# Rise of the Vermilion

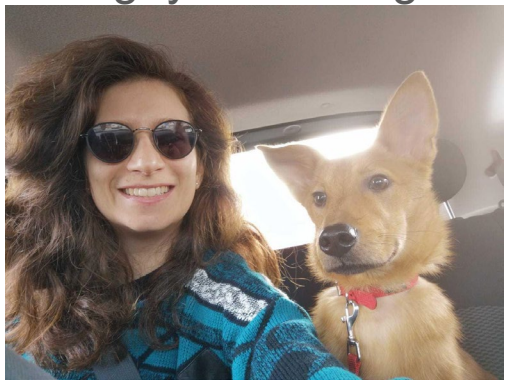
## Cross-Platform Cobalt Strike Beacon Targeting Linux and Windows

Ryan Robinson Avigayil Mechtinger

INTEZER

# Who Are We

Avigayil Mechtinger



Product Manager | Intezer

@AbbyMCH

Rvan Robinson

Security Researcher | Intezer

@MhicRoibin

# Agenda

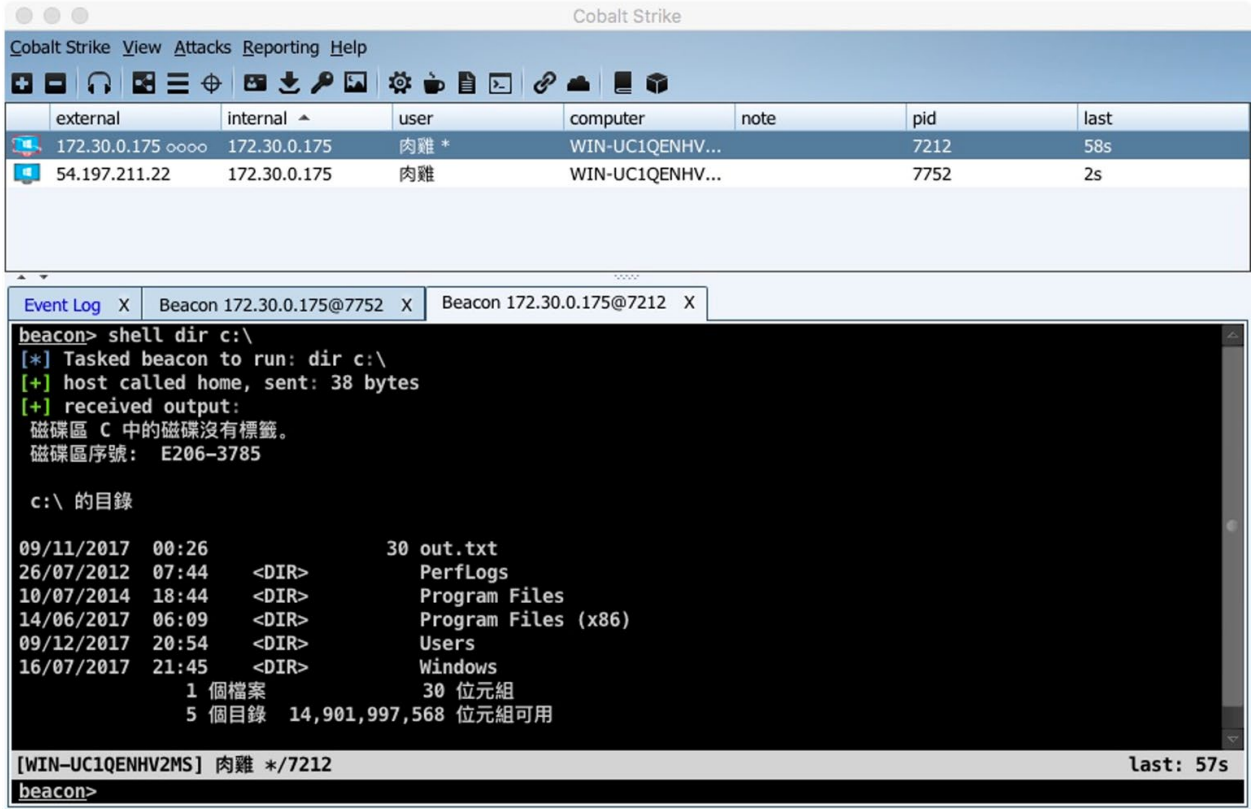
- Cobalt Strike
- Linux Malware Threat Landscape
- Vermilion Strike
  - Background
  - Technical analysis
- Discussion
- Wrap Up

