Introduction

After a very difficult 2020, filled with the pandemic, global political strife and regional societal conflicts, everyone was looking for a fresh start in 2021. Not only did last year's global discord affect us all personally, but it also brought changes to the IT world that resulted in new threat landscape trends, which required reimagined protections. Unfortunately, global events of last year's proportion don't reverse overnight, so things did not go back to normal in Q1 (and we'll likely see a new normal going forward anyway). That said, there is light at the end of the tunnel. Buddha said, "No matter how hard the past is, you can always begin again," which reminds us we can always start fresh to improve our cybersecurity anytime we want, new year or not.

As mentioned, 2021 didn't reverse the 2020 remote work trends overnight—far from it. As I write this in late Q2, remote work is still the norm among knowledge-based organizations. The good news is a return to some normalcy seems on the horizon in North America. While there are still areas of the world that will take more time to recover, we suspect many knowledge-based workers will have the option to return to the office in Q3. Does that mean office work will return to its normal level? Probably not, but we do expect to see a much better ratio of people working behind the network perimeter soon.

Why does this matter to security? The 2020 change in remote workforce had huge implications in how IT does cybersecurity and even affected the malware and network attack trends we see every quarter. At a high-level, we saw less malware detected at the network perimeter every quarter following the pandemic. However, that does not mean overall malware is down. Malware detected by endpoint security increased, following the remote workers and their devices home.

That also doesn't mean perimeter security dies with more remote work. As malware dropped, network attacks rose on the perimeter, plateauing to a three-year high in Q1 2021. Even if users moved home, the adversary realizes all our servers and supporting services still reside in our offices or our Clouds. We saw network attacks increase almost every quarter throughout the pandemic.

The Latest Firebox Feed Threat Trends

With a new year and a recovering world, you might wonder if these threat trends will start to revert to normal this year. We don't think they will. As mentioned, it'll still take a few quarters for the whole world to recover from the pandemic. Not only did Q1 see similar threat trends as 2020, but we also expect these trends to continue for Q2 and even much of Q3. I don't think our trends will really "normalize" again until 2022.

Even then, don't expect the world to go completely back to normal either. We expect to see a new normal develop. Hybrid work, with employees spending part time in the office and part time remote, seems like a new standard among tech companies. This new work habit will greatly change how attacks evolve and where you see those attacks. That also means you'll have to change the way you deliver various protections. In short, the pandemic still affects the threat trends we saw in Q1 2021, and we suspect we'll never completely return to the exact types of threats we saw before it. No worries though; every day is an opportunity for a fresh start.

One of the best ways to get a fresh start on cybersecurity is by getting a fresh perspective of what malicious cybercriminals are doing. The only way to defend yourself against an enemy is to understand how that enemy fights. Our Internet Security Report (ISR) is designed to give you that perspective by covering the latest threat trends we saw last quarter. It covers quantifiable findings we gather from our security products around the world, as well as any internal security research projects or external security stories studied throughout the quarter. Our data comes from a cascade of threat indicators delivered by tens of thousands of WatchGuard Fireboxes, which we analyze to report the most common and widespread cyber threats from last quarter. In short, this fresh threat intelligence and our analysis offer a cutting-edge view into what the adversary targets and how they carry out their malicious attacks. Knowing what the criminals are up to gives you the fresh perspective to figure out how to stop it. We also directly advise you on our top protection strategies throughout this report.

2021 may not have offered an immediate "fresh start" or reset from last year's calamities, but you can always decide to begin anew whenever you want. Regardless of how threat trends might change tomorrow, next year, or even next decade, this report will offer you the insights you need to revive your cybersecurity efforts no matter the changes.

CSO, WatchGuard Technologies

Executive Summary

As mentioned in the intro, we saw the same general network attack and malware trends play out during Q1 as we did for the rest of the pandemic. This means network malware is generally down (with a caveat this quarter), while endpoint malware is up. Meanwhile, network attacks have risen each quarter since the pandemic started. As we've said before, this makes sense as malware follows victims home but network exploits still target servers at the office and in the Cloud.

Despite the reoccurring trends, we also saw some new threat highlights. For instance, zero day malware – which is malware that signature-based detection misses during its first days – rose to an all-time high of 74%. This means signature-based protections missed almost three-fourths of malware during Q1. Unless you deployed a more proactive malware prevention solution, you should expect large amounts of malware to evade legacy defenses. We also saw a huge rise in the amounts of malicious domains our DNSWatch services blocked, in part due to a surge in phishing attacks.

This report covers plenty more, including details on the ProxyLogin zero day, a prevalent Linux malware family targeting IoT devices, a fileless threat delivered via booby-trapped XML scripts and much more.

Here's an executive-level view of the Q1 2020 threat landscape:

- **Zero day malware reached an all-time high of 74% in Q1.** This means you will miss almost three quarters of malware if you rely only on signature-based protections. You need proactive malware detection to survive today's threats. As a reminder, zero day malware is our name for polymorphic, evasive malware that bypasses signature-based protections on day "zero" of its release.
- Overall, **total perimeter malware detection decreased 16%**, with only 17.2 million detections in Q1. However, this stat is deceiving until you consider the drop in reporting Fireboxes. Taking that into account, **Fireboxes saw an average of 461 malware detections per device, which is a slight one point increase in detections.**
- **Five new malware families, Ursu, Trojan.IFrame, XML.JSLoader, Zmutzy, and Zum.Androm, made our top 10 malware volume list**, making it a pretty diverse quarter for new malware samples.
- **Malware sent over encrypted connections dropped to just under 44%** in Q1. That represents a three-point drop from Q4 2020 and ten-point drop from Q3.
- In the past, we've seen more zero day malware pass over encrypted connections than usual. However, during Q1 **only 60.3% of malware spreading over encrypted connections was zero day malware.** This is less than the overall zero day malware percentage this quarter.
- **Network attack volume reached a three-year high.** Network attacks grew to more than **4.2 million IPS hits in Q1**. This level of network attack volume is even more striking considering reporting devices decreased 17%.
- During Q1 2021, Firebox appliances' Intrusion Prevention Service (IPS) blocked **an average of 113 attacks per appliance**, which is a large 47% increase quarter over quarter (QoQ).
- **We only saw about 3% of network attacks in the APAC region.** While the AMER and EMEA region have almost equal network attack by volume, when you normalized to attacks per Firebox, **AMER devices saw at least 2.6 times more attacks compared to any other region.**
- **DNSWatch blocked over five million malicious domains during Q1.** Not only is this a whopping 281% increase over Q4 2020 but it seems particularly notable considering it reached that high while reporting devices dropped 17%.
- Malicious scripts – this quarter found in XML – continue to deliver fileless malware.
- Deeper below the top 10, we found another Linux threat called Linux.Ngioweb.B infecting consumer devices to form an Internet of things (IoT) botnet.
- **We saw exploits against the serious ProxyLogin Exchange Server flaws increase over 1,600%** from March 24th (when we first started seeing IPS hits) to the end of the month. You should have patched these flaws long ago, but if not expect to have been breached. More detail on these flaws are in our story of the quarter.

That's your quick peek at the Q1 threat landscape. Keep reading to learn additional details about these trends, as well as more technical descriptions of some of the threats and the methods and techniques they use to invade networks and infect victims.