heimdall

security research

A DIVISION OF ISH

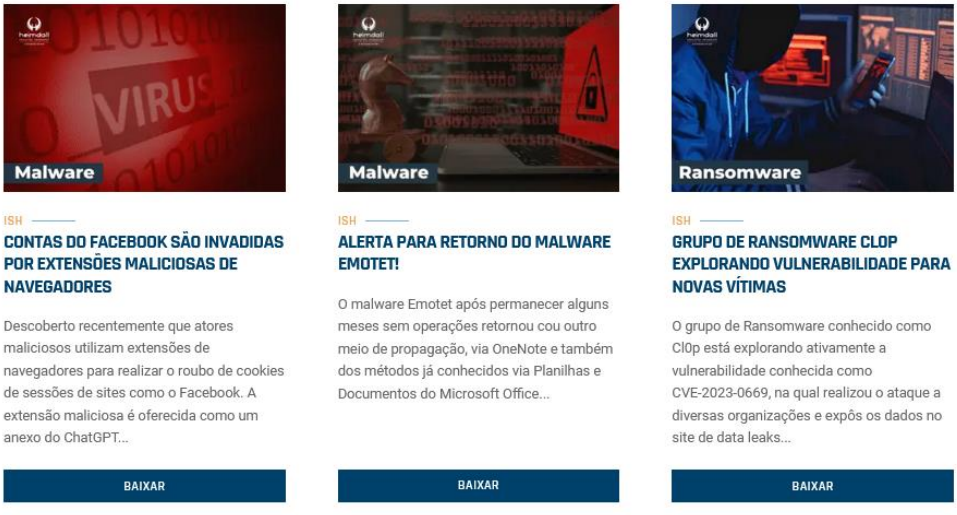
Cibercriminosos podem abusar executáveis do Microsoft Office

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 INTRODUÇÃO

A lista de arquivos LOLBAS (Living-on-the-Land-Binaries and Scripts), ou seja, os binários e scripts legítimos presentes no Windows que podem ser utilizados para fins maliciosos em breve incluirá os principais executáveis para o cliente de e-mail Outlook e o sistema de gerenciamento de banco de dados Access.

Além disso, foi confirmado que o executável principal do aplicativo Microsoft Publisher pode baixar cargas úteis de um servidor remoto.

O projeto LOLBAS, atualmente lista mais de 150 binários, bibliotecas e scripts relacionados ao Windows que podem ajudar os atores maliciosos a executar ou baixar arquivos maliciosos ou ignorar listas de programas aprovados.

O pesquisador Nir Chako, da empresa Pentera, descobriu novos arquivos LOLBAS observando os executáveis no pacote do Microsoft Office.