# What is Cobalt Strike?


https://www.cobaltstrike.com/

# Cobalt Strike Components

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



# Popular (/◕ワ◕)/*

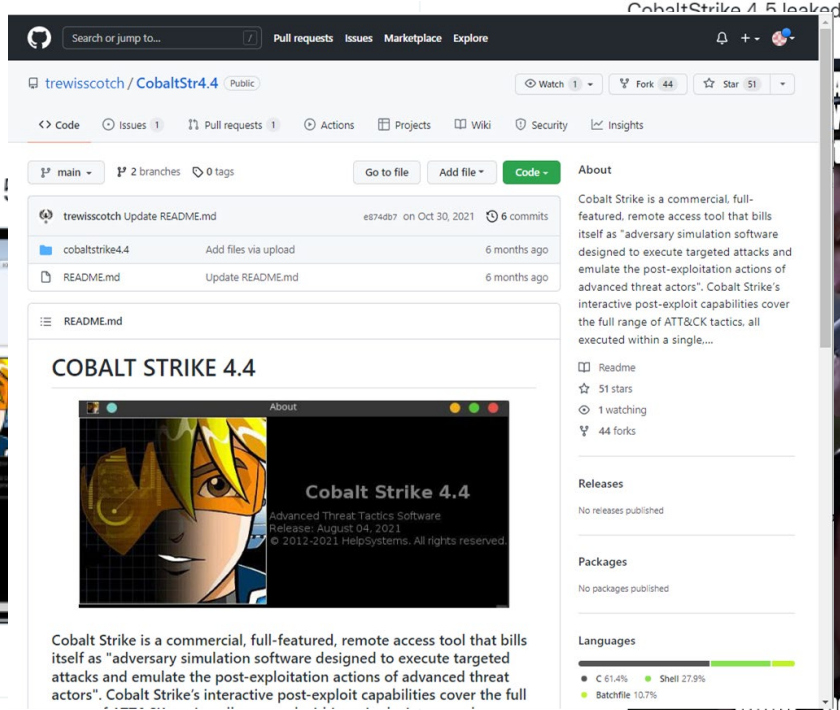
- Great features
- Hard to detect
- Easy to configure
- Generate plethora of payloads
- Command and control handled
- Hard to attribute

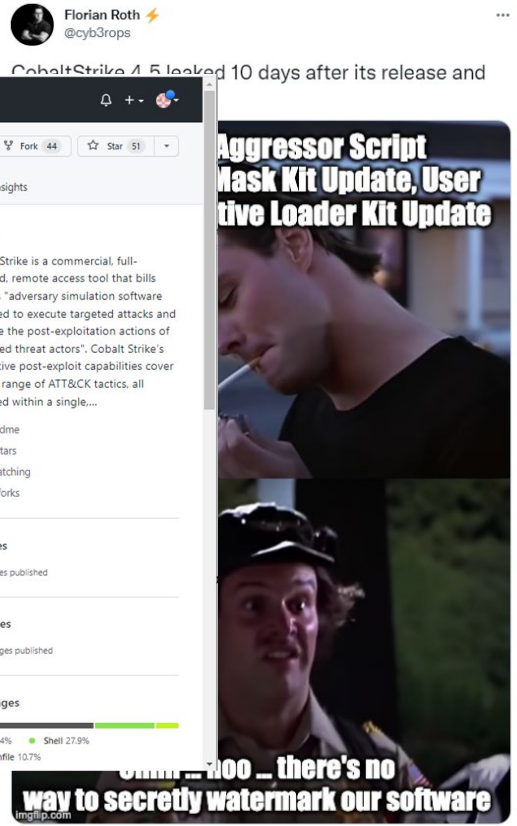
# Cobalt Strike - Users

Red teams

Adversaries

# Cobalt Strike

# Cobalt Strike in the News

threatpost Podcasts / Malware / Vulnerabilities / InfoSec Insiders / Web

## Cobalt Strike Usage Explodes Among Cybercrooks

Author: Lisa Vaas

The legit security tool has shown up 161 percent more, year-o in cyberattacks, having "gone fully mainstream in the crimewa

