Office Application Startup

Sub-techniques (6)

Adversaries may leverage Microsoft Office-based applications for persistence between startups. Microsoft Office is a fairly common application suite on Windows-based operating systems within an enterprise network. There are multiple mechanisms that can be used with Office for persistence when an Office-based application is started; this can include the use of Office Template Macros and add-ins.

A variety of features have been discovered in Outlook that can be abused to obtain persistence, such as Outlook rules, forms, and Home Page.[1] These persistence mechanisms can work within Outlook or be used through Office 365.[2]

ID: T1137

Sub-techniques: T1137.001, T1137.002, T1137.003, T1137.004, T1137.005, T1137.006

ⓘ

Tactic: Persistence

ⓘ

Platforms: Office Suite, Windows

Contributors: Loic Jaquemet; Microsoft Threat Intelligence Center (MSTIC); Nick Carr, Mandiant; Praetorian; Ricardo Dias; Sahar Shukrun

Version: 1.4

Created: 14 December 2017

Last Modified: 15 October 2024

Version Permalink

Procedure Examples

ID	Name	Description
G0050	APT32	APT32 have replaced Microsoft Outlook's VbaProject.OTM file to install a backdoor macro for persistence.[3] [4]
G0047	Gamaredon Group	Gamaredon Group has inserted malicious macros into existing documents, providing persistence when they are reopened. Gamaredon Group has loaded the group's previously delivered VBA project by relaunching Microsoft Outlook with the `/altvba` option, once the Application.Startup event is received.[5]

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. [6]
M1042	Disable or Remove Feature or Program	Follow Office macro security best practices suitable for your environment. Disable Office VBA macros from executing. Disable Office add-ins. If they are required, follow best practices for securing them by requiring them to be signed and disabling user notification for allowing add-ins. For some add-ins types (WLL, VBA) additional mitigation is likely required as disabling add-ins in the Office Trust Center does not disable WLL nor does it prevent VBA code from executing. [7]
M1054	Software Configuration	For the Office Test method, create the Registry key used to execute it and set the permissions to "Read Control" to prevent easy access to the key without administrator permissions or requiring Privilege Escalation. [8]
M1051	Update Software	For the Outlook methods, blocking macros may be ineffective as the Visual Basic engine used for these features is separate from the macro scripting engine.[9] Microsoft has released patches to try to address each issue. Ensure KB3191938 which blocks Outlook Visual Basic and displays a malicious code warning, KB4011091 which disables custom forms by default, and KB4011162 which removes the legacy Home Page feature, are applied to systems.[10]

Detection

ID	Data Source	Data Component	Detects
DS0015	Application Log	Application Log Content	Monitor for third-party application logging, messaging, and/or other artifacts that may leverage Microsoft Office-based applications for persistence between startups. SensePost, whose tool Ruler can be used to carry out malicious rules, forms, and Home Page attacks, has released a tool to detect Ruler usage.[11]
DS0017	Command	Command Execution	Monitor executed commands and arguments that may leverage Microsoft Office-based applications for persistence between startups. Microsoft has released a PowerShell script to safely gather mail forwarding rules and custom forms in your mail environment as well as steps to interpret the output.[12] SensePost, whose tool Ruler can be used to carry out malicious rules, forms, and Home Page attacks, has released a tool to detect Ruler usage.[11]
DS0022	File	File Creation	Monitor for newly constructed files that may leverage Microsoft Office-based applications for persistence between startups.
		File Modification	Monitor for changes made to files that may leverage Microsoft Office-based applications for persistence between startups.
DS0011	Module	Module Load	Monitor DLL/PE file events, specifically creation of these binary files as well as the loading of DLLs into processes. Look for DLLs that are not recognized or not normally loaded into a process.
DS0009	Process	Process Creation	Monitor newly executed processes that may leverage Microsoft Office-based applications for persistence between startups. Collect process execution information including process IDs (PID) and parent process IDs (PPID) and look for abnormal chains of activity resulting from Office processes. Non-standard process execution trees may also indicate suspicious or malicious behavior. If winword.exe is the parent process for suspicious processes and activity relating to other adversarial techniques, then it could indicate that the application was used maliciously.
DS0024	Windows Registry	Windows Registry Key Creation	Many Office-related persistence mechanisms require changes to the Registry and for binaries, files, or scripts to be written to disk or existing files modified to include malicious scripts. Collect events related to Registry key creation and modification for keys that could be used for Office-based persistence.[13][14]
		Windows Registry Key Modification	Many Office-related persistence mechanisms require changes to the Registry and for binaries, files, or scripts to be written to disk or existing files modified to include malicious scripts. Collect events related to Registry key creation and modification for keys that could be used for Office-based persistence.[13][14]