Dados da Fortinet revelam que o país foi o segundo mais visado da América Latina, atrás apenas do México

Em âmbito global, 82% dos cibercrimes motivados financeiramente envolveram o emprego de ransomware

A Fortinet® (NASDAQ: FTNT), líder global em soluções de cibersegurança, divulgou os números totais de ataques cibernéticos do ano de 2022, levantados pelo FortiGuard Labs, seu laboratório de inteligência e análise de ameaças.

O Brasil foi o segundo país mais atingido da América Latina, com 103,16 bilhões de tentativas de ataques cibernéticos, um aumento de 16% com relação a 2021 (com 88,5 bilhões). O país ficou atrás do México (com 187 bilhões) e foi seguido por Colômbia (20 bilhões) e Peru (15,4 bilhões). O total da América Latina e Caribe foi de mais de 360 bilhões de tentativas de ciberataques em 2022.

Na comparação entre o último trimestre do ano e o anterior, houve um aumento de 61,7% no número de tentativas de ataques cibernéticos sofridas pelo país. Nos meses de outubro, novembro e dezembro de 2022 foram 30,4 bilhões, contra 18,8 bilhões em julho, agosto e setembro.

“A conscientização em segurança cibernética é fundamental para evitar que os criminosos obtenham acesso aos dados e sistemas das empresas, principalmente se pensarmos que a invasão ocorre quando um usuário desavisado navega na internet e baixa involuntariamente uma arquivo malicioso ao visitar um site comprometido, abrir um anexo de e-mail ou ao clicar em um link ou janela pop-up enganosa”, explica Alexandre Bonatti, diretor de Engenharia da Fortinet Brasil. “Uma vez que um arquivo malicioso é acessado e baixado, geralmente é tarde demais para a empresa

escapar do comprometimento, a menos que tenha uma abordagem holística de segurança.”

Entre os destaques do segundo semestre divulgados pelo FortiGuard Lab estão:

- A contínua distribuição em massa do malware wiper mostra a evolução destrutiva dos ataques cibernéticos.

- Ataques de ransomware permanecem em níveis máximos, sem evidência de desaceleração em âmbito global e com novas variantes habilitadas por Ransomware-as-a-Service (RaaS).

- Os malwares mais utilizados no período foram criados há mais de um ano, o que mostra que os atacantes se beneficiam em termos de eficácia e economia de custos ao reutilizar e reciclar códigos.

- A vulnerabilidade Log4j continua a causar danos em organizações de todos os setores, principalmente em Tecnologia, Governo e Educação.

Malware wiper - A análise dos dados do malware wiper revela uma tendência dos adversários cibernéticos em usar técnicas de ataque destrutivo contra seus alvos. Os dados também revelam que, com a falta de fronteiras na internet, os adversários cibernéticos podem escalar facilmente esses tipos de ataques que foram amplamente possibilitados pelo modelo de Cybercrime-as-a-Service (CaaS). No início de 2022, o FortiGuard Labs relatou a presença de vários novos wipers atuando em paralelo com a guerra Rússia-Ucrânia. No final do ano, o malware wiper se expandiu para outros países, gerando um aumento de 53% na atividade do terceiro para o quarto trimestre. Infelizmente, a trajetória do malware wiper de destruição não parece estar diminuindo, o que significa que qualquer organização continua sendo um alvo em potencial.

Ransomware e o cibercrime motivado por lucro - Os engajamentos de resposta a incidentes (IR) do FortiGuard Labs descobriram o maior volume de incidentes do segundo semestre do ano estava motivado por ganhos financeiros (73,9%), com um distante segundo lugar atribuído à espionagem (13%).

Em todo o ano de 2022, 82% dos cibercrimes motivados financeiramente envolveram o emprego de ransomware ou scripts maliciosos, mostrando que o ransomware permanece em pleno vigor, sem evidências de desaceleração, graças à crescente popularidade do Ransomware-as-a-Service (RaaS) na dark web. Na verdade, no segundo semestre de 2022, o volume de ransomware aumentou 16% com relação ao primeiro semestre do mesmo ano.

