BOLETIM DE SEGURANÇA

Google adiciona nova camada de proteção no navegador Chrome

heimdall
security research
A DIVISION OF ISH

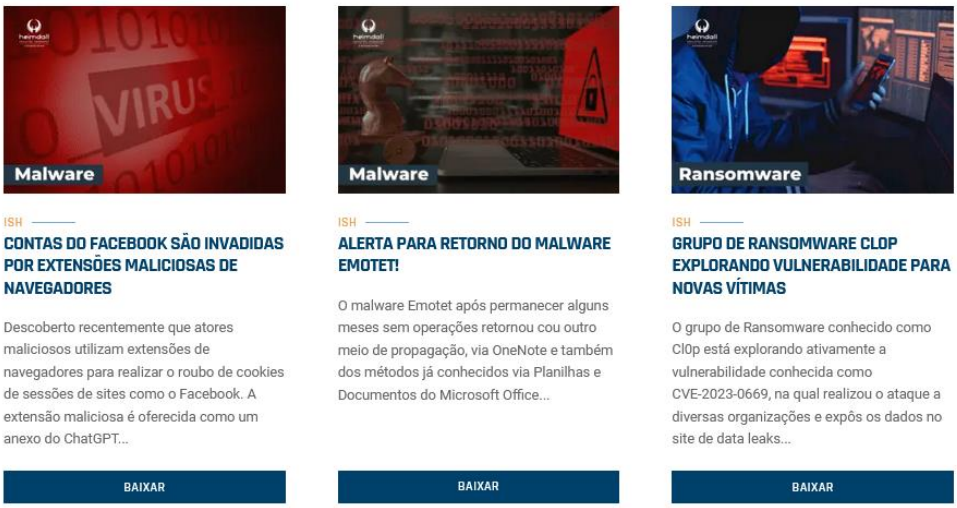
TLP: CLEAR

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 o Google anunciou que está adicionando uma nova camada de proteção ao seu navegador Chrome por meio do que é chamado de *app-bound encryption* (criptografia vinculada ao aplicativo) para evitar ataques de malwares que roubam informações (Infostealers) e melhorar a proteção de cookies em sistemas Windows.

2 INFORMAÇÕES SOBRE A ATUALIZAÇÃO

Atualmente, o Chrome utiliza as técnicas mais avançadas oferecidas por cada sistema operacional para proteger dados sensíveis, como cookies e senhas: serviços de chaveiro no macOS, kwallet ou gnome-libsecret no Linux, e a API de Proteção de Dados (DPAPI) no Windows. No entanto, embora o DPAPI possa proteger dados armazenados contra ataques de inicialização a frio ou de outros usuários em sistemas Windows, ele não é eficaz contra ferramentas maliciosas ou scripts projetados para executar código com as mesmas permissões do usuário conectado, uma vulnerabilidade que é explorada por malwares do tipo infostealer.

Conforme Will Harris, porta voz da equipe de segurança do Chrome, no Chrome 127, estamos introduzindo uma nova proteção no Windows que melhora a DPAPI ao fornecer primitivas de criptografia Application-Bound (App-Bound) . Em vez de permitir que qualquer aplicativo em execução como o usuário conectado acesse esses dados, o Chrome agora pode criptografar dados vinculados à identidade do aplicativo, semelhante a como o Keychain opera no macOS. Migraremos cada tipo de segredo para este novo sistema, começando pelos cookies no Chrome 127. Em versões futuras, pretendemos expandir essa proteção para senhas, dados de pagamento e outros tokens de autenticação persistentes, protegendo ainda mais os usuários contra malware infostealer.

