Introduction

Sometimes we have bigger problems to address than cyber attacks.

That's how I currently feel as I sit here trying to come up with some "fun" metaphorical illustration of why you should follow the cyber threat trends we present in this report. As I type this, a global pandemic has put lives and livelihoods at risk around the world, with a death rate at nearing half a million, not to mention tens of millions unemployed. Meanwhile, another unjust police murder of a black man in the United States has proven that we have a long way to go in fighting the systemic racism in my country. When there are so many immediate threats, wrongs, pain, fear, and anger going on in our world, all of which affect our lives so directly, it's hard to consider what seems like an abstract, indirect digital threat, let alone come up with a creative way to talk about it. Right now, I would rather skip the niceties and focus on helping you get to what matters most; keeping your families safe, your principles intact, and your businesses running as best they can.

Having said that, cybersecurity awareness and protection still matters to both your personal online safety and digital business viability during this pandemic. In fact, you probably need to stay more vigilant against digital threats during times like these. While your number one priority should remain keeping safe and running your business during this trying time, you should also know that cyber criminals tend to up their illegal activities during tragedies like these. Unfortunately, digital criminals prey on both the fears and philanthropy of disasters, taking advantage of both our uncertainty and generosity. This report shares their tools, tactics and procedures in hopes you can learn enough to defend yourself against their atrocious actions.

By gathering and analyzing data from tens of thousands of network security appliances, WatchGuard's quarterly Internet Security Report (ISR) aims to help you recognize and defend against the statistically relevant cyber threats that affect most businesses today. Our threat team bases most of this report on quantifiable threat intelligence we receive from Fireboxes in the field. This data allows us to measurably identify which threats affected most customers last quarter, thus extrapolating the kinds of threats that will continue to affect you going forward. Using this knowledge, you can prepare the best cyber defenses ahead of time, hopefully giving you back time to concentrate on surviving and thriving during our current global calamity. Let's get into it.

The Q1 report covers:

05 **Q1's Firebox Feed Statistic.**
As mentioned before, most of the statistical analysis in this report come from our Firebox Feed data. This feed includes statistics on malware, network attacks, and dangerous domains. Our analysts scrutinize this data, identifying the top malware, most widespread threats, and common network attacks. They also highlight interesting regional trends, and dangerous domains. This quarter, they went a step further to identify how much malware arrives via encrypted communication channels like secure web traffic. Once we've identified the most relevant threats from the quarter, we translate that result into practical security advice you can use to continue to protect yourself from the top threats next quarter.

27 **Top Story: COVID-19-Related Attacks.**
Most quarters we do a deeper dive into a top security incident from the time period, giving you a more technical look at that particular story, and sharing how you can protect yourself from it. This quarter, no one security incident is as big as the coronavirus pandemic. Rather than focusing on one story, the team highlights some of the top coronavirus-related threats and trends seen in the last few months. For instance, we explore how the overnight change to working from home has irreversibly changed the digital attack surface presented by most businesses.

31 **Layered Defense Strategies.**
With all the bad news going on in the world lately, our goal is certainly not to pile on with more fear, uncertainty or doubt (FUD). The **only** reason we share these negatively themed trends is so you can prepare for and avoid them. The last thing you need to add to your plate is a cyber security incident. If we come together to help each other, chipping in our individual expertise, society can solve and conquer any problem. We hope our learnings can help you avoid security problems so you can concentrate on what you and your businesses do best.

The world seems dark right now, but there is plenty of light emerging from the shadows. I believe we'll see more goodness from one another helping to solve our shared global problems than we will bad actors taking advantage. We hope our Q1 report helps in a small part to at least shine a little light on the threat landscape, so you have one less thing to worry about.

Executive Summary

During Q1, we saw a drop in overall malware compared to the record-setting Q4 2019; and that despite an increase in reporting Fireboxes. We suspect this slight drop coincides with businesses having to move home in early March. Perhaps malware followed their users home. That said, malware is still up year over year, with ~64% of malware evading traditional, signature-based defenses (zero day malware). However, the biggest news this quarter is just how much malware bypasses security controls through encrypted network traffic. By analyzing the malware split in Fireboxes configured to decrypt TLS connections (like HTTPS traffic), we learned that more than two-thirds of malware arrives over encrypted channels. If you are not decrypting and scanning your secure web connections, you are likely missing a large majority of malware. Beyond this key finding, the report also highlights a few relevant malware samples, shares the top network attacks and malicious domains, and covers some COVID-19-related cyber attacks.

Q1 2020 highlights include:

- **67% of malware uses encrypted communication channels** on boxes that decrypt and scan TLS traffic. If you aren't using HTTPS decryption and content inspection, you're likely missing two-thirds of the malware entering your organization.
- **Zero day malware accounts for 63.7% of all threats on Fireboxes** not decrypting TLS. However, it also jumps to **72% on Fireboxes that decrypt and scan TLS traffic.** This suggests that not only do threat actors hide their attacks using encryption, but they tend to use more sophisticated malware through these encrypted channels.
- Overall, Fireboxes blocked **31.2 million malware samples in Q1**, which is a slight drop over Q4 last year and accounts for **~730 malware samples per Firebox.**
- The **Cryxos trojan** made a comeback attempting to steal credentials from victims.
- **A legitimate greyware remote desktop product, Ammyy Admin, made our top malware lists**. As you move employees home, beware insecure remote desktop programs.
- In Q1, **Fireboxes blocked 1.66 million network attacks,** which splits to about 38 attacks per Firebox. This is a slight **19% decrease** over last quarter.
- For a second quarter, **SQL injection attacks remained the top network threat for Q1.**
- **Bellsyscdn[.]com was responsible for over half the malware domain blocks this quarter**, due to its hosting of the Bondat worm's C&C, Monero cryptomining, and WordPress-related attacks.
- **DNSWatch saw and blocked lots of cryptomining-related campaigns.** Six domains related to Monero cryptomining made our top domains lists.

Those are the report highlights, but let's dive into the interesting additional details. By the end of the report, we'll have shined a light on the dark cyber threat landscape and offered you advice to protect yourself.