WatchGuard®

# INTERNET SECURITY REPORT

Quarter 3, 2022

# Contents

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

***"To ... not prepare is the greatest of crimes; to be prepared beforehand for any contingency is the greatest of virtues."***

– Sun Tzu

***"No plan survives the first contact with the enemy"***

– A Prussian General

***"Everyone has a plan until they get punched in the mouth"***

– Mike Tyson

We've all seen or read various heist/special forces/war fiction where some specialized group of experts comes together to plan something big, but then the most experienced of the crew snickers sarcastically, and shares some version of the quote, "humans plan, God laughs." Ultimately, the point being that plan A almost never works perfectly because threat actors can also adjust. Any smart planner knows they must plan for contingencies as well, depending on what their adversary does in response. Of course, you need current knowledge and understanding of your adversary to plan for those contingencies.

That's what this Internet Security Report is about. Our goal is to give you a fresh briefing on the current tactics of cybercriminals so that you can properly plan or adjust your defenses, including real-time updates for contingencies — it's as simple as that. Why get punched in the mouth at all, if we can tell you how the enemy throws punches in the first place? Using threat intelligence delivered from tens of thousands of network security appliances and millions of clients, our security analysts will share the latest tactics of cyber adversaries so that you can update your plan before you have to encounter them.

## Our Q3 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 attacks and threatening domains we blocked during Q3, including details about the most-widespread attacks, and regional differences. Highlights from Q2 include a continued overall decline in network and malware attacks, more evidence of Emotet resurgence, and hints of state-sponsored malware.

### 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 through and various malware trends, such as whether ransomware and cryptominers have increased or decreased. This quarter we go into a bit more detail around the latest ransomware groups, which the Threat Lab has been tracking for the last few quarters.

### 31 Top Incident – EvilProxy:

Every quarter we include a section that either shares the results of the latest research project from the WatchGuard Threat Lab or covers a widespread security story or issue from the quarter. This quarter, we cover the story of EvilProxy, an attacker-in-the-middle (AitM) framework designed to make it easier for threat actors to socially engineer victims past multi-factor authentication (MFA) checkpoints, using techniques like "push bombing." More smart companies are deploying MFA throughout their organizations, which is a great thing. However, these sorts of social engineering techniques could weaken otherwise good protection. This section covers how EvilProxy and push bombing work, and how you can protect your users.

### 36 Update security plans to improve your defenses:

As mentioned in the intro, we don't want you punched in the mouth by some malicious cyber threat. The only reason we share these adversary threat trends is to help you come up with better defenses and plans to defeat them. Throughout the report, we share valuable security tips that can help you defeat the tactics we see attackers evolve every quarter.

# Executive Summary

Yet again, both malware and network attacks decreased during Q3 2022, extending a trend we haven't seen in years past. Sure, one or the other has gone up or down here and there quarter to quarter, but we haven't seen both decline this consistently for such a sustained period. Now we have seen three quarters of mostly declining volume, which is technically great news for defenders, but unexpected compared to historical results. However, we don't believe that means we are all completely safe. There are more subtle trends, lurking below the surface, which  suggest that the sophistication and potential impact of the threats we do see is increasing, despite less overall volume. And as you will soon learn, we have some reason to believe this decreasing volume may be deceiving.

For example, we continue to see most malware arriving over encrypted connections. If attackers know that most defenders aren't scanning encrypted traffic – which is the case for four-fifths of Firebox users – it doesn't take high volume for attacks to succeed. Meanwhile, while the total volume of evasive – or what we've coined zero day malware – has declined, 50 percent is still far too much, and when you look at encrypted traffic, that zero day malware number increases even more.

This increase in sophistication proves out even when we analyze the malware variants that do show up in our top lists. For instance, in Q3 we saw the first threat that we can strongly tie to a state-sponsored (government) threat actor. We have seen threats that might have been government actors before but were sometimes also used by vanilla criminals, and we couldn't say for sure. However, this quarter one of the most-widespread threats out there is only tied to a threat group associated with the Chinese government.

Finally, we did have one preliminary finding that offers a potential hypothesis for why our malware volume appears to be low. There is a chance it's actually much higher than our existing data suggests. Rather, the problem may be that not enough defenders are using the free and more advanced Firebox features necessary to catch modern malware. We detail this more in the report, but in short, we know that when a Firebox is configured to scan encrypted web traffic, most malware (over 80 percent) arrives over that encrypted connection. That said, we also know that only around 20 percent of reporting Fireboxes are configured to scan encrypted traffic. As mentioned, threat actors are increasingly transitioning to more sophisticated and evasive threat tactics, including encrypted network delivery since they likely know many defenders don't scan that kind of traffic. That means we will see less and less of that malware until those Firebox owners start to configure TLS/SSL inspection (which is a free feature with every Firebox). Unfortunately, it also means not only do we potentially not see the true volume of malware due to this missing encrypted traffic, but those defenders not decrypting are also missing an opportunity to block it, and may be receiving that malware unless other endpoint-based protections kick in. The point is, malware volume may be much higher than it seems from the data we currently get, and the owners of 80% of the reporting Fireboxes really need to enable HTTPS inspection, not necessarily to improve this report's visibility, but for their own protection.

In summary, the lowering threat volumes is interesting but not bad news for defenders. However, it also may not be entirely accurate, and just a case of user configurations not keeping up with the today's encrypted times. In either case, don't let it lull you into a sense of comfort. We still see many dangerous threats out there, and the ones we do see can get past less mature defenses.

**Below, we share some additional executive highlights from this Q3 2022 report:**

- **Network-based malware detections dropped ~4.4% percent quarter over quarter (QoQ)** during Q3. We saw a slight increase in the basic malware detected by our Gateway AntiVirus (GAV) service (~12.4 million detections) but a large decrease in evasive or zero day malware detected by advanced anti-malware services like APT Blocker (~4.9 million detections).

- **Emotet continues to haunt many networks.** Despite the FBI and global authorities' takedown of one Emotet variant's command and control (C2) infrastructure early last year, we continue to see new variants hit our top malware lists. In Q3, it topped our most-widespread malware list and placed ninth for top malware volume.

- **82% of malware hides behind encryption!** We continue to warn that most malware likes to hide in the SSL/TLS encryption used by secured websites for the past few years. Q3 continues that trend with a slight bump up. If you don't inspect this traffic, you are missing most malware – at least with your network security controls (the endpoint does still have a chance to catch it).

- **Administrators' lack of TLS/SSL inspection hides the true malware story.** As hinted in the intro, this report will share findings that have us starting to believe what we see in the normal top ten may not offer a completely accurate picture of malware trends, because so few Firebox users seem to scan encrypted traffic. Meanwhile, the Fireboxes that do scan encrypted traffic seem to have a better view of where most malware is headed and the real trends. We think you should pay closer attention to our encrypted malware lists going forward, not just the normal top 10 list.

- **Zero day malware seems to be decreasing but still remains at around 50%.** Even if it is decreasing, it is not good that around half of malware bypasses signature-based detection. However, the number may also not show the complete picture because **when you look at encrypted traffic, zero day malware rises to 72%.** As mentioned above, perhaps zero day malware hasn't decreased, it's just more of our users miss it because they fall into the ~80% of administrators that aren't decrypting HTTPS traffic for malware scanning.

- **Malicious Microsoft Office documents (Word, Excel, RTF) remain a popular malware delivery vector.** From a network detection standpoint (the endpoint sees slightly different results) many of the top malware threats arrive as Office documents leveraging well-known (and patched) vulnerabilities.

- **Network attack volume dropped drastically (46%)** QoQ, continuing its third quarter of a downward trend after Q4's four-year high. That said, it did hit an all-time high during Q4 of last year. We can only wait and see if this year's holiday season will break this downward trend and return to the higher number we saw at the end of last year.

- On average, **Fireboxes blocked ~28 network attacks per appliance,** which is also close to a 50% decrease since last quarter. We don't have enough data to know why for sure, but like malware, exploits can happen via encrypted web traffic, and most of our IPS detection comes from web-based attacks. So perhaps it is not decreasing as much as it seems. As above, we hypothesize we just can't see some of the network attacks because most admins aren't decrypting and scanning HTTPS traffic.

- **Endpoint malware detections are down ~8%.** Whether detected from network or endpoint, malware attacks were down overall in Q3 2022.

- However, **ransomware rose in Q3, nearing Q1 2022's record high.** Lockbit was by far our most detected ransomware variant last quarter. We also spend some time in this report highlighting 23 ransomware groups our Threat Lab team is tracking.

- Meanwhile, **malicious cryptocurrency miners dropped 72%**, which we presume has to do with the drastic dive the general cryptocurrency market has taken the past few quarters.

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

# Firebox Feed Statistics

## What Is the Firebox Feed?

Each quarter we gather and analyze anonymized data in the Firebox Feed from devices around the world, allowing us to identify cyberattack trends targeting small and midsize organizations. Some of the trends we review include the top threats in each region to watch out for as well as the most wide-spread threats that you will likely encounter. Every report, we try to take fresh look at the ways we analyze the Firebox Feed data and find more detail we can add to the report.

We recently added details allowing us to not only tell you the threats, but also how the threats spread. In this section, we review malware and network attacks arriving both over unencrypted and encrypted connection.  This includes threats detected with the signature-based Gateway AntiVirus (GAV) service, behavioral detection APT Blocker, and the Intrusion Prevention Service (IPS) all running on Firebox appliances worldwide. Additionally, we review malicious domains that the DNS firewalling service, DNSWatch, identified and protected would-be-victims from visiting.

This type of data can become meaningless without context. By adding context and charts we provide our own understanding of the data to highlight threat trends that organizations have faced and will continue to face. We hope business leadership, IT, MSPs, and others can better protect their networks with this information.

- **Gateway AntiVirus (GAV):** Signature-based malware detection
- **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

If you allow it, our network security appliances, or Fireboxes, provide anonymized threat intelligence from their enabled network security services, including the multiple malware scanning engines they can deploy. We gather and analyze this data to identify malware trends that help you better understand the types and amounts of malware on the Internet. This current and historical data allows us to try to forecast upcoming malware trends for you to defend against. While we don't get it right all the time, we have accurately predicted the continuation of Emotet as well as the growth in more advanced malware that signature-based detection tends to miss. Let's go over some highlights from last quarter's data.

In Q3, we saw Emotet targeting Japan yet again, but also spreading to other countries. As a reminder, Emotet disappeared for a bit when authorities took down one cybercriminal group's command and control (C2) infrastructure, but we predicted new variants would resurface, which proved correct. In Q2, we didn't see new malware in our top 10, but we did find four new malware variants in the top 10 in Q3. We cover some of these malware families later in this section and found these malware families quite interesting.

Overall malware detections have dropped slightly but malware over TLS has doubled. This continues a trend of more malware detected over encrypted connections. Before we look at the details of this trend let's investigate the overall totals.

With few exceptions, we see malware authors moving to create more advance 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.

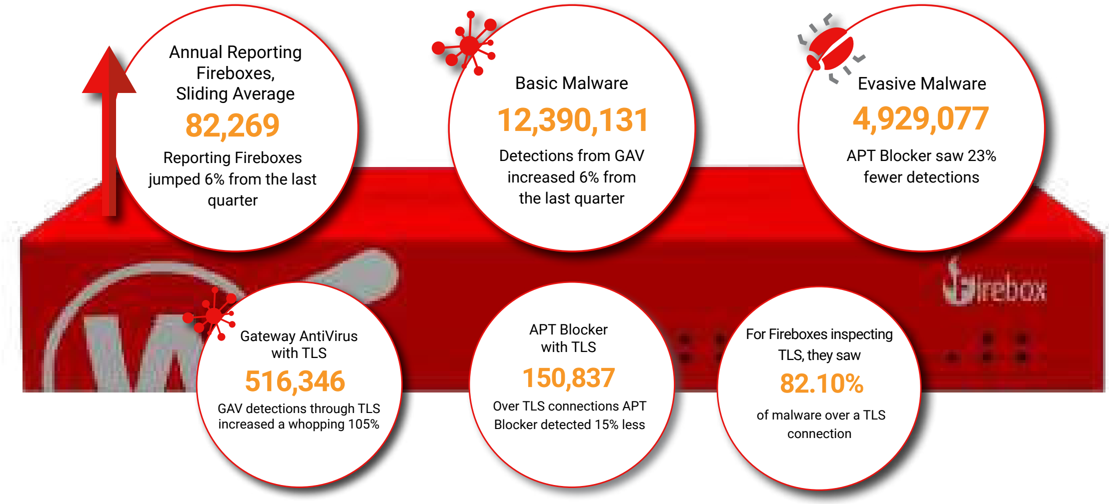
If a GAV signature doesn't exist, **IntelligentAV (IAV)** inspects the file using machine learning to identify any suspicious areas of a file.

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***



Annual Reporting Fireboxes, Sliding Average
82,269
Reporting Fireboxes jumped 6% from the last quarter

Basic Malware
12,390,131
Detections from GAV increased 6% from the last quarter

Evasive Malware
4,929,077
APT Blocker saw 23% fewer detections

Gateway AntiVirus with TLS
516,346
GAV detections through TLS increased a whopping 105%

APT Blocker with TLS
150,837
Over TLS connections APT Blocker detected 15% less

For Fireboxes inspecting TLS, they saw
82.10%
of malware over a TLS connection

## Top 10 Gateway AntiVirus (GAV) Malware Detections

We first look at malware by pure volume with our Top 10 Malware table. The malware families in this table make up a large portion of the total malware our devices see online. We occasionally get malware where only a few devices detect much of the total, which is why we complement this table with other tables like our Top 5 Widespread table, to provide a fuller picture.

Technically, we saw four new malware variants in our top 10 this quarter, though two of them, Agent.IIQ and Goooboor, made a previously appearance in the top 10 a year ago. We already detailed Goooboor in our **Q3 2021 report** and also mentioned Agent.IIQ in **Q2 2021**, so we won't recap them here. If you are interested in those variants, we encourage you to read the previous report. The third new variant was a dropper called Variant.Fugrafa, which loads different malware and game cheat engines. We saw this sample detected mostly in the US, and investigated it in more detail, which we'll cover later in this section. We also analyzed the fourth new sample, Agent.FZUW, which turned out to be part of Racoon Stealer, a cryptocurrency stealer that primarily infects users by pretending to be cracked software.

As far as trends in malware that remained on the top 10 from Q2, Trojan.Abracadabra (which is an Emotet variant) detections dropped, moving it from third to ninth in Q3's top 10. Like Q2, we still primarily see it effecting Japan, but this quarter we saw it starting to effect Europe, the Middle East, and Africa (EMEA).

**Top 10 Gateway AntiVirus Malware**

| COUNT | | THREAT NAME | CATEGORY | LAST SEEN |
|---|---|---|---|---|
| 797,133 | ● | Win32/Heri | Win Code Injection | Q2 2022 |
| 421,473 | ● | Ursu | Dropper | Q2 2022 |
| 334,972 | ● | Agent.IIQ | Dropper | New* |
| 304,244 | ● | Exploit.RTF-ObfsStrm | Office Exploit | Q3 2020 |
| 300,157 | ● | Trojan.GenericKD | Win Code Injection | Q4 2021 |
| 291,574 | ● | MSIL.Mensa | Dropper | Q2 2022 |
| 282,723 | ● | Grooboor | Office Exploit | New** |
| 231,186 | ● | Variant.Fugrafa | Dropper | New |
| 226,567 | ● | Trojan.Abracadabra (Emotet) | Win Code Injection | Q2 2022 |
| 192,147 | ● | Agent.FZUW<br>(Racoon Stealer) | Win Code Injection | New |

*Figure 1: Top 10 Gateway AntiVirus Malware Detections*

*2021 Q2 top 5 encrypted

** 2021 Q3

## Top 5 Encrypted Malware Detections

As always, we also track the volume and differences in malware that arrive over encrypted connections (primarily HTTPS), as many users do not take the time to configure their devices for TLS/SSL inspection (only one in five Fireboxes do), despite it being a free feature with all Fireboxes and our repeated recommendations that you should. In Q3, if a Firebox was inspecting encrypted traffic, 82% of the malware it detected was through that encrypted connection, leaving only a meager 18% detected without encryption. If you are not inspecting encrypted traffic on your Firebox, it's very likely that this average ratio remains true, and you are missing a huge portion of malware. Hopefully, you at least have endpoint protection to have a chance to catch it further down the cyber kill chain.

The Top 5 Encrypted Malware table only shows malware detected over an HTTPS connection.  Since so few customers configure their Fireboxes to inspect encrypted traffic, and yet the ones that do see a vast majority of malware arrives over that encrypted channel, we don't believe our normal top 10 malware list (which is actually a mix of both encrypted and non-encrypted malware) is the true representation of the top threats out there. We would only know that if all Fireboxes inspected all HTTPS traffic too. However, despite having a much smaller sample size of Fireboxes inspecting encrypted traffic, we suspect the Top 5 Encrypted Malware table actually offers a much better representation of the top malware families spreading the most, compared to the normal top 10 list. Furthermore, the malware variants we see in this top 5 list are usually significantly different than the top 10 (though some show up on both) and are more on par with what we would expect as the top threats.

For example, even though the threat Agent.IIQ placed third in the normal top 10, it is number one on our top encrypted malware list. In fact, if you look at the detections for it on both lists, you'll see all Agent.IIQ detections (334,972) come from encrypted connections. So now imagine, if four-fifths of Fireboxes aren't monitoring encrypted traffic, and yet we know most malware arrives over encrypted connections, it seems clear that Agent.IIQ would very likely be the number one malware on both lists. We just can't scientifically prove it until more Fireboxes start inspecting encrypted traffic.

