Introduction

Many of the fears that occupy peoples' attention, and drive big headlines in the media, are indeed scary and tragic. That said, they are also so statistically unlikely to happen that they shouldn't receive such a disproportionate amount of attention in comparison to threats that are more mundane, don't drive click-bait headlines, but have a much greater statistical chance of happening to us. For example, a common analogy is that some people are afraid of getting into an airline crash, but are far more likely to have a fatal car accident while driving to the airport. Or, while people are rightly afraid of contracting Ebola, many don't realize that the common flu kills 100 to 296 times more people every year. We worry about potential terrorist attacks, but don't pay attention to the staggering rates of heart disease that will likely kill around 647,000 US citizens this year. While evolution equipped us to efficiently identify immediate threats, it doesn't seem to help us properly identify and prioritize the silent killers that are far more likely to affect most of us over time.

This idea recently came to mind when I was discussing the historical **Tylenol Terrorist** with a coworker. If you don't remember, in Chicago during 1982 some degenerate murderer poisoned bottles of Tylenol with potassium cyanide, killing seven people including a 12-year-old girl. That tragic incident created a national panic, and dramatically changed our pharmaceutical and food packaging industry, forcing new safety standards. We likely have it to thank for tamper-proof packaging today.

My coworkers' thoughts on the Tylenol incident revolved around how the horrible threat led the industry to positively find new security controls to keep us safe – a silver lining in what was an otherwise horrific situation. However, I couldn't help but ask, "Was that panic justified?" I think society was panicking about the wrong thing. While those seven deaths were tragic, Tylenol actually kills 64 times more people every year all on its own. According to research, acetaminophen (the active ingredient in Tylenol) causes around 50 thousand emergency room visits, 25 thousand hospitalizations, and 450 deaths (100 unintentional) every year; all from overdose. Even if you count all the deaths from copycat poisoners, Tylenol overdose is far riskier to the average person than some killer tampering with our products. Yet we seem to fear the killer more than the common overdose. This is yet another of many examples on how humans' emotional fears don't always statistically match the biggest threats we face.

This mistake happens in information security as well. Researchers like us often focus on the newest, technically sophisticated and unusual cyber threats, likely because they are cool and a bit scary in their capabilities. Yet the truth is, run-of-the-mill phishing attacks are much more likely to cause real-world breaches than any rare or fancy APT attack. You'd do far better for your organization to defend against the statistically relevant threats than any complex yet rare ones.

WatchGuard's quarterly Internet Security Report (ISR) is designed to help us all overcome our emotional reaction to cyber threats and recognize the truly statistically relevant ones instead. A large portion of this report is based entirely on quantifiable and statistically relevant threat intelligence we receive from tens of thousands of Fireboxes in the field. Rather than guessing what malware or threats will be the most dangerous based on their capabilities, we can measurably tell you which threats affected the most customers last quarter. There is nothing wrong with you wanting to implement the next "tamper-proof" security control for your network, but you ought to apply that security focus to the risks that actually threaten your organization the most. We intend for this report to help you find those real risks.

The Q4 report covers:

Q4's Firebox Feed results.

The bulk of our report comes from threat intelligence data that tens of thousands of Fireboxes share with us, called the Firebox Feed. 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 highlight interesting regional trends, when relevant, and give you advice for protecting yourself from the latest threats. While the news might highlight one scary and emotional ransomware attack, our report will tell you the threats that actually target the most customers.

Top Story: Macys vs MageCart.

During October 2019, Macys discovered a suspicious connection from their eCommerce site to some third-party website. Turns out criminal actors had injected a malicious credit card skimming JavaScript framework called MageCart onto their site. In this report, we detail this attack and technically describe how the popular MageCart payload works.

Protection Advice.

The industry and Johnson & Johnson's reaction to the Tylenol killer was pretty admirable; besides an immediate recall, the event led the industry to adopting some great security practices that make us safer today. However, it's best to focus the right security controls on your biggest areas of risk. Not only will our report help you identify the most statistically relevant attacks, it'll offer you defense strategies and advice to make sure you avoid these top threats.

Like the Tylenol killer, headlines about the latest targeted ransomware can be frightening and you certainly want to protect yourself against those sporadic cyber threats too. However, sometimes the much bigger problem is a lesser evil you see every day. Let our Q4 report guide you towards the most prevalent malware and attacks targeting networks each quarter, and adjust your defenses accordingly.

Executive Summary

Q4 2019 saw an explosion in zero day malware (which is malware that signature-based protections missed during the first few days or weeks of its release) reaching an all-time high of 68% of total detected malware. This is up from the approximate 37% average of 2018 and 2019, making Q4 2019 the worst malware quarter on our books. We also continue to see a number of malicious Excel droppers and more Mac adware hit our top malware lists. Web application attacks continue to fill our network threat lists, with SQL injection attacks in the lead. Finally, this quarter we dissected Macys' October eCommerce site breach and describe how attackers used the malicious MageCart JavaScript to skim credit card information.

Additional Q4 2019 Internet Security Report highlights include:

- **Zero day malware, or evasive malware that sneaks past signature-based defenses, exploded to a record high of 68% of total malware.** This is up from an average of 37% over the last year. WatchGuard saw corresponding jumps in the amount of malware blocked by IntelligentAV and APT Blocker.
- **In Q4, reporting Fireboxes blocked 34.5 million malware samples,** which is about 860 malware hits per Firebox — an all-time high.
- **Old Microsoft Excel vulnerability still heavily exploited.** A Microsoft Excel vulnerability from 2017 was the 7th most common piece of malware on our top 10 malware list during Q4, showing attackers still actively exploit it in the wild.
- **Mac adware returns to the top 10 list.** One of the top compromised websites in Q4 2019 hosted macOS adware called Bundlore, which poses as an Adobe Flash update.
- **During Q4 2019, Fireboxes blocked 1.88 million network attacks,** translating to almost 47 attacks per Firebox.
- **SQL injection attacks were the major network attack of Q4 2019.** SQL Injection attacks rose an enormous 8000% in Q4 2019 compared to 2018 and was the most common network attack by a significant margin.
- **Nearly half of the network attacks were isolated to one of the three geographic regions** (AMER, EMEA, APAC).
- **Macys' eCommerce site was hit by MageCart,** a malicious JavaScript threat that skims credit card transactions as customers make them
- **DNSWatch showed that attackers still use legitimate image sharing sites to distribute malware.** See the DNS section for more info about the top compromised sites.

Now that you know the highlights, let's dig into the details. By the end of this report, you will know the right cyber threats to concentrate on and will have the defense tips to stay safe.