Office Application Startup: Outlook Home Page

Other sub-techniques of Office Application Startup (6)

Adversaries may abuse Microsoft Outlook's Home Page feature to obtain persistence on a compromised system. Outlook Home Page is a legacy feature used to customize the presentation of Outlook folders. This feature allows for an internal or external URL to be loaded and presented whenever a folder is opened. A malicious HTML page can be crafted that will execute code when loaded by Outlook Home Page. [1]

Once malicious home pages have been added to the user's mailbox, they will be loaded when Outlook is started. Malicious Home Pages will execute when the right Outlook folder is loaded/reloaded.[1]

ID: T1137.004

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
G0049	OilRig	OilRig has abused the Outlook Home Page feature for persistence. OilRig has also used CVE-2017-11774 to roll back the initial patch designed to protect against Home Page abuse.[2]
S0358	Ruler	Ruler can be used to automate the abuse of Outlook Home Pages to establish persistence.[3]

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. [4]
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.[5] 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.[1]

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 abuse Microsoft Outlook's Home Page feature to obtain persistence on a compromised system. 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.[6]
DS0017	Command	Command Execution	Monitor executed commands and arguments that may abuse Microsoft Outlook's Home Page feature to obtain persistence on a compromised system. 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.[7]
DS0009	Process	Process Creation	Monitor newly executed processes that may abuse Microsoft Outlook's Home Page feature to obtain persistence on a compromised system.

References

1. Stalmans, E. (2017, October 11). Outlook Home Page – Another Ruler Vector. Retrieved February 4, 2019.
2. McWhirt, M., Carr, N., Bienstock, D. (2019, December 4). Breaking the Rules: A Tough Outlook for Home Page Attacks (CVE-2017-11774). Retrieved June 23, 2020.
3. SensePost. (2016, August 18). Ruler: A tool to abuse Exchange services. Retrieved February 4, 2019.
4. Microsoft. (2021, July 2). Use attack surface reduction rules to prevent malware infection. Retrieved June 24, 2021.
5. Stalmans, E. (2017, April 28). Outlook Forms and Shells. Retrieved February 4, 2019.
6. SensePost. (2017, September 21). NotRuler - The opposite of Ruler, provides blue teams with the ability to detect Ruler usage against Exchange. Retrieved February 4, 2019.
7. Fox, C., Vangel, D. (2018, April 22). Detect and Remediate Outlook Rules and Custom Forms Injections Attacks in Office 365. Retrieved February 4, 2019.