

# Rise of the Vermilion

## Cross-Platform Cobalt Strike Beacon Targeting Linux and Windows

Ryan Robinson

Avigayil Mechtinger



# Who Are We

Avigayil Mechtinger



Product Manager | Intezer

 @AbbyMCH

Rvan Robinson



Security Researcher | Intezer

 @MhicRoibin

# Agenda

- Cobalt Strike
- Linux Malware Threat Landscape
- Vermilion Strike
  - Background
  - Technical analysis
- Discussion
- Wrap Up

# What is Cobalt Strike?



The image shows a screenshot of the Cobalt Strike website. At the top left is the logo "cobaltstrike by HelpSystems". To the right of the logo is a "BUY NOW" button. Further right is a navigation menu with links for "Download", "Community Kit", "Core Impact", "Contact Us", "FEATURES", "SCREENSHOTS", "TRAINING", "SUPPORT", "BLOG", and a search icon. The main content area features the headline "Software for Adversary Simulations and Red Team Operations". Below the headline are two buttons: "DOWNLOAD" and "BUY NOW". To the left of the text is a blue shield icon with a white padlock. To the right is a 3D illustration of a character in a black and blue tactical suit with orange visor, pointing at a large, glowing blue digital interface. Below the shield icon is a paragraph of text: "Adversary Simulations and Red Team Operations are security assessments that replicate the tactics and techniques of an advanced adversary in a network. While penetration tests focus on unpatched vulnerabilities and misconfigurations, these assessments benefit security operations and incident response."

