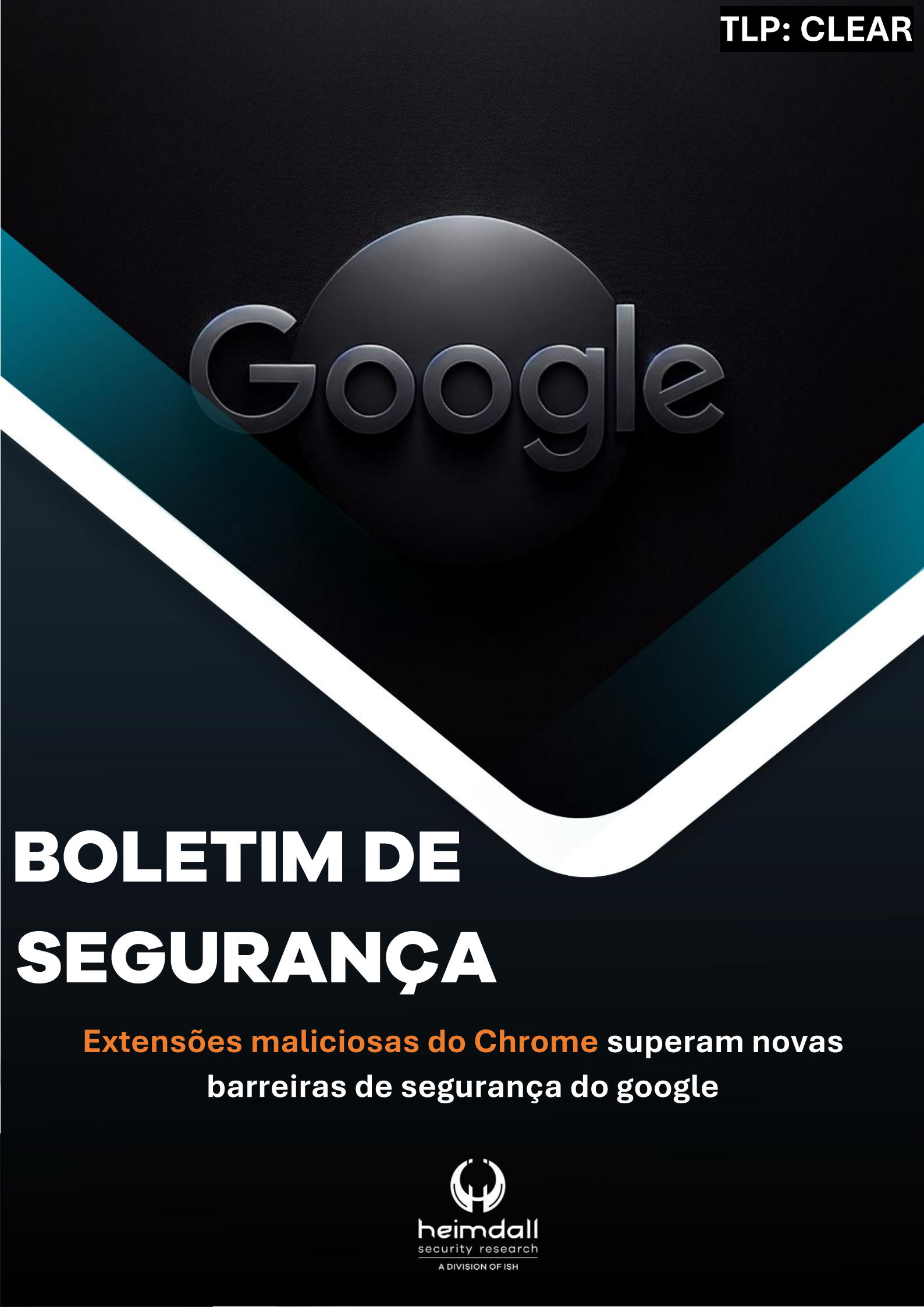
TLP: CLEAR



BOLETIM DE SEGURANÇA

Extensões maliciosas do Chrome superam novas barreiras de segurança do google

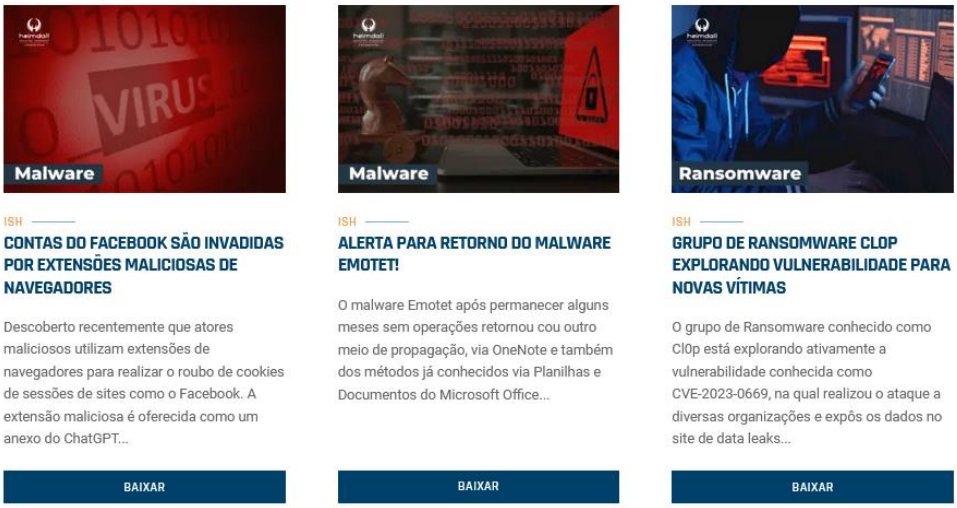
heimdall
security research
A DIVISION OF ISH

