nuspire

Q1 2022

Threat Landscape Report

nuspire.com

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

Table Of Contents

nuspire

Introduction

As we move into a new year, we've seen a slew of new vulnerabilities, although, threat actor tactics haven't changed dramatically. At Nuspire, we're still witnessing threat actors using malicious files and cashing in on newly announced vulnerabilities. Threat actors are opportunistic for the most part and seek the easiest access for the least amount of effort. We explore these ideas and cover some of the most prevalent ways we've see threat actors attempt to breach the gates. After we dig into the data, we'll provide you with actionable takeaways you can apply to your network to harden your defenses.

MALWARE

BOTNET

EXPLOIT

Summary of findings

4.76%
increase in total activity from Q4

3,418,442
Malware Events

19,971,618
Q4 Exploitation Events

3.87%
increase in total activity from Q4

12.21%
increase in total activity from Q4

812,940
Botnet Events

Methodology and Overview

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

1

GATHER

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

2

PROCESS

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

3

DETECT

Using Nuspire's cloud-based SIEM, log data is ingested and alerts the security operations center (SOC). The SOC then notifies the client and works with them to remediate the threat.

4

EVALUATE

Analysts further scrutinize the research, scoring and tracking of existing and new threats.

5

DISSEMINATE

Analysts leverage the insights to constantly improve the SOC, alerting and the community through the creation of detection rules, briefs and presentations.

Quarter in Review

February 1, 2022

New “high-priority” Linux vulnerability affects all supported Ubuntu releases

February 3, 2022

Critical vulnerabilities announced in Cisco Small Business RV Series routers

February 8, 2022

Microsoft to block Office VBA macros by default

February 9, 2022

Critical vulnerabilities affecting SAP applications employing internet communication manager (ICM)

February 24, 2022

Russian APT cyberattacks against Ukrainian assets

March 7, 2022

New Linux vulnerability gives root access on all major distributions

March 9, 2022

CISA releases advisory to patch two actively exploited Firefox zero-day attacks

March 14, 2022

Automotive giant Denso reveals ransomware attack

March 18, 2022

Russian state-sponsored threat actors exploit default MFA protocols and PrintNightmare

March 22, 2022

Okta confirms investigation into potential client breach

March 26, 2022

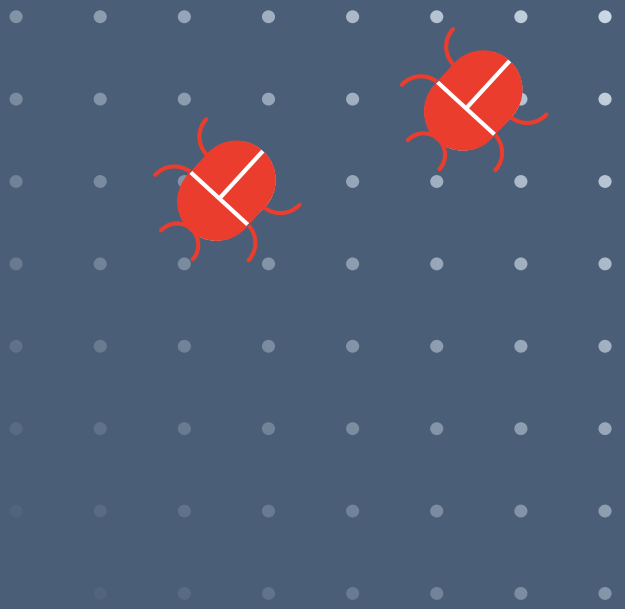
Google releases “emergency patch” for Chrome zero-day attack

March 28, 2022

Patch released for Sophos firewall vulnerability that allows remote code execution

March 31, 2022

Popular Java web app framework experiences zero-day dubbed “Spring4Shell”



Malware

3,418,442

Q1 TOTAL EVENTS

1,342

unique variants detected

284,870

detections per week

40,695

detections per day

4.76%

increase in total activity from Q4

Malware Detection

In Figure 1, average Q1 malware activity is represented in a dashed trend line. The solid line shows the true weekly numbers to help identify spikes and abnormal activity. Looking across Nuspire managed and monitored devices, there was a **4.76% increase in total malware activity** in comparison to Q4 2021, with peak activity witnessed in mid-March. Our data show VBA Agents continue to be the largest variant.

