Relatório de Ameaças Cibernéticas da SonicWall 2019

SUMÁRIO EXECUTIVO | EDIÇÃO GLOBAL

SonicWall.com

SONICWALL®

CAPTURE LABS

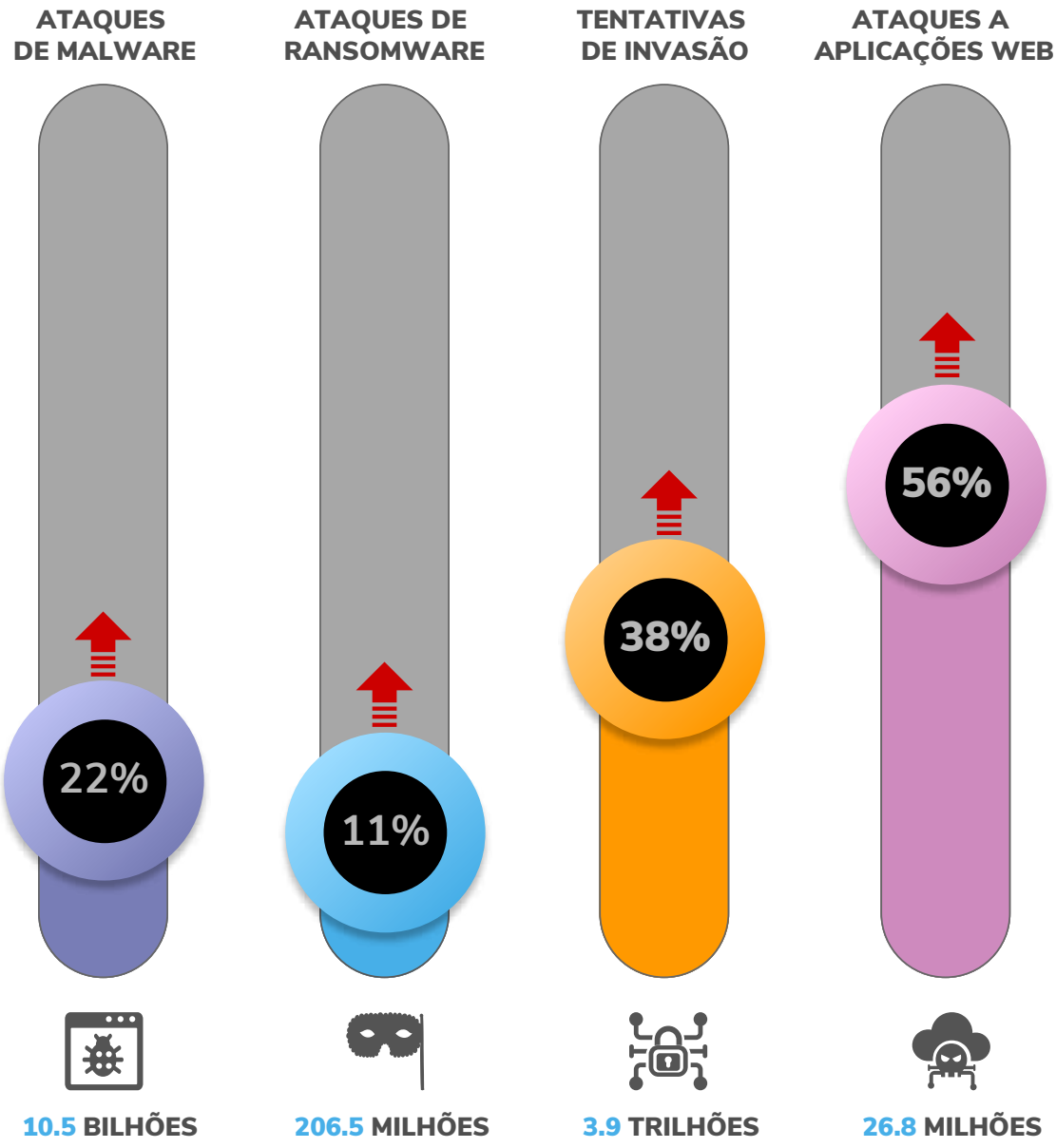
INTRODUÇÃO: EDIÇÃO GLOBAL

A guerra cibernética não tem preconceito nem faz distinção. Quando uma rede, identidade, dispositivo ou dados têm valor — particularmente informações ligadas à propriedade intelectual, finanças, arquivos confidenciais, infraestrutura ou influência política importante — os cibercriminosos identificam, miram e atacam sem piedade.

Para promover a conscientização global e facilitar diálogos importantes, a SonicWall permanece firme com seu compromisso de pesquisar, analisar e compartilhar inteligência de ameaças no Relatório de Ameaças Cibernéticas da SonicWall 2019. Complementando o relatório detalhado, este sumário executivo apresenta uma perspectiva importante na inteligência sobre ameaças dos pesquisadores de ameaças do SonicWall Capture Labs.

