BOLETIM DE SEGURANÇA

Cisco alerta para ataques de Password-Spraying direcionados a serviços VPN

heimdall
security research
A DIVISION OF ISH

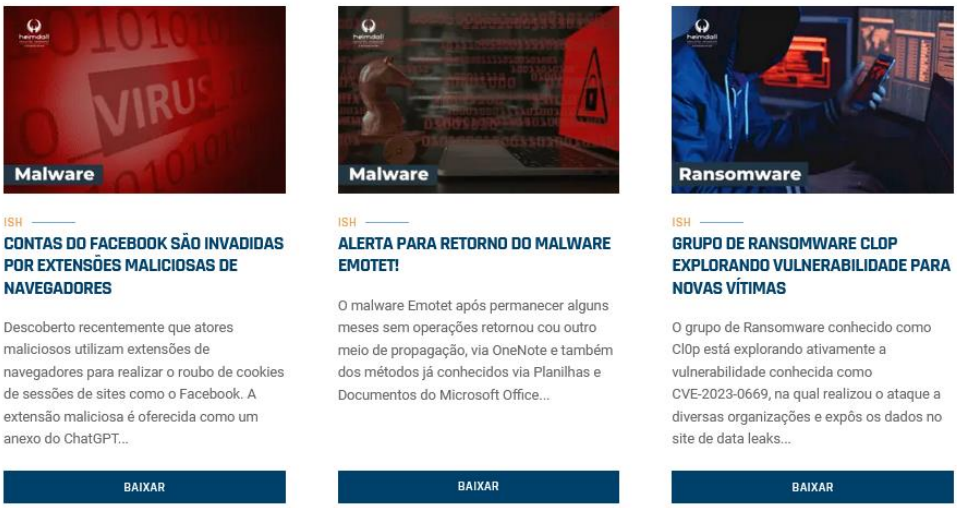
TLP: CLEAR

Receba alertas e informações sobre segurança cibernética e ameaças rapidamente, por meio do nosso **X**.

[Heimdall Security Research]

Acesse boletins diários sobre agentes de ameaças, *malwares*, indicadores de comprometimentos, TTPs e outras informações no *site* da ISH.

[Boletins de Segurança – Heimdall]



SUMÁRIO

LISTA DE TABELAS

1 SUMÁRIO EXECUTIVO

A Cisco divulgou recentemente uma série de diretrizes para ajudar os clientes a se protegerem contra ataques de *password-spraying* direcionados aos serviços VPN de acesso remoto (RAVPN) configurados em dispositivos Cisco Secure Firewall. Esses ataques não se limitam apenas aos serviços RAVPN, mas também têm como alvo outros serviços VPN de acesso remoto, sugerindo que fazem parte de atividades de reconhecimento.

2 ATAQUES DE PASSWORD-SPRAYING

Um ataque de password-spraying é um tipo de ataque cibernético onde o invasor tenta acessar uma grande quantidade de contas usando senhas comuns em vez de tentar várias senhas em uma única conta. Por exemplo, um hacker pode adquirir uma lista de e-mails de funcionários de uma empresa e usar essa lista para tentar fazer login em cada conta usando senhas amplamente utilizadas, como "123456" ou "senha". Ao contrário dos ataques de força bruta, que tentam muitas senhas em uma conta e frequentemente acionam mecanismos de bloqueio, o password-spraying visa muitas contas com tentativas limitadas, reduzindo a chance de detecção.

Em um caso prático, um atacante pode usar ferramentas automatizadas para disparar tentativas de login em contas de e-mail corporativas durante a noite, explorando a baixa probabilidade de resposta imediata e aumentando as chances de acesso não autorizado sem alertar os sistemas de segurança.

3 RECOMENDAÇÕES CONTRA OS ATAQUES

Abaixo segue as recomendações repassadas pela Cisco para proteção contra este tipo de ataque:

- Habilitar o registro em log em um servidor syslog remoto para melhorar a análise e correlação de incidentes.
- Protegendo perfis VPN de acesso remoto padrão apontando perfis de conexão padrão não utilizados para um servidor AAA sinkhole para evitar acesso não autorizado.
- Aproveitando a rejeição de TCP para bloquear manualmente IPs maliciosos.
- Configurando ACLs de plano de controle para filtrar endereços IP públicos não autorizados ao iniciar sessões VPN.
- Usando autenticação baseada em certificado para RAVPN, que fornece um método de autenticação mais seguro do que as credenciais tradicionais.

A **ISH** também recomenda medidas que poderão ser adotadas visando a mitigação da referida *ameaça*, como por exemplo:

Políticas de senha forte

- Implemente políticas que exigem senhas complexas e únicas para todos os usuários. Senhas longas, com uma mistura de letras maiúsculas e minúsculas, números e símbolos, são mais difíceis de adivinhar.

Autenticação de múltiplos fatores (MFA)

- A MFA exige que os usuários forneçam dois ou mais tipos de evidência para verificar sua identidade, significativamente aumentando a segurança. Mesmo que uma senha seja comprometida, um atacante ainda precisaria da segunda forma de autenticação.

Bloqueio de conta e detecção de anomalias

- Configure sistemas para bloquear contas após várias tentativas de login fracassadas e use soluções de detecção de anomalias para identificar tentativas de login suspeitas, como várias tentativas de várias localizações em um curto período.

Educação e treinamento em segurança

- Eduque seus funcionários sobre a importância de usar senhas fortes e únicas e os riscos associados ao reuso de senhas. Treinamentos regulares podem ajudar a construir uma cultura de segurança dentro da organização.

Lista de senhas bloqueadas

- Mantenha e atualize regularmente uma lista de senhas proibidas que inclua as senhas mais comuns e fáceis de adivinhar. Impedir que os usuários escolham essas senhas pode ajudar a proteger contra ataques de Password Spraying.

Análise de logs e monitoramento

- Monitore e analise logs de autenticação para detectar padrões suspeitos de tentativas de login. Isso pode ajudar a identificar um ataque em andamento antes que ele seja bem-sucedido.

Atualizações e patches de segurança

- Mantenha todos os sistemas, aplicativos e infraestrutura de rede atualizados com as últimas atualizações e patches de segurança. Vulnerabilidades não corrigidas podem ser exploradas por atacantes para facilitar ataques.

Controle de acesso baseado em função

- Implemente controles de acesso baseados em função para limitar o acesso a informações e recursos críticos apenas aos usuários que realmente precisam deles para suas funções de trabalho.

4 MITRE ATT&CK - TTPs

Tática	Técnica	Detalhes
Credential Access	T1110.003	Os adversários podem usar uma lista única ou pequena de senhas comumente usadas em muitas contas diferentes para tentar adquirir credenciais de conta válidas.

Tabela 1 – Tabela MITRE ATT&CK.

5 REFERÊNCIAS

- **Heimdall *by* ISH Tecnologia**
- **Cisco**
- **MITRE ATT&CK**
- **Bleepingcomputer**

heimdall
security research
A DIVISION OF ISH