# 2019 WEBROOT
# THREAT REPORT

## KEY REPORT STATS

Traditional attack approaches are still going strong, new threats emerge every day, and new vectors are being tried and tested. The details are in the data.

**WWW**

**40%** of malicious URLs were found on good domains

This percentage underscores the importance of leveraging URL-level intelligence, and not simply relying on URL whitelisting.
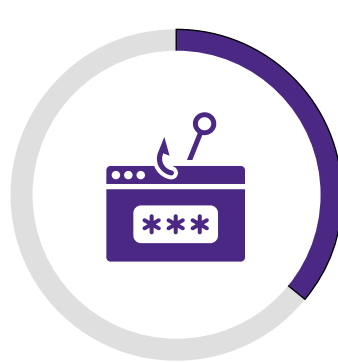
**36%** increase overall in the number of phishing attacks

As in years past, phishing attacks continue to be one of the most popular ways to attack both businesses and consumers. The number of phishing sites detected grew 220% between January and December of 2018.

**HTTPS**

**93%** of phishing domains in Sept. and Oct. 2018 offered an HTTPS site

As with all new security innovations, phishers have found a way to take advantage. They can add SSL certificates to malicious websites making them appear safe.

**54%** of devices that got infected once were re-infected the same year

"Repeat infections often have behavior-based causes. Users who frequent torrent sites for game cheats or activation keys should know these are almost always infected. Other behaviors like installing untrustworthy apps without carefully evading bundled software also contributes to repeat infections."

**– Grayson Milbourne, Security Intelligence Director**

**VS**
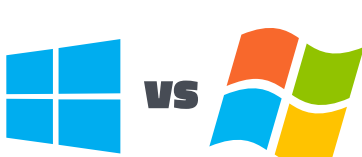
**Devices running Windows 10 are 2x as secure as those with Windows 7**

The operating system (OS) plays an important part in the amount of new malware and PUA files seen.
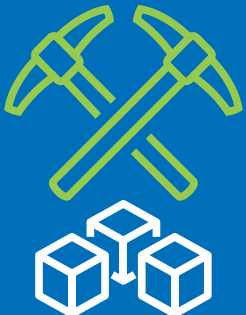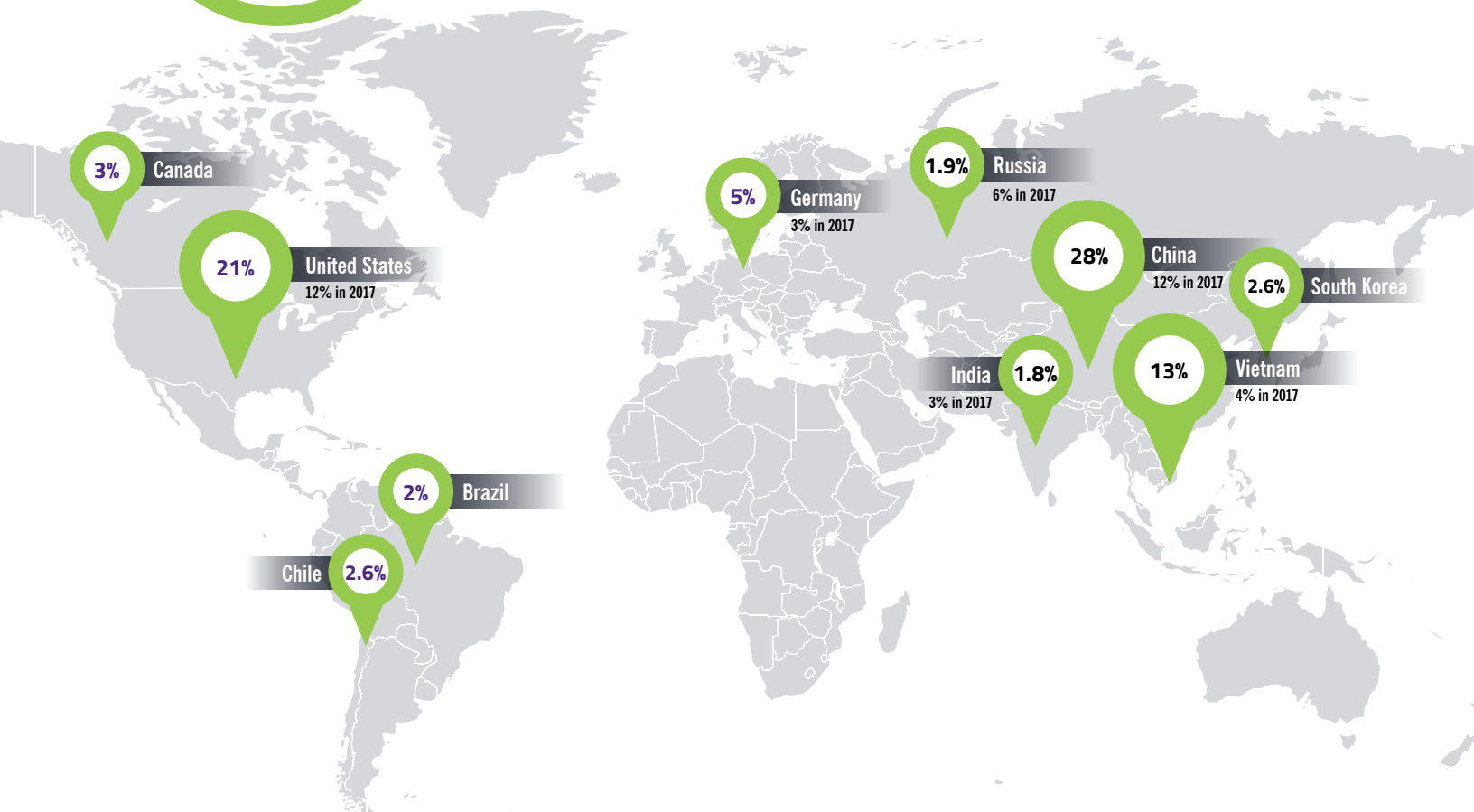
**IP**

**25 of the top recurring malicious IP addresses were reused 95 times**

It's important to keep in mind that IP addresses are not static and may cycle from malicious to benign and back multiple times.

## CHINA, THE U.S. AND VIETNAM ACCOUNT FOR 60+% OF ALL MALICIOUS IPS SEEN.

- 3% Canada
- 21% United States — 12% in 2017
- 2% Brazil
- 2.6% Chile
- 5% Germany — 3% in 2017
- 1.9% Russia — 6% in 2017
- 28% China — 12% in 2017
- 2.6% South Korea
- 1.8% India — 3% in 2017
- 13% Vietnam — 4% in 2017

## CRYPTOJACKING CONTINUES TO GROW

"Cryptojacking has been out over a year now, so people are aware of it and know how to block it. But the way they're blocking it with browser add-ons is very rudimentary. As this threat evolves and criminals start to obfuscate the domains, those add-ons will become obsolete and real-time threat intelligence will be the only effective way to block cryptojackers."

**– Tyler Moffit, Security Analyst**

The 2019 Webroot Threat Report provides a uniquely insightful global view into the analysis and discoveries made by the Webroot® Platform to provide insights on key trends and risks as seen by our users over the past year.

**WEBROOT®**
Smarter Cybersecurity™

webroot.com/2019ThreatReport