nuspire

# QUARTERLY THREAT LANDSCAPE REPORT

Q1 2020

nuspire.com

# Table of Contents

# Letter from the CEO

Every day at Nuspire, we strive to make our client's fanatically happy with our services. It's not just lip service; we live it, and our culture breathes it. Our team focuses on a relentless pursuit of excellence in everything we do. And we do it all for you; to ultimately help you achieve the outcomes you desire and help your business become more secure.

To be successful, we must understand who the adversaries are, what they're after, how they would attack someone, and the overall risk they pose to Nuspire and our clients. Our objective is to identify trends and make predictions for what we can expect from cybercriminals. By taking an intelligence-driven approach to security, we can further help organizations protect themselves.

We know that cybersecurity is complex and continually changing; but, rest assured, we will always be here to help 24 X 7. Protecting organizations from these threats isn't just what we do, it's in our DNA. We are driven to go above and beyond to make sure our customers have customized solutions, are protected from the threats most relevant to them, and that they are 100% comfortable and confident with our services.

We are all in this together, two companies but one team. I hope the following report can provide information to help your organization be better prepared, and more able to successfully respond, and ultimately win out against the bad guys.

- Lewie Dunsworth

# About Nuspire

Nuspire is the Managed Security Services (MSS) provider of choice, is revolutionizing the cybersecurity experience by taking a people first approach to cybersecurity solutions. The company's 24x7 Security Operations Centers (SOCs) and managed detection and response (MDR) service combines award-winning threat detection and response technology with human intervention and analysis, providing end-to-end protection across the gateway, network and endpoint ecosystem. Nuspire pioneered distributed, managed security services within the enterprise and franchise market and today protects thousands of locations globally.

CONTACT US TODAY TO DISCUSS YOUR UNIQUE SECURITY CHALLENGES.

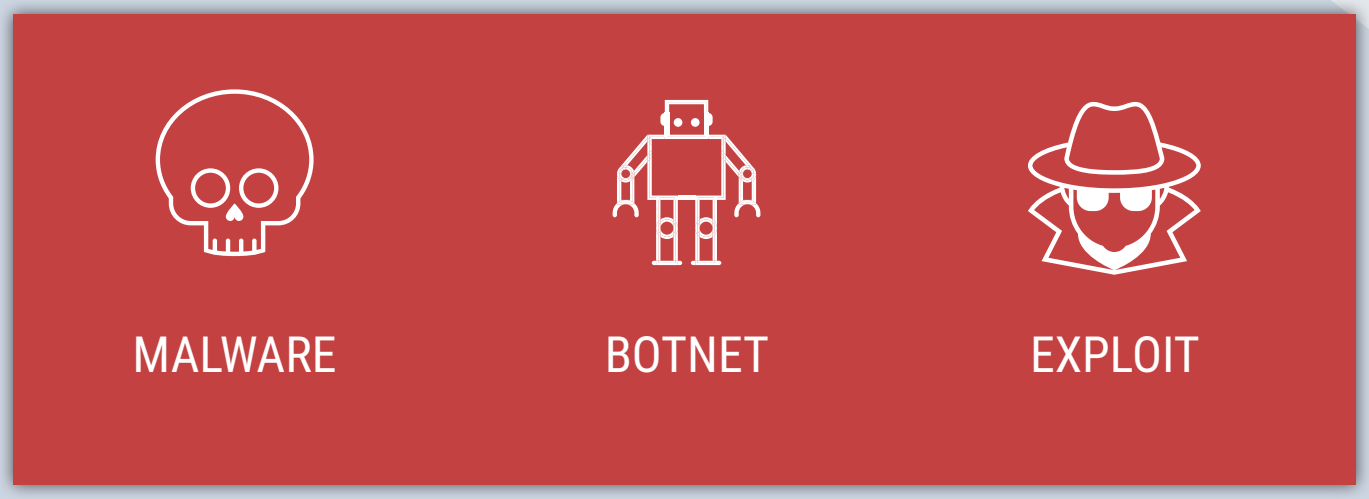
Data used in this report is sourced from Nuspire customers sites and associated thousands of devices across the globe. As a result, this report analyzes more than 90 billion traffic logs in the first quarter of 2020.

Nuspire's Security Intelligence & Analytics (SIA) Team follows a five-step data analysis methodology.

1. **Acquisition:** Nuspire 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:** Nuspire analysts further analyze with 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 will notify the customer and work with them to remediate the threat.
5. **Action:** Nuspire turns the knowledge gained from the process to action. Improvements are gained from consistenly reviewing processes, evaluation methods, and disseminating knowledge through sandboxing, malware analysis, honeypot activity, and alert creation.

Aggregated and correlated data from enterprise and mid-market clients provides a unique vantage point to threat vectors targeting vertical industries like automotive, manufacturing, and healthcare markets.

The report begins with an overview of the most prevalent cybersecurity headlines throughout the first quarter of 2020. Reported breaches and the headlines that play a crucial role in trend identification, as evidenced by findings highlighted throughout the report. Nuspire's threat report is divided into three main vector datasets: Malware, Botnet, and Exploit. The activities in each of these vectors have been compared to its activity in Q4 2019. All datasets are analyzed and identified to explain the most prolific and prevalent threats.



At the end of 2019, hackers' attack methods decrease, taking a break during the holiday season in preparation to retool tactics for 2020. The bigger threats seen in 2019, were Malware like Emotet and DoublePulsar. They were still making a significant impact in Q1, along with some newer threats.

## MALWARE

**2.4M+**
DETECTED

**1202** UNIQUE VARIANTS DETECTED
**200K+** VARIANTS DETECTED PER WEEK
**28K+** VARIANTS DETECTED PER DAY
**22%** DECREASE IN TOTAL ACTIVITY

## BOTNET

**1.2M+**
DETECTED

**46** UNIQUE BOTNETS DETECTED
**107K+** INFECTIONS PER WEEK
**15K+** INFECTIONS PER DAY
**52%** DECREASE IN TOTAL ACTIVITY