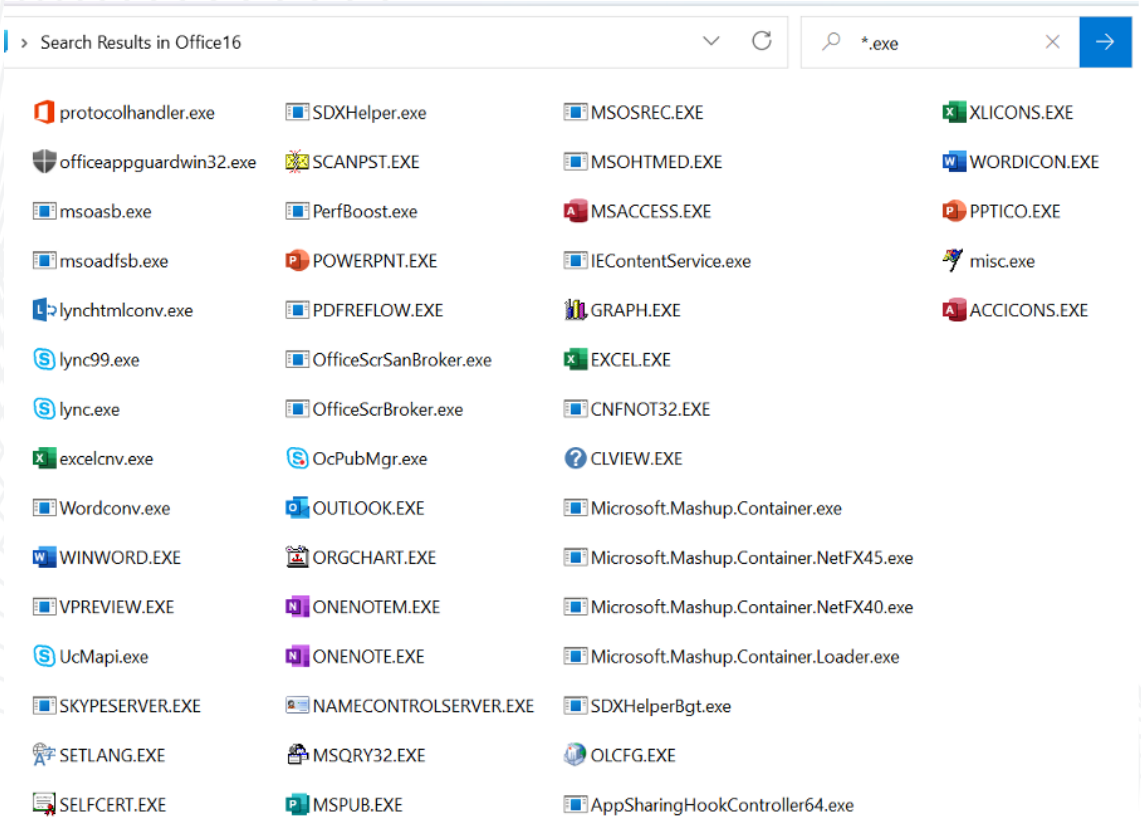


Figura 1 – Arquivos Microsoft Office.

O pesquisador testou todos manualmente e encontrou três **"MsoHtmEd.exe, MSPub.exe e PortocolHandler.exe"** que poderiam ser utilizados como downloaders para arquivos de tericeiros, ajustando-se assim aos critérios do LOLBAS.

Para comprovar os fatos, o pesquisador realizou a execução do MsoHtmEd realizando requisições para um servidor HTTP de teste com uma solicitação GET, indicando a tentativa de realizar o download de um arquivo.