**cobaltstrike**  
by HelpSystems

Download Community Kit Core Impact Contact Us

BUY NOW FEATURES SCREENSHOTS TRAINING SUPPORT BLOG

## Software for Adversary Simulations and Red Team Operations

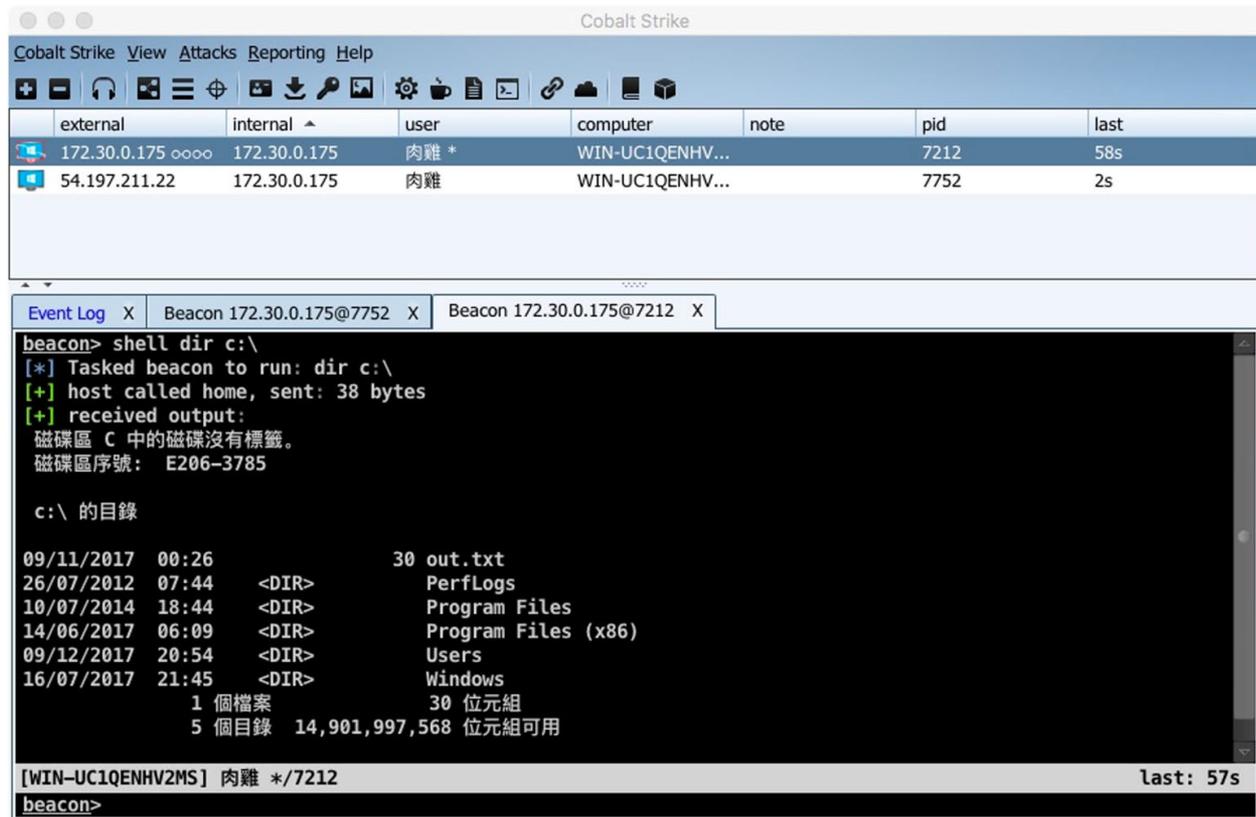
DOWNLOAD BUY NOW

Adversary Simulations and Red Team Operations are security assessments that replicate the tactics and techniques of an advanced adversary in a network. While penetration tests focus on unpatched vulnerabilities and misconfigurations, these assessments benefit security operations and incident response.

<https://www.cobaltstrike.com/>

# Cobalt Strike Components

- Beacon
  - Stager
  - Backdoor
- Loader
- Team Server
- Client



The screenshot displays the Cobalt Strike interface. At the top, there is a menu bar with 'Cobalt Strike', 'View', 'Attacks', 'Reporting', and 'Help'. Below the menu is a toolbar with various icons. The main area features a table of active beacons:

	external	internal	user	computer	note	pid	last
	172.30.0.175	172.30.0.175	肉雞 *	WIN-UC1QENHV...		7212	58s
	54.197.211.22	172.30.0.175	肉雞	WIN-UC1QENHV...		7752	2s

Below the table, there are tabs for 'Event Log', 'Beacon 172.30.0.175@7752', and 'Beacon 172.30.0.175@7212'. The active terminal window shows the following output:

```
beacon> shell dir c:\
[*] Tasked beacon to run: dir c:\
[+] host called home, sent: 38 bytes
[+] received output:
磁碟區 C 中的磁碟沒有標籤。
磁碟區序號: E206-3785

c:\ 的目錄

09/11/2017  00:26                30 out.txt
26/07/2012  07:44         <DIR>          PerfLogs
10/07/2014  18:44         <DIR>          Program Files
14/06/2017  06:09         <DIR>          Program Files (x86)
09/12/2017  20:54         <DIR>          Users
16/07/2017  21:45         <DIR>          Windows
                1 個檔案          30 位元組
                5 個目錄  14,901,997,568 位元組可用

[WIN-UC1QENHV2MS] 肉雞 */7212
beacon>
```

# Popular (ノロワロ)ノ\*

- Great features
- Hard to detect
- Easy to configure
- Generate plethora of payloads
- Command and control handled
- Hard to attribute