PRINCIPAIS DESCOBERTAS DE 2018

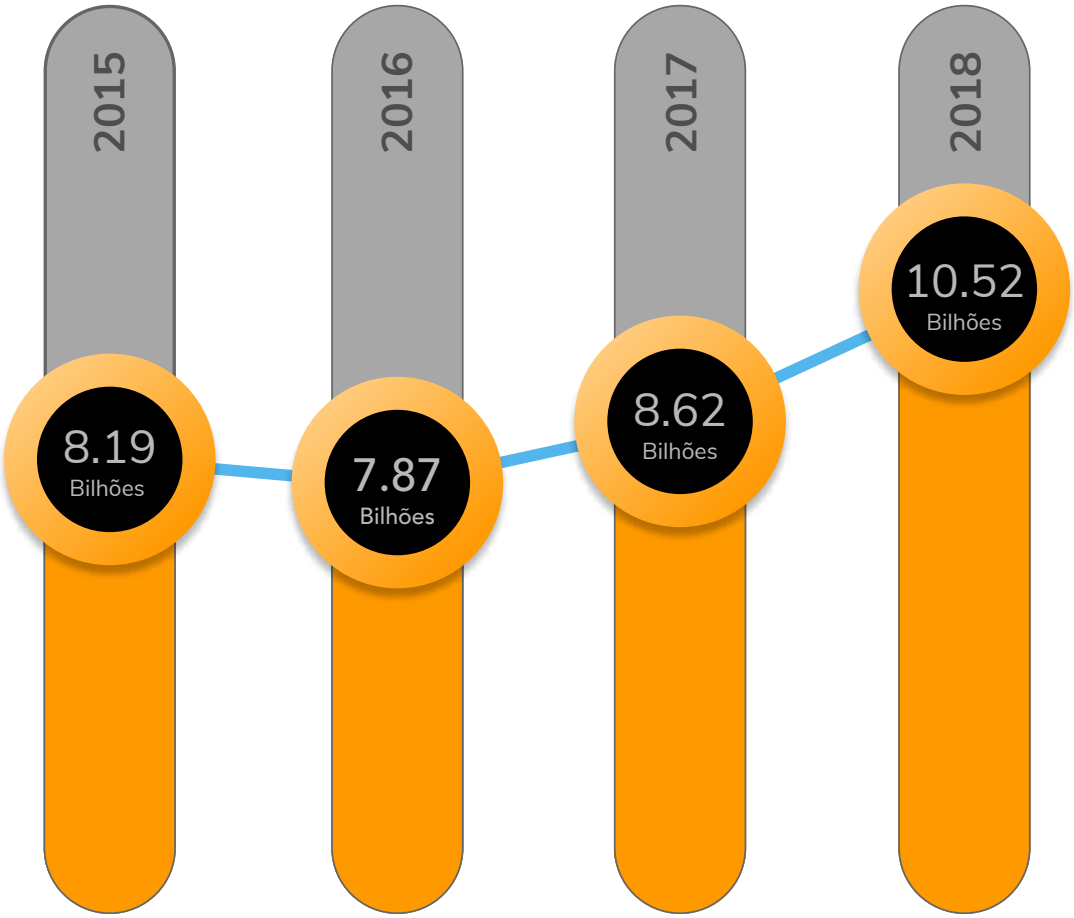
TENDÊNCIAS DE CIBERATAQUES GLOBAIS DE 2018



SONICWALL®

PRINCIPAIS DESCOBERTAS DE 2018

Em 2016, o setor testemunhou um declínio no volume de malware, levando alguns a especular que o cibercrime estaria diminuindo. Desde então, **os ataques de malware aumentaram 33,4%.** A SonicWall registrou no mundo todo 10,52 bilhões* de ataques de malware em 2018 — o número mais alto já registrado.