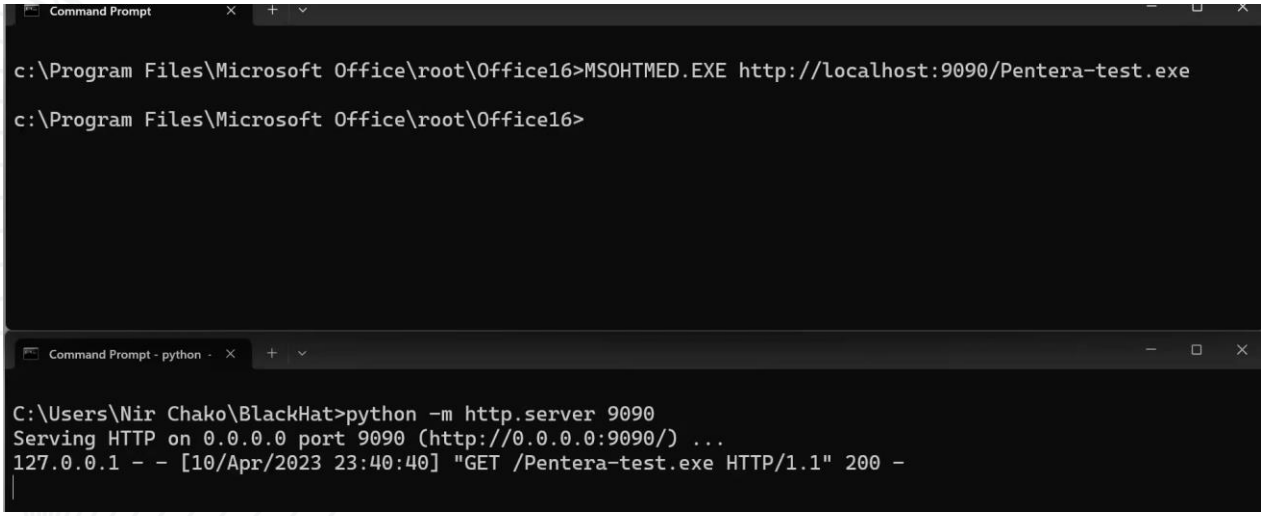


Figura 2 – Caso de uso com a ferramenta MSOHTMED.exe.

Além dos mencionados, o pesquisador descobriu mais 11 novos arquivos com funcionalidades de download e execução que atnedem aos princípios do projeto LOLBAS.

LOLBAS	Functionality	LOLBAS projectStatus
ProtocolHandler	Download	Aceitaram
MSPub	Download	Aceitaram
MsoHtmEd	Download, Execute	Aceitaram
PresentationHost	Download	Aceitaram
ConfigSecurityPolicy	Download	Aceitaram
InstallUtil	Download	Aceitaram
MSHta	Download	Aceitaram
Outlook	Download	Solicitação de pull
MSAccess	Download	Solicitação de pull

Sftp	Execute	Solicitação de pull
Scp	Execute	Solicitação de pull

Tabela 1 – 11 novos arquivos com funcionalidades de download e execução.

Destacou-se o MSPub.exe, Outlook.exe e MSAccess.exe, que um invasor ou pentest pode utilizar para baixar arquivos de terceiros.

Embora o MSPub tenha confirmado que pode baixar cargas arbitrárias de um servidor remoto, os outros dois ainda não foram adicionados a lista do LOLBAS.

2 NOVAS FONTES LOLBAS

Além dos binários da Microsoft, o pesquisador também encontrou arquivos de outros desenvolvedores que atendem aos critérios LOLBAS, sendo um exemplo o popular pacote PyCharm para desenrolvimento Python.

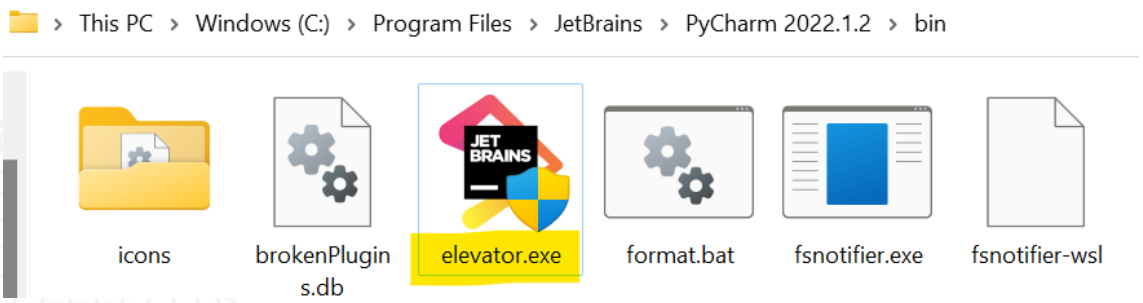


Figura 3 – Executável assinado na pasta de instalação do PyCharm.

A pasta de instalação do PyCharm contém o arquivo "Elevator.exe" que pode executar arquivos binários com privilégios elevados. Além disso, o arquivo WinProcessListHelper.exe poderá servir para fins de reconhecimento, enumerando todos os processos em execução no sistema.

Portanto, podemos concluir que entender e conhecer as ameaças LOLBAS é importante, visto que poderão ser monitoradas para verificar a sua utilização para fins ilícitos ou ações maliciosas por um ator malicioso.

3 REFERÊNCIAS

- **Heimdall *by* ISH Tecnologia**
- **Projeto LOLBAS**
- **Pentera – LOLBAS, novas ferramentas**

heimdall
security research

A DIVISION OF ISH