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

INTEZER

GhostWriter APT targets state en

Cobalt Strike Beacon

March 28, 2022 By Pierluigi Paganini

Ukraine CERT-UA warns that

GhostWriter APT group is targ

Ukraine with Cobalt Strike Be

Ukraine CERT-UA uncovered a spear-phishing campaig APT group targeting Ukrainian state entities with Cobal

The phishing messages use a RAR-archive named "Sa "Saboteurs 21.03.rar." This second archive contains Sf reported that the file name contains the right-to-left ov extension.

*"The archive contains documents and images of the ba 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,

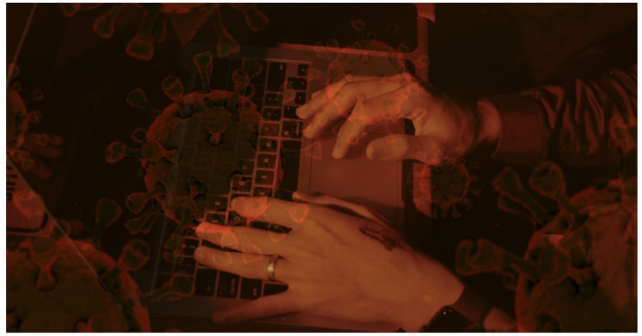
The Hacker News

Subscri

Home Data Breaches Cyber Attacks Vulnerabilities Malware Offers Contact

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

February 09, 2022 Ravie 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 We

GitHub Says Breached Do Organization OAuth Acces

Microsoft Iss 2 Windows Z 126 Other Vu

Google Relea Chrome Upd Actively Expl Flaw

Russian Hac Attacking Uk Grid with Ind Malware

Lazarus Grou Million Axie I Hack and Att Chemical Se

Critical VMw Director Bug Hackers Take

# Cobalt Strike & Linux

Cookie Preferences

cobaltstrike
by HelpSystems

## 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?

## 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

## CobaltStrike support

Support CobaltStrike's security assessment of other platforms (Linux/MacOS/ support of Unix post-penetration module

## Geacon

Using Go to imple

*This project is for*
*please contact me*

## How to play

1. Setup the tea
   `.cobaltstri`
2. Compile the BeaconTool with JetBrains Idea, use command `java -jar BeaconTool.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 `GOOS="darwin" && export GOARCH="amd64" && go build cmd/main.go` to compile an ex running on MacOS.

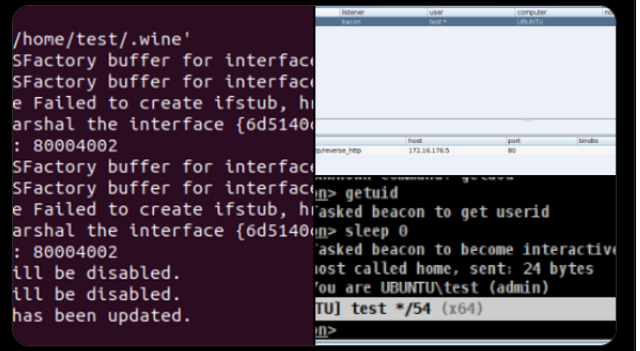
taha ד
@lordx64

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

wine beacon.exe

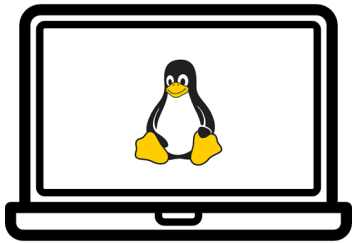
thank me later.

