BOLETIM DE SEGURANÇA

Ataque cibernético provoca fechamento de lojas da rede London Drugs

heimdall
security research
A DIVISION OF ISH

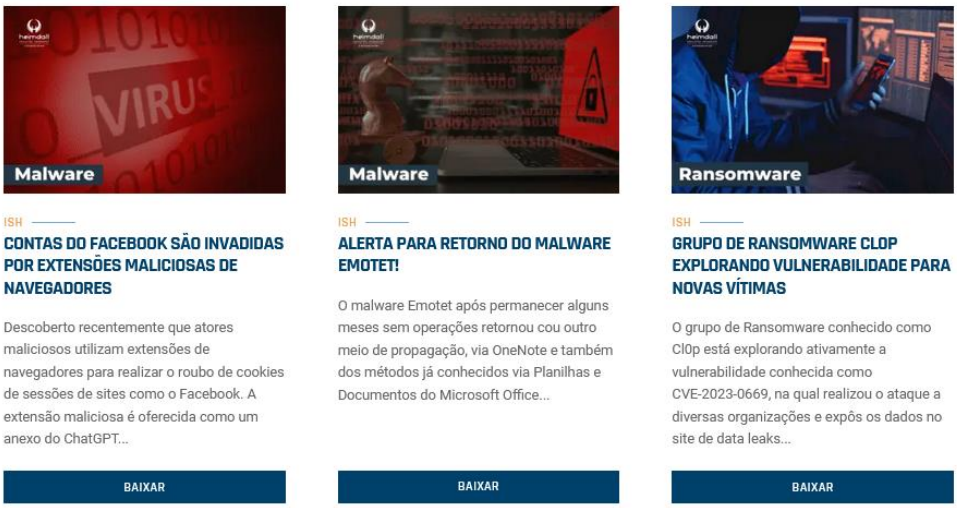
TLP: CLEAR

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 rede de farmácias canadense London Drugs suspendeu temporariamente as operações de suas lojas de varejo em resposta a um incidente de segurança cibernética, conforme descreveu a empresa em nota. No dia 28 de abril de 2024, a empresa percebeu que havia sido alvo de um ataque cibernético, como medida de segurança, optou por fechar todas as suas unidades no oeste do Canadá até segunda ordem, segundo um anúncio oficial. "Assim que tomamos conhecimento do incidente, agimos rapidamente para implementar medidas de proteção para nossa rede e dados, incluindo a assistência de consultores especializados em segurança cibernética para auxiliar na contenção e na investigação forense", afirmou a London Drugs.

Para enfrentar os desafios causados pelo ataque digital ocorrido no último fim de semana, a London Drugs recorreu à ajuda de especialistas em segurança cibernética contratados externamente. A empresa também informou que, até o momento, não há indícios de que os dados de clientes ou funcionários tenham sido afetados pelo incidente.

A London Drugs orienta os clientes a entrarem em contato com a farmácia mais próxima em caso de necessidades urgentes. Abaixo, segue o post da empresa em sua página na plataforma X.

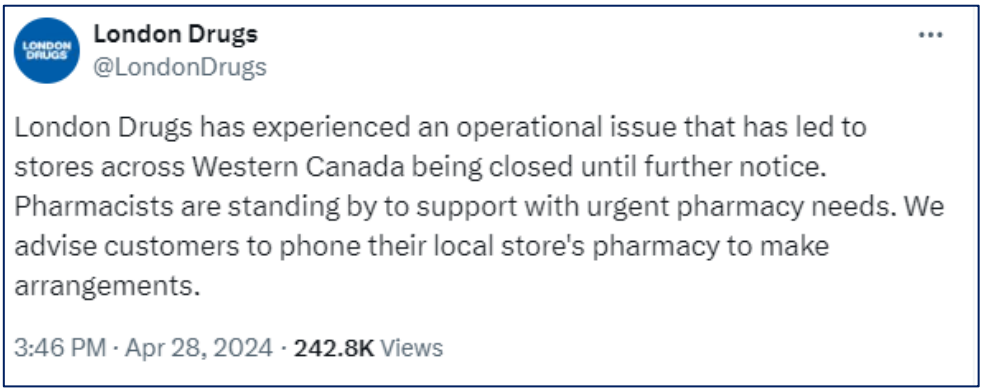


Figura 1 – Nota da London Drugs em sua plataforma na plataforma X.