Let us digress for a second to hammer home these important points, even though they are probably obvious by now. We hope you take two things from this finding:

1. We can't emphasize enough how important we feel it is for you to enable HTTPS inspection, despite the fact that it requires some tuning and exceptions to do it properly. We've said it before, but the majority of malware arrives over encrypted HTTPS, and not inspecting it means you are missing it! More importantly, it turns out the most common malware is likely only detectable if you are inspecting encrypted traffic.

2. While the normal top 10 list does still offer some valuable and actionable intelligence, it's likely a limited and even false picture of the most common threats, because so few of the Fireboxes that generate that list inspected HTTPS. We suspect this top encrypted malware list probably offers a more accurate list of the common malware you should worry about, even if it only comes from the fewer Fireboxes inspecting encrypted traffic. So, weigh that in your defense decisions.

Returning to what we actually saw in this encrypted malware list this quarter, it included two web-based malware families (Trojan.HTML.Hidden and JS.Agent.UJY) that use HTML and JavaScript to ultimately steal credentials from victims. Interestingly, it also included a malware family called Taidoor, that we have only seen used by Chinese government cyber actors and no one else. In other words, some of our customers' Fireboxes may have detected and blocked parts of a state-sponsored cyberattack. We share more details on Taidoor a bit later.

| Top 5 Encrypted Malware Detections | | |
|---|---|---|
| COUNT | THREAT NAME | CATEGORY |
| 334,972 | Agent.IIQ | Dropper |
| 45,473 | Trojan.HTML.Hidden | Phishing |
| 10915 | JS.Agent.UJY | Scam File |
| 9,499 | SpamMalware-RAR | Email Dropper |
| 5,822 | Generic.Taidoor | Win Code Injection |

*Figure 2: Top 5 Encrypted Malware Detections*

## Top 5 Most-Widespread Malware Detections

When we only analyze malware by pure volume, we don't really know how widespread those threats are because it could turn out that only a small share of Fireboxes sees that same threat repeatedly in high volume. Meanwhile, that could leave the remaining larger share of Fireboxes seeing little to none of that threat. That's why we also created the Top 5 Widespread Malware table, to measure the variants that hit the widest share of individual Fireboxes. In our widespread malware table, we also share additional regional information about which countries see the most of each malware variant.

Q3's widespread malware list looks similar to Q2, with three of the top threats returning, though changing in placement, and two new but similar style malware variants making the list. We highlighted Trojan.Abracadabra, which is a trojan that distributes an Emotet variant, in our Q2 report and it returned in Q3 rising from second to the topmost widespread malware spot. Like last time, it still highly targets Japan, though we see it affecting other countries a lot more in Q3, which was not the case last time.

The remaining four samples on this list, though technically different, are all malware variants that are delivered via malicious Microsoft Office documents, by leveraging specific Office exploits. While we can't tell why, we find it interesting that all four of these Office exploit-related malware detections primarily happened in Greece.

| Top 5 Most-Widespread Malware | Top 3 Countries by % | | | EMEA % | APAC % | AMER % |
|---|---|---|---|---|---|---|
| XLM.Trojan.Abracadabra (Emotet) | Japan - 42.25% | Indonesia - 24.78% | Hungary - 24.47% | 10.64% | 26.47% | 2.42% |
| Trojan.Groooboor | Greece - 24.64% | Hungary - 24.47% | Germany - 23.98% | 15.05% | 7.92% | 2.43% |
| Exploit.CVE-2018-0802.Gen | Greece - 26.07% | Hong Kong - 23.85% | Germany - 21.25% | 14.00% | 6.30% | 2.55% |
| Exploit.RTF-ObfsStrm.Gen | Greece - 20.57% | Germany - 20.5% | Turkey - 20.28% | 13.35% | 5.51% | 2.34% |
| Exploit.RTF-ObfsObj-Dat.Gen | Greece - 22.81% | Turkey - 20.85% | Hungary - 20.21% | 12.55% | 6.22% | 2.33% |

*Figure 3: Top 5 Most-Widespread Malware Detections*

## Geographic Threats by Region

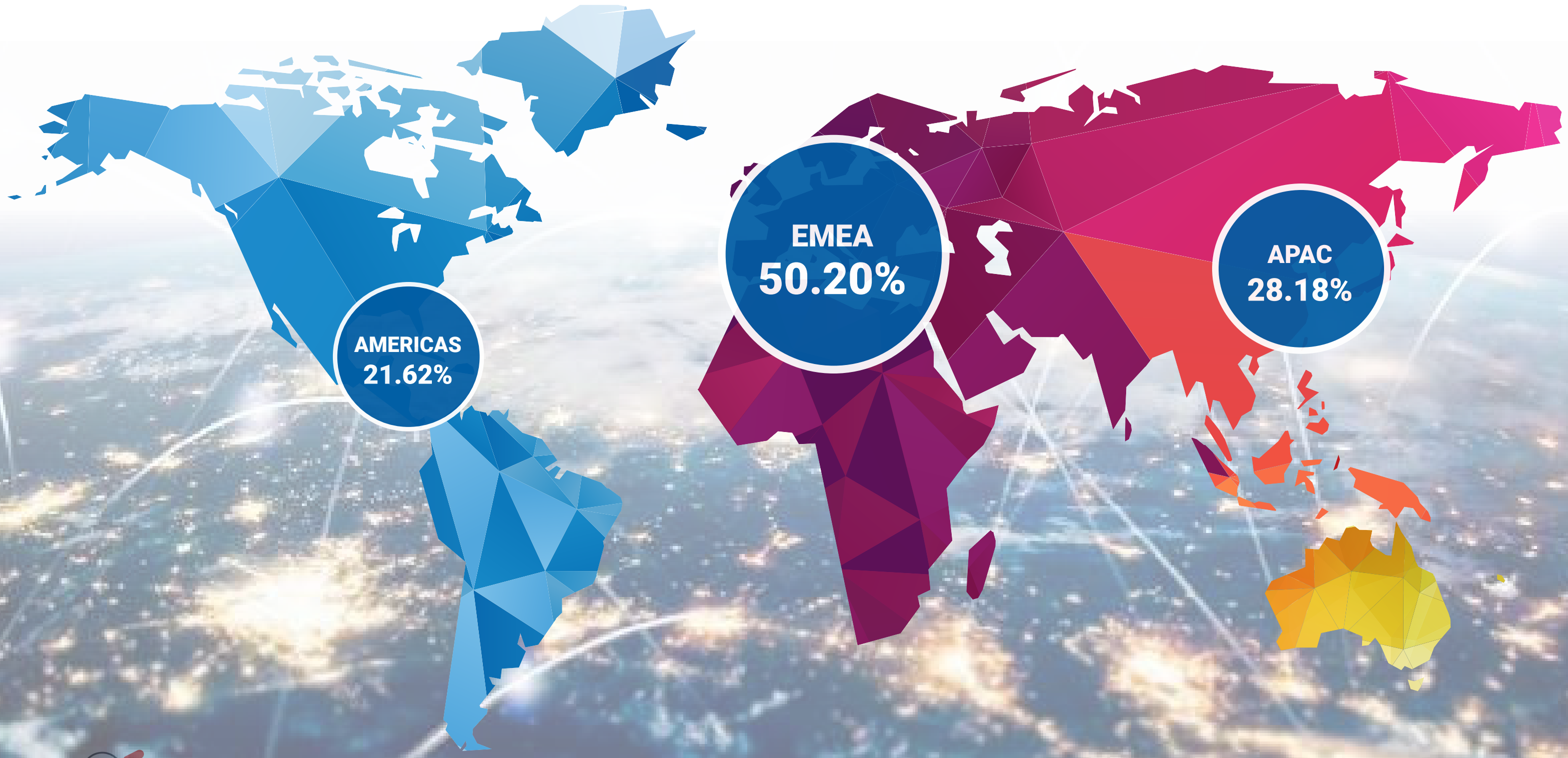
We believe it is interesting to know which general regions of the world received the highest percentage of malware attacks each quarter, even if we don't always have enough data to explain why some regions see more malware than others. Our regional table shows this. However, know that we have weighted the results to compensate for the differences in the number of Fireboxes in each region as well, otherwise one region may appear to see more malware only because we happen to sell more of our product in that region.

Not much changed from Q2 to Q3 2022 when it comes to total threats in each region except for Europe, the Middle East, and Africa (EMEA). EMEA saw fewer total threats but only saw 2.4% fewer threats when you account for the reduced number of reporting Fireboxes. AMER and APAC both increased by just over 1%.

| Region | Detections per Firebox | Average % IPS Detections per Firebox |
|---|---|---|
| EMEA | 5,263,480 | 50.20% |
| AMER | 8,816,405 | 21.62% |
| APAC | 3,264,935 | 28.18% |

*Figure 4: Geographic Threats by Region*

## Malware Detection by Region



## Catching Evasive Malware

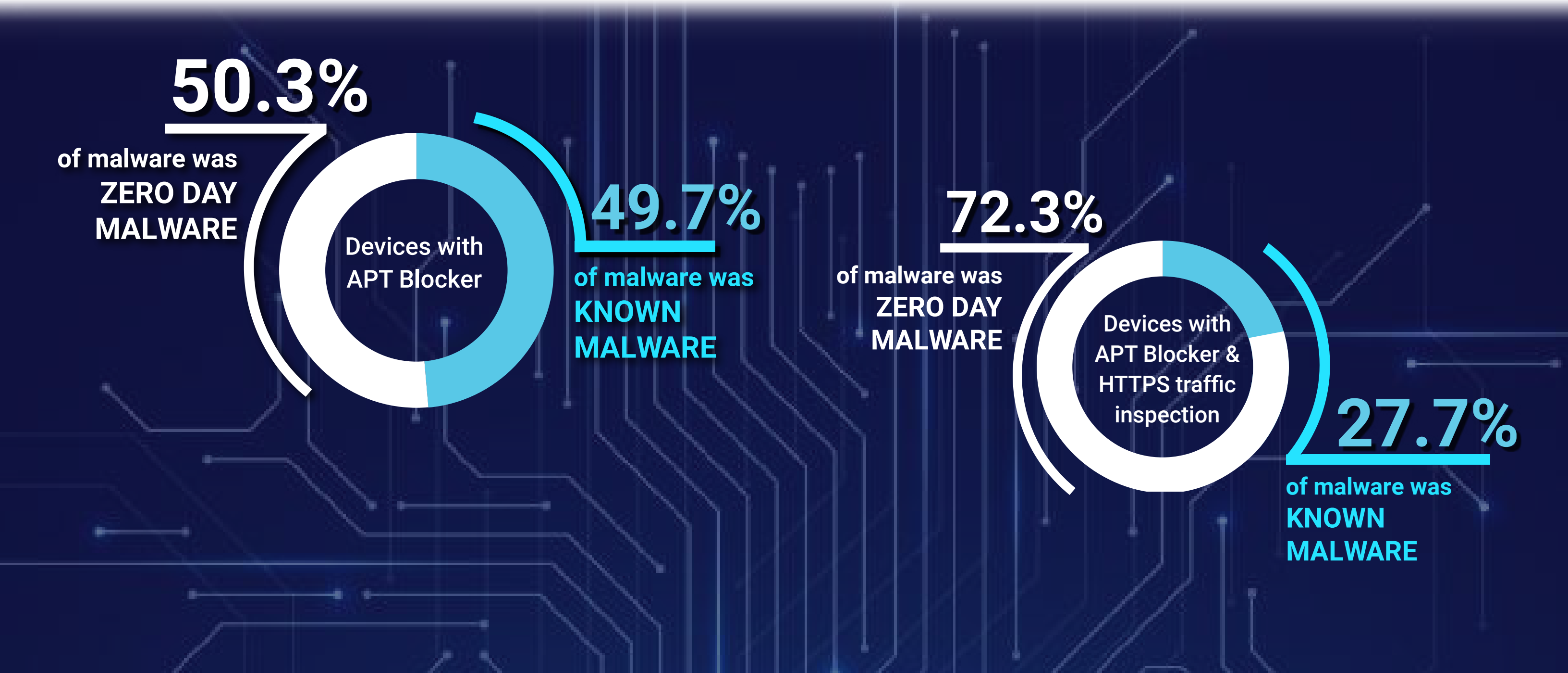
Let's look at some of the more concerning malware. Zero day malware is malware that is so new that human analysts may not have seen it before and created a signature for it and thus it will bypass signature-based malware detection engines like our Gateway AntiVirus (GAV). The creators of this malware tend to have more advanced knowledge of cybersecurity and leverage evasion techniques that bypass defenses that catch traditional malware.

In Q3, we just barely saw slightly more zero day malware (50.3%) than traditional malware (49.7%). This continues an interesting decline in our zero day malware trend. It is about a 3% decrease from Q2, and in past years, zero day malware averaged at around two-thirds of all malware. From a defense perspective, this is good news. However, this still means signature-based malware detection misses half of all malware, which is far too much. Be sure to also deploy more proactive, signature-less malware detection solutions, such as the behavioral detection of our APT Blocker malware engine, to catch these more evasive threats.

We also measure this zero day malware statistic for encrypted (TLS/SSL or HTTPS) traffic. As has been the case in almost all reports, we saw far more evasive malware show up in encrypted traffic. Specifically 72.3%, which is an eight-point decline from Q2, but still a higher amount than the 50% for non-encrypted traffic. This seems to confirm our long-standing theory that the threat actors that take the time to encrypt their malware delivery vectors will also put in the effort to deliver more evasion malware.

Network admins and security professionals know we must stop malware at soon as possible or face the consequences of malware in our networks. Using advance network malware detection, like WatchGuard's APT Blocker, at the perimeter will stop this zero day malware before it enters your network. WatchGuard's Endpoint Protection Detection and Response (EPDR) clients will also protect your devices directly, but we still recommend a layered defense. There are cases where endpoint-based protection can catch something a network solution would miss, but there are also use cases where network protection is more convenient and required.  We recommend users have both, and don't skip some sort of advance malware detection on the network perimeter, such as the Firebox's APT Blocker solution thatcomes with the Total Security Suite package.

### Zero Day Malware



# Individual Malware Sample Analysis

## Generic.Taidoor

In recent quarters, we have started to see more detections of malware that is sometimes known to come from government supported actors but is also used by criminal actors too. In our Q2 report, we described how Gothic Panda – a state-sponsored threat actor connected to China's Ministry of State Security – was known to use one of the top malware detections from that quarter called Heur.BZC.YAX.Boxter. However, not just government actors happen to also sometimes use Heur.BZC.YAX.Boxter, so we couldn't unequivocally tie it to Gothic Panda.

In contrast, we know cyber actors supported by the Chinese government created Generic.Taidoor, and we have yet to find anyone else using this malware. We believe that means this detection is really coming from state-sponsored threat actors.

Getting to how it's delivered and what it does, Taidoor tends to arrive as a zip-compressed file often received through email. When a user opens the zip file and runs its contained executable file it starts the infection process. The infection starts with a dynamic link library (DLL) loader running as a Windows service. DLL files contain code to perform one or more functions. The DLL files can call on other library files already installed in the operating system to perform tasks as well. The DLL file will load the second portion of the infection that contains an encrypted binary file.  It loads this encrypted binary into memory then decrypts it using a hard-coded key. The decrypted file loaded into memory is also a DLL file and it contains the main remote access trojan (RAT).

The sample we found connects to its command and control (C2) servers at cnaweb.mrslove.com and infonew.dubya.net and seems to target Taiwanese and Japanese victims.

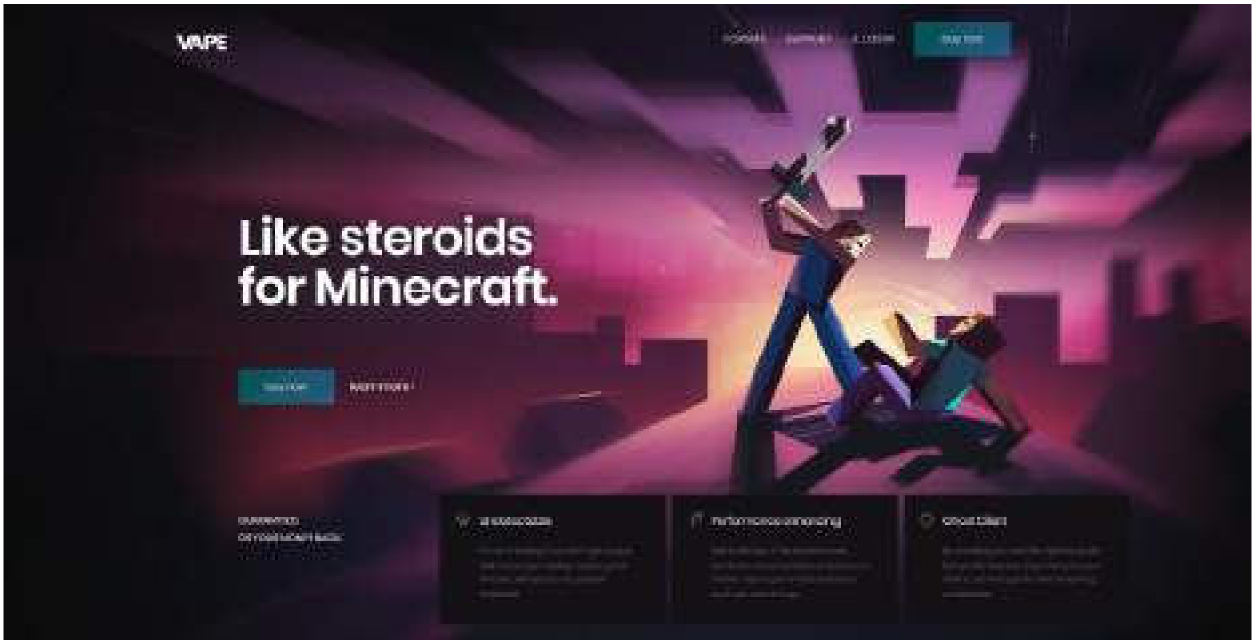
We encourage you to review a more detailed analysis of this malware at https://blog.reversinglabs.com/blog/taidoor-a-truly-persistent-threat and https://www.cisa.gov/uscert/ncas/analysis-reports/ar20-216a.

