MID-YEAR UPDATE

2020 SONICWALL CYBER THREAT REPORT

GET THE UPDATE »

#KnowTheThreats

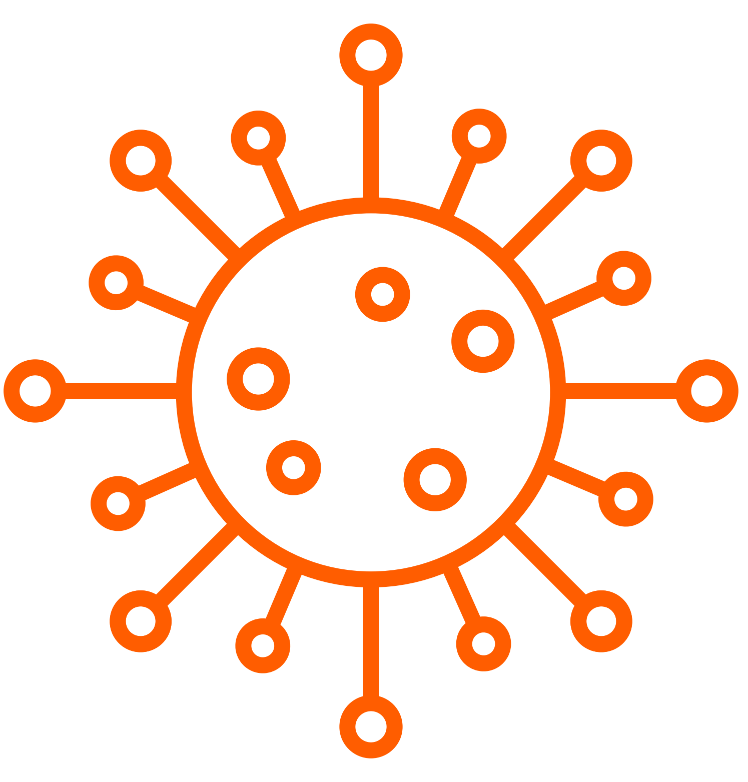
OVER THE PAST SIX MONTHS,

as the COVID-19 pandemic ravaged its way across the globe, we've seen shifts — that we thought would take decades — happen virtually overnight.

While the historic disruption has been challenging for businesses and governments, it's been a boon for cybercriminals.

121.4m RANSOMWARE MORE SURGICAL THAN EVER.

Despite a drop in overall malware (-33%), ransomware remains the payload of choice for cybercriminals. **Ransomware attacks are up 20% in the first half of 2020 globally**, and spiked 109% in the United States.



PROFITING OFF THE PANDEMIC.

SonicWall began seeing attacks, scams and exploits specifically based around COVID-19 on Feb. 4, and since then have detailed **at least 20 different types of attacks** across just about every category, including:

