INTRODUCTION

Upon our planet, an intricate and vibrant ecosystem thrives, where diverse life forms engage in a symbiotic dance that sustains and enriches all. Birds, animals, plants, insects, and humans coexist in a delicate balance, each doing its part to support the health and growth of everyone. Think of the diligent bee pollinating blossoms and promising fruit. Grazing animals control vegetation, preserving landscapes for the future. Trees exchange carbon for oxygen in a silent pact that provides the air we breathe. This is a world of deep interconnection, where mutual reliance underpins existence itself.

Yet, within this symphony of life, threats lurk. Invasive species upset the balance by snatching resources and spreading unchecked. Pollutants seep into pristine environments, threatening the stability on which life depends. Viruses act like phantom infiltrators, leaving destruction in their wake. These dangers remind us how fragile and vulnerable the natural world can be.

Much like this dynamic natural ecosystem, the cyber landscape is a rich and varied ecosystem. Businesses, governments, and individuals over time have connected a vast array of digital systems and technologies, which all interact in a web that fuels communication, trade, and innovation. This interconnected digital ecosystem fosters growth and opportunity, crossing borders to benefit all.

However, just as invasive species and pollution threaten nature, the digital world faces its own threats. Malicious actors like hacktivists, cybercriminals, and state-sponsored spies mimic nature's invaders. They launch a range of cyberattacks, from simple to sophisticated, that continue to evolve and disrupt information flow, exploit vulnerabilities, and threaten the digital terrain for their own gain.

Enter our Quarterly Internet Security (ISR) report as your guide. We, as cyber defenders, act like digital ecologists, analyzing every byte, signal, and network to understand the digital threat landscape. Using our insights, we build strong defenses that mimic nature's resilience. By understanding the attacker's perspective, we can help preserve the integrity and vitality of our shared digital ecosystem.

As you explore this report, think of it as a map of the digital jungle, highlighting recent threat evolutions and offering ways to keep this cyber ecosystem safe. More specifically, this report shares key threat trends seen by many of our products, including malware developments observed from both network and endpoint solutions, network attack findings from our intrusion prevention service (IPS), ransomware development throughout the quarter, and much more.

In our connected world, general cybersecurity awareness and proactive defense actions or refinements are our most powerful tools, which this report hopes to provide. Like ecologists protecting the Earth, we all have a part to play in safeguarding what sustains us to ensure a secure future.

In this report, we cover:

EXECUTIVE SUMMARY

Like last quarter, network malware close to doubled this quarter, rising 171 percent, while total endpoint malware detection dropped. However, we also saw a huge (712 percent) rise in new unique malware variants on the endpoints. Combine that with a substantial increase in zero-day malware detection on the network and this signals a sharp rise in evasive and sophisticated malware, which delivered trojans, information stealers, coinminers, and phishing threats. While our data doesn't always provide us with the explanations behind the changes we see, we theorize that the growth in AI tools on the underground has accelerated threat actors' ability to develop sophisticated threats quickly at scale.

Meanwhile, network-based attacks and exploits remained stable, only growing by one point. Malicious attackers also targeted a lower number of specific software flaws, with unique network exploits down 16 percent. Beyond that, we saw little change in our network attack trends, with no new exploits rising to our top 10 list, and old exploits like ProxyLogon and HAProxy still hanging around, despite their age.

Finally, our endpoint section was rife with interesting changes. While total malware is down, new unique malware variants exploded, as we shared above. We all saw pretty big changes in some of the regular trends concerning malware delivery vectors. However, ransomware and cryptominers declined.

To round things out, here are some executive highlights from our Q1 2025 report:

- **Total network-based malware detections increased again, rising 171% quarter-over-quarter (QoQ).** We saw this despite a small decrease in signature-based and behavioral detection engines, .as the lion's share of the growth (323% increase) came from our proactive AI and machine-learning service IntelligentAV.
- Endpoint total malware volume was down, but **we saw a surge in unique malware detection, increasing about 712%** QoQ, which paired with our network malware trends, shows threat actors are focusing on new evasive and complex malware.
- Threat actors continue to use encryption to spread malware, with **71% of malware arriving over encrypted (TLS) connections during Q1,** which is an 11-point increase from last quarter, and an continued increase for the year.
- Our "per Firebox" malware results for various network malware detection services:
  - **Average total malware detections per Firebox:** 4,204 (171% increase)
  - **Average malware detections by GAV per Firebox:** 374 (31% decrease)
  - **Average malware detections by IAV per Firebox:** 3,735 (323% increase)
  - **Average malware detections by APT Blocker per Firebox:** 95 (25% decrease)
- **We extrapolate** that if all the estimated currently active (licensed) Fireboxes enabled all malware detection security services and were reporting to us, **Fireboxes would have seen 1,624,555,924 malware detections during Q1 2025.**
- **Almost three-quarters (71%) of malware evaded signature-based methods.** We call this zero-day malware, as it requires more proactive techniques (IAV/APT) to catch this never-before-seen malware. The rise was completely due to a rise in malware detected via our machine-learning and AI methods.
- Adding to this, **zero-day malware accounts for 87% of malware detected over encrypted connections,** proving a continued rise in evasive malware delivery.
- Meanwhile, **network attacks increase by a single point during Q1 2025, with only 93 software exploits per Firebox caught by IPS signatures – one more than seen last quarter.** We also saw a decline in the number of unique exploits attackers tried, with unique IPS signature hits down 16%.
- **Ransomware declined 85% from the previous quarter.** This supports the industry trend of a decrease in crypto ransomware. Attackers are now shifting toward data theft instead of encryption, as improvements in data backups and recovery have been made.
- **Endpoints malware delivery vectors shifted appreciably in Q1.** For years, malicious scripts, primarily PowerShell, have remained the most common way malware arrives on an endpoint by a fairly large margin, while Windows binaries have continued to gain ground as the second-most common vector. However, this quarter we saw browsers and "other" vectors rising significantly on the list, suggesting that threat actors are returning to "drive-by download" tactics and delivering malware more often in piracy-related tools and remote software.

That's just a glimpse of the trends in invasive cyber species infiltrating our shared digital ecosystem. For much more detail and tips that will make you a better cybersecurity ecologist, read on.