2019 SONICWALL
Cyber Threat Report

EXECUTIVE SUMMARY | EUROPE EDITION

SonicWall.com

SONICWALL®
CAPTURE LABS

INTRODUCTION: EUROPE EDITION

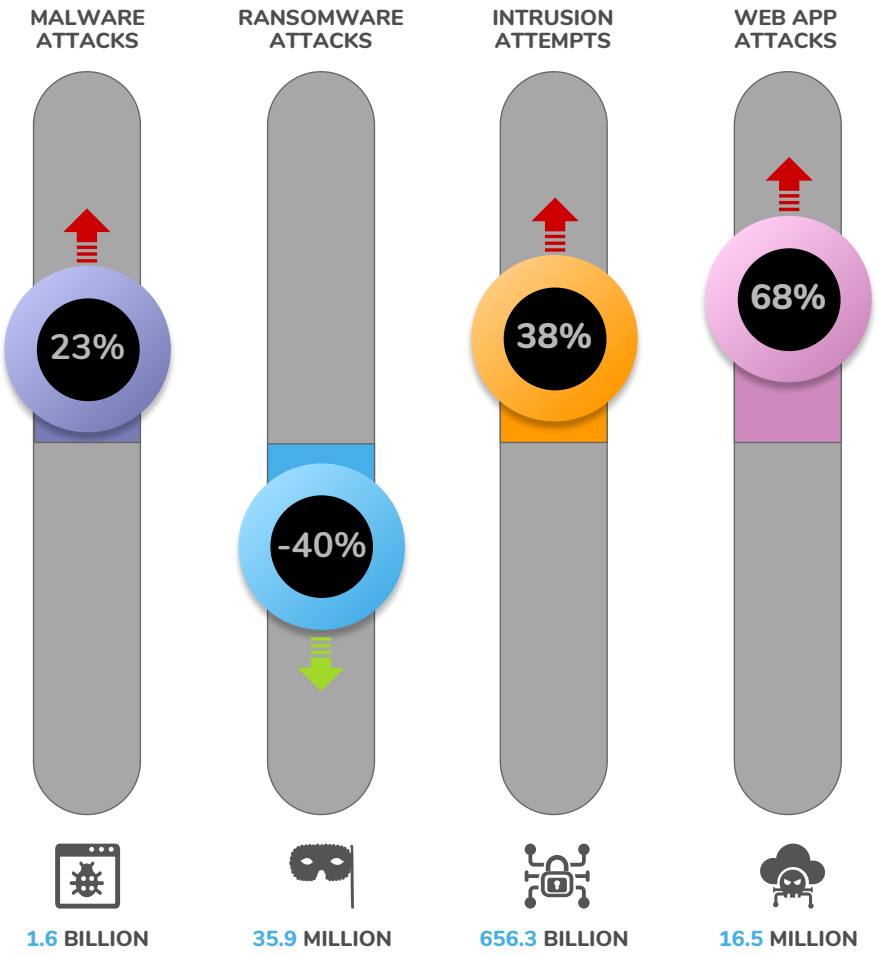
The cyber arms race does not discriminate or differentiate. If a network, identity, device or data is valuable — particularly information tied to intellectual property, financials, sensitive files, critical infrastructure or political leverage — cybercriminals will identify, target and ruthlessly attack.

To promote global awareness and facilitate important dialogues, SonicWall remains steadfast in its commitment to research, analyze and share threat intelligence via the 2019 SonicWall Cyber Threat Report. A complement to the in-depth report, this executive summary provides a high-level perspective on the threat intelligence from SonicWall Capture Labs threat researchers.

SONICWALL®

KEY FINDINGS FOR 2018

2018 EUROPEAN CYBERATTACK TRENDS



- Albania
- Andorra
- Austria
- Belarus
- Belgium
- Bosnia & Herzegovina
- Bulgaria
- Croatia
- Cyprus
- Czechia
- Denmark
- Estonia
- Finland
- France
- Germany
- Gibraltar
- Greece
- Guernsey
- Hungary
- Iceland
- Ireland
- Isle of Man
- Italy
- Jersey
- Latvia
- Liechtenstein
- Luxembourg
- Macedonia
- Malta
- Netherlands
- Norway
- Poland
- Portugal
- Lithuania
- Romania
- Russia
- San Marino
- Serbia
- Slovakia
- Slovenia
- Spain
- Sweden
- Switzerland
- Ukraine
- United Kingdom

