BOLETIM DE SEGURANÇA

Ataque do ransomware Cactus a Gigante de energia Schneider Electric

heimdall
security research
A DIVISION OF ISH

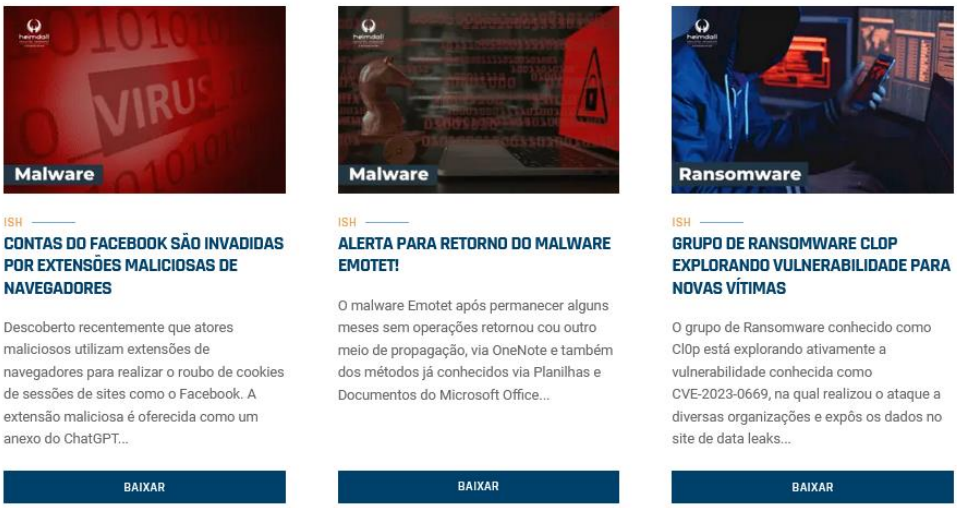
TLP: CLEAR

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

Ocorreu em janeiro de 2024 um ataque do ransomware Cactus à Schneider Electric, uma gigante no setor de gestão de energia e automação, o ataque foi direcionado especificamente à divisão de Sustentabilidade da empresa. Esta divisão é responsável por fornecer serviços de consultoria relacionados a soluções de energia renovável e conformidade regulatória climática para organizações empresariais pelo mundo. Durante o ataque, os sistemas de plataforma em nuvem da empresa, especificamente o *Resource Advisor*, foram interrompidos, e ainda enfrentam problemas de interrupção.

Figura 1 – Logo da Schneider Electric.

2 DETALHES DO ATAQUE OCORRIDO

As informações do ataque são descritas logo abaixo, separadas por tópicos par ao melhor entendimento do ocorrido.

1. **Infiltração e roubo de dados**

A gangue de ransomware conseguiu infiltrar-se na rede da Schneider Electric e roubar terabytes de dados corporativos. O tipo específico de dados roubados não é conhecido, mas pode incluir informações sensíveis sobre os clientes da divisão, suas utilizações de energia, sistemas de controle industrial e automação, e dados relacionados à conformidade com regulamentações ambientais e energéticas em todo o mundo.

Figura 2 – Mensagem de interrupção na plataforma Resource Advisor da Schneider Electric.

2. **Ameaça de vazamento de dado**

Os criminosos estão agora extorquindo a Schneider Electric, ameaçando vazar os dados roubados, a menos que suas demandas de resgate sejam atendidas.

3. **Isolamento da divisão afetada**

A divisão de Sustentabilidade da Schneider Electric opera com uma infraestrutura de rede isolada, o que impediu a propagação do ataque para outras partes da empresa.

4. **Medidas de recuperação e segurança**

A Schneider Electric confirmou o ataque e afirmou estar tomando medidas de recuperação para restaurar as plataformas de negócios a um ambiente seguro. A empresa também está realizando uma análise forense detalhada do incidente, com a assistência de firmas líderes em cibersegurança.

