BOLETIM DE SEGURANÇA

Novo ataque iLeakage roubando e-mails e senhas do Apple Safari

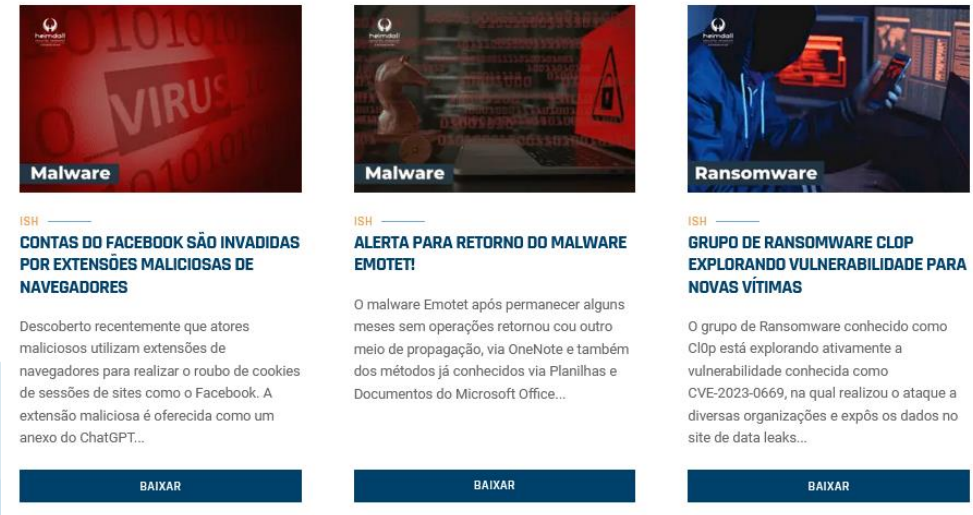
heimdall
security research
A DIVISION OF ISH

Receba alertas e informações sobre segurança cibernética e ameaças rapidamente, por meio do nosso Twitter.

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

Pesquisadores acadêmicos **criaram um ataque especulativo de canal lateral chamado iLeakage**, que funciona em todos os dispositivos Apple recentes e pode extrair informações confidenciais do navegador Safari.

iLeakage é a primeira demonstração de um ataque de execução especulativa contra CPUs Apple Silicon e o navegador Safari. Vale salientar que ele foi usado para recuperar dados com "precisão quase perfeita" do Safar, bem como do Firefox, Tor e Edge no iOS. Em tese, é um **ataque Spectre** sem tempo que ignora as proteções padrão de canal lateral implementadas por todos os fornecedores de navegadores.

2 ROUBANDO SEGREDOS DO SAFARI

O iLeakage foi desenvolvido por uma equipe de acadêmicos da Georgia Tech, da Universidade de Michigan e da Ruhr University Bochum, que examinou a resiliência do canal lateral do Sfari e conseguiu contornar as contramedidas existentes, implementando um método agnóstico e atemporal de arquitetura baseado em condições de corrida.

