

Segurança da Informação



Competências:

- Implementar práticas e condutas de segurança da informação no ambiente de TI.

Bases Tecnológicas, científicas e instrumentais (conteúdos):

- Tipos de Malware;

Situação de Aprendizagem:

- Apresentação dos principais tipos de malwares.

Malware

» Malware: Programa criado com objetivos prejudiciais, comprometendo, assim a segurança dos sistemas de informação

– Dos mais variados tipos...

- Vírus
- Worm (verme)
- Bomba lógica
- Cavalo de tróia (Trojan)
- Backdoor
- Exploit
- Downloaders
- Auto-rooter
- Kit (gerador de vírus)
- Programas de spam
- Flooders
- Spyware (keyloggers e screenloggers)
- Adware
- Rootkit
- Zumbi
- Port Scanner
- Sniffer
- Ransomware



Malware



» Vírus

- Um programa (ou parte de um programa) que:
 - Necessita de um hospedeiro para existir (um vírus se “anexa” ao conteúdo de um arquivo para viver)
 - Consegue se replicar (copiar) sozinho para outros arquivos (hospedeiros)
- Quando um arquivo for infectado por um vírus de computador...
 - ... é copiado para o disco rígido do computador do usuário, este micro não é infectado.
 - ...é aberto no computador do usuário, este vírus torna-se ativo naquele computador e fará o que foi programado para fazer.

Malware



» Worm

- Programa que propaga cópias de si mesmo a outros computadores
 - Um programa que usa a estrutura das redes para se copiar de micro para micro, degradando a velocidade da comunicação nesta estrutura
- Não precisa de hospedeiro, pois ele próprio é o arquivo que se copia, nem precisa ser acionado pelo usuário, pois se utiliza de falhas nos protocolos e serviços da rede para se espalhar
- O processo de propagação e infecção dos worms ocorre da seguinte maneira:
 - a) Identificação dos computadores alvos
 - b) Envio das cópias
 - c) Ativação das cópias
 - d) Reinício do processo (Infecção de novas máquinas)

Fonte: Cartilha Cert.br

Malware



» Bomba lógica

- Dispara uma ação quando ocorre uma determinada condição

» Cavalo de Tróia (*Trojan Horse*)

- Programa que contém funcionalidade adicional inesperada
 - Programa que se apresenta como algo inofensivo (um jogo, um cartão de Natal, etc.) mas, esconde objetivos maliciosos, como apagar dados, roubar informações e, mais comumente, abrir portas de comunicação para que se possa invadir o computador que o executou

» Backdoor (trapdoor)

- Brecha intencional, não documentada, em programa legítimo, que permite o acesso ao sistema por parte de seus criadores ou mantenedores
- Modificação de um programa que permite o acesso não autorizado à alguma funcionalidade

Malware



» Exploit

- Um programa construído para tirar vantagem de alguma falha, ou vulnerabilidade, conhecida em um sistema de informações
- Um Exploit é construído por um hacker (ou cracker) para permitir que usuários menos “conhecedores” possam invadir ou prejudicar o funcionamento de computadores. É um programa para “script kiddies” (amadores)

» Downloaders

- Programa que instala outros itens em uma máquina sob ataque. Normalmente, um downloader é enviado por email

» Auto-rooter

- Ferramentas utilizadas para invasão de novas máquinas remotamente
- Permite que um hacker obtenha acesso remoto ao computador afetado, para executar as seguintes ações, entre outras: formatar a unidade de disco rígido, adicionar novos usuários, etc.

Malware



O CVE, sigla inglesa para vulnerabilidades e exposições comuns, é uma lista pública de falhas de segurança. Quando alguém se refere a um CVE, isso significa uma falha de segurança atribuída a um número de ID correspondente.