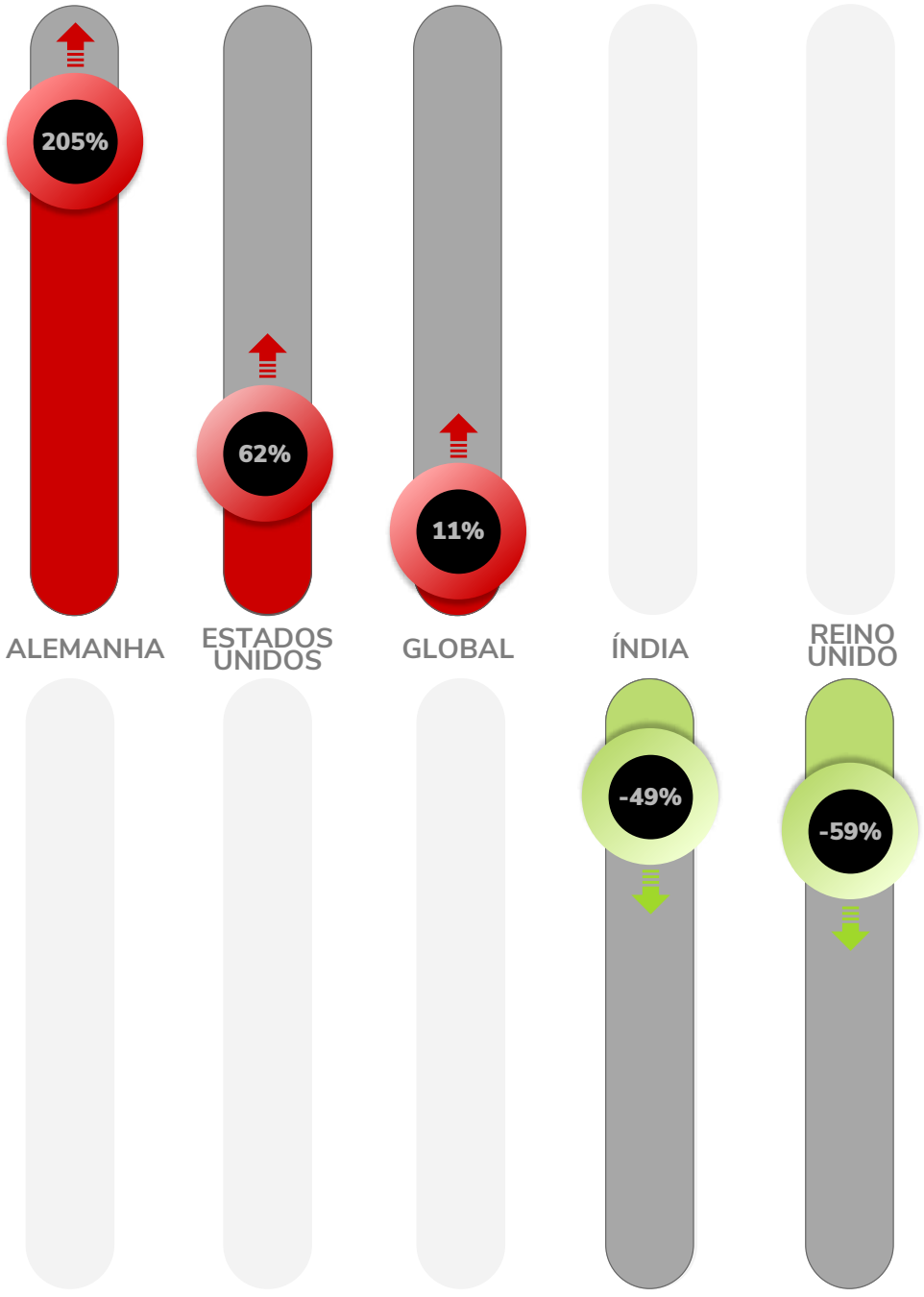


* A SonicWall adota a melhor prática de otimizar regularmente suas metodologias de coleta de dados, análise e relatório. Isso inclui melhorias na limpeza de dados, alterações nas fontes de dados e consolidação dos feeds de ameaças. Os números publicados nos relatórios anteriores podem ter sido ajustados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

REINO UNIDO E ÍNDIA COMBATEM DURAMENTE O RANSOMWARE

Uma revelação chocante foi feita depois que os pesquisadores de ameaças do SonicWall Capture Labs terminaram de analisar os dados de ameaças de todo o ano de 2018. O ransomware aumentou em praticamente todas as regiões geográficas, com exceção de duas: Reino Unido e Índia.

Enquanto grandes países da América do Norte, Europa e Ásia estavam passando por aumentos consideráveis nos ataques ransomware, **o Reino Unido e a Índia silenciosamente tiveram reduções de 59% e 49%**, respectivamente, no volume do ransomware.



SONICWALL®

AMEAÇAS PERIGOSAS À MEMÓRIA E ATAQUES LATERAIS IDENTIFICADOS ANTECIPADAMENTE

A RTMITM (Real-Time Deep Memory Inspection) da SonicWall não detecta apenas ataques de malware nunca antes vistos, mas também atenua ataques laterais perigosos que utilizam esta tecnologia com patente pendente. Os ataques laterais são o principal veículo usado para explorar e extrair dados a partir de vulnerabilidades de processador, como Foreshadow, PortSmash, Meltdown, Spectre e Spoiler.

Infelizmente, a pesquisa atual declara que **"o Spectre veio para ficar"** e reconhece que diversas vulnerabilidades nos processadores não podem ser corrigidas, seja no software, seja no hardware, e são uma preocupação de segurança muito mais profunda. Com isso, os ataques laterais serão um risco constante para o panorama de computação, e uma tecnologia que consiga mitigar esses ataques será extremamente necessária.