- MALWARE
- RANSOMWARE
- CRYPTOMINERS
- TROJANS
- RATs
- SPAM
- SCAREWARE & OTHERS

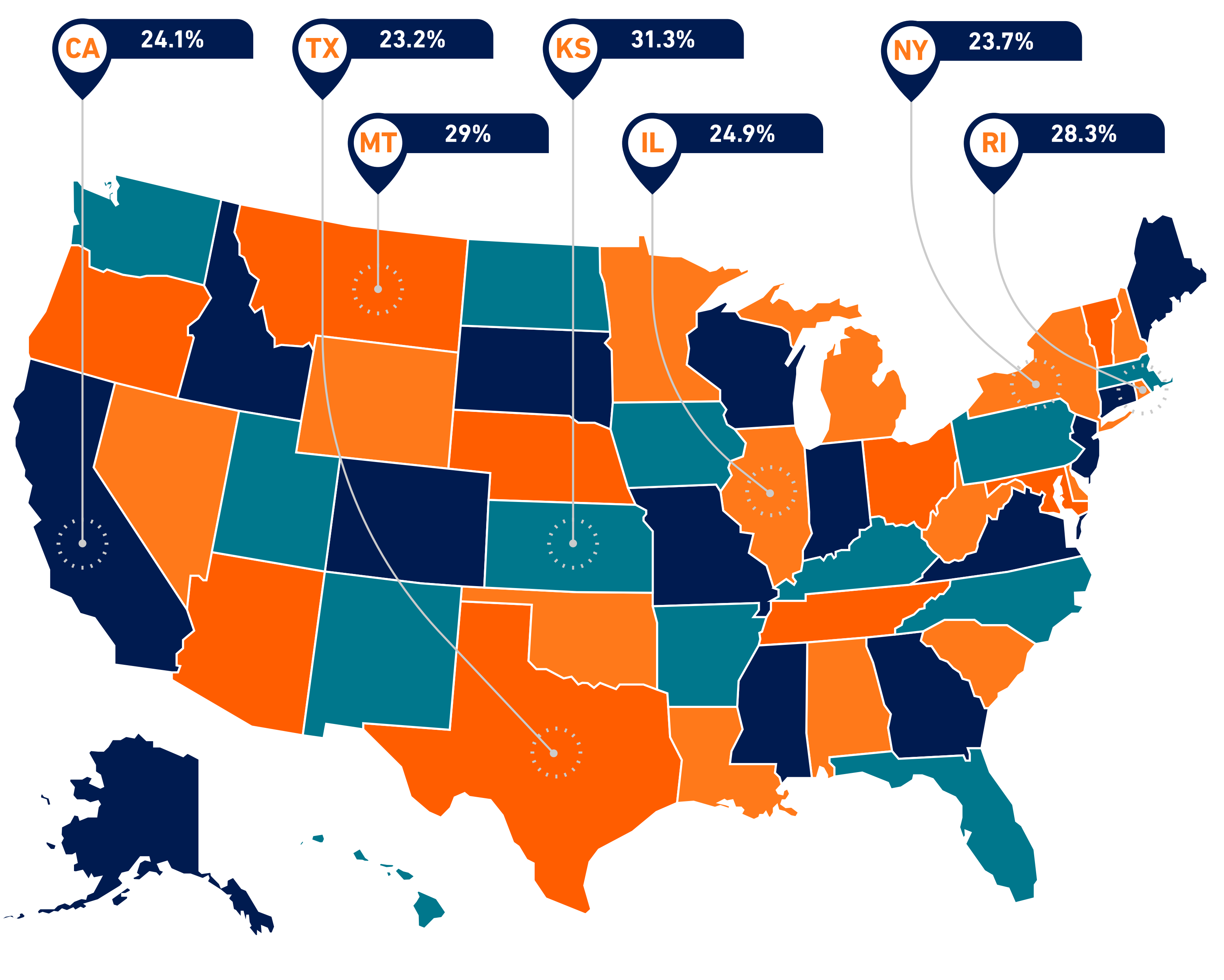
> "It was only a matter of time before a nation state resorted to cybercrime to influence or control global healthcare during a time of great need."
>
> BILL CONNER | PRESIDENT & CEO | SONICWALL | NEWSWEEK INTERNATIONAL, JULY 16, 2020

IS YOUR STATE AT RISK TO A CYBERATTACK?

In the U.S., California had by far the largest number of malware hits with **304.1 million** total. But it isn't the riskiest state — or even in the top half.

In fact, an organization is more likely to encounter malware in Kansas, where nearly a third (31.3%) of SonicWall sensors registered a hit.

% of SonicWall sensors that registered malware hits by state

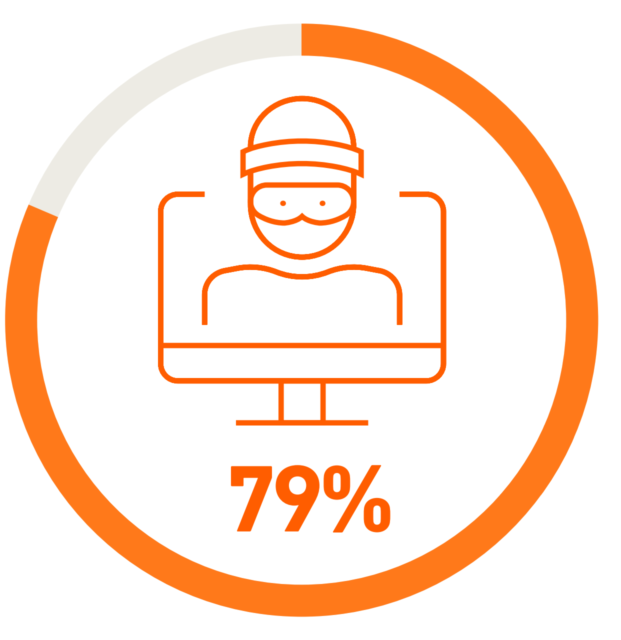


IOWA 28.1%
HAWAII 27.7%
WEST VIRGINIA 27.4%
VERMONT 27.2%

IDAHO 27.2%
LOUISIANA 27.2%
FLORIDA 26.7%
VIRGINIA 26.6%

OREGON 26.5%
NEW MEXICO 26.4%
MICHIGAN 26.3%
NEBRASKA 26.3%

NEW JERSEY 26.3%
PENNSYLVANIA 26.1%
NEVADA 26%
MARYLAND 26%



RANSOMWARE IS TOP OF MIND.