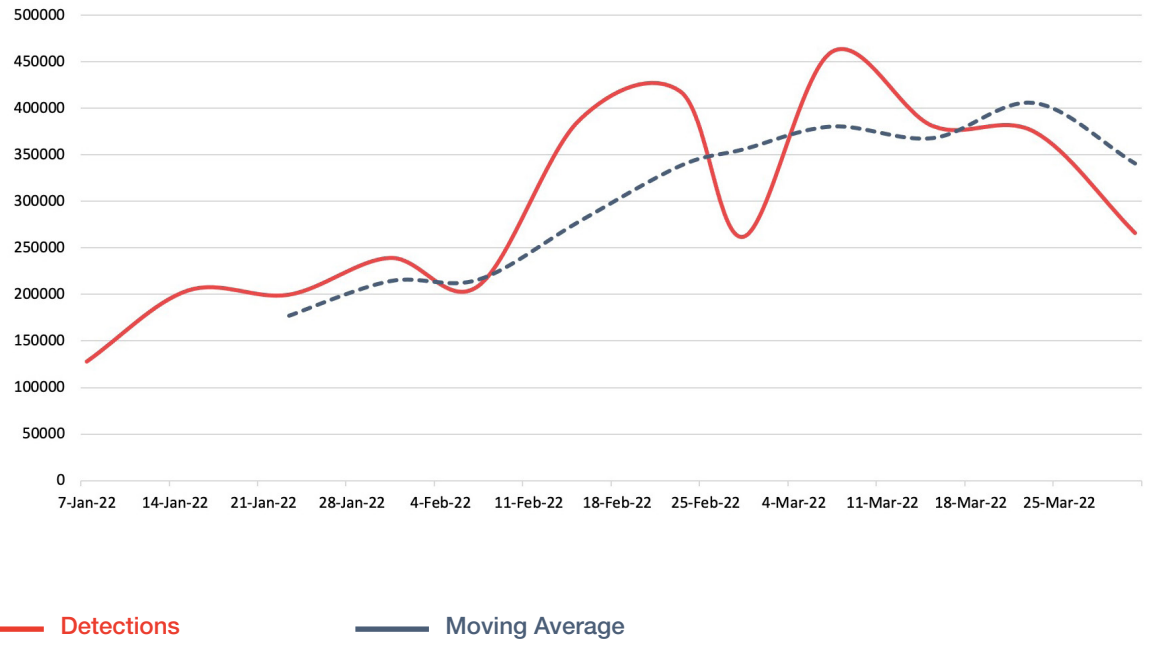


Figure 1. Malware detection
Nuspire, Q1 2022

As shown in Figure 2, the top five malware variants witnessed over Q1 were Visual Basic for Applications (VBA) Trojan variants, password-protected Microsoft Office files, JavaScript agents, malicious Excel files, and Emotet loaders. As previously seen, VBA agents continue to lead the way in malware activity. These are commonly deployed in phishing malspam campaigns and act as an initial loader for other malware families, as do all of the other
variants listed.

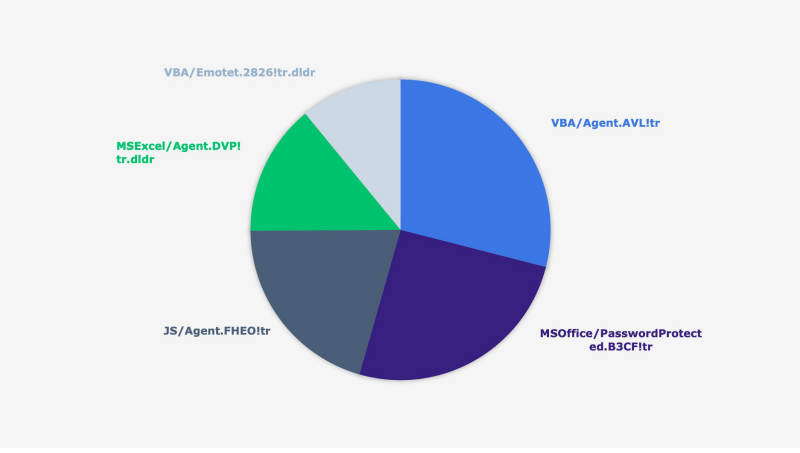


Figure 2. Top five malware variants
Nuspire, Q1 2022

VBA Agent Activity

VBA agent activity typically attributes a large percentage of Nuspire's witnessed malware activity, and during Q4, activity was on a downtrend. Except for a spike in mid-February, activity remained relatively static throughout Q1. Microsoft's announcement around blocking VBA macros by default on Office products will likely cripple this attack vector. The rollout of these changes begins in early April 2022, so we will not see the effects until next quarter.

Threat actors are aware of the changes as well. This likely attributes to why activity is stagnant and should continue to decrease over time as they phase these attacks out. Numerous ransomware groups and advanced persistent threat (APT) groups utilize malicious attachments as an initial infection vector against organizations. With it becoming more difficult for threat actors to leverage these types of attacks, we would expect to see an increase in activity from other variants such as JavaScript loaders and malicious PDFs.

VBA agents operate by imitating legitimate 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 server to download an additional payload on the victim machine, which may contain ransomware or other advanced malware.