Malware

<https://www.cve.org/>



CVE [About](#) [Partner Information](#) [Program Organization](#) [Downloads](#) [Resources & Support](#) [Report Request](#)

Enter CVE ID (CVE-YYYY-NNNN)

Find CVE Records by keyword on [cve.mitre.org](#)

Welcome to the new CVE Beta website! CVE List keyword search & downloads will be temporarily hosted on the old [cve.mitre.org](#) website until we complete the transition. Please use the [CVE Program web forms](#) for any comments or concerns.

CVE® Program Mission

Identify, define, and catalog publicly disclosed cybersecurity vulnerabilities.

Currently, there are **182,271** CVE Records accessible via [Download](#) or [Search](#)

The CVE Program partners with community members worldwide to grow CVE content and expand its usage. Click below to learn more about the role of [CVE Numbering Authorities \(CNAs\)](#) and [Roots](#).

[Learn More](#)

[Become a Partner](#)



News

- CVE List Download Formats Are Changing
- Creston Electronics, Inc. Added as CVE Numbering Authority (CNA)
- OpenHarmony Added as CVE Numbering Authority (CNA)

Malware



<https://www.cve.org/>

O CVE é administrado pela MITRE Corporation e financiado pela Agência de Segurança Cibernética e de Infraestrutura, que integra o Departamento de Segurança Interna dos EUA.

As entradas do CVE são curtas. Não incluem dados técnicos, nem informações sobre riscos, impactos ou correções. Essas informações aparecem em outros bancos de dados, como o National Vulnerability Database (NVD) dos Estados Unidos, o Vulnerability Notes Database do CERT/CC e várias listas criadas por fornecedores e outras organizações. Nesses vários sistemas, os IDs CVE oferecem aos usuários uma forma confiável de diferenciar as falhas de segurança.

Malware



Como funciona o sistema CVE?

O CVE é administrado pela MITRE Corporation e financiado pela Agência de Segurança Cibernética e de Infraestrutura, que integra o Departamento de Segurança Interna dos EUA.

As entradas do CVE são curtas. Não incluem dados técnicos, nem informações sobre riscos, impactos ou correções. Essas informações aparecem em outros bancos de dados, como o National Vulnerability Database (NVD) dos Estados Unidos, o Vulnerability Notes Database do CERT/CC e várias listas criadas por fornecedores e outras organizações. Nesses vários sistemas, os IDs CVE oferecem aos usuários uma forma confiável de diferenciar as falhas de segurança.

Malware



NIST | NATIONAL INSTITUTE OF
STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

≡ NVD MENU

[Information Technology Laboratory](#)

NATIONAL VULNERABILITY DATABASE

NVD

General

Vulnerabilities

Vulnerability Metrics

Products

Developers

Contact NVD

Other Sites

Search

**CISA KNOWN EXPLOITED
VULNERABILITIES
CATALOG**

Now available
in the NVD



New Parameters

API →
2022

Changes to Data Feeds and API

CVSS

Retirement of CVSS v2

The NVD is the U.S. government repository of standards based vulnerability management data represented using the Security Content Automation Protocol (SCAP). This data enables automation of vulnerability management, security measurement, and compliance. The NVD includes databases of security checklist references, security-related software flaws, misconfigurations, product names, and impact metrics.

For information on how to cite the NVD, including the database's Digital Object Identifier (DOI), please consult NIST's Public Data Repository.








Malware



» Exploit

- Um programa construído para tirar vantagem de alguma falha, ou vulnerabilidade, conhecida em um sistema de informações
- Um Exploit é construído por um hacker (ou cracker) para permitir que usuários menos “conhecedores” possam invadir ou prejudicar o funcionamento de computadores. É um programa para “script kiddies” (amadores)

