# Introduction

It's September, which in the U.S. means the end of summer but the beginning of the American football season. Along with real football comes Fantasy Football, where groups of friends and co-workers "fake draft" real football players into imaginary teams and see which of them would have won pretend games based on each individual player's real performance. If you're into sports, stats, and a little fun competition, Fantasy Football is an entertaining past time. However, if you want to win, you'll have to understand long-term, historical player trends. Sure, last week's player results, or even three years of a player's results can't perfectly predict what that player will score next week. The universe is full of entropy. However, statistically you'll have a much better chance of understanding how a player will perform in the future if you take a large enough sample of his past into account.

WatchGuard's quarterly Internet Security Report (ISR) is the historical "player statistics" of the threat landscape. The more you know about what attackers have been doing the past quarter – or even the past few years – the more you will understand what they'll likely do in the future. Obviously, this knowledge gives you a big leg up in your defense, allowing you to win your threat landscape pool. And unlike fantasy games, that pool has real-world consequences if you lose.

This report includes detailed threat intelligence about the top and most-widespread malware, the most common network attacks seen in the wild, and the top domains targeting your users. In short, it's the historical attack data that can help you pick your security starter lineup for next quarter. Besides the raw numbers, our Threat Lab experts also offer their detailed analysis and opinions on the data we report, acting as the top fantasy sports commentator to your threat landscape league. If you're responsible for securing your organization, or even marginally interested in protecting yourself online, this report should help you win more matches against cyber criminals… and who doesn't want to win their fantasy sport pool.

**If you play fantasy sports, you're probably someone who likes to win; especially when money is on the line. In information security, your business's money is always on the line, potentially costing you millions if you lose the next game. That's why fantasy players often turn to advice from the experts. Let us act as your threat landscape experts by reading this quarter's report.**

## Now that you know why you should keep reading, here's what we cover this quarter:

06

### *Q2's Firebox Feed results.*

As always, the WatchGuard Threat Lab analyzes threat intelligence from tens of thousands of Fireboxes. This feed includes historical data about the top malware, both by volume and percentage of victims affected. It also includes network attack statistics based on our intrusion prevention service and our DNS security service. We also try to highlight regional trends, when relevant, and share defense strategies for the trends we find. In short, these are the key "player" stats you can leverage to figure out what attackers might do next.

24

### *Top Story: The Baltimore Ransomware Attack.*

Unless you've cut all online connections (in which case, how are you reading this?), you probably heard about the huge ransomware attack in Baltimore during Q2. This attack will likely cost Baltimore at least $17 million in recovery costs (even though they didn't pay the ransom). What you may not know is all the details about how the attack happened, and how you can avoid the same. We cover both in this report.

28

### *Research Section: Q2 MSP Attacks.*

Unfortunately, the Baltimore incident wasn't the only big ransomware story for Q2. Sophisticated attackers also hijacked three managed service providers (MSPs) and used their tools to spread ransomware to all their customers. An involved MSP shared some of the malware samples from these attacks with us, which we analyzed. In this report, we share our technical findings, and some important MSP defense tips. Throughout the report, and in conclusion, we share many valuable defensive strategies to avoid some of the threats we highlight from Q2 2019.

40

### *Words of Security Advice.*

By the end of the report, you should have some idea of how dangerous some of the opposing team players can be. However, you'll also have great insight on their playbook. We fill that out by sharing our expert analysis, offering strategies on how you can win this important security game next quarter.

# Executive Summary

This quarter, malware was down but network attacks were up; we saw an increase in backdoor shell scripts coming from a well-known Linux penetration testing distribution; and ransomware was up with two major stories of targeted infections. The good news is, a properly configured WatchGuard Firebox with Total Security could have blocked all these threats, so hopefully none affected you. That said, it's worth learning from these trends, especially if you haven't implemented all of the different security services required to block them. Read on to learn Q2's threat landscape stats, and receive your security playbook for Q3.

**Our Q2 2019 Internet Security Report highlights:**

- **Zero day malware accounted for 38% of all malware** detections, within a few percentage points of the previous two quarters.
- Overall **malware detections trended down around 5% this quarter** compared to Q1 2019. Malware is still up 64% compared to Q2 2018.
- **DNSWatch blocked** multiple campaigns that used **Content Delivery Networks** (CDNs) to host browser-hijacking malware.
- In Q2 2019, there was **an increased overlap between the most-widespread malware detection affecting individual networks and the most prolific malware** by volume, with three threats found in both lists.
- **The EMEA region saw the most malware detections per Firebox**, with APAC in a close second and AMER bringing up the rear. This is almost the perfect opposite to the previous quarter.
- Multiple popular backdoor shell scripts, used by both penetration testers and cyber criminals, showed up in our top malware attacks. Both the **Backdoor.Small.DT and Trojan.GenericKD (SSB) tools come pre-installed with Kali Linux**.
- **11% of the sextortion (sexual extortion) phishing emails associated with Trojan. Phishing.MH targeted Japan**. We aren't positive why but suspect it could have to do with sextortion being more effective in conservative cultures.
- **Network attacks more than doubled from Q1 to Q2**. This was the largest percent increase we've seen since 2017.
- In Q2 2019, WatchGuard Fireboxes blocked **22,619,836 malware variants** (549 per device) across all three anti-malware engines and **2,265,425 network attacks** (60 per device).

Now that you know what to expect, it's time to dive into the nitty gritty. Read on to learn more about the opposing players, and how you can build a security defense that wins.