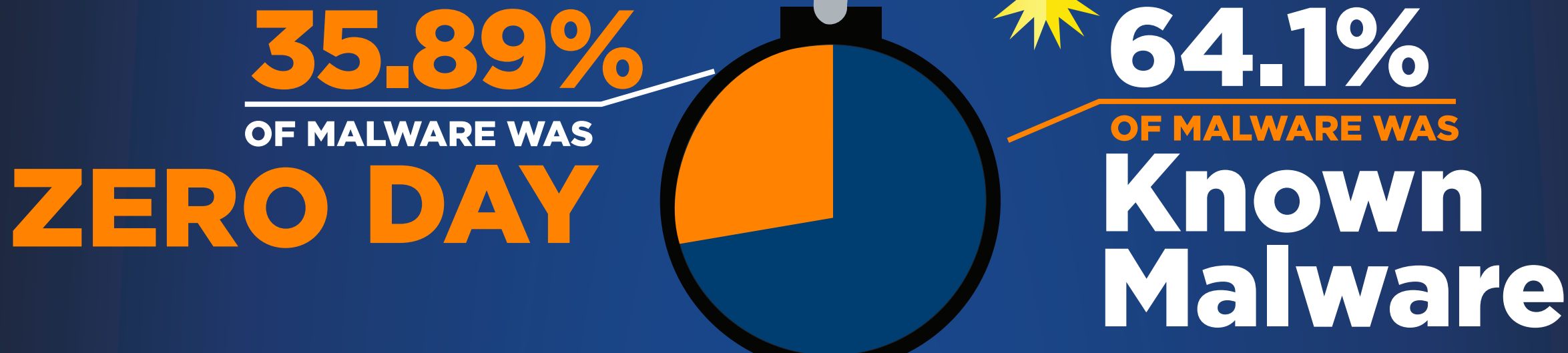
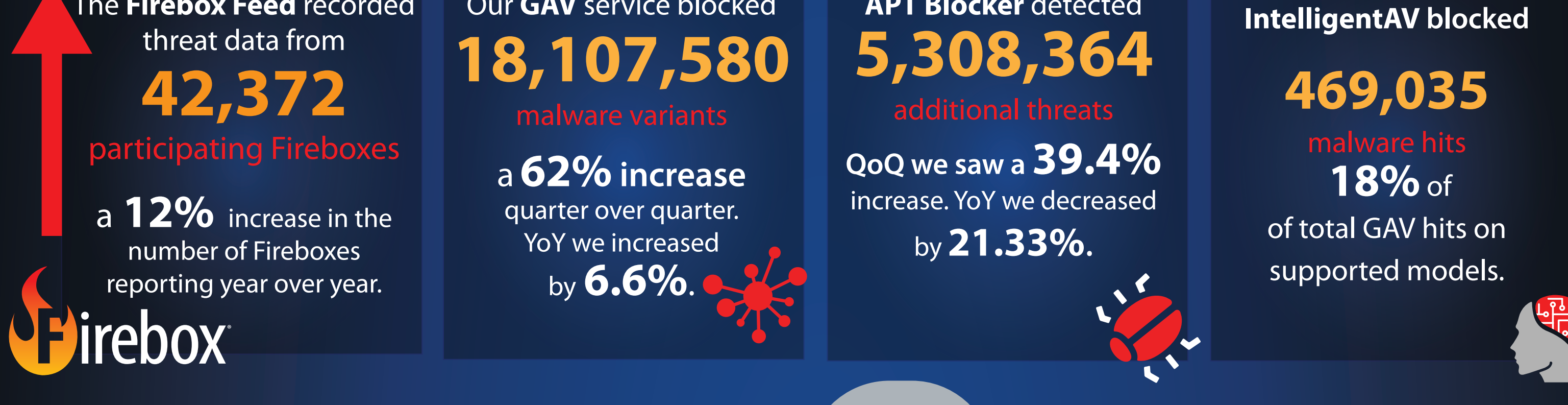


Q1 2019 Internet Security Insights

WatchGuard Threat Lab

This quarter, we saw an unexpected increase in malware, a decrease in network attacks, two wide-spread Mac adware variants, and a surge in web application attacks (specifically, XSS and SQLi). We also saw an unknown attacker steal millions in cryptocurrency using a 51% attack.

Malware Trends



High-level Threat Trends for Q1 of 2019

Mimikatz remains the #1 threat, accounting for **3,728,249** or **20.6%** of all malware hits

Overall malware unexpectedly increased in Q1 2019
this quarter malware rose **62%** QoQ and **6.6%** YoY.

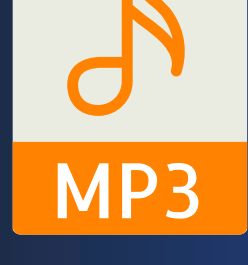
Gateway AntiVirus (GAV) alone blocked over **18,107,580** malware variants compared to 16,986,850 the previous year.

Total Network Attack Volume Went Down



New & Notable Network Attacks

We saw four new attacks this quarter reach the top 10. Winamp ID3v2 Tag Buffer Overflow, Meterpreter Windows Payload Delivery, and two SQL injection attacks.



Winamp ID3v2 Tag Buffer Overflow

Only affects Winamp version 5.093 or below and was patched almost 14 years ago. If attackers can trick your users into loading a specially crafted audio (MP3) file with Winamp, they could exploit this flaw to execute arbitrary code on your computer. This buffer overflow probably showed up due to automated attacks.