<https://github.com/Hacker5preme/Exploits>

 Hacker5preme Update README.md		2d84e88 on 21 Feb	 208 commits
	CVE-2014-8722-Exploit	GetSimple CMS 3.3.4 - Information Disclosure	15 months ago
	CVE-2017-14535-Exploit	Trixbox 2.8.0.4 - 'lang' Remote Code Execution (Unauthenticated)	15 months ago
	CVE-2017-14537-Exploit	Trixbox 2.8.0.4 - 'lang' Path Traversal	15 months ago
	CVE-2017-9380-Exploit	OpenEMR 5.0.0 - Remote Code Execution (Authenticated)	14 months ago
	CVE-2018-15139-Exploit	OpenEMR 5.0.1.3 - 'manage_site_files' Remote Code Execution (Auth_...	14 months ago

Malware



CVE-2014-8722-Exploit

Exploit Title: GetSimple CMS 3.3.4 - Information Disclosure

CVE description:

GetSimple CMS 3.3.4 allows remote attackers to obtain sensitive information via direct requests.

- <https://nvd.nist.gov/vuln/detail/CVE-2014-8722>

ExploitDB:

- <https://www.exploit-db.com/exploits/49928>

Exploit Description:

- Vendor Homepage: <http://get-simple.info>
- Software Link: <https://github.com/GetSimpleCMS/GetSimpleCMS/archive/refs/tags/v3.3.4.zip>
- Version: 3.3.4
- Tested on Ubuntu 20.04

Usage:

```
python3 exploit.py Target_IP Target_Port CMS_path
```


Malware



```
hacker5preme@hacker5preme-TUXEDO Book E14 Gen 13: ~/Exploitdev/CVE-2014-8722
hacker5preme:~/Exploitdev/CVE-2014-8722$ python3 exploit.py 127.0.0.1 80 /GetSimpleCMS-3.3.4/
Do you know the username? Y/N: Y
Please enter the username: root
Informations:
[*] API Key: 18eb79bf154cb8c0f263d5
[*] Hashed Password: dc76e9f0c0006e8f919e0c515c66dbba3982f785
[*] Email: root@proto.de
hacker5preme:~/Exploitdev/CVE-2014-8722$ python3 exploit.py 127.0.0.1 80 /GetSimpleCMS-3.3.4/
Do you know the username? Y/N: N
No problem, you will still get the API key
Informations:
[*] API Key: 18eb79bf154cb8c0f263d5
hacker5preme:~/Exploitdev/CVE-2014-8722$
```

Malware



- » Kit (gerador de vírus)
 - Conjunto de ferramentas para gerar novos vírus automaticamente
- » Programas de spam
 - Envio em massa de mensagens de e-mail não autorizadas pelos destinatários



Malware



» Flooders

- Usados para atacar sistemas de computador em rede com um grande volume de tráfego para executar um ataque de negação de serviço

» Spyware

- Um programa que monitora e registra os “hábitos” de navegação e acesso à Internet do micro infectado
 - Um spyware para conter keyloggers (capturadores de teclado) e screenloggers (capturadores de tela) para “copiar” o que o usuário está fazendo no computador.

» Adware

- um programa que fica “fazendo anúncios de propaganda” no micro infectado
 - Pode ser um programa lícito, acompanhando outros programas como programas mensageiros instantâneos ou programas de compartilhamento de arquivos
 - Fica “abrindo páginas” ou mostrando imagens e links de cassinos, lojas, etc.