CRESCIMENTO CONSTANTE DOS ATAQUES CRIPTOGRAFADOS

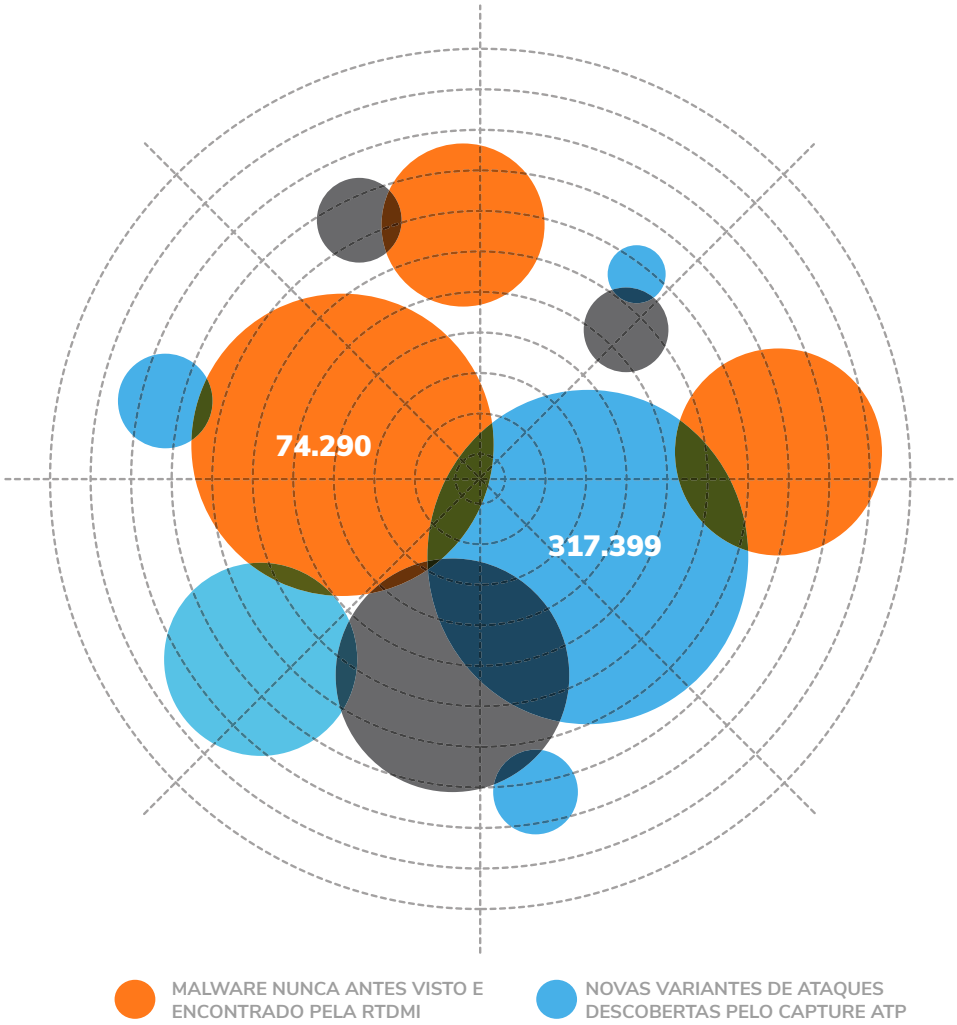
O crescimento do tráfego criptografado coincide com o aumento dos ataques camuflados pela criptografia TLS/SSL. Mais de **2,8 milhões de ataques foram criptografados** em 2018, um aumento de 27% em relação a 2017.

AMADURECIMENTO DA APRENDIZAGEM DE MÁQUINA PARA DETER VARIANTES DE MALWARE NUNCA ANTES VISTAS

O SonicWall Capture Advanced Threat Protection (ATP, ou Proteção contra Ameaças Avançadas) identificou 391.689 novas variantes de ataque em 2018. Isso dá em média mais de **1.072 novos ataques descobertos e bloqueados todos os dias.**

O Capture ATP utiliza um sandbox multimotor baseado na nuvem paralelamente com a tecnologia RTMI™. Esses dois recursos passaram por autoaprendizagem e autoaperfeiçoamento dinâmicos durante o ano de 2018.

Especificamente, a **RTDMI™ identificou 74.290 ataques nunca antes vistos em 2018**. Essas variantes de malware são tão novas, únicas ou complexas que nenhum outro fornecedor no mundo havia sido capaz de monitorar ou criar assinaturas para elas no momento em que a SonicWall as descobriu.

