Threat Thursday: Malicious Macros Still Causing Chaos

blogs.blackberry.com/en/2022/03/threat-thursday-malicious-macros

The BlackBerry Research & Intelligence Team

Documents and spreadsheets may seem like innocuous, fancified text files. But with the presence of macros, they have the capability within them to cause great pain.

Malicious macros are a tool used by well-known threat actors such as APT28 and Muddy Water to gain entry to target systems, yet they have been around and causing trouble for decades. And while Microsoft® Office has recently made some changes to its default behavior, blocking several common macro threat vectors, certain Windows Startup techniques commonly used by cyber criminals have yet to be addressed.

These startup techniques abuse built-in features of Office in a way that lets adversaries establish persistence on a victim's system. Because the macros will infect other files that the victim uses after the initial file is opened, this can make the malicious code hard to purge.

Operating System

Windows	MacOS	Linux	Android
Yes	No	No	No

Risk & Impact

Impact	High
Risk	Medium

What are VBA Macros?

Visual Basic for Application (VBA) is a scripting language for use within Microsoft Office documents. It allows you to include code that does everything you can normally do on your computer. Most casual users might think of Office as “just” for making simple documents and spreadsheets, but it's actually an incredibly powerful, potentially operating system-agnostic format that makes doing things behind the scenes very "user-friendly" (for better or for worse).

It might help if you think of an Office file as a file system, rather than just a single file. You can rename a .DOCX file to .ZIP and unpack it like you would a regular ZIP file. And within that structure, you can embed things like scripts, images, PDF files and even EXE files, all of which can be weaponized by bad actors.

Technical Analysis

Adversaries will always prefer to achieve persistence on a victim’s machine over having to re-infect it, as repeated deployment of malware is less efficient and more likely to get them caught by defenders.

Today we will be looking at two methods that are specific to Microsoft Office macros:

Office Test (MITRE ATT&CK - T1137.002)

Office Template Macros (MITRE ATT&CK - T1137.001)

Office Test

Office Test is a simple registry key that can be abused to load arbitrary DLLs whenever an Office application is started. These keys are not installed by default, and are believed to be loaded as part of a Microsoft internal automation and testing suite.

Writing to either of the following two registry keys will allow a DLL at the path value specified to be loaded during the startup of all Office products, every time the applications are opened, without any security warnings or any user authorizations required.

- HKEY_CURRENT_USER\Software\Microsoft\Office test\Special\Perf
- HKEY_LOCAL_MACHINE\Software\Microsoft\Office test\Special\Perf

Office Template Macros

Office Template Macros are a startup technique that is much more familiar and prevalent. This tactic leverages the fact that every Office document is based on a template file, even brand-new, “blank” files, such as the empty page you see when you open a new Word document.

A huge number of virus families have used this tactic over the years, with a few notable examples. The Concept virus was the first macro virus. It tampered with Microsoft® Word’s global template file, which was named “Normal.dot” at the time. The Laroux virus came soon after, bringing the technique to Excel® spreadsheets on Windows® machines.

For many years, macro viruses were all but extinct, after Microsoft disabled macros by default on all documents in the early 2000s. However, this feature was turned off by many companies that used in-house (that is to say, useful and benign) macros. Threat actors soon wised up to the fact that they could simply ask victims to click the “enable” button that was right there on the notification message from Microsoft, allowing their creations to execute. Before long, this tactic had once again reached its former glory and was employed by a multitude of threat actors.

We still see customers being hit by threats from before the “macro extinction,” such as Divi. And newer threats that have only been around for a couple years, such as Modfek, are still causing significant pain.

Templates and Startup Functionality

The Office template attack consists of an attacker placing a malicious, macro-enabled document in the folder that the Office product uses to store its templates. Placing it here will cause this base document and its macros to be loaded every time the program is opened.

For Word, this location is:

%AppData%\Roaming\Microsoft\Templates\Normal.dotm

For Excel, this location is:

%AppData%\Roaming\Microsoft\Excel\XLSTART\$NAME$.XLSB

The name must be specifically “Normal.dotm” in recent versions of Word. However, in the Excel folder, the name of the file is irrelevant, though the default in recent versions of Excel is “Personal.xlsb”.

