AGGIORNAMENTO SEMESTRALE

RAPPORTO SONICWALL 2020 SULLE CIBERMINACCE

#KnowTheThreats

SCARICATE L'AGGIORNAMENTO »

NEGLI ULTIMI SEI MESI,

con il diffondersi della pandemia di COVID-19 nel mondo, abbiamo assistito a cambiamenti – che pensavamo avrebbero richiesto decenni – praticamente da un giorno all'altro.

Mentre questo sconvolgimento storico ha messo a dura prova aziende e governi, per i cibercriminali è stato una manna.

121,4 milioni DI RANSOMWARE PIÙ CHIRURGICI CHE MAI.

Nonostante il calo complessivo dei malware (-33%), il ransomware resta la scelta vincente per i cibercriminali. **Gli attacchi ransomware sono aumentati del 20% nella prima metà del 2020 a livello globale**, toccando il 109% negli Stati Uniti.

SFRUTTARE LA PANDEMIA.

Il 4 febbraio SonicWall ha iniziato a notare attacchi, truffe ed exploit riconducibili al COVID-19, e da allora ha individuato almeno **venti diversi tipi di attacchi** nelle varie categorie:

- MALWARE
- RANSOMWARE
- CRIPTOMINAZIONE
- TROJAN
- RAT
- SPAM
- SCAREWARE E ALTRI

> "È stata solo una questione di tempo perché gli stati nazionali facessero ricorso al cibercrimine per condizionare o controllare l'assistenza sanitaria globale in un momento di grande bisogno."

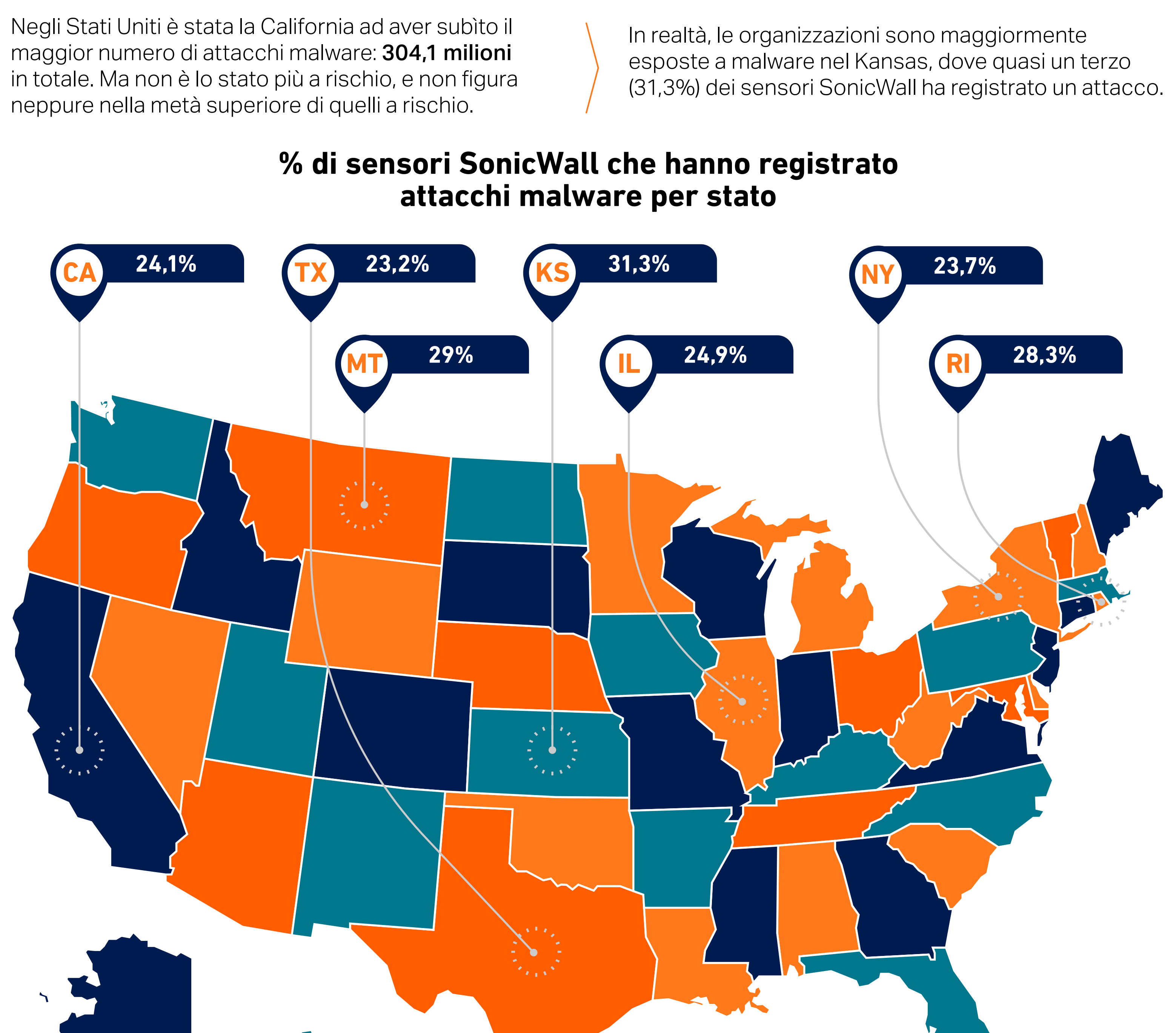
BILL CONNER | PRESIDENTE E CEO | SONICWALL | NEWSWEEK INTERNATIONAL, 16 LUGLIO 2020

