BOLETIM DE SEGURANÇA

Ator de ameaça oferecendo acessos a dispositivos Fortinet

heimdall
security research
A DIVISION OF ISH

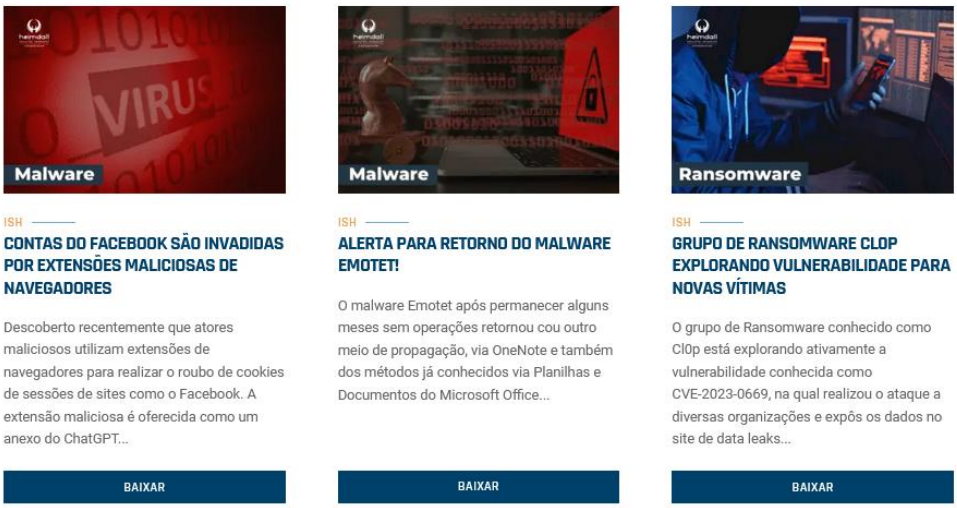
TLP: CLEAR

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 FIGURAS

1 SUMÁRIO EXECUTIVO

A segurança das informações se torna cada vez mais crucial à medida que atores maliciosos encontram métodos sofisticados para comprometer dados sensíveis de organizações. Estes indivíduos ou grupos, muitas vezes motivados por ganhos financeiros, exploram vulnerabilidades em sistemas para obter acesso não autorizado a redes corporativas. Uma vez dentro, eles podem vender estes acessos no mercado negro para outros criminosos, que podem utilizar estas brechas para fins nefastos como roubo de dados, espionagem industrial, ou lançamento de ataques de ransomware. Este comércio ilícito não apenas coloca em risco a integridade e a confidencialidade das informações empresariais, mas também pode ter um impacto devastador na reputação e na sustentabilidade financeira das organizações afetadas.

2 Ator de ameaça vendendo acessos a dispositivos Fortinet

Recentemente foi observado em um fórum hacker que um ator de ameaça conhecido como DBLand, afirma disponibilizar acesso não autorizado às redes **Fortinet** de diversas corporações. Esse agente de ameaça anuncia a venda desses acessos, classificando-os conforme a avaliação das empresas afetadas, porém, sem especificar a quais setores pertencem. As evidências mostram que, embora as entidades mais afetadas sejam pequenas empresas, o ator malicioso também garante ter acesso às redes de grandes empresas.

Figura 1 – Post da venda dos acessos .

Na imagem acima é possível notar os valores das vendas como países das organizações onde o mesmo alega ter os acessos.

3 RISCOS DO VAZAMENTO DE CREDENCIAIS PARA ORGANIZAÇÕES

Quando as credenciais de organizações são vazadas em fóruns clandestinos, o perigo é iminente. Esses vazamentos representam uma ameaça direta à segurança das informações, possibilitando que criminosos tenham acesso a dados sensíveis, sistemas internos e infraestruturas críticas. Além de comprometer a integridade dos dados, os ataques resultantes podem interromper as operações da empresa, causando danos financeiros significativos e perda de reputação. Os adversários podem utilizar essas credenciais para executar ataques de phishing mais sofisticados, visando empregados ou clientes, ampliando o escopo do dano. A exposição de credenciais também aumenta o risco de violações de compliance e legais, expondo a organização a penalidades e ações judiciais.

No ambiente competitivo de hoje, as informações vazadas podem ser usadas por concorrentes de forma antiética, prejudicando ainda mais a posição de mercado da organização afetada. Por fim, a recuperação de um vazamento de credenciais pode exigir um esforço significativo e recursos para reforçar a segurança, investigar o alcance do comprometimento e restaurar a confiança dos stakeholders.

4 CONCLUSÃO

Para fortalecer a segurança contra vazamentos de credenciais, especialmente em produtos Fortinet ou sistemas similares, organizações devem adotar uma abordagem multifacetada que inclua políticas rigorosas de senha, medidas de segurança técnica, e práticas de conscientização.

Abaixo destacamos recomendações detalhadas para proteger as credenciais da sua organização:

Políticas e práticas de senha

- **Uso de senhas fortes**: Implemente políticas que exijam senhas complexas, combinando letras maiúsculas e minúsculas, números e símbolos.
- **Alteração regular de senhas**: Estabeleça uma política para a mudança regular de senhas, evitando a reutilização de senhas anteriores.
- **Autenticação multifator (MFA)**: Ative MFA para adicionar uma camada adicional de segurança, garantindo que mesmo que uma senha seja comprometida, o acesso não autorizado ainda possa ser bloqueado.

Segurança técnica

- **Atualizações e patches**: Assegure-se de que todos os sistemas, especialmente aqueles fornecidos por Fortinet ou outros fornecedores de tecnologia, estejam sempre atualizados com os patches de segurança mais recentes.
- **Ferramentas de gerenciamento de senhas**: Utilize gerenciadores de senhas corporativos para armazenar e gerenciar credenciais de forma segura, reduzindo o risco de vazamentos de senhas.
- **Segurança de rede**: Implemente firewalls de próxima geração, sistemas de prevenção de intrusão, e soluções de detecção e resposta estendida (XDR) para monitorar e proteger a rede contra atividades suspeitas.

Educação e conscientização

- **Treinamento de funcionários**: Realize treinamentos regulares de conscientização em segurança cibernética para educar os funcionários sobre os riscos associados ao uso inadequado de credenciais e as melhores práticas para mantê-las seguras.
- **Simulações de phishing**: Conduza simulações de phishing para testar a resposta dos funcionários a tentativas de engenharia social, fortalecendo a conscientização sobre táticas comuns usadas por atacantes.

Monitoramento e resposta

- **Análise de logs e monitoramento**: Monitore continuamente os logs de acesso e segurança para detectar tentativas de acesso não autorizado ou padrões suspeitos que possam indicar uma violação de segurança.

- **Plano de resposta a incidentes**: Desenvolva e mantenha um plano de resposta a incidentes atualizado, garantindo que a equipe esteja preparada para responder rapidamente a qualquer vazamento de credenciais.

Avaliação e testes de segurança

- **Auditorias de segurança regular**: Realize auditorias de segurança e testes de penetração regulares para identificar vulnerabilidades potenciais e garantir que as medidas de segurança sejam eficazes.
- **Revisão de políticas de acesso**: Implemente o princípio do menor privilégio, garantindo que os usuários tenham apenas o acesso necessário para realizar suas tarefas.

5 REFERÊNCIAS

- **Heimdall *by* ISH Tecnologia**
- **Dailydarkweb**

heimdall
security research
A DIVISION OF ISH