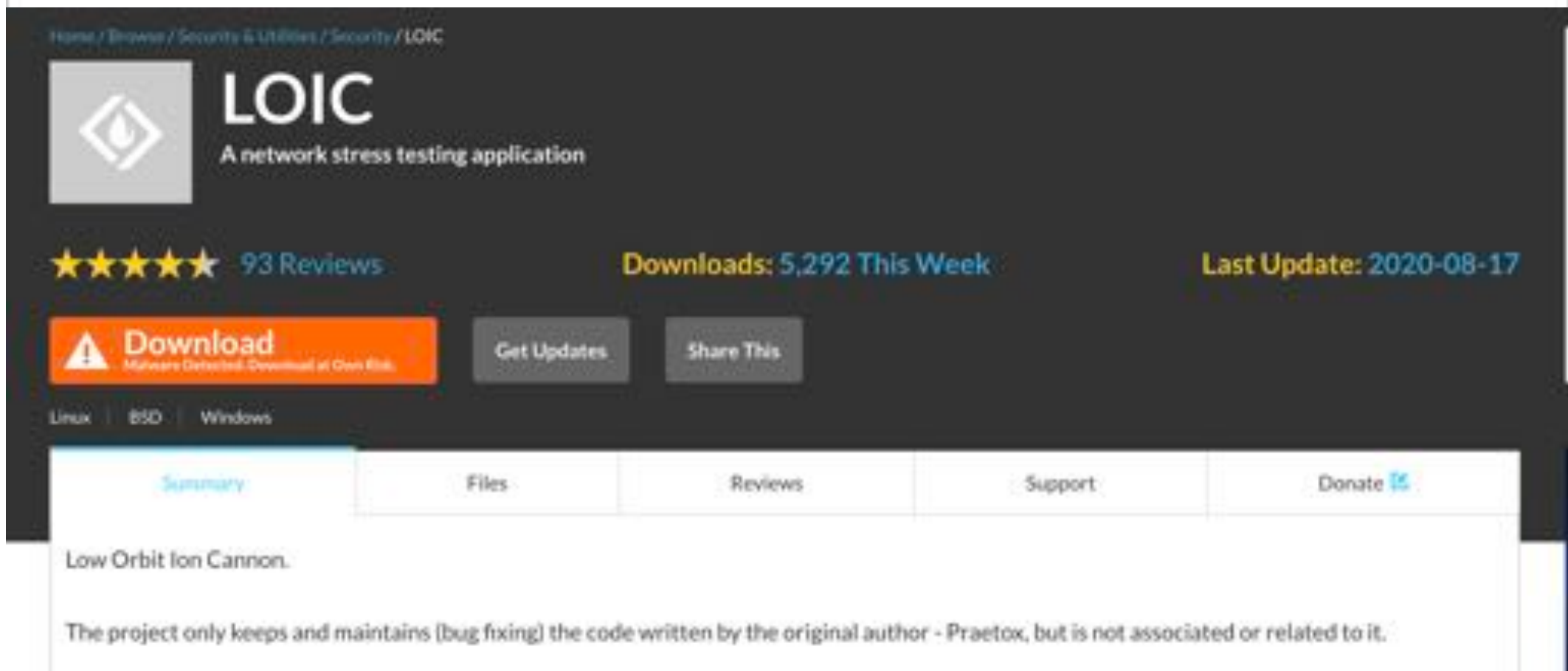
Malware



» Flooders

- Usados para atacar sistemas de computador em rede com um grande volume de tráfego para executar um ataque de negação de serviço