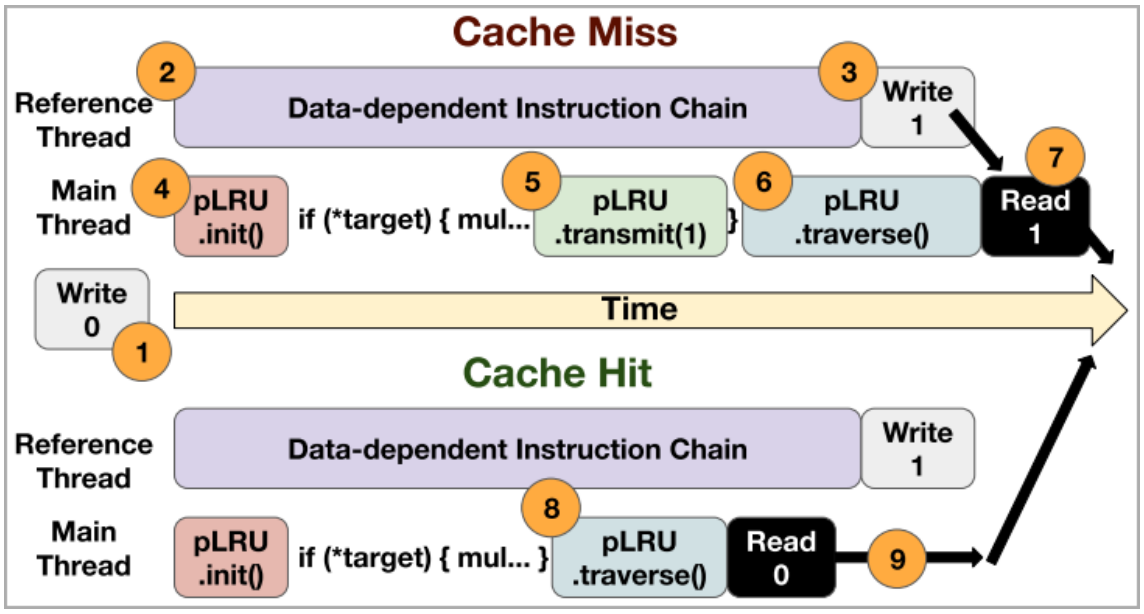


Figura 1 – Diagrama de ataque.

Os pesquisadores se concentram na leitura de informações confidenciais do Sfari e conseguiram roubar dados criando um primitivo que pode ler e vazar especulativamente qualquer ponteiro de 64 bits no espaço de endereço que o navegador da Apple usa para o processo de renderização.

Eles conseguiram esta técnica por meio de bypass em proteções de canal lateral que a Apple implementou em seu navegador, por isso, o temporizador de baixa resolução, endereçamento compactado de 35 bits e envenenamento de valor.

Eles ainda contornaram a política de isolamento de sites no Safari, que separa os sites em diferentes espaços de endereço com base em seu domínio de nível superior efetivo (eTLD) mais um subdomínio. Eles teriam utilizado uma técnica que usa a API JavaScript "window.open" que

permite que uma página do invasor compartilhe o mesmo espaço de endereço que as páginas arbitrárias da vítima.

Ao utilizar a confusão de tipo especulativo para contornar o endereçamento compactado de 35 bits da Apple e as contramedidas de envenenamento de valor, os pesquisadores poderiam vazar dados confidenciais da página de destino, como senhas e e-mails.

A PoC está em JavaScript e WebAssembly, as duas linguagens de programação para entrega de conteúdo dinâmico da Web.

Os pesquisadores divulgaram um vídeo demonstrando como as mensagens do Gmail no Safari rodando em um iPad foram recuperadas usando o ataque iLeakage. De acordo com o ataque, o requisito básico para que o ataque funcione é que o usuário vítima interaja com a página do invasor.

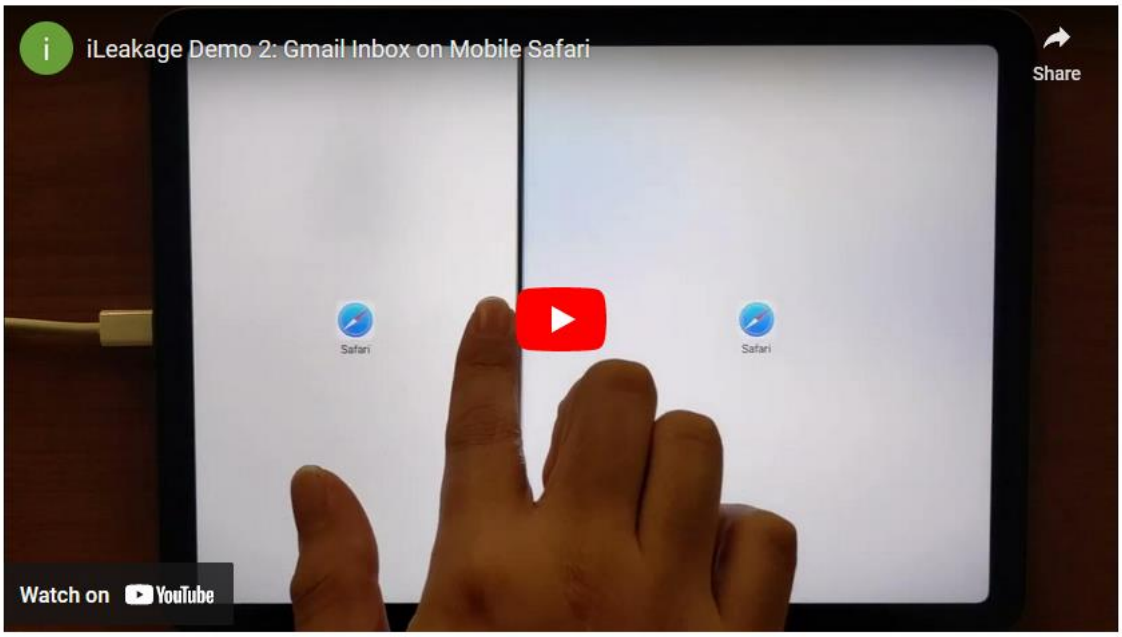


Figura 2 – Vídeo 1 disponível no Youtube..

https://www.youtube.com/watch?v=2uH9slLKTjw

Os pesquisadores usaram o mesmo método para recuperar uma senha de uma conta de teste do Instagram que foi preenchida automaticamente no navegador Safari usando o serviço de gerenciamento de senha LastPass.

