



QUARTERLY

# Threat Landscape Report

Q3 2020

[NUSPIRE.COM](https://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

<b>Introduction</b>	<b>4</b>						
<b>Summary of Findings</b>	<b>6</b>						
<b>Methodology and Overview</b>	<b>7</b>						
<b>Quarter in Review</b>	<b>8</b>						
<b>Malware</b>	<b>9</b>						
<b>Botnets</b>	<b>15</b>						
<b>Exploits</b>	<b>20</b>						
<b>The New Normal</b>	<b>28</b>						
<b>Conclusion and Recommendations</b>	<b>31</b>						
<b>About Nuspire</b>	<b>33</b>						

# Introduction

In Q2 2020, Nuspire observed the increasing lengths threat actors were going to in order to capitalize on the pandemic and resulting crisis. New attack vectors were created; including VPN usage, home network security issues, personal device usage for business purposes and auditability of network traffic.

In Q3 2020, we've observed threat actors become even more ruthless. Shifting focus from home networks to overburdened public entities including the education sector and the Election Assistance Commission (EAC).

Many school districts were forced into 100% virtual or hybrid learning models by the pandemic. Attackers have waged ransomware attacks at learning institutions who not only have the financial resources to pay ransoms but feel a sense of urgency to do so in order to avoid disruptions during the school year. Meanwhile, the U.S. Elections have provided lures for phishers to attack. Nuspire witnessed Q3 attempts to guide victims to fake voter registration pages to harvest information while spoofing the Election Assistance Commission (EAC).

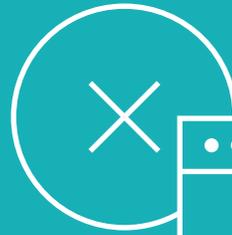
Like these examples, cybercriminals taking advantage of prominent media themes are expected. We anticipate our Q4 2020 Threat Report

to find campaigns leveraging more of the United States Presidential election as well. This is simply due to the fact that cybercriminals are predictable. Keeping up with the latest threat intelligence can help your organization prepare for current themes and understand your risk. Knowing what is in your environment and what assets will likely be targeted by cybercriminals is crucial to build a resilient security program. Reading this

report each quarter is a great step to gain that knowledge.

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

# Summary of Findings



▲ 128.21%  
increase in total activity from Q2

3,646,448  
MALWARE  
EVENTS

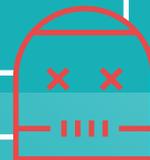


30,480,289  
EXPLOITATION  
EVENTS



▲ 1.84%  
increase in total activity from Q2

▼ -6.23%  
decrease in total activity from Q2



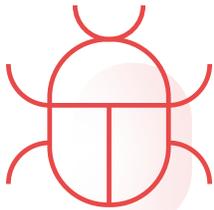
1,519,869  
BOTNET  
EVENTS



# Methodology and Overview

Nuspire's 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

 Microsoft Warns of Office365 Phishing via Malicious OAuth Applications

**JULY 8**

 After Period of Inactivity, Emotet Trojan Returns to Target Users Globally

**JULY 20**

 Twitter Hack was Started by Phone-based Spearphishing

**JULY 31**

 New FritzFrog Botnet Attacks Millions of SSH Servers

**AUGUST 20**

 Mimikatz Update Adds Exploit for Zerologon (CVE-2020-1472)

**SEPTEMBER 21**

**JULY 14**

Critical Microsoft DNS Server Remote Code Execution Vulnerability Disclosed (CVE-2020-1350) 

**JULY 22**

Emotet Trojan Spreads OakBot Malware via Spam Campaign 

**AUGUST 17**

New Emotet Campaign Uses COVID-19 Lures to Target US Organizations 

**SEPTEMBER 20**

CISA Releases Emergency Directive on Microsoft Windows Netlogon Remote Protocol (Zerologon) 

# Malware



## Malware Events

**3,646,448**

TOTAL MALWARE EVENTS

**128.21%** 

INCREASE IN TOTAL ACTIVITY FROM Q2

**1,168**

UNIQUE VARIANTS DETECTED

**43,410**

VARIANTS DETECTED PER DAY

**303,870**

VARIANTS DETECTED PER WEEK

**1.6%** 

INCREASE IN UNIQUE VARIANTS DETECTED FROM Q2

## Malware Detection

In Figure 1, the average of Q3 malware activity is represented in a navy trend line. The red line shows the true weekly numbers to help identify spikes and abnormal activity. Looking across Nuspire In devices, there was a 128.21% increase in total malware activity in comparison to Q2 numbers. We also observed a

1.6% increase in unique variants. From start to finish, Q3 activity continued to trend up throughout the quarter with activity peaking in week 11 at a 670% increase from the beginning of the quarter.

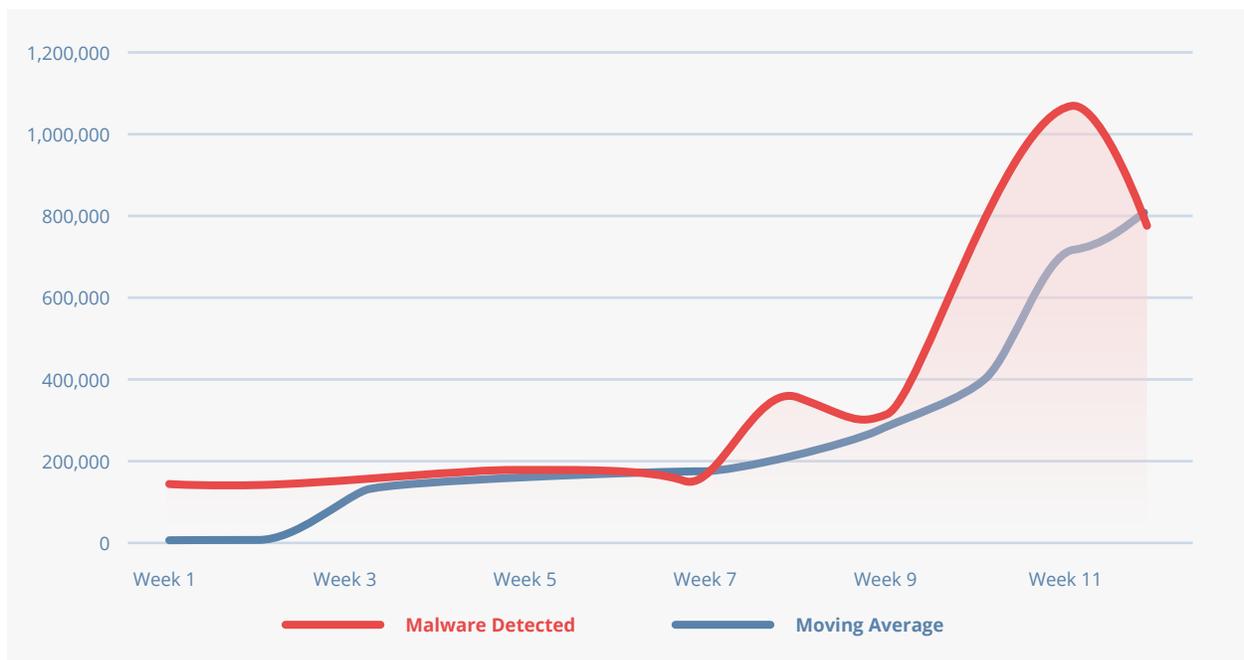


Figure 1. Malware detection, Nuspire, Q3 2020

Malware activity remained consistent with Q2's average, until the end of August and beginning of September when activity began to significantly increase. The largest contribution to increased activity was Visual Basic for Applications based documents.