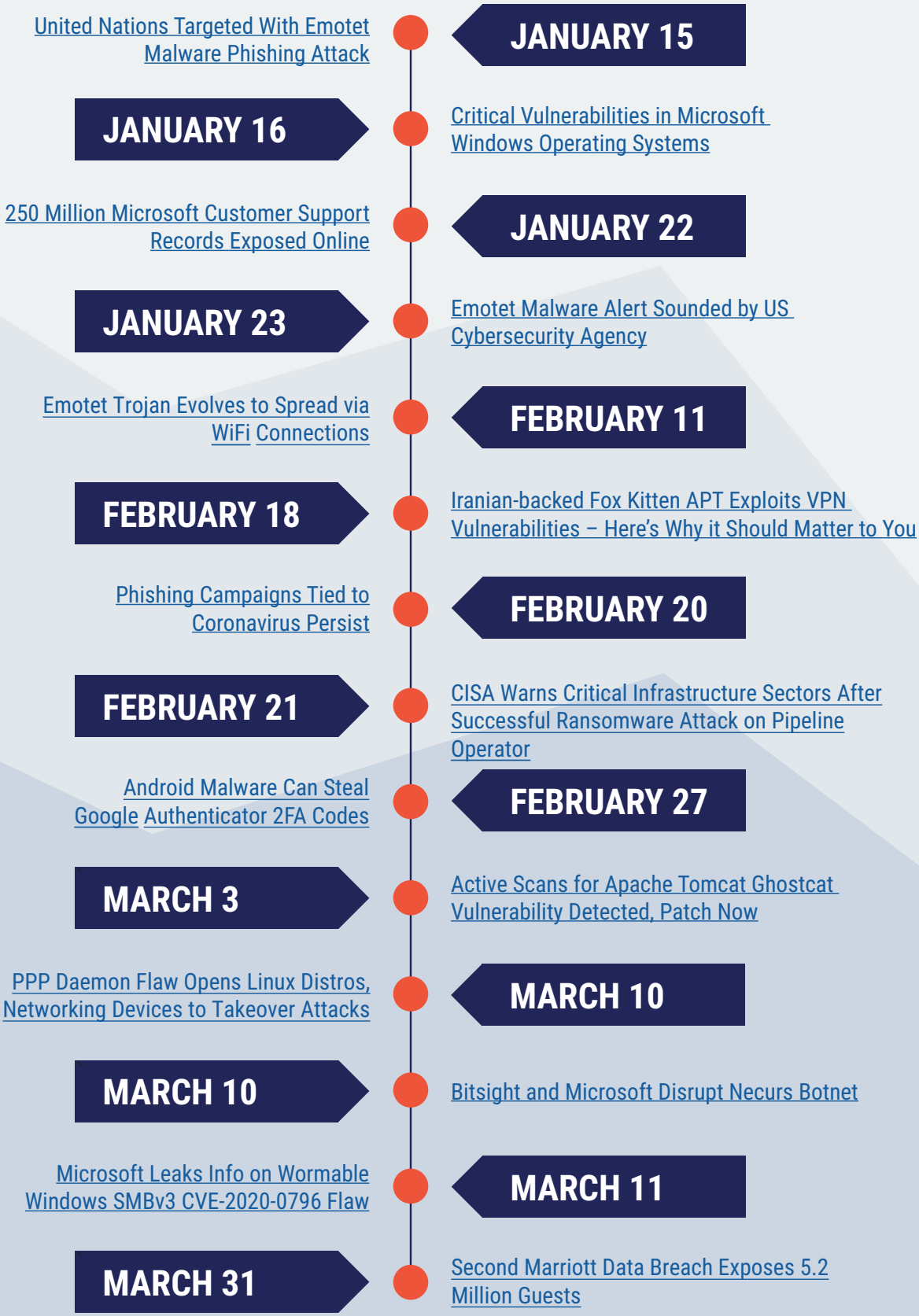
## EXPLOITS

**23M+**
DETECTED

**404** UNIQUE EXPLOITS DETECTED
**2M+** DETECTIONS PER WEEK
**278K+** DETECTIONS PER DAY
**6.3%** INCREASE IN TOTAL ACTIVITY

## HIGHLIGHTS FROM THE HEADLINES IN Q1 2020

In the first quarter of 2020, there were significant headlines about major threats and reported breaches affecting both businesses and consumers. Many of these threats were ones previously seen, but re-skinned to appear as legitimate sources during the COVID-19 crisis.



# MALWARE

**2.4M+** DETECTED

**1202** UNIQUE VARIANTS DETECTED

**200K** VARIANTS DETECTED PER WEEK

**28K+** VARIANTS DETECTED PER DAY

**5.6%** INCREASE IN UNIQUE VARIANTS DETECTED FROM Q4

**22%** DECREASE IN WEEKLY DETECTIONS FROM Q4

**24%** DECREASE IN DAILY DETECTIONS FROM Q4

While there was a 22% overall decrease in malware activity in Q1 2020 compared to Q4 2019, the two most prominent malware events had a significant spike in activity: Emotet and Executable and Linkable Format (ELF) variants. (See Figure 1)

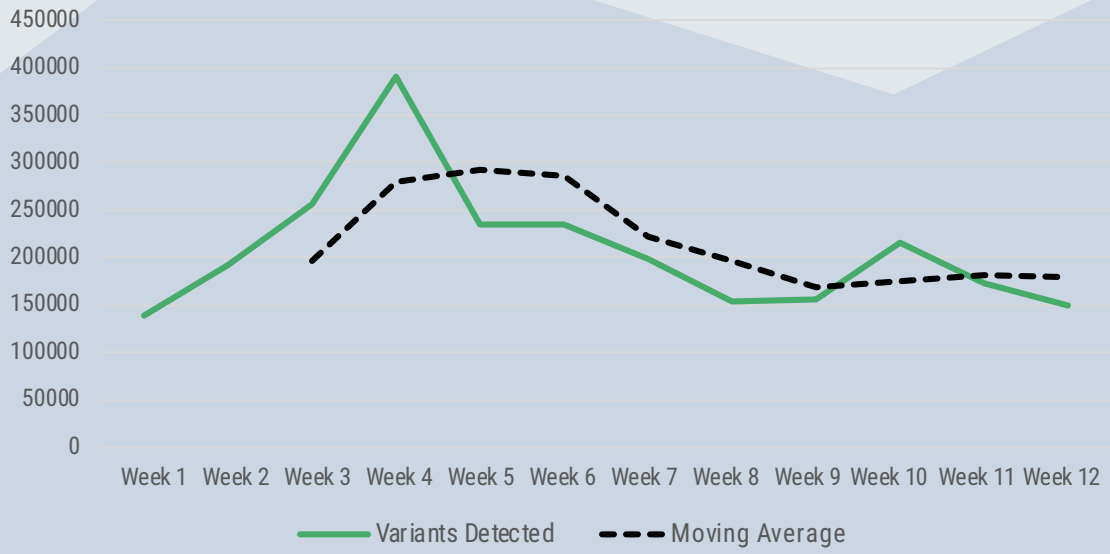



**Figure 1:** The moving average of malware activity throughout Q1 is shown as a dashed line, whereas the solid line represents the true weekly numbers of variants detected to help identify spikes and abnormal activity.