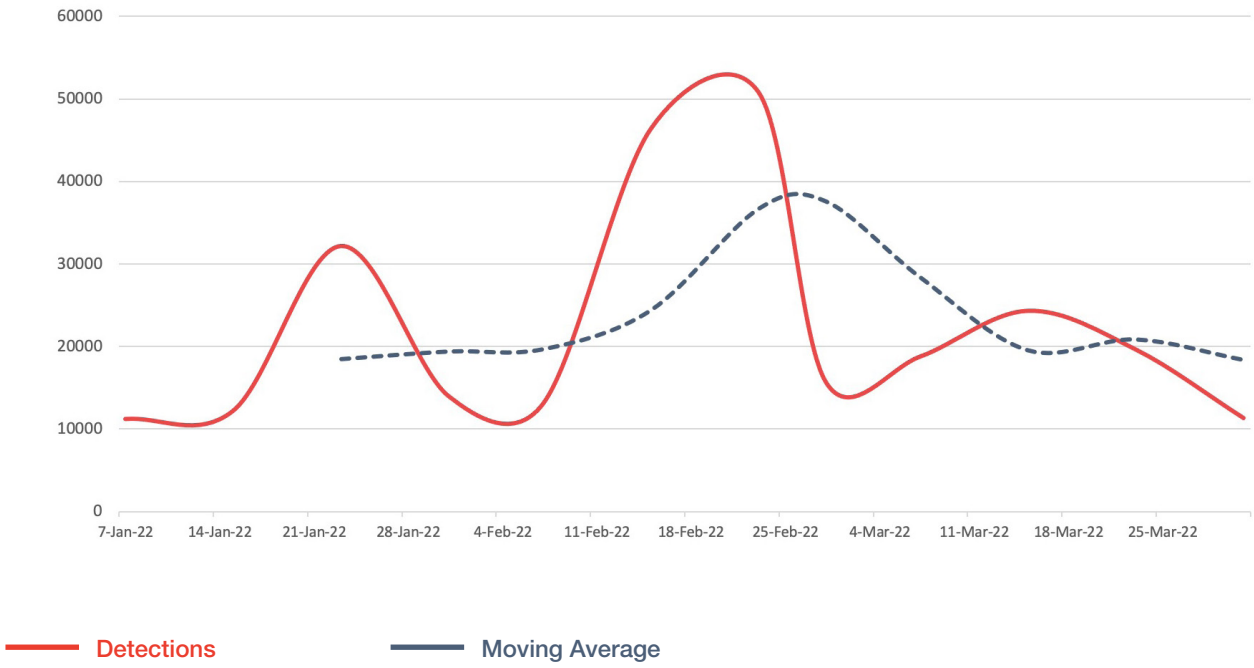


Figure 3. VBA Agent Activity
Nuspire, Q1 2022

JavaScript Agents

JavaScript agents are a type of malware loader that typically deploy via drive-by download. When a user visits either a legitimate website that has been compromised or a malicious site, a payload is silently downloaded and installed on the victim machine, giving the threat actors access. These loaders can additionally be packaged up with the appearance of a legitimate email attachment and deployed during malicious spam campaigns. Once on the victim machine, the loaders typically reach out to a command-and-control server to download and install additional malware. These are utilized by numerous malware families and threat actors, including the STRRAT botnet discussed in the botnet section below.

Of note is the timing of the activity spike in mid-February, which is closely related to the announcement of Microsoft blocking VBA macros by default as discussed in the previous section. This may show threat actors are testing and adapting to different attack vectors as the popular VBA agent loses efficacy. Additionally, this activity aligns with a spike in activity from the STRRAT botnet, which may indicate this spike was the launching of their campaign. Throughout the quarter, average activity increased. If threat actors and malware families are indeed branching into other types of loaders and begin avoiding VBA agents, we would expect to see JavaScript activity continue to increase.

Figure 4. JavaScript Activity
Nuspire, Q1 2022

How to Combat

Proactive Detection and Mitigation Measures

Endpoint Protection Platforms (EPP)

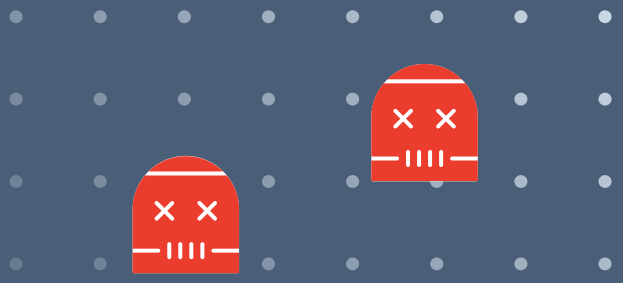
Implement security in-depth while utilizing advanced, next-generation antivirus (NGAV). NGAV will detect malicious software not only through signatures, but also through heuristics and behavior analysis detecting suspicious behavior and stopping it in its tracks. Legacy AV is typically only signature-based.

Network Segregation

Higher risk internet of things (IoT) devices that are exposed increase your network's vulnerability. Segregate these devices behind a DMZ to minimize lateral movement of an attacker or spread of ransomware in case of infection.

Cybersecurity Awareness Training

Cybersecurity Awareness Training is often overlooked in a security program and should be a prioritized element. An organization that can from top to bottom detect phishing and suspicious attachments, and knows how to report these events within their company, can help prevent an infection or a ransomware attack from happening.



Botnets
812,940

Q1 TOTAL EVENTS

45

unique variants detected

67,745

detections per week

9,677

detections per day

12.21%

increase in total activity from Q4

Botnet Detection

Figure 5 below shows a moving average of botnet activity throughout Q1 as a dashed line, whereas the solid line illustrates the true weekly numbers to help identify spikes and abnormal activity. When compared against Q4 2021, Nuspire witnessed a 12.21% increase in botnet activity. The increase can be mostly attributed to the STRRAT botnet's rise in activity throughout Q1.