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

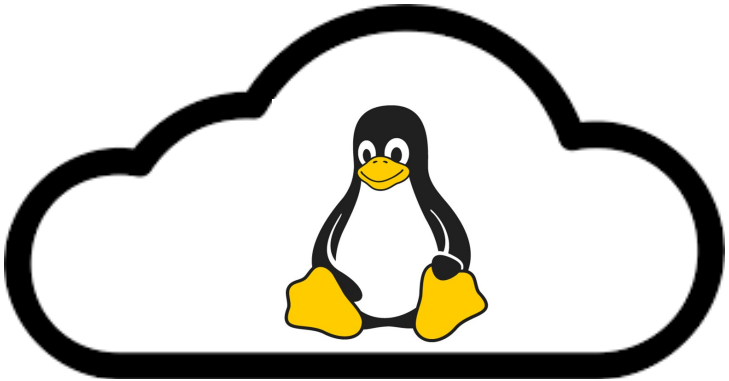



4:08 PM · Sep 13, 2021 · Twitter Web App

# Linux Market Share



2%
Desktop

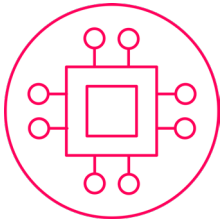


90%
Cloud

# Linux Malware Threat Landscape

Backdoors

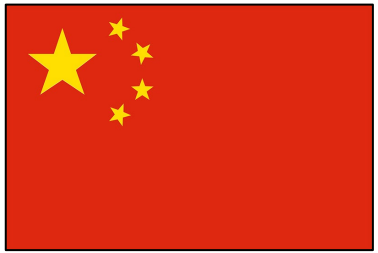
Coin Miners



Botnets

Ransomware

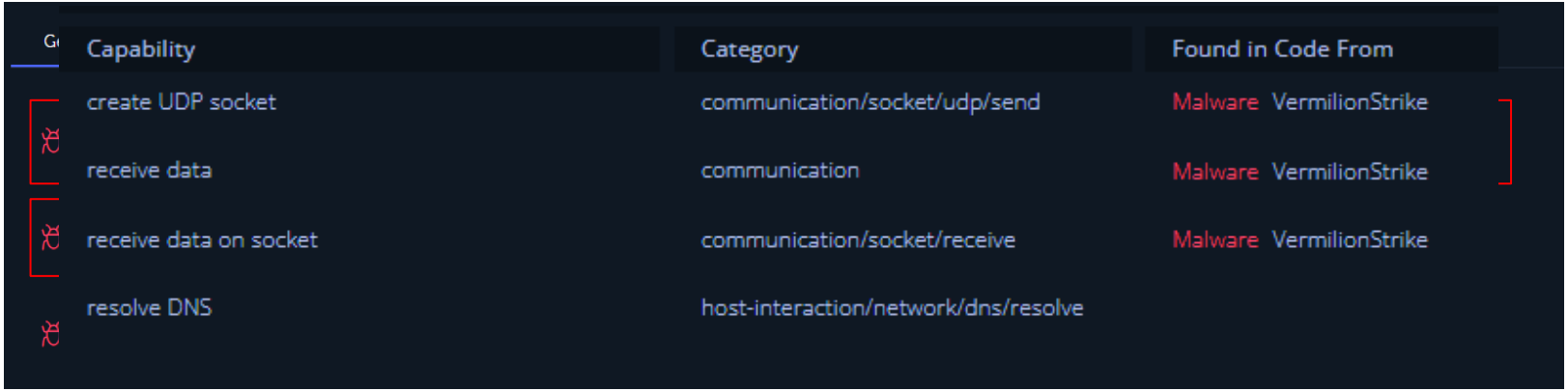
# Nation State Targets Linux Systems



# Rise of the Vermilion

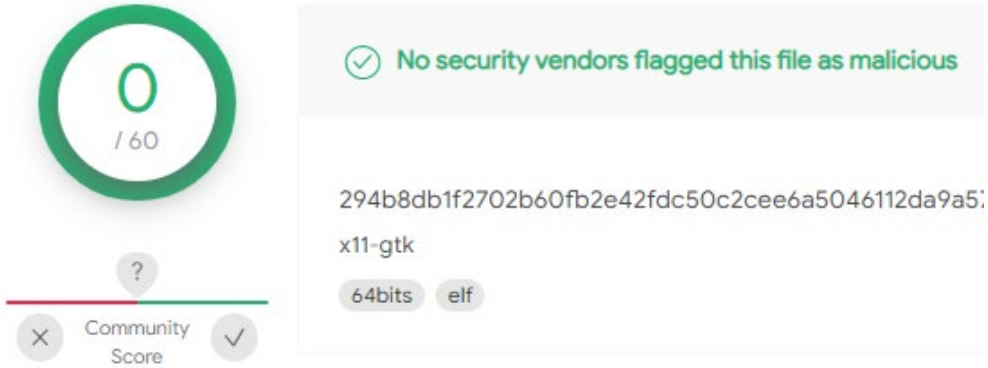
# Vermilion Strike - Background

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



| Capability | Category | Found in Code From |
|---|---|---|
| create UDP socket | communication/socket/udp/send | Malware VermilionStrike |
| receive data | communication | Malware VermilionStrike |
| receive data on socket | communication/socket/receive | Malware VermilionStrike |
| 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

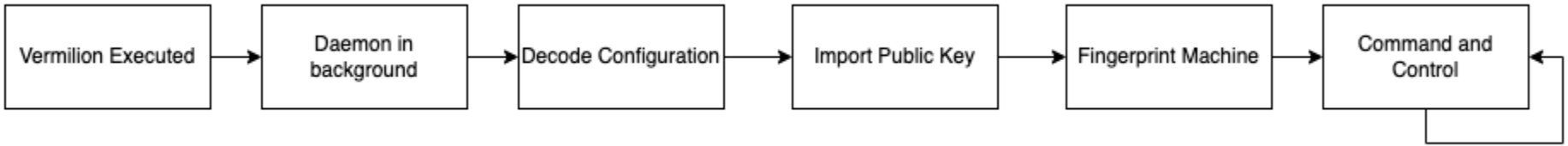
# Vermilion Strike

become a vict

REFERENCE: https://twitter.com/MichalKoczwara/status/1381170082445987842
RULE_AUTHOR: Florian Roth