Malware increased throughout Q1 with some dramatic spikes with some variants. As a result, the overall activity from the beginning of Q1 to the end, was a 7% increase. The most notable spike was in week 4 of Q1 with a 179% increase in activity from the quarterly low. The spike was attributed to Microsoft Word macro-based trojan activity that correlated with the resurgence of reported phishing campaigns. Some of these were used to spread Emotet malware. Phishing campaign themes were consistently seen throughout all of Q1 included leveraging communications regarding with IRS Tax documents, financial invoices, and lately COVID-19 information.

**Emotet**

In 2018 and 2019 the security industry began to notice of the size of Emotet. Email spam distributors appear to have shifted from cryptomining payloads to distributing Emotet and remote access trojans (RATs), making Emotet impact even greater. In fact, some Emotet infections have cost up to $1 million to clean up[1].

Usually spread within Malspam campaigns, Emotet had taken the lead as the highest detected variant in Q1. Typically, Emotet is delivered in an email as a fake invoice and/or banking statement. As headlined in early January, Emotet was also seen used in highly targeted spear-phishing campaigns against the United Nations. These emails contained the same generic word documents as previously witnessed requesting users to enable editing or to enable content. When content is enabled, it allowed macros to be executed and load Emotet onto the victim's device.

Emotet can be challenging as a wormable malware that spreads to other network connected devices, and without the right protection can load additional malware like ransomware on infected machines. Additionally, Emotet has been known to contact command and control servers to receive updates from its authors. It has made such a resurgence in Q1, that the Cybersecurity and Infrastructure Security Agency (CISA) released an advisory regarding the increased activity to alert the information security community of the increase in attacks.

As shown in Figure 2, Emotet activity peaked in week 10. That was a 1317% increase from the lowest point of the quarter. A new variant of Emotet was discovered in the wild publicly published on February 7th, that includes a Wi-Fi Spreader module. This allowed Emotet to scan for wireless networks and infect devices that were connected to them. The new Emotet sample found had a time stamp of April 16th, 2018, but with the Wi-Fi spreader capability being brought to light in a public setting, it may have alerted attackers to the full potential of the variant sparking a new campaign. By the end of the quarter, attacks began to trail off dropping by 45% from its observed peak, but still 673% higher than beginning of quarter.

[1] US-Cert, Emotet Malware Alert, Jan 2020

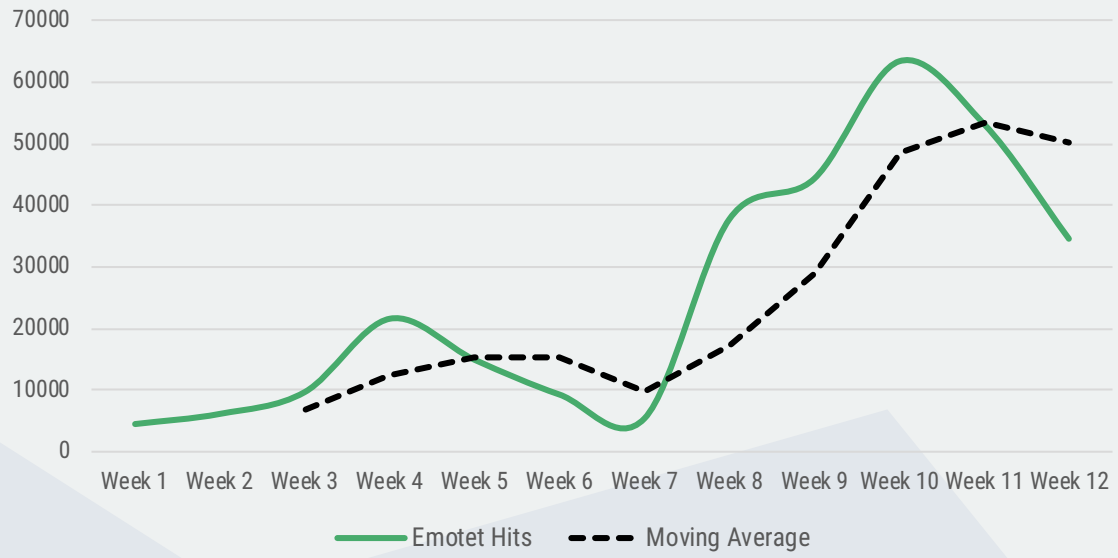



**Figure 2:** The moving average of Emotet activity throughout Q1 is shown as a dashed line, whereas the solid line represents weekly Emotet hits.

### ELF Variants

In Q1 we saw an increase in Executable and Linkable Format (ELF) variants targeting Internet of Things (IoT) devices with an attempt to further spread the Mirai Botnet. As shown in Figure 3, at the peak in week 11, there was an observed 86% increase in activity since the beginning of Q1. Often attackers would scan for IoT devices with open Secure Shell (SSH) or Telnet ports to gain brute-force access. Once shell access is gained, attackers would download a payload of the ELF based Mirai malware and added the device to the botnet. As mentioned later in the report, Microsoft announced they disrupted the Necurs botnet in week 11 and operators may have increased attempts to infect devices with Mirai. Activity at end of quarter remained steady at an 84% increase since the beginning of Q1.

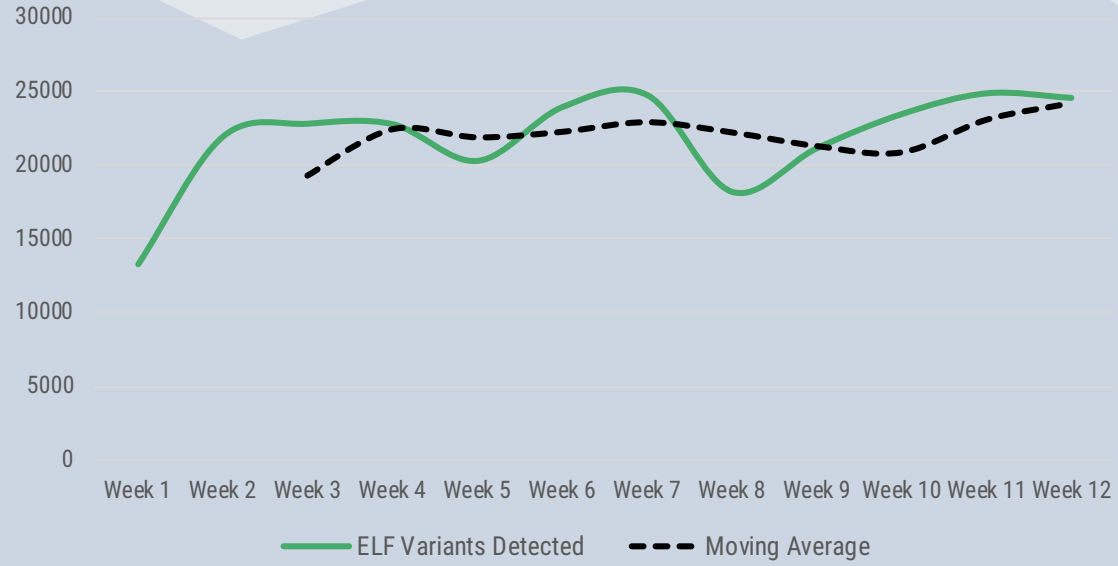



**Figure 3:** The moving average of ELF activity throughout Q1 is shown as a dashed line, whereas the solid line represents the true weekly numbers of ELF variants detected to help identify spikes and abnormal activity.

