Introduction

Have you ever wondered what types of cyber attacks affect small to midsize businesses (SMBs) and distributed enterprises (DEs)? Well, you've come to the right place.

WatchGuard's Internet Security Report is based on Firebox Feed data coming more than 26,000 unified threat management (UTM) appliances that are monitoring and protecting SMBs and distributed enterprises around the world. This data gives us insights into what types of network exploits, malware infections, and advanced attacks are launched by cyber criminals every month, and how they change and update their attacks over time. We share these trends and insights with you every quarter in our Internet Security Report.

The report for Q1 2017 includes:

Many trends and discoveries from the Firebox Feed

What types of malware do we catch most often in the wild? Which network services do attackers commonly target? What are the most popular attacks in different regions of the world? Which delivery mechanisms do cyber criminals most regularly rely on? You can learn all this and more in our Firebox Feed Statistics section.

Top Story: CIA Vault 7 leaks

Every quarter, you're flooded with interesting and relevant information, security stories and incidents. Some of them can have industry-wide effects. This quarter our researchers comment on the CIA Vault 7 leak from Q1 2016 and share some additional technical analysis you didn't see in the news.

Latest Internet of Things (IoT) research

The WatchGuard Threat Lab constantly runs security research projects to study the threats and issues affecting businesses today. For the last few quarters, our researchers have been analyzing the security of consumer IoT devices. This quarter we disclose a vulnerability we found in the Ouvic C2 HD Security Camera.

Most importantly, defensive learnings

While some might consider the threat landscape interesting on anecdotal merit alone, you can put these trends and learnings to good use. We share these trends and findings so that you can cater your defenses to the latest attacks. We share various protective tips throughout this report, and summarize with our top learnings.

We're excited to share our second report based on data analysis from our Firebox Feed, and our additional research projects. We believe this quantifiable data gives us a deeper insight into the most prevalent threats our customers face and how cyber criminals craft their latest attacks. Our quarter-over-quarter analysis also shows how attackers evolve their techniques and focuses over time. We hope this report provides useful information, and you make it a regular part of your InfoSec awareness and training. Thanks for joining us this quarter, and read on for our latest threat landscape findings.

Executive Summary

Even when malware declines, other attacks rise. Consumers and businesses are under the constant deluge of network attacks, phishing, and malware. Criminals target Brazilian banks, nation-states anonymize their tools, and advanced threats get past legacy defenses. If you want to keep your business online, you need to stay vigilant against these attack trends so you can identify defenses for them.

This report provides some details around those and other trends. Here's a high-level summary of some of the things you'll learn from this report:

- **Linux malware is on the rise, making up 36% of the top malware** we detected in Q1 (if you count PERL/Shellbot). We believe this increase comes from attackers targeting IoT devices.
- **Legacy AV missed 38% of malware.** In Q4, signature-based AV missed 30% of the threats we caught overall. This quarter, those misses increased 8% despite a general decline in malware detection overall. This means increasingly more malware evades traditional AV solutions.
- **Threat actors take a break from hacking the holidays.** Overall, threat volume decreased 52% in Q1 2017 compared to Q4 2016. We believe the drop in malware detections can be attributed to the absence of seasonal malware campaigns associated with various Q4 holidays, which increased overall malware instances during that period.
- **Conversely, network attacks are up 37% compared to Q4**, likely due to automated tools that always look for new victims.
- **The web battleground shifted towards web servers.** Last quarter, we saw more exploits that were used for drive-by downloads (web client attacks). In Q1, 82% of the top network attacks targeted web servers (or other web-based services).
- **Our top ten XSS attack primarily targeted Spain.** We aren't sure why this particular cross-site scripting exploit was popular in Spain, but it was.
- **Attackers still exploit the Android StageFright flaw.** A mobile device vulnerability cracked our top ten attack list this quarter, breaking the previously unchallenged web attack theme.
- **Criminals target Brazilian banks with cross-platform malware.** We detected a large amount of email-based Java malware sent to victims in Brazil. We suspect this is part of the well-known Banloader banking malware campaign.

Those are just a few of the many trends this report explores. Read on for more in-depth explanations and