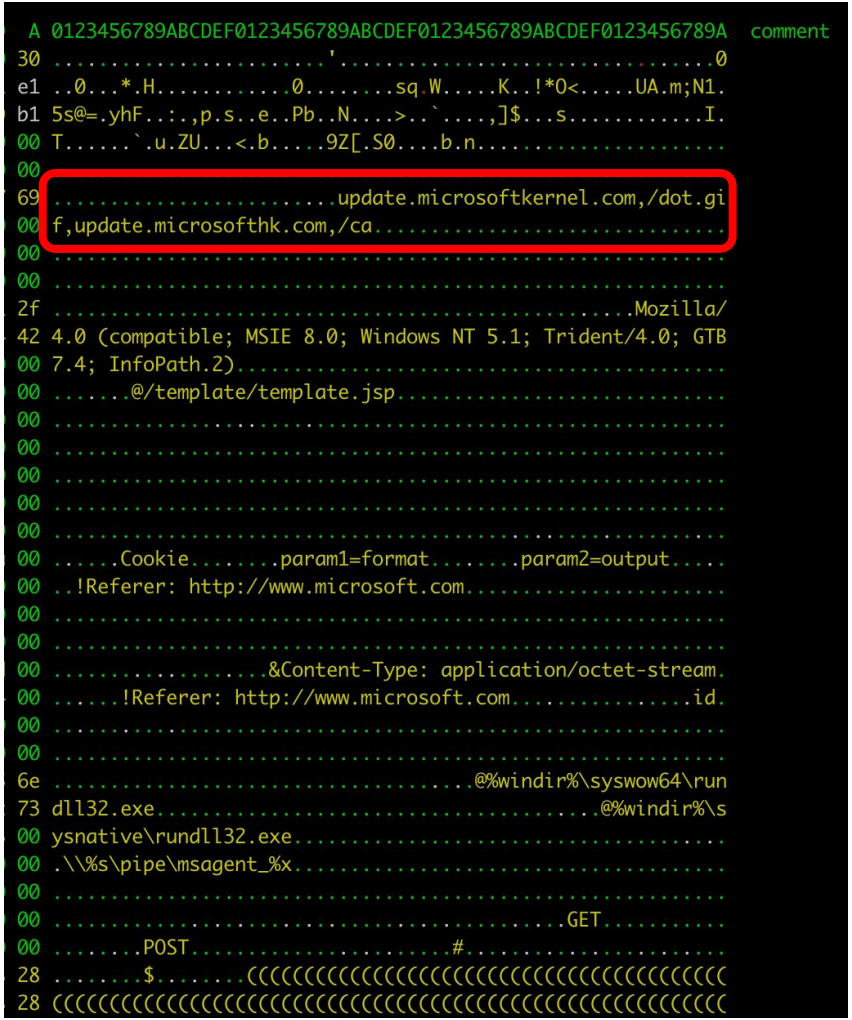
# Vermilion Strike - Technical Analysis

# Flow Chart


Vermilion Executed
Daemon in background
Decode Configuration
Import Public Key
Fingerprint Machine
Command and Control

# Configuration

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