Nation state actors like the Chinese government and those working for them continue to covertly target other countries' infrastructure to steal secrets from private companies and national defense secrets, as well as spy on political, journalist, and activist targets of interest. In years past, a private company without military contacts didn't really need to worry about these threats but we recently have seen nation state actors targeting any company, especially if they work in infrastructure or a related field. In response, we recommend reviewing your security policies to include threats from nation state actors.

## Variant.Fugrafa

Fugrafa downloads malware that injects malicious code. In one sample we found it in a cheat engine for the popular game Minecraft. A file shared primarily on Discord claims to be the Minecraft cheat engine Vape V4 Beta. This file will install Vape, a potentially unwanted program (PUP) that allows users to cheat at Minecraft, but that's not all it contains.

The official website for Vape claims, "It's not cheating if you don't get caught," among other sleazy ads, and allows you to buy the official program for $35 or pay a monthly fee of $10. However, the malicious versions of the program we found largely shared on Discord don't cost anything, or so it seems.



Like steroids for Minecraft.

*Figure 5: dllinject-vape4*

In addition to the cheat engine, the “free” version shared on Discord contains other malware. Depending on what version of the malware you have, it may contain a coinminer that uses your computer’s resources to mine cryptocurrency, or a trojan that attempts to download a botnet. During our analysis, we weren’t able to verify that botnet download infrastructure still worked though.

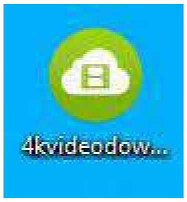
Many PUPs like Vape don’t harm the computer directly but open the door to security vulnerabilities and other malware. Stay far away from anyone trying to give you a cheat engine if you care at all about security. More importantly, not only are cheating app and piracy morally questionable, piracy is rarely truly free. Pirate programs, mobile apps, and even cheat programs often use their “free” lure only to get you to voluntarily install malware, which will cost you in worse ways.

### Trojan.Agent.FZUW Racoon Stealer

Agent.FZUW has some similarities to Variant.Fugrafa, but instead of installation through a cheat engine the file itself pretends to have cracked software. We found this sample has connections with Racoon Stealer, a cryptocurrency hacking campaign to hijack account information from cryptocurrency exchange services.

We saw these trojans first in the middle of July 2022 and noticed they stopped near the end of August 2022. Most of the time we saw the filename “4kvideodownloader.exe” or “applicationkey” in filename. 4K Video Downloader is a legitimate freeware application that allows you to easily download high resolution video from many video streaming sites like YouTube, Vimeo, and Facebook. It also has a paid option with many additional options and capabilities. We believe this malware is attached to the pirated “key cracking generator” that allows you to get the paid version for free, but again with hidden costs and ulterior motives.

The sample we found creates a proxy to hijack any domain related to binance, huobi, or okx and redirects to 35[.]236[.]159[.]79:8183. These names all relate to domain names for popular cryptocurrency exchanges.



***FZUM Icon***

Loading the program in our sandbox, we noticed it tried to access Iplogger[.]org/1RCgX4 to track the external IP of the victim's computer. Extracting some text from the executable, we found the IP address 62[.]204[.]41[.]144:14096. This didn't respond to our tests on that port, but we did find the IP address responds to HTTPS on port 443.

When accessing the web page at 62[.]204[.]41[.]144I we saw a copy of the page for the hardware wallet Trezor and could even open the page to connect the wallet. We didn't have a wallet to test here but we assume any information on the wallet would become compromised if we tried connecting it.

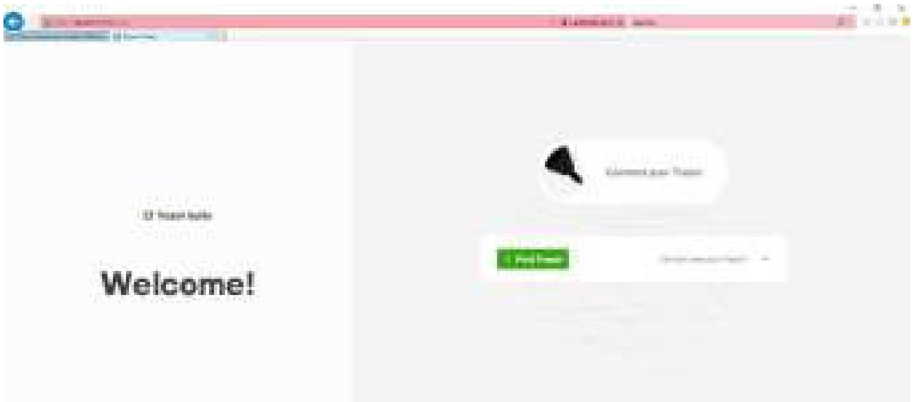


***Figure 6: Connect Trezor***

While the cryptocurrency stealing campaign we investigated may have stopped, other campaigns to steal cryptocurrency continue using the same resources set up previously. During the entire campaign of the malware variants, we see them consistently connect with two IP addresses in Taiwan 35.236.159[.]79 and 104.155.207[.]188, likely command and control (C2) servers where the malware sends the victims details.

You should never allow any type of cracked software on corporate networks, not just for the obvious legal reasons alone, but for the security of your organization as well.  While I am sure most of you – IT, technical and/or security professionals – already know both the legal and malicious software risks posed by piracy, the average non-technical employee may not. Often, we find an employee downloads pirated or cracked software on their own, not knowing the cybersecurity risks (even if they realize piracy is wrong), so user education, as well as an acceptable use policy that expressly forbids it, is key here as well.

# Network Attack Trends

Security is a cat-and-mouse game. Attackers, hackers, and no-goodniks get an initial advantage by initiating offensives tactics. But as any Tom and Jerry viewer well knows, a cat like Tom may have the fangs, but the mouse Jerry has got the brains. Attackers continually seek ways to circumvent defensive tools, and either proactively or reactively, we adapt and fine-tune our services to counter any new threats. The Intrusion Prevention Service (IPS) is one of those defenses that employs a catalog of signatures (new and old) to counteract network attacks. Packets are inspected for unique patterns of attack traits documented in the IPS database. Now, should there be a match, the potential threats are halted, and an alert is generated to notify the network administrators.

This quarter saw quite a fall in total detections. A 46% decrease from last quarter and a 77.6% decrease since Q3 2021. That is, total detections this quarter were 2,306,140. In Q2 2022 it was over 4.2 million and over the past three years, at its peak, it reached 5.68 million in Q4 2021. Those are big shifts. Wild swings in total detections quarter over quarter (QoQ) were discussed in the last ISR report. That reflection involved looking at periods consisting of several years and looking at individual signatures that tended to dominate within the total volume. One example is the #1 signature 1059160 (a SQL injection attack) in Q1 2022 that delivered almost 34% of the total detections. That signature and other regulars in the top 10 have begun to have a reduced presence. Signature 1059160 had 1/24th of the total detections compared to last quarter, which brought it down from 1st place in Q2 2022 to 15th this quarter. A few select signatures with an outsized presence seems to be slowly reversing, and perhaps reducing total detection numbers. That may be because of changing telemetry sharing enrollment from our customers, or perhaps a shake-up by attackers who are being more selective about automated attacks to improve their return on investment.

As stated earlier, we had 5.68 million detections in Q4 2021. A view of Figure 7 will make it evident that 5.68 million detections was not a common volume, but a culmination in increases of detections QoQ during 2020 and part of 2021. It was not long ago that we had 1.66 million detections in Q1 2020. In a further look back since Q1 2017 (data not included in Figure 7), we reached under a million detections twice. As discussed in the previous paragraph, signature 1059160 and other signatures regularly appearing in the top 10 had an abnormal volume ratio compared to most signatures. Our top four signatures last quarter all had a greater total of detections than the top signature this quarter. In summary, total volume is only one metric, and it's tough to pin down definitive reasons for the shift in volume.

Unique detections decreased by 2% to 437. A glance at the chart in Figure 8 shows that it has been on a steady 2.14% increase since Q3 2019. There are three new signatures in the top 10 signatures by volume this quarter. A common theme among the new signatures is their connection to management software, both industrial and non-industrial. A little later, we'll discuss the changing dominance of top 10 signatures in terms of volume in this section.

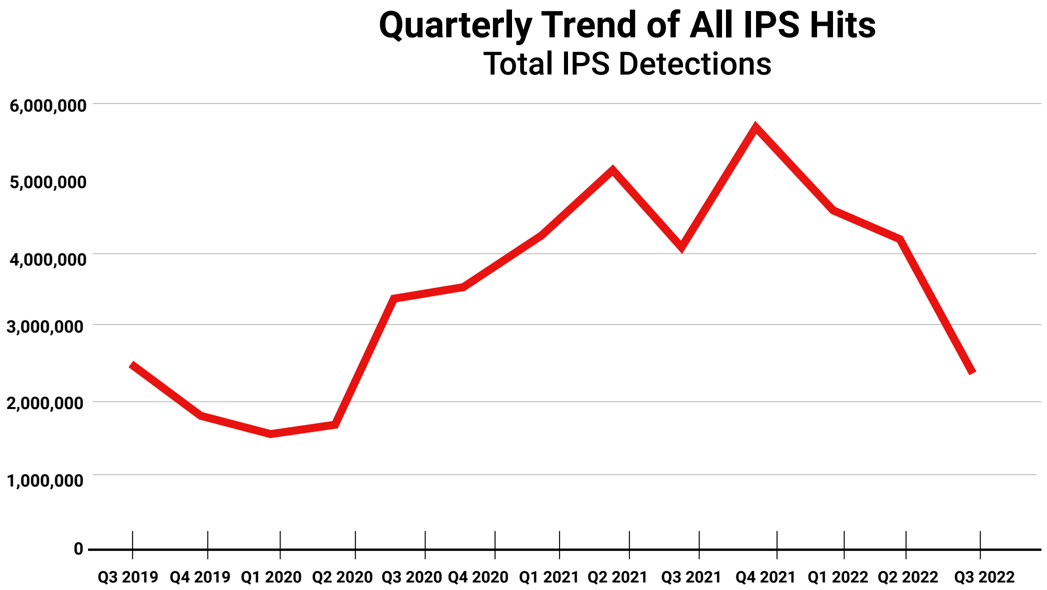


*Figure 7: Total IPS Detections*

| Quarter/ Year | IPS Hits |
|---|---|
| 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 |
| Q3, 2022 | 2,306,140 |

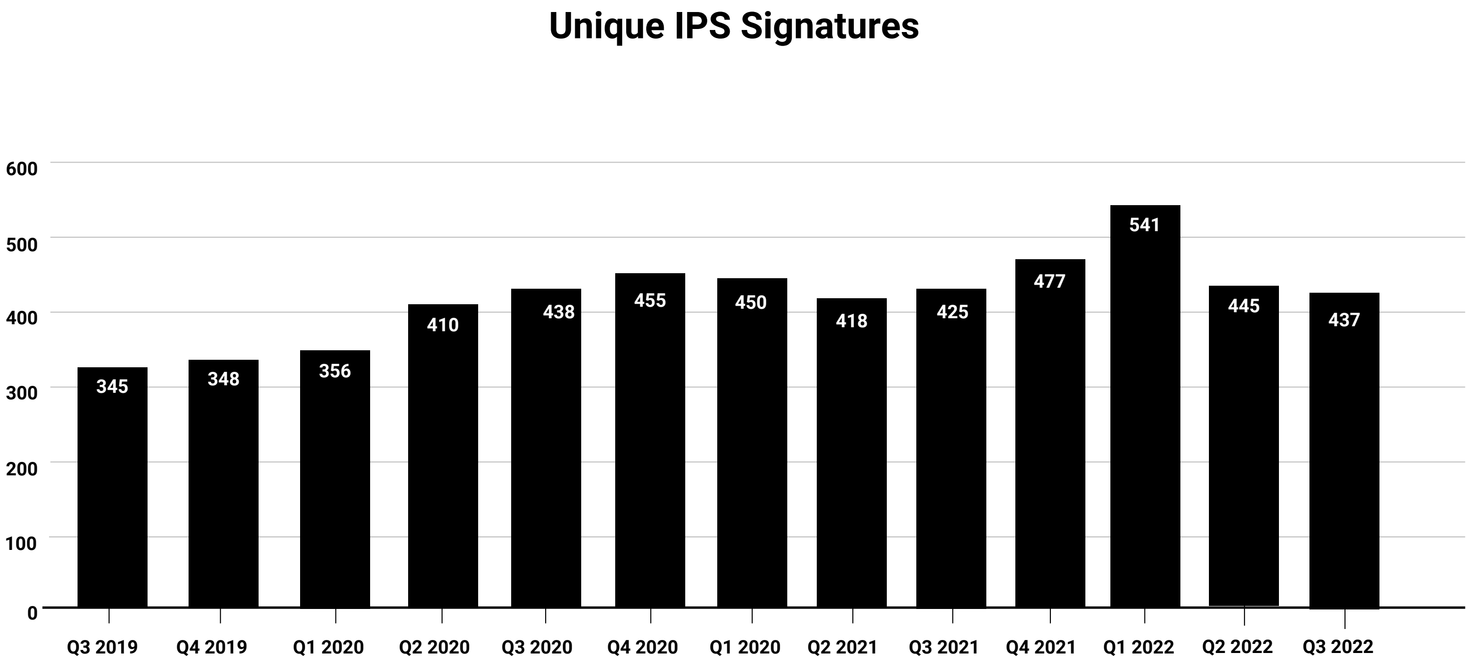


*Figure 8: Quarterly Trends of Unique IPS Signatures*

## Top 10 Network Attacks Review

**Signature 1058077 – 'WEB SQL injection attempt -1.b'**

*Affected Technology:*

*'Advantech WebAccess before 7.2'*
*'Flexbb 1.0.0 10005 Beta Release 1'*
*'Schneider Electric's U.motion Builder software versions 1.2.1 and prior'*
*'Core Config Manager in Nagios XI 5.2.x through 5.4.x before 5.4.13'*

*Associated CVE's: CVE-2014-0763, CVE-2007-1729, CVE-2017-7973, CVE-2018-8734*

Signature 1058077, new to the top 10 this quarter, detects SQL injection-type attacks against several vendors. One of the vendors is Advantech, whose WebAccess portal is used for SCADA systems across a variety of critical infrastructure. The **vulnerabilities included**: numerous locations in the software where attackers could run an SQL Injection, many pathways for initiating a Stack Buffer Overflow, revealing information through a JavaScript exploitation that fails to ensure URL validation, and an opportunity for a command injection to run a remote file. This discovery is from 2014 and has since been fixed with an updated version.

Flexbb is PHP-based message board software. It is likely a fork of Fluxbb, a more widely adopted forum software. Flexbb has a minimal presence online, therefore references and documentation are thin. The Internet Archive shows a web page for the form in late 2008, but since then, the domain has been owned and used for other unrelated content. The software was vulnerable to SQL injections, which would allow attackers to attack its SQL database.  This vulnerability was **discovered** by user 'trueend5' from the Security Science Researchers Institute of Iran in 2007.

A serious exploit involved Schneider Electric's U.motion Builder software versions 1.2.1 and prior. Schneider Electric is an energy management company whose software reaches into residential and commercial sectors. U.motion is a web server used for smart home automation. The hardware device installed at the home or office then connects to either a smart screen panel, app, or web interface. It does what you can imagine a centralized smart home system would do, by controlling lighting and heating, tracking energy use, monitoring IP cameras, handling other features such as email and weather data, and many other uses. U.motion Builder is the configuration software for customizing your U.motion automation operations. The software connects to the U.motion hardware remotely to export new settings, but requires admin access to allow the export.

The CVE score for their software vulnerability was 9.8 out of 10 – a severe issue that required immediate remediation. An unauthenticated user could run arbitrary SQL commands against their database. Within the software were several layers of vulnerabilities. They included the ability to cause a stack-based buffer overflow, and failure to handle proper input validation in addition to a failure to handle cross-site scripting (XSS) attacks against malicious scripts. Many of us may be early adopters or in the process of transitioning to a smart home-connected lifestyle, whether we like it or not. With Internet-connected thermostats, cheap security cameras, and virtual assistants via smart speakers all around, it becomes easy to imagine how significant it would be if someone hacked into your centralized smart system and were able to acquire personal details. That threat level can be even more significant were it at a commercial office or industrial location. As their software is used in the energy industry, it is notable that we are seeing this signature's presence in the top 10 list. Those attacks may very well be attacking other software connected to this signature. We hope any of our customers using U.motion Builder software has updated their software. The CVE was **published**
in 2018.

Nagios is the remaining software associated to signature 1058077. An open-source monitoring software, it was vulnerable to SQL injection via one of the value parameters in the core config manager. This CVE is from 2018. As signature 1058077 is a multivendor vulnerability, the intended target could have been one or all these vendors. It stands out that this was the #2 signature by volume, with over 236,000 detections (10.2% total volume). Like last quarter, we saw some of our top signatures target industrial control system management technology. Both Advantech WebAccess portal and U.motion Builder software are new this quarter. It was only last quarter that SpecView, Zoho ManageEngine DC, Oracle Enterprise Manager Grid Control, and SysAid Help Desk, were discussed. This reinforces the idea that attackers are focusing their efforts on management systems, industrial and non-industrial.