## WHAT TO DO: MITIGATION AND DETECTION

**Endpoint Protection Platforms (EPP).** Implement security-in-depth while utilizing Advanced, Next-Gen Anti-Virus (Next-Gen AV). Next-Gen AV will detect malicious software not only through signatures, but through heuristics and behavior. Legacy AV is strictly signature based which can only detect already known variants of malware.

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

**User Awareness.** User 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

**1.2M+** DETECTED

**46** UNIQUE BOTNETS DETECTED

**107K+** INFECTIONS PER WEEK

**15K+** INFECTIONS PER DAY

**52%** DECREASE IN TOTAL ACTIVITY FROM Q4

**28%** DECREASE IN UNIQUE BOTNETS FROM Q4

**61%** DECREASE IN WEEKLY DETECTIONS FROM Q4

**59%** DECREASE IN DAILY DETECTIONS FROM Q4

Throughout the quarter, the two most detected botnet events identified were Necurs and Andromeda. (See Figure 4)

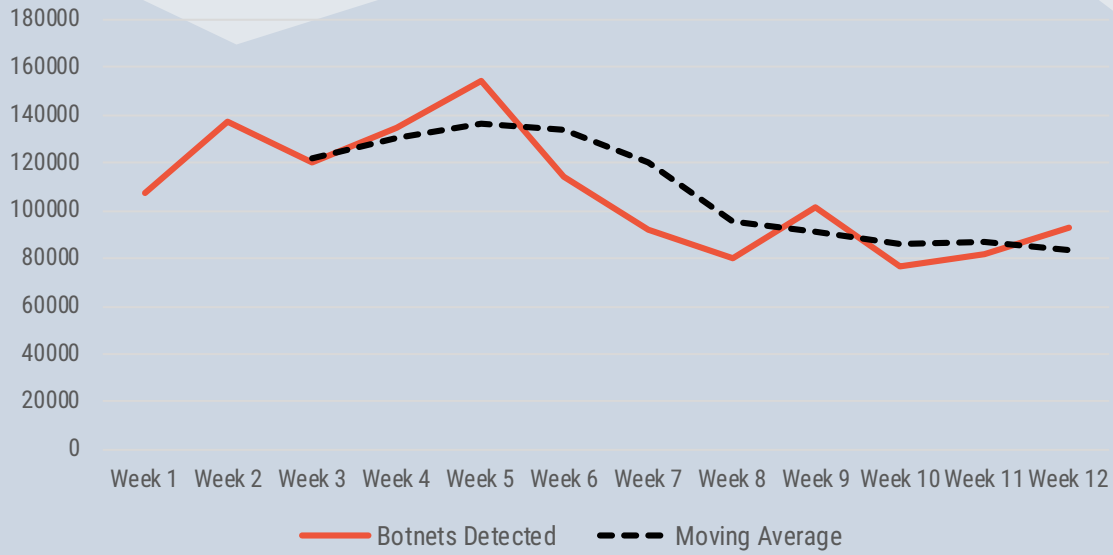



**Figure 4:** The moving average of botnet activity throughout Q1 is shown as a dashed line, whereas the solid line represents the true weekly numbers of botnets detected to help identify spikes and abnormal activity.

In Q4 (2019) there was a drawdown in botnet activity that carried over into Q1 2020. From the beginning of the quarter to the end, there was an overall decrease of 13% in activity. The top three botnets and associated traffic have all been disrupted or abandoned, and are expected to continually decrease.

**Necurs**

In March, Microsoft and their partners took action to disrupt Necurs botnet which was responsible for over nine million infections worldwide. A court-order was issued that allowed Microsoft to take control of U.S. based infrastructure used by Necurs, while they also working with their partners to prevent the registration of new domains to be used in any attacks.

You'll see below in Figure 5, Necurs traffic sharply decreased after the announcement from Microsoft[2] about disrupting the botnet. In week 12, zero traffic from the Necurs botnet was observed on devices.

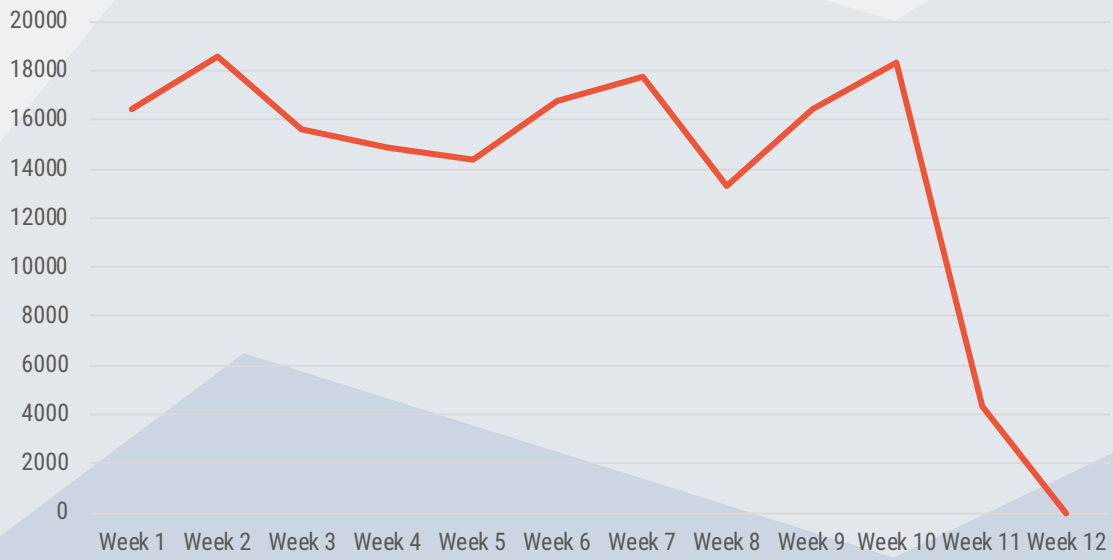



**Figure 5:** Necurs weekly activity shown throughout Q1.

[2] Microsoft, New action to disrupt world's largest online criminal network, March 2020

**Andromeda**

In 2017, command and control operations servers were shut down for Andromeda, it remained the largest botnet on devices with traffic sourced in Asia and the Middle East. Overall, traffic has decreased from beginning of Q1 to end by 58% and is expected to continue to draw down as devices are cleaned up and remediated.