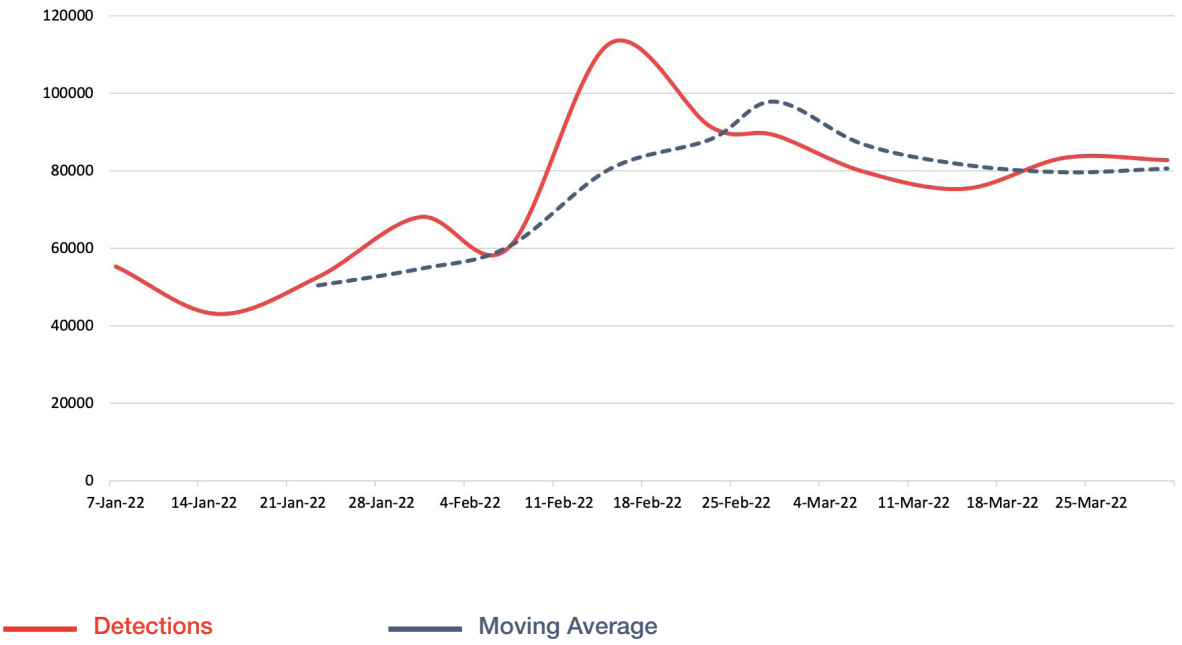


Figure 5. Botnet infections
Nuspire, Q1 2022

Figure 6 shows the top observed botnets during Q1 2022.

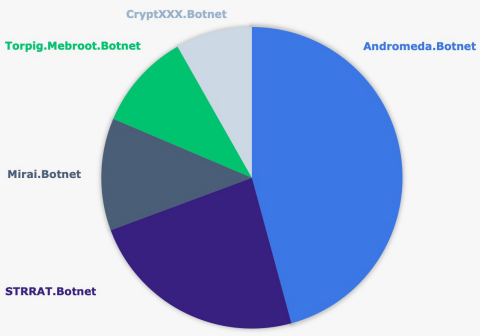


Figure 6. Top Five Botnets
Nuspire, Q1 2022

STRRAT Botnet

STRRAT malware contains multiple capabilities such as information stealing, keystroke logging, and credential harvesting from browsers and email clients. It is typically deployed via phishing campaigns and uses JavaScript agents and malicious Microsoft Excel files with embedded macros. Near the end of January, **Fortinet's FortiGuard Labs announced** the identification of a new STRRAT phishing campaign. Shortly after, Nuspire began to witness a significant increase in STRRAT activity.

Threat actors use numerous lures to try to get their victims to engage with their malicious payload. One common theme seen in the campaign was emails about shipping and logistics. Threat actors ultimately look to entice users with anything that will pique their curiosity or subject matter that elicits urgency or punishment. This time of year, another extremely common theme is the U.S. tax season and notifications from the IRS or popular tax software.

Figure 7. STRRAT Botnet Activity
Nuspire, Q1 2022

Mirai Botnet

Mirai malware is a notorious group that typically seeks out IoT devices to add to their botnet. Historically, Mirai botnet has been used to launch distributed denial of service (DDoS) attacks to overwhelm and deny access to internet services or cripple an organization's ability to function. They scan the internet searching for exposed devices and will employ common and known vulnerabilities to exploit the device's firmware, or if a login is exposed, attempt to bruteforce it to gain access. Mirai's source code has been used to spawn numerous other malware families.

Near the end of Q1, a zero day attack was discovered dubbed "Spring4Shell" (CVE-2022-22965). Shortly after, reports came from the threat intelligence community that Mirai was witnessed exploiting this vulnerability almost immediately to add additional devices to its botnet. Because IoT devices can easily be deployed and forgotten about, there will likely be increases in Mirai activity throughout Q2 as these threat actors continue to exploit unpatched devices.

