Your IT Company

Campanha Global de Comprometimento de Credenciais Afeta Aproximadamente 75 Mil Dispositivos FortiGate da Fortinet

Sumário

1. Objetivo

Este documento foi desenvolvido com base em informações divulgadas por pesquisadores de segurança, fabricantes e fontes públicas especializadas em cibersegurança, com o objetivo de analisar a campanha global de comprometimento de credenciais associada a dispositivos FortiGate da Fortinet, seus impactos, riscos operacionais e medidas de mitigação recomendadas.

2. Campanha Global de Comprometimento de Credenciais Afeta Aproximadamente 75 Mil Firewalls FortiGate

2.1. Descrição da Ameaça

Pesquisadores de segurança identificaram uma campanha de grande escala envolvendo o comprometimento de credenciais associadas a aproximadamente 75 mil dispositivos FortiGate distribuídos em 194 países.

A operação teve como alvo interfaces VPN SSL e administrativas expostas à internet, afetando organizações de diversos setores econômicos ao redor do mundo.

Segundo a Hudson Rock, a exposição envolve 21.632 domínios únicos, indicando um potencial impacto global sobre empresas que utilizam soluções FortiGate para acesso remoto e proteção perimetral.

Entre as organizações mencionadas nas análises públicas estão FoxConn, Samsung, Comcast, Siemens, Lenovo, FedEx, PxW, Accenture e Oracle.

Embora a Fortinet tenha informado que os dados correspondem a incidentes anteriores e a campanhas conhecidas de força bruta, o elevado volume de credenciais expostas representa um risco significativo para organizações que ainda mantêm essas credenciais ativas.

2.2. Impacto

A utilização indevida de credenciais válidas pode permitir que invasores:

- Obtenham acesso remoto não autorizado à infraestrutura corporativa;
- Comprometam contas administrativas;
- Realizem movimentação lateral entre ativos internos;
- Coletem informações sensíveis;
- Viabilizem atividades de espionagem corporativa e governamental.
- Comprometam ambientes Active Directory;
- Facilitem ataques de ransomware;
- Estabeleçam persistência na rede;

2.3. Exploração

Tipo de Ameaça

Campanha global de comprometimento de credenciais (Credential Theft Campaign).

Vetor de Ataque

- Interfaces VPN SSL expostas à internet;

- Interfaces administrativas acessíveis externamente;
- Utilização de credenciais comprometidas;
- Ausência de autenticação multifator (MFA);
- Ambientes com segmentação inadequada.

Cadeia de Exploração

- Identificação de dispositivos FortiGate expostos à internet.
- Obtenção e utilização de credenciais válidas.
- Acesso inicial aos dispositivos comprometidos.
- Expansão para ambientes internos.
- Comprometimento de serviços críticos, incluindo Active Directory.
- Movimentação lateral e estabelecimento de persistência.

Dados Observados

- 75.000 dispositivos FortiGate potencialmente afetados;
- 21.632 domínios únicos envolvidos;
- 1,16 bilhão de tentativas de autenticação direcionadas a 320.777 dispositivos FortiGate;
- 2,1 bilhões de tentativas direcionadas a 163.650 servidores Microsoft SQL Server;
- Pelo menos quatro organizações totalmente comprometidas, segundo os pesquisadores.

2.4. Mitigação

Ação Prioritária:

- Redefinir imediatamente todas as credenciais associadas às VPNs Fortinet.
- Alterar as credenciais das interfaces administrativas.
- Habilitar autenticação multifator (MFA) em todos os acessos remotos.
- Revisar permissões e contas privilegiadas.
- Investigar atividades suspeitas nos ambientes internos.

Monitorar:

- Tentativas anômalas de autenticação.
- Logins provenientes de localidades incomuns.
- Alterações indevidas em contas privilegiadas.
- Eventos suspeitos no Active Directory.
- Movimentação lateral entre ativos críticos.

Detecção:

- Utilizar soluções EDR para identificar atividades pós-comprometimento.
- Monitorar continuamente logs de autenticação VPN.
- Correlacionar eventos em plataformas SIEM.

2.5. Prevenção

Controles Técnicos:

- Habilitar MFA em todos os acessos remotos
- Restringir acessos administrativos a endereços IP confiáveis.
- Restringir a exposição de interfaces administrativas à internet.

Governança e Segurança:

- Estabelecer políticas periódicas de rotação de credenciais.
- Revisar regularmente contas privilegiadas.
- Realizar auditorias frequentes nos ambientes Fortinet.
- Adotar princípios de Zero Trust.

2.6. Avaliação de Risco Estratégico

A campanha representa um risco elevado para organizações que utilizam dispositivos FortiGate expostos à internet, principalmente devido ao potencial de comprometimento de ambientes internos por meio de credenciais válidas.

Os principais fatores de risco incluem:

- Escala global da operação, abrangendo 194 países;
- Grande volume de credenciais corporativas expostas;
- Possibilidade de ataques de ransomware e espionagem corporativa;
- Potencial comprometimento de ambientes Active Directory;

Para saber informações mais detalhadas sobre esta vulnerabilidade acesse: https://www.cybersecbrazil.com.br/post/ataque-rouba-senhas-de-75-mil-firewalls-fortinet-no-mundo.

Esta publicação tem como objetivo orientar a equipe interna no ambiente cibernético, possibilitando assim ações proativas de prevenção para tornar a infraestrutura de nossas empresas cada vez mais segura.

Produzido por: Equipe de Cyber Threat Intelligence da Service IT Security