# Cobalt Strike - Users



Red teams



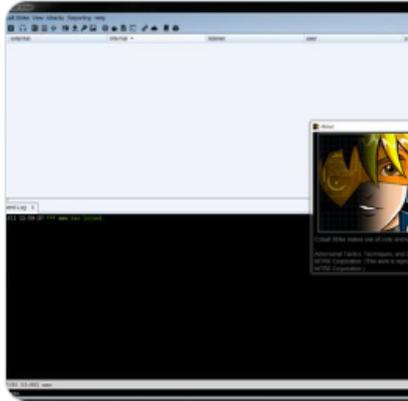
Adversaries

# Cobalt Strike

← Tweet

 **Cryptolnsane**  
@Cryptolnsane

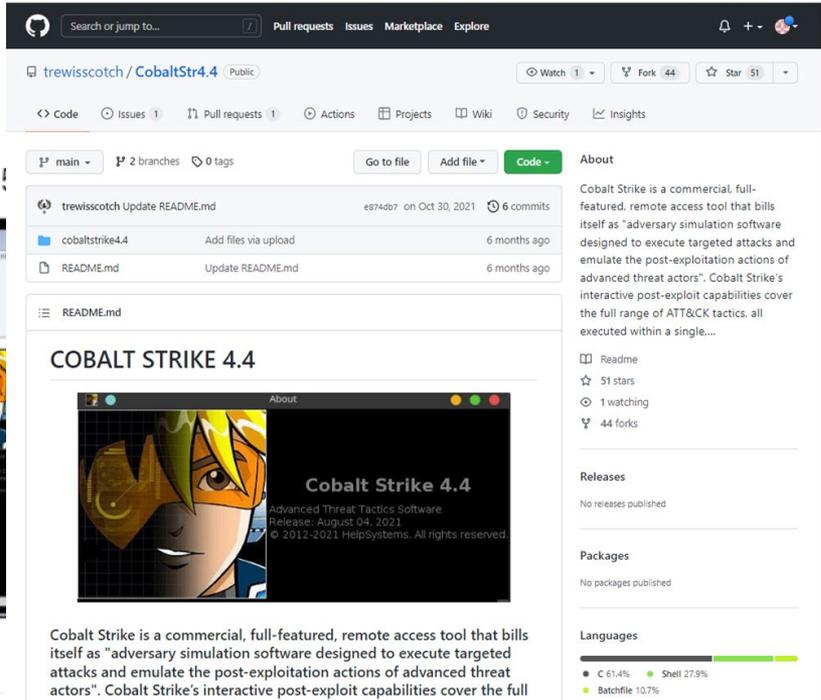
This is bad. Cobalt Strike 4.4!



7:04 PM · Feb 11, 2022 · Twitter Web App

 **Florian Roth** ⚡  
@cyb3rops

CobaltStrike 4.5 leaked 10 days after its release and



Search or jump to... Pull requests Issues Marketplace Explore

trewiscotch / CobaltStr4.4 Public

Code Issues 1 Pull requests 1 Actions Projects Wiki Security Insights

main 2 branches 0 tags

Go to file Add file Code

File	Commit	Author	Date	Commits
trewiscotch Update README.md	e874db7	on Oct 30, 2021	6 commits	
cobaltstrike4.4		Add files via upload	6 months ago	
README.md		Update README.md	6 months ago	

README.md

## COBALT STRIKE 4.4



**About**

**Cobalt Strike 4.4**

Advanced Threat Tactics Software  
Release: August 04, 2021  
© 2012-2021 HelpSystems. All rights reserved.

Cobalt Strike is a commercial, full-featured, remote access tool that bills itself as "adversary simulation software designed to execute targeted attacks and emulate the post-exploitation actions of advanced threat actors". Cobalt Strike's interactive post-exploit capabilities cover the full

**About**

Cobalt Strike is a commercial, full-featured, remote access tool that bills itself as "adversary simulation software designed to execute targeted attacks and emulate the post-exploitation actions of advanced threat actors". Cobalt Strike's interactive post-exploit capabilities cover the full range of ATT&CK tactics, all executed within a single...

Readme  
51 stars  
1 watching  
44 forks

**Releases**

No releases published

**Packages**

No packages published

**Languages**

- C 61.4%
- Shell 27.9%
- Batchfile 10.7%

**Aggressor Script  
Mask Kit Update, User  
Active Loader Kit Update**



... there's no  
**way to secretly watermark our software**  
imgflip.com

6:19 PM · Jan 5, 2022 · TweetDeck

# Cobalt Strike in the News

## Cobalt Strike Usage Explodes Among Cybercrooks



Author:  
Lisa Vaas

INTEZER

The legit security tool has shown up 161 percent more, year-over-year in cyberattacks, having “gone fully mainstream in the crimewar

The use of Cobalt Strike – the legitimate, commercially available tool used by r

## GhostWriter APT targets state entities with Cobalt Strike Beacon

March 28, 2022 By Pierluigi Paganini

## Ukraine CERT-UA warns that GhostWriter APT group is targeting Ukraine with Cobalt Strike Beacon

Ukraine CERT-UA uncovered a spear-phishing campaign by a GhostWriter APT group targeting Ukrainian state entities with Cobalt Strike Beacon.

The phishing messages use a RAR-archive named “Saboteurs 21.03.rar.” This second archive contains a file named “injector.exe” which is a Cobalt Strike Beacon. The file name contains the right-to-left extension.

“The archive contains documents and images of the beacon which will create and run the .NET program “dhdhk0k3 CERT-UA.

The attack chain ends with the delivery of a malicious compilation for the “injector” (“inject.exe”) is March 15,

## Russian APT Hackers Used COVID-19 Lures to Target European Diplomats

February 09, 2022 Ravi Lakshmanan



The Russia-linked threat actor known as APT29 targeted European diplomatic missions and Ministries of Foreign Affairs as part of a series of spear-phishing campaigns mounted in October and November 2021.

