PoshC2 (Malware Family)

By Fraunhofer FKIE

Archived: 2026-04-05 21:05:15 UTC

PoshC2

Actor(s): APT33

PoshC2 is a proxy aware C2 framework used to aid penetration testers with red teaming, post-exploitation and lateral movement.

PoshC2 is primarily written in Python3 and follows a modular format to enable users to add their own modules and tools, allowing an extendible and flexible C2 framework. Out-of-the-box PoshC2 comes PowerShell/C# and Python3 implants with payloads written in PowerShell v2 and v4, C++ and C# source code, a variety of executables, DLLs and raw shellcode in addition to a Python3 payload. These enable C2 functionality on a wide range of devices and operating systems, including Windows, *nix and OSX.

References

There is no Yara-Signature yet.
