Q1 2017 Internet Security Insights
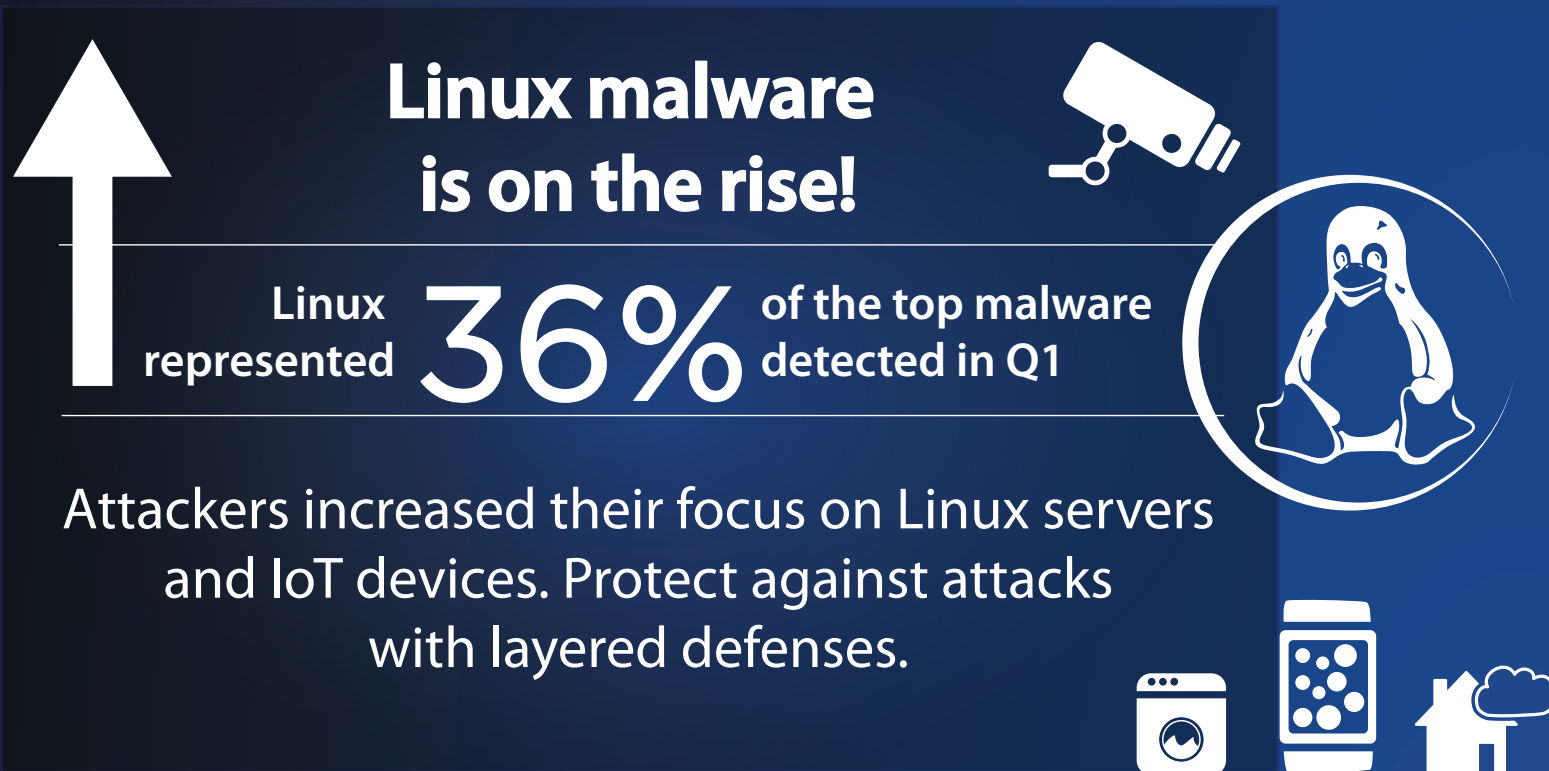## | Q1 2017 | WatchGuard Threat Lab

Before taking action to protect your business, you must understand the threat landscape. The team at WatchGuard Threat Lab created the quarterly Internet Security Report to help you do just that. Enjoy!

Malware Trends

Linux malware is on the rise!