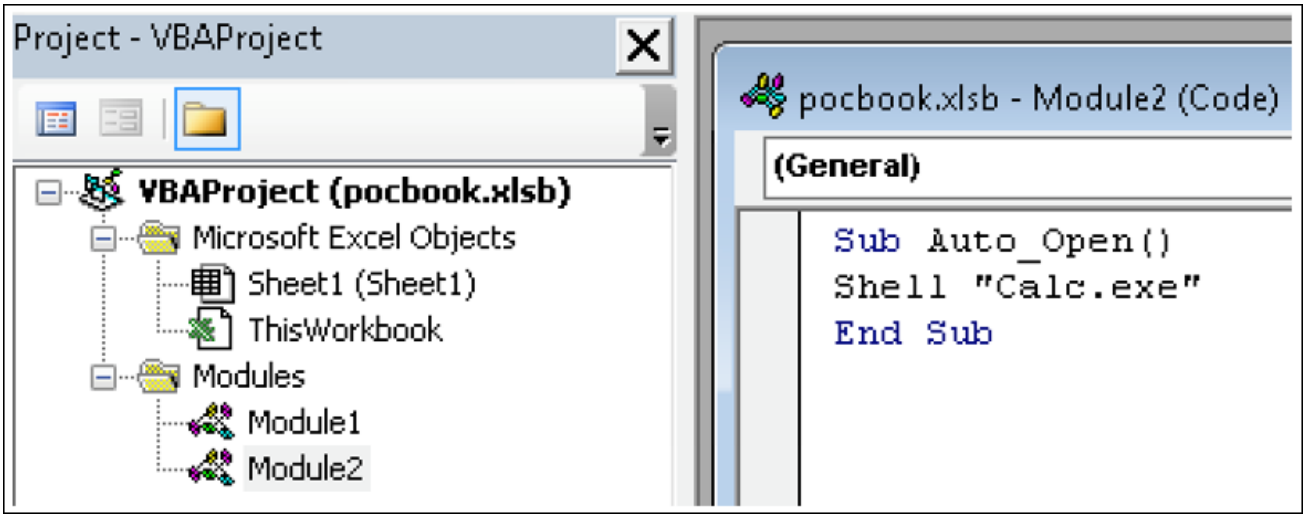

Figure 1 - Simple proof of concept macro to open Calculator, as a benign example of code execution

Now that the template file is infected, any notebook that is opened will execute this VBA code.

Some macro viruses, like Modfek, take this a step further and will write macros to any subsequent files that are opened. This allows a persistence mechanism to move back and forth, so that it will continue to persist even if the template is cleaned out.