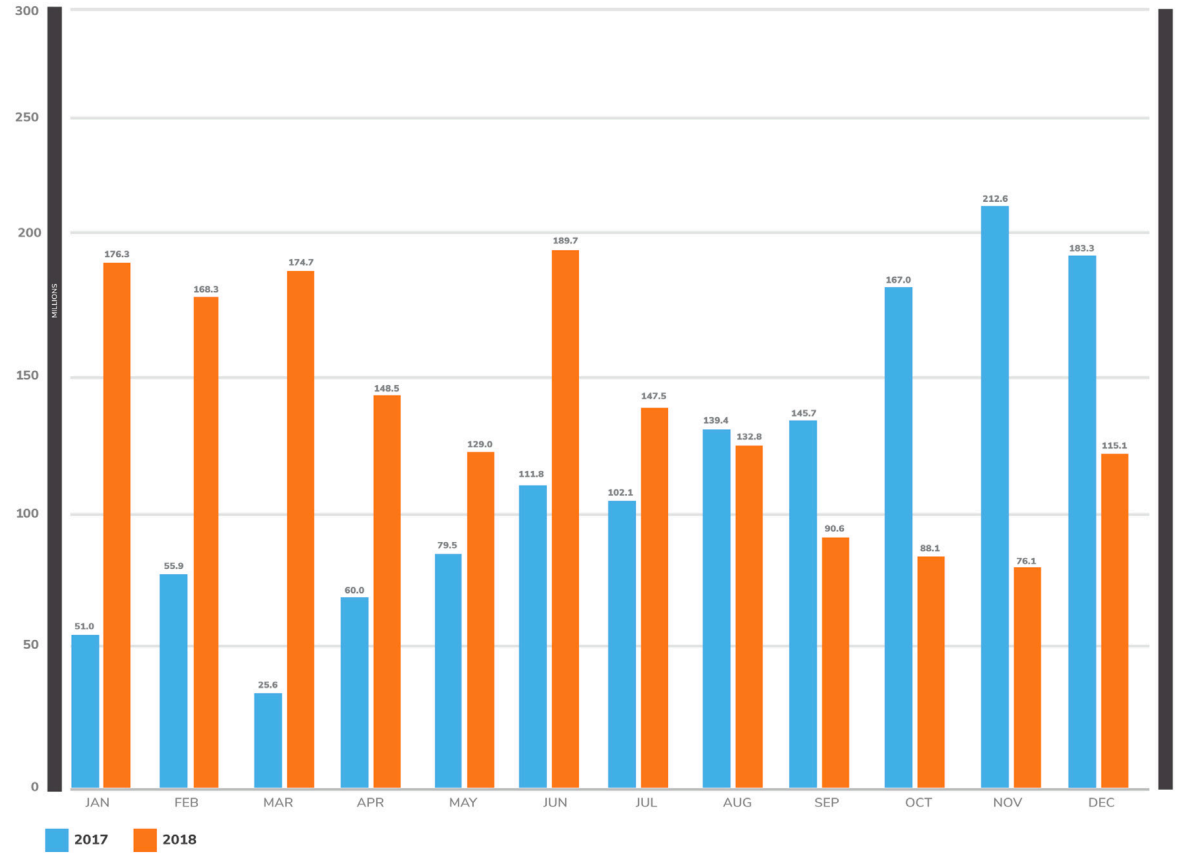
SONICWALL®

MALWARE VOLUME STILL CLIMBING

In 2016, the industry witnessed a decline in malware volume, leading some to speculate that cybercrime was on the decline. Since then, **malware attacks have increased 33.4 percent.**

Globally, SonicWall logged 10.52 billion* malware attacks in 2018 — the most ever on record. In Europe, SonicWall identified **1.64 billion** malware attacks, a 23 percent spike over 2017. Interestingly, despite the increased volume in 2018, attack volume began to trend down in June 2018.

