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

Ryan 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 (/◕ヮ◕)/

- 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

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 APT & CE tactics, all executed within a single...

INTEZER
Cobalt Strike in the News

Cobalt Strike Usage Explodes Among Cybercrooks

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.

The phishing messages use a RAR-archive named "Saboteurs 21.03.rar." This second archive contains a file which contains the right-to-left overflow extension.

"The archive contains documents and images of the beacon which will create and run the .NET program "dhdk8k3 CERT-UA."

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

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.
Cobalt Strike & Linux

Geacon

Using Go to impl

This project is for please contact me

README | 中文文档 | README_FULL | 中文完整文档

How to play

1. Setup the tea .cobaltstrike
2. Compile the Beacons 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 used in the code just for the record)
4. Compile the geacon whenever platform you want to run: for example, use the command 600s=darwin & export GOARCH="amd64" & go build cmd/main.go to compile an executable running on MacOS.

CrossC2 framework

Coast views Linux, MacOS, issues, release v3.2.2, Release Download 251

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.
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

<table>
<thead>
<tr>
<th>Capability</th>
<th>Category</th>
<th>Found in Code From</th>
</tr>
</thead>
<tbody>
<tr>
<td>create UDP socket</td>
<td>communication/socket/udp/send</td>
<td>Malware VermilionStrike</td>
</tr>
<tr>
<td>receive data</td>
<td>communication</td>
<td>Malware VermilionStrike</td>
</tr>
<tr>
<td>receive data on socket</td>
<td>communication/socket/receive</td>
<td>Malware VermilionStrike</td>
</tr>
<tr>
<td>resolve DNS</td>
<td>host-interaction/network/dns/resolve</td>
<td>Malware VermilionStrike</td>
</tr>
</tbody>
</table>
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

DESCRIPTION: Detects CobaltStrike beacons based on XORed beacon configs
REFERENCE: https://twitter.com/MichalKoezwara/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
Fingerprinting

- Process ID
- Kernel Version
- Network
- User
Command & Control

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

● Pivot through C2 address
● Sample was a stager using PowerShell
● DLL was fetched and executed in memory
● This DLL was from 2019!
● Functionality is largely the same
Vermilion Strike In the Wild

*Based on McAfee Enterprise ATR

IT companies

Government agencies

Financial institutions

Telecom companies

Advisory companies

*Based on McAfee Enterprise ATR
Attribution

- Backdoor
- Written from scratch
- Multi-platform
- Found in live attacks
Why Linux Malware Fly Under the Radar?

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 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/