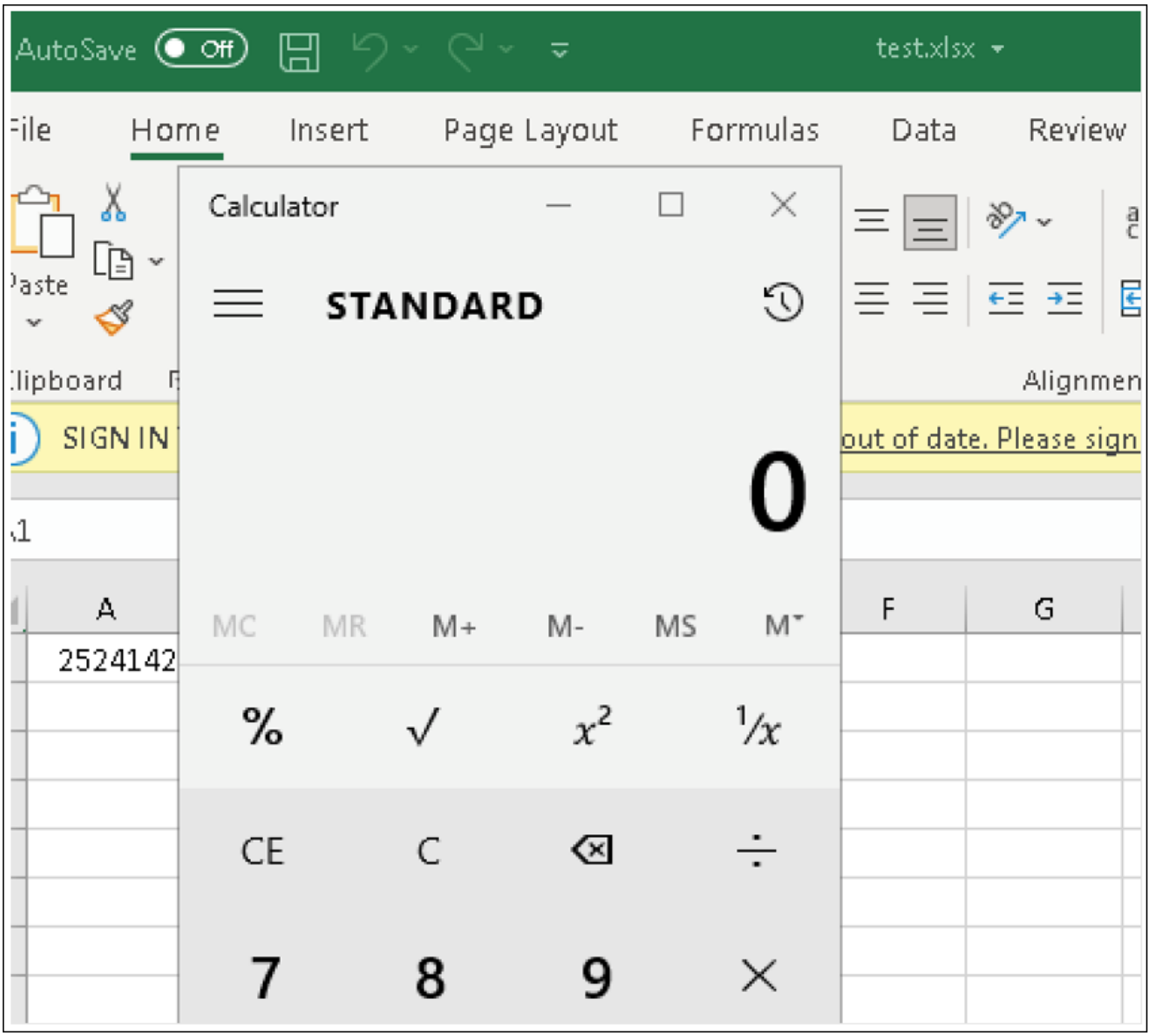

Figure 2 - The macro runs without the security ribbon

This execution happens without any macro warning or necessary authorization by the victim. This occurs without settings needing to be changed in the macro policy.

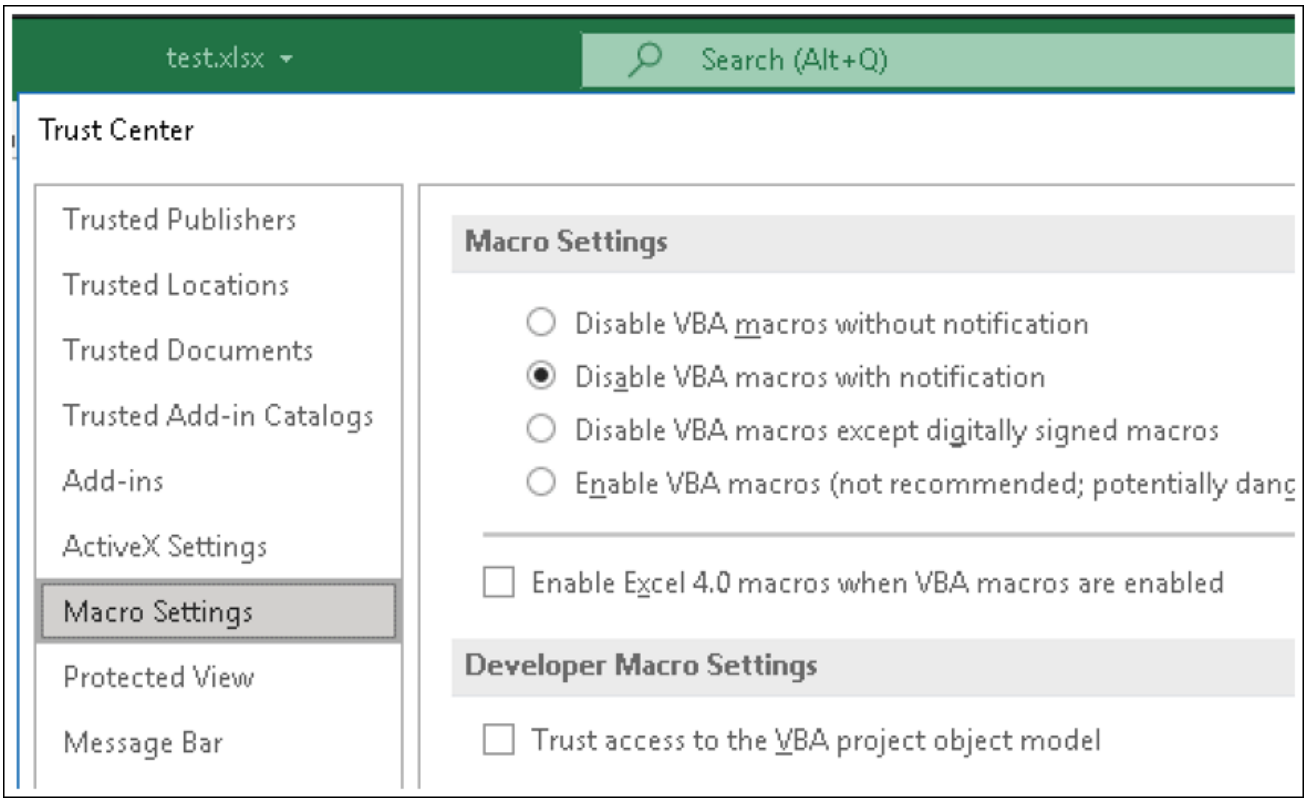

Figure 3 - The behavior has overridden the defined Macro Settings

Many macro viruses use their code to check if the Startup folder is infected, and if not, to add its code to the template.