**Signature 1130366 – 'WEB Directory Traversal -16'**
*CVE: CVE-2014-5445*

ZOHO ManageEngine is a popular enterprise IT software and the sole affected vendor of signature 1130366 (new this quarter). One of the products within the software is NetFlow Analyzer, a solution for monitoring NetFlow data. The other product, IT360, is used for monitoring performance, such as server downtime, across all the organization's infrastructure. The specific versions are NetFlow Analyzer 8.6 through 10.2 and IT360 10.3. The vulnerability from 2014 allowed attackers on NetFlow Analyzer to remotely execute a directory traversal to file paths intended to remain private. IT360 only required access via an authenticated user to run the attack.

This vulnerability's release may be more interesting than the vulnerability itself. Pedro Ribeiro, a researcher, released a zero day Proof-of-Concept to exploit the Zoho software. It was not out of malice (some may see it otherwise) that the zero day was released, but out of frustration as Pedro had been in communication with Zoho for over three months without any results on closing the vulnerability. He had been continually strung along to believe that the software would be patched soon. His words were a bit stronger, that ManageEngine had been "twiddling their thumbs (and making a fool out of me) for 105 days" (**source**).  There are several other exploits that Pedro discovered in ManageEngine and published – some of them zero days. You can find them at the bottom of the page **here**.

**Signature 1138800 – 'WEB Microsoft Exchange Server Remote Code Execution Vulnerability -6'**
*CVE: CVE-2021-26855*

The most recent CVE among our new signatures this quarter, **CVE-2021-26855**, is a Microsoft Exchange Server Remote Code Execution vulnerability for on-premises servers. You may know this flaw by its 'marketed' name in the research community, ProxyLogon. It is not a surprise to anyone in the IT industry that this remote code execution vulnerability was given a 9.8 CVE score. In addition, this was known to have been exploited. The date and severity of this vulnerability likely sounds familiar to you, and it should be because it is one of the exploits used by the group HAFNIUM. On-premises Exchange servers for 2013, 2016, and 2019 were all vulnerable. Microsoft released on March 2nd, 2021, both the CVE and **security updates** for the Exchange servers. It isn't a surprise to see this signature in the top 10 based on the severity of the attack and attention it had garnered in the media.

We were curious what the detection levels were since the inception of this vulnerability. The table below shows the history of the signature. Initially, with almost 32,000 detections in Q2 2021 at a total 0.6% of total volume, it has nearly tripled in detections to under 90,000 this quarter. It's proportion of volume at 3.9% shows that attackers are increasingly shifting their resources towards attacks with large returns. We expect most Exchange servers affected by this vulnerability to have been patched by now, but most does not equate to all. Therefore, risks remain.

| Quarter | Rank by Volume | Detections | % of Total Volume |
|---|---|---|---|
| **Q3 2022** | #9 | 89,609 | 3.9% |
| **Q2 2022** | #14 | 74,185 | 1.8% |
| **Q1 2022** | #20 | 20,052 | 0.4% |
| **Q4 2021** | #26 | 16,876 | 0.3% |
| **Q3 2021** | #22 | 20,261 | 0.5% |
| **Q2 2021** | #20 | 31,991 | 0.6% |

***Figure 9: Placement of Signature 1138800 (CVE-2021-26855) since Q2 2021***

As has been the case in past quarters, the signatures in the top 10 by volume list tend to be familiar signatures. Of the ten signatures, six were from last quarter, and signature 1054838 was last seen in Q4 2020. It is a local file inclusion (LFI) vulnerability where the attacker runs a directory traversal attack to acquire files outside the scope of what should be publicly accessible. This impacted a wide range of vendors, including Dell Storage Manager versions before 16.3.20, ArcServe UDP before 5.0 Update 4, Oracle Application Testing Suite component in Oracle Enterprise Manager Grid Control 12.4.0.2 and 12.5.0.2, Brocade Network Advisor version 14.0.2 and prior, and Microsoft SharePoint Server 2010 SP1 and SharePoint Foundation 2010 SP. All the software, in one form or another, is used for managing or hosting centralized IT data.

After reading through this top 10 by volume section, hopefully you are thinking, “is our organization’s centralized management as secure as it should be?” It doesn’t hurt to re-review admin access, remote access firewall rules, security logging maturity, and anything else that could allow an attacker to weasel their way into one of your management systems. As the data shows, the IPS service does prevent millions of attacks. That shouldn’t create complacency. Instead, it should act as a jolt to your security team to enact the necessary security polices and enforce them (the best that is humanly possible by often over-stretched teams) to ensure your network and management software stay far from compromised.

| Signature | Type | Name | Affected OS | Count |
|---|---|---|---|---|
| 1132092 | Buffer Overflow | FILE Invalid XML Version -2 | Windows | 374822 |
| 1058077 | Web Attacks | WEB SQL injection attempt -1.b | Windows, Linux, FreeBSD, Solaris, Other Unix, Mac OS | 236314 |
| 1059877 | Access Control | WEB Directory Traversal -8 | Windows, Linux, FreeBSD, Solaris, Other Unix | 187384 |
| 1055396 | Web Attacks | WEB Cross-site Scripting -9 | Windows, Linux, FreeBSD, Solaris, Other Unix, Network Device | 121099 |
| 1059958 | Web Attacks | WEB Directory Traversal -27 | Windows | 100849 |
| 1054837 | Web Attacks | WEB Remote File Inclusion /etc/ passwd | Windows, Linux, FreeBSD, Solaris, Other Unix | 91192 |
| 1130366 | Web Attacks | WEB Directory Traversal -16 | Windows, Linux, FreeBSD, Solaris, Other Unix, Mac OS | 90712 |
| 1138800 | Web Attacks | WEB Microsoft Exchange Server Remote Code Execution Vulnerability -6 (CVE-2021-26855) | Windows | 89609 |
| 1230275 | Web Attacks | WEB Apache log4j Remote Code Execution -1.h (CVE-2021-44228) | Linux | 88937 |
| 1054838 | Web Attacks | WEB Local File Inclusion win.ini -1.u | Windows | 72545 |

***Figure 10: Top 10 Network Attacks by volume***

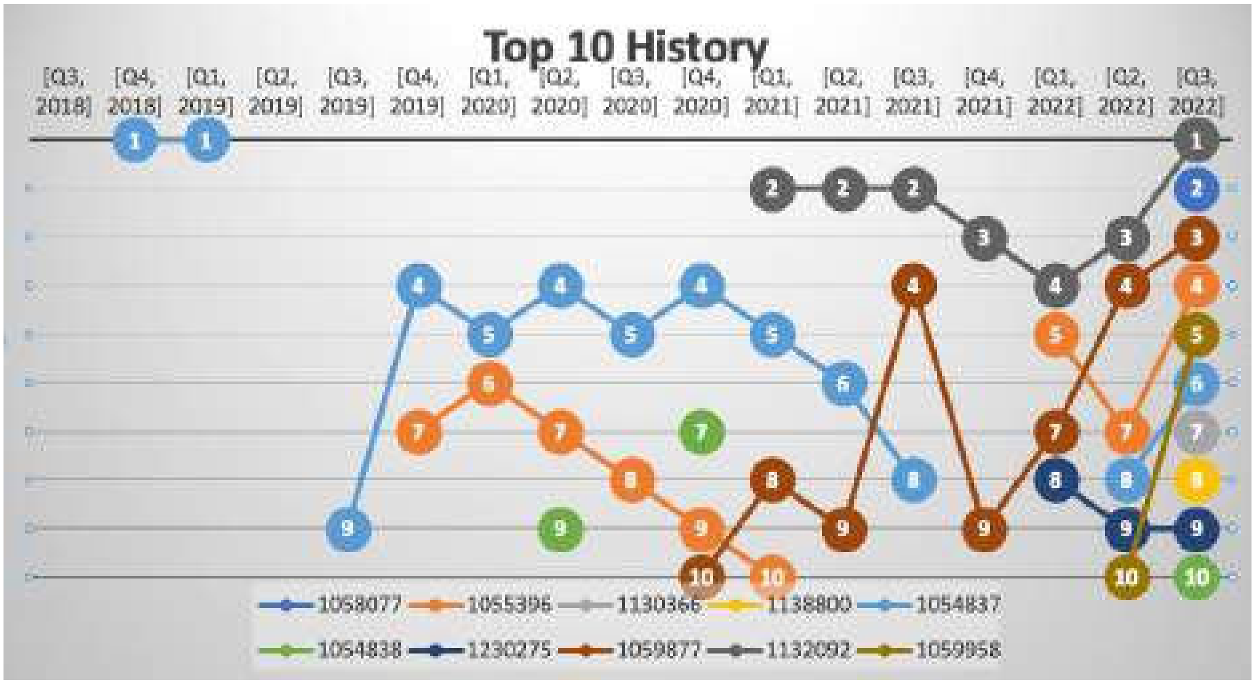


***Figure 11: History of prominent signatures in the Top 10 since Q2 2018.***

Already discussed in the introduction, signature 1059160, a SQL injection attack, has been on every top 10 list until Q1 2019. This time it fell to the 15th spot. What is interesting is that it had the #1 spot on the top 10 since Q2 2022, and for the first time has dropped, significantly, by fourteen places. It had 1.6% of the total detections (36,064). It always stayed above 20% of total detections, with it recently hitting 33% in Q1 2021. That then dropped by over 13-points from Q1 2022 to Q2 2022, and to a nearly 19-point decrease from last quarter.

Many signatures have had a lengthy stay on this top list. None were around in Q3 2018, and the current signature with the greatest longevity (light blue colored signature 1054837) has been in and out of the top 10 placement over the past three years. One signature that is neither new nor was on the list in Q2 2022 is signature 1054838 (discussed earlier), in 10th place. It was last seen in Q4 2020 and then before in Q2 2019.

The top 3/5/10 signature totals show how the concentration of alerts is for only a select few signatures. Total detection percentages continue to decrease since we began tracking it in Q1, 2022. The top 10 signatures have often had a dominant presence among all the other signatures. It was not uncommon for the signature in first place to be 10-30 times the size of the 10th place signature on the top 10 list. It was only recently in Q1 2022 that the top three signatures took up nearly 87% of the total detections!

| | Top 3 | Top 5 | Top 10 |
|---|---|---|---|
| **Hits** | 789,520 | 1,020,468 | 1,453,463 |
| **Total Detection %** | 34.63% | 44.25% | 63.03% |

***Figure 12: 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 37.42% | France 34.4% | US 34.39% | 32.20% | 25.06% | 24.81% |
| 1132518 | WEB-CLIENT Javascript Obfuscation in Exploit Kits - 57 (Possible Exploit Kit) | UK 44.8% | US 40.34% | Germany 25.87% | 31.30% | 21.69% | 17.78% |
| 1110932 | FILE Microsoft Windows GDIplus PNG tEXt Chunk Processing Integer Overflow | Germany 24.94% | Portugal 24.47% | Brazil 23.87% | 12.34% | 22.72% | 17.41% |
| 1059877 | WEB Directory Traversal -8 | Germany 28.41% | Portugal 23.4% | Australia 18.18% | 14.60% | 18.47% | 17.41% |
| 1132092 | FILE Invalid XML Version -2 | Australia 25.76% | Italy 24.84% | UK 21.87% | 15.50% | 15.16% | 21.11% |

*Figure 13: Top 5 Most-Widespread Network Attacks*

**Signature 1132518 – 'WEB-CLIENT Javascript Obfuscation in Exploit Kits - 57' (Possible Exploit Kit)**

There was one new most-widespread signature this quarter. Signature 1132518 from 2016 is a generic vulnerability for detecting JavaScript obfuscation attacks against browsers. An exploit kit is a piece of malicious software with the means of attacking its victim without prior knowledge of the user's environment. Just like a Swiss army knife, it is a multi-packaged tool prepared for encountering most situations. The typical path for an exploit kit is to compromise a website and wait for a victim to arrive. A path to accelerate that process is to involve the compromised domain in a phishing campaign so that the user is directed to that compromised website. JavaScript is a common vector for attacking users, and as the defensive fortifications have improved on browsers, so have the attacker's ability to obfuscate the malicious JavaScript code.

**Examples of Obfuscation:**

AES 256 and JavaScript, where there's a normal encryption value, can hide malicious code. The web content may look benign to a browser security filter, but a call to a publicly available JavaScript function will decrypt the code and release the contents for the user to see.

Base64 encoding, URL encoding (Escape), and JavaScript, where a Base64 variable string is backwards to disguise its contents. The string is then reversed and decoded. The content is then processed through URL encoding to turn non-ASCII and reserved characters into a Uniform Resource Identifier (URI) format universally used among browsers.

‘Exclusive or’ XOR Encoding and JavaScript, where the string can be charCode and then have the contents XOR’d to unwrap the code. XOR is a logical operation that compares two values, and if one is false and the other true, it will produce a true value. That was the process in decoding the charCode. ‘charCode’ returns a Unicode character based on the keyboard key pressed. That Unicode value then needs to be converted to a character, which is done with the fromCharCode() method. After those conversions, the malicious content should then be visible.

In each of the three examples above, the malicious JavaScript had to take one or more obfuscation steps to disguise the content. Those methods can be used in different orders of operation, and in different quantities, to achieve the hidden goal of displaying a phishing or other malicious page to the user.

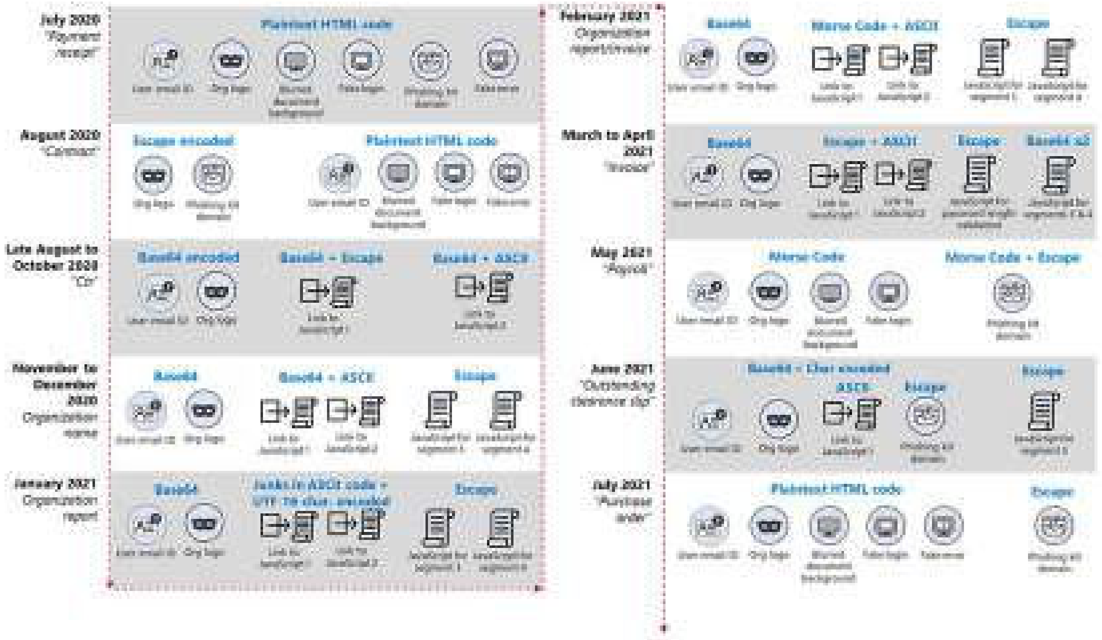
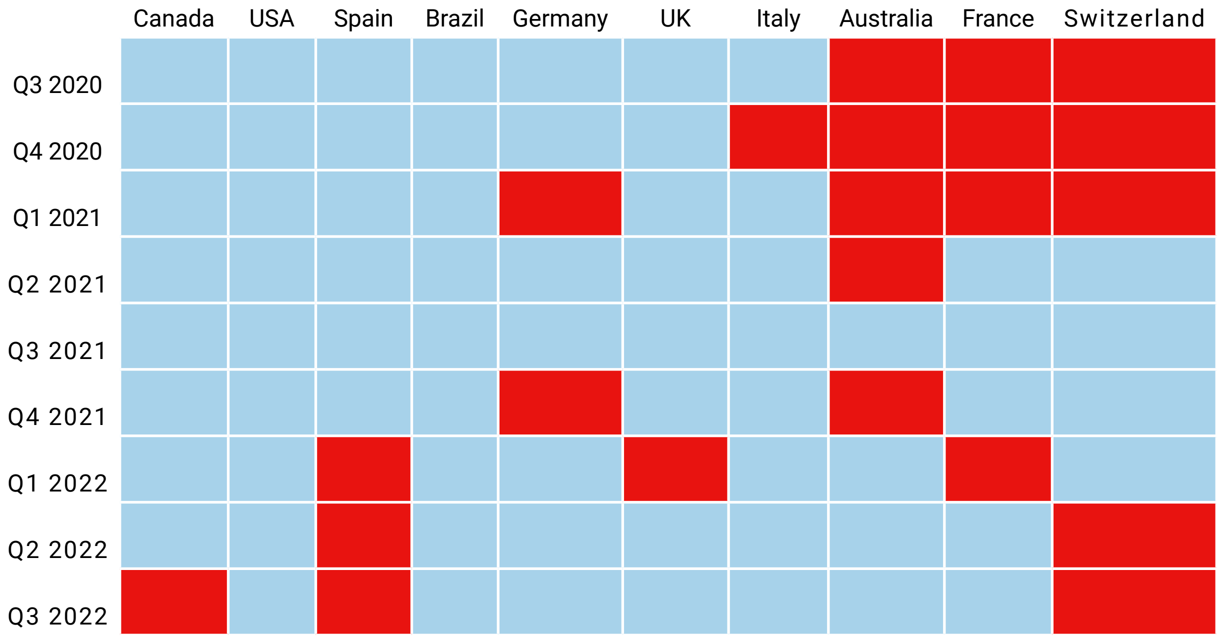


***Figure 14: JavaScript obfuscation, [Microsoft Blog Post]()***

Microsoft published a nifty graphic documenting an invoice-themed phishing campaign using HTML attachments with obfuscated malicious content. The graphic below demonstrates how tricky it can be to catch malicious web pages with JavaScript obfuscation (and some without) when the strategy is being constantly tweaked.

