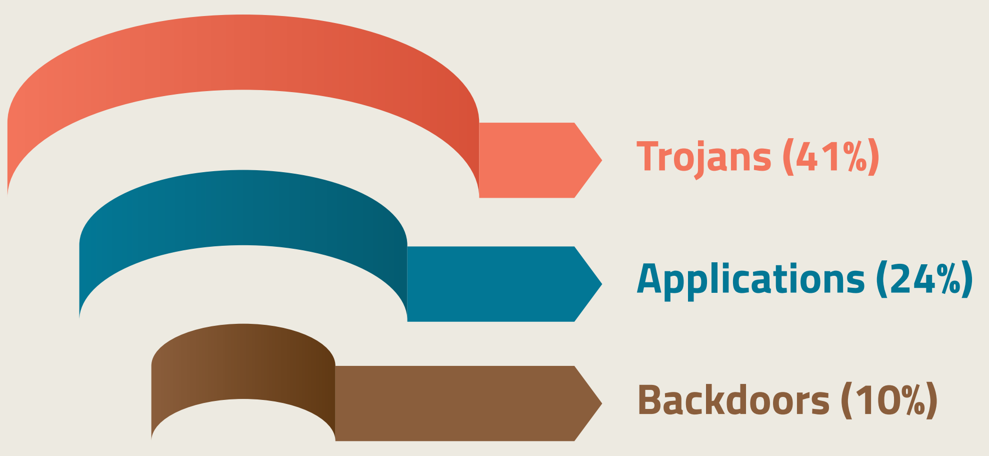
2017 Year of the Information Breach and Cyber Geopolitical Turmoil

Top Malware Types



Comodo Malware Detections

Trojans in 225 countries; **Russia #1** at **9%**

Applications in 226 countries; **U.S. #1** at **3%**

Backdoors in 184 countries; **Russia #1** at **19%**

Worms in 200 countries; **Russia #1** at **19%**

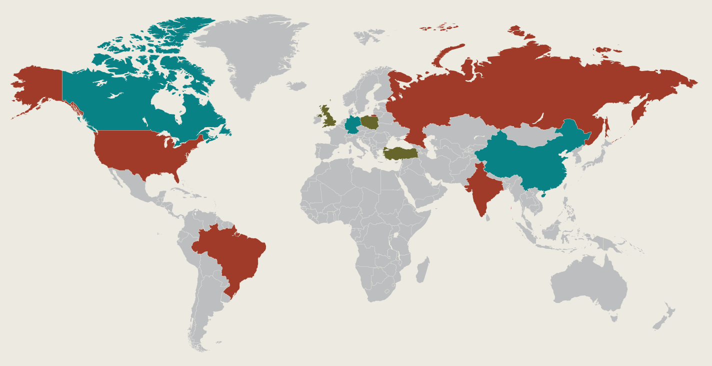
Unsafe applications in 183 countries; **U.S. #1** at **4%**

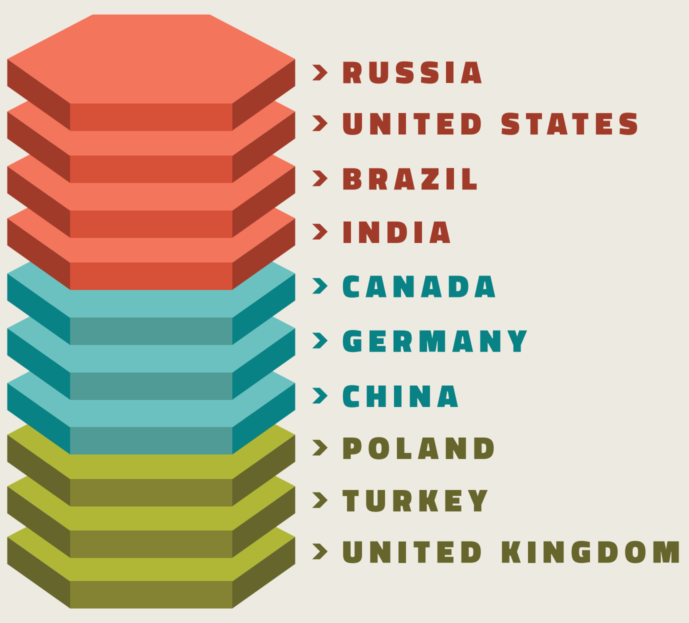
Unwanted applications in 184 countries; **U.S. #1** at **5%**

Viruses in 190 countries; **U.S. #1** at **9%**

Malware packers in 189 countries; **U.S. #1** at **2%**

Top Ten Countries of Detection





Malware Trends

Most malware types remained even or declined in Q4 2017. Notable exception: backdoors saw a significant rise in Q4 2017

Online services and technology the most- targeted verticals in 2017

From elections to North Korea nuclear threats and missile launches, it was also a year of geopolitical events that corresponded with major malware spikes.

KEY FINDINGS:

U.S. elections:

Massive spike in Kryptik trojans on Oct. 24, 2017, 94%+ of nearly 300,000 trojans focused on Virginia, where a close and hard-fought gubernatorial election took place

East Asia:

China experienced malware growth, with a virus surge of nearly 20,000 when President Xi visited U.S. in April 2017 and North Korea fired test missiles

Trojan attacks in China spiked to 30,000 during the Silk Road Summit in early to mid-May 2017, 40,000 in early August 2017 after an earthquake and a U.S.-China naval dispute, and 55,000 on Sept. 3, 2017, after China joined the U.S. and Russia in condemning a North Korea nuclear test

North Korea:

Startling Trojan increase on Sept. 19, 2017, corresponding with a speech at the United Nations where U.S. President Donald Trump threatened to destroy North Korea

Looking toward 2018, Comodo malware trendlines show:

- detection rate for trojans, worms, unsafe applications, and malware packers is currently down
- Holding steady are applications, unwanted applications, and viruses
- Most importantly for Q1 2018, backdoors are now on the rise
- Enterprises should shift some of their focus to the detection and mitigation of backdoors

Full report: https://www.comodo.com/ctrlquarterlyreport/2017summary/Comodo_2017Report.pdf