TLP: CLEAR

BOLETIM DE SEGURANÇA

Malware que bloqueia totalmente o sistema Windows continua a se espalhar

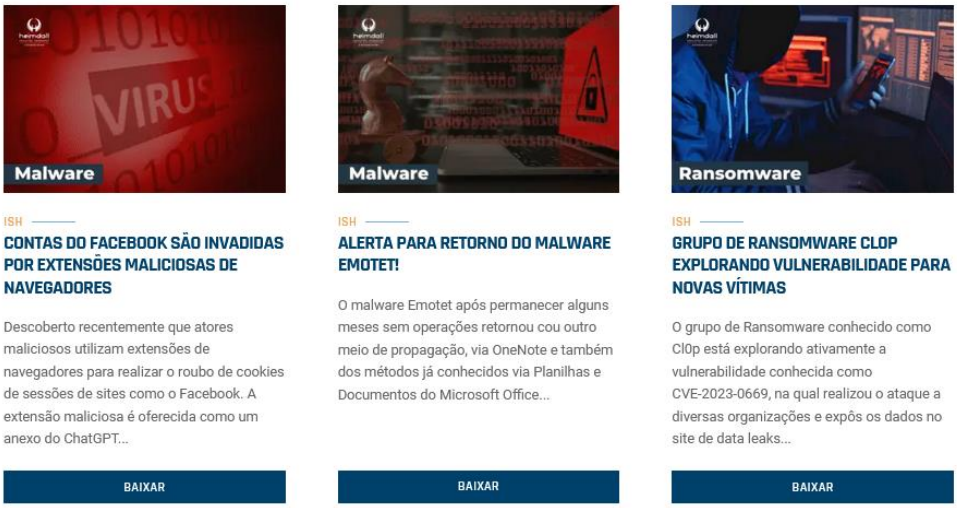
heimdall
security research
A DIVISION OF ISH

Acesse a nossa nova comunidade através do WhatsApp!

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

Um novo malware que impede o acesso completo ao Windows tem sido alvo de diversos relatos nas redes sociais, especialmente no Reddit. O ataque se manifesta logo na inicialização do computador, onde o usuário encontra uma mensagem de "Microsoft Blocked" em vez do nome de usuário, impossibilitando o login.

2 INFORMAÇÕES SOBRE A AMEAÇA

Imagine ter seu computador com Windows completamente bloqueado, sem acesso a nenhum dos seus dados ou programas. Isso é o que está acontecendo com várias vítimas de um malware que continua a se espalhar rapidamente. O bloqueio ocorre sem qualquer aviso prévio e a infecção pode se dar ao clicar em links suspeitos ou baixar programas desconhecidos, mas ainda não se sabe ao certo como o malware se instala.

Esse tipo de infecção maliciosa bloqueia completamente o sistema, removendo as contas de acesso e exigindo, em alguns casos, um resgate para que o controle do PC seja restaurado. O malware, cuja origem ainda não está completamente clara, é disseminado por meio de links suspeitos e downloads não confiáveis. Vítimas estão enfrentando grandes dificuldades para recuperar seus dispositivos, com muitos recorrendo a especialistas em TI.

Ao tentar fazer login, o sistema informa que a senha está incorreta, deixando evidente que o PC foi comprometido. O malware atua removendo a conta de acesso do usuário, impedindo qualquer tentativa de login. Esse tipo de ataque é conhecido como "sequestro digital" do computador, e seus efeitos são graves: além de bloquear o sistema operacional, o malware afeta todos os dados armazenados no dispositivo. Em muitos casos, os criminosos exigem um pagamento para devolver o acesso.

Mesmo que o malware já seja conhecido, a remoção não é simples e exige conhecimentos avançados de TI e o uso de softwares especializados em remoção de pragas virtuais. Muitos usuários de Windows 10 afetados têm relatado dificuldades em solucionar o problema por conta própria.

3 RECOMENDAÇÕES

A principal recomendação para evitar a infecção é reforçar as medidas de precaução ao navegar na internet, mantendo o sistema operacional e o antivírus atualizados, além de realizar backups regulares. Para se proteger, é importante tomar algumas medidas de segurança, como evitar links de origem duvidosa e downloads de programas não confiáveis. Manter o sistema operacional e o antivírus atualizados é essencial, além de realizar backups frequentes dos dados para facilitar a recuperação em caso de infecção.

4 REFERÊNCIAS

- **Heimdall *by* ISH Tecnologia**
- **Microsoft**
- **Hardware**

5 AUTORES

- **Leonardo Oliveira Silva**

heimdall
security research
A DIVISION OF ISH