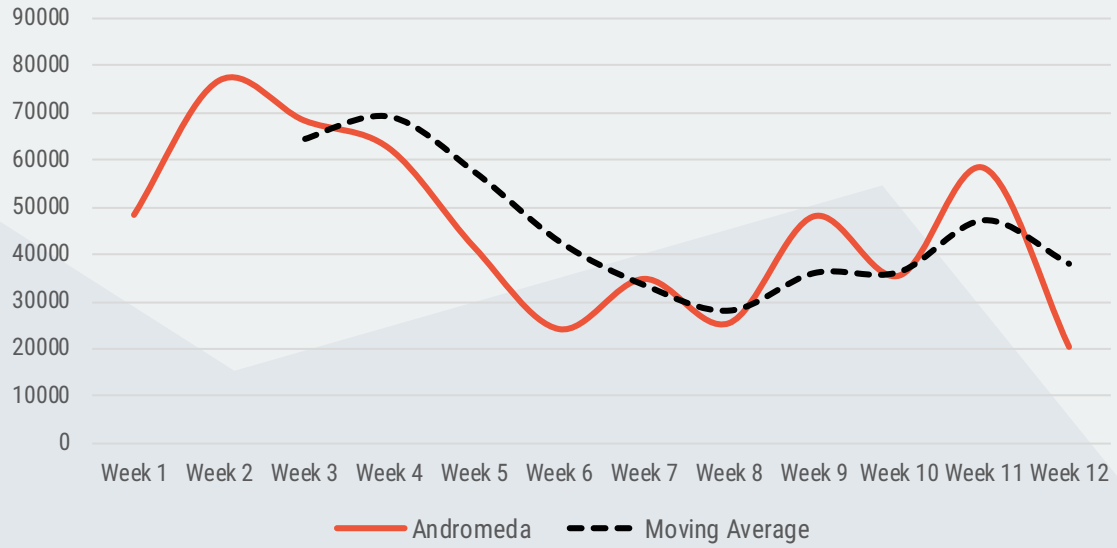



**Figure 6:** The moving average of Andromeda activity throughout Q1 is shown as a dashed line, whereas the solid line represents weekly Andromeda hits.

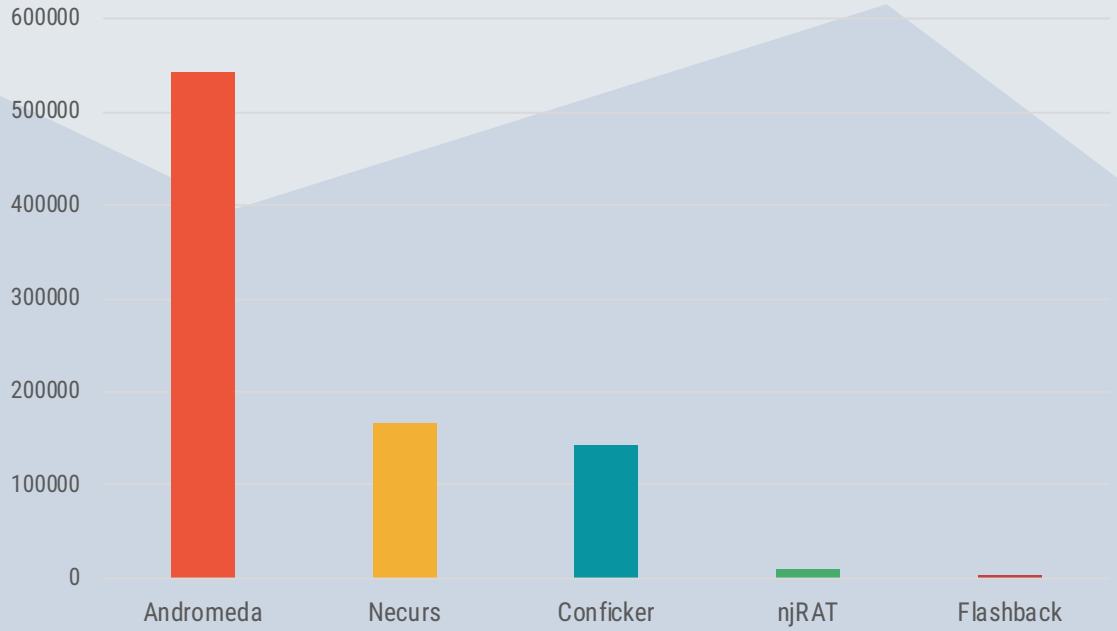



**Figure 7:** The most observed botnet traffic over Q1 with Andromeda being the most observed and Flashback being the 5th most observed.

## WHAT TO DO: MITIGATION AND DETECTION

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

**Leverage Threat Intelligence.** Threat Intelligence will help 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.

# EXPLOITS

**23.4M+** DETECTED

**404** UNIQUE EXPLOITS DETECTED

**2M+** DETECTIONS PER WEEK

**278K+** DETECTIONS PER DAY

**6.3%** INCREASE IN UNIQUE DETECTIONS FROM Q4

**5.2%** INCREASE IN WEEKLY DETECTIONS FROM Q4

**9%** INCREASE IN DAILY DETECTION FROM Q4

In Q1, there was an increase across the board in exploit activity. (see Figure 8) The most prominent exploit activities identified were DoublePulsar, Apache Tomcat 'GhostCat', Telnet Default Credential Scans and Operation Fox Kitten.