<https://sourceforge.net/projects/loic/>



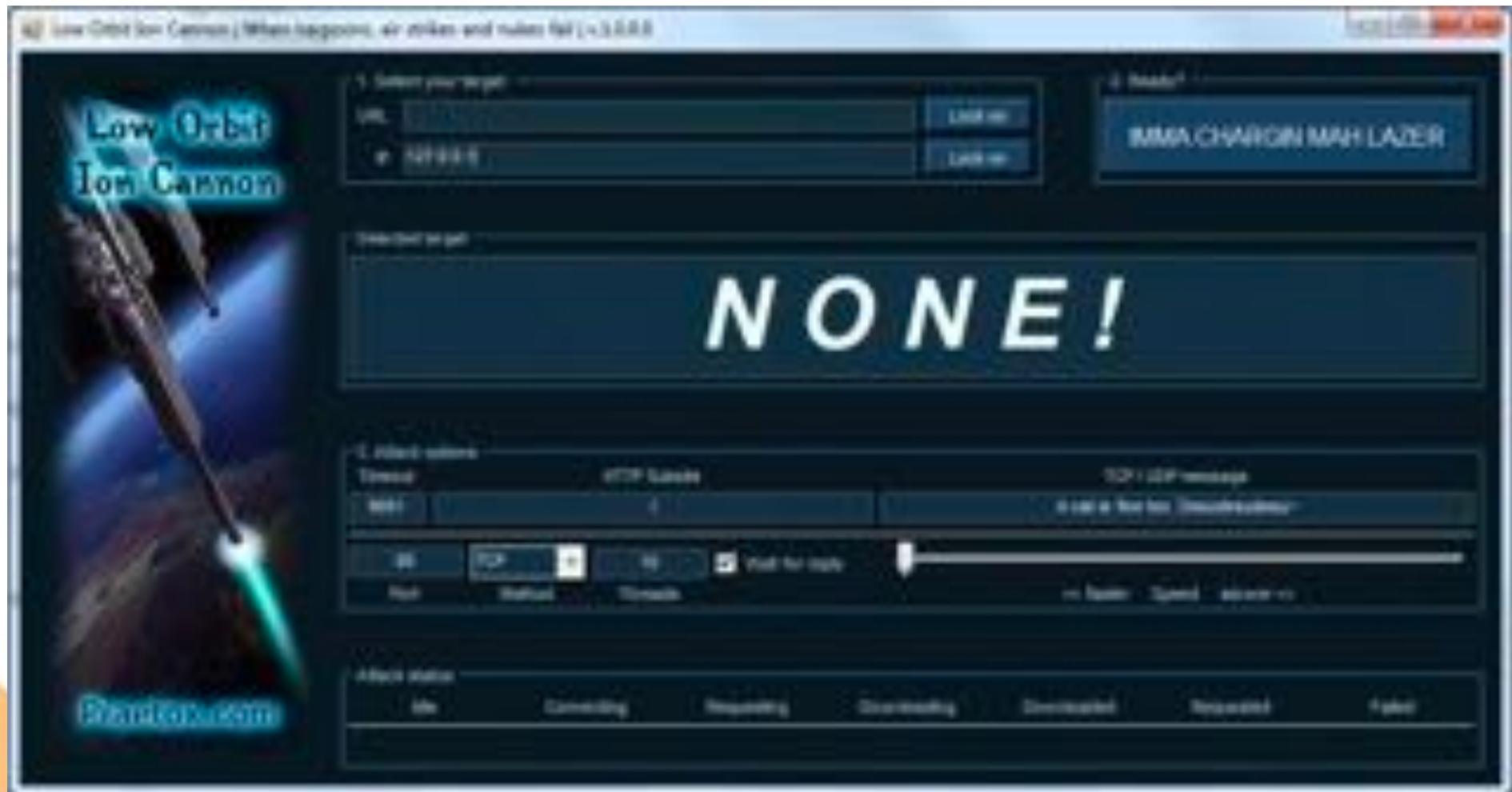
The screenshot shows the SourceForge project page for LOIC (Low Orbit Ion Cannon). The page has a dark theme. At the top, the breadcrumb navigation reads "Home / Browse / Security & Utilities / Security / LOIC". The main header features the LOIC logo (a diamond with a flame) and the text "LOIC A network stress testing application". Below this, there are three statistics: "★★★★★ 93 Reviews", "Downloads: 5,292 This Week", and "Last Update: 2020-08-17". A prominent orange "Download" button is present, with a warning icon and the text "Malware Detected! Download at Own Risk." To the right of the download button are "Get Updates" and "Share This" buttons. Below these buttons, there are tabs for "Linux", "BSD", and "Windows". A horizontal menu bar contains links for "Summary", "Files", "Reviews", "Support", and "Donate". The "Summary" tab is currently selected. The content area under the "Summary" tab shows the text "Low Orbit Ion Cannon." and a disclaimer: "The project only keeps and maintains [bug fixing] the code written by the original author - Praetox, but is not associated or related to it."

