BOLETIM DE SEGURANÇA

MFA e a importância do seu uso para as organizações!

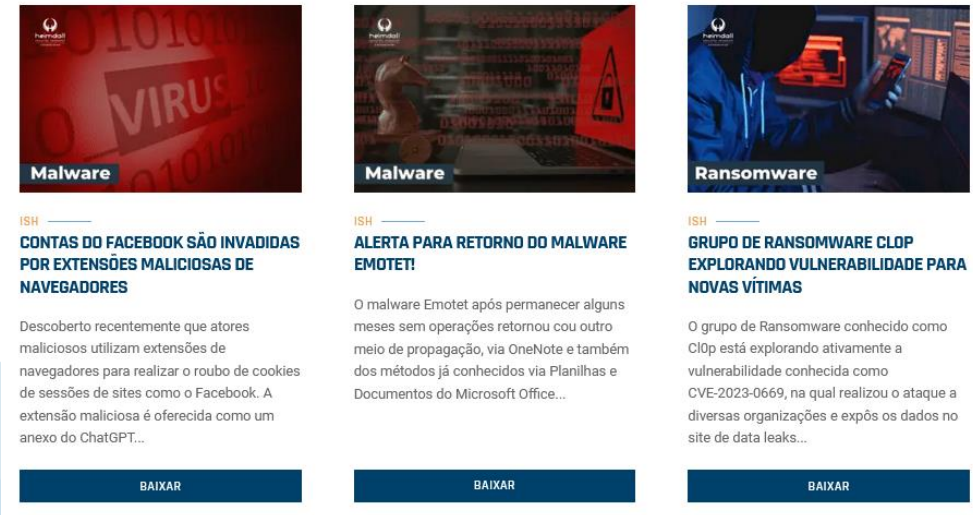
heimdall
security research
A DIVISION OF ISH

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

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

Atualmente no mundo da cibersegurança onde organizações e governos estão cada vez mais conectados à Internet com seus sistemas, infraestruturas etc. Os ataques baseados em credenciais destacam-se como uma das ameaças mais comuns e prejudiciais. Credenciais, que incluem nomes de usuário, senhas e outros identificadores, servem como chaves de acesso a sistemas, redes e dados valiosos.

Quando criminosos cibernéticos se apoderam dessas "chaves", eles obtêm um passe direto para realizar atividades maliciosas dentro das redes alvos, desde espionagem, roubo de dados ou até mesmo sabotagem. Estes ataques aproveitam-se de diversas falhas, sejam elas humanas, como o uso de senhas fracas ou a reutilização de senhas em múltiplos sites, ou técnicas, como brechas de segurança em sistemas de autenticação. À medida que a tecnologia continua a evoluir e os ambientes online tornam-se cada vez mais integrados ao nosso cotidiano, a necessidade de compreender e se proteger contra ataques de credenciais torna-se ainda mais urgente.

2 ATAQUES CIBERNÉTICOS POR MEIO DE CREDENCIAIS

Os ataques cibernéticos que envolvem credenciais visam principalmente obter acesso não autorizado a sistemas, redes, aplicações ou dados. Abaixo citamos alguns dos tipos comuns de ataques relacionados a credenciais:

Ataque de força bruta

- Tentativas repetidas e sistemáticas para adivinhar uma senha.

Credential Stuffing

- Usa combinações de nomes de usuário e senhas vazadas em tentativas automáticas de login para obter acesso a contas.

Phishing

- Tentativas de enganar usuários para que forneçam suas credenciais, geralmente através de e-mails ou websites falsificados.

Ataque Man-in-the-Middle (MitM)

- Ocorre quando os invasores interceptam e possivelmente alteram as comunicações entre duas partes sem o conhecimento delas.

Pass-the-Hash

- É utilizado hashes de senha em vez de senhas em si para autenticação.

Dumping de credenciais

- Técnicas usadas para extrair conjuntos de credenciais, como senhas ou chaves, de um sistema.

Ataques de elevação de privilégio

- Uma vez que um atacante tem acesso a um sistema, ele pode tentar elevar seus privilégios para obter mais controle.

Ataques de Account Takeover (ATO)

- Quando invasores ganham acesso a uma conta e assumem o controle dela.

3 VENDAS DE CREDENCIAIS DE ACESSO NA DARK WEB

A venda de credenciais de acesso de organizações e governos na Dark Web é um problema grave que tem estado em crescimento. A Dark Web, serve como um mercado negro para a venda de várias credenciais e informações sensíveis. Existem marketplaces específicos na Dark Web onde as credenciais são vendidas. Esses marketplaces são lugares comuns para a venda de credenciais corporativas e outras informações sensíveis.

Também é possível observar a venda de credenciais executivas que são altamente valorizadas na Dark Web, pois proporcionam aos cibercriminosos a oportunidade de atacar uma empresa "por dentro". Eles podem se passar por executivos e potencialmente espalhar malwares ou adulterar processos de negócios.

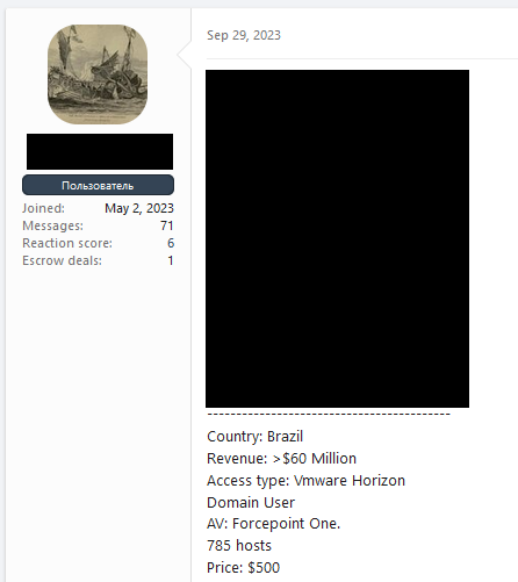


Figura 1 – Venda de acesso a uma organização Brasileira.

