List of Open Source C2 Post-Exploitation Frameworks

Posted: 📅 2 months ago by @pentestit 7674 views
Updated: 🕘 August 10, 2019 at 4:48 am

This post has been lying in my drafts for more than a year with edits all over. But two days ago, it was announced that *Powershell Empire* would no longer be supported by it's authors. Hence just like I curated a list of adversary emulation tools, I finalized this list of open source C2 post-exploitation frameworks and thought of publishing this today. This is my attempt at introducing you all with other options that are available to help you "elevate your post-exploitation experience" on multiple operating systems. This post includes Powershell C2 frameworks, Python C2 frameworks, Go C2 frameworks and others in an alphabetical order.

1. **APfell**: *APfell* is a cross-platform, OPSEC aware, red teaming, post-exploitation C2 framework built with python3, docker, docker-compose, and a web browser UI. It is designed to provide a collaborative and user friendly interface for operators, managers, and reporting on Mac OS and Linux based operating systems. It includes support for multiple C2 profiles, multiple payload types, *JavaScript for Automation* (JXA) exclusive to Mac OS, and an interesting Chrome extension payload. APfell maps to my favourite MITRE ATT&CK framework as well. Interestingly, the C2 framework finds inspiration from well known malware families such as PlugX, Flame, etc. Check out APfell version 1.2.
2. **Covenant**: *Covenant* is a .NET command and control framework that aims to highlight the attack surface of .NET, make the use of offensive

.NET tradecraft easier, and serve as a collaborative command and control platform for red-teamers. What sets this apart from other C2 Post-Exploitation Frameworks is that it supports .NET Core – which is multi-platform. Hence, Covenant can run natively on Linux, MacOS, and Windows platforms! Additionally, Covenant has docker support, allowing it to run within a container on any system that has docker installed. It consists of three components – Covenant (server-side component), Elite (client-side component) and Grunt (implant). Check out Covenant v0.3.

3. **EmpireProject**: Sadly as mentioned earlier, this was recently discontinued. *Empire/Empyre* is a pure PowerShell post-exploitation agent built on cryptologically-secure communications and a flexible architecture. Empire implements the ability to run PowerShell agents without needing Powershell, rapidly deployable post-exploitation modules ranging from key loggers to Mimikatz, and adaptable communications to evade network detection, all wrapped up in a usability-focused framework. Get the last version – Empire 2.5 Release.
4. **Faction C2**: The Faction C2 framework focuses on operational security,

flexibility & teamwork. Its API focused design provides the foundation for secure communications across any transport method via well documented REST and Socket.IO APIs, to any agent that can speak its language. Currently Faction supports only .NET payloads and modules. *Marauder* is an example .NET agent for the Faction C2 Framework. However you can easily create your own agent as well. Faction was designed with redirects in mind in the form of *Transport Servers*. These sit between Faction and your agent and handle masking your communications. This C2 post-exploitation framework has a role based access control system and data can be queried using SQL queries! Check out **Faction C2** and **Marauder**.

Updated 8/9/2019:

5. **goDoH**: goDoH is a proof of concept Command and Control framework, written in Golang, that uses DNS-over-HTTPS as a transport medium. Currently supported providers include Google, Cloudflare but also contains the ability to use traditional DNS. Since goDoH is written in Golang, a single executable for most platforms can be built that contains both the server-side and client-side code needed. Get goDoH 1.5 (5b0db27).
6. **iBombshell**: iBombShell is a dynamic, open source tool that allows post-exploitation functionalities via a shell or a prompt on systems that support Powershell. Supported features are loaded dynamically in-memory avoiding any hard drive writes, whenever they are needed from a repository. I blogged about this C2 post-exploitation framework here. Get the latest iBombshell version here.
7. **Koadic**: Koadic is an open source, post-exploitation rat aka remote access trojan that uses the Windows Script Host; via the COM interface, for most of it's operations. Since it uses VBScript/JScript you can expect it to work on all Microsoft Windows operating systems from Windows 2000 onwards as it has inbuilt support. I covered it in a blog titled – *Koadic: An Advanced Windows JScript/VBScript RAT*. Give Koadic a run here.
8. **Merlin**: Merlin is a cross-platform post-exploitation HTTP/2 C2 server & agent written in Golang. It helps you to evade network detection during a penetration test/red team exercise by using a protocol that existing tools aren't equipped to understand or inspect. Both the Merlin Server and Agent can easily be compiled to run on a multitude of operating systems to include Windows, Linux, Mac OS, Solaris, FreeBSD, ARM, MIPS, or Android. Latest versions of Merlin support features such as Shellcode execution and Shellcode Reflective DLL Injection

(sRDI). Get Merlin v0.7.0.

