Office Application Startup: Office Template Macros

Other sub-techniques of Office Application Startup (6)

Adversaries may abuse Microsoft Office templates to obtain persistence on a compromised system. Microsoft Office contains templates that are part of common Office applications and are used to customize styles. The base templates within the application are used each time an application starts. [1]

Office Visual Basic for Applications (VBA) macros [2] can be inserted into the base template and used to execute code when the respective Office application starts in order to obtain persistence. Examples for both Word and Excel have been discovered and published. By default, Word has a Normal.dotm template created that can be modified to include a malicious macro. Excel does not have a template file created by default, but one can be added that will automatically be loaded.[3][4] Shared templates may also be stored and pulled from remote locations.[5]

Word Normal.dotm location:
`C:\Users\<username>\AppData\Roaming\Microsoft\Templates\Normal.dotm`

Excel Personal.xlsb location:
`C:\Users\<username>\AppData\Roaming\Microsoft\Excel\XLSTART\PERSONAL.XLSB`

Adversaries may also change the location of the base template to point to their own by hijacking the application's search order, e.g. Word 2016 will first look for Normal.dotm under `C:\Program Files (x86)\Microsoft Office\root\Office16\`, or by modifying the GlobalDotName registry key. By modifying the GlobalDotName registry key an adversary can specify an arbitrary location, file name, and file extension to use for the template that will be loaded on application startup. To abuse GlobalDotName, adversaries may first need to register the template as a trusted document or place it in a trusted location.[5]

An adversary may need to enable macros to execute unrestricted depending on the system or enterprise security policy on use of macros.

ID: T1137.001

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
S0475	BackConfig	BackConfig has the ability to use hidden columns in Excel spreadsheets to store executable files or commands for VBA macros.[6]
S0154	Cobalt Strike	Cobalt Strike has the ability to use an Excel Workbook to execute additional code by enabling Office to trust macros and execute code without user permission.[7]
G0069	MuddyWater	MuddyWater has used a Word Template, Normal.dotm, for persistence.[8]

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. [9]
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. [10]

Detection

ID	Data Source	Data Component	Detects
DS0017	Command	Command Execution	Monitor executed commands and arguments that may abuse Microsoft Office templates to obtain persistence on a compromised system.
DS0022	File	File Creation	Monitor for newly constructed files that may abuse Microsoft Office templates to obtain persistence on a compromised system.
		File Modification	Monitor for changes made to files that may abuse Microsoft Office templates to obtain persistence on a compromised system. Modification to base templates, like Normal.dotm, should also be investigated since the base templates should likely not contain VBA macros. Changes to the Office macro security settings should also be investigated
DS0009	Process	Process Creation	Monitor newly executed processes that may abuse Microsoft Office templates to obtain persistence on a compromised system.
DS0024	Windows Registry	Windows Registry Key Creation	Collect events related to Registry key creation for keys that could be used for Office-based persistence.[11][12]
		Windows Registry Key Modification	Collect events related to Registry key modification for keys that could be used for Office-based persistence.[11][12]

References

1. Microsoft. (n.d.). Change the Normal template (Normal.dotm). Retrieved July 3, 2017.
2. Austin, J. (2017, June 6). Getting Started with VBA in Office. Retrieved July 3, 2017.
3. Nelson, M. (2014, January 23). Maintaining Access with normal.dotm. Retrieved July 3, 2017.
4. Hexacorn. (2017, April 17). Beyond good ol' Run key, Part 62. Retrieved July 3, 2017.
5. Shukrun, S. (2019, June 2). Office Templates and GlobalDotName - A Stealthy Office Persistence Technique. Retrieved August 26, 2019.
6. Hinchliffe, A. and Falcone, R. (2020, May 11). Updated BackConfig Malware Targeting Government and Military Organizations in South Asia. Retrieved June 17, 2020.
7. Mavis, N. (2020, September 21). The Art and Science of Detecting Cobalt Strike. Retrieved September 12, 2024.
8. Reaqta. (2017, November 22). A dive into MuddyWater APT targeting Middle-East. Retrieved May 18, 2020.
9. Microsoft. (2021, July 2). Use attack surface reduction rules to prevent malware infection. Retrieved June 24, 2021.
10. Knowles, W. (2017, April 21). Add-In Opportunities for Office Persistence. Retrieved July 3, 2017.
11. Parisi, T., et al. (2017, July). Using Outlook Forms for Lateral Movement and Persistence. Retrieved February 5, 2019.
12. Soutcast. (2018, September 14). Outlook Today Homepage Persistence. Retrieved February 5, 2019.