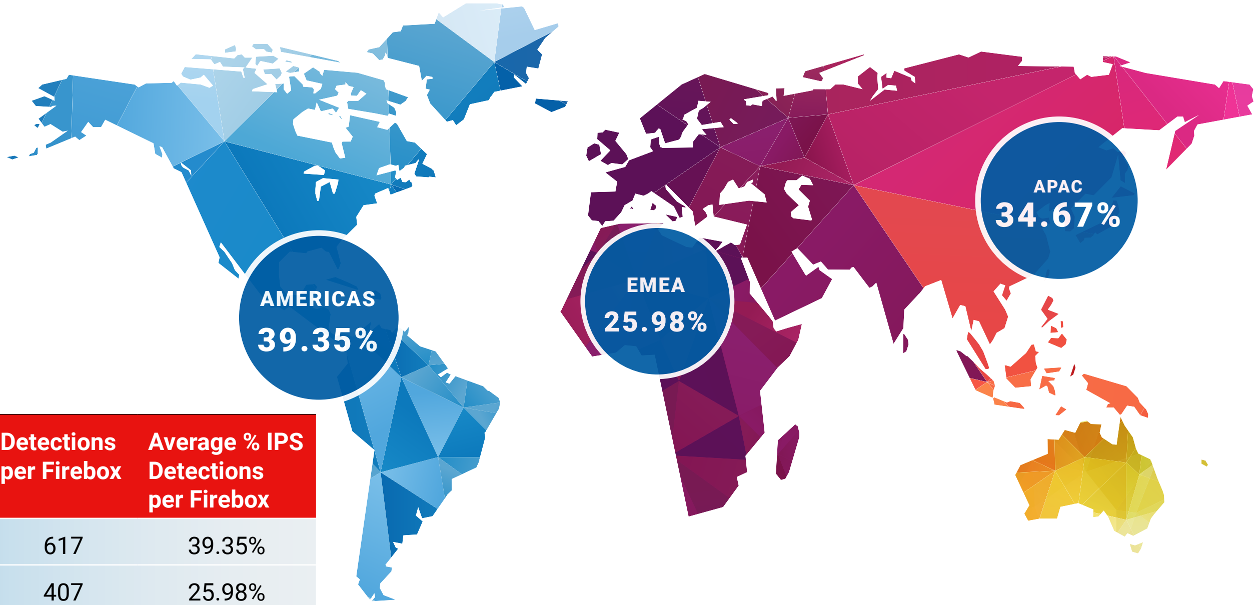
Each quarter, we review the top 5 most-widespread networks attacks. For each signature we track, the top three countries most widely affected by the signature are included. Canada is the only country not present this quarter among the countries present last quarter. We track countries most impacted by these signatures to glean any possible connections to current events and ransomware campaigns. It is often Western nations with greater average incomes and common languages that continue to be among the select few countries impacted by widespread attacks. We don’t foresee drastic changes in this unless the ransomware and other malicious cyber activities economies begin to change. As national cybersecurity agencies and companies’ relationships mature, and the means for paying out ransoms becomes illegal (the idea is beginning to take traction), then we could see a change in environment where attackers focus their efforts elsewhere.



| | Canada | USA | Spain | Brazil | Germany | UK | Italy | Australia | France | Switzerland |
|---|---|---|---|---|---|---|---|---|---|---|
| Q3 2020 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟥 | 🟥 | 🟥 |
| Q4 2020 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟥 | 🟥 | 🟥 | 🟥 |
| Q1 2021 | 🟦 | 🟦 | 🟦 | 🟦 | 🟥 | 🟦 | 🟦 | 🟥 | 🟥 | 🟥 |
| Q2 2021 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟥 | 🟦 | 🟦 |
| Q3 2021 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 |
| Q4 2021 | 🟦 | 🟦 | 🟦 | 🟦 | 🟥 | 🟦 | 🟦 | 🟥 | 🟦 | 🟦 |
| Q1 2022 | 🟦 | 🟦 | 🟥 | 🟦 | 🟦 | 🟥 | 🟦 | 🟦 | 🟥 | 🟦 |
| Q2 2022 | 🟦 | 🟦 | 🟥 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟥 |
| Q3 2022 | 🟥 | 🟦 | 🟥 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟦 | 🟥 |

***Figure 15: Countries Present at Least Once in the Most-Widespread Attacks per Quarter***

## Network Attacks by Region



| Region | Detections per Firebox | Average % IPS Detections per Firebox |
|---|---|---|
| AMER | 617 | 39.35% |
| EMEA | 407 | 25.98% |
| APAC | 543 | 34.67% |

This quarter saw significant change in total detections per Firebox. APAC had 2,979 detection per Firebox last quarter, whereas it now sits at around under a 1/6th of that. Although not at the same scale, but AMER went from 1,470 detections per Firebox to 617 detections since last quarter. EMEA decreased by nearly a 1/5th. That is not insignificant, but less notable than the other two regions.
This is the first quarter since we began tracking the average percentage of IPS detections per Firebox (since Q 2021) that there has been such a relative balance between the regions. There isn't a singular reason behind this, but it is possible to make some inferences. One could be a shift in attackers being less region bound as ransomware payments are becoming increasingly hard to pay due to government regulation. Another reason could be that companies have rapidly matured their security posture and are better positioned to repel attacks and recover data. For many companies, this was something unreachable just a few years ago.

A third consideration could be the change in signature dominance that we spoke on earlier. Several of the signatures that used to take up a large amount of the volume may have had most of the traffic sitting in one region, therefore obfuscating the regional data. That is, the outliers are finally dissipating and leading to more normal data sets.

## Conclusion

I (the one reading this right now) should check that ________________ is properly secured from any
IT Management Software

known vulnerabilities and potential exploits. I'm going to reach out to _____________ to confirm that
Head of IT Security

________________ is up to date and has had a recent enough security audit. If I don't double-check
IT Management Software

this and we are compromised during winter break I will be _________ .
Emotion

A researcher ___________ submitted a vulnerability for ______________ ___ ________ days ago.
Hacker Name Software Number

Any period longer than ________ days should be addressed immediately. If __________ releases
Number Hacker Name

the exploit out of frustration due to being strung along then they are ____________ but I'm still going to
Adjective

have to answer to ___________ since now I need to address this zero day.
Manager's Name

Okay, so now you have done a Mad Lib in its worst form. In all seriousness, we've got threats all around us. Threats against our management software, threats of zero day releases, and threats of the unknown. That is why using a tool like IPS can free you in one area to focus on critical risks and vulnerabilities elsewhere. You are aware of the attacks that have been blocked after reviewing IPS alerts, which in turn helps remind you that attackers aren't quietly waiting for an opportunity. They are actively seeking system compromise wherever possible. The big prizes for attackers like an Exchange Server or a SCADA management system rightfully so deserve extraordinary attention. So, when a patch is available, it's important to update immediately, as attackers will eventually benefit from any organization who failed to heed the latest security advisories.

# DNS Analysis

In Q3 of 2022 we saw a decrease in activity from the previous quarter, with blocked connections coming in at 5,513,653. This was a decrease of roughly one hundred and fifty thousand fewer blocked threats worldwide compared to the previous quarter, or roughly 3%. We attribute this trend to students leaving educational facilities, workers heading to summer vacations, and many businesses deciding that a work-from-home option is a valid solution for the workforce. 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 Q3.

**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 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 three new additions to the top malware domains list.

### t[.]awcna[.]com

This domain has been used multiple times in the past to help assist the command and control networks of LemonDuck malware. This malware steals credentials, redistribute itself via email, and attempt to bypass security controls by removing them entirely. LemonDuck has been an evolving malware as it originally started to steal cryptocurrency, but has evolved to general information stealing.

### T[.]zz3r0[.]com

While this is an aging domain, meaning that activity has not been as prevalent in recent years, the domain is also a former LemonDuck malware domain that is still listed as malicious by many of our feed partners. Leaving this domain blocked and classifying it as malware is not only a way to track the history of the domain for further malicious behavior, but a way to prevent infections brought on to a protected network by continuing to request commands.

### pstests[.]ru

This domain is part of an emotet classified domain. Emotet is a malspam trojan that is distributed by malicious spam emails that the end user might click and become infected. Once the payload runs, there are multiple types of impact that could be a symptom of the malware. Variants of Emotet can steal account details, redistribute themselves to other systems to spread, or even deliver ransomware to affected systems.

**Malware**

| Domain | Hits |
|---|---|
| t[.]awcna[.]com | 93,614* |
| newage[.]newminersage[.]com | 91,816 |
| newage[.]radnewage[.]com | 90,494 |
| t[.]zz3r0[.]com | 15,479* |
| h1[.]ripway[.]com | 13,036 |
| hrtests[.]ru | 7,072 |
| profetest[.]ru | 6,768 |
| testpsy[.]ru | 6,654 |
| toknowall[.]com | 6,476 |
| pstests[.]ru | 6,414* |

* Denotes the domain has never been in the top 10

## 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 they have been cleaned of the malicious content. Below are some examples of interest from top compromised domains during the quarter.

**www[.]granerx[.]com**

This domain claims to be a full-service pharmacy providing discount drugs and medical equipment. The domain, however, has requested user log in and credentials for admin users from a WordPress exploit and it appears that an attacker has taken over the domain. While not directly malicious, websites that have consistent issues with WordPress exploits can easily become landing spots for more malicious content.

**www[.]sunf[.]com**

The domain is a tire sales sight based out of Canada. The domain has had issues in the past with adware and pop-ups, but currently is clean. We regularly review compromised websites and update our domain feeds to remove those that have been cleaned up as long as they are not repeat offenders.

Compromised

| Domain | Hits |
|---|---|
| differentia[.]ru | 705,942 |
| ssp[.]adriver[.]ru | 1,405 |
| www[.]granerx[.]com | 1,205* |
| users[.]atw[.]hu | 658 |
| d[.]zaix[.]ru | 519 |
| shit-around[.]com | 509 |
| facebook[.]apps[.]fiftyfive[.]co | 234 |
| track[.]dobermanmedia[.]com | 203 |
| 0[.]nextyourcontent[.]com | 151 |
| www[.]sunf[.]com | 78* |

* Denotes the domain has never been in the top 10

## 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.

**retcode-us-west-1[.]arms[.]aliyuncs[.]com**

The domain has had multiple subdomains tied to multiple phishing campaigns. The most prolific destination has been triggering alerts as a Microsoft look-alike campaign requesting Office365 credentials. We were able to prevent just over two-thousand users from potentially falling for the phish.

Phishing

| Domain | Hits |
|---|---|
| unitednations-my[.]sharepoint[.]com | 58,855 |
| edusoantwerpen-my[.]sharepoint[.]com | 5,885 |
| nucor-my[.]sharepoint.com | 4,822 |
| firebasestorage[.]googleapis[.]com | 2,752 |
| retcode-us-west-1[.]arms[.]aliyuncs[.]com | 2,158* |
| e[.]targito[.]com | 1,772 |
| t[.]go[.]rac[.]co[.]uk | 1,391 |
| data[.]over-blog-kiwi[.]com | 998 |
| keyrocks-my[.]share-point[.]com | 586 |

* Denotes the domain has never been in the top 10

## Conclusion

Even with a dip in total blocked or tracked domains for the third quarter of 2022, it is easy to see that attacks on unsuspecting users are still high. This month more malware and attempted malware sites were newer domains than we have seen in recent months. This trend will change and modify with the landscape of cryptocurrency in turmoil as attackers look for other venues to trick users. Keeping DNS protection enabled is a way to monitor and block unsuspecting users from allowing malware or other serious issues into your organization.

# Firebox Feed: Defense Learnings

Its not every year that we have the World Cup, and not every quarter will we see the biggest hits. But malicious cyber actors never stop trying. It may appear that we have a slight upper hand now but only if we keep on our toes to catch and deflect the next attack. They say you need to train 10,000 hours to become an expert at something. Not everyone needs to become a cybersecurity expert but if everyone spends just a fraction of that time training on best practices, then we will all be a little more secure on the web. Training can come from studying and learning or simply keeping up on the latest security trends like in this report. With these ideas in mind here are some defensive tips. This game never ends.

1

## Free As in Free Malware

To some users, it sounds simple to just download the software you need off some unknown website you found on Google or discord link, but users should never do this. Two new malware samples we found act as a trojan to try and trick the unsuspecting user into installing the malware. Vape_V4_Beta and 4kvideodownloader can have the legitimate installer and install legitimate software but you may never know what else the installer delivers. One may conclude that only gamers and video downloaders need to worry about this, but we also commonly see programs that contain malware imbedded in them like Adobe and Microsoft Office. We've even seen malware in popular coding programs. The only sure way to avoid these traps is to only download software from a trusted website. Even then, it doesn't hurt to run it through your favorite anti-malware scanner before installing the program.

2

## Duck Out of These Domains

When it comes to malware domains, we saw LemonDuck spread malware through multiple sites over the quarter. The malware spreading sites t[.]awcna[.]com and T[.]zz3r0[.]com don't have easily recognizable domain names for a reason. They also both have short names because they need to hide in the botnet code. LemonDuck has grown by spreading through emails, exploits, and even over a USB drive. Once established it will always try to contact its command and control (C2) servers. If we properly monitor our networks, then we will be alerted about this communication, and we can stop it before it causes any more damage. We want to stop malware before it enters the network but if malware somehow slips by, we need our security software to alert us as soon as possible.

3

## Phishing Campaigns Evolve

Attachments usually go for the low-hanging fruit. This means, if the attackers can create a phish that catches just enough users, then they will continue this phishing campaign. We usually catch on quick but so do they. The attackers will try to change different parts of the phishing emails to obfuscate it in order to bypass email protection. They will try using JavaScript with Base64 encoding, then converting to different encoding methods, and we sometimes see this done multiple times, all to prevent deobfuscation and bypass protections. You can easily prevent the phish from becoming successful. Always check with the sender of an email before opening an unexpected attachment or link. Also, we recommend training to spot a phishing email as this goes a long way in keeping your email system secure.

# Endpoint Threat Trends

WatchGuard

# Endpoint Threat Trends

Every quarter, the WatchGuard Threat Lab ingests endpoint data from our Endpoint Protection, Detection, and Response (EPDR) service, including Panda Security's AD360 service, which is part of WatchGuard. Endpoints are the physical network components used to communicate within a network. Examples include desktops, laptops, servers, phones, and virtual machines. If it can communicate with another device, it's an endpoint. WatchGuard's EPDR detects abnormal behavior and prevents malicious action from taking place at the source – the endpoint.

This section highlights the trends within the endpoint data, so decision-makers can digest historical malware trends to give insight into future cyber-defensive decisions. We are grateful for the anonymous data we receive, as it allows us to aggregate, analyze, and relay it back to the cybersecurity community to understand the threat landscape better. This quarter we are happy to announce that we have added ransomware-related data external to the EPDR data we receive. We are excited to share it with you and continue building on the data set in future iterations of the report. Let's get started!

## Malware Frequency

The Malware Frequency section showcases the overall detections from all endpoints and extracts the trend within the data. A detection occurs when an endpoint observes malicious or suspicious activity and blocks it based on a signature, heuristic or behavior. This quarter's overall detections were down 8% from the prior quarter, continuing the trend from Q1. However, detections from Q1 to Q2 saw an 18% reduction, a significant difference from this quarter's 8%. You can observe the bottoming-out effect of detections in Figure 16.