2018 EUROPEAN MALWARE VOLUME



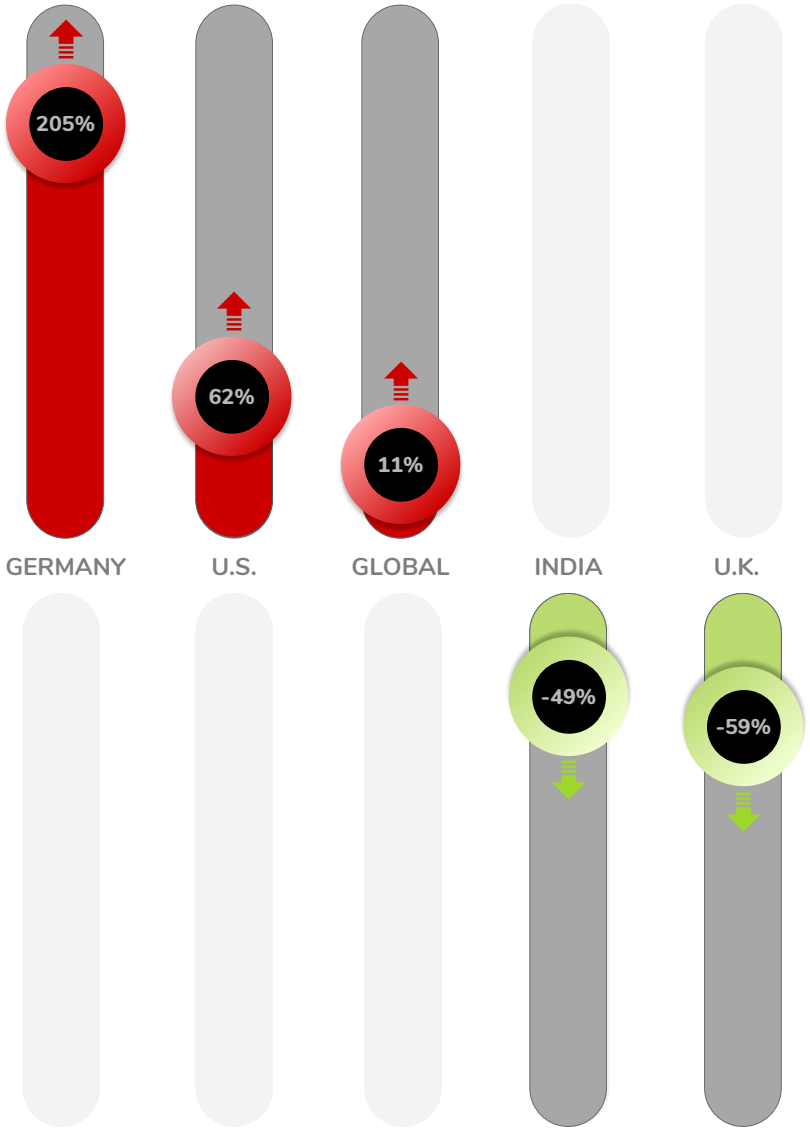
* As a best practice, SonicWall routinely optimizes its methodologies for data collection, analysis and reporting. This includes improvements to data cleansing, changes in data sources and consolidation of threat feeds. Figures published in previous reports may have been adjusted across different time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

U.K., INDIA HARDEN AGAINST RANSOMWARE

After SonicWall Capture Lab threat researchers finished analyzing full-year 2018 threat data, a shocking revelation was made. Ransomware was up in just about every geographic region but two: the U.K. and India.

While major countries across North America, Europe and Asia were all experiencing significant increases in ransomware attacks, the **U.K. and India quietly faced 59 and 49 percent reductions,** respectively, in ransomware volume.

At a country level, **Germany was targeted in 27.6 percent of all European ransomware attacks**. Italy (23 percent), the U.K. (13.2 percent), the Netherlands (10.7 percent) and France (9.9 percent) rounded out the region's top targets.



DANGEROUS MEMORY THREATS, SIDE-CHANNEL ATTACKS IDENTIFIED EARLY

SonicWall Real-Time Deep Memory Inspection (RTDMI™) mitigates dangerous side-channel attacks utilizing patent-pending technology. Side-channels are the fundamental vehicle used to exploit and exfiltrate data from processor vulnerabilities, such as Foreshadow, PortSmash, Meltdown, Spectre and Spoiler.