Malware



» Flooders

- Usados para atacar sistemas de computador em rede com um grande volume de tráfego para executar um ataque de negação de serviço



Malware



» Rootkit

- é um conjunto de programas e técnicas que permite esconder e assegurar a presença de um invasor ou de outro código malicioso em um computador comprometido.
- O conjunto de programas e técnicas fornecido pelos rootkits pode ser usado para:
 - remover evidências em arquivos de logs;
 - instalar outros códigos maliciosos, como backdoors, para assegurar o acesso futuro ao computador infectado;
 - esconder atividades e informações, como arquivos, diretórios, processos, chaves de registro, conexões de rede, etc;
 - mapear potenciais vulnerabilidades em outros computadores, por meio de varreduras na rede;
 - capturar informações da rede onde o computador comprometido está localizado, pela interceptação de tráfego.

Malware



» Zumbi

- Programa ativado em uma máquina infectada, que é preparado para desferir ataques a outras máquinas

» Port Scanner

- Um programa que vasculha um computador alvo à procura de portas (serviços) abertas para que, através delas, se possa perpetrar uma invasão àquele micro
 - Um port scanner, na verdade, envia sucessivos pacotes a várias portas diferentes, esperando receber um pacote de resposta por uma delas

Malware



» Port Scanner

- Um programa que vasculha um computador alvo à procura de portas (serviços) abertas para que, através delas, se possa perpetrar uma invasão àquele micro
 - Um port scanner, na verdade, envia sucessivos pacotes a várias portas diferentes, esperando receber um pacote de resposta por uma delas

```
# echo-server.py
```

```
import socket
```

```
HOST = "127.0.0.1" # Standard loopback interface address (localhost)  
PORT = 65432 # Port to listen on (non-privileged ports are > 1023)
```

```
with socket.socket(socket.AF_INET, socket.SOCK_STREAM) as s:  
    s.bind((HOST, PORT))  
    s.listen()  
    conn, addr = s.accept()  
    with conn:  
        print(f"Connected by {addr}")  
        while True:  
            data = conn.recv(1024)  
            if not data:  
                break  
            conn.sendall(data)
```

Malware



» Port Scanner

- Um programa que vasculha um computador alvo à procura de portas (serviços) abertas para que, através delas, se possa perpetrar uma invasão àquele micro
 - Um port scanner, na verdade, envia sucessivos pacotes a várias portas diferentes, esperando receber um pacote de resposta por uma delas

```
# echo-client.py
```

```
import socket
```

```
HOST = "127.0.0.1" # The server's hostname or IP address
```

```
PORT = 65432 # The port used by the server
```

```
with socket.socket(socket.AF_INET, socket.SOCK_STREAM) as s:
```

```
    s.connect((HOST, PORT))
```

```
    s.sendall(b"Hello, world")
```

```
    data = s.recv(1024)
```

```
print(f"Received {data!r}")
```


Malware



» Sniffer

- Um programa que é instalado na máquina do atacante e serve para capturar os quadros da rede que chegam àquela máquina, mesmo os que não estão oficialmente direcionados a ela
- A placa de rede passa a operar em “modo promíscuo”, não rejeitando nenhum quadro que chegou

Malware



» *Ransomware*

- é um tipo de código malicioso que torna inacessíveis os dados armazenados em um equipamento, geralmente usando criptografia, e que exige pagamento de resgate (*ransom*) para restabelecer o acesso ao usuário.
- O pagamento do resgate geralmente é feito, normalmente, via bitcoins.
- Existem dois tipos de ransomware:
 - **Ransomware Locker**: impede que você acesse o equipamento infectado.
 - **Ransomware Crypto**: impede que você acesse aos dados armazenados no equipamento infectado, geralmente usando criptografia.



Malware



[python-file-encryption](#)

Este é um script educacional escrito em Python para demonstrar como criptografar e descriptografar arquivos em um diretório, agindo como ransomware.