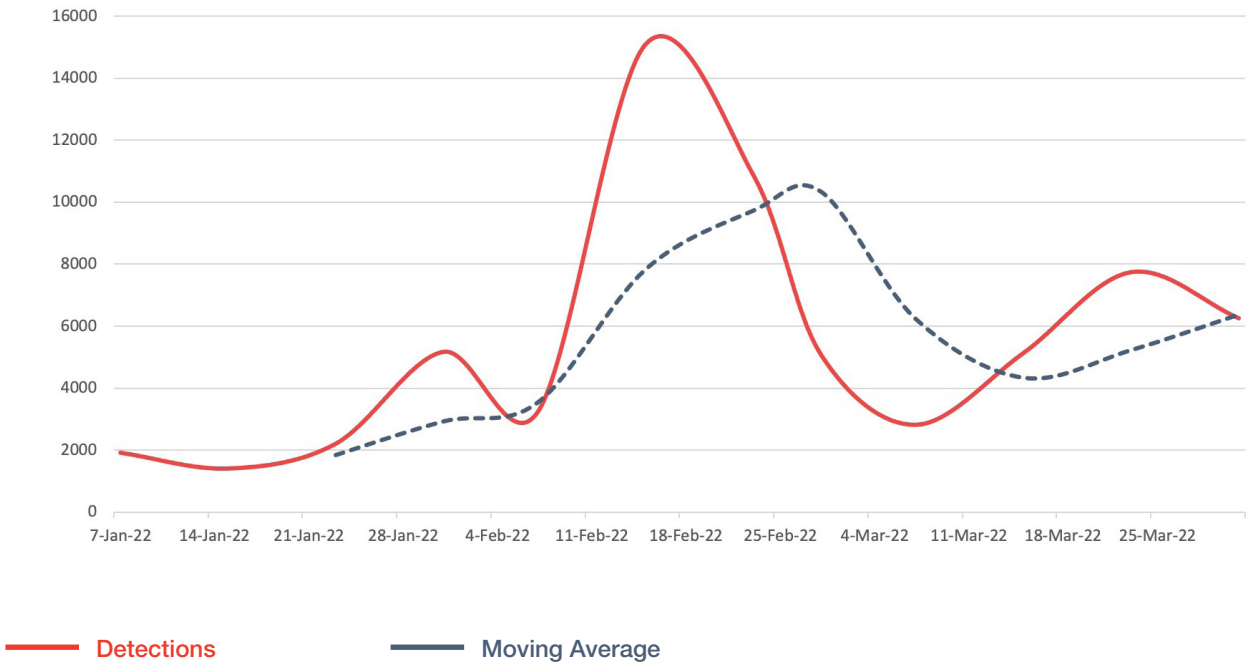


Figure 8. Mirai Botnet Activity
Nuspire, Q1 2022

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

How to Combat

Proactive Detection and Mitigation Measures

Leverage Threat Intelligence

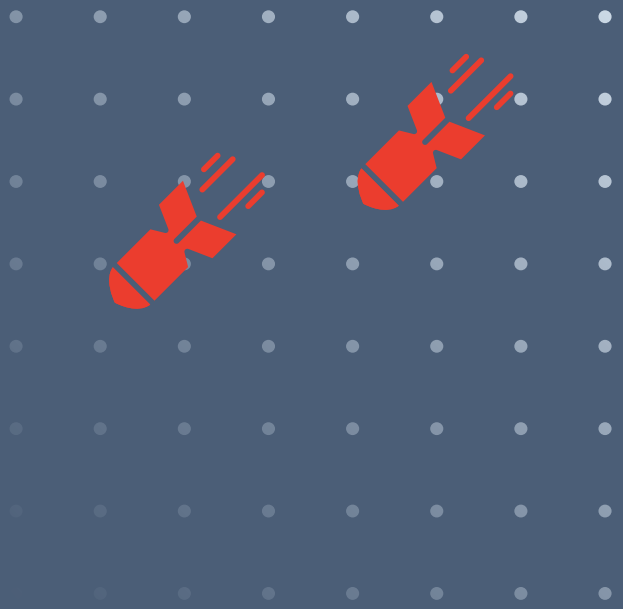
Threat intelligence provides insight on botnet command-and-control infrastructure, alerting you when your organization is communicating with things it should not be. Botnet communications happen after infection when the device attempts to reach out and communicate. Knowing when that network traffic is headed to a malicious destination allows you to take action.

Use Next-Generation Antivirus

Since botnet communications happen after infection, the best case is to prevent the infection to begin with. Using next-generation AV goes beyond signature-based, legacy AV, using behavior analysis to detect when malicious activity is happening on your devices.

Threat Hunt

New command-and-control infrastructure is created daily and may not be publicly known yet. Threat hunt within your environment for abnormal activity. Ask questions about why systems are doing things and if they should be. If not, dig deeper to determine if activity is malicious or not.



Exploits
19,971,618

Q1 TOTAL EVENTS

639

unique variants detected

1,664,301

detections per week

237,757

detections per day

3.87%

increase in total activity from Q4

Exploit Detection

Figure 9 below shows a moving average of exploit activity throughout Q1 as a dashed line, whereas the solid line illustrates the true weekly numbers to help identify spikes and abnormal activity. Witnessed exploitation activity versus Q4 2021 **shows a 3.87% increase**. Threat actors remain focused on newly announced vulnerabilities, especially with remote code execution capability, and exposed services.

