Office Application Startup: Add-ins

Other sub-techniques of Office Application Startup (6)

Adversaries may abuse Microsoft Office add-ins to obtain persistence on a compromised system. Office add-ins can be used to add functionality to Office programs. [1] There are different types of add-ins that can be used by the various Office products; including Word/Excel add-in Libraries (WLL/XLL), VBA add-ins, Office Component Object Model (COM) add-ins, automation add-ins, VBA Editor (VBE), Visual Studio Tools for Office (VSTO) add-ins, and Outlook add-ins. [2][3]

Add-ins can be used to obtain persistence because they can be set to execute code when an Office application starts.

ID: T1137.006

Sub-technique of: T1137

Tactic: Persistence

Platforms: Office Suite, Windows

Version: 1.2

Created: 07 November 2019

Last Modified: 15 October 2024

Version Permalink

Procedure Examples

ID	Name	Description
S0268	Bisonal	Bisonal has been loaded through a `.wll` extension added to the `%APPDATA%\microsoft\word\startup\` repository.[4]
S1143	LunarLoader	LunarLoader has the ability to use Microsoft Outlook add-ins to establish persistence. [5]
S1142	LunarMail	LunarMail has the ability to use Outlook add-ins for persistence.[5]
G0019	Naikon	Naikon has used the RoyalRoad exploit builder to drop a second stage loader, intel.wll, into the Word Startup folder on the compromised host.[6]

Mitigations

ID	Mitigation	Description
M1040	Behavior Prevention on Endpoint	On Windows 10, enable Attack Surface Reduction (ASR) rules to prevent Office applications from creating child processes and from writing potentially malicious executable content to disk. [7]

Detection

ID	Data Source	Data Component	Detects
DS0017	Command	Command Execution	Monitor executed commands and arguments that may abuse Microsoft Office add-ins to obtain persistence on a compromised system.
DS0022	File	File Creation	Monitor for newly constructed files that may abuse Microsoft Office add-ins to obtain persistence on a compromised system.
		File Modification	Monitor for changes made to files that may abuse Microsoft Office add-ins to obtain persistence on a compromised system.
DS0009	Process	Process Creation	Monitor newly executed processes that may abuse Microsoft Office add-ins to obtain persistence on a compromised system.
DS0024	Windows Registry	Windows Registry Key Creation	Audit the Registry entries relevant for enabling add-ins.[8][2]
		Windows Registry Key Modification	Audit the Registry entries relevant for enabling add-ins.[8][2]

References

1. Microsoft. (n.d.). Add or remove add-ins. Retrieved July 3, 2017.
2. Knowles, W. (2017, April 21). Add-In Opportunities for Office Persistence. Retrieved July 3, 2017.
3. Caban, D. and Hirani, M. (2018, October 3). You've Got Mail! Enterprise Email Compromise. Retrieved April 22, 2019.
4. Mercer, W., et al. (2020, March 5). Bisonal: 10 years of play. Retrieved January 26, 2022.
5. Jurčacko, F. (2024, May 15). To the Moon and back(doors): Lunar landing in diplomatic missions. Retrieved June 26, 2024.
6. CheckPoint. (2020, May 7). Naikon APT: Cyber Espionage Reloaded. Retrieved May 26, 2020.
7. Microsoft. (2021, July 2). Use attack surface reduction rules to prevent malware infection. Retrieved June 24, 2021.
8. Shukrun, S. (2019, June 2). Office Templates and GlobalDotName - A Stealthy Office Persistence Technique. Retrieved August 26, 2019.