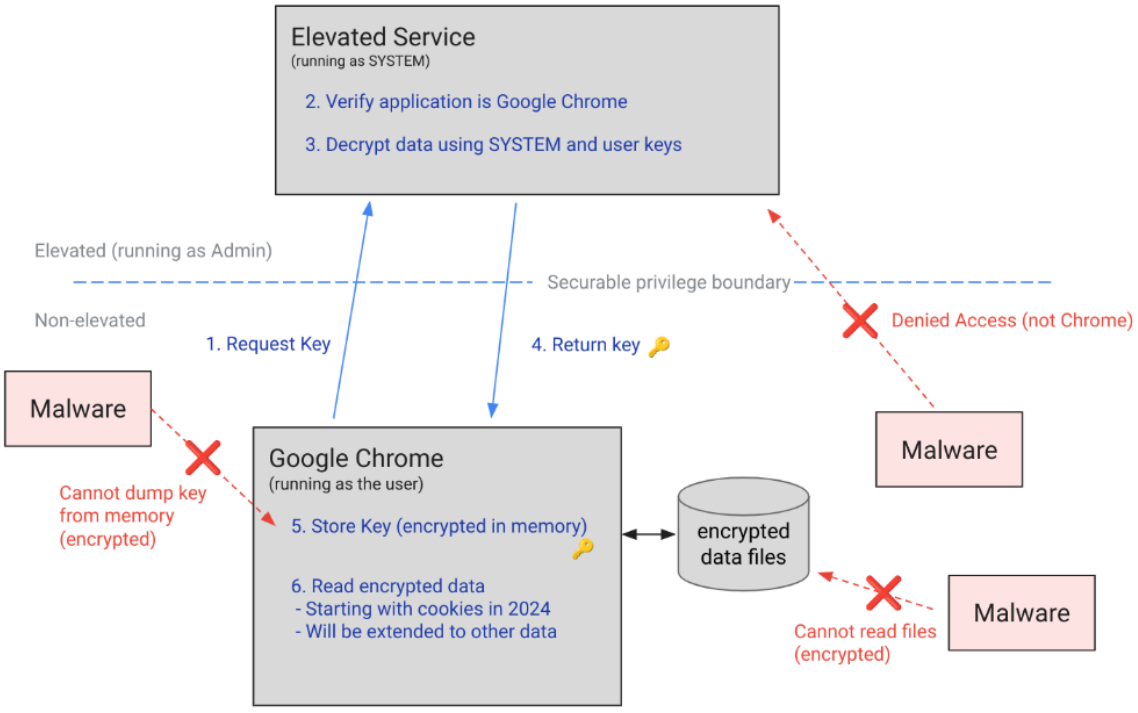


Figura 1 – Funcionamento do App-Bound Encryption.

O App-Bound Encryption necessita de um serviço privilegiado para confirmar a identidade do aplicativo que está fazendo a solicitação. Durante o processo de criptografia, o serviço App-Bound Encryption incorpora a identidade do aplicativo nos dados criptografados e, ao tentar a descriptografia, verifica sua

validade. Caso outro aplicativo no sistema tente descriptografar esses dados, o processo falhará.

Como o serviço App-Bound opera com privilégios de sistema, os invasores precisam mais do que simplesmente convencer um usuário a executar um aplicativo malicioso. O malware agora precisa obter privilégios de sistema ou injetar código no Chrome, ações que o software legítimo não deve realizar. Isso torna as ações do malware mais suspeitas para o software antivírus e mais propensas a serem detectadas. Nossas outras iniciativas recentes, como fornecer logs de eventos para a descriptografia de cookies, trabalham em conjunto com essa proteção, com o objetivo de aumentar o custo e o risco de detecção para invasores que tentam roubar dados do usuário.

Ambientes corporativos

Como o malware pode contornar essa proteção ao executar tarefas com privilégios elevados, ambientes corporativos que não permitem que os usuários executem arquivos baixados como Administrador se beneficiam particularmente dessa medida de segurança. Nesse contexto, o malware não consegue simplesmente solicitar privilégios administrativos e é obrigado a empregar técnicas como a injeção de código, que podem ser mais facilmente detectadas por softwares de segurança de endpoint. A Criptografia Vinculada ao Aplicativo associa fortemente a chave de criptografia à máquina específica, o que impede seu funcionamento adequado em ambientes onde os perfis do Chrome são utilizados em várias máquinas.

A Criptografia Vinculada a Aplicativos (App-Bound Encryption) aumenta significativamente o custo e a dificuldade para invasores que tentam roubar dados, além de tornar suas ações mais detectáveis no sistema. Essa abordagem ajuda os defensores a definir claramente o comportamento aceitável para aplicativos no sistema.

3 REFERÊNCIAS

- **Heimdall *by* ISH Tecnologia**
- **Google**

heimdall
security research
A DIVISION OF ISH