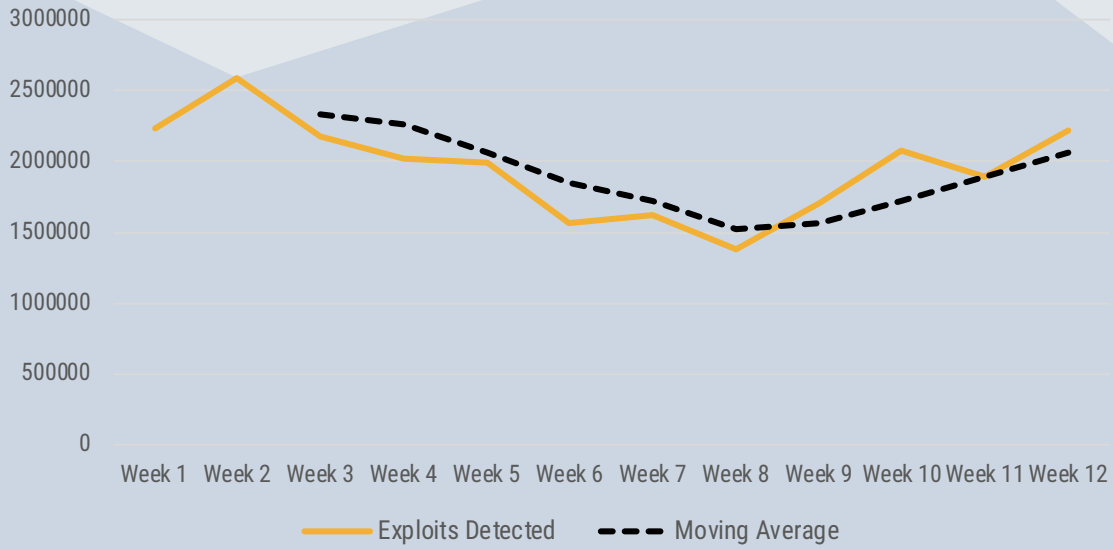



**Figure 8:** The moving average of exploits activity throughout Q1 is shown as a dashed line, whereas the solid line represents weekly exploits detected.

As you'll see in Figure 9, DoublePulsar continued from prior quarters, to be the most attempted exploit witnessed. Additionally, a new signature was introduced this quarter that specifically looks for attempts to use default credentials over Telnet. With the release of the new signature, data was reviewed to explore the attempts made against devices.

In addition, discovered and reviewed were the Apache 'GhostCat' vulnerability and Operation Fox Kitten, a hacking campaign that were conducted by Iranian Advanced Persistent Threat (APT) groups. Overall, Exploit activity increased by 6.3%.

**DoublePulsar**

In Q1, the highest exploit was DoublePulsar which was leaked by the ShadowBrokers group in 2017 through an exploitation framework called FuzzBunch. DoublePulsar is infamous in the deployment of the WannaCry ransomware and Nyeta worms and is an extremely sophisticated payload. Once a device is infected, it opens a backdoor to allow additional malware to be loaded further infecting its target. Every SMB and RDP exploit within FuzzBunch used DoublePulsar as the primary payload. It is expected that DoublePulsar will continue to be a highly used exploit regardless of the 12% decrease in activity by end of quarter.

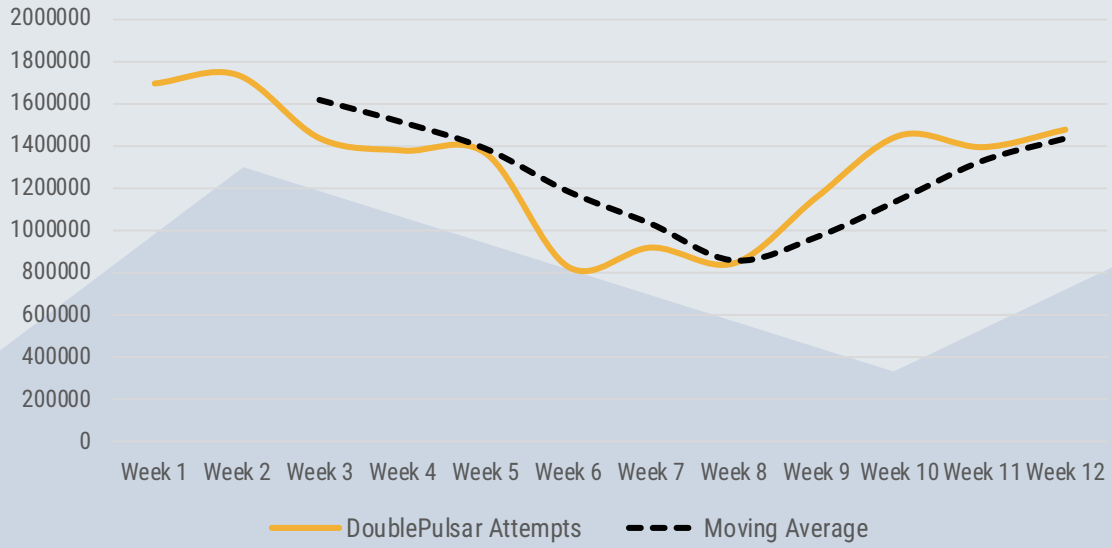



**Figure 9:** The moving average of DoublePulsar activity throughout Q1 is shown as a dashed line, whereas the solid line represents weekly exploits detected.

**Apache Tomcat 'GhostCat'**

The critical CVE-2020-1938 dubbed 'GhostCat' was a vulnerability announced in February 2020 with a criticality of 9.8 that highlighted a flaw in the Tomcat AJP protocol. This allowed an attacker to execute code using a Remote Code Execution (RCE) attack. After the public announcement of the vulnerability, the witnessed attempts remained very low. As attackers continue to create tools more user-friendly tools, there may be an increase in GhostCat attempts in Q2 as it becomes easier to exploit.

**Telnet Default Credential Scans**

Referenced in Figure 10, week 2 of Q1, a new signature became available to detect attempts to login using the default credentials of an IoT device through Telnet. Some malware, such as Mirai, actively scan for open Telnet ports and attempt to login using default credentials. As IoT devices are installed and forgotten about, they introduce very real security risks to networks. There were a maximum of 113K attempts in week 7 and a low point of 69K attempts in week 5. This serves as a reminder to administrators regarding the real threat of leaving open ports on devices, especially with default credentials.