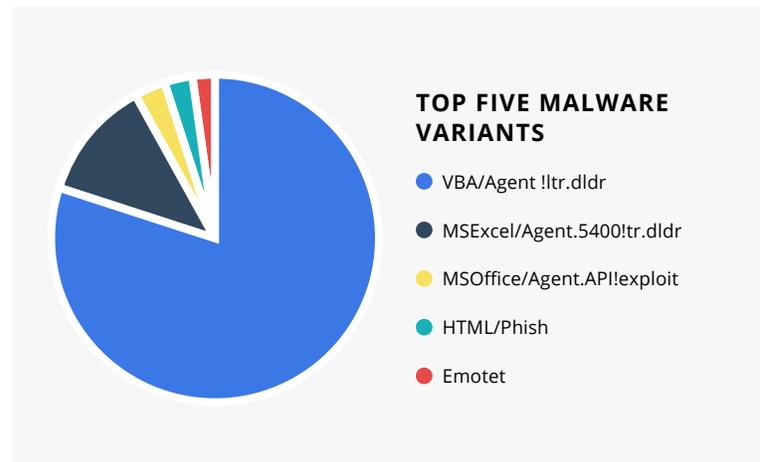


Figure 2. Top five malware variants, Nuspire, Q3 2020

## VBA Agents Activity

Visual Basic for Applications (VBA) Agents are a generic type of trojan that utilize Microsoft Office applications such as Microsoft Word and Microsoft Excel. These are often deployed in malspam campaigns and include common lures such as legal documents, invoices, or may be themed after prominent media events. Once the embedded macros are activated, the agent executes commands utilizing PowerShell to interact with a command and control server which pushes the next-stage payload down to the victim machine. Figure 3 shows VBA activity for the duration of Q3.

VBA Agents are a commonly used tactic for malware such as Emotet. Threat intelligence in Q3 suggested a new Emotet campaign was launching and Nuspire witnessed activity increasing shortly after. Additionally, VBA Malware was seen supporting instances of Dridex, Zeppelin

Ransomware, njRAT, Agent Tesla Keylogger, AZOrult and more were observed.

Organizations should be extremely cautious when interacting with email attachments, especially ones from unknown senders and those that contain macros. User awareness training is critical to prevent interaction with these files along with next generation antivirus with heuristics and behavioral analysis in the circumstance the malicious macros are enabled.

Nuspire’s Managed Gateway Service automatically detects this type of activity and sends an alert to our security operations center (SOC). A SOC engineer will review the activity and connect with the client to provide remediation support while checking for any signs of compromise.

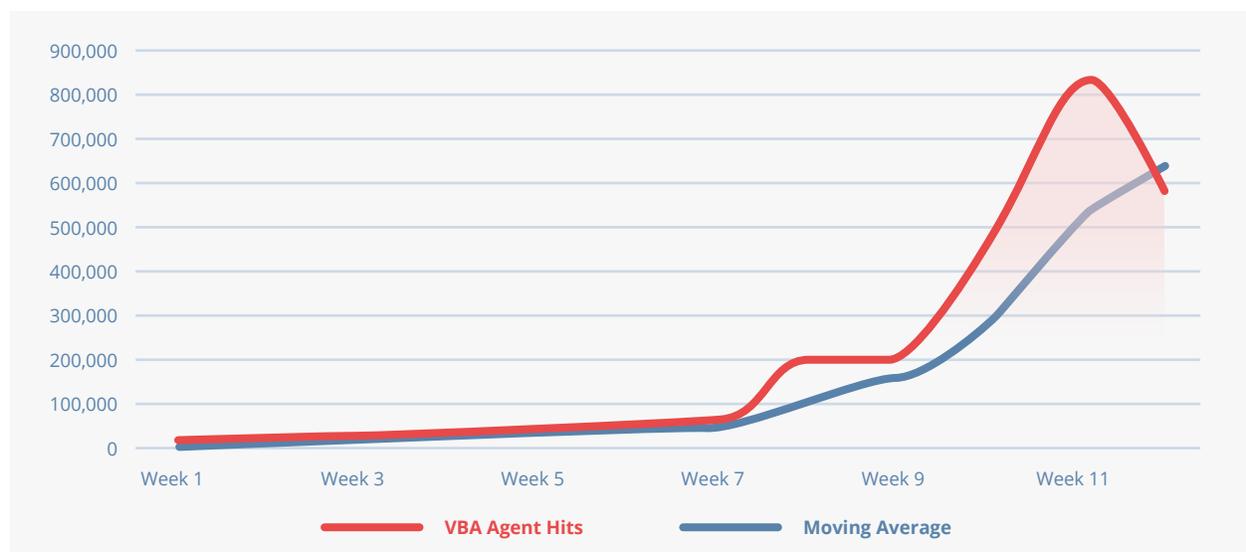


Figure 3. VBA Agent Activity, Nuspire, Q3 2020

## Emotet

Emotet has consistently been one of the top offenders in Nuspire threat reports. Activity trailed off during Q2 and ceased completely during the beginning of Q3. Threat intelligence suggested

mid-quarter that Emotet was making a resurgence and near the end of August activity was seen rising again through monitored devices as shown in Figure 4 below.

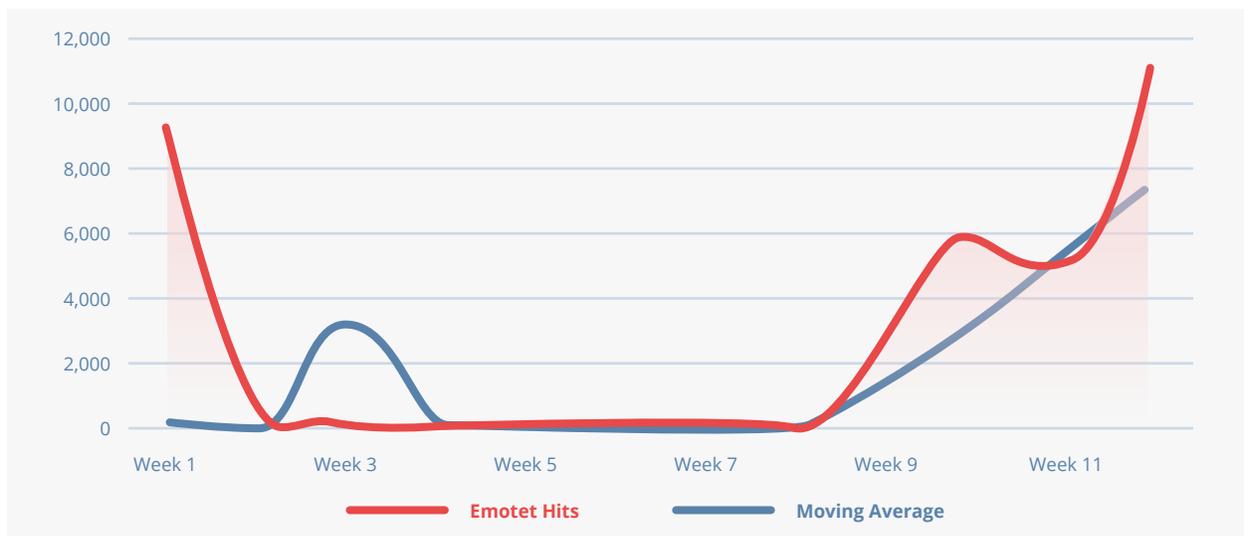


Figure 4. Emotet Activity, Nuspire, Q3 2020

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.