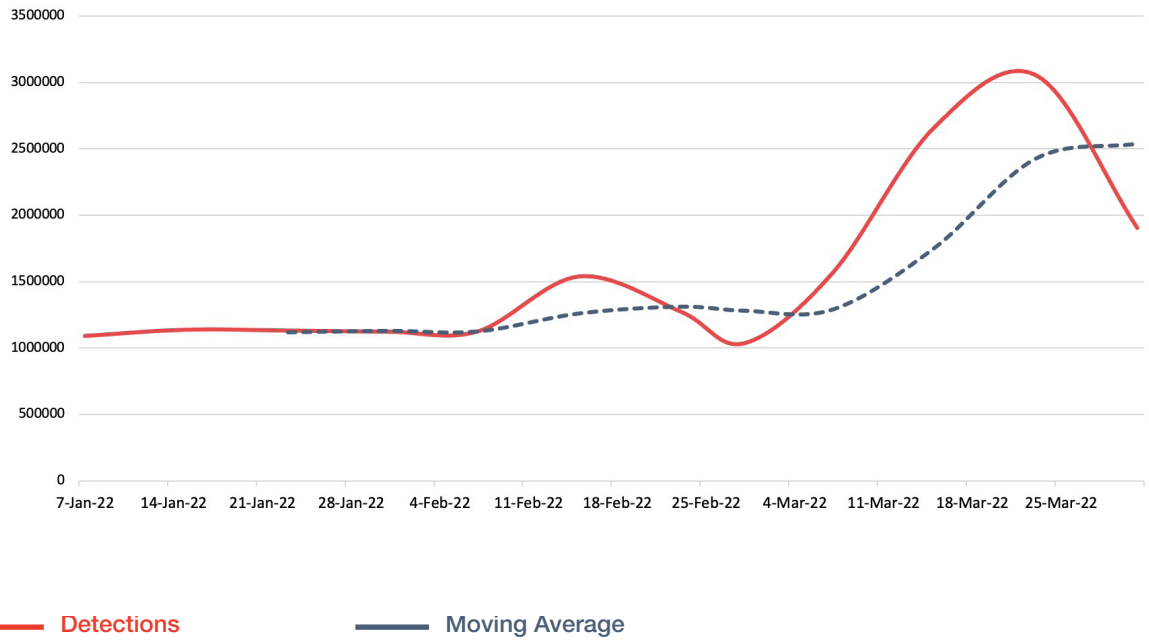


Figure 9. Q1 Exploit Activity
Nuspire, Q1 2022

While reviewing all exploit attempts during Q1, SMB Brute Force (47.89%), SSH Brute Force (29.66%), Apache Log4j (8.83%), HTTP Directory Traversal (6.00%), and DoublePulsar (4.30%) consisted of the top five most witnessed attempts.

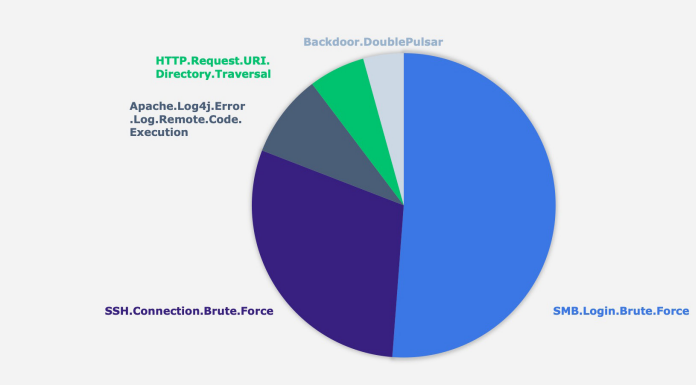


Figure 10. Q1 Top Witnessed Exploits
Nuspire, Q1 2022

Bruteforce Attacks

Bruteforcing remains dominant as we close out Q1 and likely will remain a prevalent attack vector if provided to threat actors. Threat actors are consistently scanning for exposed services such as SMB and SSH, and if found, will immediately attempt to gain access. In addition to bruteforcing, threat actors will also leverage known and recently announced vulnerabilities against these exposed services to gain access. As of writing Shodan detected **over 1,300,000 exposed SMB ports** and **over 22,000,000 exposed SSH ports**, with the highest concentration within the United States.

It is critical that organizations understand their digital footprint and what services are exposed. Administrators should secure access behind a VPN or disable the services completely if not used. If the service must be exposed, administrators need to prioritize patching and ensure login attempts are locked out with subsequent failures. These exposed services are a prime target for threat actors.

