BOLETIM DE SEGURANÇA

Ascension Healthcare desativa sistemas após ser alvo de ataque cibernético

heimdall
security research
A DIVISION OF ISH

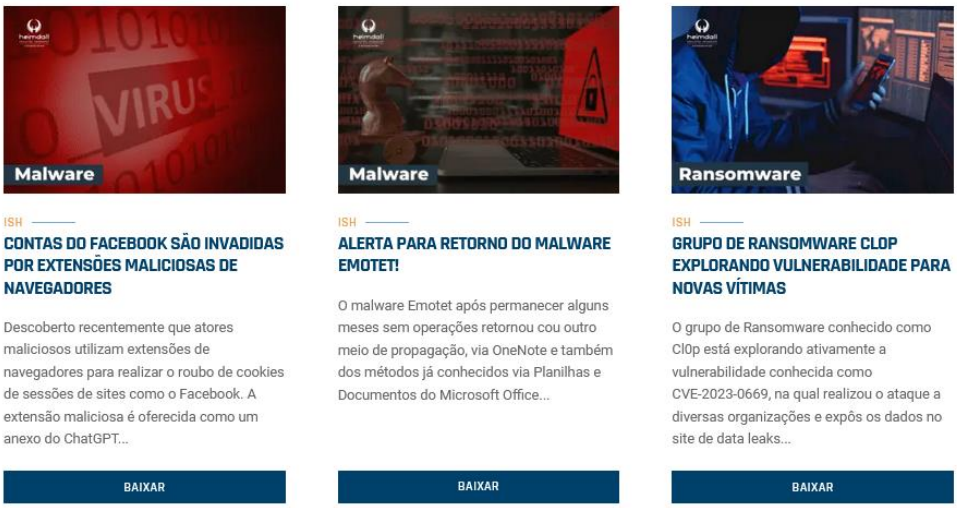
TLP: CLEAR

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

A Ascension Healthcare, um dos maiores sistemas de saúde sem fins lucrativos dos Estados Unidos, operando cerca de 140 hospitais em 19 estados e em Washington, D.C, empregando aproximadamente 134 mil pessoas, interrompeu certos sistemas para investigar o que chamou de "evento de segurança cibernética". Conforme publicação da mesma em sua página na plataforma X, antigo Twitter.

Figura 1 – Nota da Ascension em sua página na plataforma X.

A Ascension destacou hoje em seu site, sobre a atualização do evento de segurança, a seguinte mensagem: *Na quarta-feira, 8 de maio, detectamos atividade incomum em sistemas de rede de tecnologia selecionados, que agora acreditamos ser devido a um evento de segurança cibernética. Neste momento continuamos investigando a situação. Respondemos imediatamente, iniciamos nossa investigação e ativamos nossos esforços de remediação. O acesso a alguns sistemas foi interrompido à medida que esse processo continua.*

Até o momento não se tem mais detalhes sobre o ocorrido porém no mês passado o Departamento de Saúde e Serviços Humanos (**HHS**) dos EUA emitiu um aviso sobre uma nova abordagem adotada por agentes de ameaças no setor de Cuidados de Saúde e Saúde Pública (HPH). Eles estão agora recorrendo a estratégias de manipulação psicológica para atingir os help desks de TI. Esses invasores estão conseguindo ludibriar os funcionários para que registrem novos dispositivos de autenticação multifator (MFA) sob o controle deles, o que, por sua vez, concede acesso aos recursos corporativos.

2 CONCLUSÃO

O setor de saúde tem sido um alvo crescente de atores de ameaças, com hospitais enfrentando uma variedade de ataques cibernéticos sofisticados. Estes ataques frequentemente envolvem ransomware, roubo de dados sensíveis e perturbação de serviços críticos, colocando em risco não apenas a privacidade e a segurança dos dados dos pacientes, mas também a capacidade dos hospitais de fornecer cuidados essenciais, esses incidentes sublinham a necessidade urgente de medidas de segurança robustas. É vital que o setor invista em soluções avançadas de segurança e mantenham uma postura de vigilância constante para proteger-se contra essas ameaças crescentes

3 RECOMENDAÇÕES

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

Gerenciamento de acesso e controle de identidade

- Implementar autenticação de dois fatores e políticas de controle de acesso estritas para garantir que apenas pessoal autorizado tenha acesso a sistemas e dados sensíveis.

Criptografia de dados

- Utilizar criptografia forte tanto para dados em repouso quanto em trânsito para proteger informações sensíveis, incluindo dados dos pacientes.

Segurança de dispositivos e endpoint

- Garantir que todos os dispositivos conectados à rede do hospital, como computadores, tablets e dispositivos móveis, sejam protegidos com antivírus, anti-malware e outras ferramentas de segurança.

Atualizações e patching regulares

- Manter todos os sistemas operacionais, softwares e aplicativos atualizados com as últimas versões e patches de segurança para proteger contra vulnerabilidades conhecidas.

Treinamento e conscientização em segurança

- Realizar treinamentos regulares de conscientização em segurança para todos os funcionários, focando em práticas recomendadas, como identificação de phishing e outras táticas de engenharia social.

Monitoramento e análise de segurança

- Implementar soluções de monitoramento contínuo para detectar e responder rapidamente a atividades suspeitas ou maliciosas na rede.

Gerenciamento de risco e avaliações de segurança

- Realizar avaliações regulares de risco e auditorias de segurança para identificar e mitigar possíveis vulnerabilidades dentro da organização.

Plano de resposta a incidentes

- Desenvolver e manter um plano de resposta a incidentes abrangente para garantir uma resposta rápida e eficaz em caso de uma violação de segurança.

Backup e recuperação de dados

- Manter políticas robustas de backup e recuperação de dados para garantir a continuidade dos serviços em caso de ataques cibernéticos ou falhas de sistema.

Segurança física

- Reforçar a segurança física das instalações para prevenir acessos não autorizados aos locais críticos onde dados e infraestrutura de TI são mantidos.

4 REFERÊNCIAS

- **Heimdall *by* ISH Tecnologia**
- **Ascension**
- **Bleepingcomputer**
- **HHS**

5 AUTORES

- **Ismael Pereira Rocha**

heimdall
security research
A DIVISION OF ISH