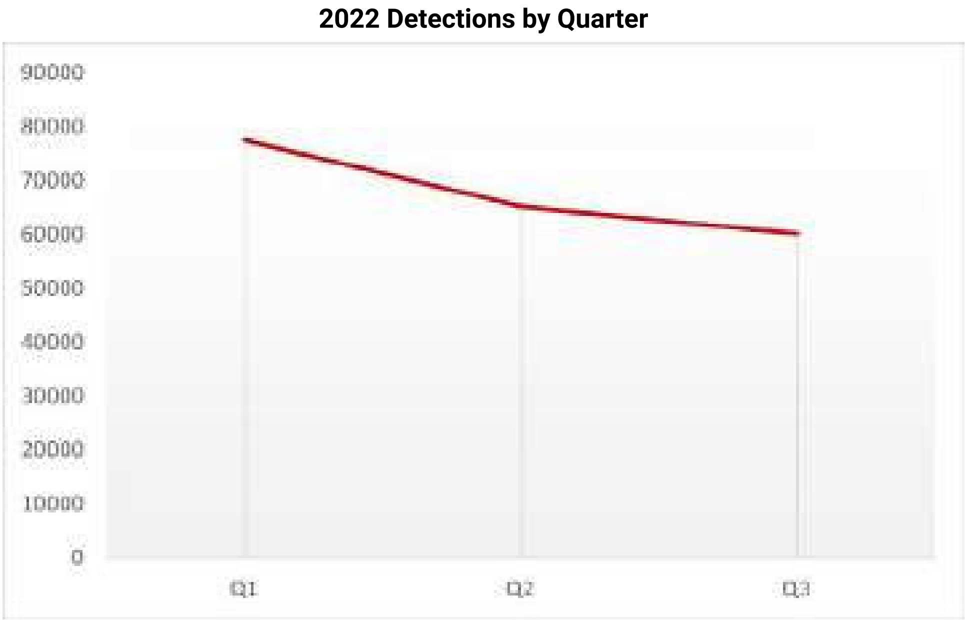


*Figure 16: 2022 Total Detections by Quarter*

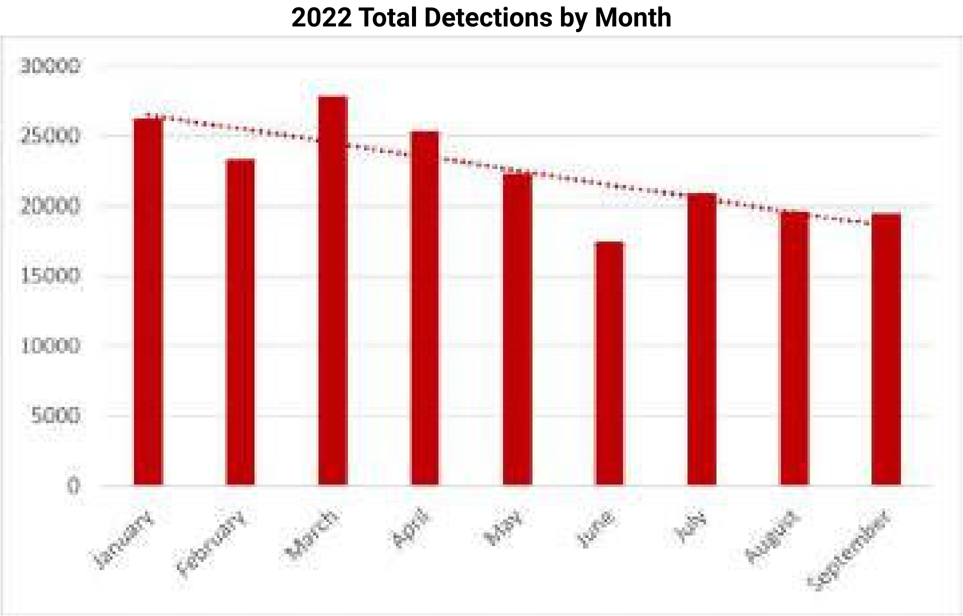


*Figure 17: 2022 Total Detections by Month*

## Malware Origin

Each quarter, we break down the overall detections from each quarter into, what we call, attack vectors. Based on the activity of a file or process, we group them into their appropriate attack vector, which dynamically changes every quarter. The usual attack vectors from quarter to quarter are Adobe Acrobat, Browsers, Nvidia, Office, Scripts, and Windows. Previously, we included attack vectors such as Java, AutoKMS, and Remote Services. However, based on our inclusion criteria of at least 100 detections, no other attack vector is included this quarter. However, we have introduced an “other” category that includes “everything else.” More information about each attack vector is below.

## 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.

**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 stored credit cards – making them common targets for information-stealing malware.

**Nvidia** – Nvidia is a corporation that designs and manufactures 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, or processor, 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 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 didn't fit any other category. This includes AutoKMS tools, Remote Services, and third-party applications, among many others that change every quarter.

**Scripts** – Scripts, which always invoke the most detections each quarter, are those files derived from a scripting programming language. Malware utilizes PowerShell, Python, Bash, and AutoIT scripts to download other malware and deliver payloads, among others. 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 attack vector. It contains the most detections but not in the highest quantities. The files included under the Windows name are those that ship with the Windows operating system. Examples include explorer.exe, msiexec.exe, rundll32.exe, and notepad.exe. Trojans commonly impersonate these files or inject malicious code into them because they exist on every Windows machine out of the box and are inherently trusted.

## Attack Vector Detections

Although the overall detections have decreased, that doesn't tell the whole story. Typically, Scripts are responsible for over 80% of all quarterly detections, often even 90%. A vast majority of the Scripts detections are from PowerShell. Thus, PowerShell is responsible for a majority of all detections each quarter. In Q3, 83% of all detections were from the Scripts attack vector, driven primarily by PowerShell detections. Windows follows with 12% of all detections. Then, Browsers with 3% and Office and Acrobat with 1% each. Finally, Nvidia and the Other category comprise less than 1% of all detections. These numbers can be observed in Figure 18.

Considering the Scripts attack vector overshadows the detection numbers of the other categories, we've decided to include another figure of the attack vectors – Figure 19 – with PowerShell detections removed from Scripts. Suddenly, Windows becomes the dominant attack vector with 67% of all detections, and the other attack vectors show more of themselves. Browsers now contain 15% of all detections, and we can see that Acrobat edges out Office with 6% of detections as opposed to 5%, respectively. The other categories contain less than 5% of all detections, including Scripts at 2%! This data shows that PowerShell is the method of choice for threat actors against endpoints.

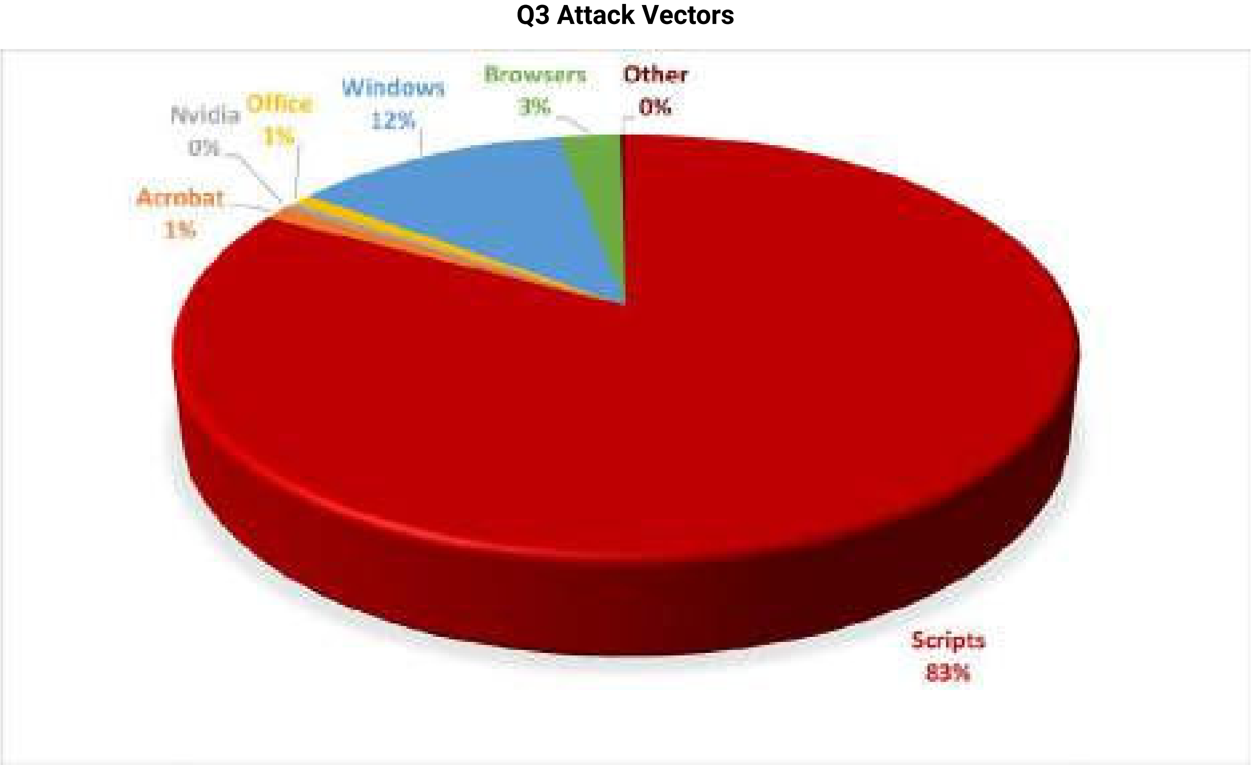


*Figure 18: Q3 Attack Vectors*

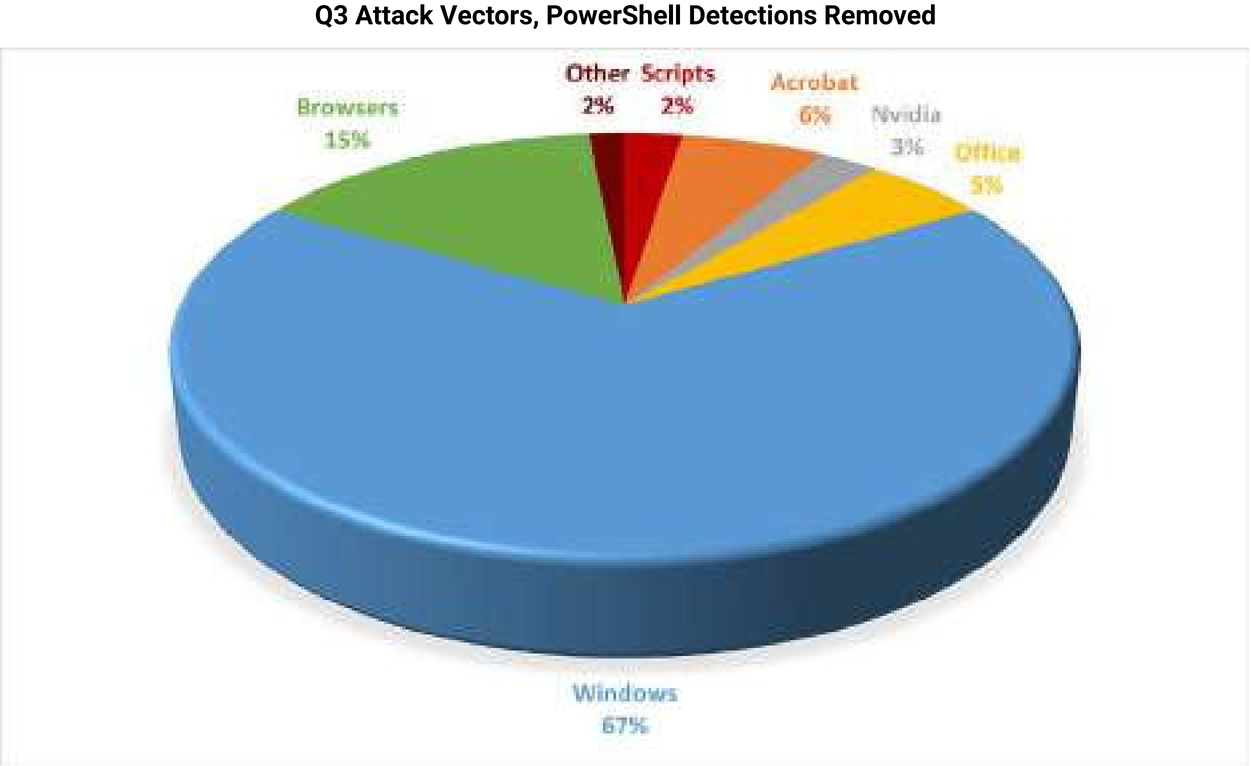


*Figure 19: Q3 Attack Vectors, PowerShell Detections Removed*

To get a more granular view of the detections, we've also included Figure 20, showing the number of detections for each attack vector by quarter. As stated prior, the overall detections have reduced from Q1 to Q2 and from Q2 to Q3. Looking at Figure 20, Scripts have followed this same trend. This is because Scripts (PowerShell) skew the data. The only other attack vector that declined from Q2 to Q3 was Office detections. Every other attack increased.

**2022 Attack Vectors by Quarter**

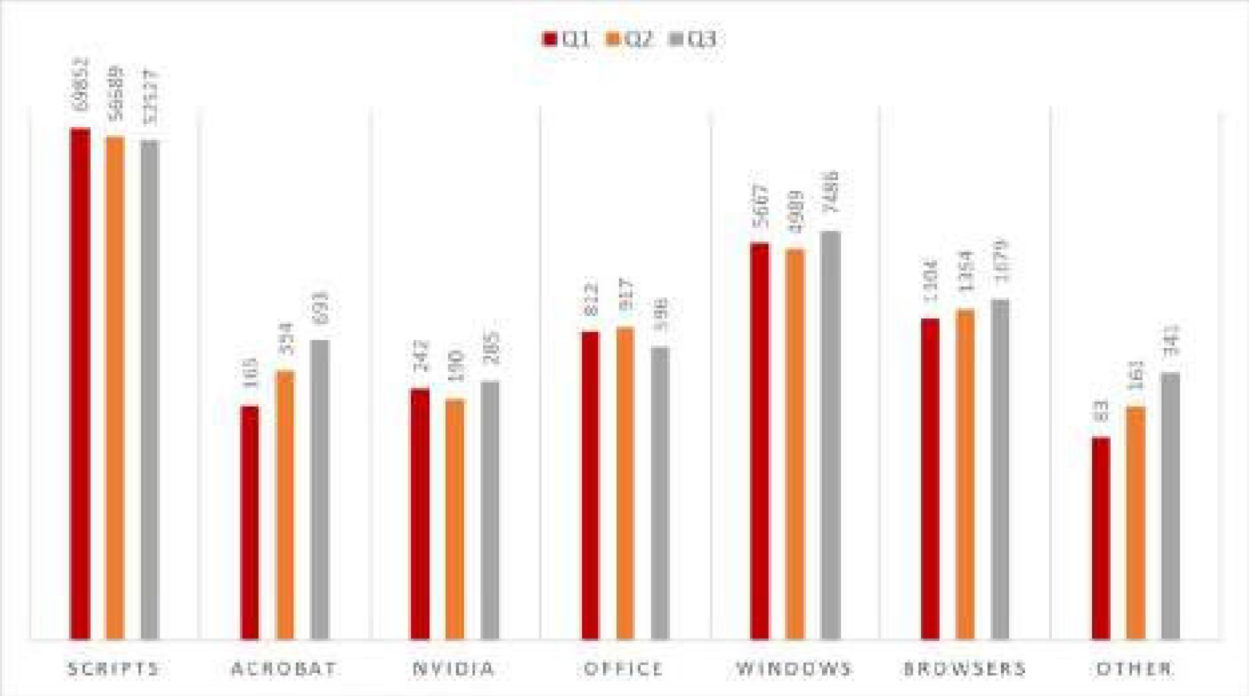


***Figure 20: 2022 Attack Vectors by Quarter***

Detections were slightly up from the prior quarter, continuing their climbing trend. Nvidia detections have increased after decreasing from Q1 to Q2. Windows-based detections have increased by 50%, following Nvidia in reversing a declining trend. Acrobat and Other have effectively doubled quarter over quarter this year. We don't anticipate that those two attack vectors will double again next quarter, but you never know. Looking at Figures 19 and 20, we can see that the overall detections don't tell the whole story. Obscuring PowerShell detections and looking at individual attack vectors allows us to discover underlying trends. One of these underlying trends is diving into the Browser attack vector to understand which web browser threat actors prefer in their attacks.

## Browser Malware Detections

The browsers we have detections from this quarter are Internet Explorer (IE), Firefox, Chrome, Edge, Opera, and, for the very first time, Brave. The Brave browser is a privacy-focused browser derived from the open-source Chromium project. Users of the browser tend to be cryptocurrency aficionados because of its built-in cryptocurrency wallet and implementation of Basic Attention Tokens (BAT). BAT is the native currency of the browser, and users can earn BAT for viewing privacy-based content (ads) and opt to pay content creators for their services, all within the browser. However, since there was only one Brave detection and a combined 11 detections between Opera and Edge, we have decided to bundle these three together.

IE and Firefox continue to lead the way with 43% and 39% of all browser detections, respectively. Chrome is responsible for about 17% of all detections. The bundled trio of Brave, Edge, and Opera combine for 1% of all detections with a measly 12 total detections between the three. Figure 6 shows these numbers. It's important to note that IE has seen a slight but steady increase in detections since the end-of-life support on June 15th of this year. Due to this, we anticipate that detections from IE will continue to rise steadily in the short term.

**Q3 Browser Malware Detections**

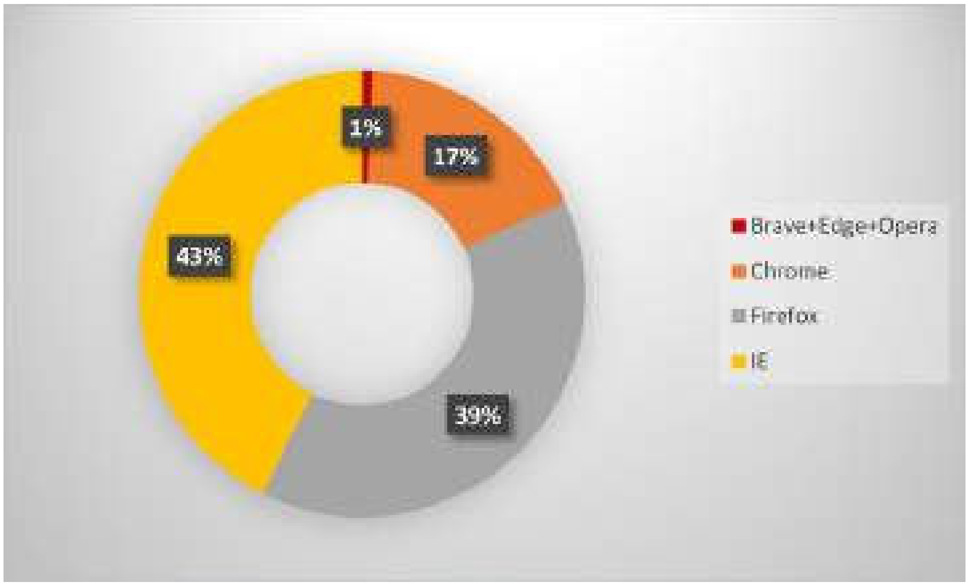


*Figure 21: Q3 Browser Malware Detections*

## Mozilla Detections

In addition to a large composition of Firefox detections, we've discovered another trend within the browser data – an increase in Mozilla detections. In June, we saw a noticeable rise in detections related to Thunderbird, Mozilla's email client, and Ping Sender, Mozilla's telemetry service for Firefox. We assumed it was a one-off event because it only occurred in June. However, these detections not only persisted, but we detected a noticeable increase in detections through all of Q3. Figure 22 and Figure 23 show the monthly and quarterly detection rates for Mozilla. These detections comprise about 1% of all detections, so it's not an immediate cause for concern, but it is something the WatchGuard Security Team is monitoring going forward.