A rede London Drugs ainda não comunicou às autoridades competentes sobre o incidente de segurança cibernética, pois não existem evidências de que dados pessoais ou de saúde de clientes e funcionários tenham sido afetados. “Ao encontrar qualquer indício de comprometimento de informações pessoais durante nossa investigação, informaremos as pessoas impactadas e os órgãos reguladores de privacidade conforme necessário pelas leis vigentes”, complementou a empresa.

2 CONCLUSÃO

O setor farmacêutico, com sua vasta gama de dados confidenciais e inovações valiosas, enfrenta riscos cibernéticos significativos, tornando-se um alvo atraente para grupos de atores maliciosos. Informações sobre fórmulas de medicamentos, dados de pacientes e resultados de ensaios clínicos são particularmente valiosas para cibercriminosos, que podem explorar esses dados para fins de chantagem, espionagem industrial ou venda no mercado negro. A interrupção dos sistemas de produção e distribuição através de ataques cibernéticos podem ter implicações graves não apenas financeiras, mas também para a saúde em geral, comprometendo o acesso a medicamentos essenciais. A proteção contra essas ameaças é crucial, exigindo investimentos contínuos em segurança cibernética para defender a integridade e a confiabilidade de operações críticas neste setor.

3 RECOMENDAÇÕES

São elencados abaixo pela ISH, medidas que poderão ser adotadas visando a proteção do setor, como por exemplo:

Gerenciamento de acesso

- Implemente controles rigorosos de acesso para garantir que apenas os funcionários autorizados tenham acesso a informações sensíveis. Isso inclui usar autenticação multifatorial e gerenciar as permissões de acordo com o princípio do menor privilégio.

Criptografia de dados

- Use criptografia tanto para dados em repouso quanto em trânsito. Isso ajuda a proteger informações confidenciais, como dados de ensaios clínicos e fórmulas de medicamentos, contra interceptações e acessos não autorizados.

Proteção contra malware e ransomware

- Instale soluções robustas de antivírus e anti-malware e mantenha-as atualizadas. Realize regularmente varreduras de segurança para detectar e isolar ameaças potenciais.

Treinamento em conscientização de segurança

- Eduque os funcionários sobre os riscos de segurança cibernética e as melhores práticas para evitar ataques. Isso inclui treinamento sobre phishing, gestão de senhas e medidas de segurança ao usar dispositivos móveis.

Backup e recuperação de dados

- Estabeleça políticas robustas de backup e teste regularmente os planos de recuperação de dados para garantir a integridade e disponibilidade das informações, especialmente para dados críticos de pesquisa e desenvolvimento.

Monitoramento e análise de segurança

- Implemente ferramentas de detecção de intrusão e sistemas de gestão de eventos e informações de segurança (SIEM) para monitorar, registrar e analisar atividades suspeitas em tempo real.

Gerenciamento de vulnerabilidades

- Realize avaliações de vulnerabilidade e testes de penetração regulares para identificar e mitigar vulnerabilidades no software e na infraestrutura de rede.

Segurança em nuvem

- Se você utiliza soluções baseadas em nuvem, assegure-se de que as políticas e controles de segurança da nuvem estão em conformidade com os padrões da indústria e específicos do setor farmacêutico.

Resposta a incidentes

- Desenvolva e mantenha um plano de resposta a incidentes de segurança cibernética. Isso deve incluir procedimentos para isolar o incidente, comunicar-se com as partes interessadas e recuperar as operações com mínimo impacto.

4 REFERÊNCIAS

- **Heimdall *by* ISH Tecnologia**
- **LondonDrugs**
- **Bleepingcomputer**

heimdall
security research
A DIVISION OF ISH