When asked what type of cyberattacks influenced their decision to purchase a SonicWall TZ firewall, 79% of surveyed organizations said "ransomware."

SOURCE: TECHVALIDATE SURVEY OF 250 CUSTOMERS OF SONICWALL NETWORK SECURITY

WHAT'S HIDING IN YOUR OFFICE FILES?

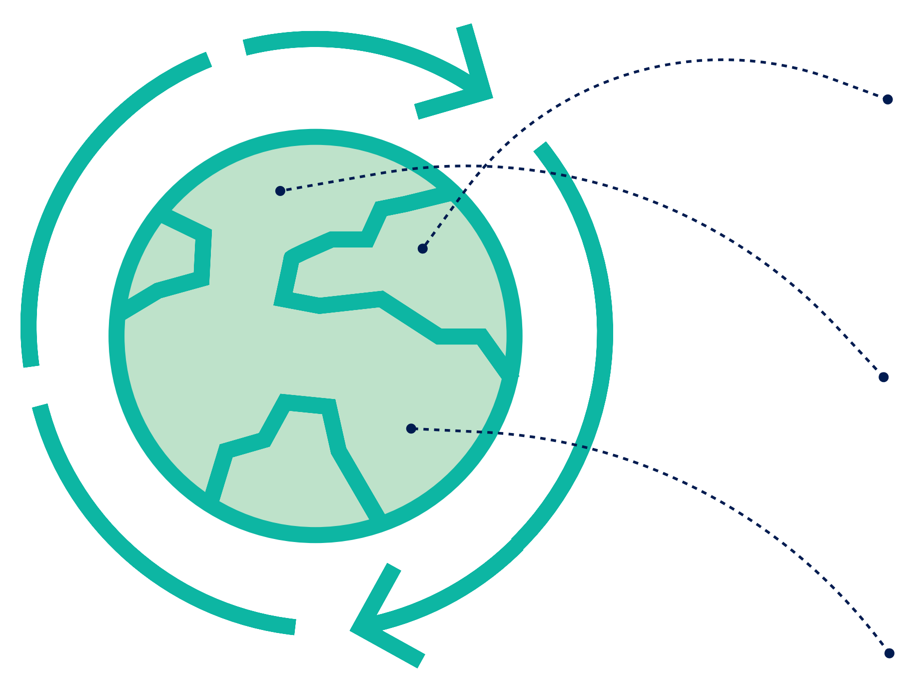
More and more malware is hidden within trusted Office files. In the first half of 2020, SonicWall recorded a 176% increase in all-new malicious Office files. See full report for breakdown >

#WFH DRIVING SPIKE IN IoT ATTACKS.

Since January, SonicWall recorded 20.2 million IoT attacks — a 50% spike year-to-date. If the current pattern holds, total IoT attacks will surpass both 2018 and 2019 levels. Unchecked IoT devices can provide cybercriminals an open door into what may otherwise be a well-secured organization.

IoT ATTACKS +50%
YEAR-TO-DATE

GLOBAL CYBERATTACK TRENDS



41.4m Cryptojacking Attacks

+19% Intrusion Events

1in12 Customers Saw an Encrypted Attack

THRIVE IN THE NEW BUSINESS NORMAL.

Visit **SonicWall.com/ThreatReport** to download the complimentary mid-year update to the 2020 SonicWall Cyber Threat Report. Gain the latest cyber threat intelligence for navigating the new business normal.

GET THE UPDATE »

#KnowTheThreats

SONICWALL
CAPTURE LABS

SonicWall.com

*As a best practice, SonicWall routinely optimized its methodologies for data collection, analysis and reporting. This includes adjustments 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.

Infographic-2020ThreatReportMidYear-COG-2452