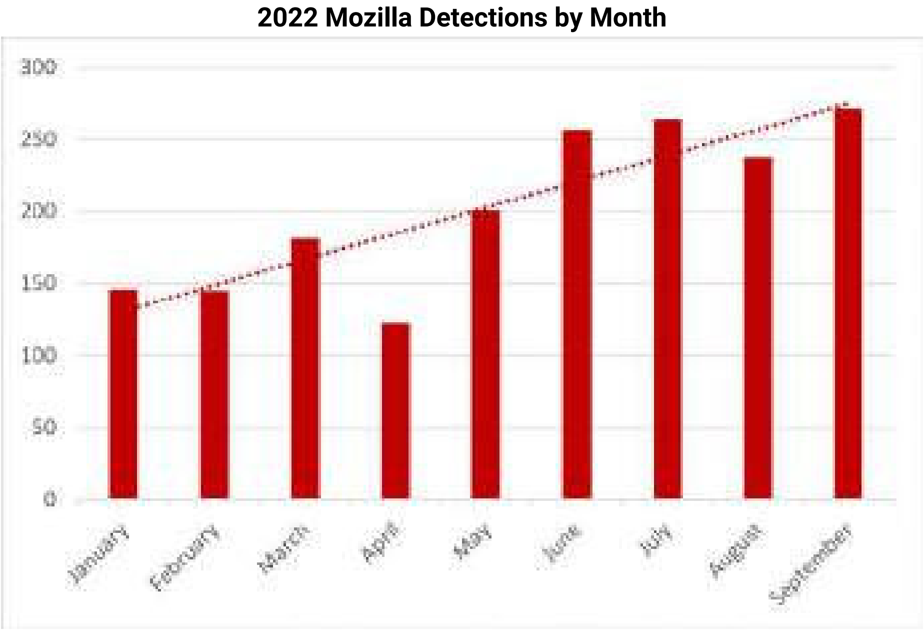


*Figure 22: 2022 Mozilla Detections by Month*

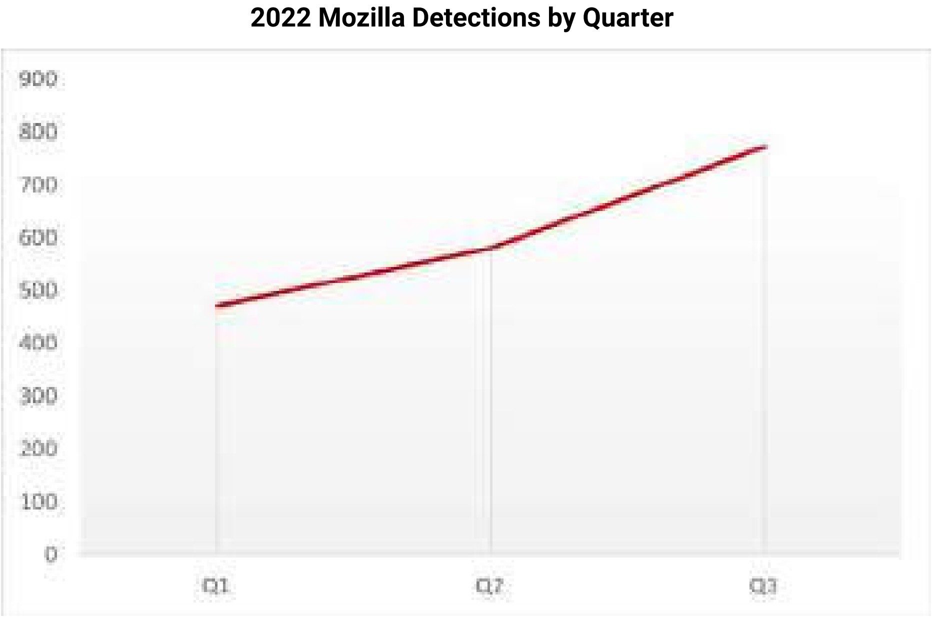


*Figure 23: 2022 Mozilla Detections by Quarter*

## Cryptominers

Detections of cryptominers have drastically reduced in Q3. The rate of detections for cryptominers has been steadily decreasing quarter over quarter, with around an 8% reduction on average. However, from Q2 to Q3, the rate of detection reduced by 72%. The cause for this is likely more apparent than not. The market capitalization of cryptocurrency has decreased drastically. In addition, threat actors no longer use cryptominers as a stand-alone mechanism. Attackers commonly bundle cryptominers with other information-stealing malware and, thus, are labeled as information stealers instead of just cryptominers. If this trend continues, we will likely phase out this section in Q1 of 2023.

**Cryptominer Detections by Quarter**

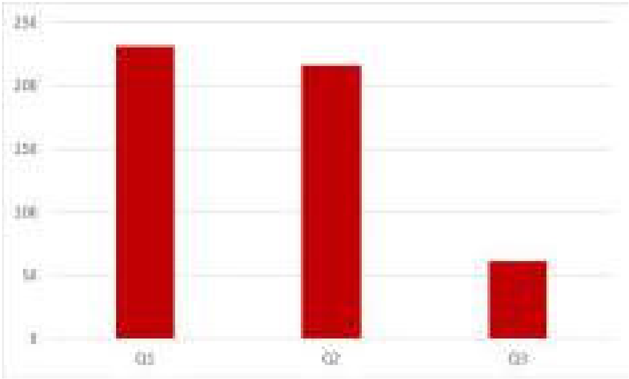


*Figure 24: Cryptominer Detections by Quarter*

## Ransomware Landscape

Unfortunately, ransomware continues to wreak havoc on organizations from all industries. In Q1, we saw a record number of ransomware detections for any quarter. It surpassed the annual total of the entire year prior. Although the numbers aren't that high, they exceed average ransomware detections for a quarter. Considering Q1 was a record quarter, it was only standard for detections to decrease the next quarter. However, Q3 saw much higher than average detections. Figure 25 displays the ransomware detections by quarter.

**Ransomware Detections by Quarter**

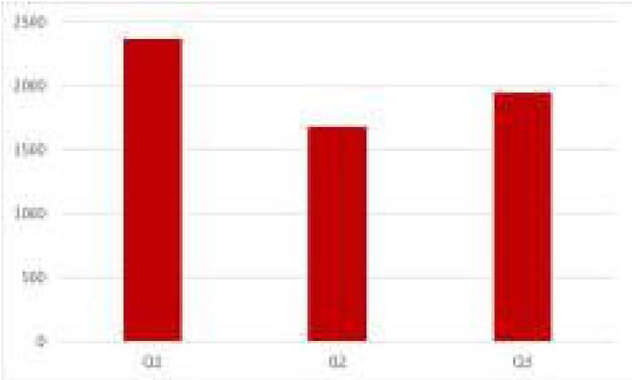


*Figure 25: Ransomware Detections by Quarter*

## Extortion Groups

It seems every day a new ransomware or extortion group appears on the dark web with alleged stolen documents from a ransomware deployment. This quarter, we're excited to announce that we have begun a concerted effort to track current ransomware extortion groups and build our threat intelligence capabilities to provide more ransomware-related information in future reports. Figure 26 shows the known public extortions by well-known ransomware groups that we discovered in Q3. LockBit, with well over 1,000 public extortions, had over 200 in Q3 alone. Other active groups are Basta (Black Basta/Basta News), BlackCat (ALPHV), Hive Leaks, Bian Lian, Avos Locker, and Vice Society. As you can see in the figure, many more contributed to the chaos aside from these groups.

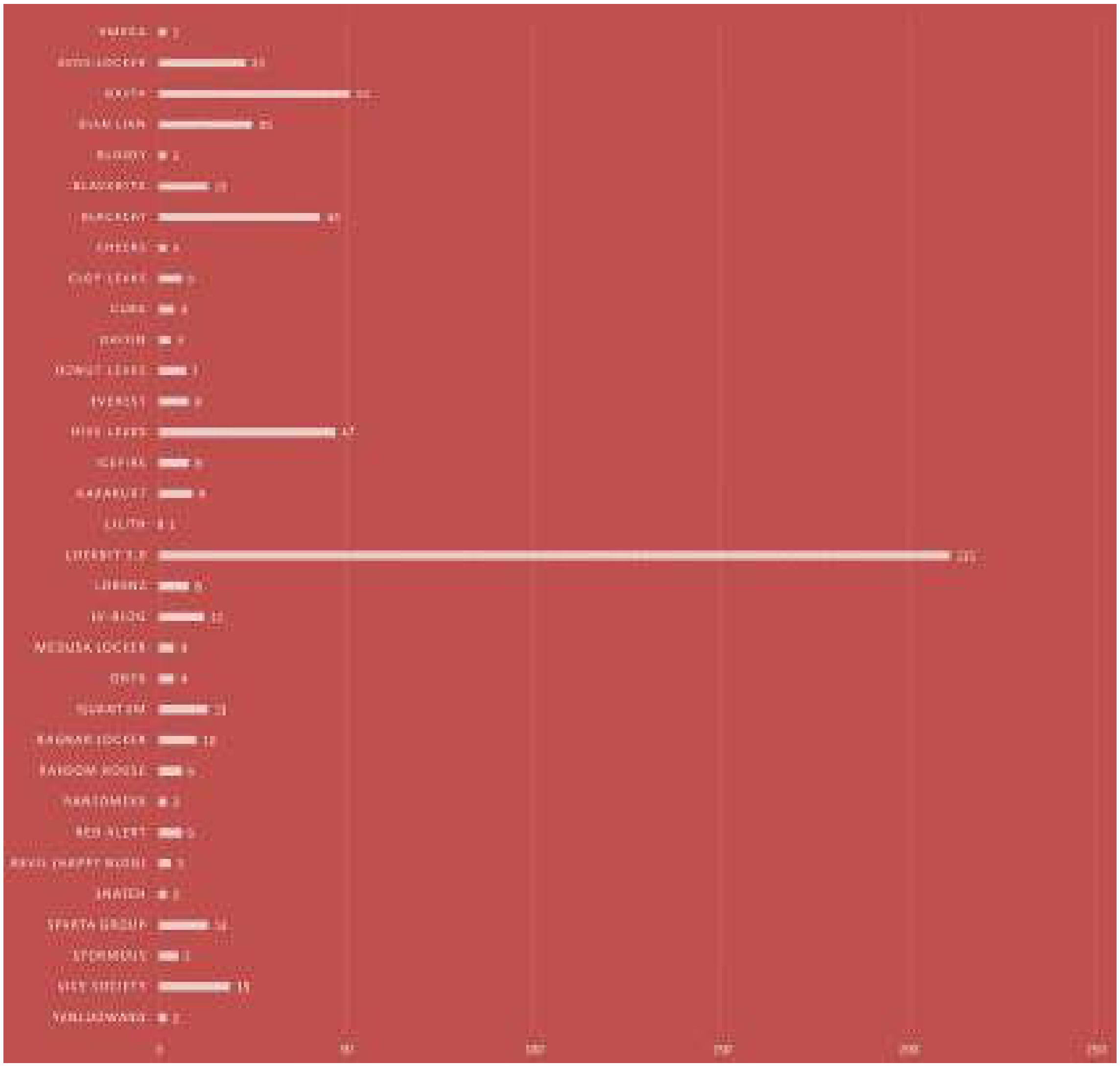


*Figure 26: Extortion Groups*

## New Ransomware

In addition to tracking the current ransomware extortion groups, the WatchGuard Security Team is also now tracking new ransomware in the wild. For this quarter, we have detected 23 new ransomware (groups). Six of these groups posted public extortions on their extortion web pages – 0mega, Bian Lian, Bl00dy, Donut Leaks, Lilith, and Red Alert. You will see in Q4 that one of these groups has caused a lot of destruction since being newly discovered in Q3. Hint, the name starts with ‘R’ and is in Figure 27 to the right.

| Ransomware Name |
|---|
| 0mega |
| ARCrypter (ChileLocker) |
| Bian Lian |
| Bisamware |
| Bl00dy |
| DAGON Locker |
| DataBankasi |
| Donut Leaks |
| FileRec |
| GwinsinLocker |
| H0lyGh0st |
| Lilith |
| Luna |
| MeowCorp |
| Moisha |
| NewWave (N3ww4v3) |
| Prestige |
| Raptor |
| Red Alert |
| Rever |
| Royal |
| Stop 24/7 |
| TheGodFather83 |

*Figure 27: Q3 Newly Discovered Ransomware*

## Key Findings

This final subsection serves as a summary of key findings:

- Overall detections have declined by 8% from Q2 to Q3, continuing the trend from Q1 –albeit at a slower rate (18% decline from Q1 to Q2).
- We now include detections that don’t fit within an attack vector. We have labeled this as “Other” and include detections from AutoKMS tools, remote access services, and third-party applications, among several others.
- Scripts still lead the pack with 83% of all detections.
- The only other attack vector that decreased from Q2 to Q3 is Office. All other attack vectors increased from the quarter prior.
- Windows detections are up 50% from Q2 to Q3, reversing the declining trend from Q1 to Q2.
- Acrobat and Other have effectively doubled quarter over quarter this year.
- Firefox and IE continue to be the browsers of choice for attackers.
- Since IE reached the end of life on June 15th of this year, we have noticed a slight increase each month, and we anticipate this to continue in the short term.
- Scripts have a lower detection rate from the previous quarter, and since PowerShell is responsible for about three-fourths of all detections, this has skewed the data.
- In addition to Firefox, we noticed an uptick in detections with Mozilla services, primarily Thunderbird and Firefox’s telemetry service – Ping Sender.
- Cryptominer detections decreased by 72% from Q2 to Q3. We predict this is because of the current state of the cryptocurrency market and the fact that information-stealing malware utilizes cryptominers as a tool.
- If the trend with cryptominers continues, we anticipate phasing this section out.
- Ransomware detections by EDPR continue to remain relatively high.
- We have introduced new ransomware-related threat intelligence information in the form of extortion groups and newly discovered ransomware.
- LockBit had over 200 public extortions on their dark web page, almost quadruple more than the next group, Basta.
- We discovered 23 new ransomware (groups), 6 of which posted public extortions on their dark web page.

# Top Security Incident

# Top Security Incident

## EvilProxy

Multi-factor authentication (MFA) adoption is slowly starting to pick up steam across the modern world, largely thanks to reduced management complexity in the business world and normalization by the likes of Apple and Google in the personal world. If you follow any security advisories from organizations like CISA or the threat research teams of security vendors, you're probably already numb to seeing "use MFA everywhere" as a leading bullet point in mitigation recommendations.

Its undeniable that MFA is the single best technology you can deploy to protect against the bulk of authentication attacks. Unfortunately, MFA on its own is not a silver bullet against all attack vectors and cyber adversaries have made that clear with the rapid rise and commoditization of adversary-in-the-middle (AitM) attacks. In September of 2022, adversaries released an AitM toolkit called EvilProxy, which significantly lowered the barrier for what was previously a sophisticated attack technique.

### Basic Authentication Attacks

The underground market for sharing and selling stolen credentials is flourishing. Freely shared collections containing billions of usernames and passwords have enabled waves of authentication attacks against organizations. Password spraying (trying common passwords against an account) and credential stuffing (taking a stolen username and password from one app and using it to log in to another one) have disappointingly high success rates largely thanks to end users' inability or unwillingness to maintain strong and unique passwords for individual accounts.

Despite the efforts of Microsoft and other tech behemoths to kill off password-based authentication, passwords remain a popular factor for most users. MFA, when deployed correctly, can make basic authentication attacks like password spraying and credential stuffing significantly more difficult to succeed by making a stolen password not enough on its own to log in to an account. This hardened barrier has forced cyber threat actors to devote more resources and apply a "human touch" of social engineering to successfully compromise an account.

