BOLETIM DE SEGURANÇA

Cisco alerta para campanha de ataques de força bruta direcionados a serviços VPN e SSH

heimdall
security research
A DIVISION OF ISH

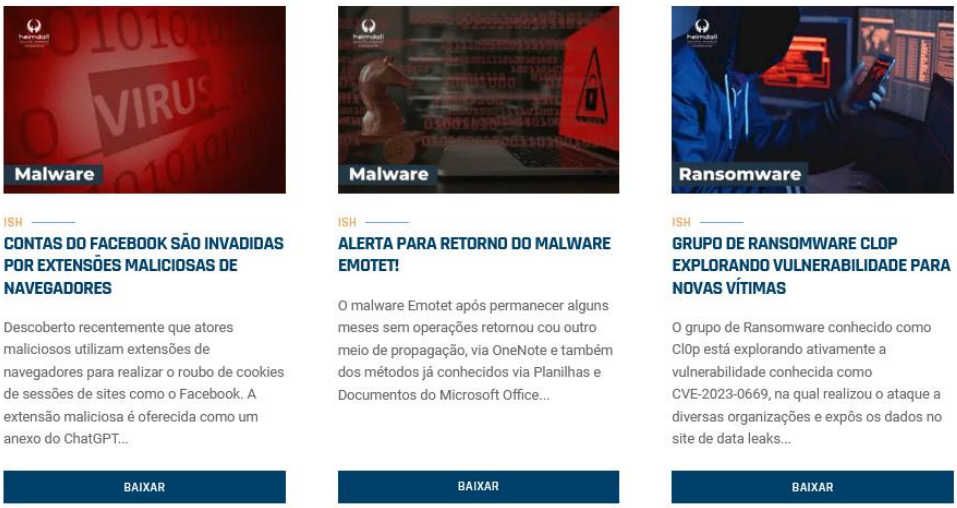
TLP: CLEAR

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 alertou sobre uma campanha de ataques de força bruta em larga escala direcionada a serviços de VPN e SSH em dispositivos de várias marcas, incluindo Cisco, CheckPoint, Fortinet, SonicWall e Ubiquiti. Os ataques começaram em 18 de março de 2024 e foram conduzidos por meio de nós de saída TOR e outras ferramentas de anonimato para evitar bloqueios. Estes ataques visam obter credenciais de acesso válidas para assumir dispositivos e redes internas. A Cisco Talos, que reportou os ataques, observou um aumento no tráfego malicioso, sugerindo que essa tendência de ataques provavelmente continuará a crescer.

2 SERVIÇOS AFETADOS E TÉCNICA USADA

Em ambientes visados, ataques bem-sucedidos podem resultar em acesso não autorizado à rede, bloqueio de contas ou interrupções de serviço por sobrecarga. Com o tempo, o tráfego ligado a esses ataques tem crescido e espera-se que continue a aumentar. Uma lista de serviços já identificados como afetados foi fornecida, mas é possível que outros serviços também estejam vulneráveis a esses tipos de ataques, conforme a lista abaixo disponibilizada pela Cisco.

- Cisco Secure Firewall VPN
- Checkpoint VPN
- Fortinet VPN
- SonicWall VPN
- RD Web Services
- Miktrotik
- Draytek
- Ubiquiti

As tentativas de ataque de força bruta utilizam tanto nomes de usuário genéricos quanto específicos para determinadas organizações. A abordagem desses ataques é ampla, sem focar em regiões ou setores específicos. Os IPs de origem desses ataques frequentemente provêm de serviços de proxy, que incluem, entre outros como:

- TOR
- VPN Gate
- IPIDEA Proxy
- BigMama Proxy
- Space Proxies
- Nexus Proxy
- Proxy Rack

Segundo a Cisco, a lista fornecida acima não é exaustiva, pois serviços adicionais podem ser utilizados pelos atores da ameaça.

3 CONCLUSÃO

Os recentes ataques de força bruta contra serviços de VPN podem impactar organizações de qualquer setor. Esses ataques, ao decifrarem credenciais de acesso, abrem caminho para invasores acessarem redes empresariais de maneira não autorizada, expondo dados confidenciais a riscos significativos. Além de causar interrupções diretas no serviço, comprometem a integridade e a confiabilidade dos sistemas de TI. A utilização de IPs associados a serviços de proxy facilita o anonimato dos atacantes, complicando a defesa e resposta a incidentes por parte das equipes de segurança. Portanto, a adoção de estratégias robustas de segurança, torna-se essencial para mitigar esses riscos.

4 MITRE ATT&CK - TTPs

Tática	Técnica	Detalhes
Credential Access	T1110.001, T1110.002, T1110.003, T1110.004	Os adversários podem usar técnicas de força bruta para obter acesso a contas quando as senhas são desconhecidas ou quando hashes de senha são obtidos.

Tabela 1 – Tabela MITRE ATT&CK.

5 RECOMENDAÇÕES

Além dos indicadores de comprometimento disponibilizados no Github da Cisco, poderão ser adotadas medidas visando a mitigação da referida *ameaça*, como por exemplo:

Políticas de senha forte

- Imposição de senhas complexas que combinam letras, números e símbolos para dificultar adivinhações.

Limitação de tentativas de login

- Configuração de um limite máximo de tentativas de login falhas antes de bloquear temporariamente o acesso ou alertar administradores.

Autenticação multifator (MFA)

- Implementação de uma camada adicional de segurança exigindo dois ou mais métodos de verificação.

Monitoramento de acesso

- Uso de ferramentas de segurança para monitorar e registrar tentativas de acesso, facilitando a identificação de padrões suspeitos.

Bloqueio de IPs suspeitos

- Restrição de acesso a partir de IPs conhecidos por serem usados em ataques ou que apresentam comportamento suspeito.

Alertas de segurança

- Configuração de sistemas para alertar os administradores sobre atividades suspeitas, permitindo uma resposta rápida.

Atualizações de segurança

- Manter software e sistemas operacionais atualizados para corrigir vulnerabilidades que poderiam ser exploradas em ataques de força bruta.

6 REFERÊNCIAS

- **Heimdall *by* ISH Tecnologia**
- **Cisco**

heimdall
security research
A DIVISION OF ISH