1000 - Persisting with Microsoft Office: Abusing Extensibility Options

Saturday at 10:00 in 101 Track
20 minutes | Demo

William Knowles*MWR InfoSecurity*

One software product that red teamers will almost certainly find on any compromised workstation is Microsoft Office. This talk will discuss the ways that native functionality within Office can be abused to obtain persistence. The following opportunities for Office-based persistence will be discussed:

(1) WLL and XLL add-ins for Word and Excel - a legacy add-in that allows arbitrary DLL loading.
(2) VBA add-ins for Excel and PowerPoint - an alternative to backdoored template files, which executes whenever the applications load.
(3) COM add-ins for all Office products - an older cross-application add-in that leverages COM objects.
(4) Automation add-ins for Excel - user defined functions that allow command execution through spreadsheet formulae.
(5) VBA editor (VBE) add-ins for all VBA using Office products - executing commands when someone tries to catch you using VBA to execute commands.
(6) VSTO add-ins for all Office products - the newer cross-application add-in that leverages a special Visual Studio runtime.

Each persistence mechanism will be discussed in terms of its relative advantages and disadvantages for red teamers. In particular, with regards to their complexity to deploy, privilege requirements, and applicability to Virtual Desktop Infrastructure (VDI) environments which hinder the use of many traditional persistence mechanisms.

The talk isn't all red - there's also some blue to satisfy the threat hunters and incident responders amongst us. The talk will finish with approaches to detection and prevention of these persistence mechanisms.
William Knowles
William Knowles is a Security Consultant at MWR InfoSecurity. He is primarily involved in purple team activities, which involves objective-based testing to simulate real-world threats, and helping organizations to identify effective defenses against them with regards to both prevention and detection. Prior to joining the security industry, he completed a PhD in

Computer Science at Lancaster University. His research interests include post-exploitation activities and offensive PowerShell.

@william_knows

#defcon25/by_track/101/saturday #defcon25/By_Day/_saturday