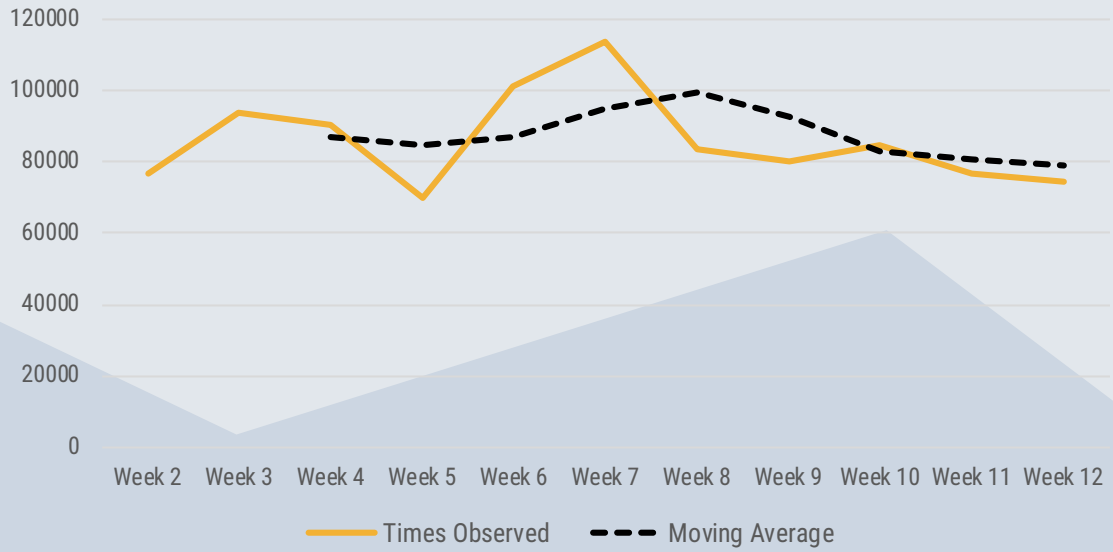



**Figure 10:** Weekly observed Telnet default credential scans in Q1.

**Operation Fox Kitten**

In February, there was a widespread Iranian Espionage-Offensive Campaign tied to multiple advanced persistent threat groups that were specifically targeting vulnerabilities in VPNs. There were exploitation attempts against CVE-2019-11510 (Pulse Secure "Connect" VPN), CVE-2018-13379 (Fortinet FortiOS VPN), and CVE-2019-19781 (Citrix "ADC" VPN) throughout Q1. With the workforce moving into remote settings as a response to COVID-19, it is important that system administrators are mitigating against vulnerabilities by applying vendor patches and upgrading to non-affected firmware.

In week 4 (see Figure 11), Citrix released patches to fix CVE-2019-19781 (Citrix) and in response there was a drop from week 3 peak of 1928 attempts to one attempt in week 5. While previously patched in 2019, shortly after the Citrix patch, a spike in activity was witnessed against CVE-2018-13379 (FortiOS). This may have been the attackers shifting their tactics to attempt a different VPN vulnerability in hopes administrators had not applied patches. As activity on CVE-2018-13379 (FortiOS) trailed off in week 11, activity in CVE-2019-11510 (Pulse Secure) began to rise until end of quarter.

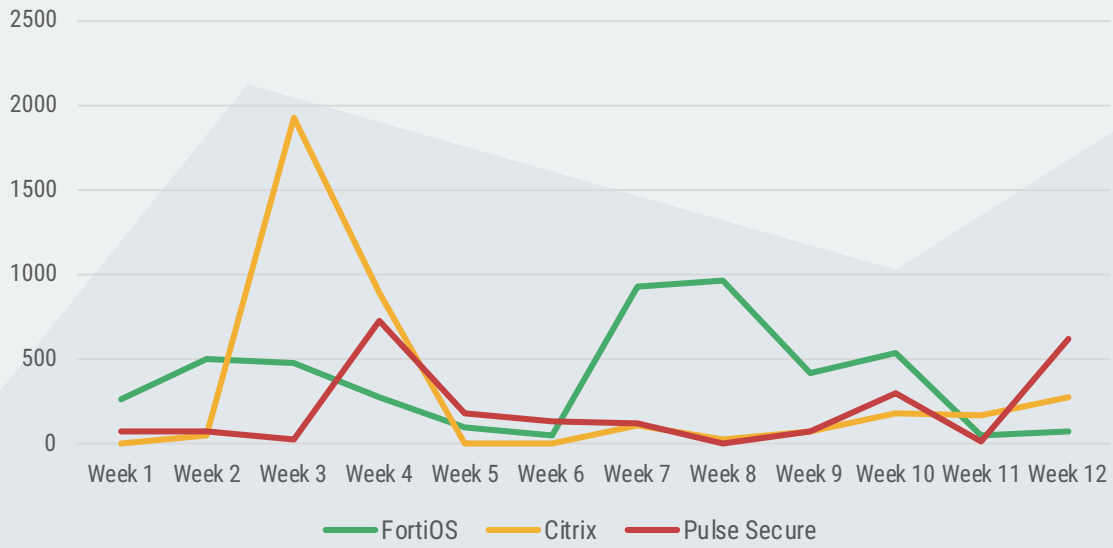



**Figure 11:** Graph shows activity of FortiOS, Citrix and Pulse Secure every week throughout Q1.

## WHAT TO DO: MITIGATION AND DETECTION

Exploitation activity is a race against the clock for all parties involved. Attackers are attempting to exploit vulnerabilities before vendors have an opportunity to patch them and to continue exploiting them before the consumer patches them. It is important for consumers to monitor vulnerabilities that relate to their tech stack and apply vendor patches as soon as feasible. In addition to keeping systems and applications updated, a firewall with an IPS can monitor, alert, and stop attack signatures that are targeting your environment.

### COVID-19 Themed Attack

In Q1 of 2020, the world was shaken by the effects of COVID-19 and the ensuing quarantine as organizations scrambled to move their workforce into remote settings. Unfortunately, the confusion, panic, and fear associated with the event has become a breeding ground of opportunity for attackers to take advantage of some of the un-prepared.

The World Health Organization (WHO) publicly announced they were seeing a rise in phishing attempts that claimed to originate from WHO. Nuspire witnessed some of these phishing attempts within our own e-mail sandbox, which you can see in Figure 12 below.