According to ESET’s T3 2021 Threat Report shared with The Hacker News, the intrusions paved the way for the deployment of Cobalt Strike Beacon on compromised systems, followed by leveraging the foothold to drop additional malware for gathering information about the hosts and other machines in the same network.

### Popular This Week

GitHub Says Breached Do Organization OAuth Access

Microsoft Issued 2 Windows Zero Days, 126 Other Vulnerabilities

Google Releases Chrome Update, Actively Exploiting a Critical Flaw

Russian Hackers Attacking UK Grid with Industrial Malware

Lazarus Group Million Axies Hack and Attacked Chemical Sector

Critical VMware Director Bug Hackers Take Control

# Cobalt Strike & Linux



## Linux, Left out in the Cold?

Posted on March 23, 2016 by Raphael Mudge

I've had several folks ask about Linux targets with Cobalt Strike 3.0 and later. **Beacon** is a Windows-only payload. The big question becomes, how do you use Cobalt Strike to operate against Linux, BSD, and other UNIX flavored targets?

### Beacon

Using Go to imple

This project is for please contact me

### CrossC2 framework

os linux os macOS issues 112 closed release v3.0.2 Release Download 28k



[README](#) | [中文文档](#) | [README\\_FULL](#) | [中文完整文档](#)

### How to play CobaltStrike support

1. Setup the tea `.cobaltstri` Support CobaltStrike's security assessment of other platforms (Linux/MacOS/ support of Unix post-penetration module
2. Compile the Beacon1001 with JetBrains idea, use command `java -jar beacon1001.jar` keystore to PEM format.
3. Replace the RSA key pair in the file `cmd/config/config.go` (the RSA private key is not r the code just for the record)
4. Compile the geacon whatever platform you want to run: for example, use the command `G00S="darwin" && export GOARCH="amd64" && go build cmd/main.go` to compile an ex running on MacOS.



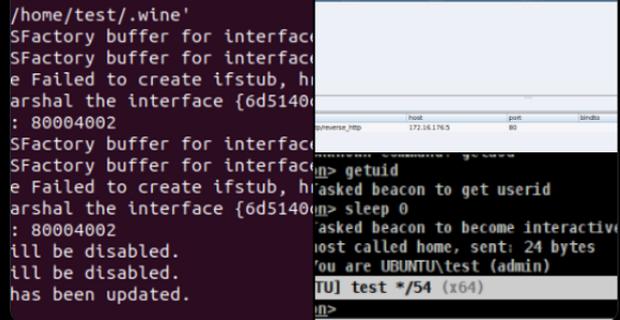
taha r @lordx64

Here's a one liner to use Cobalt Strike Beacon on Linux

wine beacon.exe

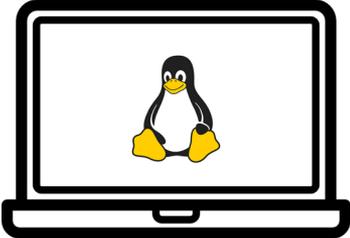
thank me later.

Wait you don't believe me? see screenshots below, it works.