### Recorded Future®

Recorded Future finds that because of this, Emotet remains one of the most prominent and prolific threats to enterprises in 2020, as its continued innovation creates footholds to load various other banking trojans and ransomware families. After going dormant earlier this year for approximately five months beginning in February 2020, Emotet email campaigns resumed around July 17, 2020. Since July 17, 2020, Proofpoint has reported over seven million messages observed over a 40-day timespan. An average volume of just over 180,000 messages per day from Emotet were reported.

This resurgence of Emotet campaigns has impacted entities globally, including Quebec's Department of Justice and french companies and administrations. In addition, Recorded Future has observed its operators using major events (COVID-19 pandemic, U.S. elections) as phishing lure themes to assist in delivery.

Major shifts in Emotet's TTPs include:

- The replacement of TrickBot with QakBot as a final payload
- A 1,000% increase in Emotet downloads, correlating with Emotet's packer change, which causes the Emotet loader to have a lower detection rate across antivirus software
- Operators using new Microsoft Word document templates
- Operators using password protected archives containing malicious macros to bypass detections

Emotet's spreading mechanisms include hijacked email threads or mass spam campaigns, but both methods often rely on Word document attachments containing macros to download the Emotet binary. 2020 spam campaigns capitalize on a variety of lures themed around invoices, shipping information, COVID-19 information, resumes, financial documents and other financial documents.

It is used to download third-party banking malware such as Trickbot and Qakbot to launch widespread email campaigns on an international scale, and load Emotet modules for spamming, credential stealing, email harvesting and spreading on local networks.

Emotet has maintained a consistent, blistering operational tempo since at least 2014. In the summer of 2020, new features implemented in Emotet modules implied that the group will likely continue operations throughout the remainder of the next quarter (at a minimum) to successfully gauge the viability of these new features.



Nuspire actively threat hunts against newly observed campaigns within our client environments utilizing indicators of compromise (IOC) and threat intelligence. IOCs observed in Q3 can be found in the [appendix](#).

## 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.

---



**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.

---



# Botnets



## Botnet Events

**1,519,869**

TOTAL BOTNET EVENTS

**-6.23%** 

DECREASE IN TOTAL ACTIVITY FROM Q2

**46**

UNIQUE BOTNETS DETECTED

**18,093**

INFECTIONS PER DAY

**126,655**

INFECTIONS PER WEEK

**0%**

CHANGE IN UNIQUE BOTNETS DETECTED FROM Q2

## Botnet Detection

Botnet activity varied throughout Q3 with most activity being attributed to H-Worm and ZeroAccess botnets. Lowered activity in weeks seven through nine correlates to a slowdown in activity from H-Worm during that period. This could indicate the end of one campaign and the start of another. No new botnets were detected on monitored devices,

but overall, there was a decrease in activity by -6.23% compared to Q2 activity.

Figure 5 below shows a moving average of botnet activity throughout Q3 as a navy line, whereas the red line illustrates the true weekly numbers to help identify spikes and abnormal activity.

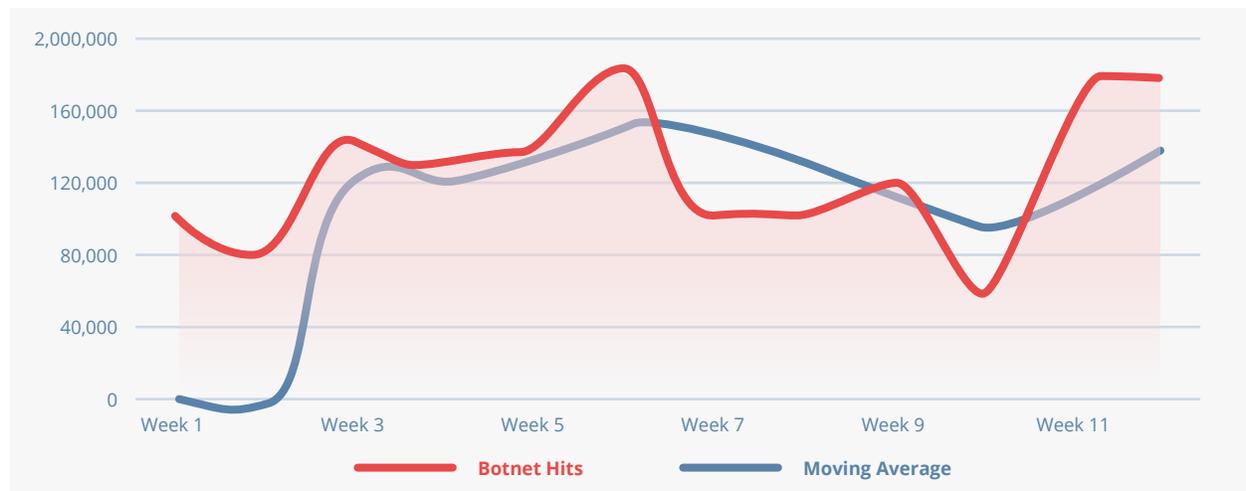


Figure 5. Botnet infections, Nuspire, Q3 2020

Figure 6 shows the top five botnets witnessed in Q3. Andromeda, as witnessed in Nuspire’s Q1 threat report has worked its way back into the top 5, while Necurs and ZeroAccess remain. Cidox, Conficker, and Mirai all fell out of the top 5 in Q3.

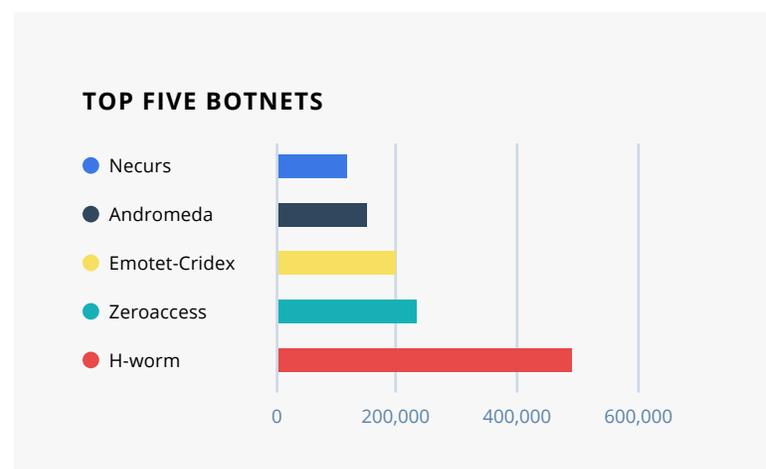


Figure 6. Top Five Botnets, Nuspire, Q3 2020

## H-Worm

H-Worm Botnet, also known as Houdini, Dunihi, njRAT, NJw0rm, Wshrat, and Kognito, surged to the top of Nuspire’s witnessed Botnet traffic for Q3. Activity was witnessed during Q2 and Q3 from the actors behind the botnet by deploying instances of Remote Access Trojans (RATs) using COVID-19 phishing lures and executable names. H-Worm

Botnet can contain features such as executing files, rebooting victim machines, keylogging, and stealing information from popular web browsers like Google Chrome and Mozilla Firefox. As indicated by the name it also has the ability to worm and spread itself throughout a network.