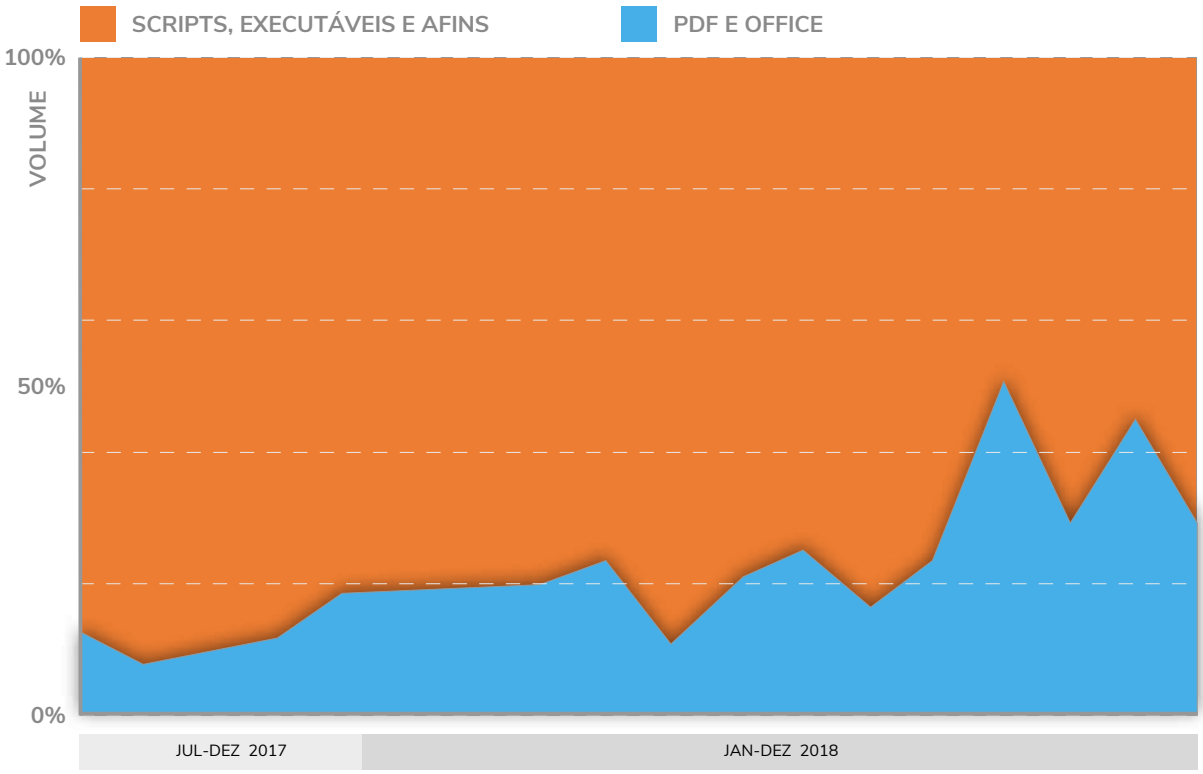


SONICWALL®

PDF E ARQUIVOS DO OFFICE MAL-INTENCIONADOS DRIBLAM CONTROLES DE SEGURANÇA ANTIGOS

Os cibercriminosos estão manipulando arquivos confiáveis do Office e PDFs para ajudar o malware a contornar firewalls tradicionais e até mesmo sandboxes de motor único.