Meterpreter Windows Payload Delivery

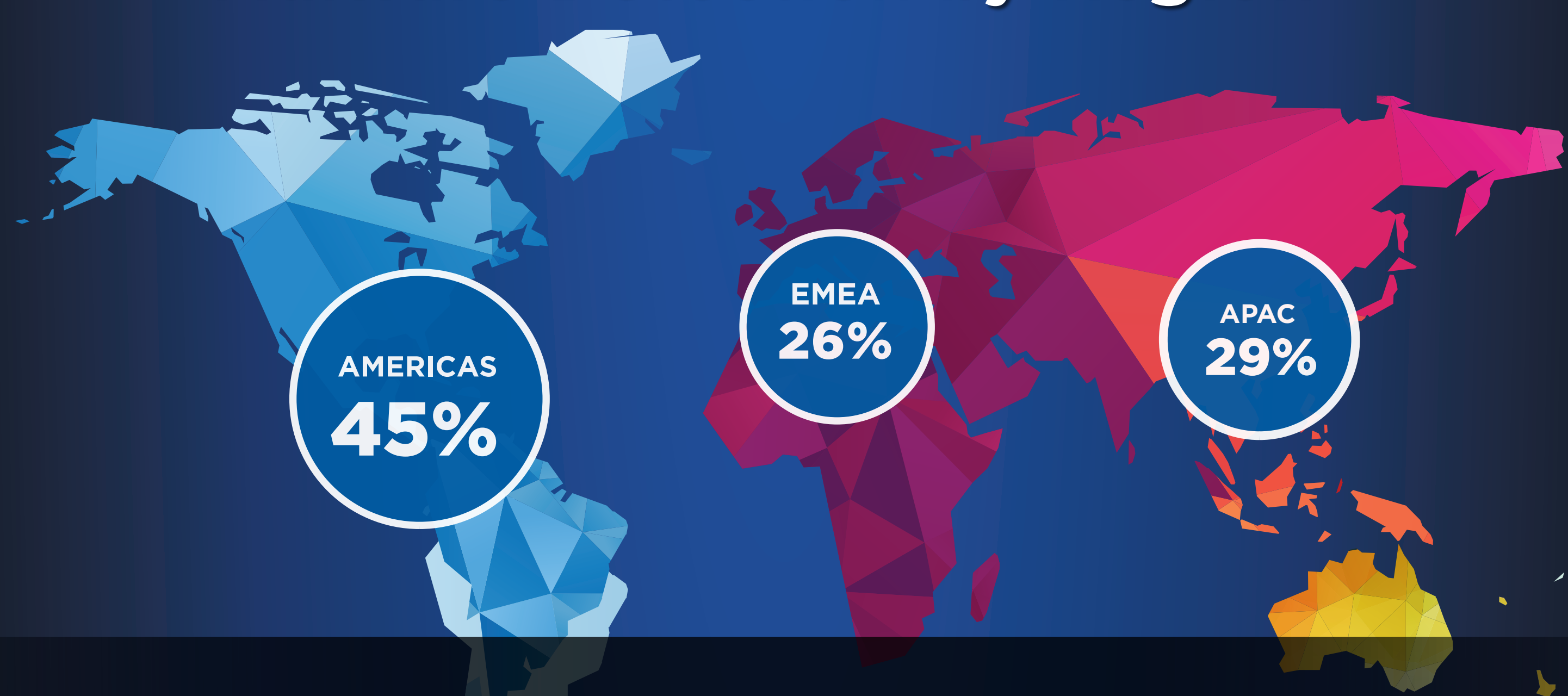
This signature matches the popular Metasploit fileless malware tool, Meterpreter. It creates a tunnel back to the attacker's server and allows them to load additional malware or execute commands. Penetration testers and malicious hackers often use Meterpreter and Mimikatz together as a one-two punch to infect a system and steal credentials.



WEB SQL injection attempt -33 & WEB SQL injection attempt -7

SQL is one of the oldest well-known web application attacks. SQL injections exploit web servers that don't properly sanitize user input, allowing the attacker to issue their own SQL commands. The attacker often tries to obtain unauthorized access to the web server or to dump the user and password database from the SQL database.

Malware Detection by Region



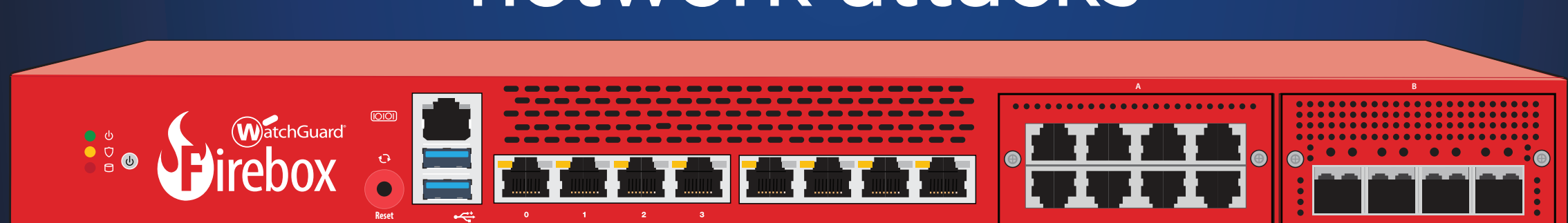
Trojan.JS.Agent favored the **AMER** region overall, but also had the top three countries fall outside of AMER.

Cryxos was clear in its **AMER** makeup, with the U.S. taking over **31%** of the hits and Canada in a close second with **30%** of hits.

RTF malware favored **EMEA**; Estonia claimed **4.1%** of the attacks. Slovenia and Jordan tied in second place with **3.7%** each.

Firebox Feed included threats captured from **42,372 Firebox appliances** deployed across the world

In Q1 2019, WatchGuard Fireboxes blocked over **989,759** network attacks



→ **23** attacks per device



18,107,580

malware variants blocked by WatchGuard in Q1 2019

→ **427** malware samples per device

Read the full Internet Security Report at www.watchguard.com/security-report

