

# 2019 SONICWALL CYBER THREAT REPORT

Know their plans.  
Know their attacks.  
Know how to stop them.

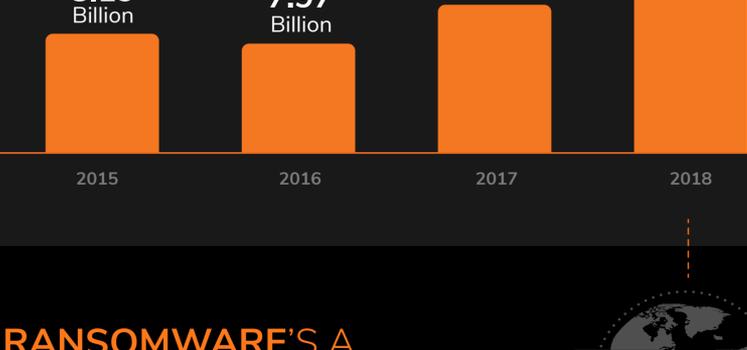
A cyberattack is personal. At its core, they strip organizations, their employees, partners and customers of intellectual property, identities, privacy, reputation and monetary assets. Follow the attack trends to understand how and where cybercriminals are targeting enterprises, government agencies and SMBs.

## MALWARE SPIKES TO RECORD VOLUME

# 10.52 Billion

malware attacks were logged by SonicWall in 2018 — the most ever on record. Since 2016, global malware attacks are up 33.4 percent.

GLOBAL MALWARE ATTACKS



## RANSOMWARE'S A GLOBAL RACKET

# 206.4 Million

ransomware attacks were recorded globally by SonicWall in 2018 — an 11 percent year-over-year spike. Some regions experience balanced attack volume. In others, like North America and Asia, attacks are targeted against specific countries, organizations or entities.



## KNOW WHAT YOU'RE FACING

Global data doesn't resonate until it affects a given person, business or organization. And actionable threat data helps organizations defend against the right attack vectors.

**24,979**  
Malware Attacks

**490**  
Ransomware Attacks

**1,276**  
Encrypted Threats

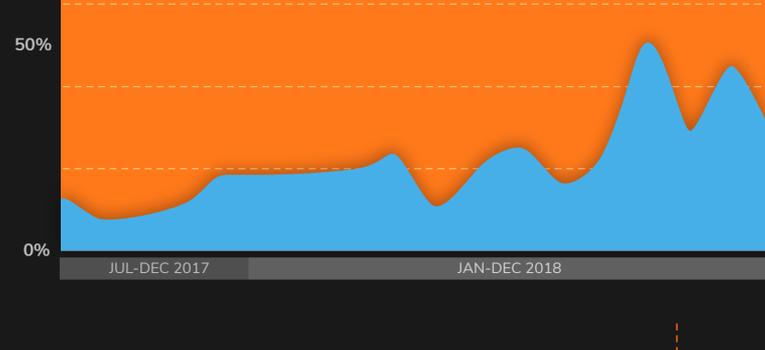


AVERAGE CYBERATTACKS FACED PER CUSTOMER

## DON'T TRUST THAT PDF

Cybercriminals are using PDFs and Office files to hide malware and circumvent network defenses. Most security controls cannot identify and mitigate malware hidden in these types of files. In 2018, SonicWall Capture ATP discovered and blocked new malware variants hidden in

# 47,073 PDF & 50,817 Office files



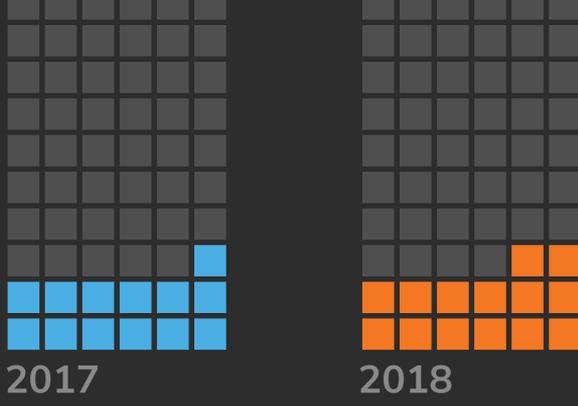
## NON-STANDARD PORTS ARE RIPE FOR EXPLOITATION

Locking the front door of your house but leaving the windows open isn't a sound security strategy. That's why cybercriminals are targeting a range of non-standard ports to ensure their payloads can be deployed undetected.

# 19.2% of all malware attacks came across non-standard ports in 2018.

Most organizations aren't safeguarding this vector because of performance and cost concerns, leaving millions of attacks unchecked.

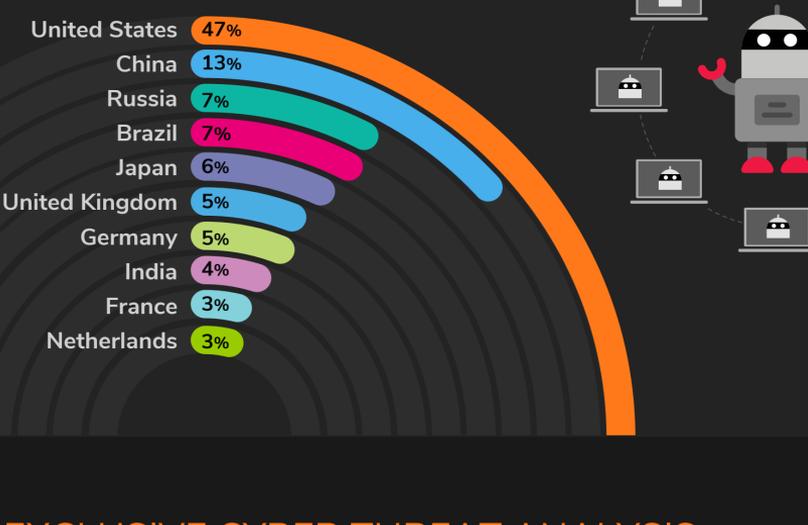
**17.7%** (2017) vs **19.2%** (2018)



## BOTNETS ARE LURKING, BUT NOT WHERE YOU THINK

Illegal botnets are created by compromising servers, routers, computers, IoT devices and other hardware connected to the internet. They're used to perform distributed denial-of-service (DDoS) attacks, steal data and send spam.

TOP 10 COUNTRIES HOSTING BOTNETS



## EXCLUSIVE CYBER THREAT ANALYSIS ONLY FROM SONICWALL CAPTURE LABS

**26 Million**  
Phishing Attacks

**3.9 Trillion**  
Intrusion Events

**27%**  
Jump in Encrypted Threats

Visit [SonicWall.com/ThreatReport](https://www.sonicwall.com/ThreatReport) to download the complete 2019 SonicWall Cyber Threat Report. You'll gain new perspectives on cybercriminal attack strategies and understand how to properly defend your organization or business from the most sophisticated cyberattacks.

[LEARN MORE](#)



[Twitter](#) [LinkedIn](#) [Facebook](#) [Instagram](#) | [SonicWall.com](https://www.sonicwall.com) | [#KnowTheThreats](#)

\* As a best practice, SonicWall routinely optimizes its methodologies for data collection, analysis and reporting. This includes improvements to data cleansing, changes in data sources and consolidation of threat feeds. Figures published in previous reports may have been adjusted across different time periods, regions or industries.

The materials and information contained in this document, including, but not limited to, the text, graphics, photographs, artwork, icons, images, logos, downloads, data and compilations, belong to SonicWall or the original creator and is protected by applicable law, including, but not limited to, United States and international copyright law and regulations.