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

Pesquisadores de segurança da **SquareX**, revelaram que extensões maliciosas de navegador estão contornando os mais recentes padrões de segurança e privacidade do Google para o Chrome, conhecidos como Manifest V3. Essas extensões estão conseguindo entrar na Chrome Web Store, expondo organizações e indivíduos a riscos significativos. A pesquisa demonstra como criminosos podem introduzir complementos prejudiciais, apesar das atualizações de segurança do Google.

2 INFORMAÇÕES SOBRE A AMEAÇA

Durante a **DefCon 32**, pesquisadores demonstraram que extensões maliciosas podem capturar transmissões de vídeo ao vivo de plataformas como Google Meet e Zoom sem precisar de permissões especiais. Eles também mostraram como invasores podem usar extensões baseadas no **Manifest V3** que é uma plataforma de extensões da google, para redirecionar usuários a páginas de phishing, adicionar colaboradores a repositórios privados no GitHub e roubar cookies, histórico de navegação e outros dados dos usuários com facilidade. O Google lançou o Manifest V3, 2018 para resolver problemas do Manifest V2, que facilitava a criação de extensões maliciosas. Um estudo da Universidade de Stanford revelou que 280 milhões de extensões maliciosas foram instaladas entre julho de 2020 e fevereiro de 2023.

Segundo o Google, o Manifest V3 visa melhorar a privacidade, a segurança e o desempenho das extensões. As melhorias incluem uma política de segurança de conteúdo mais rigorosa, APIs mais seguras, controle de permissão mais detalhado e mudanças nas solicitações de origem cruzada. Algumas atualizações, como a que afeta extensões de bloqueio de conteúdo, geraram controvérsias, com defensores da privacidade alegando que restringem a capacidade de bloquear anúncios e rastreamento. No entanto, o objetivo geral do Manifest V3 é aprimorar a segurança e a privacidade das extensões do Chrome.

Vivek Ramachandran, CEO da SquareX, afirma que o modelo de permissão do Manifest V3 ainda é muito amplo, permitindo que agentes maliciosos explorem permissões mínimas para roubar dados. Um exemplo significativo são as permissões de host, que permitem que uma extensão modifique ou leia qualquer conteúdo da Web nas páginas visitadas. A SquareX demonstrou uma extensão que roubava fluxos do Google Meet, necessitando apenas dessa permissão. Esse tipo de permissão é comum no armazenamento de extensões, sendo essencial para muitas, como verificadores gramaticais. Estima-se que já existam centenas, senão milhares, de extensões maliciosas baseadas no Manifest V3 na Chrome Web Store, e espera-se que esse número aumente à medida que mais extensões migrem para o Manifest V3.

No entanto, a gigante da Internet já admitiu que, com mais de 250.000 extensões na Chrome Web Store, algumas podem representar riscos aos usuários e solicitar permissões que violam políticas empresariais. Como qualquer software, as extensões também podem apresentar riscos, afirmou o Google em um blog após pesquisadores de Stanford divulgarem um artigo sobre extensões arriscadas na Chrome Web Store.

Em atualizações anteriores, como a de abril de 2023, o Google destacou seus esforços para reforçar a segurança das extensões do Chrome. Isso inclui recursos de gerenciamento de extensões que as equipes de segurança podem usar para definir políticas para todas as extensões instaladas e revisar extensões antes da instalação. Os recursos de segurança do Chrome também alertam os administradores quando um usuário tenta instalar uma nova extensão, facilitando o rastreamento e gerenciamento. No ano passado, o Google introduziu duas ferramentas de avaliação de risco, a **CRXcavator** e **Spin.AI Risk Assessment**, que permitem aos administradores corporativos avaliar e pontuar extensões quanto ao risco.

O Google também aponta para sua página de extensões do Chrome (**chrome://extensions/**) como um recurso para verificar se as extensões instaladas representam um risco de segurança; um aviso aparece se o Google detectar extensões suspeitas. Isso inclui navegadores com malware, extensões que violam políticas da Chrome Web Store, extensões não publicadas e aquelas que não são claras sobre suas práticas de privacidade e coleta de dados. O Google estabeleceu um prazo para junho passado para que os desenvolvedores migrassem para o Manifest V3 e começou a desabilitar extensões do Manifest V2 em versões pré-estáveis do Chrome. As organizações empresariais têm até junho de 2025 para migrar para a nova versão. Em 4 de outubro, 60,4% das extensões do Chrome já haviam migrado para o Manifest V3.

3 RECOMENDAÇÕES

Recomenda-se que as empresas auditem extensões instaladas e limitem suas permissões e que as organizações melhorem a visibilidade e controle sobre as extensões no ambiente.

4 REFERÊNCIAS

- **Heimdall *by* ISH Tecnologia**
- Darkreading
- GoogleStats

5 AUTORES

- **Leonardo Oliveira Silva**

heimdall
security research
A DIVISION OF ISH