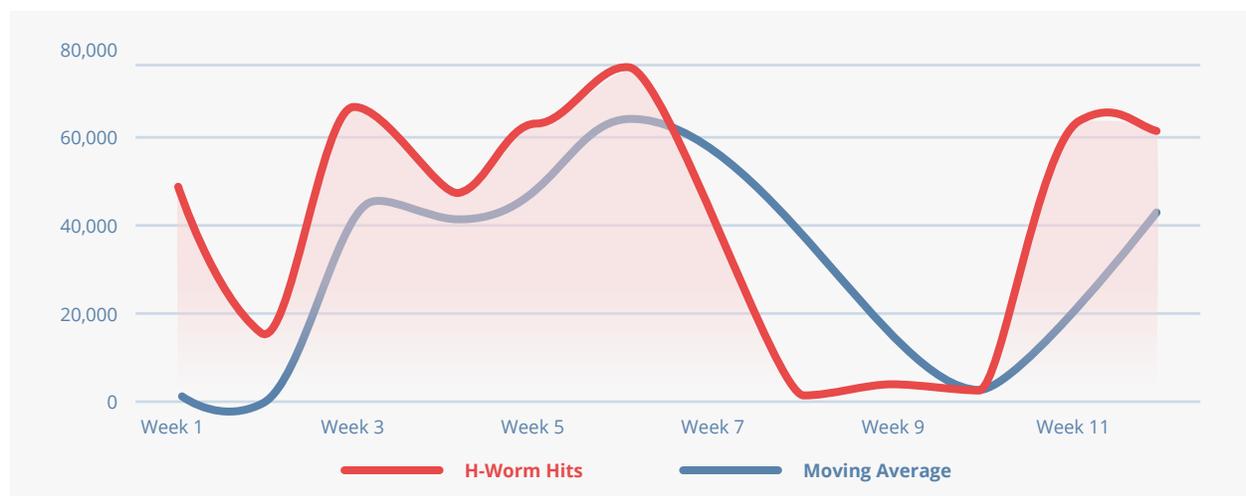


Figure 7. H-Worm Botnet infections, Nuspire, Q3 2020

The worm does include a builder which allows the attacker to customize the communication ports for the command and control server, utilizing port 1888 as the default. Once connected, the threat actor is able to see information like the operating system, system users and attached USB devices. The source code was leaked and the popular njRAT remote access trojan was created based on the leaked Njw0rm code and is considered the next generation of it.

njRAT has been included in an exploit kit called “Lord Exploit Kit” and exploits a vulnerability in Adobe Flash (CVE-2018-15982). Once exploited, it launches shellcode to download additional payloads such as ransomware.

Activity peaked around week 6, 61.42% higher than beginning of quarter, where it appears the active campaign ceased activity for a few weeks. This could be due to retooling / re-theming of payloads before activity began again in week 10 of the quarter and maintained until the end of the quarter.



Nuspire actively threat hunts for Botnet activity like H-Worm and contacts clients if it is found within their environment with remediation assistance. Observed IOCs for Q3 can be found in the [appendix](#).

## ZeroAccess

ZeroAccess peaked as the top offender in Q2 before activity completely trailed off. Starting in week 7 of Q3, the botnet ended its hibernation and spiked in activity as seen below in Figure 8.

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.

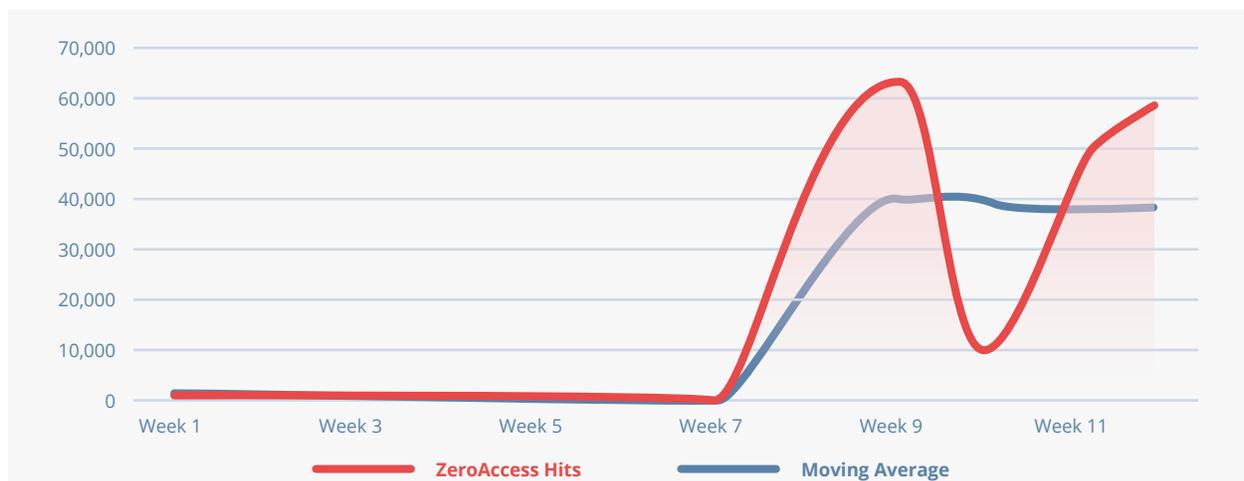


Figure 8. ZeroAccess botnet activity, Nuspire, Q3 2020

Over time ZeroAccess has evolved but its motivations remain the same. Add a victim to the botnet and monetize the device. ZeroAccess has been known to be included in illicit software, such as pirated games and programs, along with being deployed through phishing campaigns using social engineering lures.



Nuspire actively threat hunts for Botnet activity like ZeroAccess and contacts clients if it is found within their environment with remediation assistance. Observed IOCs for Q3 can be found in the [appendix](#).

# 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

**30,480,289**

TOTAL EVENTS

**1.84%** 

INCREASE IN TOTAL ACTIVITY FROM Q2

**371**

UNIQUE EXPLOITS

**362,860**

EXPLOITS DETECTED PER DAY

**2,540,024**

EXPLOITS DETECTED PER WEEK

**3.34%** 

INCREASE IN UNIQUE EXPLOITS DETECTED FROM Q2

## Exploit Detection

Q2 ended with a decrease in activity and Q3 activity remained low in the opening weeks before picking up and gaining traction into the end of the quarter. DoublePulsar remained King in exploit activity, closely followed by a surge of

activity regarding HTTP Server Authorization Buffer Overflow attempts. Activity surged over 317.84% from opening of quarter to close. With regard to protocols targeted, NetBIOS remained the highest targeted, the same as Q2.