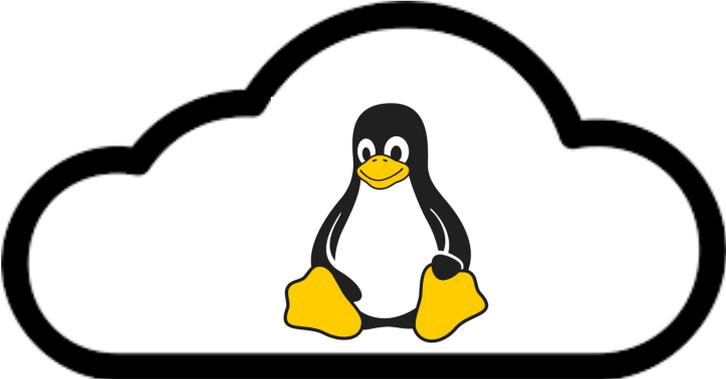


4:08 PM · Sep 13, 2021 · Twitter Web App

# Linux Market Share

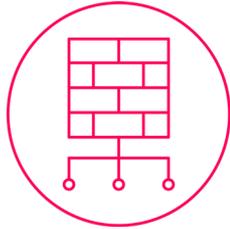


2%  
Desktop



90%  
Cloud

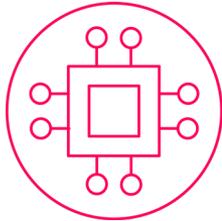
# Linux Malware Threat Landscape



Backdoors



Coin Miners



Botnets



Ransomware

# Nation State Targets Linux Systems



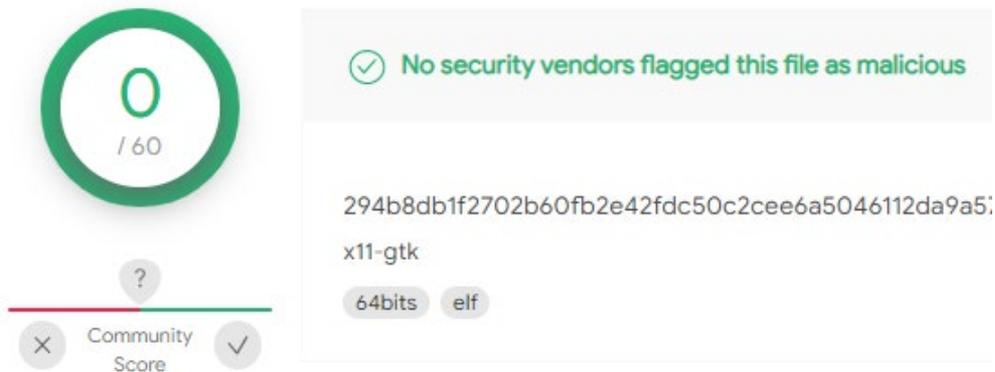
# Rise of the Vermilion

# Vermilion Strike - Background

1. **ELF sample** shares strings with Cobalt Strike
2. Previously unseen code
3. Network related capabilities

Gi	Capability	Category	Found in Code From
	create UDP socket	communication/socket/udp/send	Malware VermilionStrike
RR	receive data	communication	Malware VermilionStrike
RR	receive data on socket	communication/socket/receive	Malware VermilionStrike
RR	resolve DNS	host-interaction/network/dns/resolve	

# Vermilion Strike



**X11** - graphical environment for most Unix or Unix-like systems

**GTK** - widget libraries, which provide higher level abstraction above the X11 libraries

# Vermilion Strike



become a vict

DESCRIPTION: Detects CobaltStrike beacons based on XORed beacon configs

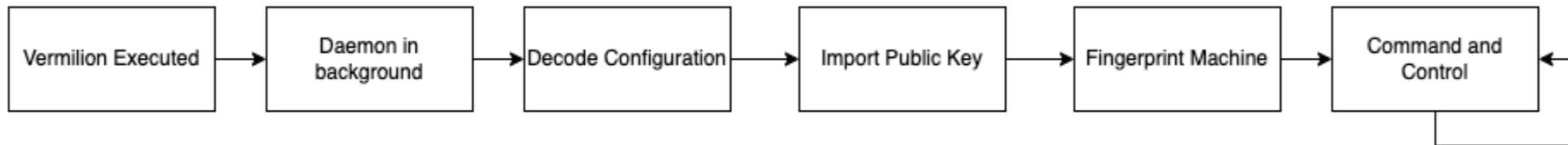
REFERENCE: <https://twitter.com/MichalKoczwara/status/1381170082445987842>

RULE\_AUTHOR: Florian Roth

# Vermilion Strike - Technical Analysis



# Flow Chart



# Configuration

- Simple XOR Cipher
- 0x69
- Can use standard tools for Cobalt Strike on this configuration too
- Windows artifacts still exist in Linux version

```
A 0123456789ABCDEF0123456789ABCDEF0123456789ABCDEF0123456789 comment
30 .....!.....0
e1 ..0...*.H.....0.....sq.W.....K..!*0<.....UA.m;N1.
b1 5s@=.yhF...:,p.s..e..Pb..N....>..`.....,]$.s.....I.
00 T.....`.u.ZU...<.b.....9Z[.S0...b.n.....
00
69 .....update.microsoftkernel.com,/dot.gi
00 f,update.microsoftkernel.com,/ca.....
00
00 .....Mozilla/
2f .....Mozilla/
42 4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0; GTB
00 7.4; InfoPath.2).....
00 .....@/template/template.jsp.....
00 .....
00 .....
00 .....
00 .....Cookie.....param1=format.....param2=output.....
00 .....!Referer: http://www.microsoft.com.....
00 .....
00 .....&Content-Type: application/octet-stream.
00 .....!Referer: http://www.microsoft.com.....id.
00 .....
00 .....@%windir%\syswow64\run
6e .....@%windir%\s
73 dll32.exe.....@%windir%\s
00 ysnative\rundll32.exe.....
00 .\%s\pipe\msgagent_%x.....
00 .....
00 .....GET.....
00 .....POST.....#.....
28 .....$.s.....
28 .....
```