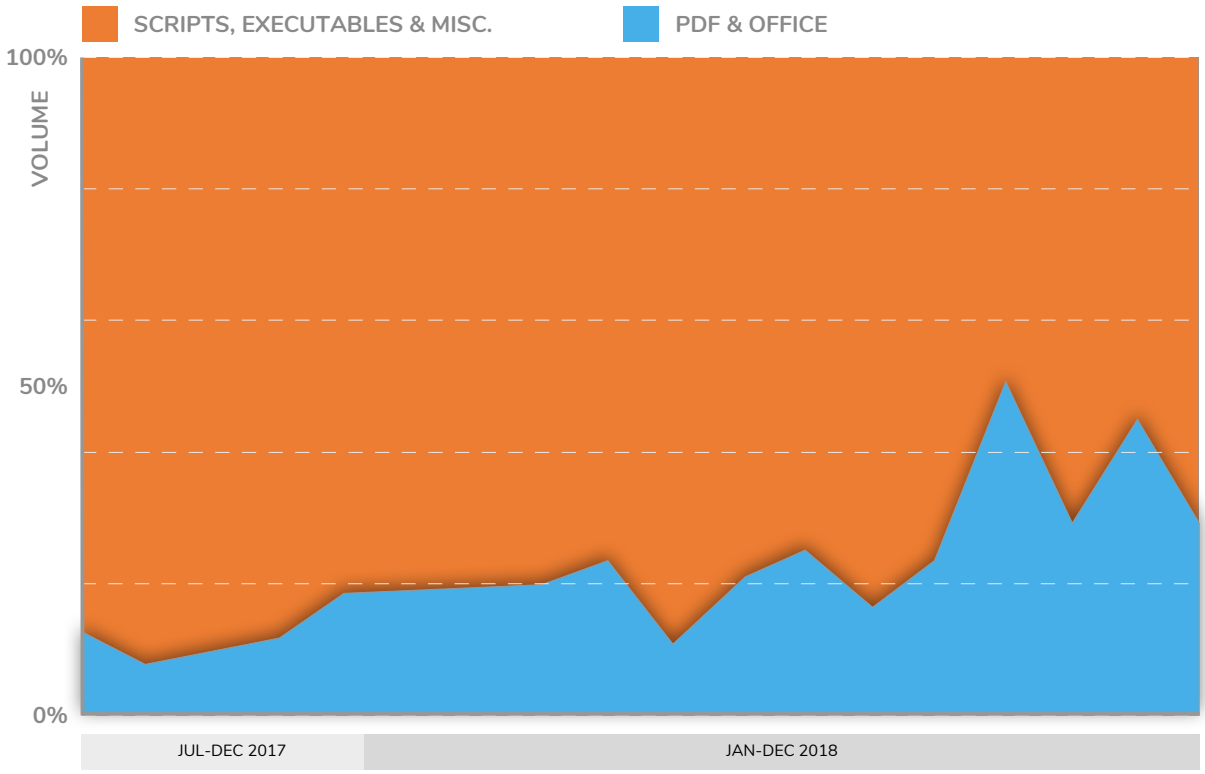
Unfortunately, current research declares **'Spectre is here to stay'** and acknowledges various vulnerabilities in processors cannot be patched — either in software or hardware — and are a much deeper security concern. As such, side-channel attacks will be a continued risk to the computing landscape, which will make technology that can mitigate these attacks a necessary requirement.

SONICWALL®

MALICIOUS PDF & OFFICE FILES BEATING LEGACY SECURITY CONTROLS

Cybercriminals are tooling trusted PDFs and Office files to help malware circumvent traditional firewalls and even single-engine sandboxes.

