BOLETIM DE SEGURANÇA

Scattered Spider incorpora RansomHub e Qilin ransomware em sua estratégia de ataque cibernético

heimdall
security research
A DIVISION OF ISH

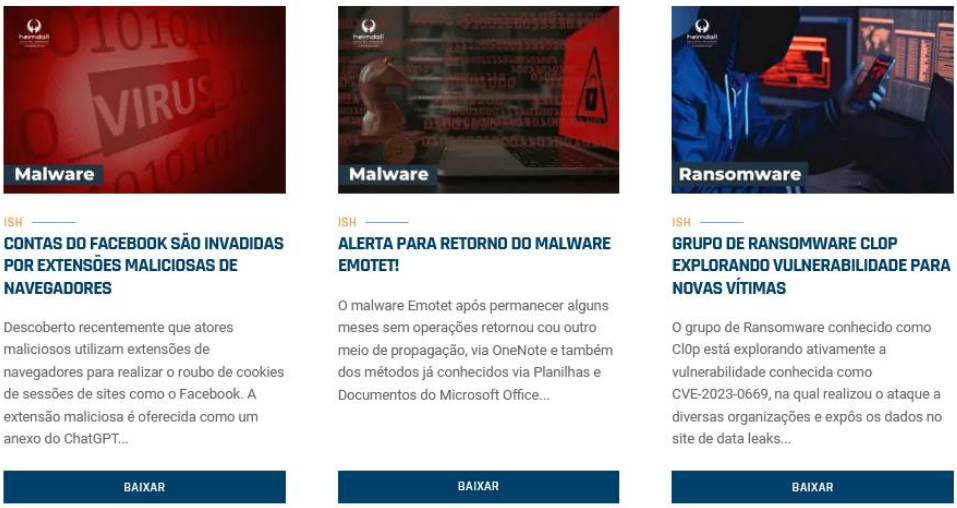
TLP: CLEAR

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

1 SUMÁRIO EXECUTIVO

O notório grupo de cibercriminosos, Scattered Spider, recentemente ampliou seu arsenal de ataques com a inclusão de variantes de ransomware como RansomHub e Qilin, conforme divulgado pela Microsoft.

2 INFORMAÇÕES SOBRE A AMEAÇA

O Scattered Spider, é um conhecido agente de ameaças, é famoso por suas táticas avançadas de engenharia social para comprometer alvos e estabelecer persistência para futuras explorações e roubo de dados. Ele tem um histórico de atacar servidores VMWare ESXi e implantar o ransomware BlackCat. Este grupo tem sobreposições com clusters de atividades monitorados pela comunidade de segurança cibernética sob os nomes Gold Harvest, 0ktapus, Octo Tempest e UNC3944. Recentemente, foi relatada a prisão de um membro importante do grupo na Espanha.

O RansomHub, que foi lançado no mercado em fevereiro, foi avaliado como uma versão reformulada de outra variante de ransomware chamada Knight, de acordo com uma análise da Symantec, uma empresa da Broadcom. A Microsoft afirmou que o RansomHub é uma carga útil de ransomware como serviço (RaaS) cada vez mais utilizada por agentes de ameaças, incluindo aqueles que historicamente usaram outras cargas úteis de ransomware (como o BlackCat), tornando-se uma das famílias de ransomware mais difundidas atualmente.

A Microsoft também observou o RansomHub sendo implantado como parte da atividade pós-comprometimento pelo Manatee Tempest (também conhecido como DEV-0243, Evil Corp ou Indrik Spider) após o acesso inicial obtido pelo Mustard Tempest (também conhecido como DEV-0206 ou Purple Vallhund) por meio de infecções do FakeUpdates (também conhecido como Socgholish). É importante mencionar que o Mustard Tempest é um corretor de acesso inicial que, no passado, utilizou FakeUpdates em ataques que levaram a ações semelhantes ao comportamento pré-ransomware associado à Evil Corp. Essas intrusões também foram notáveis pelo fato de que o FakeUpdates foi entregue por meio de infecções existentes do Raspberry Robin.

Este desenvolvimento ocorre em meio ao surgimento de novas famílias de ransomware como FakePenny (atribuído ao Moonstone Sleet), Fog (distribuído pelo Storm-0844, que também propagou o Akira) e ShadowRoot, este último observado atacando empresas turcas usando faturas falsas em PDF. A Microsoft aconselha que, à medida que a ameaça de ransomware continua a aumentar, expandir e evoluir, usuários e organizações devem seguir as melhores práticas de segurança, especialmente higiene de credenciais, princípio do menor privilégio e Zero Trust.

3 RECOMENDAÇÕES

Faça backup de seus dados

- Se você for infectado por um ransomware, deverá desconectar imediatamente todos os dispositivos infectados de suas redes para evitar que ele se espalhe.

Altere suas credenciais

- Se você descobrir que um vazamento de dados ou um ataque de ransomware comprometeu uma empresa com a qual interagiu, aja imediatamente e altere as senhas de todas as suas contas.

Nunca clique em links inseguros

- Evite clicar em links em mensagens de spam ou em sites desconhecidos.

Evite a divulgação de informações pessoais

- Se você receber uma chamada, mensagem de texto ou e-mail de uma fonte não confiável solicitando informações pessoais, não responda.

Não abra anexos de e-mail suspeitos

- O ransomware também pode entrar em seu dispositivo por meio de anexos de e-mail.

Use software de segurança

- As chances de infecção podem ser significativamente reduzidas usando um software de segurança.

Verifique as vulnerabilidades

- Uma verificação de vulnerabilidades, que pode ser realizada pelo seu software de segurança, pode corrigir isso.

Treinamento de conscientização

- Treine os usuários para detectar ransomware.

4 REFERÊNCIAS

- **Heimdall *by* ISH Tecnologia**
- [Thehackernews]

heimdall
security research
A DIVISION OF ISH