BOLETIM DE SEGURANÇA

Halliburton, gigante petrolífera dos EUA, revela que ataque cibernético foi responsável por interrupção de sistemas

heimdall
security research
A DIVISION OF ISH

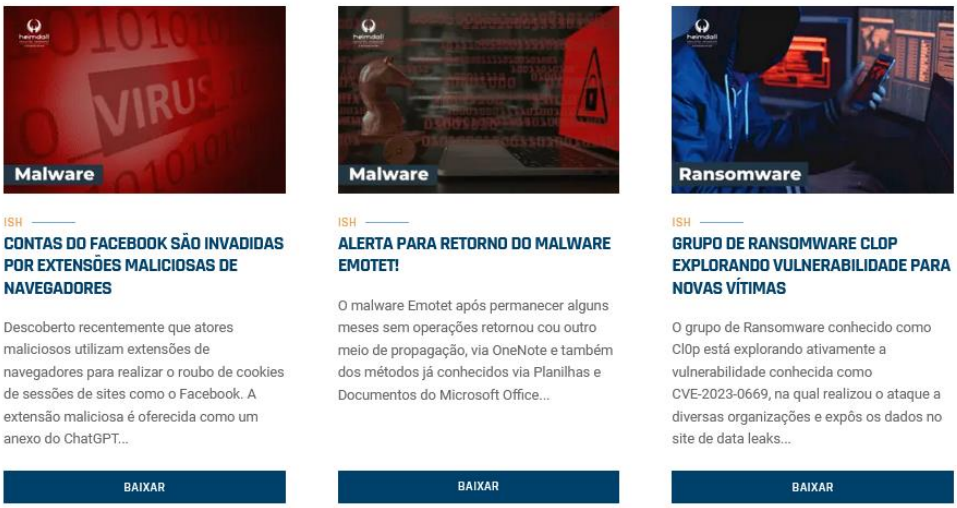
TLP: CLEAR

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

1 Sumário Executivo 4

2 Natureza do ataque não revelada 5

3 Recomendações 6

4 Referências 8

1 SUMÁRIO EXECUTIVO

A Halliburton, uma das principais fornecedoras globais de serviços para o setor energético, confirmou ter sofrido um ataque cibernético que resultou na necessidade de desativar alguns de seus sistemas na semana passada.

Em um documento submetido à Comissão de Valores Mobiliários dos Estados Unidos (SEC), a gigante do setor de petróleo declarou: "Em 21 de agosto de 2024, a Halliburton Company (a 'Empresa') tomou conhecimento de que terceiros não autorizados conseguiram acessar alguns de seus sistemas." Assim que a empresa identificou o problema, ativou seu plano de resposta a incidentes cibernéticos e deu início a uma investigação interna, contando com o apoio de consultores externos para avaliar e mitigar a atividade não autorizada.

Segundo a empresa, o incidente, que foi inicialmente reportado pela Reuters na quarta-feira com base em informações de fontes anônimas, resultou na desativação de certos sistemas para conter a violação.

A Halliburton também notificou as autoridades competentes sobre o ocorrido, enquanto sua equipe de TI trabalha na recuperação dos dispositivos afetados e na avaliação do impacto do ataque. "Como parte da resposta, a empresa tomou medidas preventivas, desativando proativamente determinados sistemas para protegê-los e notificando as autoridades. A investigação e as ações corretivas em andamento incluem a restauração dos sistemas e a avaliação da gravidade do incidente", informou a Halliburton. "A empresa está em contato com seus clientes e outras partes interessadas, seguindo rigorosamente seus padrões de segurança operacional baseados no Halliburton Management System, e continua trabalhando para identificar quaisquer efeitos decorrentes do incidente."

2 NATUREZA DO ATAQUE NÃO REVELADA

A Halliburton ainda não divulgou oficialmente qual ator de ameaças foi responsável pelo ataque mencionado. No momento, a natureza exata do incidente e a identidade dos autores permanecem desconhecidas. É comum que detalhes específicos sobre os atacantes sejam revelados posteriormente, após investigações mais aprofundadas.