INCREASE IN MALICIOUS PDFs & OFFICE FILES



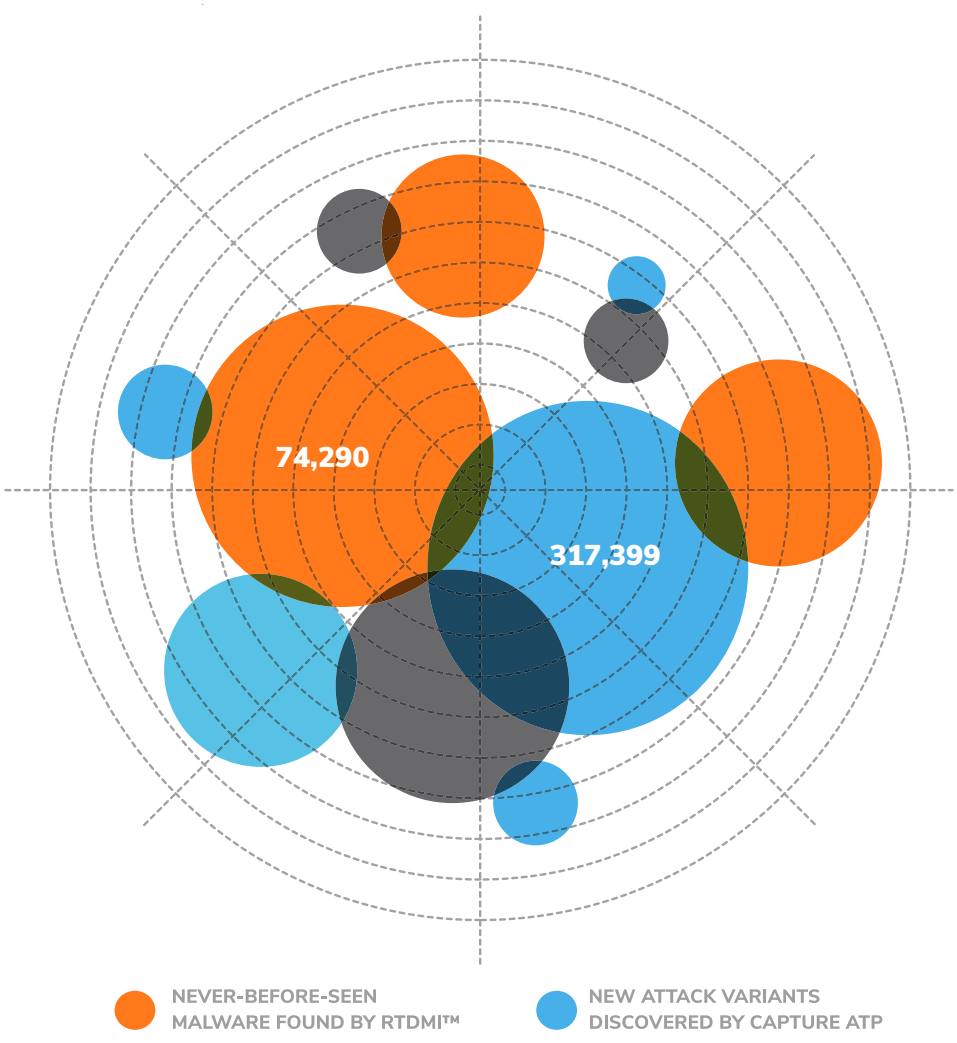
The multi-engine SonicWall Capture ATP sandbox service found **malware hidden in 47,073 PDFs and 50,817 Office files** in 2018. While volume appears low at a glance, most security controls cannot identify and mitigate malware hidden in these files, greatly increasing the success of the payload.

MACHINE LEARNING MATURING TO STOP NEVER-BEFORE-SEEN MALWARE VARIANTS

SonicWall Capture Advanced Threat Protection (ATP) identified 391,689 new attack variants in 2018. That averages to more than **1,072 new attacks discovered and blocked each day.**

Capture ATP utilizes a multi-engine cloud sandbox in parallel with SonicWall RTDMI™ technology. Both of these capabilities have been dynamically self-learning and self-enhancing throughout 2018.

Specifically, **RTDMI™ identified 74,290 never-before-seen attacks in 2018.** These are malware variants that are so new, unique or complex that no other vendor in the world had been able to track or create signatures for them at the time SonicWall discovered them.