# Fingerprinting

- Process ID
- Kernel Version
- Network
- User

# Command & Control

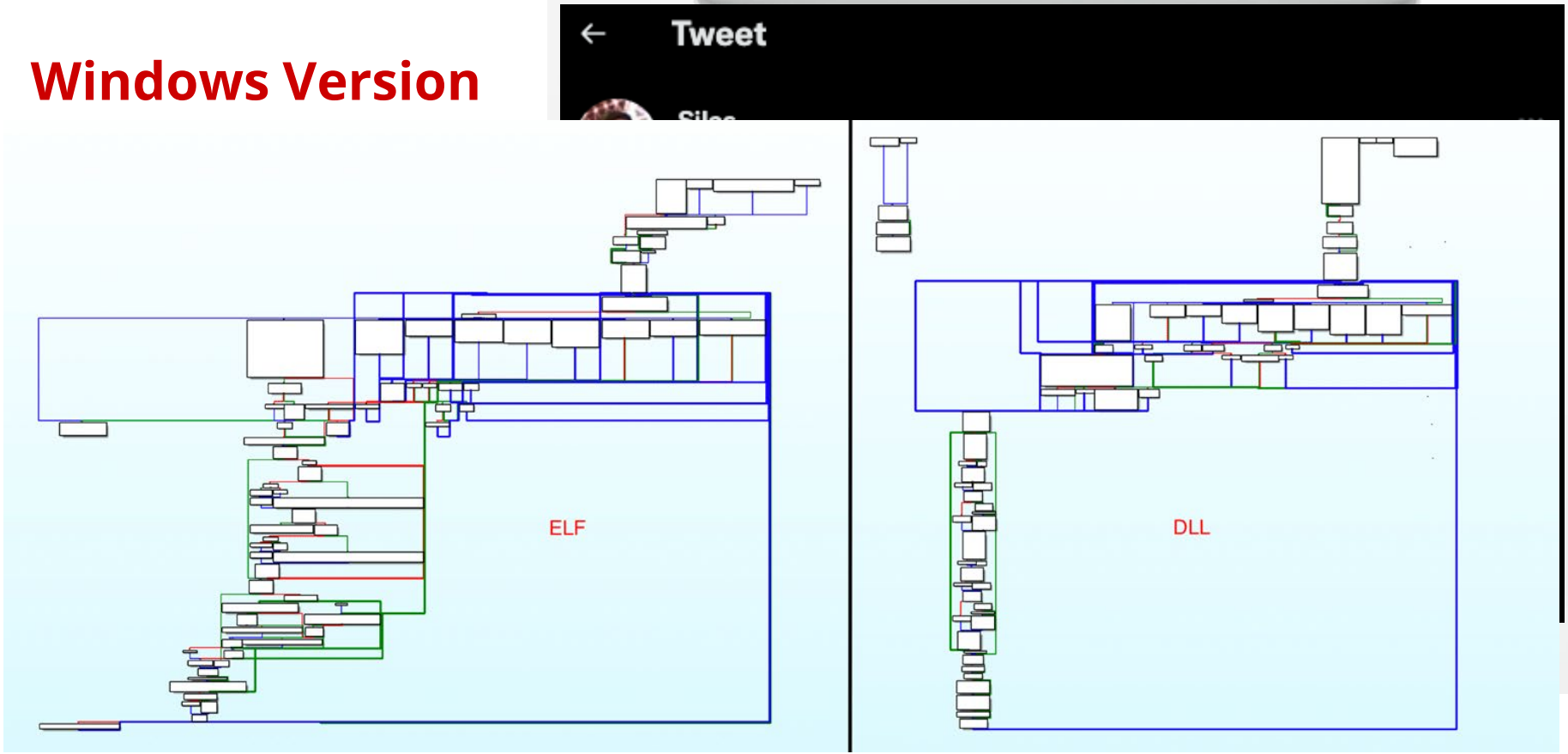
- DNS & HTTP
- Primarily DNS
- Commands received over Address (A) and Text (TXT) records

```
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//f8aaRop4UADOtum/j2pBhxqGg==
:>
```

