Introduction

As digital technology has evolved and become much more interconnected, your individual company's cybersecurity posture has expanded to affect others far beyond just your own organization. This complex cyber-ecosystem means it's now in your best interest to improve everyone's cybersecurity stance, not just your own. I believe cybersecurity needs to become a community effort that creates a tide to lift all boats.

Both the pandemic and the SolarWinds breaches seeded my reflections on why it's so important to help others improve their security posture too. Deep down, I'm sure we all realize how interconnected human society is. While we don't know the names of all the thousands of the different people we rely on regularly, everything from food, to energy, to products and services, comes from countless other individuals who we truly need to live in the way society has become used to. When the pandemic started, seeing the results of supply chain disruptions due to these interconnections made that fact much starker than we may have consciously realized before. When the shelves are bare at your local grocery store, you really start to comprehend how much you rely on other people, even if you live a very introverted life.

This complex, interconnected reliance is completely true with digital technologies as well, as has become greatly apparent thru the SolarWinds breach (which we detail later in this report). You may not have had a direct relationship with SolarWinds or their products, but there is a chance their breach may have affected you anyway. For instance, their breach affected at least a hundred other big companies, who downloaded a legit-looking, but trojanized version of a product installer. Mimecast was among the affected companies, and as a result the attackers also stole private Mimecast digital certificates, which gave the attackers access to Mimecast customers' Microsoft 365 (M365) tenants. So already, those Mimecast customers are affected by a breach that started with a company they may not have any direct connection to. And each of those Mimecast customers probably has partners and customers of their own, who may now be affected by the Mimecast breach as well. Our digital connections probably go far deeper than we ever really contemplate – like the six degrees of Kevin Bacon game, if he were a digital android.

The Q4 report covers:

If any of that interests you, keep reading to learn more

In short, no matter what type of business, organization, or person you are, collectively we are all interconnected in many ways and rely on one another. Your good cybersecurity posture is in my best interest because of these complex connections. Likewise, my good cybersecurity posture is in your best interest as well. Of course, we only have control of our own resources, and can only directly secure ourselves. However, I propose cybersecurity should be a community effort, and we all need to try and influence our friends and partners to raise their boats as well. Security experts often remind us that our security is only as good as the weakest link. However, the recent supply chain breaches show us that the weakest link may extend to various partners and technological connections beyond our own organization as well.

This quarterly report is the WatchGuard Threat Lab's attempt to lift all boats and help strengthen weak links across the entire technology landscape. We believe that by sharing threat intelligence and security awareness, as well as the best practices associated with each finding or attack, we can encourage more companies to execute on the right security strategies. Making other companies and organizations more secure also improves our security too, as we are surely connected with many of you.

Our Internet Security Report (ISR) covers the quantifiable findings we gather from our various security products around the world, as well as any internal security research projects or external security stories we find throughout the quarter. We start by helping you understand the threat landscape through the analysis of the latest real-world attacks. Our data comes from a deluge of threat indicators delivered by over 45,000 WatchGuard Fireboxes, which we analyze to report most-common and -widespread cyber threats from last quarter.
I am also excited to announce the recent inclusion of Panda Adaptive Defense 360 (AD360) data into our quarterly report. In June of 2020, we closed our acquisition of Panda Security, a company that provided advanced endpoint protection to millions of endpoints for over 30 years. In this report, we share the annual view of malware from the perspective of millions of endpoints. While we have reported on malware trends since the start of this report, it was all from a network perspective. The types of early stage "droppers" that network anti-malware defenses detect is quite different than the final stage payload attackers deliver to a victim endpoint. We hope and expect our new endpoint data will give you a nuanced perspective of the threats actually making it to your employees' computers. While this quarter's endpoint data covers the full year of 2020, we hope to give you quarterly slices in our upcoming reports.

In any case, between all our network and endpoint threat intelligence, we receive a cutting-edge view into what the adversary targets and how they carry out their malicious campaigns. Knowing what criminal hackers are up to gives us the insights we need to tell you how to stop them. This report also highlights the top protection strategies you can deploy to avoid incidents in the first place. We share defensive tips throughout the report, but also summarize the most important high-level strategies at the end.

Your first priority should always be your own defense. However, supply chain breaches have proven that we are a lot more connected to each other than we might realize. We hope this report spreads the security awareness to lift all boats, but also inspires you to influence and improve the security of others within your own circles of connection.

