


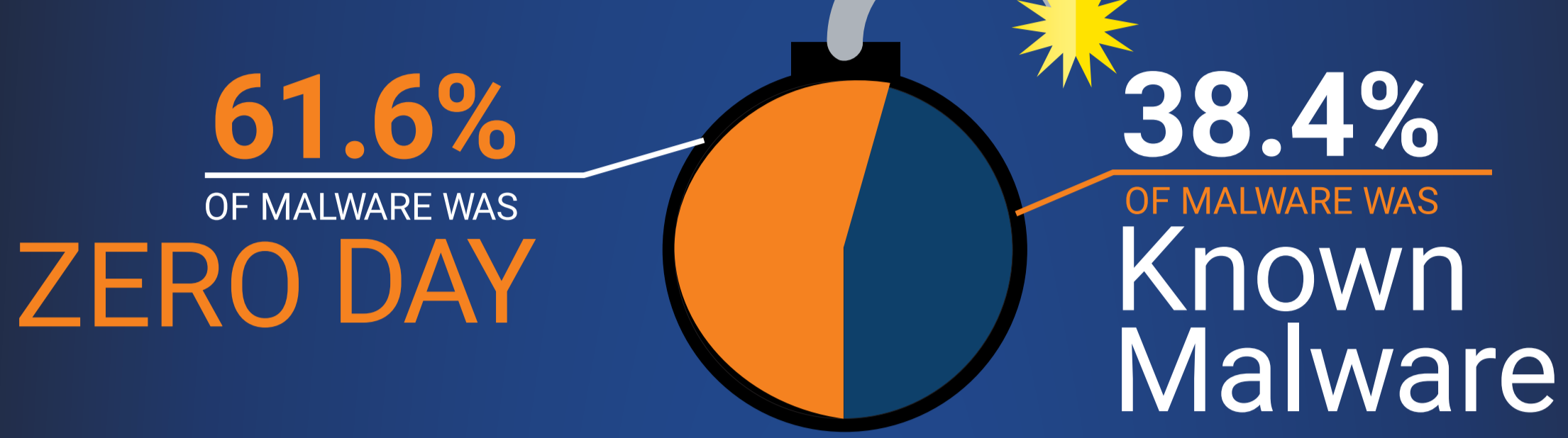
Q4 2020 Internet Security Insights

WatchGuard Threat Lab

The WatchGuard Threat Lab team is a group of analytical, science-based threat experts who want to help you truly quantify the cyber threats your business faces. By statistically measuring the most relevant risks, we help you validate your security strategy with practical defense tips and mitigations. Our quarterly Internet Security Report (ISR) contains measurable threat intelligence on the most prevalent and far-reaching malware, the top network attacks seen in the wild, and the common malicious domains victimizing your employees and users.

Malware Trends

 <p>The Firebox Feed recorded threat data from 45,306 participating Fireboxes 5% increase from the previous quarter</p>	<p>Our GAV service blocked 13,334,615 malware variants 11% decrease in basic malware</p>	<p>APT Blocker detected 7,077,680 additional threats 11% increase in zero day hits</p>	<p>IntelligentAV blocked 264,425 malware hits 52% QoQ decrease in IAV hits</p>
-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	---------------------------------------------------------------------------------------------------------------	-------------------------------------------------------------------------------------------------------------	-----------------------------------------------------------------------------------------------------



High-Level Threat Trends for Q4 of 2020

Cryptominers are back on the rise following a 2019 lull, with **unique variants climbing more than 25% year-over-year (YoY)** reaching 850 unique variants during 2020.

Fileless malware attacks skyrocket. According to a year's worth of endpoint threat intelligence from WatchGuard Panda products, **fileless malware rates in 2020 increased by 888% over 2019.**

New and Notable Threats

Let's take a look at a few of the top threats from this quarter's report.



The Moon

The Moon, a relatively new IoT (router) botnet, made our top 10 malware list during Q4. After an initial investigation, we learned this malware is part of a network of servers pushing this and similar malware to Linux-based, consumer-grade network devices like routers.