# Fingerprinting

- Process ID
- Kernel Version
- Network
- User

```
>>> px @ rsi
- offset - 0 1 2 3 4 5 6 7 8 9 A B C D E F 0123456789ABCDEF
0x00a151a0 0000 beef 0000 005d 9974 8fa9 fac2 af10 .....].t.....
0x00a151b0 1284 997d 61e9 909a 3533 3935 3809 3531 ...].a...53958.51
0x00a151c0 094c 696e 7578 2d35 2e31 302e 3235 2d6c .Linux-5.10.25-l
0x00a151d0 696e 7578 6b69 7409 3137 322e 3137 2e30 inuxkit.172.17.0
0x00a151e0 2e32 0964 6636 6164 3338 3661 6136 3109 .2.df6ad386aa61.
0x00a151f0 726f 6f74 202a 0931 0931 0930 0931 2e30 root *.1.1.0.1.0
0x00a15200 2e31 2e4c 5200 0000 b100 0000 0000 0000 .1.LR.....

Text

>>> px @ rsi
- offset - 0 1 2 3 4 5 6 7 8 9 A B C D E F 0123456789ABCDEF
0x00a19020 70ed 5b00 b566 da53 d958 fef5 adad 55f4 p.[. .f.S.X....U.
0x00a19030 e0ae 9b54 d7f9 d591 c759 61c3 2b28 35c6 ...T....Ya.+(S.
0x00a19040 ec52 d6f3 876f 807e 194a af77 1ff5 5556 .R...o~.J.W..UV
0x00a19050 6c35 27de eb7b f406 e21c b464 b141 1670 15'..{....d.A.p
0x00a19060 eb5d ef85 4f0f f6ca 9548 9953 .]..0...I<...d.H
0x00a19070 b460 b1ab a640 f000 9953 .'.@...S...*[..S
0x00a19080 b36f b1f2 19a4 a548 7669 .o....G....`vi
0x00a19090 c476 a2c2 27a4 951b 6ffe 3703 a53c 97b6 .v..'...o.7...<

RSA Encrypted

>>> px @ rsi
- offset - 0 1 2 3 4 5 6 7 8 9 A B C D E F 0123456789ABCDEF
0x00a1a610 634f 3162 414c 566d 326c 505a 5750 3731 c01bALVm21PZWP71
0x00a1a620 7261 3156 394f 4375 6d31 5458 2b64 5752 ra1V90Cum1TX+dWR
0x00a1a630 7831 6c68 7779 736f 4e63 6273 5574 627a x1lhwysoNcbsUtbz
0x00a1a640 6832 2b41 6668 6c4b 7233 6366 3956 5657 h2+zAfh1Kr3cf9VWV
0x00a1a650 6244 556e 3375 7437 3941 6269 484c 526b bDUn3ut79AbiHLrk
0x00a1a660 7355 4557 634f 7464 3734 5650 442f 6168 sUEWc0td74VPD/ah
0x00a1a670 5354 7a2f 7a4c 706b 6c55 6930 594c 4772 STz/zLpk1Ui0YLG
0x00a1a680 706b 4477 41 6c54 pkDwAF0pyybxZLT
0x00a1a690 7332 2b78 38 a 3863 s2+x8hmkpUfjmJ8c
0x00a1a6a0 386d 4232 61 a 5562 8mB2acR2osTnpJUb
0x00a1a6b0 622f 3433 4136 5538 6c37 593d 0000 0000 b/43AGU817Y=...

Base64 Encoded
```

# Command & Control

- DNS & HTTP
- Primarily DNS
- Commands received over Address (A) and Text (TXT) records