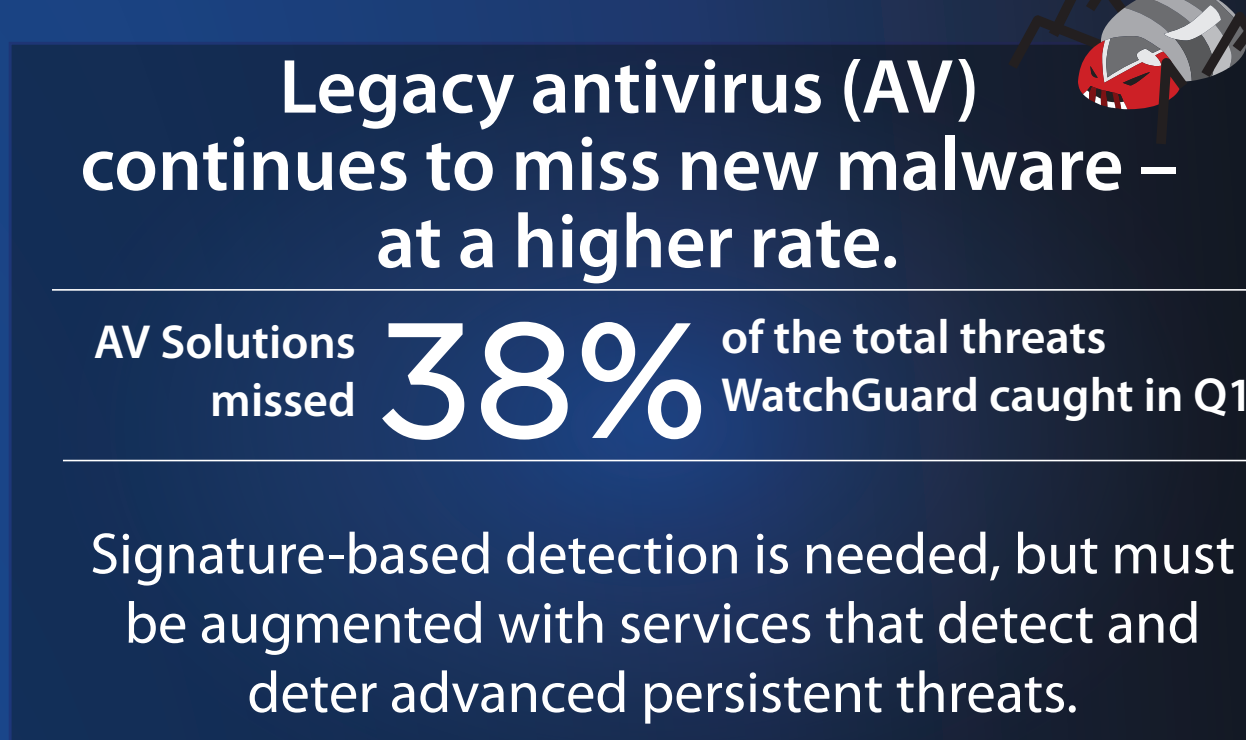Linux represented **36%** of the top malware detected in Q1

Attackers increased their focus on Linux servers and IoT devices. Protect against attacks with layered defenses.

Legacy antivirus (AV) continues to miss new malware – at a higher rate.

AV Solutions missed **38%** of the total threats WatchGuard caught in Q1

Signature-based detection is needed, but must be augmented with services that detect and deter advanced persistent threats.

The cyber security battleground is shifting toward web servers.

Drive-by downloads and browser-based attacks were predominant in Q1.

82%
of the **top network attacks** targeted **web servers** (or other web-based services)

Users should strengthen web server defenses by **hardening permissions**, **limiting resource exposure**, and **patching server software**.

Trending Threats

Android StageFright
Attackers still exploit the **Android StageFright** flaw

Bitcoin Mining Trojan
The **Bitcoin mining trojan** was entirely delivered via **FTP**.

Malicious JavaScript
97.2% of the **malicious JavaScript** we saw arrived in **email**.

WatchGuard for the Win

2.5M
network attacks blocked by WatchGuard in Q1 2017

→ **156** attacks per participating **device**.

7M
malware variants blocked by WatchGuard in Q1 2017

→ **266** variants per participating **device**.

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

WatchGuard