IL VOSTRO STATO È A RISCHIO DI CIBERATTACCO?

Negli Stati Uniti è stata la California ad aver subìto il maggior numero di attacchi malware: **304,1 milioni** in totale. Ma non è lo stato più a rischio, e non figura neppure nella metà superiore di quelli a rischio.

In realtà, le organizzazioni sono maggiormente esposte a malware nel Kansas, dove quasi un terzo (31,3%) dei sensori SonicWall ha registrato un attacco.

% di sensori SonicWall che hanno registrato attacchi malware per stato



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%

79%

IL RANSOMWARE È IL PRIMO PROBLEMA.

Alla domanda su quale tipo di ciberattacchi avesse influenzato la loro decisione di acquistare un firewall SonicWall TZ, il 79% delle organizzazioni intervistate ha risposto "il ransomware."

FONTE: INDAGINE TECHVALIDATE SU 250 CLIENTI DI SONICWALL NETWORK SECURITY

+176%

CHE COSA SI NASCONDE NEI FILE DI OFFICE?

Sempre più malware si nascondono in file di Office apparentemente affidabili. Nella prima metà del 2020 SonicWall ha registrato un aumento del 176% in file Office dannosi completamente nuovi.
Per l'analisi vedere il rapporto completo >

#WFH PICCO DI ATTACCHI IoT.

Da gennaio SonicWall ha registrato 20,2 milioni di attacchi IoT, con un picco del 50% da inizio anno. Se prosegue la tendenza attuale, gli attacchi IoT totali supereranno i livelli del biennio 2018-2019. I dispositivi IoT non controllati possono offrire ai cibercriminali una porta aperta in organizzazioni altrimenti ben protette.

+50% DI ATTACCHI IoT
DA INIZIO ANNO

TENDENZE GLOBALI DEI CIBERATTACCHI

41,4 milioni
Attacchi di cryptojacking

+19%
Eventi intrusivi

1su12
Attacchi crittografati notati dai clienti

PROSPERARE NELLA NUOVA NORMALITÀ OPERATIVA.

Visitare **SonicWall.com/ThreatReport** per scaricare gratuitamente l'aggiornamento semestrale del Rapporto SonicWall 2020 sulle ciberminacce. Acquisite le ultime informazioni in materia di ciberintelligenza delle minacce per orientarvi nella nuova normalità operativa.

SCARICATE L'AGGIORNAMENTO »

#KnowTheThreats

SONICWALL CAPTURE LABS

SonicWall.com

*A livello di miglior prassi, SonicWall ottimizza di routine le sue metodologie di acquisizione, analisi e reportistica dei dati. Ciò si espleta anche attraverso adeguamenti al filtraggio dei dati, cambiamenti a livello delle fonti dei dati e consolidamento dei feed delle minacce. I dati pubblicati nei rapporti precedenti possono essere stati adeguati per periodi, regioni e settori industriali diversi.

Infographic-2020ThreatReportMidYear-COG-2452