11	11.623868235	10.0.2.15	168.63.129.16	DNS	...	Standard query	0x77a4 A 86907.update.microsoftkernel.com
12	11.933851334	168.63.129.16	10.0.2.15	DNS	...	Standard query response	0x77a4 A 86907.update.microsoftkernel.com A 255.255.255.242
13	11.934029265	10.0.2.15	168.63.129.16	DNS	...	Standard query	0xfbfe A apple.dPk8sNHbf.86907.update.microsoftkernel.com
14	12.370098937	168.63.129.16	10.0.2.15	DNS	...	Standard query response	0xfbfe A apple.dPk8sNHbf.86907.update.microsoftkernel.com A 0.0.0.64
15	12.370263557	10.0.2.15	168.63.129.16	DNS	...	Standard query	0xd56b TXT facebook.aNjQhxc3l.86907.update.microsoftkernel.com
16	12.683275494	168.63.129.16	10.0.2.15	DNS	...	Standard query response	0xd56b TXT facebook.aNjQhxc3l.86907.update.microsoftkernel.com TXT

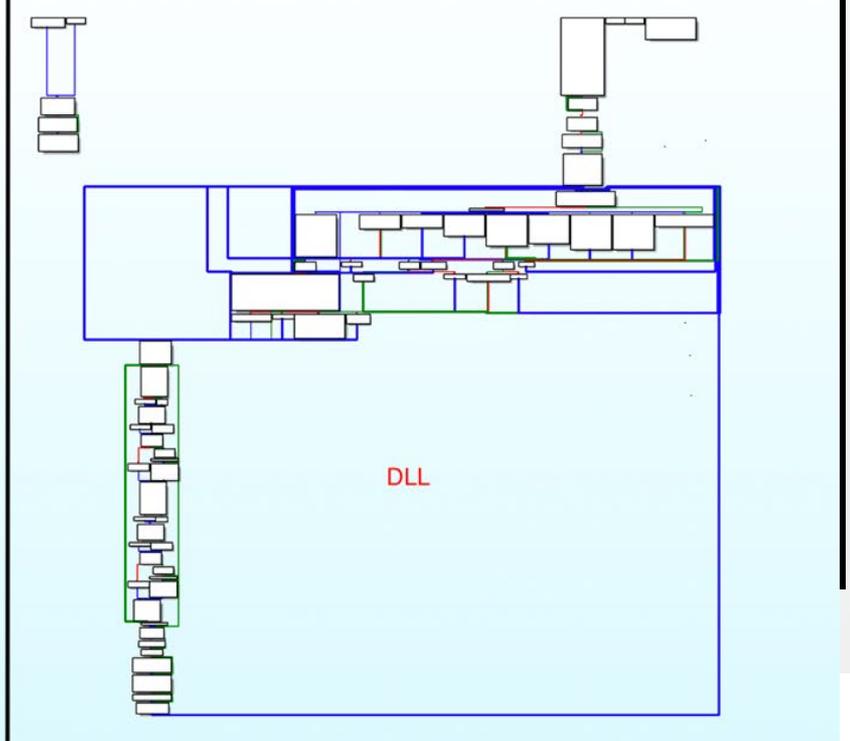
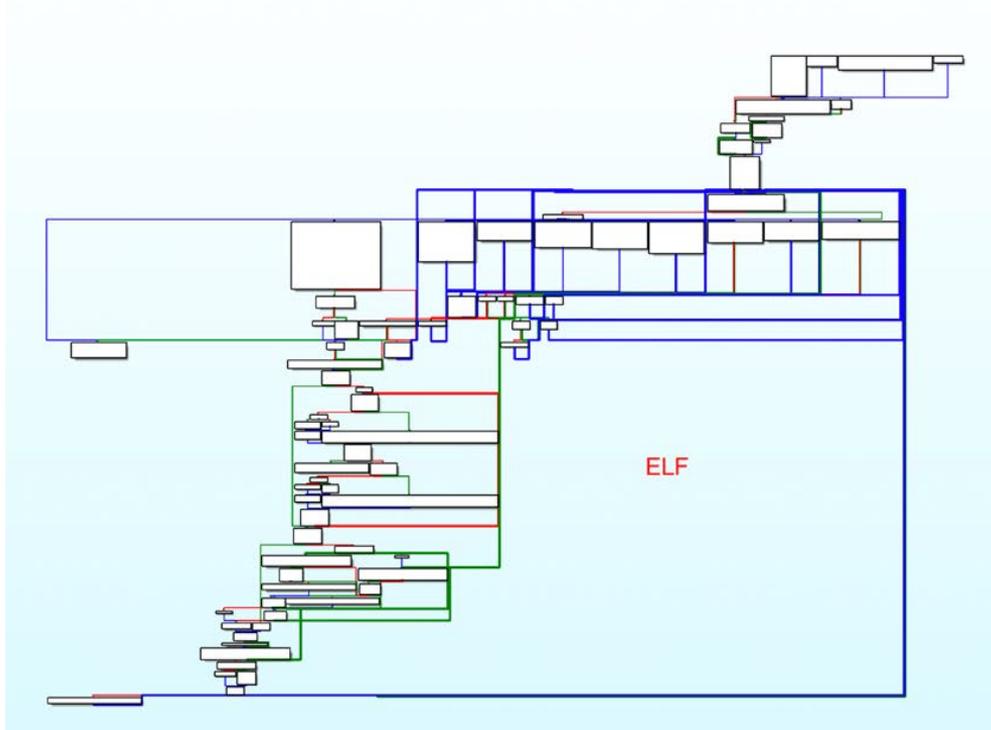


```
:> ps @ [rdi]
wQ7mYmyLh2gijCitUJCe5hI2hjrY5HmdSwc0d0ARn+TQKYLpuMioT59HiMW//f8aaRop4UAD0tum/j2pBhxqGg==
```