AUMENTO DE ARQUIVOS OFFICE E PDFS MAL-INTENCIONADOS

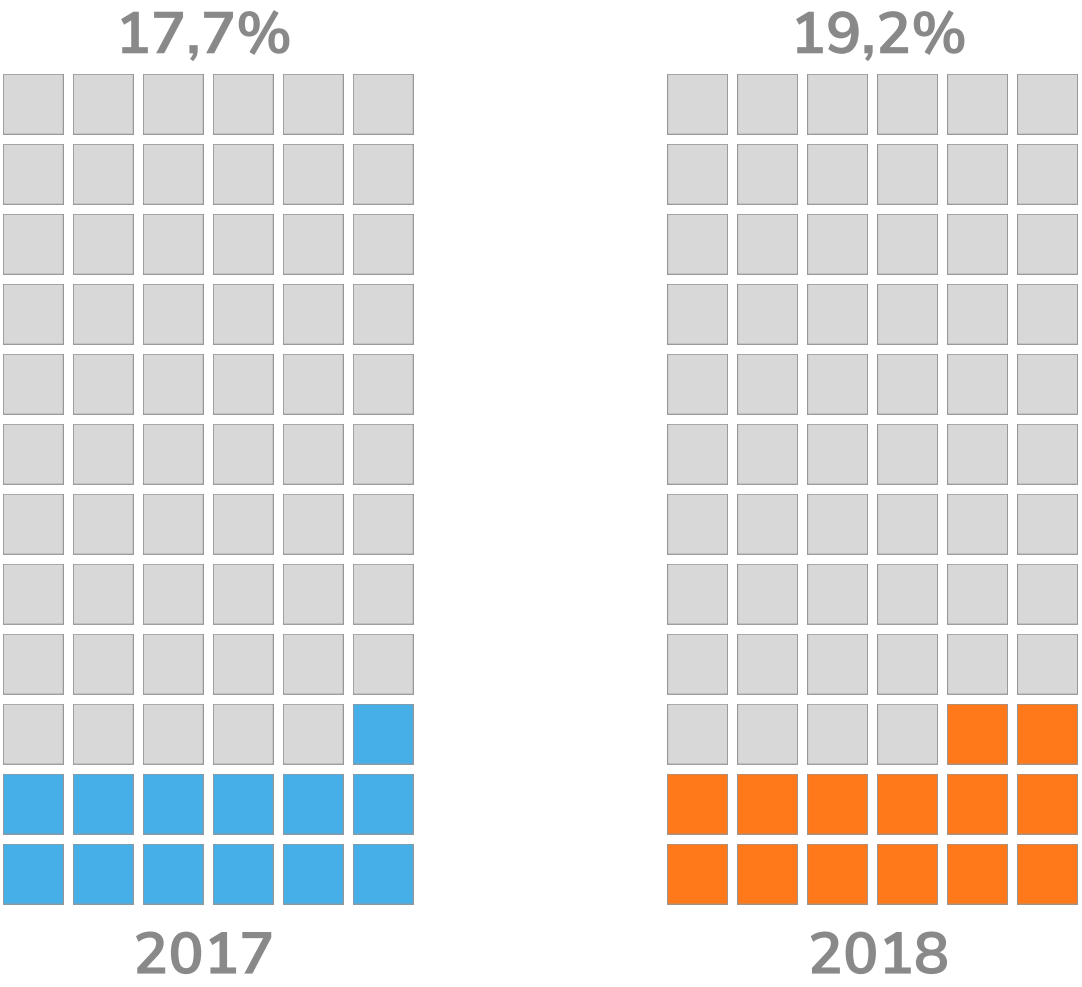


O serviço de sandbox multimotor do SonicWall Capture ATP encontrou **malware oculto em 47.073 PDFs e 50.817 arquivos do Office** em 2018. Embora à primeira vista o volume pareça pequeno, a maioria dos controles de segurança não consegue identificar e mitigar o malware oculto nesses arquivos, aumentando enormemente o êxito do payload.

PORTAS NÃO PADRÃO PRONTAS PARA EXPLORAÇÃO

As portas 80 e 443 são portas padrão de tráfego na Web, por isso recebem o foco da proteção da maioria dos firewalls. Em resposta, os cibercriminosos estão mirando portas não padrão para garantir que os payloads possam ser implantados sem ser detectados em um ambiente-alvo.

ATAQUES DE MALWARE EM 2018
POR PORTAS NÃO PADRÃO



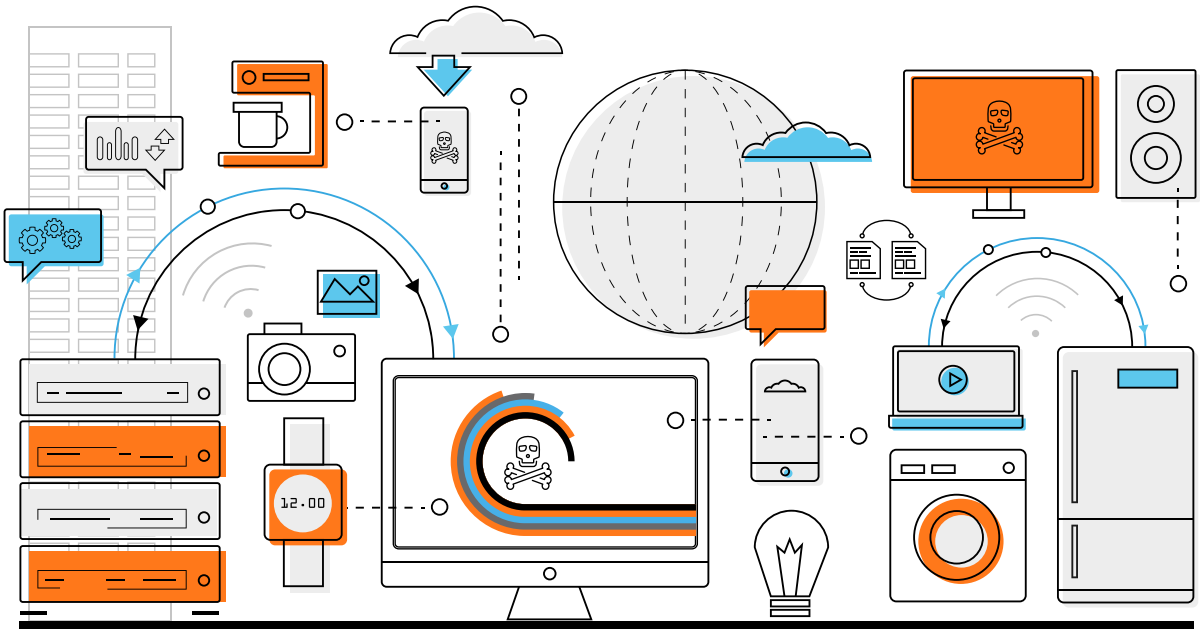
Com base em uma amostra de mais de 700 milhões de ataques de malware, a SonicWall descobriu que **19,2% de todos os ataques de malware entraram por portas não padrão** em 2018. Como são muitos para monitorar, os firewalls de proxy tradicionais não conseguem mitigar os ataques por portas não padrão (para tráfego criptografado e não criptografado).