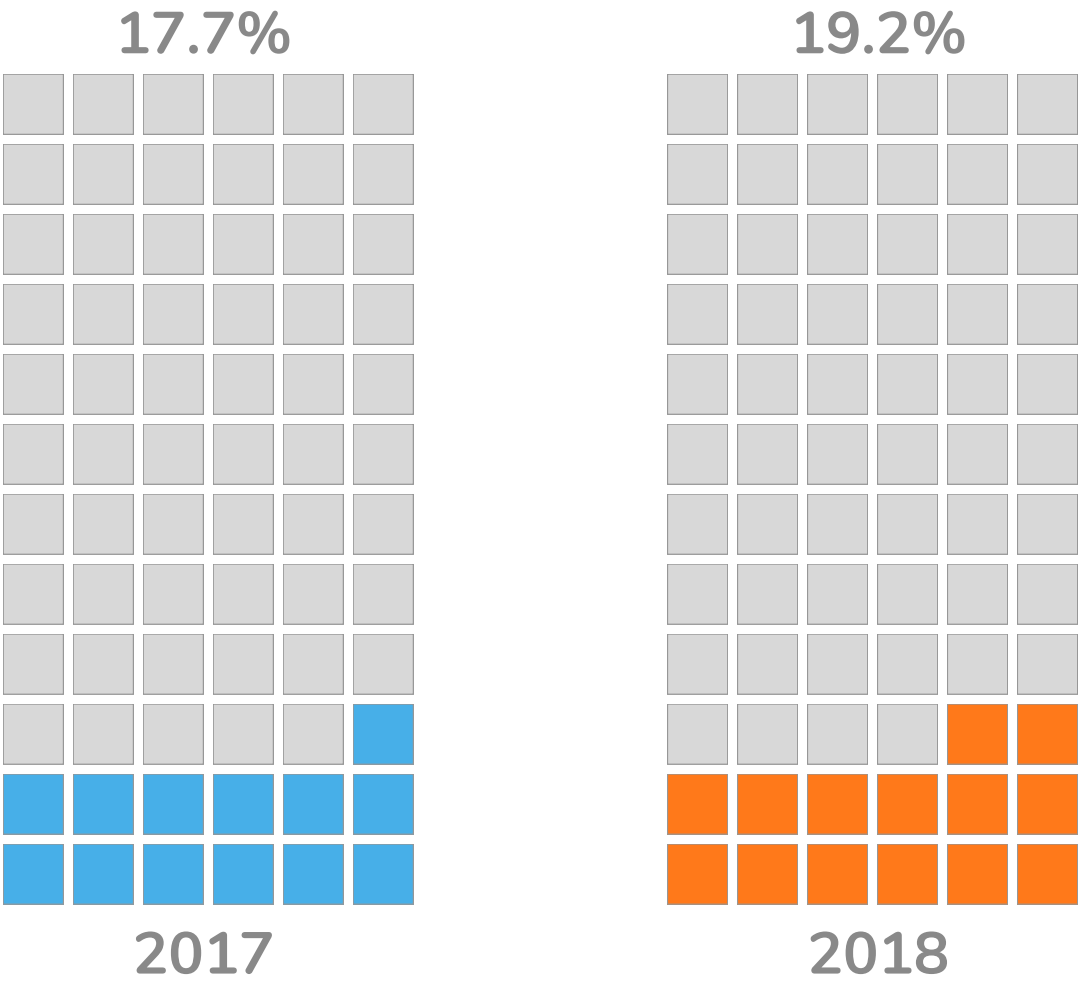


SONICWALL®

NON-STANDARD PORTS RIPE FOR EXPLOITATION

Ports 80 and 443 are standard ports for web traffic, so they are where most firewalls focus their protection. In response, cybercriminals are targeting non-standard ports to ensure their payloads can be deployed undetected in a target environment.

