2020

RELATÓRIO DE AMEAÇAS CIBERNÉTICAS DA SONICWALL

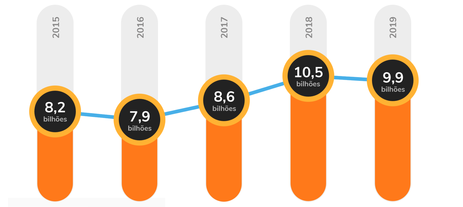
O perímetro de seu império digital não tem mais fronteiras. O que antes era um espaço finito e fácil de proteger agora é um território sem limites — uma área imensa e caótica de dispositivos, aplicações, appliances, servidores, redes, nuvens e usuários.

Explore a inteligência sobre ameaças, exclusiva da SonicWall, para entender melhor como os cibercriminosos pensam — e esteja totalmente preparado para o que farão em seguida.

O MALWARE RECUOU, PORÉM TORNOU-SE MAIS DIRECIONADO E EVASIVO

9,9 bilhões

de ataques de malware foram registrados* pela SonicWall em 2019, uma queda de 6% em relação ao recorde de 10,52 bilhões registrados em 2018.



RANSOMWARE ENCONTROU UM NOVO ALVO

187,9 milhões

Ransomware está sendo usado para atacar, com precisão, vítimas com maior probabilidade de pagar pelos dados confidenciais que possuem ou que têm recursos financeiros à sua disposição (ou ambos).

Em 2019, isso significou que muitos dos 187,9 milhões de ataques de ransomware tiveram como alvos governos em diversos níveis, além de sistemas de educação.

O CRYPTOJACKING ESTÁ DESABANDO

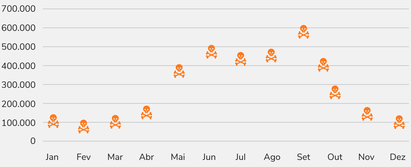
O preço do bitcoin e de criptomoedas complementares criou uma situação insustentável entre o malware de cryptojacking baseado em Coinhive e o serviço legítimo de mineração Coinhive.

78% ↓ Após o encerramento do Coinhive, o volume de ataques bem-sucedidos de cryptojacking caiu 78% durante o segundo semestre de 2019.

PICOS DE FILELESS MALWARE NO TERCEIRO TRIMESTRE

O fileless malware existe exclusivamente como artefato baseado em memória e não grava nenhuma parte da atividade mal-intencionada no disco rígido do computador, tornando-se muito resistente a estratégias forenses. O volume atingiu um pico no terceiro trimestre, com mais de 570.000 ataques registrados pela SonicWall apenas em setembro de 2019.

Volume de fileless malware em 2019



AS AMEAÇAS CRIPTOGRAFADAS CONTINUAM AUMENTANDO SEM PARAR

Os cibercriminosos experientes continuam usando a criptografia TLS/SSL para ocultar seus ataques da inspeção por controles de segurança tradicionais. Em 2019, os pesquisadores de ameaças do SonicWall Capture Labs registraram um aumento de 27,3% ano após ano de malware enviado por tráfego TLS/SSL.

27% ↑ aumento do malware enviado sobre o tráfego de TLS/SSL em 2019.

AUMENTO DO VOLUME DE ATAQUES À IOT

Em 2019, a SonicWall descobriu um aumento de 5% no malware direcionado à IoT, com volume total chegando a 34,3 milhões de ataques.

No entanto, com uma enxurrada de novos dispositivos de IoT conectando-se todos os dias, não basta apenas esperar o aumento de ataques de malware direcionados à IoT, mas criar planos para lidar com eles.

34,3 MILHÕES ↑

PREPARE-SE PARA O QUE VEM EM SEGUIDA

Visite SonicWall.com/ThreatReport para baixar o **Relatório de Ameaças Cibernéticas da SonicWall 2020 completo**. Você obterá informações críticas sobre ameaças para ajudá-lo a entender melhor como os cibercriminosos pensam — e estará totalmente preparado para o que farão em seguida.

FAÇA O DOWNLOAD DO RELATÓRIO

SONICWALL®

SonicWall.com

* A SonicWall adota a melhor prática de otimizar regularmente suas metodologias de coleta de dados, análise e relatório. Isso inclui ajustes na limpeza de dados, alterações nas fontes de dados e consolidação dos feeds de ameaças. Os números publicados nos relatórios anteriores podem ter sido ajustados entre períodos, regiões ou setores diferentes.