SONICWALL®

AUMENTO DE ATAQUES NA IoT

Os consumidores estão vorazes por dispositivos conectados. Mas esse apetite resultou em uma enxurrada de lançamentos de dispositivos da Internet das Coisas (IoT) no mercado sem os devidos controles de segurança. Em muitos casos, os dispositivos de IoT são criados com configurações de segurança padrão, facilitando o comprometimento por meio de credenciais conhecidas ou botnets poderosos.

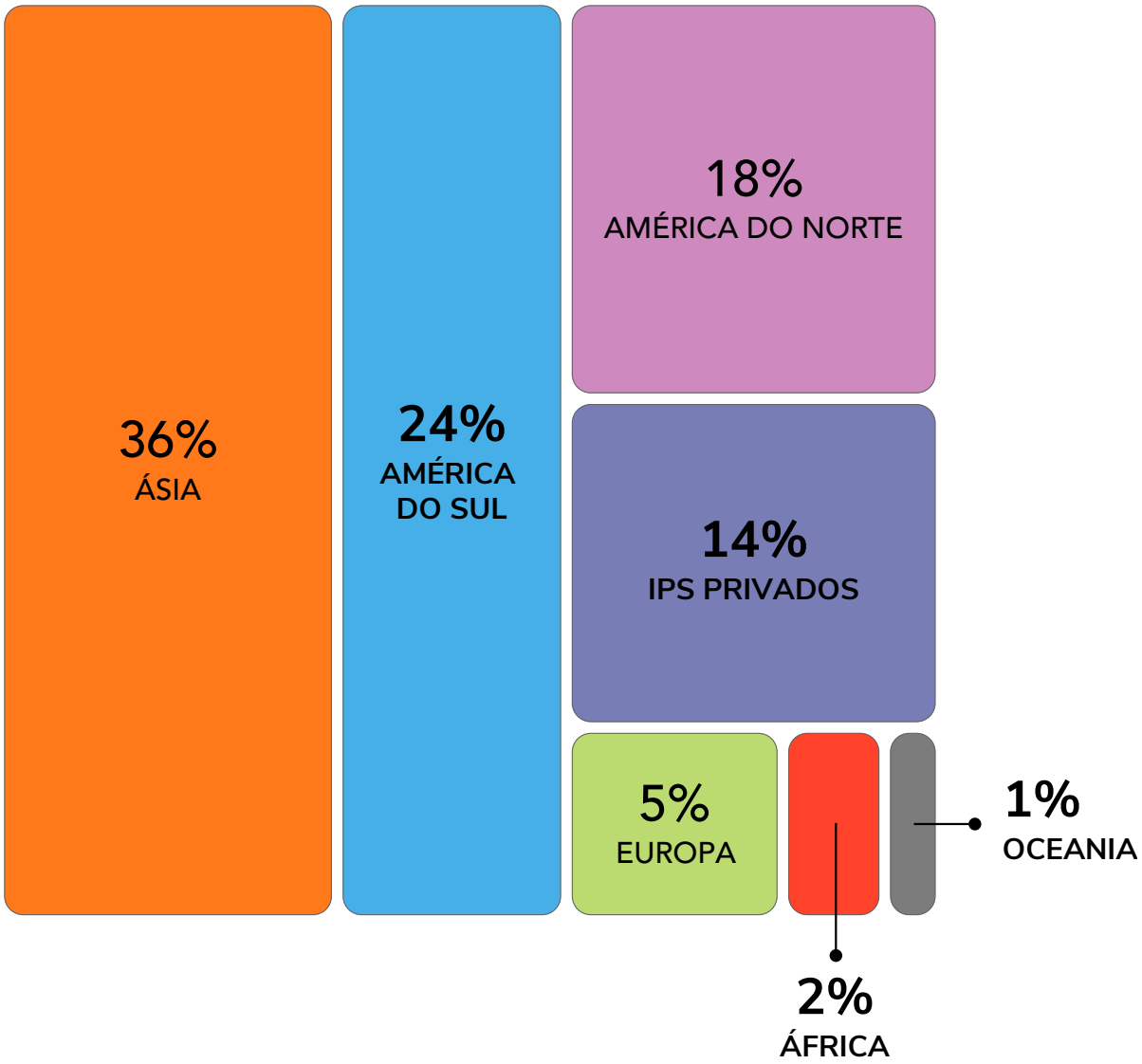
Com isso, a SonicWall registrou **32,7 milhões de ataques na IoT em 2018**, um aumento de 217,5% em relação aos 10,3 milhões de ataques na IoT que a empresa registrou em 2017.