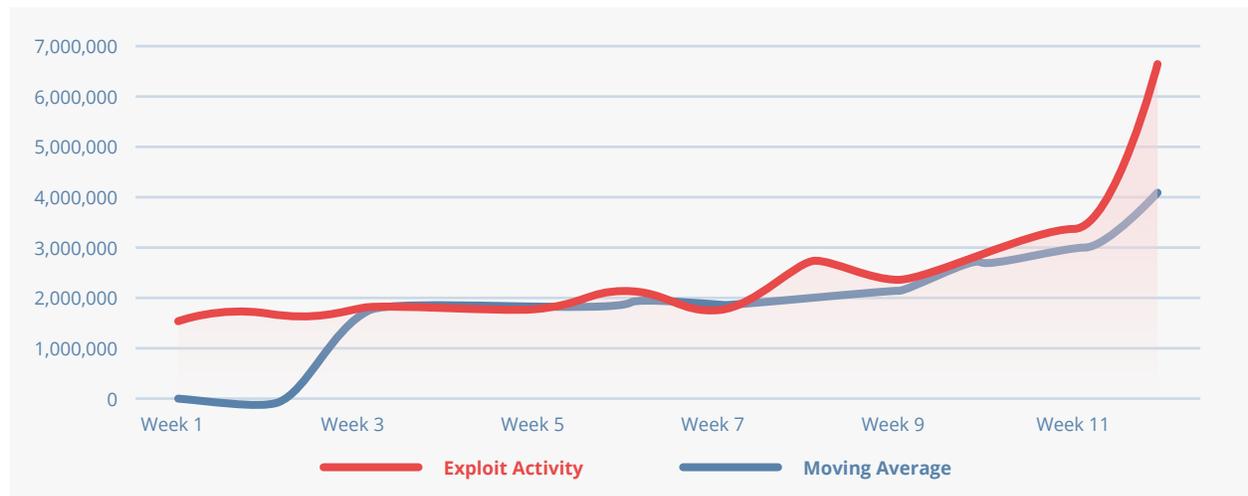


Figure 9. Exploits detected, Nuspire, Q3 2020

NetBIOS remained the highest protocol targeted, the same as in Q2. NetBIOS is an insecure protocol

primarily used for name resolution when DNS is not available. It is highly recommended that it is

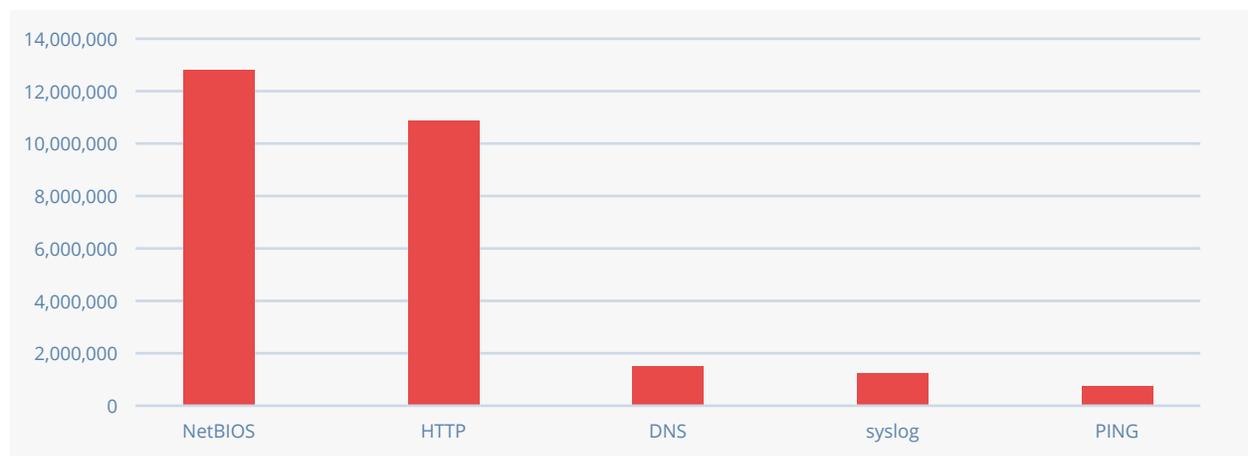


Figure 10. Protocols Exploited, Nuspire, Q3 2020

disabled within your network if not utilized as it often comes enabled by default for network adapters in Windows.

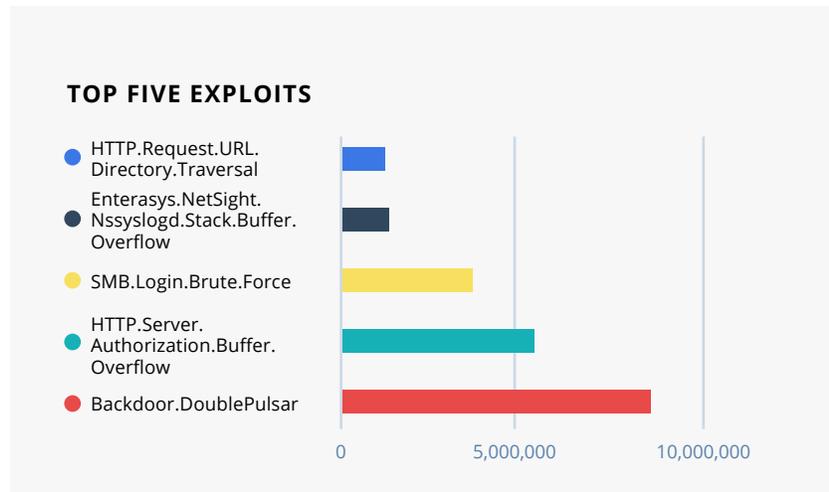


Figure 11. Top Five Exploits, Nuspire, Q3 2020

## DoublePulsar

DoublePulsar reigns again in Q3 as the top utilized exploit. It is expected to continue as the top exploit in Q4 due to its sophistication, the low technical ability needed to execute it and ease of access.

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.

Microsoft released security bulletin containing patching information, [MS17-010](#). Further information can be found on EternalBlue the underlying exploit via [CVE-2017-0143](#), [CVE-2017-0144](#), [CVE-2017-0145](#), [CVE-2017-0146](#), [CVE-2017-0147](#), and [CVE-2017-0148](#).

