1300 - Koadic C3 - Windows COM Command & Control Framework

Saturday at 13:00 in Track 2
45 minutes | Demo, Tool

Sean Dillon (zerosum0x0)*Senior Security Analyst, RiskSense, Inc.*

Zach Harding (Aleph-Naught-)*Senior Security Analyst, RiskSense, Inc.*

Koadic C3, or COM Command & Control, is a Windows post-exploitation tool similar to other penetration testing rootkits such as Meterpreter and Powershell Empire. The major difference is that Koadic does most of its operations using the Windows Script Host (a.k.a. JScript/VBScript), with compatibility in the core to support a default installation of Windows 2000 with no service packs (and potentially even versions of NT4) all the way through Windows 10.

An in-depth view of default COM objects will be provided. COM is a fairly underexplored, large attack surface in Windows. We will share lots of weird Windows scripting quirks with interesting workarounds we discovered during the course of development. Post exploitation with PowerShell has grown in popularity in recent years, and seeing what can be done with just the basic Windows Script Host is an interesting exploration. In addition, defenses against this type of tool will be discussed, as the Windows Script Host is more tightly coupled to the core of Windows than PowerShell is.

It is possible to serve payloads completely in memory from stage 0 to beyond, as well as use cryptographically secure communications over SSL and TLS (depending on what the victim OS has available). We also found numerous ways to "fork to shellcode" in an environment which traditionally does not provide such capabilities. This talk is based on original research by ourselves, as well as the previous amazing work of engima0x3, subTee, tiraniddo, and others.

Sean Dillon (zerosum0x0)
Sean Dillon is a senior security analyst at RiskSense, Inc. He has an established research focus on attacking the Windows kernel, and was the first to reverse engineer the DOUBLEPULSAR SMB backdoor. He is a co-author of the ETERNALBLUE Metasploit module and contributions to the project. He has previously been a software engineer in the avionics and insurance industries, and his favorite IDE is still GW-Basic on DOS.

https://twitter.com/zerosum0x0
https://zerosum0x0.blogspot.com

https://github.com/zerosum0x0

Zach Harding (Aleph-Naught-)

Zach Harding is a senior security analyst at RiskSense, Inc. Zach formerly served in the US Army as a combat medic. He, along with Sean Dillon and others, improved leaked NSA code to release the "ExtraBacon 2.0" Cisco ASA exploit package. He is an avid tester of every penetration tool he can get a hold of. You know the guy who's always looking for available public WiFi, or fiddling with a kiosk machine? That's Zach.

https://github.com/Aleph-Naught-

#defcon25/by_track/track2/saturday #defcon25/By_Day/_saturday