ASCENSÃO E QUEDA DO CRYPTOJACKING

Em 2018, o cryptojacking desapareceu quase tão rapidamente quanto seu surgimento. A SonicWall registrou **57,5 milhões de ataques de cryptojacking** no mundo todo entre abril e dezembro. O volume atingiu seu ápice em setembro, com 13,1 milhões de ataques registrados, mas desde então vem diminuindo constantemente. Apesar da queda dos preços, as criptomoedas continuam sendo uma mercadoria valiosa para os cibercriminosos em decorrência de seu anonimato.

CRYPTOJACKING POR REGIÃO EM 2018



REDUÇÃO DO VOLUME DE PHISHING GLOBAL, ATAQUES MAIS DIRECIONADOS

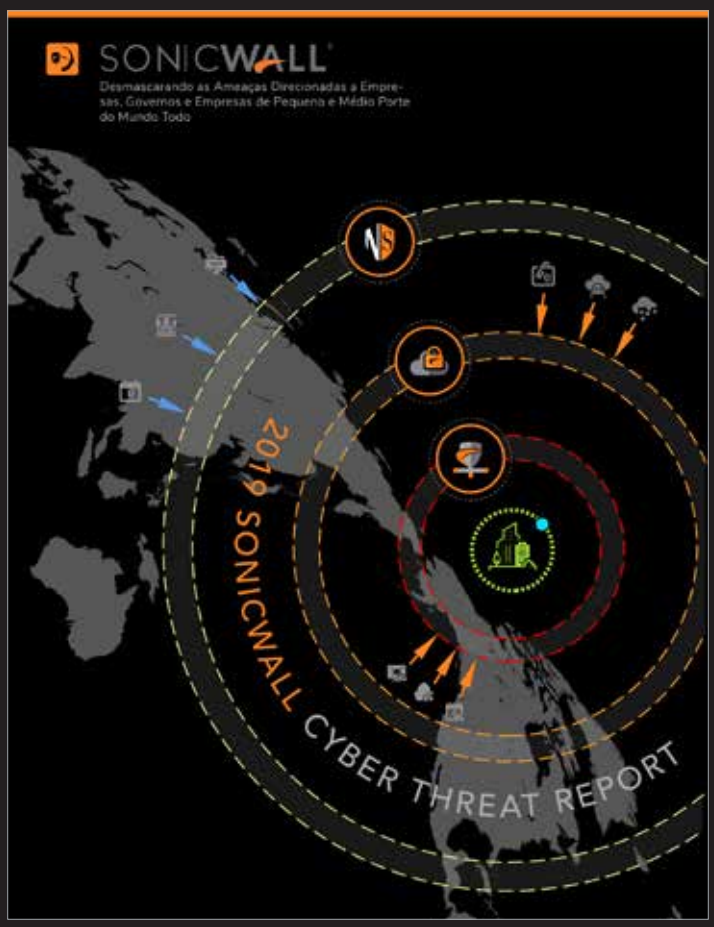
ATAQUES DE PHISHING
NO MUNDO TODO **26 MILHÕES**

Os invasores estão trocando de tática à medida que as empresas melhoram seus métodos de bloqueio de ataques de e-mail e fazem o possível para que os funcionários possam detectar e excluir e-mails suspeitos. Eles estão reduzindo o volume de ataque geral e lançando ataques de phishing mais segmentados (por exemplo, comprometimento de e-mail corporativo, invasões de contas, whale phishing, etc.).

Em 2018, a SonicWall registrou **26 milhões de ataques de phishing no mundo todo,** uma queda de 4,1% em relação a 2017. Um cliente médio da SonicWall sofreu 5.488 ataques de phishing em 2018.

Inteligência e análise exclusiva de ameaças cibernéticas. Somente do SonicWall Capture Labs.

SAIBA MAIS



Visite SonicWall.com/ThreatReport para fazer o download do Relatório de Ameaças Cibernéticas da SonicWall 2019 completo. Você obterá novas perspectivas sobre as estratégias de ataque dos cibercriminosos e entenderá como proteger adequadamente sua organização ou empresa contra os ciberataques mais sofisticados.

* A SonicWall adota a melhor prática de otimizar regularmente suas metodologias de coleta de dados, análise e relatório. Isso inclui melhorias 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.

SONICWALL