BOLETIM DE RECOMENDAÇÃO

Recomendações para vazamentos de credenciais!

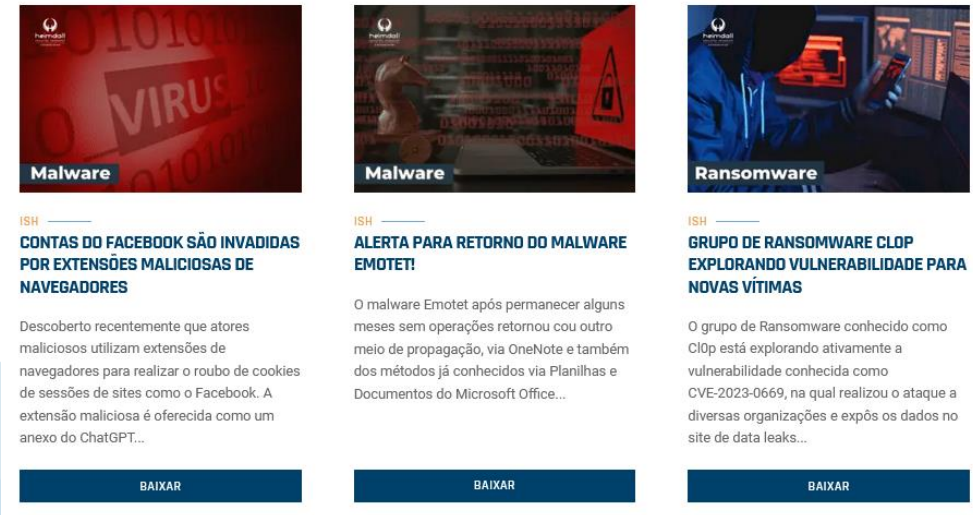
heimdall
security research
A DIVISION OF ISH

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

1 INTRODUÇÃO

As credenciais de acessos são a primeira linha de defesa, atuando como chaves para acesso a informações, sistemas e redes protegidas. No entanto, com a crescente digitalização dos processos empresariais e governamentais dos últimos anos, as violações de dados tornaram-se uma ocorrência comum. Uma vez que estas credenciais são vazadas, elas podem ser usadas por atores maliciosos para ganhar acesso não autorizado a sistemas, o que pode potencialmente levar a ataques mais avançados, espionagem, sabotagem ou roubo de informações confidenciais.

A exposição de credenciais, muitas vezes oriunda de violações de grandes bases de dados ou através de técnicas como o "*phishing*", torna-se uma commodity valiosa no mercado negro cibernético. Atacantes frequentemente adquirem, trocam ou vendem listas de credenciais vazadas em fóruns clandestinos. Estas listas, em seguida, podem ser usadas para uma variedade de propósitos maliciosos como: acesso direto, ataques de força bruta e preenchimento de credenciais, movimentação lateral, engenharia social entre outros.

2 RECOMENDAÇÕES DE SEGURANÇA

A seguir, nós da Heimdall preparamos as principais dicas de seguranças para aumento da maturidade da organização quanto ao tema.

Políticas de Senhas:

- **Política de senhas fortes:** Exija combinações de letras maiúsculas, minúsculas, números e caracteres especiais.
- **Política de senhas longas:** Incentive o uso de frases secretas sempre que possível.
- **Bloqueio de reutilização de senhas:** Implemente políticas que bloqueiem o uso das últimas 10 senhas utilizadas e suas variações.
- **Vencimento de senha:** Defina um tempo de vida para as senhas, forçando a alteração a cada período determinado, geralmente não superior a 90 dias.

Autenticação e Segurança em Acesso:

- **Autenticação de dois fatores (2FA):** Implemente o uso de autenticação de dois fatores, preferencialmente com OTP, e evite autenticação por SMS.
- **Monitoramento de acesso:** Registre atividades de login e ações para identificar comportamentos suspeitos.
- **Segurança em camadas:** Utilize firewalls, antivírus, sistemas de detecção de intrusões e segregação de redes para criar camadas de segurança.

Atualizações e Treinamento:

- **Atualizações e patches:** Mantenha sistemas e software atualizados com as últimas correções de segurança.
- **Treinamento de conscientização:** Forneça treinamento em segurança cibernética para funcionários, ensinando-os a reconhecer ameaças e práticas inseguras.

Controle de Acesso e Dispositivos:

- **Controle de acesso:** Use princípios de controle de acesso para garantir que apenas pessoas autorizadas tenham acesso a informações críticas.

- **Política de uso de dispositivos pessoais:** Estabeleça políticas claras sobre o uso de dispositivos pessoais na rede corporativa, com medidas de segurança apropriadas.
- **Acesso remoto seguro:** Se oferecer acesso remoto, utilize conexões VPN seguras e autenticação forte.

