BOLETIM DE SEGURANÇA

Dados médicos dos pacientes da DocGo roubados em ataque virtual

heimdall
security research
A DIVISION OF ISH

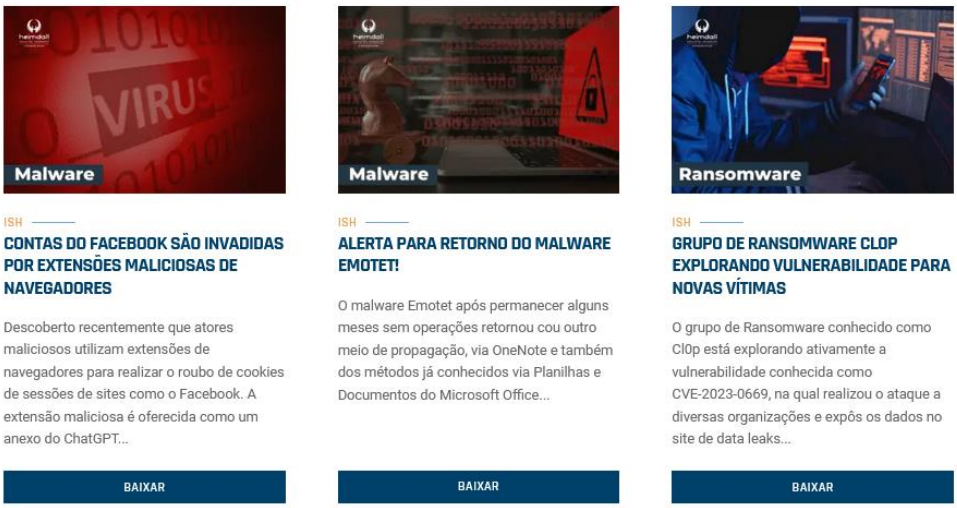
TLP: CLEAR

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

A DocGo, um provedor de serviços de saúde, divulgou em seu relatório 8-K a ocorrência de um incidente de segurança cibernética envolvendo alguns de seus sistemas. Após investigação, a empresa confirmou que o invasor obteve acesso e adquiriu dados, incluindo informações de saúde protegidas. A empresa oferece serviços móveis de saúde, ambulância e monitoramento remoto para pacientes em 30 estados dos EUA e no Reino Unido, com mais de 7 milhões de interações registradas. A violação afetou um número limitado de registros de saúde dentro do setor de transporte de ambulâncias nos EUA da DocGo, sem impacto em outras áreas de negócio. Conforme a DocGo está em contato com os indivíduos afetados pelo ataque, buscando ativamente soluções.

Até o momento, a natureza exata do ataque não foi determinada e nenhum agente de ameaça assumiu a responsabilidade pela violação, mas é comum que grupos de ransomware usem dados roubados como forma de pressionar as vítimas a pagar o resgate.

2 CONCLUSÃO

Conforme citado em outro alerta de segurança sobre o setor de saúde, o mesmo 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 DE SEGURANÇA PARA O SETOR

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**
- Form 8-K
- Malwarebytes

5 AUTORES

- **Ismael Pereira Rocha**

heimdall
security research
A DIVISION OF ISH