O script `locker.py` executa duas operações apenas no diretório de trabalho atual (não recorre a subdiretórios):

1. criptografa o conteúdo de cada arquivo
2. adiciona uma segunda extensão de arquivo, `.encrypted`.












O script `unlocker.py` restaura os arquivos para seu formato não criptografado.



Malware



[python-file-encryption](#)

 raresteak Update README.md	02cb280 on 7 Jun	🕒 13 commits
 LICENSE	Initial commit	3 months ago
 README.md	Update README.md	2 months ago
 document1.odt	Initial commit	3 months ago
 document2.docx	Initial commit	3 months ago
 file1.txt	Initial commit	3 months ago
 file2.txt	Initial commit	3 months ago
 locker.py	Update locker.py	3 months ago
 spreadsheet1.ods	Initial commit	3 months ago
 spreadsheet2.xlsx	Initial commit	3 months ago
 unlocker.py	Fixed typo	3 months ago



Malware



[python-file-encryption](#)

```
git clone https://github.com/raresteak/python-file-encryption.git
```



Malware



[python-file-encryption](#)

locker.py

```
Encrypting: file2.txt
Encrypted: file2.txt.encrypted
Encrypting: file1.txt
Encrypted: file1.txt.encrypted
Encrypting: LICENSE
Encrypted: LICENSE.encrypted
Encrypting: document2.docx
Encrypted: document2.docx.encrypted
Encrypting: spreadsheet2.xlsx
Encrypted: spreadsheet2.xlsx.encrypted
Encrypting: README.md
Encrypted: README.md.encrypted
Encrypting: spreadsheet1.ods
Encrypted: spreadsheet1.ods.encrypted
Encrypting: document1.odt
Encrypted: document1.odt.encrypted
Your files are encrypted, have a nice day.
```



Malware



[python-file-encryption](#)

locker.py

```
Encrypting: file2.txt  
Encrypted: file2.txt.encrypted  
Encrypting: file1.txt  
Encrypted: file1.txt.encrypted  
Encrypting: LICENSE  
Encrypted: LICENSE.encrypted  
Encrypting: document2.docx  
Encrypted: document2.docx.encrypted  
Encrypting: spreadsheet2.xlsx  
Encrypted: spreadsheet2.xlsx.encrypted  
Encrypting: README.md  
Encrypted: README.md.encrypted  
Encrypting: spreadsheet1.ods  
Encrypted: spreadsheet1.ods.encrypted  
Encrypting: document1.odt  
Encrypted: document1.odt.encrypted  
Your files are encrypted, have a nice day.
```





Malware



[python-file-encryption](#)

unLocker.py

```
Encrypting: file2.txt
Encrypted: file2.txt.encrypted
Encrypting: file1.txt
Encrypted: file1.txt.encrypted
Encrypting: LICENSE
Encrypted: LICENSE.encrypted
Encrypting: document2.docx
Encrypted: document2.docx.encrypted
Encrypting: spreadsheet2.xlsx
Encrypted: spreadsheet2.xlsx.encrypted
Encrypting: README.md
Encrypted: README.md.encrypted
Encrypting: spreadsheet1.ods
Encrypted: spreadsheet1.ods.encrypted
Encrypting: document1.odt
Encrypted: document1.odt.encrypted
Your files are encrypted, have a nice day.
```

```
Decrypting: spreadsheet1.ods.encrypted
Decrypted: spreadsheet1.ods
Decrypting: file2.txt.encrypted
Decrypted: file2.txt
Decrypting: document2.docx.encrypted
Decrypted: document2.docx
Decrypting: spreadsheet2.xlsx.encrypted
Decrypted: spreadsheet2.xlsx
Decrypting: file1.txt.encrypted
Decrypted: file1.txt
Decrypting: LICENSE.encrypted
Decrypted: LICENSE
Decrypting: document1.odt.encrypted
Decrypted: document1.odt
Decrypting: README.md.encrypted
Decrypted: README.md
Your files are decrypted, have a nice day.
```