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

– John "Chris" Inglis, the White House National Cyber Director

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

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

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

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

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

Our Q2 2022 report includes:

Executive Summary

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

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

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

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

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

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