5. **Contexto mais amplo**

Este ataque está inserido em um contexto de aumento de ataques cibernéticos ao setor de energia, que é considerado um alvo atraente para grupos

de ransomware devido ao seu papel essencial na sociedade e às consequências significativas que as interrupções podem causar.

6. Histórico da Schneider Electric com ataques cibernéticos

A Schneider Electric já havia sido alvo anteriormente de ataques de ransomware, incluindo o ataque de grande escala da gangue Cl0p no MOVEit data theft, que afetou mais de 2.700 empresas ao longo de vários meses.

3 CONCLUSÃO

O grupo por trás do Cactus também se destaca por suas técnicas de extorsão, empregando o que é conhecido como "tríplice extorsão". Além de criptografar e roubar dados das vítimas, eles se comunicam diretamente com partes interessadas relevantes para aumentar a urgência das demandas de resgate. Eles têm como alvo informações sensíveis para extorquir as vítimas, ameaçando vender informações pessoais, segredos comerciais, bancos de dados e códigos-fonte para múltiplos atores de ameaças caso o resgate não seja pago.

O Cactus é notável por sua rápida ascensão, sendo classificado entre os dez principais grupos de ransomware em termos de vítimas mensais até novembro de 2023. Eles focam em pagamentos substanciais e têm como alvo principalmente entidades comerciais de grande porte. A natureza sofisticada de seus ataques e a habilidade de evadir defesas cibernéticas destacam a importância da higiene cibernética básica, além da monitorização e detecção para proteção contra ransomwares mais novos.

4 RECOMENDAÇÕES

Além dos indicadores de comprometimento elencados abaixo pela ISH, poderão ser adotadas medidas visando a mitigação da infecção do referido *ransomware*, como por exemplo:

Backups regulares

- Faça backups regulares e completos de todos os dados críticos. Armazene esses backups em um local seguro, preferencialmente desconectado da rede principal, para evitar que sejam afetados pelo ransomware.

Atualizações de segurança

- Mantenha todos os sistemas operacionais e softwares atualizados. Isso inclui a aplicação regular de patches de segurança para proteger contra vulnerabilidades conhecidas que podem ser exploradas por ransomwares.

Treinamento de conscientização de segurança

- Eduque os funcionários sobre as práticas de segurança de TI, incluindo a identificação de e-mails de phishing e sites maliciosos, que são métodos comuns usados para disseminar ransomware.

Soluções de antivírus e anti-malware

- Use soluções robustas de antivírus e anti-malware, e mantenha-as atualizadas. Configure-as para fazer varreduras regulares e monitorar o sistema em tempo real.

Controle de acesso e privilégios

- Implemente uma política de privilégio mínimo, garantindo que os usuários tenham apenas os acessos necessários para realizar suas funções. Isso limita o potencial de propagação do ransomware se uma conta for comprometida.

Segmentação de rede

- Divida a rede em segmentos para limitar a propagação do ransomware. Se uma parte da rede for comprometida, a segmentação pode evitar que o ransomware se espalhe para outras partes.

Firewalls e filtros de conteúdo

- Utilize firewalls e sistemas de detecção e prevenção de intrusões para monitorar e controlar o tráfego de rede. Implemente filtros de conteúdo para bloquear o acesso a sites suspeitos ou maliciosos.

Plano de resposta a incidentes

- Desenvolva e mantenha um plano de resposta a incidentes de segurança cibernética. Isso deve incluir procedimentos específicos para lidar com um ataque de ransomware, incluindo a restauração de dados a partir de backups.

Monitoramento contínuo de segurança

- Monitore continuamente a rede para detectar atividades suspeitas ou anômalas, o que pode indicar a presença de malware ou uma tentativa de ataque.

Avaliação de vulnerabilidades

- Realize avaliações regulares de vulnerabilidades e testes de penetração para identificar e remediar possíveis pontos fracos na segurança da rede.

5 REFERÊNCIAS

- **Heimdall *by* ISH Tecnologia**
- **Bleepingcomputer**
- **Secureworld**

heimdall
security research
A DIVISION OF ISH