# Commands

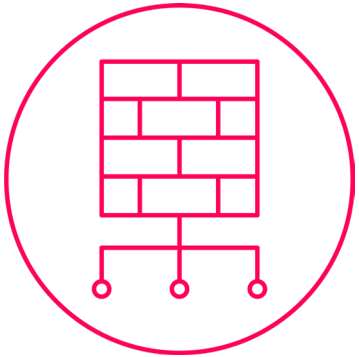
# Windows Version



# Vermilion Strike In the Wild


*Based on McAfee Enterprise ATR

# Attribution



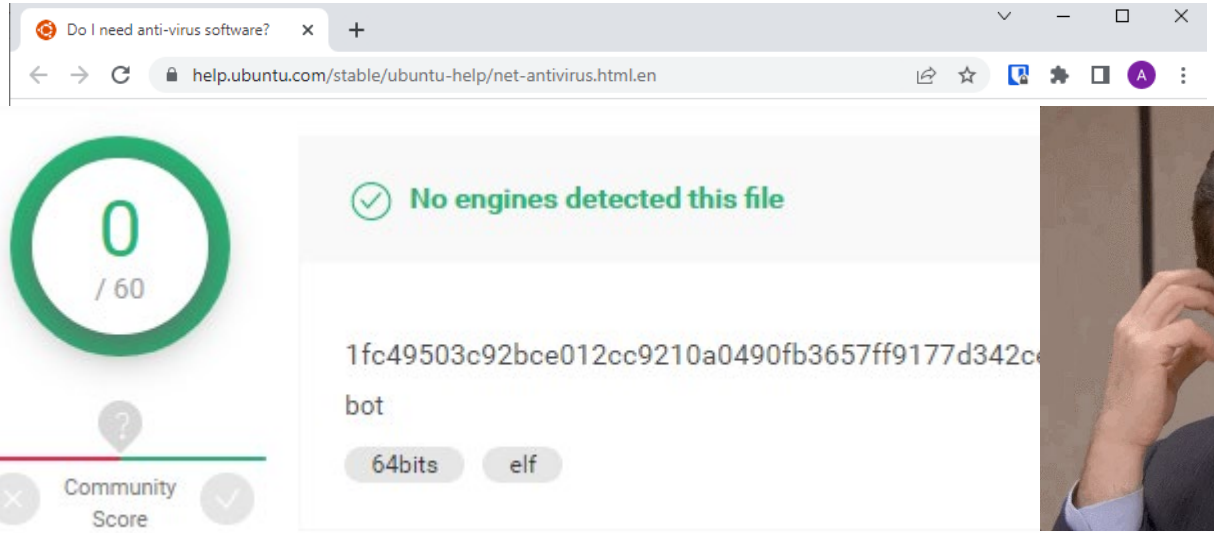
Backdoor

Written from scratch

Multi-platform

Found in live attacks

# Why Linux Malware Fly Under the Radar?




# 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 Vermilion 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/

INTEZER