2018 MALWARE ATTACKS
OVER NON-STANDARD PORTS

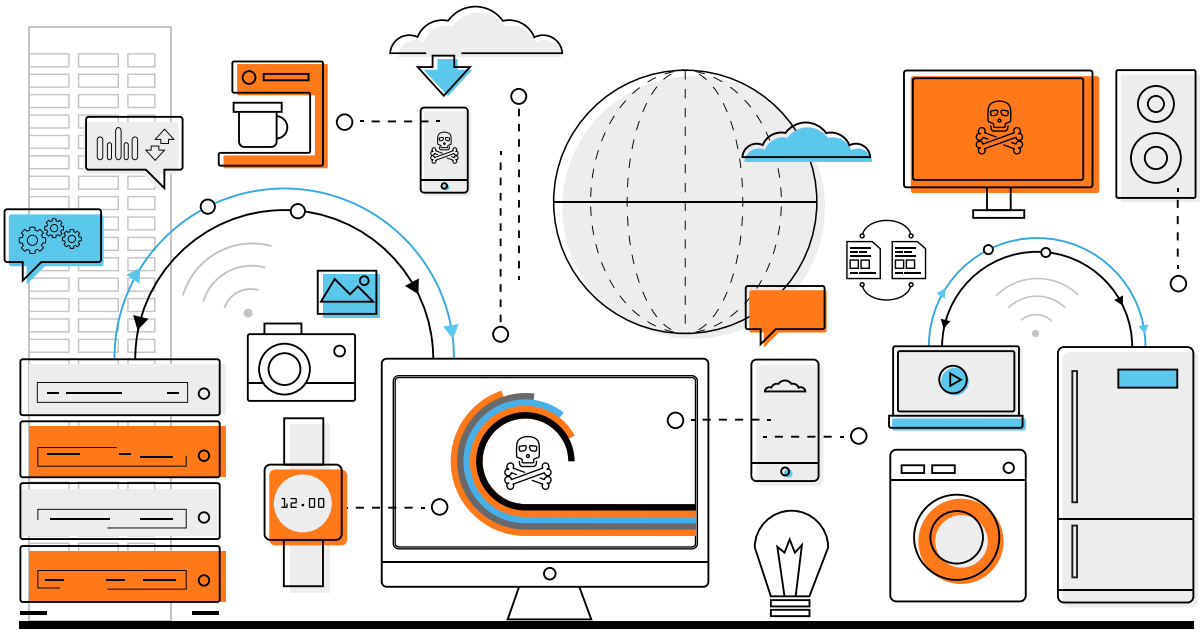


Based on a sampling of more than 700 million malware attacks, SonicWall found that **19.2 percent of all malware attacks came across non-standard ports** in 2018. Because there are so many to monitor, traditional proxy-based firewalls can't mitigate attacks over non-standard ports (for both encrypted and non-encrypted traffic).

IoT ATTACKS ESCALATING

Consumers are hungry for connected devices. But this appetite has resulted in a deluge of Internet of Things (IoT) devices rushed to market without proper security controls. In many cases, IoT devices are set up with default security settings, making them easy to compromise via known credentials or powerful botnets.

All told, SonicWall recorded **32.7 million IoT attacks in 2018**, a 217.5 percent increase over the 10.3 million IoT attacks the company logged in 2017.



ENCRYPTED ATTACKS GROWING STEADY

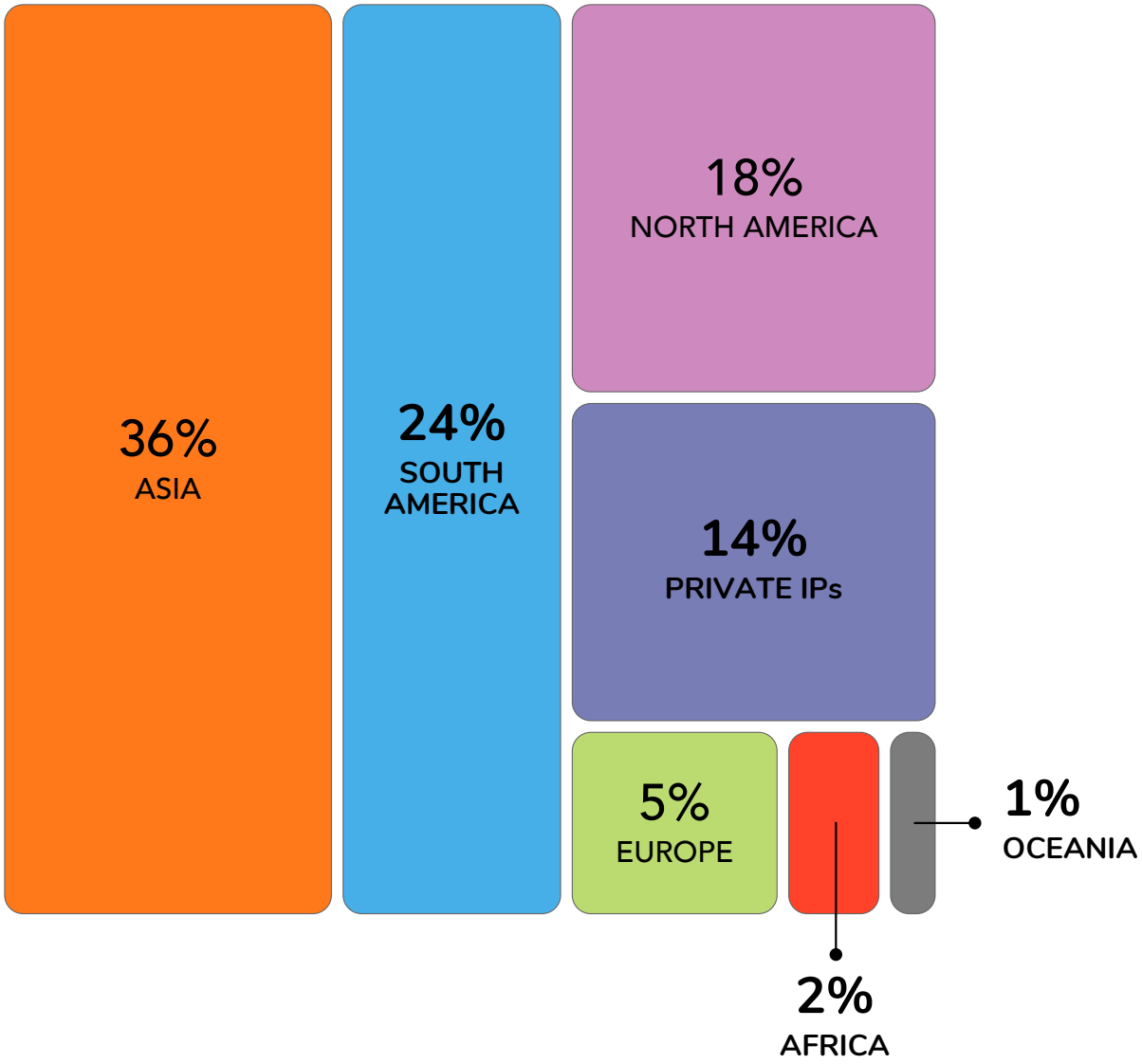
The growth in encrypted traffic is coinciding with more attacks being cloaked by TLS/SSL encryption. More than **2.8 million attacks were encrypted** in 2018, a 27 percent increase over 2017.