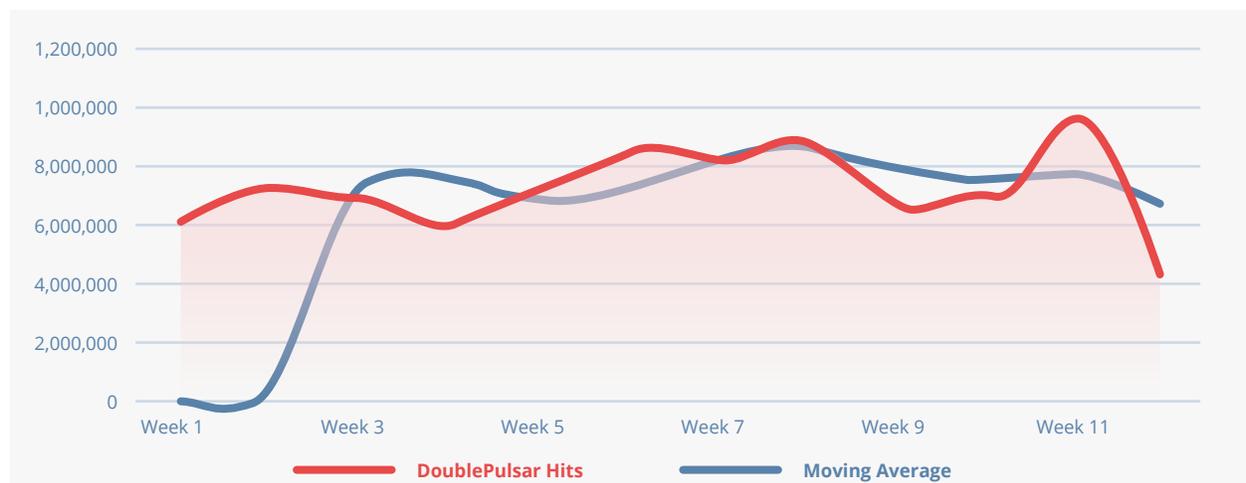


Figure 12. DoublePulsar Activity, Nuspire, Q3 2020

As shown in the Figure 12 above, DoublePulsar activity peaked in week 11—increasing by 36.05% from the beginning of the quarter. Attackers are often searching for exposed RDP connected in an attempt to exploit them and resell connections or to launch an additional attack once in the network. Compromised RDP connections can sell for up to \$15 each and attackers can use tools like Shodan to scout out potential targets.

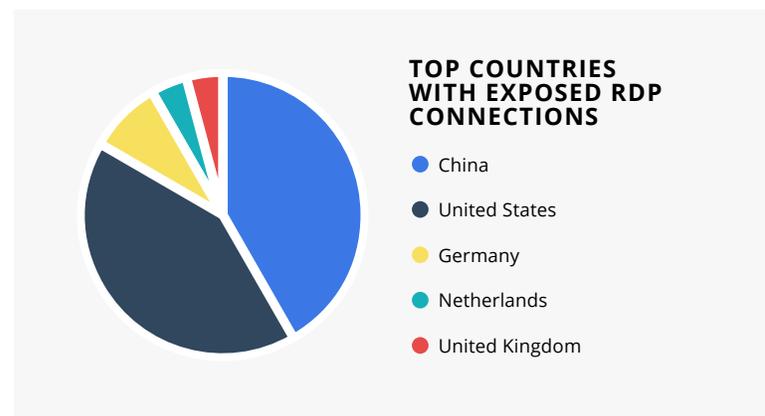


Figure 13. Exposed RDP Connections, Nuspire, Q3 2020

Utilizing Shodan, there are currently 3,948,878 exposed connections. The majority are hosted from China with the United States very closely behind as seen in Figure 13. Some observed were tagged operating datacenter versions of Windows Server and would be a very attractive target for attackers. Top organizations supporting these connections were Tencent cloud computing, Amazon, Microsoft Azure, Google Cloud and Choopa, LLC.

Once attackers gather enough compromised RDP connections, they will sell them in bulk on dark web forums and websites to collect their bounty. During Q3, 2,331 instances of sales involving

RDP connections were witnessed on dark web marketplaces.

In response to the COVID-19 pandemic, many organizations have shifted to working from home for the foreseeable future — this means that organizations will have a largely (or entirely) remote workforce for the first time. Cybercriminals and nation-state actors have continued to target and exploit vulnerabilities in remote access tools and VPNs to deploy ransomware, engage in cyberespionage and steal sensitive business information.



**Recorded Future finds that there has been a reported 127% increase in exposed RDP (port 3389) systems on the internet since the beginning of the Covid-19 outbreak in early 2020. We believe this is likely a side effect of a rapid and massive increase in remote workers. RDP is a known weak point in network defense that is commonly used by ransomware operators and other cybercriminals and nation-state actors to gain access to—and move laterally within—enterprise networks.**

## Additional Remote Exploits Observed

**CVE-2020-0688.** A remote code execution vulnerability exists in Microsoft Exchange software when the software fails to properly handle objects in memory, aka 'Microsoft Exchange Memory Corruption Vulnerability'. According to NSA and CISA, unnamed nation-state actors have been observed targeting CVE-2020-0688 for exploitation.

**CVE-2020-0796.** A remote code execution vulnerability exists in the way that the Microsoft Server Message Block 3.1.1 (SMBv3) protocol handles certain requests, aka 'Windows SMBv3 Client/Server Remote Code Execution Vulnerability'. This vulnerability has reportedly been exploited to deploy ransomware variants such as Zeppelin, Smaug, and RagnarLocker.

**CVE-2019-11510.** This vulnerability is found In Pulse Secure Pulse Connect Secure (PCS) 8.2 and 9.0. If the vulnerability is successfully exploited, an unauthenticated remote attacker can send a specially crafted URI to perform an arbitrary file reading vulnerability. This vulnerability has reportedly been exploited to deploy ransomware variants such as REvil and by the WellMess espionage campaign targeting healthcare entities.

**CVE-2018-13379.** This is a path traversal vulnerability found in Fortinet FortiOS products, specifically under the SSL VPN web portal. If the vulnerability is successfully exploited an unauthenticated attacker can download system files via specially crafted HTTP resource requests.

**CVE-2020-5902.** A remote code execution vulnerability exists in F5 BIG-IP devices, in the Traffic Management User Interface (TMUI). The threat actor Parisite (aka Pioneer Kitten) has been observed targeting this vulnerability en masse.

**CVE-2019-19781.** A remote code execution vulnerability exists in Citrix Application Delivery Controller (ADC) formerly known as NetScaler ADC and Citrix Gateway formerly known as NetScaler Gateway.

**CVE-2019-1579.** A remote code execution vulnerability exists in Palo Alto Networks "Global Protect" VPN servers.

## HTTP Server Authorization Buffer Overflow

Surging in week seven of the quarter, a campaign utilizing HTTP Server Authorization Buffer Overflow attacks was launched by an unknown threat actor specifically involving [CVE-2018-5955](#) (CVSS 3.0 Score 9.8 of 10 (Critical)).

This vulnerability is regarding an issue that was discovered in GitStack through version 2.3.10 where if user-controlled input is not properly sanitized, it can allow an unauthenticated attacker

to add a user to the server via the username and password fields. Exploits against this vulnerability are included in the Metasploit framework making access easy for attackers.

GitStack has released a patch resolving this issue and any administrators using the software should ensure they are upgraded to a version higher than 2.3.10 to mitigate this vulnerability.