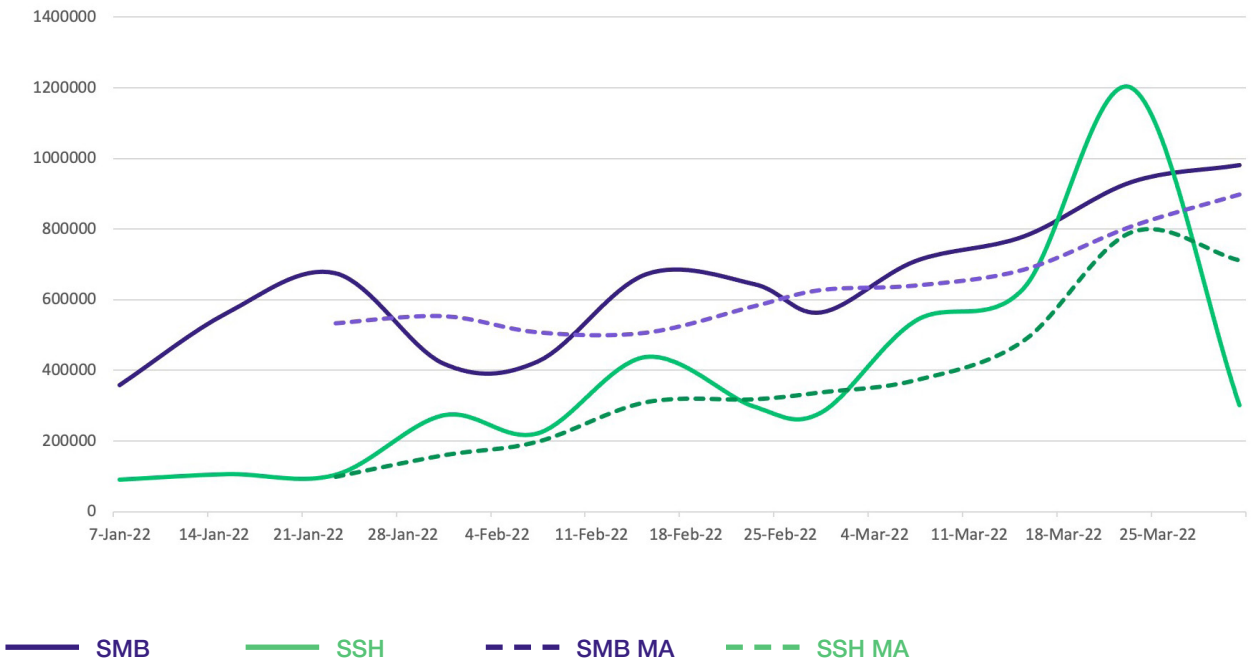


Figure 11. Q1 Bruteforcing Attempts
Nuspire, Q1 2022

Apache Log4j

Announced in December 2021, this vulnerability shook organizations worldwide and threat actors immediately began to launch attacks against it. As an open-source product provided by Apache Software Foundation, it is used in numerous programs and technologies. When a widely used software has a critical vulnerability, it provides threat actors many opportunities to attack. Activity throughout Q1 maintained relatively busy compared to other attempts, showing this exploit has become part of threat actors' toolkits. When compared against December 2021, we've witnessed overall activity against this vulnerability decrease. Regardless of the decrease, this likely will remain a highly attempted exploit and continue to be prominent within datasets.

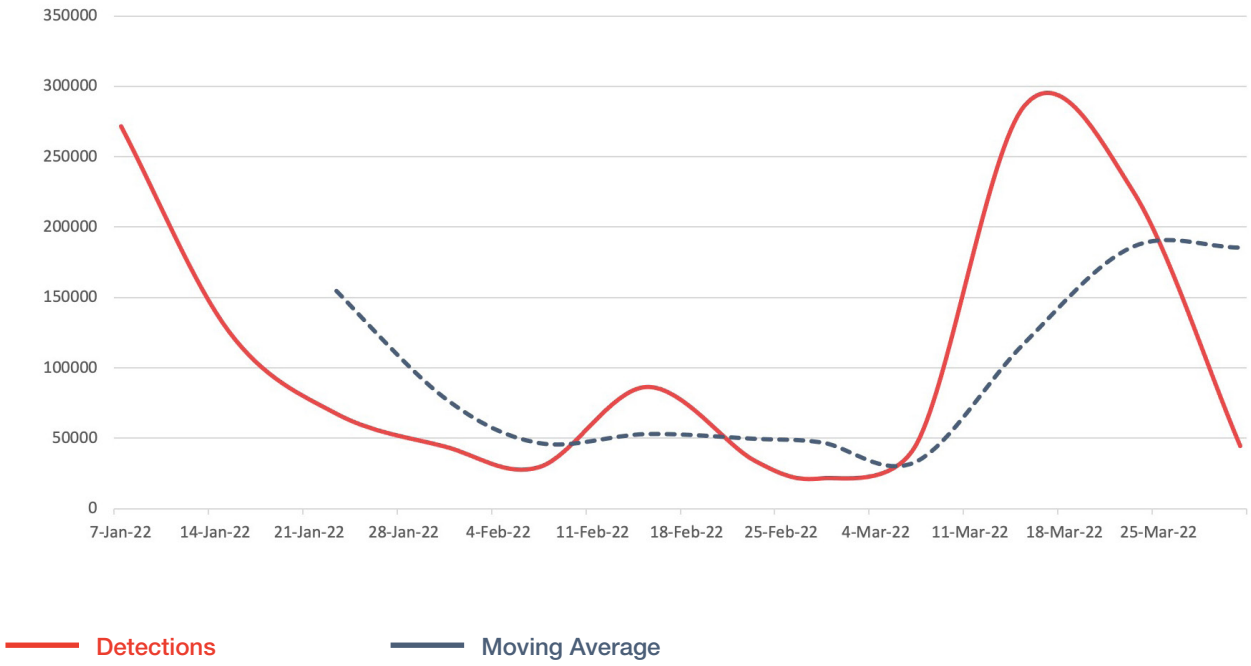


Figure 12. Q1 Log4j Attempts
Nuspire, Q1 2022

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

How to Combat

Proactive Detection and Mitigation Measures

Patch your systems ASAP

Threat actors are actively hunting for organizations that have not applied patches to their systems and technology. Organizations must understand their technology stack and focus efforts on quickly applying patches/mitigations when available. The highest priority should be applied for high- and critical-rated vulnerabilities, especially those involving remote access, as they are particularly attractive to malicious groups.

Use a Firewall with IPS

Having a firewall installed with an intrusion prevention system can provide networks a layer of security by detecting and blocking exploitation attempts. Ensure you keep your signature up to date as provided from your security vendor to thwart the latest attacks.

Monitor Security News and Vendor Security Bulletins

If you do not know about a new vulnerability, you cannot protect against it. Most vendors have security bulletins to which you can subscribe. These provide your organization with critical patching and mitigation information. Subscribe to and monitor those postings to keep up to date.

Disable Unused Services

If your systems do not need a particular service to be running, disable it! Services can introduce additional vulnerabilities to your organization, and if you are not using it, there is no need to introduce that additional attack vector. Additionally, organizations should be aware of what services they have exposed to the internet and secure them behind VPN technology.

Industry Spotlight: Automotive

The automotive industry is a diverse field where manufacturing, operations and sales all blend, offering threat actors multiple vectors of attack. From headquarters to manufacturing plants, distribution centers and dealerships, each location can have different technologies and its own unique challenges. Multiple threat actor groups and advanced persistent threat groups have placed a target on the automotive industry due to its intellectual property and client data. In this section, we'll explore some of these threat actors and their primary ways of launching an attack, along with a historical case study.