THE RISE & FALL OF CRYPTOJACKING

In 2018, cryptojacking vanished nearly as fast is it appeared. SonicWall recorded **57.5 million cryptojacking attacks** globally between April and December. The volume peaked in September with 13.1 million recorded attacks, but has been on a steady decline since.

According to SonicWall data, Europe only faced 5 percent of all global cryptojacking attacks in 2018. Despite falling prices, cryptocurrencies remain a valuable commodity to cybercriminals because of its anonymity.

2018 CRYPTOJACKING BY REGION



GLOBAL PHISHING VOLUME DOWN, ATTACKS MORE TARGETED

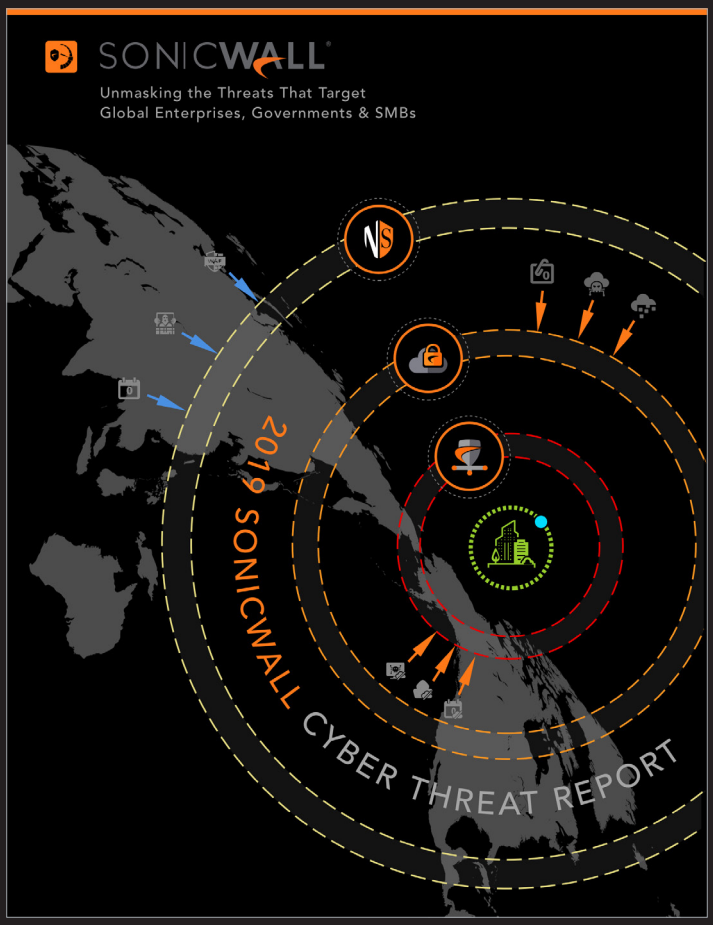
PHISHING ATTACKS WORLDWIDE **26 MILLION**

As businesses get better at blocking email attacks and ensuring employees can spot and delete suspicious emails, attackers are shifting tactics. They're reducing overall attack volume and launching more highly targeted phishing attacks (e.g., business email compromise, account takeovers, whale phishing, etc.).

In 2018, SonicWall recorded **26 million phishing attacks worldwide**, a 4.1 percent drop from 2017. The average SonicWall customer faced 5,488 phishing attacks in 2018.

Exclusive cyber threat intelligence and analysis. Only from SonicWall Capture Labs.

LEARN MORE



Visit 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.

* 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.

SONICWALL