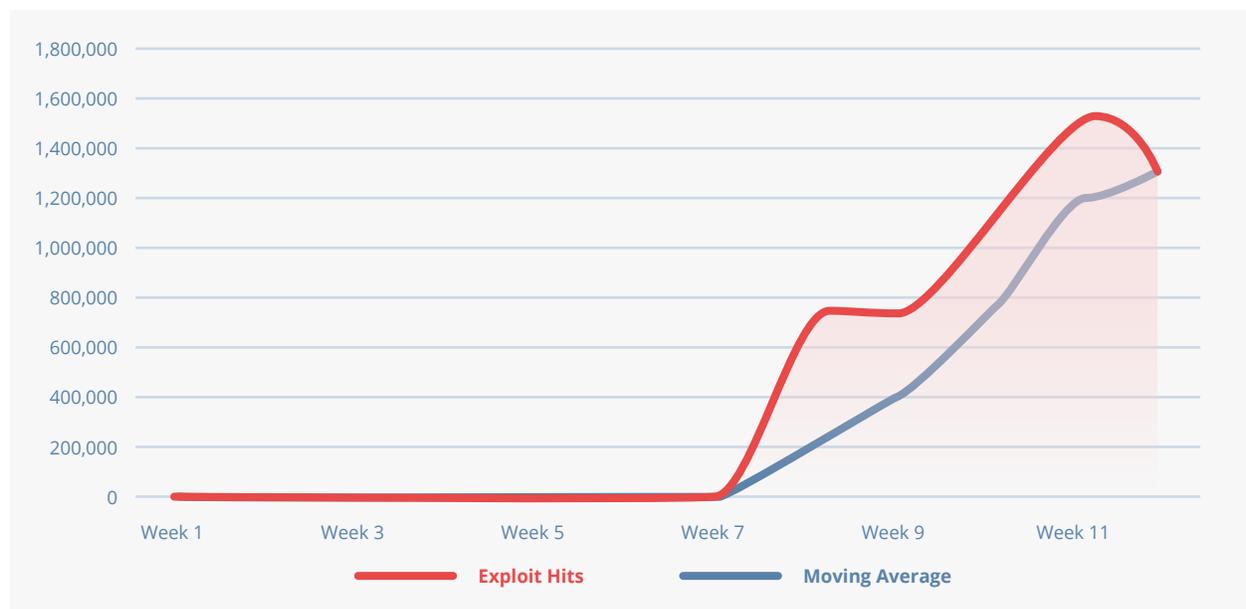
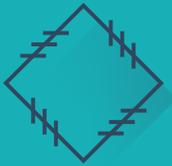


Figure 14. HTTP Server Authorization Buffer Overflow Activity, Nuspire, Q3 2020

# How to Combat

## PROACTIVE DETECTION AND MITIGATION MEASURES

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



**Patch your systems ASAP.** 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 avert 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.

---

## The New Normal

COVID-19 dramatically shifted the daily activities of countless people across the globe. Cybersecurity was not shielded from this shift as numerous organizations scrambled during Q2 to move their workforce to a remote environment and maintain operations. As restrictions relaxed, organizations have slowly begun to re-enter the office while some now are permanently working remote. These shifts provide opportunities for threat actors to launch attacks in the midst of the chaos. Additionally, the U.S. Elections have provided lures for phishers to attack. Nuspire witnessed Q3 attempts to guide victims to fake voter registration pages to harvest information while spoofing the Election Assistance Commission (EAC).

Often, these phishing attacks lead into an entry point for attackers to launch additional attacks like

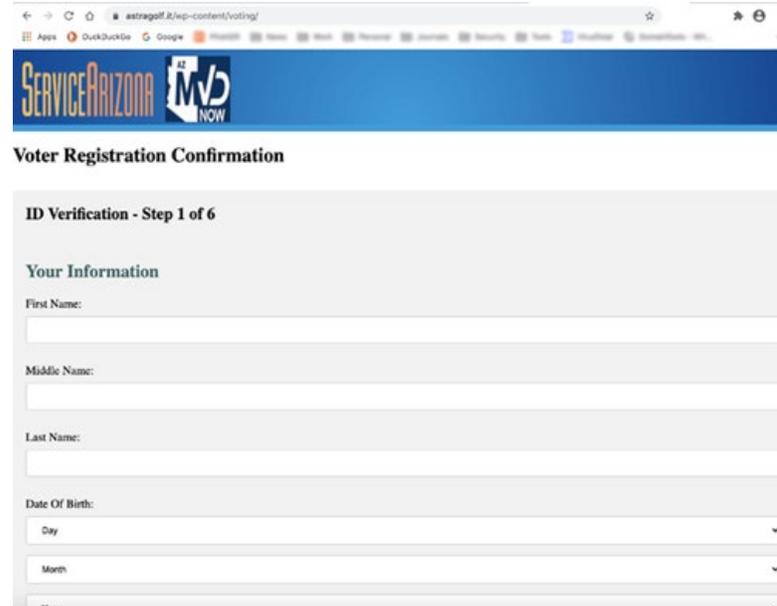


Figure 15. Phishing Example, KnowBe4, 2020

ransomware on an organization. Below Figure 16 shows observed malicious email activity during Q3. Activity trended consistently on average across the quarter.

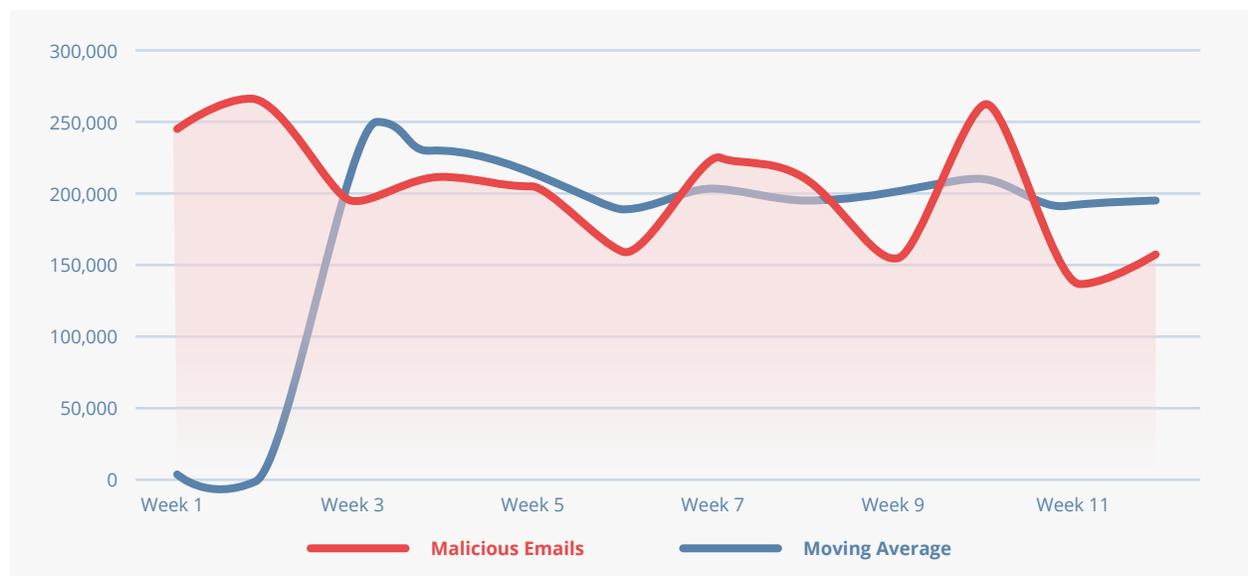


Figure 16. Malicious Emails Detected, Nuspire, Q3 2020

### Q3 SPEAR-PHISHING CASE STUDY

During Q3, Nuspire was involved with an incident response where the attacker gained a foothold into the network utilizing spear-phishing against the organization. Once the attackers had access to an email account, they created inbox rules to move messages to a folder called “RSS Subscriptions” and rules to forward emails to the attacker’s accounts. Additionally, they used the compromised account to spread malware internally and externally in an attempt to compromise additional accounts.