Phishing

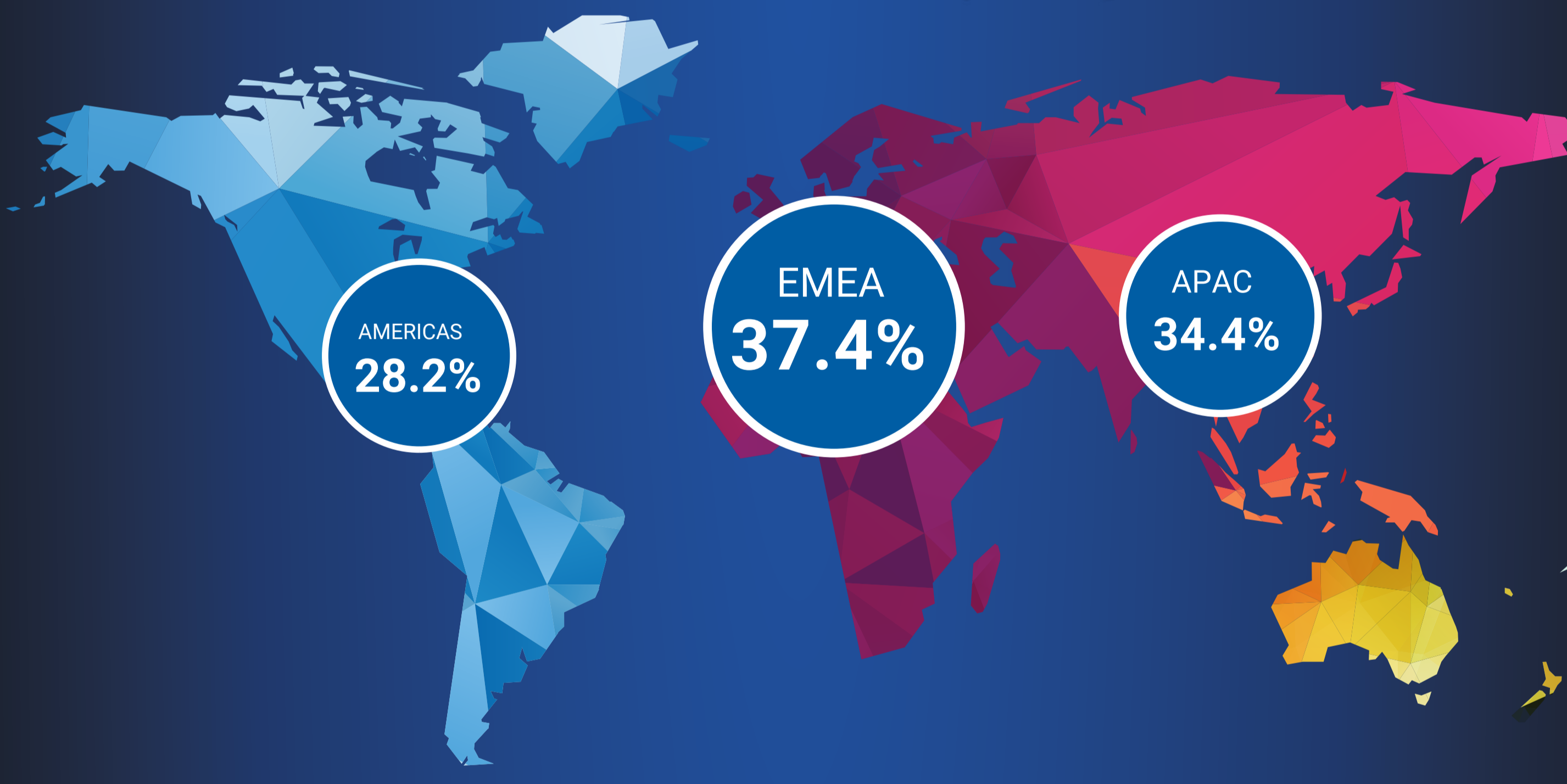
We encountered multiple malware attacks that began with a phish in Q4, many of them abusing Cloud-hosting services to hide their tracks.



Trojan.Script.1026663

One popular malware threat from Q4 came in the form of a macro-enabled Word document. This malware tried to trick users into enabling editing which gave the document sufficient permissions to launch an exploit.

Malware Detection by Region

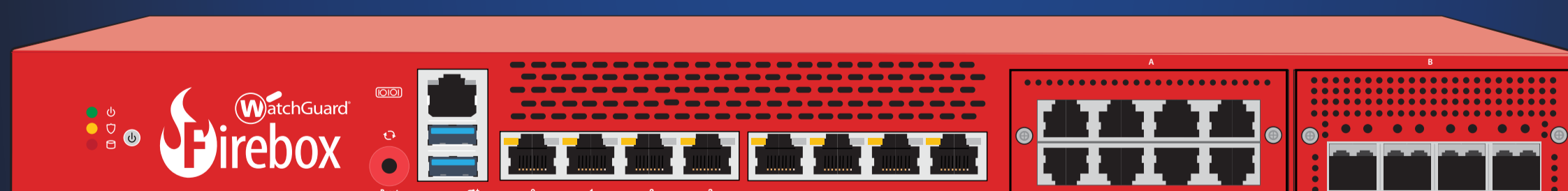


Win32/Heri took the number one spot with **2,140,536** detections this quarter.

COUNT	THREAT NAME	CATEGORY	LAST SEEN
2,140,536	Win32/Heri	Win Code Injection	Q3 2020

Firebox Feed included threats captured from **45,306** Firebox appliances deployed across the world

In Q4 2020, WatchGuard Fireboxes blocked over **3.49 million** network attacks



→ **77** attacks per device



20.6 million

malware variants blocked by WatchGuard in Q4 2020

→ **4% decrease** in malware

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

