Patch your systems ASAP. Attackers monitor vulnerability postings and will attempt to exploit them. Administrators need to focus on patching their technology stacks as soon as possible and understand the risks involved with pushing those patches to the



Use a Firewall with IPS. Firewalls with an intrusion prevention system (IPS) have the ability to block known exploits via signature. It is important to update these signatures to ensure new known vulnerabilities are blocked.



Monitor Security News and Vendor Security Bulletins.

Vendors often have a service for subscribers to receive notifications about new vulnerabilities with patching information or workarounds/mitigations. This ensures you receive the information as soon as possible and can plan for patches in your environment.

Targeted Ransomware Campaign - Healthcare

During Q4, the Cybersecurity and Infrastructure Agency (CISA), the Federal Bureau of Investigation (FBI) and Department of Health and Human Services (HHS) [released a joint cybersecurity advisory](#) regarding the increased targeting of healthcare organizations specifically by a threat actor known as [UNC1878 \(WIZARD SPIDER\)](#). Healthcare is always an attractive target for threat actors due to the nature of the sensitive data their healthcare organizations handle, especially those involved in the COVID-19 supply chain who were highly targeted during Q4. Nation states are extremely interested in the proprietary data involved with COVID-19 vaccination creation either to use it to build their own, disrupt other countries, or to sell the data, and COVID supply chains fit the bill.

This particular campaign is identified as attacks

launched via Trickbot and BazarLoader malware, which then leads into the exfiltration of data followed by a ransomware attack deploying Ryuk ransomware. Exfiltrated data is sold to the highest bidder on the dark web or used to launch additional targeted attacks.

As shown in Figure 19, Nuspire witnessed strong Trickbot activity that declined sharply just before the joint advisory was released. This could indicate that the threat actors were shifting tactics as the cybersecurity community was beginning to disclose the activity in an attempt to stay ahead of defenders. Nuspire witnessed no signatures of BazarLoader during Q4. Newly observed indicators of compromise (IOCs) and those gathered from our threat intelligence partner Recorded Future for Trickbot and BazarLoader can be found in the [appendix](#).