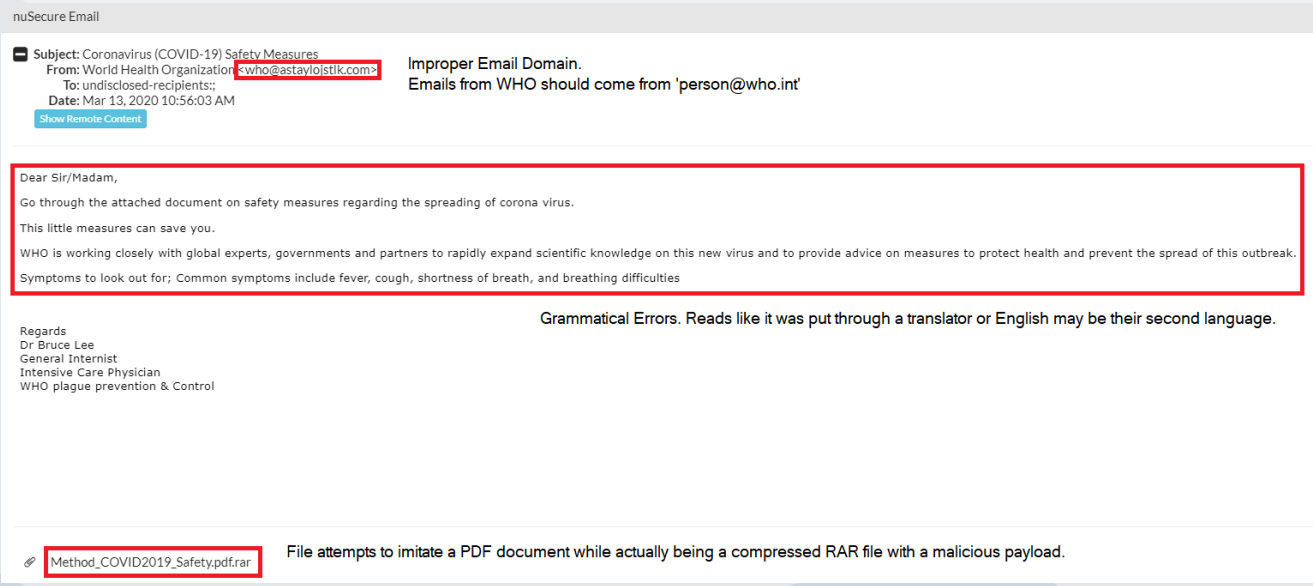



**Figure 12:** A COVID19 related phishing attempt identified in Nuspire's sandbox.

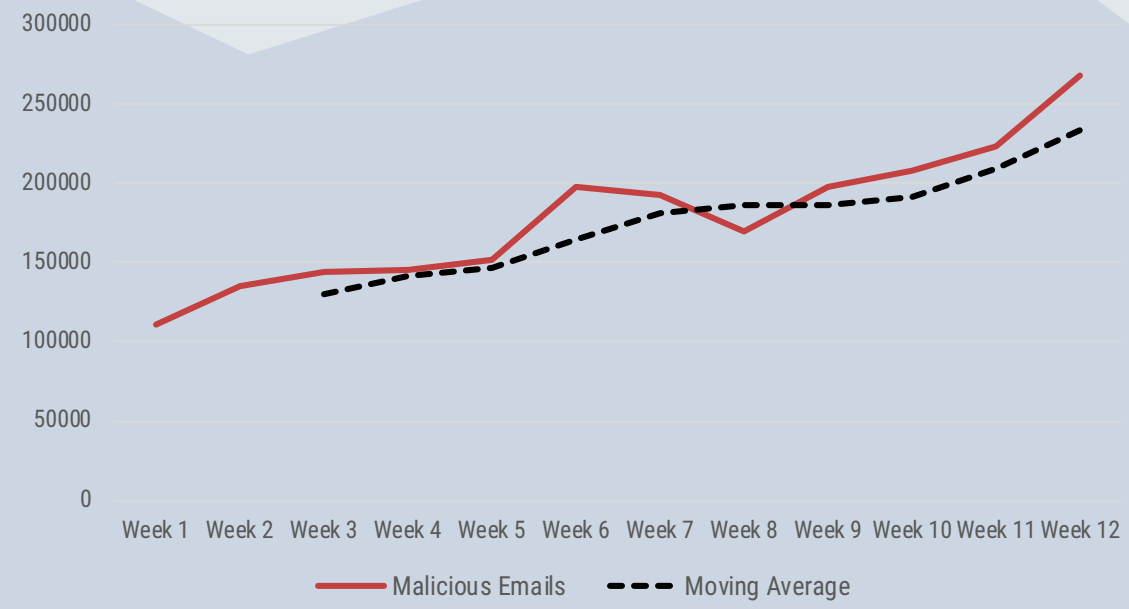
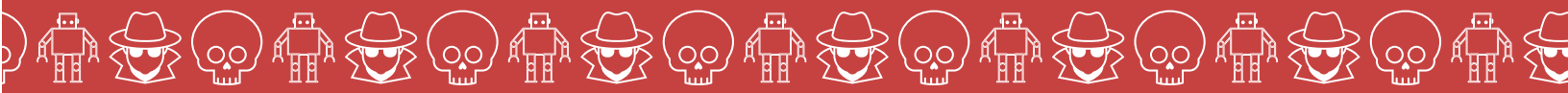



**Figure 13:** The moving average of malicious email activity throughout Q1 is shown as a dashed line, whereas the solid line represents weekly malicious email activity.

Numerous COVID-19 themes were witnessed in Q1 as a delivery mechanism for phishing and malware.

- World Health Organization Alerts
- Center for Disease Control Alerts
- Health Advice
- Vaccines or Miracle Cures
- Map Tracking Software
- Donation/Charity Scam Pages

As COVID-19 continues to be an impacting event worldwide, it is expected that attackers will continue to shift to COVID-19 based themes to entice victims to interact with their malicious payloads.



# CONCLUSION AND RECOMMENDATIONS

As cybersecurity threats and tactics continue to evolve, they are becoming increasingly more sophisticated, with the potential of doing more harm faster than ever before. The opportunity is cyberattacks can be predicted. Any organization that is connected to the Internet are a potential target.

There are simple things organizations can do to help keep their organizations safe and prevent them from becoming breached.

User awareness is one of the most powerful and cost-effective ways to prepare your organization against cyberattacks. Train your users how to identify phishing emails and to have a level of suspicion with email 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.

A layered approach to security will better protect businesses than a single cybersecurity product. It ensures that every individual defense component has a backup to counter any gaps in other defenses of security.

Advanced malware detection and protection technology (such as EPR) can track unknown files, block known malicious files, and prevent the execution of malware on endpoints; Network Security such as Security Device Management (SDM) can detect malicious files attempting to enter a network from the Internet or move within a network.

Organizations can further harden defenses by segregating higher-risk devices from their internal network (like IoT devices that are Internet facing). Administrators should ensure these devices have default passwords changed as attackers are actively searching for devices that provide them easy access into a network. Furthermore, Administrators should ensure that vendor patches are applied as soon as feasible within their environments as these critical patches can secure vulnerabilities from attackers.

Navigating cybersecurity can be difficult, but it doesn't have to be. If organizations are being challenged and unsure where to turn, Nuspire can be your partner on the digital battlefield.

**About the Nuspire Threat Report**

Throughout the past decade, Nuspire has published a wealth of definitive security and threat intelligence information for security professionals interested in the state of global cybersecurity. These comprehensive reports provided detailed accounts of threat landscapes and their organizational implications, as well as best practices to defend against the adverse impacts of data breaches.

For more information, visit www.nuspire.com.