Parceiros e Testes de Segurança:

- **Monitoramento de terceiros (Parceiros):** Garanta que fornecedores e parceiros também sigam práticas de segurança adequadas.
- **Testes de penetração:** Realize testes de penetração regulares para identificar vulnerabilidades e corrigi-las antes de serem exploradas.

Criptografia e Isolamento de Redes:

- **Criptografia:** Proteja dados em repouso, trânsito e armazenamento com criptografia.
- **Isolamento de redes:** Separe sistemas sensíveis em redes isoladas para evitar comprometimento em larga escala.

Gerenciamento de Identidade e Conformidade:

- **Gerenciamento de identidade e acesso (IAM):** Utilize soluções de IAM para controlar o acesso dos usuários a sistemas e dados.
- **Conformidade com regulamentações:** Esteja em conformidade com regulamentações de segurança cibernética relevantes ao seu setor.

Preparação e Resposta a Incidentes:

- **Equipe de inteligência de ameaças:** Considere ter uma equipe dedicada para monitorar ameaças e implementar medidas de segurança.
- **Planos de resposta a incidentes:** Desenvolva planos detalhados para responder a incidentes de segurança, incluindo notificação de partes interessadas e recuperação de dados.

Backup e Outras Medidas:

- **Backup regular:** Faça backup regular de dados importantes e armazene-os em locais seguros.
- **Restrição de senhas salvas no navegador:** Implemente regras para evitar o salvamento de senhas no navegador.

- **Utilize blocklist de senhas vazadas:** Bloqueie senhas comuns utilizando listas de senhas vazadas.
- **Aplique um timeout:** Implemente um tempo limite de inatividade para forçar o login novamente.

3 RECOMENDAÇÕES APÓS VAZAMENTOS DE CREDENCIAIS

A seguir, nós da Heimdall preparamos as principais dicas de segurança para que após identificação de vazamento de credenciais sejam adotadas e preserve o ambiente da empresa evitando possíveis incidentes de seguranças.

Confirmação e Isolamento:

- **Confirme a autenticidade do vazamento:** Verifique a autenticidade do vazamento usando ferramentas de verificação e fontes confiáveis.
- **Isolamento e contenção:** Isole imediatamente as contas ou sistemas afetados para evitar a propagação do vazamento. Revogue as credenciais comprometidas e interrompa o acesso não autorizado.

Comunicação e Avaliação:

- **Notificação interna:** Informe a equipe de segurança cibernética, pessoal de TI e gerência sênior sobre o vazamento para garantir que todos estejam cientes da situação e das medidas a serem tomadas.
- **Avaliação do escopo:** Determine a extensão do vazamento, identificando informações expostas e sistemas ou contas afetadas.

Medidas de Segurança e Legal:

- **Alteração de credenciais:** Exija a alteração imediata de todas as senhas comprometidas, tanto nas contas afetadas quanto em outras que compartilhem as mesmas credenciais.
- **Monitoramento de atividade:** Aumente o monitoramento de atividade nas contas e sistemas afetados para detectar comportamentos anômalos.
- **Notificação legal:** Se aplicável, notifique as autoridades relevantes e esteja em conformidade com regulamentações locais ou internacionais sobre divulgação de violações de dados.

Preparação e Prevenção Futura:

- **Plano de comunicação pública**: Desenvolva um plano de comunicação pública se o vazamento tiver impacto amplo ou estiver sujeito a regulamentações específicas.

- **Análise de causa raiz:** Investigue as causas do vazamento para entender como ocorreu e prevenir incidentes semelhantes no futuro.
- **Ações corretivas:** Implemente ações corretivas com base na análise de causas, como atualizações de software, revisões de políticas ou reforços de segurança.
- **Revisão de processos de segurança:** Reavalie os processos de segurança cibernética para identificar melhorias e evitar futuros incidentes.
- **Treinamento e conscientização:** Reforce o treinamento em segurança cibernética entre os funcionários para prevenir futuros vazamentos.

Recuperação e Aprendizado:

- **Avaliação de danos e recuperação:** Avalie os danos causados pelo vazamento e desenvolva um plano de recuperação para restaurar a normalidade.
- **Relatório e aprendizado:** Prepare um relatório detalhado sobre o incidente, as medidas tomadas e as lições aprendidas para melhorar a postura de segurança da organização.

Lidar com um vazamento de credenciais é um processo complexo, mas seguir esses passos pode ajudar a minimizar os danos e a evitar problemas futuros. A colaboração entre equipes de TI, segurança cibernética, gerência e comunicação é fundamental durante esse período.

4 REFERÊNCIAS

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


heimdall
security research
A DIVISION OF ISH