BOLETIM DE SEGURANÇA

Cidade de Cleveland encerra operações após ciberataque a sistemas de TI

heimdall
security research
A DIVISION OF ISH

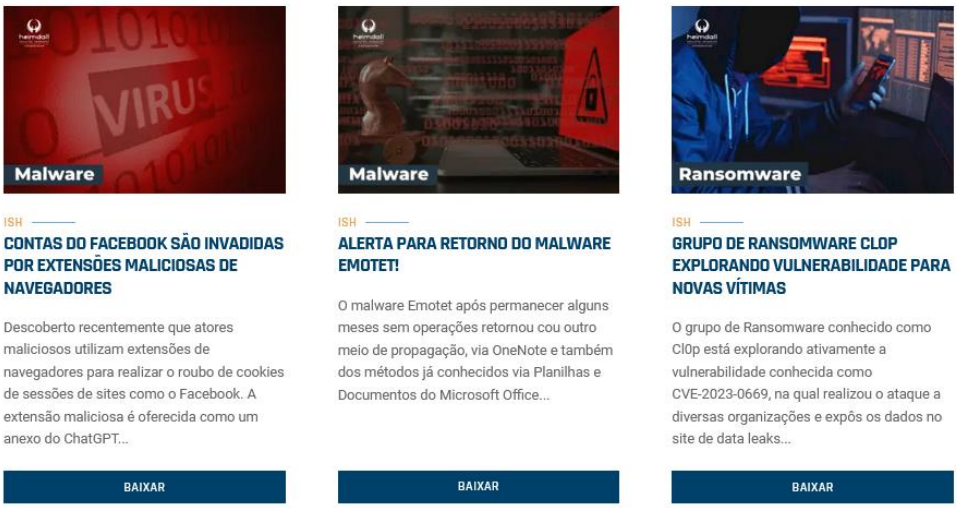
TLP: CLEAR

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

Recentemente a Cidade de Cleveland, uma cidade dos Estados Unidos, no estado do Ohio, informou em um comunicado na plataforma X antigo Twitter que a prefeitura e Erieview estariam fechadas, 10 e 11 de junho, exceto para funcionários essenciais, enquanto era investigado um incidente cibernético. Desligamos os sistemas afetados para proteger e restaurar serviços. Os serviços de emergência e serviços públicos não são afetados. As atualizações serão fornecidas conforme disponíveis, informaram as autoridades da cidade em nota.

2 ATUALIZAÇÃO DO INCIDENTE CIBERNÉTICO

Conforme outros Tweets da cidade, estão investigando a natureza e o escopo do incidente. A cidade está colaborando com vários parceiros importantes que fornecem conhecimento especializado e profunda experiência neste trabalho.

Figura 1 – Nota de atualização sobre o ocorrido.

Apesar do evento cibernético, os serviços básicos da cidade, incluindo segurança pública, obras públicas, serviços públicos e operações aeroportuárias, permanecem funcionais, embora com capacidades informáticas limitadas. O incidente não afetou os serviços de emergência, como polícia, bombeiros e EMS.

O FOX 8 I-Team informou que a cidade de Cleveland estava investigando ativamente o incidente. O comissário de tecnologia da informação da cidade, Kim Roy Wilson, revelou que as autoridades identificaram “anormalidades” em seu ambiente de TI porém não foram reveladas informações exatas sobre o ocorrido, enfatizando a importância de reter detalhes que poderiam comprometer a investigação da cidade.

3 CONCLUSÃO

Ataques cibernéticos que paralisam sistemas de TI causam impactos devastadores em organizações e órgãos públicos. A interrupção dos serviços pode resultar na perda de dados críticos, afetando diretamente a capacidade de operação e tomada de decisões. Financeiramente, os custos com reparos, recuperação de dados e medidas de segurança adicionais são significativos. A confiança dos usuários e stakeholders é abalada, o que pode levar à perda de clientes e reputação. Além disso, a exposição de informações sensíveis pode causar danos irreparáveis à privacidade e segurança. Em órgãos públicos, a paralisação pode afetar serviços essenciais, como saúde, segurança e infraestrutura, causando um efeito cascata na sociedade.

4 RECOMENDAÇÕES

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

Backup regular

- Implementar e manter backups regulares de todos os dados críticos, armazenando-os em locais seguros e separados dos sistemas principais.

Plano de resposta a incidentes

- Desenvolver e testar um plano de resposta a incidentes para garantir que a organização esteja preparada para reagir rapidamente a ataques cibernéticos.

Treinamento de funcionários

- Realizar treinamentos regulares de conscientização sobre segurança cibernética para todos os funcionários, enfatizando a importância de práticas seguras e a detecção de ameaças.

Autenticação multifator (MFA)

- Implementar autenticação multifator para acessar sistemas críticos, reduzindo o risco de comprometimento de contas devido a senhas fracas ou comprometidas.

Atualizações e patches

- Manter todos os sistemas e software atualizados com os patches de segurança mais recentes para corrigir vulnerabilidades conhecidas.

Monitoramento contínuo

- Estabelecer sistemas de monitoramento contínuo para detectar atividades suspeitas e responder a ameaças em tempo real.

Segmentação de rede

- Segmentar a rede para limitar o movimento lateral de atacantes dentro da infraestrutura, protegendo áreas críticas de serem acessadas a partir de compromissos iniciais.

Controle de acesso

- Implementar controles de acesso rigorosos para garantir que apenas pessoas autorizadas possam acessar informações e sistemas sensíveis.

Testes de penetração (Pentest)

- Realizar testes de penetração regulares para identificar e corrigir vulnerabilidades antes que sejam exploradas por atacantes.

Colaboração e compartilhamento de informações

- Participar de redes de compartilhamento de informações sobre ameaças cibernéticas com outras organizações e agências de segurança para se manter atualizado sobre novas ameaças e melhores práticas.

5 REFERÊNCIAS

- **Heimdall *by* ISH Tecnologia**
- **X-Cleveland**
- **fox8**
- **gbhackers**

6 AUTORES

- **Ismael Pereira Rocha**

heimdall
security research
A DIVISION OF ISH