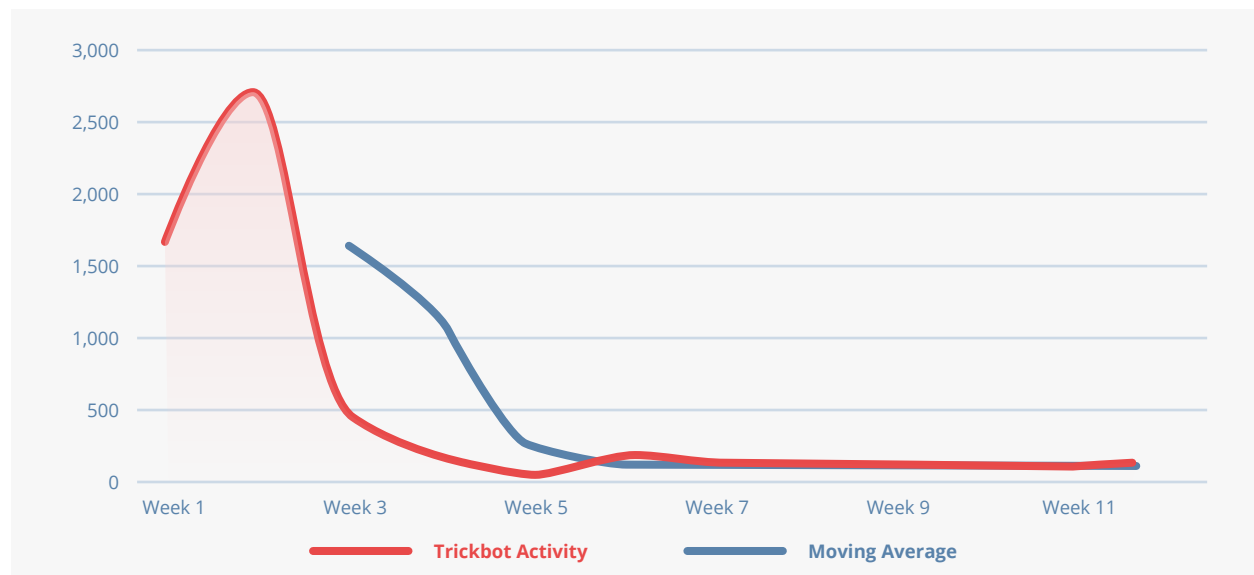


Figure 19. Q4 Trickbot Activity Nuspire, Q4 2020

In an average month, a healthcare organization may face the following attempted executions on its endpoints:

73 Malicious File Execution Attempts

70 Exploitation Attempts

9 Trojan Execution Attempts

2 Ransomware Execution Attempts

The top tactics, techniques, and procedures (TTPs) sourced by MITRE ATT&CK of threat actors targeting the healthcare industry can be found below. These should be a starting point for your network security program and used to help identify gaps within your program.

Technique	Name	Tactic
T1204.002	Malicious File	Execution
T1059.003	Windows Command Shell	Execution
T1059.001	PowerShell	Execution
T1566.001	Spearphishing Attachment	Initial-Access
T1547.001	Registry Run Keys/Startup Folder	Persistence
T1105	Ingress Tool Transfer	Command and Control
T1027	Obfuscated Files or Information	Defense-Evasion

While reviewing data for all monitored endpoints, we saw ransomware activity greatly increase during weeks nine and 10 by more than 10,000%, then decrease sharply to the prior witnessed average as shown in Figure 20. The activity did not appear to be targeted at a specific industry vertical as endpoints from multiple industries were found.

The data indicates a large campaign launched near the end of Q4 shortly after the U.S. election and at the beginning of the U.S. holiday season by unknown threat actors as of the date of writing this report. While threat actors are normally opportunistic, this is the largest volume of activity Nuspire has witnessed to-date.