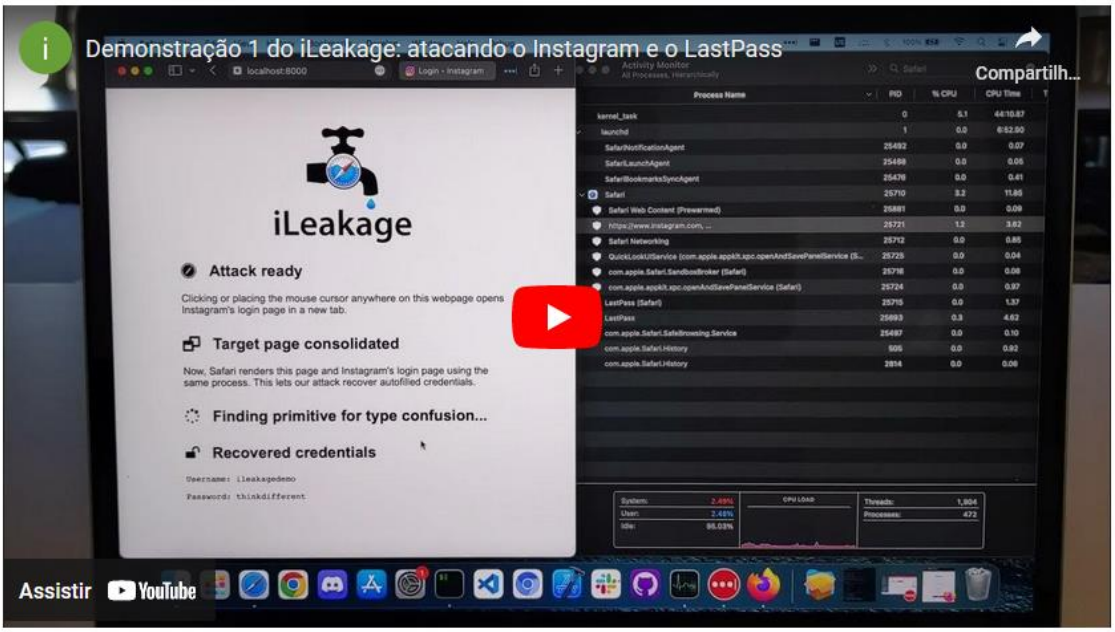


Figura 3 – Vídeo 2 disponível no Youtube.

https://youtu.be/Z2RtpN77H8o

Em outro experimento, os pesquisadores demonstraram como os ataques do iLeakage também funcionam no Chrome para iOS e conseguiram recuperar o histórico de exibição do YouTube. Eles explicaram ainda que a política da Apple força todos os navegadores iOS de terceiros a se sobreporem ao Safari e usarem o mecanismo JavaScript do navegador Apple.