Corey Nachreiner

CTO, WatchGuard Technologies

Executive Summary

The network malware and attack trends we have seen since the start of the pandemic have continued during Q4, 2020. We see much less malware detection at the office perimeter, which makes sense with many employees working from home. However, we also see record network attacks or IPS detections hitting organizations' perimeters. While the phishing and other email attacks that tend to introduce users to malware have followed them home, the adversary realizes we still deploy network and remote access services at our offices. In fact, you probably deployed even more network services at your organization when the pandemic first started, in order to allow your new remote work requirements. In short, while you need endpoint protections to guard your remote workers, you still need to maintain your network defenses to secure all your network services at the office and in the Cloud.

While network-based malware detections are down, we are seeing plenty of malware, the only difference is it now hits endpoints at home. **WatchGuard's newly acquired** Adaptive Defense 360 has caught and blocked a great deal of malware through 2020, and this quarter we share some of those endpoint trends. Our endpoint detection saw a decline in unique ransomware variants, likely because it's now mostly targeted, but also saw a huge 888% increase in fileless malware, or threats that use living-off-the-land (LotL) techniques. In short, don't take the lack of network-based malware volume as an excuse to lower your guard. Rather, make sure you have layered endpoint protection that can keep your home workers safe.

Outside those high-level trends, zero day malware (malware that evades signature-based protection) increased significantly in Q4, making up over 61% of all malware. We also saw encrypted threats hiding in TLS communications increase to almost 62%. As we mentioned in past reports, cyber criminals continue to increase their sophistication and evade traditional defense, even as they refocus their targets due to the pandemic.

This report covers a lot more, including details on fileless malware growth, an IoT or consumer router trojan called The Moon, a resurgence of cryptominers, the latest top malicious domains, and many other interesting details.

Some top-level Q4 2020 highlights include:

- Overall perimeter-detected **malware is down 4% quarter-over-quarter (QoQ)**, which we continue to expect due to the pandemic causing many employees to work from home.
- **Over 61% of malicious files are zero day malware,** meaning the malware is not detected using signature-based protections. This is **up 11 points compared to last quarter.**
- We saw a slight decrease in malware arriving over encrypted channels, with **47% of malware using TLS** (down 7 points compared to Q3). Decrease aside, this malware tends to be more sophisticated than average, with **~61% of it being zero day malware.**
- Overall, **Fireboxes blocked 20.6 million malware samples** in Q4, which averages to ~456 per Firebox.
- **Network attacks and unique exploit detections hit another two-plus year high.** Network attacks swelled to more than **3.49 million in Q4**, while unique network attack signatures grew just under 4% in Q4. This shows that criminals are still targeting the office with a larger variety of network exploits.
- During Q4 2020, Firebox appliances' intrusion prevention service (IPS) blocked an average of **77 attacks per appliance.**
- Despite an increase overall, **network attacks targeting the Asia and Pacific (APAC) regions declined 16 points,** while attacks in AMER and EMEA made up the difference.
- During Q4, **DNSWatch blocked a combined 1,313,686 malicious domain connections.**
- Fileless malware attacks skyrocket. According to a year's worth of endpoint threat intelligence from WatchGuard Panda products, **fileless malware rates in 2020 increased by 888% over 2019.**
- **The number of unique ransomware payloads (not volume) trended downward, falling ~48% in 2020** (2,152 unique payloads from 4,131 in 2019). The steady decline in ransomware volume indicates attackers continue to shift away from the unfocused, widespread campaigns of the past toward highly targeted attacks against healthcare organizations, manufacturing firms and other victims.
- **Cryptominers are back on the rise following a 2019 lull, with unique variants climbing more than 25% year-over-year (YoY),** reaching 850 unique variants during 2020.
- In Q4, **"The Moon" (Linux.Generic virus) made its debut on WatchGuard's list of top 10 malware list.** It directly targets Linux-based IoT devices, NAS servers, and consumer-grade routers, like those from Linksys, Seagate, and more.
- A new trojan (Trojan.Script.1026663) dupes email scanners with a multi-staged installation approach.

That's just a glimpse of what this quarter's report offers. The individual sections contain much more detail, including our first annual analysis of endpoint threats from Panda Security software. Read on to learn all the interesting specifics, as well as the many defense strategies and tips throughout this report.