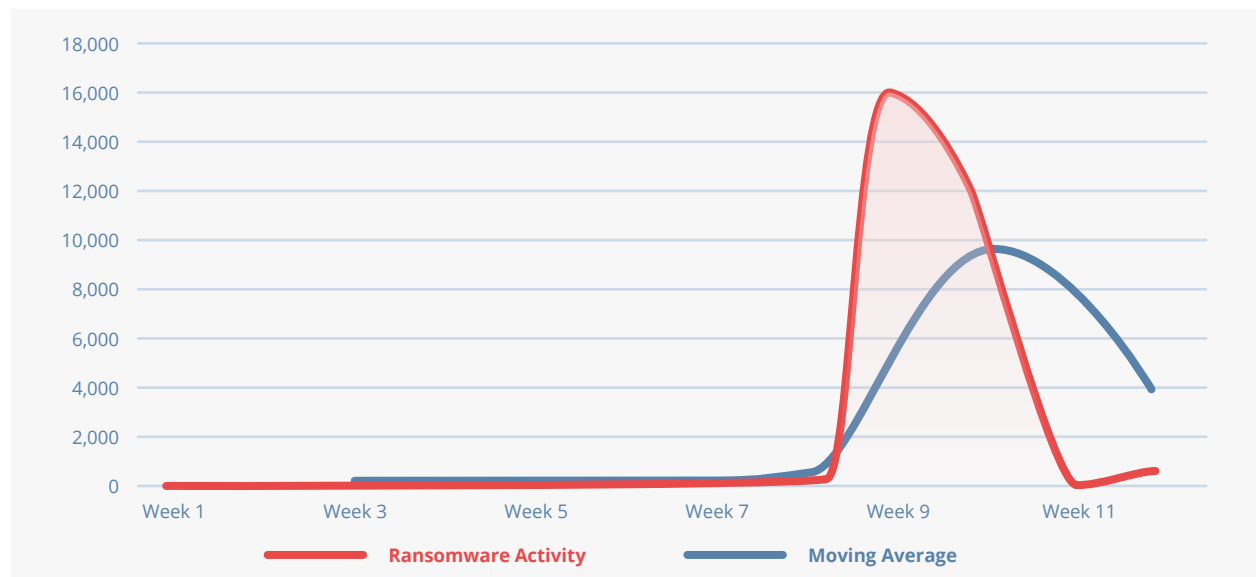


Figure 20. Q4 Ransomware Activity Nuspire, Q4 2020

2021 Predictions

This past year, organizations prioritized cybersecurity more than ever before. The events in 2020 proved that no one is immune to a cyberattack. As we enter a new year, the threat experts at Nuspire offer the following predictions:

Unsecure remote access along with any kind of RDP or VPN vulnerability will be highly targeted as our world/workforce remains remote. As our workforce has moved remote due to the impacts of COVID-19, organizations had to make significant changes to their infrastructure to support remote access. This increases the possibility of unsecurely configured remote access and new vulnerabilities. Threat actors are opportunistic and are actively hunting for these unsecure connections. Expect any new RDP vulnerabilities or VPN vulnerabilities, to be highly targeted.

Ransomware will continue to evolve, and new tactics will present themselves over the year. Ransomware threat actors consistently look for ways to apply more pressure to their victims to force them into paying the ransom. As we've seen, they create extortion websites to publish data from those who don't pay. Expect to see further evolution of these tactics. More threat actors will get onboard with creating extortion sites, while others will develop completely new tactics. Ransomware will continue to be a major threat to organizations during 2021.

Another threat group will attempt to fill the power vacuum left by Emotet. One of the largest malware/botnet families, Emotet was effectively shut down in January 2021. The threat actors remain at large and have taken a significant financial blow. However, they are likely looking into ways to rebuild their infrastructure or look to partner with an existing botnet to continue the distribution of Emotet. We may see a "rebrand" of Emotet as they attempt to distance themselves from the name "Emotet" while they rebuild, but the tactics will likely point to their work.

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 to counter these attacks is in their predictability. Learn what are the most active threats and look at your organization's digital perimeter to assess what actions need to be taken to mitigate risk.

Security leaders can take the following five simple actions to safeguard their organizations 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 to identify suspicious attachments, social engineering and scams that are circulating. Inform them of common theming and instruct them to be suspicious regarding any major events that could be turned 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. After an attacker has compromised an email account, they often 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 does 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 security defenses. Utilize vulnerability scanning to determine your weak spots and build your security around them. Enrich your logs with threat intelligence and perform threat modeling in your organization to determine how advanced persistent threat 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 if interactions occur. Network security solutions, such as secure device management, can detect malicious files attempting to enter a network from the internet or moving laterally 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 High-risk Devices from Your Internal Network.** Internet-facing devices are high-value targets. Administrators should ensure the default passwords of these devices are changed because attackers are actively searching for devices that provide them easy access into a network. IoT devices should be inventoried. A full understanding of your digital footprint is critical. Network segregation can help limit where an attacker can move laterally within an environment in the circumstance of a breach.
5. **Patch, Patch and 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 that 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 www.nuspire.com and follow @Nuspire.

GET IN TOUCH →

About Recorded Future

Recorded Future®

Recorded Future delivers security intelligence to amplify the effectiveness of security and IT teams in reducing exposure by uncovering unknown threats and informing better, faster decisions. Working to provide a singular view of digital, brand and third party risk, the Recorded Future platform provides proactive and predictive intelligence, analyzing data from open, proprietary and aggregated customer-provided sources. Recorded Future arms threat analysts, vulnerability management teams, security operations centers, and incident responder with context-rich, actionable intelligence in real time that's ready for integration across the security ecosystem. Learn more at www.recordedfuture.com and follow us on Twitter @RecordedFuture.