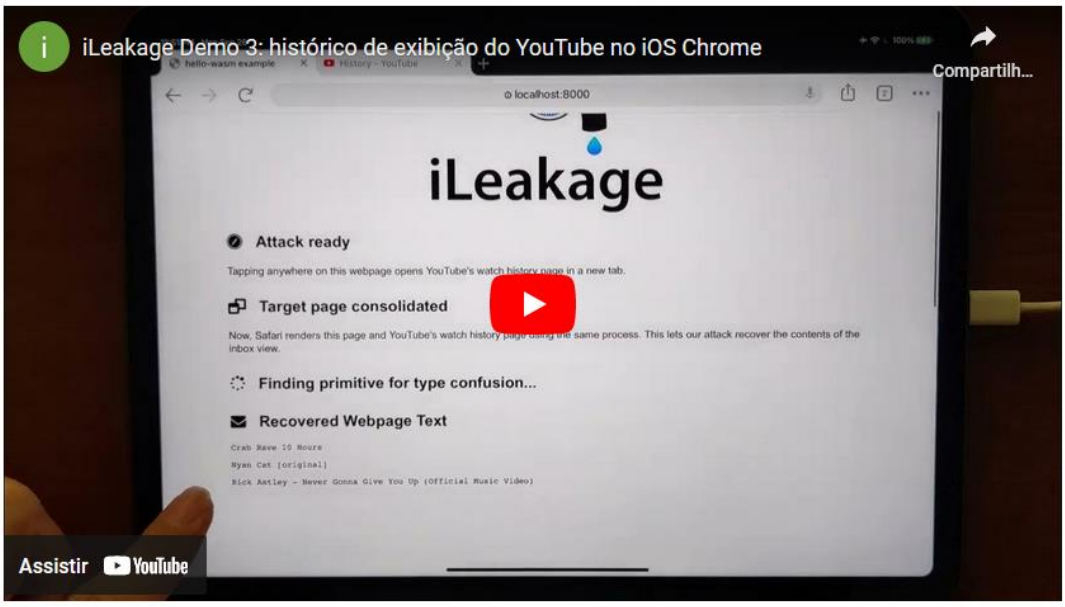


Figura 4 – Vídeo disponível no Youtube.

https://youtu.be/sNdyrCtajP4

O iLeakage depende da exploração da execução especulativa em chips Apple Silicon (M1, M2) onde a execução preditiva da CPU executa tarefas com maior probabilidade de serem necessárias, mas antes de saber se são necessárias ou não.

O mecanismo está presente em todas as CPUs modernas, melhora drasticamente o desempenho; no entanto, falhas de design podem causar vazamentos de dados, como comprovado pelos ataques Meltdown e Spectre divulgados há quase seis anos.

Os detalhes sobre o ataque e os métodos individuais usados para contornar as mitigações da Apple estão disponíveis no artigo técnico publicado pelos pesquisadores.

3 DICAS DE IMPACTO E DEFESA

O iLeakage afeta todos os dispositivos Apple lançados a partir de 2020 que são equipados com processadores ARM das séries A e M da Apple. O ataque é praticamente indetectável, não deixando rastros no sistema da vítima na forma de logs, exceto talvez uma entrada da página web do invasor no cache do navegador. No entanto, os pesquisadores sublinharam que o ataque é difícil de realizar "e requer conhecimentos avançados de ataques de canal lateral baseados em navegador e implementação do Safari".

O iLeakage foi relatado de forma privada à Apple em 12 de setembro de 2022 e a empresa ofereceu as seguintes mitigações para macOS:

1. Abra o Terminal e execute **"defaults write com.apple.Safari IncludeInternalDebugMenu 1"** para ativar o menu de depuração oculto do Safari.
2. Abra o Safari e vá para o menu Debug recém-visível.
3. Selecione **"Recursos internos do WebKit".**
4. Role e ative **"Trocar processos na janela entre sites aberta".**

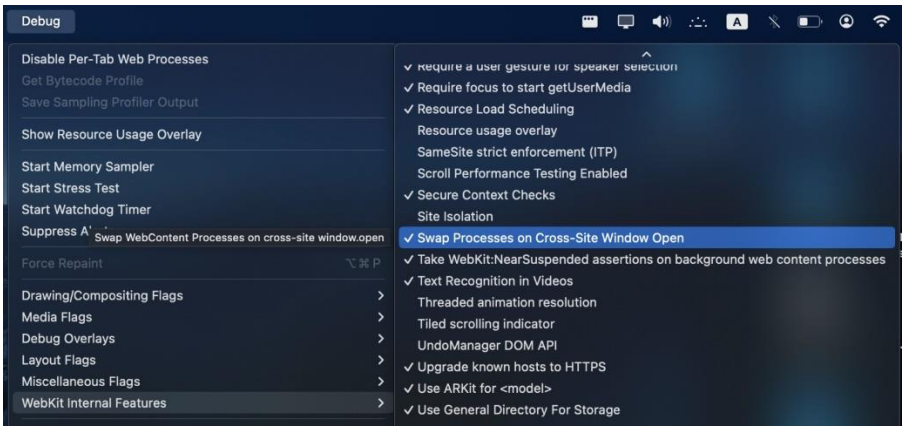


Figura 5 – Painel de menu de configuração de depuração do Safari.

A mitigação vem com o aviso de que pode introduzir alguma instabilidade. Se os usuários quiserem desativá-lo, eles podem fazê-lo no menu de depuração executando no terminal o comando **"defaults write com.apple.Sfari IncludeInternalDebugMenu 0"**.

Além das implicações reais do iLeakage, esta pesquisa destaca os potenciais riscos de execução especulativa em plataformas emergentes baseadas em ARM que não foram examinadas tão intensamente quanto as arquiteturas x86.

4 REFERÊNCIAS

- **Heimdall *by* ISH Tecnologia**
- **Pesquisa sobre o iLeakage – Apple**

heimdall
security research
A DIVISION OF ISH