Ransomware Gangs

No industry is immune to ransomware attacks, and it remains the most serious threat organizations face today. The majority of threat actors have one motive: financial gain. Threat actors realize if they can break their way into an automotive dealership or a manufacturing plant, they can cripple sales and operational time. Because of this added financial pressure on an organization, these ransomware gangs are hoping the victim will quickly pay out to restore operations.

One of the most prevalent ransomware gangs as of writing is **Conti Ransomware**. The Cybersecurity & Infrastructure Security Agency (CISA) has released numerous **notifications and alerts** regarding this gang. Once Conti gains access to an organization, they will exfiltrate data, encrypt a network and publish the data on their extortion site if the ransom isn't paid. Conti uses multiple ways to gain access to a network, including:

- Spearphishing campaigns that often leverage malicious Microsoft Office documents. They typically install Cobalt Strike, TrickBot or IcedID malware.
- Bruteforcing exposed remote desktop protocol or using stolen credentials to gain access.
- Deploying fake software "updates" that are actually malware. They promote these "updates" through search engine optimization (SEO).
- Exploiting newly announced and common vulnerabilities on exposed/external assets.

Conti Ransomware isn't unique in these tactics. Numerous threat actors use these methods because they're typically looking for the easiest level of effort to access an organization. CISA has stated that **more than 90%** of successful cyberattacks start with a phishing email.

Mofang (Superman)

Mofang is a Chinese-based cyber-espionage group operating since at least 2012. Their motives typically align with intellectual property theft, and they focus their attacks on organizations of interest to the Chinese government that may impact their financial sector. Mofang has previously launched known attacks against at least two German companies within the automotive industry. Mofang's methods have historically been limited to social engineering to gain entrance to a network:

- Utilizes specifically crafted spearphishing emails containing a Microsoft Office file or malicious PDF.
- If executed, the payload downloads a remote access trojan and reconnaissance begins to find data they value.

Case Study:

Ransomware Attack

Situation

In 2020, it was announced that a large automotive company fell victim to a ransomware attack on their industrial control system (ICS), which caused operational outages. While it is publicly unknown how the initial entry into the network happened, what can be learned from the situation is regarding network segmentation. Due to a lack of network segmentation, the ransomware was able to spread between departments and impact more of the organization.

Lessons Learned

Segment your network and operations to prevent lateral movement in the event of infection. Minimizing the spread may save your organization critical downtime and prevent multi-site impact.

Conclusion and Recommendations

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

The following are five simple actions

security leaders can take to safeguard their organization and reduce risk of breach.

1 EDUCATE ALL USERS, OFTEN

User awareness is one of the most powerful and cost-effective ways to defend your organization from a cyberattack. Educate your end users on how to identify suspicious attachments, social engineering and scams in circulation. Inform them on common theming, including any major events that could be created into a phishing lure. 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. Often once an attacker has compromised an email account, they 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 will not secure your business. A comprehensive ‘defense in depth’ approach with an integrated zero trust cybersecurity program protects businesses by ensuring that every single cybersecurity product has a backup. Integrating defense components counters any gaps in other defenses of security. Utilize vulnerability scanning to determine your weak spots and build your security around them. Enrich your logs with threat intelligence and perform threat modeling on your organization to determine how APT groups are targeting your industry vertical.

3 UP YOUR MALWARE PROTECTION

Advanced malware detection and protection technology (such as endpoint protection and response solutions) can track unknown files, block known malicious files and prevent the execution of malware on endpoints. Network security solutions, such as secure device management, can detect malicious files attempting to enter a network from the internet or laterally moving within a network. This advanced protection can provide threat responders additional tools like quarantining a specific device on the network and deep visibility into events happening on a device during investigations.

4 SEGREGATE HIGHER-RISK DEVICES FROM YOUR INTERNAL NETWORK

Devices that are internet-facing are high-value targets. Administrators should make sure to change the default passwords on these devices, as attackers are actively searching for devices that provide them easy access into a network. IoT devices should be inventoried, and a full understanding of your digital footprint is critical. Network segregation can help limit where an attacker can laterally move within an environment in the event of a breach.

5 PATCH, PATCH, AND THEN PATCH SOME MORE

Administrators should ensure that vendor patches are applied as soon as feasible within their environments. These critical patches can secure vulnerabilities from attackers. Administrators need to monitor security bulletins from their technology stack vendors to stay on top of newly discovered vulnerabilities attackers may exploit.

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

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

About Nuspire

Nuspire is a leading managed security services provider (MSSP) that is revolutionizing the cybersecurity experience by taking an optimistic and people first approach. Our deep bench of cybersecurity experts, world-class threat intelligence and 24x7 security operations centers (SOCs) detect, respond and remediate advanced cyber threats. We offer comprehensive services that combine award-winning threat detection with superior response capabilities to provide end-to-end protection across the gateway, network and endpoint ecosystem. Our client base spans thousands of enterprises of all sizes, across multiple industries, and achieves the greatest risk reduction per cyber-dollar spent. At Nuspire, we are laser focused on delivering an extraordinary cybersecurity experience that exceeds client expectations.

For more information, visit nuspire.com and follow us on LinkedIn @Nuspire.

nuspire.com
LinkedIn @Nuspire
Twitter @NuspireNetworks