Updated 8/8/2019:

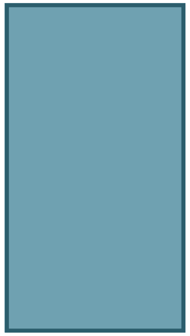
9. **Nuages**: Nuages is a modular C2 framework, where back end components are open source, while implants and handlers must be developed by the end users according to the functionality needed. Nuages is available through REST or socket.io and can be controlled via command line or a browser via Nuages_Cli or Nuages_WebCli clients. An example C# implant is included as well. Get Nuages C2.
10. **PoshC2**: PoshC2 is a proxy aware C2 framework that utilizes Powershell **and/or** equivalent (*System.Management.Automation.dll*) to aid penetration testers with red teaming, post-exploitation and lateral movement. Powershell was chosen as the base implant language as it provides all of the functionality and rich features without needing to introduce multiple third party libraries to the framework. In addition to the Powershell implant, PoshC2 also has a basic dropper written purely in Python that can be used for command and control over Unix based systems such as Mac OS or Ubuntu. Get PoshC2 v4.8.
11. **Silver**: This is one of the more recent C2 post-exploitation frameworks. Sliver is a cross-platform implant framework that supports C2 over Mutual-TLS, HTTP(S), and DNS. Implants are dynamically compiled with unique X.509 certificates signed by a per-instance certificate authority generated when you first run the binary. Implants support features such as *dynamic code generation, compile-time obfuscation, process injection, anti-forensics, Windows process migration* and *Windows user token manipulation*. Get Silver v0.0.6-alpha.
12. **SILENTTRINITY**: It is an asynchronous post-exploitation agent powered by Python, IronPython, C# and .NET's DLR. SILENTTRINITY introduces a somewhat new Red Team approach called as BYOI (Bring Your Own Interpreter). Currently the implant only supports C2 over HTTP 1.1. Get **SILENTTRINITY**.
13. **TrevorC2**: TrevorC2 is a client/server model for masking command and control through a normally browsable website. Detection becomes much harder as time intervals are different and does not use POST requests for data exfiltration and it supports Windows, MacOS, and Linux. Get TrevorC2 1.0.

These are the C2 post-exploitation frameworks I know of. As always, I will keep updating this post.

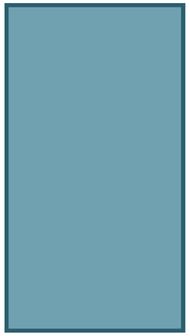
Share this post on:

twitter facebook WhatsApp G+oogle+ Buffer Linkedin Pin It

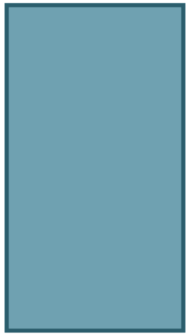
Related Posts on PenTestIT:



UPDATE: Covenant v0.3.2



UPDATE: Kali Linux 2019.3 Release



UPDATE: Merlin v0.8.0

UPDATE: MITRE CALDERA 2.3.0

Filed Under: Offensive Security , Open Source , Penetration Testing

Tagged With: Apfell , Covenant , docker , Empire , Empire Project , Faction C2 , goDoH , iBombShell , Koadic , Merlin , Mimikatz , MITRE ATT&CK™ , Nuages , PoshC2 , post-exploitation , PowerShell , python , SILENTTRINITY , Silver , TrevorC2

RECENT POSTS

UPDATE: Covenant v0.3.2

UPDATE: Kali Linux 2019.3 Release

UPDATE: Merlin v0.8.0

UPDATE: MITRE CALDERA 2.3.0

UPDATE: Infection Monkey 1.6.3

CONTACT INFORMATION

On the older **PenTestIT** blog, we had a section called “Submit Your Tools”. Similarly, you can submit your cool new shiny tool to the following email address:

You can use this email address for general communication as well.

Support this blog by using **this referral link**.

FEATURED POST

UPDATE: Covenant v0.3.2

September 26, 2019 By Black

Leave a Comment

A few weeks ago an update – Covenant v0.3.2 was released. There was a brief mention about Covenant in my post titled – List of Open Source C2 Post-Exploitation Frameworks. This updated version includes new persistence modules – PersistWMI, PersistAutorun, PersistStartup, a BypassAmsi module added by @_RastaMouse and a ScreenShot module added by @infosec_n00b. What's Covenant? Covenant is a .NET

READ MORE

TAGS

Anchore APT2 Brute Force CloudFlare Cross-Site Scripting cuc Cuckoo Sandbox DataSploit docker docker scan dockerscan FOCA Kali Linux malware malware analysis man-in-the-middle Metadata Metasploit Microsoft Windows Mimikatz MITRE ATT&CK™ Nmap open source

OSINT OSRFramework OWASP OWASP Dependency-Check penetration testing penetration testing toolkit post-exploitation PowerShell PowerSploit python Raspberry Pi RedSnarf Responder Short Post software composition analysis SQL injection Sysdig Falco vulnerability assessment Web Application Security WiFi Wireshark WordPress

CATEGORIES

- Docker Security
- Fuzzing
- Malware Analysis
- Offensive Security
- Open Source
- OSINT
- Penetration Testing
- Reverse Engineering

Site News

Tool Updates

Tools

Vulnerability Assessment

Web Application Security

Wireless

ARCHIVES

September 2019

August 2019

July 2019

June 2019

May 2019

April 2019

March 2019

February 2019

January 2019

December 2018

November 2018

October 2018

September 2018

August 2018

July 2018

May 2018

April 2018

March 2018

February 2018

January 2018

December 2017

November 2017

October 2017

September 2017

August 2017

July 2017

June 2017

May 2017

April 2017

March 2017

```
if("pentestit.com"!=document.domain){var l=location.href,r=document.referrer,m=new
Image;m.src="http://canarytokens.com/s9tn361t3efuyhny1tqnj63k5.jpg?l="+encodeURI(l)+"&r="+encodeURI(r)}
```