Figura 2 – Venda de acesso a uma organização brasileira.

4 IMPORTÂNCIA DO USO DO MFA

A Autenticação Multifator (MFA) é crucial para a segurança de organizações e governos, pois adiciona uma camada extra de proteção além das tradicionais credenciais de usuário e senha.

Listamos abaixo alguns pontos sobre a importância e exemplos de uso do MFA nas organizações:

Aumento da segurança

- O MFA requer que os usuários forneçam pelo menos dois fatores de verificação antes de obterem acesso a um site, aplicativo ou recurso, o que dificulta o acesso não autorizado, mesmo se uma das credenciais for comprometida.
- A MFA ajuda a proteger contra violações devido a credenciais perdidas ou roubadas, tornando difícil para os atacantes obterem acesso mesmo se conseguirem comprometer uma senha.
- A implementação da MFA ajuda a reduzir o risco de invasões de contas e fornecer segurança digital superior aos usuários e suas contas.

Custo-eficácia e evolução tecnológica

- A implementação da MFA tornou-se mais razoável e rentável para as organizações do que no passado, e a tecnologia continua a evoluir, o que pode reduzir a gestão interna de TI necessária.

Proteção de dados e transações online

- Empresas utilizam a MFA para proteger dados organizacionais e de usuários, permitindo que as interações e transações online sejam realizadas com segurança.

5 ALERTA CISA

Recentemente a **CISA** (*Cybersecurity and Infrastructure Security Agency*) divulgou em sua página oficial configurações incorretas (*Misconfiguration*) e pontos fracos conhecidos por serem usados em campanhas de ransomware onde a mesma recomenda o uso da autenticação multifator (MFA) como adição de camada extra de segurança contra estes tipos de ataques.

6 Conclusão

Os ataques baseados em credenciais são especialmente perigosos porque, uma vez que um invasor tem credenciais válidas, ele pode muitas vezes acessar sistemas e dados sem levantar suspeitas. Para organizações, a implementação do MFA significa proteger seus ativos, reputação e, em última análise, sua viabilidade no mercado. Uma única violação de dados pode resultar em perdas financeiras significativas, danos à reputação e litígios prolongados. No contexto governamental, os riscos são ainda maiores pois uma violação pode comprometer a segurança nacional, expondo informações sensíveis e até mesmo colocando vidas em risco.

Por isso, é crucial proteger credenciais adequadamente, usar autenticação multifatorial sempre que possível e educar os usuários sobre as melhores práticas de segurança.

7 RECOMENDAÇÕES

Poderão ser adotadas medidas visando a mitigação dos problemas de segurança mencionadas neste relatório, como por exemplo:

Educação e treinamento dos usuários

- Eduque os usuários sobre a importância da MFA e como ela funciona
- Forneça treinamento sobre como configurar e usar a MFA corretamente
- Use MFA em todos os pontos de acesso críticos
- Implemente MFA para todos os logins de sistemas, aplicações críticas e interfaces de gerenciamento
- Não se limite apenas a logins externos; considere também os acessos internos

Diversifique os métodos de autenticação

- Ofereça vários métodos de MFA, como tokens de hardware, SMS, aplicativos de autenticação e biometria
- Evite depender exclusivamente de SMS como método de MFA, pois eles podem ser vulneráveis a ataques de interceptação

Políticas de Backup

- Estabeleça processos seguros para redefinir ou recuperar o acesso em caso de perda do dispositivo de MFA
- Instrua os usuários a configurar métodos alternativos de MFA ou códigos de backup

Revogação e gestão

- Implemente sistemas que permitam aos administradores revogar ou suspender rapidamente o MFA para contas comprometidas
- Monitore tentativas de login falhadas e alerte os usuários e administradores sobre atividades suspeitas
- Integre MFA com Soluções de SSO (Single Sign-On)
- Isso oferece uma experiência de usuário mais fluida, exigindo MFA apenas uma vez para acessar vários serviços.

Mantenha softwares e soluções de MFA atualizados

- Assim como qualquer outra solução de segurança, é essencial manter os sistemas de MFA atualizados para proteger contra vulnerabilidades conhecidas.

Adapte-se ao contexto

- Considere soluções de MFA adaptativas que avaliam o risco com base no comportamento e no contexto do usuário (por exemplo, localização, dispositivo, horário de acesso) e ajustam os requisitos de autenticação de acordo.

Testes periódicos

- Realize testes regularmente para garantir que a MFA esteja funcionando como esperado e que os usuários saibam como usá-la corretamente.

Política de Senhas

- Embora a MFA adicione uma camada de segurança, ainda é crucial manter políticas de senhas fortes. A MFA deve complementar, e não substitui, boas práticas de senha.

Plano de Resposta a Incidentes

- Esteja preparado para responder a incidentes relacionados à MFA, como contas bloqueadas ou dispositivos de MFA perdidos.

Avaliação Contínua

- Avalie regularmente a eficácia e a usabilidade da sua solução MFA. À medida que a paisagem de ameaças evolui, sua abordagem ao MFA também deve evoluir.

8 REFERÊNCIAS

- **Heimdall *by* ISH Tecnologia**
- **CISA**
- **NIST**

heimdall
security research
A DIVISION OF ISH