PANORAMA DE AMEAÇAS CIBERNÉRTICAS NO BRASIL

ANO 2020

BRASIL

8,4 BILHÕES
de tentativas de ataques cibernéticos em 2020

AMÉRICA LATINA

41 BILHÕES
de tentativas de ataques cibernéticos em 2020

Fonte: FortiGuard Labs, laboratório de investigação e inteligência de ameaças da Fortinet

TRENDING TOPICS: PHISHING - MALWARE - RANSOMWARE

Alta atividade de e-mails de **phishing com arquivos HTML maliciosos anexados.**

O malware baseado na web é o meio mais comum para a distribuição de arquivos infectados.

As campanhas de phishing são **a porta de entrada para o ransomware.**

MAIS SOFISTICAÇÃO EFICIÊNCIA DOS ATAQUES

Alto grau de sofisticação e eficiência em ataques cibernéticos.

Uso de tecnologias avançadas e IA para ataques direcionados com maior probabilidade de sucesso

Em menos tentativas, os cibercriminosos podem **causar mais danos.**

DESTAQUES DO 4° TRIMESTRE DE 2020:

Campanhas de phishing como o principal vetor de ataque: foram detectadas numerosas campanhas de cavalos de Tróia no período.

Trabalho remoto como porta de entrada para redes corporativas: exploração de vulnerabilidades em roteadores domésticos. Mais pessoas trabalham em casa, com menos proteção e mais acesso aos dados corporativos.

Botnets visam dispositivos IoT
A botnet Mirai se tornou mais forte, mais rápida, mais resiliente e mais evasiva. Os dispositivos IoT estão menos protegidos e mais visados pelos atacantes.

Antigas botnets ainda estão ativas na América Latina Gh0st e Andromeda aparecem como as mais detectadas. Aplicar os patches e atualizações dos fabricantes é essencial.

CONCLUSÕES

✓*O ano de 2020 demonstrou a capacidade dos criminosos de* ***investir tempo e recursos em ataques mais lucrativos, como o ransomware.***

✓ **Eles se adaptaram à nova era do trabalho remoto** com ações mais sofisticadas para enganar as vítimas e acessar redes corporativas.

✓ **É necessária uma maior cultura de cibersegurança** e a implementação de controles para redes, dispositivos, aplicações e nuvens.

✓ **As plataformas de segurança devem operar de forma integrada** e automatizada na rede principal, em ambientes multi-cloud, em filiais e nas residências de trabalhadores remotos.

✓ **Soluções de segurança que incorporam inteligência artificial e aprendizado** de máquina tornam-se aliadas para prevenir, detectar, mitigar e responder em tempo real.

Relatório completo: www.fortiguardthreatinsider.com

www.fortinet.com/lat