3 RECOMENDAÇÕES

São elencadas abaixo pela ISH, medidas que poderão ser adotadas visando a mitigação da referida *ameaça,* como por exemplo:

Fortalecimento da segurança da rede

- **Segmentação de rede**: Dividir a rede em segmentos menores para limitar o impacto de um possível ataque.
- **Monitoramento contínuo**: Implementar sistemas de detecção e resposta a intrusões (IDS/IPS) e realizar monitoramento contínuo para identificar e mitigar ameaças rapidamente.
- **Firewall e VPN**: Utilizar firewalls robustos e VPNs seguras para proteger o tráfego de rede, especialmente entre sites remotos e sistemas internos.

Gestão de acessos e identidade

- **Autenticação multifator (MFA)**: Implementar MFA em todos os sistemas críticos para evitar acessos não autorizados.
- **Privilégios mínimos**: Aplicar o princípio do menor privilégio, garantindo que os usuários tenham apenas as permissões necessárias para suas funções.
- **Revisão regular de acessos**: Realizar auditorias regulares de contas e acessos para garantir que apenas pessoas autorizadas possam acessar sistemas sensíveis.

Proteção de dados

- **Criptografia de dados**: Criptografar dados em repouso e em trânsito, especialmente informações sensíveis e de propriedade intelectual.
- **Backup regular**: Implementar um plano de backup regular e testar as restaurações periodicamente para garantir que os dados possam ser recuperados em caso de ataque.

Educação e conscientização dos funcionários

- **Treinamento em cibersegurança**: Realizar treinamentos regulares de conscientização sobre cibersegurança para todos os funcionários, com foco em phishing, engenharia social e boas práticas de segurança.
- **Simulações de ataques**: Conduzir simulações de ataques cibernéticos, como campanhas de phishing, para avaliar a preparação dos funcionários e ajustar treinamentos conforme necessário.

Plano de resposta a incidentes

- **Desenvolvimento de um plano de resposta**: Criar e manter um plano de resposta a incidentes detalhado que abranja a detecção, contenção, erradicação, recuperação e comunicação.

- **Equipes dedicadas**: Ter equipes dedicadas à resposta a incidentes, com membros treinados em procedimentos específicos para lidar com ataques cibernéticos.
- **Parcerias com especialistas**: Estabelecer parcerias com empresas de segurança cibernética para suporte em resposta a incidentes e recuperação.

Gestão de vulnerabilidades

- **Atualizações e patches**: Garantir que todos os sistemas e softwares estejam atualizados com os patches mais recentes, especialmente em sistemas críticos de operação.
- **Testes de penetração**: Realizar testes de penetração regularmente para identificar e corrigir vulnerabilidades antes que possam ser exploradas.

Conformidade e regulamentações

- **Adesão a normas e padrões**: Assegurar conformidade com normas de segurança cibernética específicas do setor energético, como o NIST, ISO 27001, e regulamentos locais e internacionais.
- **Auditorias regulares**: Conduzir auditorias de segurança regulares para garantir a conformidade contínua com as melhores práticas e regulamentações do setor.

Proteção de infraestrutura crítica

- **Segurança física e cibernética integradas**: Integrar medidas de segurança física e cibernética para proteger a infraestrutura crítica, como sistemas SCADA (Supervisory Control and Data Acquisition).
- **Redundância e resiliência**: Implementar sistemas redundantes e planos de continuidade de negócios para garantir operações contínuas mesmo em caso de um ataque cibernético.

Investimento em tecnologias de segurança

- **Inteligência Artificial e Machine Learning**: Investir em tecnologias avançadas de segurança que utilizam IA e ML para detectar padrões anômalos e responder rapidamente a ameaças emergentes.
- **Zero Trust Architecture**: Adotar uma arquitetura de segurança Zero Trust, onde nenhum acesso é automaticamente confiável e todas as solicitações de acesso são verificadas e autenticadas.

4 REFERÊNCIAS

- **Heimdall *by* ISH Tecnologia**
- **Documento disponibilizado sobre o incidente**
- **Reuters**
- **Bleepingcomputer**

heimdall
security research
A DIVISION OF ISH