Nuspire quickly provided the following remediation assistance:

- 
- 
- 

Ransomware activity varied from week to week throughout Q3 on Nuspire managed endpoints

with the lowest amount of activity during week five and increasing 136.36% into week eight.

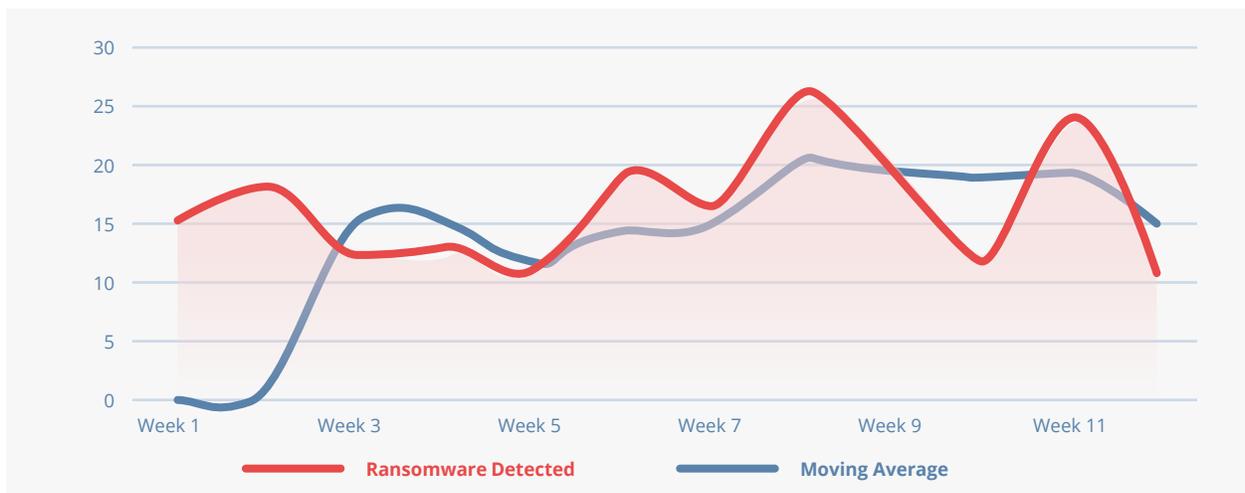


Figure 17. Ransomware Activity, Nuspire, Q3 2020

At the end of Q2, automotive giant Honda fell victim to SNAKE ransomware and attacks like these are costly. Organizations take on operational losses as well as reputational and brand damage. Threat Intelligence shows attacks on the automotive industry are on the rise. In 2019, attacks against the industry were referenced 10,219 times. At the end of Q3 2020, references have already surpassed the 2019 total at 18,307, an increase of 79.15% with Q4 still remaining. A typical automotive dealership in the United States experiences the following events in one month:

- 2,500 malicious website access attempts blocked
- 192 intrusion attempts blocked
- 491 viruses detected and blocked

84% of surveyed consumers say they “would not buy a car from a dealership after their data had been compromised.” It is imperative with the increases seen in the automotive industry that organizations take measures to protect themselves from threat actors.



**Recorded Future believes that ransomware operators will likely continue to extort educational institutions as well, who not only have the financial resources to pay ransoms, but feel a sense of urgency to do so in order to avoid disruptions during the school year. This sense of urgency is especially heightened as a result of the COVID-19 pandemic, as many schools have transitioned to virtual learning and thus are heavily reliant on digital resources and communications. Additionally, while some educational institutions do have large budgets, they often do not allocate enough towards cybersecurity controls or staff—making them a more susceptible target.**

Shifts in targeted industries and ransomware extortion website activity were prevalent in ransomware operations throughout Q3 2020. Operators of at least five ransomware families stood up new extortion websites of their own. Multiple organizations in the education sector were targeted, and Sodinokibi (also known as REvil) activity decreased while Netwalker (also known as Mailto) activity increased.

It is highly likely that ransomware operators will continue to persist, impact industries and continue using extortion tactics. However, the

Treasury Department advisories may impact the proliferation of organizations who are involved in facilitating the ransomware payments and will likely shift the calculations of cyber insurance companies (who have frequently been willing to pay the ransom even in cases where an alternative existed) based on overall cost calculations. Despite the advisory, victims are likely to continue to face few options other than paying the ransom for fear of facing the public relations and legal repercussions of the sensitive data of their clients being leaked on the extortion sites.

# 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. Organizations that are connected to the internet, or even with potential of internet connections, should know they are a potential target. Which means, understanding what the most active threats are and what an organization's digital perimeter is comprised of will help determine 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.

- 1. Conduct regular user awareness training.** End users can be overlooked in a security program where often the newest technology is chased. Educating your end users so they understand how to identify attacks and how to have a defensive mindset can be one of the most cost-effective ways to improve your organization's security posture. Create a culture of reporting suspicious activity and ensure you test internal policies and procedures. Ensuring your organization has all of the necessary security essentials covered will result in stronger security.
- 2. Take a defense in depth approach.** No single cybersecurity technology will secure your entire environment. Your organization should have multiple layers of defense from the edge device, endpoint protection, email/spam filtering, and end user awareness. All of the mentioned defensive elements have their strengths

and weaknesses and can help complement each other in depth. A strategic security assessment is a great first step to identify and fill any gaps. 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.

- 3. Upgrade your antivirus.** Traditional antivirus looks only at signatures of known malware, where next generation antivirus utilizes heuristics and behavior analysis to detect previously unknown malware when the execution of a file performs suspicious activity. These also provide security teams additional tools such as forensic storylines and remote quarantine.
- 4. Segregate your network.** High risk devices, like Internet of Things (IoT) devices, should be segregated on your network in case of compromise to minimize movement throughout the network. IoT devices should have their firmware updated as soon as vendor patches are available, and administrators should ensure default credentials are changed. Adopting a secure device management strategy enables you to harden security, no matter where or how your employees access your network.
- 5. Patch your Tech Stack.** Administrators should sign up for vendor security bulletins and apply patches as soon as possible within their environment. Attackers often seek new vulnerabilities in a race to exploit before organizations can patch. 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](http://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](http://www.recordedfuture.com) and follow us on Twitter @RecordedFuture.