# Commands



# Windows Version

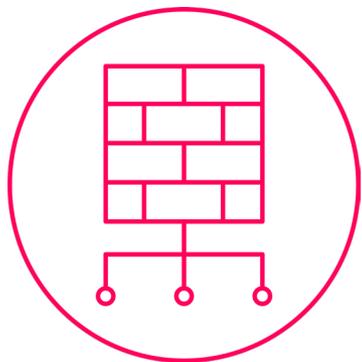


# Vermilion Strike In the Wild



\*Based on McAfee Enterprise ATR

# Attribution



Backdoor



Written from scratch

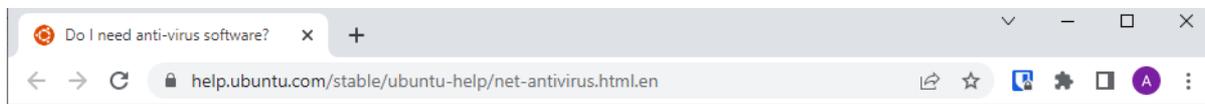


Multi-platform



Found in live attacks

# Why Linux Malware Fly Under the Radar?



✔ No engines detected this file

1fc49503c92bce012cc9210a0490fb3657ff9177d342cc

bot

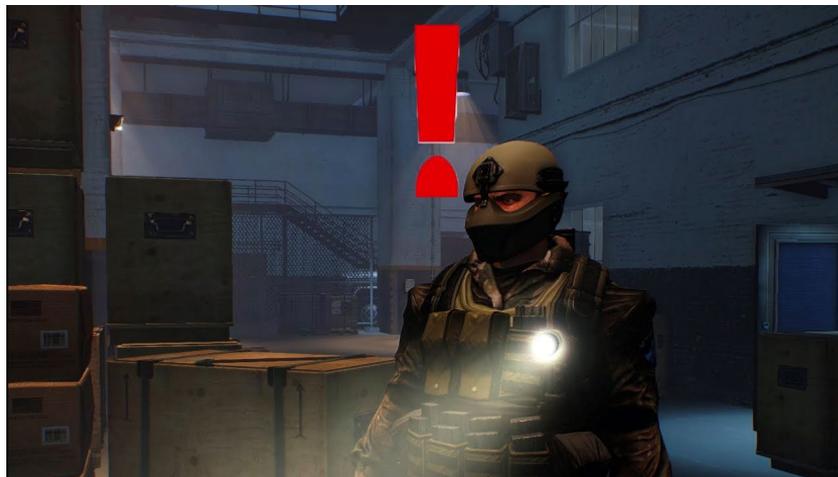
64bits elf



If you want to be extra-safe, or if you want to check for viruses in files that you are passing between yourself and people using Windows and Mac OS, you can still install anti-virus software. Check in the software installer or search online; a number of applications are available.

# Detection & Response

- Vermillion Strike for Windows needs to be detected in memory
- One can detect via the stager too
- Linux version can be detected on disk
- Some Cobalt Strike detection methods can be used to detect Vermillion Strike
- Can be detected via network



# Predictions

- Cobalt Strike will remain a big issue for Windows
- Vermilion Strike has an unsure future
- Cross platform malware will continue



# Thank You!



<https://www.intezer.com/blog/malware-analysis/vermilionstrike-reimplementation-cobaltstrike/>