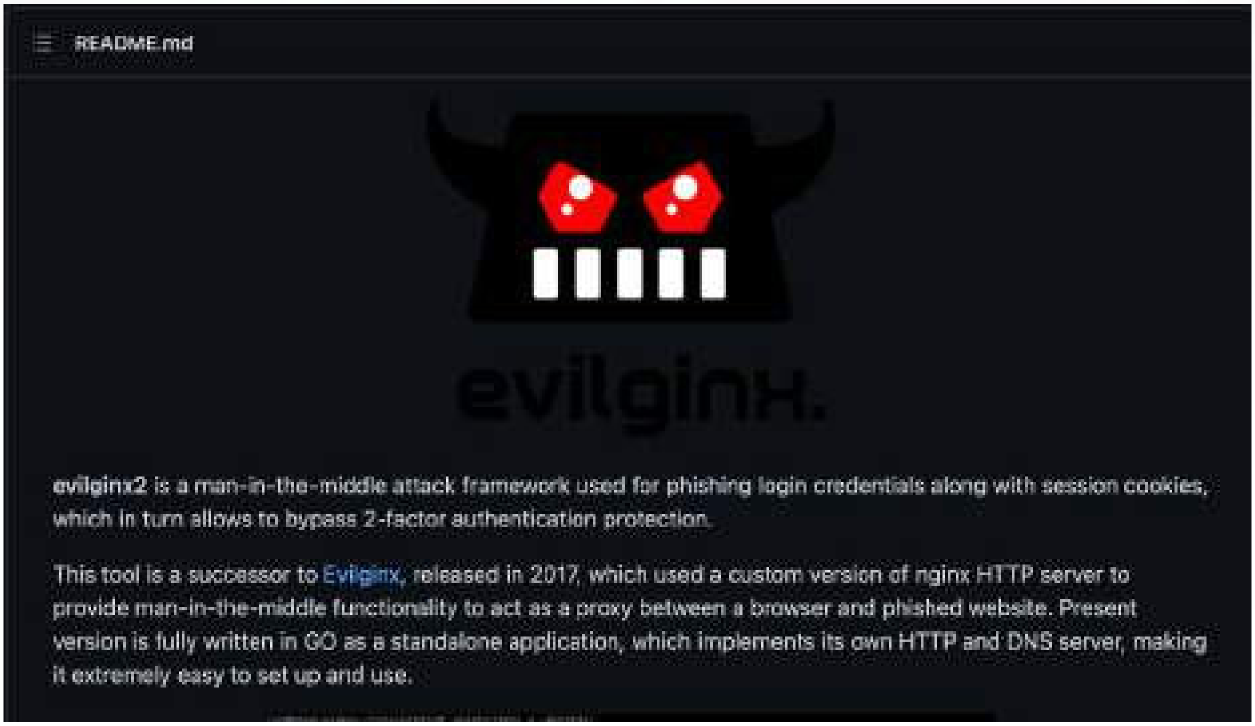
### Social Engineering in Authentication Attacks

On September 15, 2022, Uber publicly announced they were responding to a cybersecurity incident after screenshots of their internal Slack system began circulating online showing an alleged malicious hacker announcing his presence publicly to the whole company. The individual went on to take screenshots of various internal systems as well as comment on open bug bounty reports in Uber's HackerOne portal. As the dust settled, the individual disclosed they had obtained their access through a social engineering technique known as "push bombing." After obtaining an Uber employee's password, likely by purchasing it from an underground marketplace as was this threat actor's modus operandi, they repeatedly tried to log into the employee's account, triggering a deluge of MFA push notifications as the second authentication factor. The attacker then contacted the employee through WhatsApp, posing as Uber IT support, and instructed them to accept the prompt. This attack against Uber was an unfortunately perfect example of MFA as a great tool to protect against authentication attacks while being vulnerable to social engineering.

Social engineering luckily does not typically scale well. Any time an adversary must personally perform some action like sending a chat message or making a phone call both reduces the chance of success and increases their time investment into the attack. This has, until recently, left MFA circumvention as a relatively sophisticated and limited style of attack.

## Phishing in Authentication Attacks

Basic phishing attacks are a popular method for collecting credentials before an attack against an organization. Through previous versions of this report, we've highlighted popular phishing domains disguised to look like a legitimate authentication portal for apps like Microsoft 365 or Google. While this style of phishing can easily snatch a valid username and password from an unaware victim, they historically have not solved the issue of breaking into MFA-enabled accounts. In recognition of this limitation, cyber adversaries have started pivoting to more sophisticated adversary-in-the-middle techniques that place them in a position where they can not only trick users into giving up their passwords, but also complete an actual authentication with the targeted application and retrieve a valid authenticated session cookie.



**evilginx2** is a man-in-the-middle attack framework used for phishing login credentials along with session cookies, which in turn allows to bypass 2-factor authentication protection.

This tool is a successor to Evilginx, released in 2017, which used a custom version of nginx HTTP server to provide man-in-the-middle functionality to act as a proxy between a browser and phished website. Present version is fully written in GO as a standalone application, which implements its own HTTP and DNS server, making it extremely easy to set up and use.

***Figure 28: Evilnginx Github Page***

One example toolkit that attackers have used is Evilnginx (not to be confused with the commoditized EvilProxy we'll dive into later).  Evilnginx, originally released in 2017 and re-released as Evilnginx2 in 2018, is a reverse proxy application, allowing an attacker to place themselves in the middle of a phishing victim and a legitimate application. It comes with a few pre-configured targets like Google, Microsoft365, or Apple where the tool knows the authentication flow logic and can easily forward web requests back and forth between the victim and the target application while spying on the details in the middle.

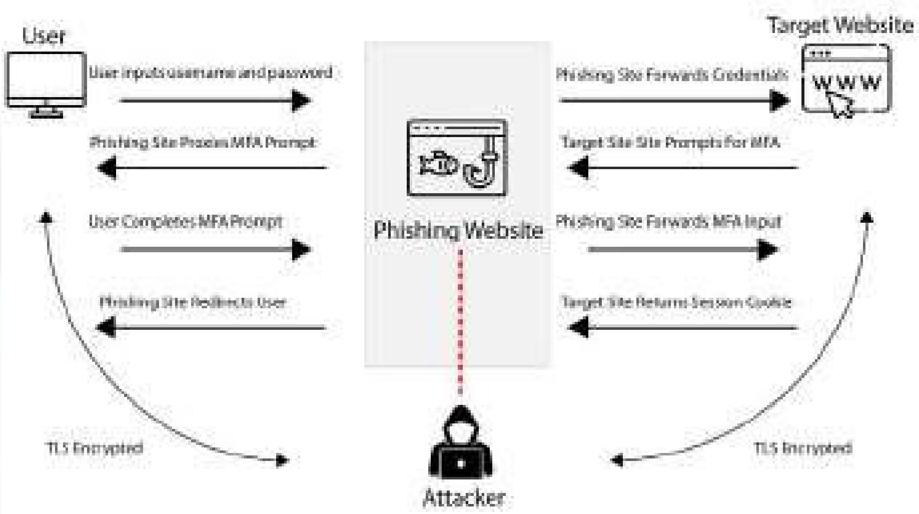

User
Target Website
User inputs username and password
Phishing Site Forwards Credentials
WWW
Phishing Site Proxies MFA Prompt
Target Site Site Prompts For MFA
User Completes MFA Prompt
Phishing Website
Phishing Site Forwards MFA Input
Phishing Site Redirects User
Target Site Returns Session Cookie
TLS Encrypted
TLS Encrypted
Attacker

*Figure 29: Evilnginx deployment architecture*

Even with its rich set of preconfigured targets, EvilNginx still requires a bit of technical skill to deploy and configure. This has for the most part limited the type of malicious hacker that can successfully utilize it in an authentication attack against a victim user or organization. Unfortunately, as we often see with relatively sophisticated attacks, the tech behind EvilNginx has now been commoditized and made available for sale on the underground as a toolkit known as EvilProxy.

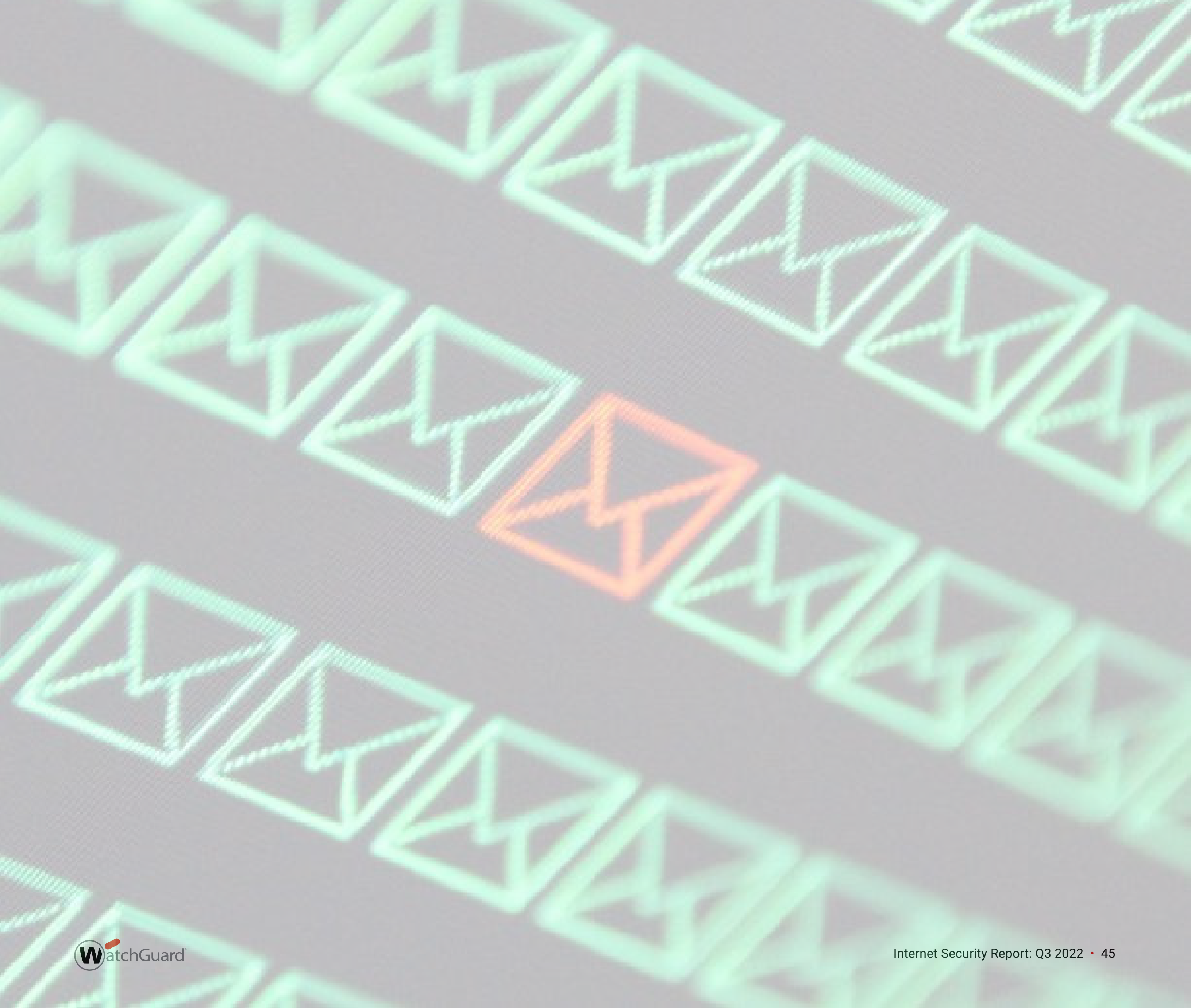
## EvilProxy

EvilProxy first popped up for sale on an underground hacking forum in July 2022. The service advertised itself as a full-suite Phishing as a Service (PaaS) program for “security awareness programs.” For a few hundred dollars in cryptocurrency, the EvilProxy developers will create and license out a pre-configured proxy deployment for a specific target (Google, Microsoft, etc), a management console for visibility into successful attacks, and a domain manager to easily manage phishing domains.

*Figure 30: EvilProxy service listing*

This commoditized offering, like the Ransomware as a Service (RaaS) offerings made popular in recent years, significantly lowered the barrier of entry for executing an adversary-in-the-middle attack. With EvilProxy, a cybercriminal doesn't need any web development or management experience and only needs to create the phishing email itself. In a successful attack, the adversary would receive not only a valid username and password, but an authenticated session cookie which they could then use to hijack the victim's account even if MFA is enabled. Meanwhile, to the victim it looks like they logged into the normal app with nothing out of the ordinary if they aren't paying close attention to the browser URL.

Any time a complex cyberattack technique becomes packaged up and sold, it enables a wider range of criminals to execute attacks, which ultimately leads to more indiscriminate attacks against organizations of any size. What previously may have only affected larger organizations, is now simplified enough to be target smaller businesses while remaining economical for the attackers.



# 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.

1

## Phishing Awareness Training Is More Important Now Than Ever

Attackers must aquire tools to steal and use stolen credentials at scale. EvilProxy and similar toolkits allow attackers to circumvent MFA protections without having to individually interact with each victim. While there are technical controls you can use to help protect against some common phishing techniques, nothing beats an end user that is both aware of social engineering tactics and bought into an organization's security program. Make sure phishing awareness and overall security awareness are available and engaging enough to train your users on spotting common social engineering techniques.

2

## Use Tools That Can Neuter Malicious URLs

Even with a robust phishing awareness program, you will never realistically get your click rate down to 0. You'll always need technical tools in place to pick up the slack where your user training fails. Tools that can spot and block or neuter malicious URLs in phishing emails and text messages can be that important line of defense to protect users that are tricked into clicking a link. There are many options out there, but some of ours include DNS firewall's like DNSWatch, or our Firebox network security services like WebBlocker, which can block malicious sites in addition to its productivity features. We even offer endpoint-based tools in products like Adaptive Defense 360 (AD360) or WatchGuard Endpoint Protection Detection and Response (EPDR). Whether you use our or other vendors' tools, layering network and endpoint options improves your protection.

3

## MFA Isn't Perfect, But It's Still Critically Important

Push bombing and adversary-in-the-middle toolkits prove that there are still ways for cyber threat actors to circumvent MFA-protected accounts. Just because MFA isn't a silver bullet though, doesn't mean organizations shouldn't deploy it fully wherever possible. Cybersecurity is a game of reducing and mitigating risk wherever possible and MFA remains one of the best tools available to make authentication attacks significantly more difficult to succeed. Fully deploying MFA across your organization, to every user and supported service, should be a top priority.

# Conclusion & Defense Highlights

WatchGuard

# Conclusion & Defense Highlights

As mentioned in the intro, everyone (hopefully) plans but few plans survive the first encounter with your adversary. Even if you are a super-experienced defender, we often miss things in our initial plans, or simply don't realize new tactics a threat actor may have changed to get past our previous defenses. Your plan must evolve as you learn how the adversary will adjust to it. Hopefully, this quarter's report gave you enough insight to adjust plan A of your defense strategy.

For example, even though it appears malware and network attacks are down, we are seeing a big growth of these attacks in encrypted network traffic. In fact, the volume of encrypted threats may even be smaller than it seems, simply because so few administrators scan that traffic today. This is a perfect example of a change needed to your defense strategy if you aren't already one of the few scanning this traffic.

With that in mind, here are a few final learnings and defense tips from the threat trends we covered in this report.

## Securely scan encrypted traffic, whether at the network or endpoint

I know we sounds like a skipping record here, as we make this tip very often in many of our quarterly security reports. However, we repeat it because the trends continue to prove malware evading network detection via encrypted connections is a big deal, and many people still aren't solving for this problem, at least on a network level.

The first part of the tip is that we highly recommend you enable the Firebox's HTTPS scanning capability, even if it requires work and tuning to get right. We know the huge majority (~80%) of malware arrives over encrypted channels, so you are missing a chance to catch most threats early if you don't do this. It is totally worth the effort.

That said, if you aren't going to do this at a network level, at least be sure to deploy multiple layers of good endpoint protection, including an advanced endpoint protection (EPP) and detection and response (EDR) solution, such as WatchGuard EPDR (or AD360). Traffic is decrypted naturally at the endpoint, so these solutions will have a chance to block encrypted threats later in the cyber kill chain. You need at least one solution that has a chance to catch encrypted threats. Having said that, even the most advanced endpoint protection suite is not perfect, which is why we still strongly recommend the additional layer of scanning at the network level, before threats even have a chance to touch the endpoint.

## Communicate policy against piracy

Not only does piracy not pay; it absolutely costs, often in more ways than one. During the quarter, and of course in previous ones, we have seen threat actors include malware in pirated software or the cracking software used to steal programs. People deserve money for their work if you are going to use it, so obviously you should pay for your organization's software. Not only is it wrong to pirate, but if done at an organizational level, it could cost in fines and legal feels, let alone other consequences. However, morality and legality aside, it would suck to also learn a pirate product is what caused your organization to have a data breach, which could cost you tens of thousands – if not more – in breach costs as well.

Usually, piracy in a business is not institutional, rather it's often the act of one user who somehow is self-justifying it to get something done quickly. You need to both communicate and guard against this. As an information security expert, you probably already have created an acceptable use policy for employees of your organization. Make sure you have paragraphs in there warning against pirating software and servers. While most people should honor that policy purely on ethics, you also so make sure to mention pirated software has hidden costs. Warn that much of the pirated software easily found on the Internet tends to include hidden malware. Make this "pirated potentially equals dangerous cyber risk" idea a core part of your security awareness training.

## Your Business Continuity / Disaster Recovery (BCDR) plan is plan Z

This last tip doesn't coincide with any particular trend this quarter but is an excellent reminder that matches the introduction and theme of the report; plan A is never perfect, and that's why you need to invest in and test your BCDR plan.

Sure, your goal as a defender is to try and prevent any threat from affecting your business, and we share the trends from the report in hopes that data about the latest threats helps you do that. However, no one is perfect, and adversaries can be good at their activities too. While you want to win the war, you will never win every battle. That's why you really need to make sure you are planning for the day that you miss something and must recover systems and your business despite your best prevention efforts.

If you don't have a plan on bringing back all your critical business systems in the event of the worst disaster, you really need to make one. It's not just to withstand cyberattacks, but natural disasters and other tragedies too. If you must lose a battle, knowing you can recover quickly and not lose the whole war really helps. There are many guides to starting your recovery plan, but here's a **good overview for SMBs**, if you really are starting from scratch.

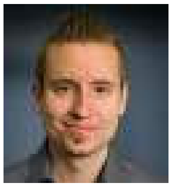
That said, I'm guessing most of you at least have a basic recovery plan, so step two to your BCDR maturity is updating it every year, and step three is making sure to test it. In fact, testing your plan is the best way to help with updates. As the intro of this report suggested, no new plan survives its first use without some new learning about something you might have missed. Regular tabletop tests of your plan can help you identify what works well, but also find areas you may have missed until the test made them apparent. So don't just write a BCDR policy and wait until the first disaster to see if it works. Give it a few run-throughs to find out what you can improve.

That covers the threat we saw during Q3 2022. We hope you were able to find some additional tweaks to your defenses from the analysis found in this report. At the very least, we hope it at least shows the solutions you have in place are doing their jobs. Make sure to check back every quarter as there are always attack evolutions that will force us to rethink and alter our current defense plans. 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 Stuifbergen

*Intrusion Analyst*

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

**About WatchGuard Threat Lab**

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

**About WatchGuard Technologies**

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

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