Reutilização de códigos - Os adversários cibernéticos são empreendedores por natureza e sempre buscam maximizar os investimentos e conhecimentos existentes para tornar seus esforços de ataque mais eficazes e lucrativos. A reutilização de códigos é uma maneira eficiente e lucrativa para os criminosos obterem resultados enquanto fazem ajustes em seus ataques para superar obstáculos defensivos. Quando o FortiGuard Labs analisou os malwares mais prevalentes no segundo semestre de 2022, a maioria dos primeiros lugares foi ocupada por malwares com mais de um ano de criação. Os adversários cibernéticos não estão apenas automatizando ameaças, mas adaptando ativamente os códigos para torná-los ainda mais eficazes.

Botnets antigas e a cadeia de suprimentos dos criminosos - Além da reutilização de códigos, os adversários também estão aproveitando a infraestrutura existente e as ameaças mais antigas para maximizar as oportunidades. Ao examinar as ameaças de botnet por prevalência, muitas das principais botnets não são novas. Essas botnets “antigas” ainda são difundidas por um motivo: elas ainda são muito eficazes. Especificamente, no segundo semestre de 2022, os principais alvos da Mirai incluíram provedores de serviços de segurança gerenciados (MSSPs), o setor de telecomunicações/operadoras e o setor de manufatura, conhecido pela utilização de tecnologia operacional (OT) generalizada. Os criminosos estão fazendo um esforço concentrado para atingir essas indústrias com métodos comprovados.

Log4j continua atingindo organizações - Mesmo com toda a publicidade que a Log4j recebeu em 2021 e no início de 2022, um número significativo de organizações ainda não corrigiu ou aplicou os controles de segurança apropriados para proteção contra essa que é uma das vulnerabilidades mais notáveis da história. No segundo semestre de 2022, a Log4j ainda estava fortemente ativa em todas as regiões.

“Para os adversários cibernéticos, manter o acesso e evitar a detecção não é uma tarefa fácil, pois as defesas cibernéticas continuam avançando para proteger as organizações. Para superar esses desafios, os atacantes estão evoluindo suas técnicas de reconhecimento e implantando alternativas de ataque mais sofisticadas, com métodos de ameaças semelhantes ao APT, como o malware wiper”, diz Derek Manky, estrategista-chefe de Segurança e vice-presidente Global de Inteligência de Ameaças do FortiGuard Labs. “Para se protegerem contra essas táticas persistentes de cibercrime avançado, as organizações precisam de inteligência de ameaças coordenada e acionável orientada por aprendizado de máquina em tempo real em todos os dispositivos de segurança para detectar ações suspeitas e iniciar a mitigação em toda a superfície de ataque estendida.”

Visão geral do relatório - Este último relatório do cenário global de ameaças reflete a visibilidade da inteligência coletiva do FortiGuard Labs, extraída da ampla gama de sensores da Fortinet, empresa responsável por 64,79% dos equipamentos de segurança instalados no Brasil, segundo a IDC [*]. Usando a estrutura MITRE ATT&CK, que classifica táticas adversárias, técnicas e procedimentos, o relatório descreve como os agentes de ameaças visam vulnerabilidades, constroem uma infraestrutura maliciosa e exploram seus alvos. O relatório também abrange perspectivas globais e regionais, bem como tendências de ameaças que afetam os ambientes de TI e OT.

[*] *H22021 IDC Latin America Security Appliances Tracker*.

Sobre a Fortinet

A Fortinet (NASDAQ: FTNT) é uma força motriz na evolução da segurança cibernética e na convergência de rede e segurança. Nossa missão é proteger pessoas, dispositivos e dados em todos os lugares, e hoje oferecemos segurança cibernética onde você precisar com o maior portfólio integrado de mais de 50 produtos de nível empresarial. Mais de meio milhão de clientes confiam nas soluções da Fortinet, que estão entre as mais implantadas, mais patenteadas e mais validadas do setor. O Fortinet Training Institute, um dos maiores e mais amplos programas de treinamento do setor, dedica-se a disponibilizar treinamento em segurança cibernética e novas oportunidades de carreira para todos. O FortiGuard Labs, o laboratório de pesquisa e inteligência de ameaças de elite da Fortinet, desenvolve e utiliza aprendizado de máquina de ponta e tecnologias de IA para fornecer aos clientes inteligência de ameaças acionável e proteção oportuna e consistente com a melhor classificação do mercado. Saiba mais em www.fortinet.com/br, Fortinet Blog e FortiGuard Labs.

Fonte: Fortinet Brasil, em 27.02.2023