Several aspects of the Office Startup directory are configurable through registry keys in the following location.

HKCU\Software\Microsoft\Office\<version>\Common\General

The “Xlstart” key controls the template location for Excel (shown in Figure 4 with the value changed to TEMP), and the “Startup” key controls the template location for Word files.

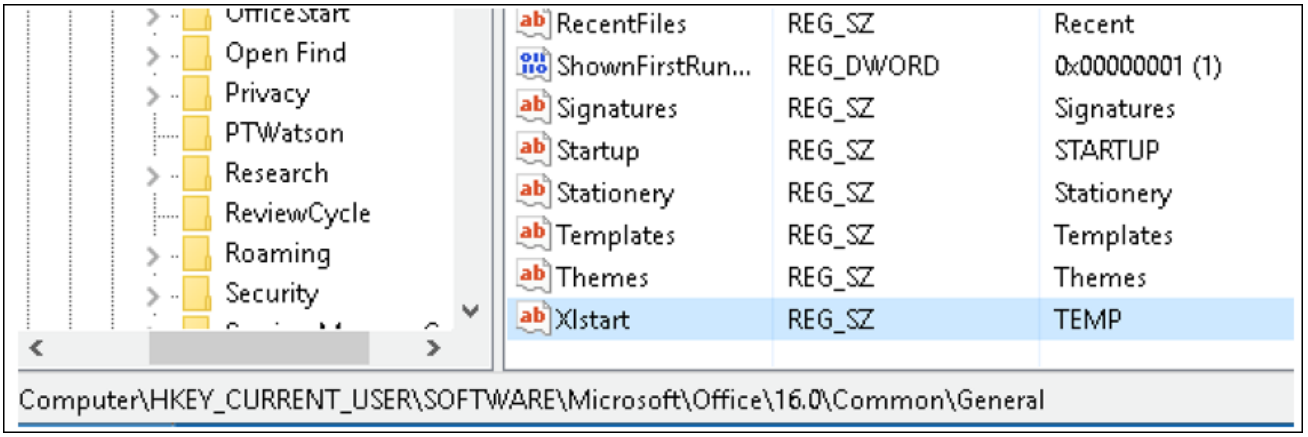

Figure 4 - Registry keys for configuring startup folders

Conclusion

Microsoft will soon begin natively blocking macros on files sourced from the Internet, with a stronger warning that makes it harder to re-enable this functionality. While this could reduce the impact of some of the attack features, macros in startup documents still have the ability to bypass the security policy set by users. It is unclear when or whether this will be fixed by Microsoft.

A few of the changes in the upcoming update to macro functionality seem to prioritize usability over the security of this policy. For example, saving files (even from the Internet) to any Trusted Location will make Office ignore this policy, and it will open the files with VBA enabled.

Microsoft does not plan to roll this out to most users until Summer 2022, and fixes for Office versions LTSC 2021, 2019, 2016, and 2013 have not yet been revealed.

The question also remains why all macros are being disabled rather than just removing "Auto" functions, as these tend to be the top choice for malicious activity in Office files.

Until this is sorted, there are several other mitigation tactics you can take.

Mitigation

Registry key permissions should be in line with least privilege for their respective users, which can include creation and lockdown of non-default option keys. Furthermore, monitoring of value changes to unusual keys should create potential events. These same protections should be enacted on the modification of template files themselves, as appropriate to the organization.

A number of Microsoft Attack Surface Reduction rules can be used to limit different functionalities of Office, including:

- Office apps launching child processes
- Office apps/macros creating executable content
- Office apps injecting code into other processes
- Win32 imports from Office macro code – block Win32 API calls from Office

CylanceOPTICS® provides the following XDR rule to combat these threats:

office_application_startup_mitre

BlackBerry Assistance

If you're battling this malware or a similar threat, you've come to the right place, regardless of your existing BlackBerry relationship.

The BlackBerry Incident Response team is made up of world-class consultants dedicated to handling response and containment services for a wide range of incidents, including ransomware and Advanced Persistent Threat (APT) cases.

We have a global consulting team standing by to assist you, providing around-the-clock support where required, as well as local assistance. Please contact us here: https://www.blackberry.com/us/en/forms/cylance/handraiser/emergency-incident-response-containment

About The BlackBerry Research & Intelligence Team

The BlackBerry Research & Intelligence team examines emerging and persistent threats, providing intelligence analysis for the benefit of defenders and the organizations they serve.

Back