What Is Registry Abuse in Malware?

The Windows Registry is an important part of the operating system. It stores configuration settings that determine how Windows behaves, how software runs, and even how users interact with the system. From startup routines to driver settings and user preferences, the registry touches almost every part of the OS.

As it's central, the registry is also a target for malware authors. By modifying registry keys and values, malware can silently manipulate system behavior to:

- **Stay persistent** by adding itself to autorun keys, it ensures execution every time the system boots.
- **Hide from users** disabling Task Manager, hiding file extensions, or suppressing warnings to avoid detection.
- **Weaken security** turning off Windows Defender or blocking updates to bypass protection.
- **Control user behavior** redirecting browser traffic, setting fake proxies, or hijacking default apps.

The Fastest Way to Spot Registry Abuse inside ANY.RUN Sandbox

Traditional security tools often miss subtle but critical signs of registry abuse, especially when malware hides behind scripts or legitimate-looking processes.

By running suspicious files or links inside ANY.RUN's interactive sandbox, analysts can observe real-time registry changes as they happen, without waiting for static scans to catch up.

Why It's So Effective:

- **Instant visibility** into registry modifications, autorun key changes, and process behaviors
- **Behavior-based detection**, not just signatures; perfect for catching new or obfuscated threats
- **Clear labeling and process tree** that highlight when a script or binary tampers with the registry
- **Integrated threat intelligence** tags (e.g., FormBook) to identify malware families quickly
- **Interactive control**, so you can simulate real user actions that trigger registry abuse (like opening a file or clicking a button)

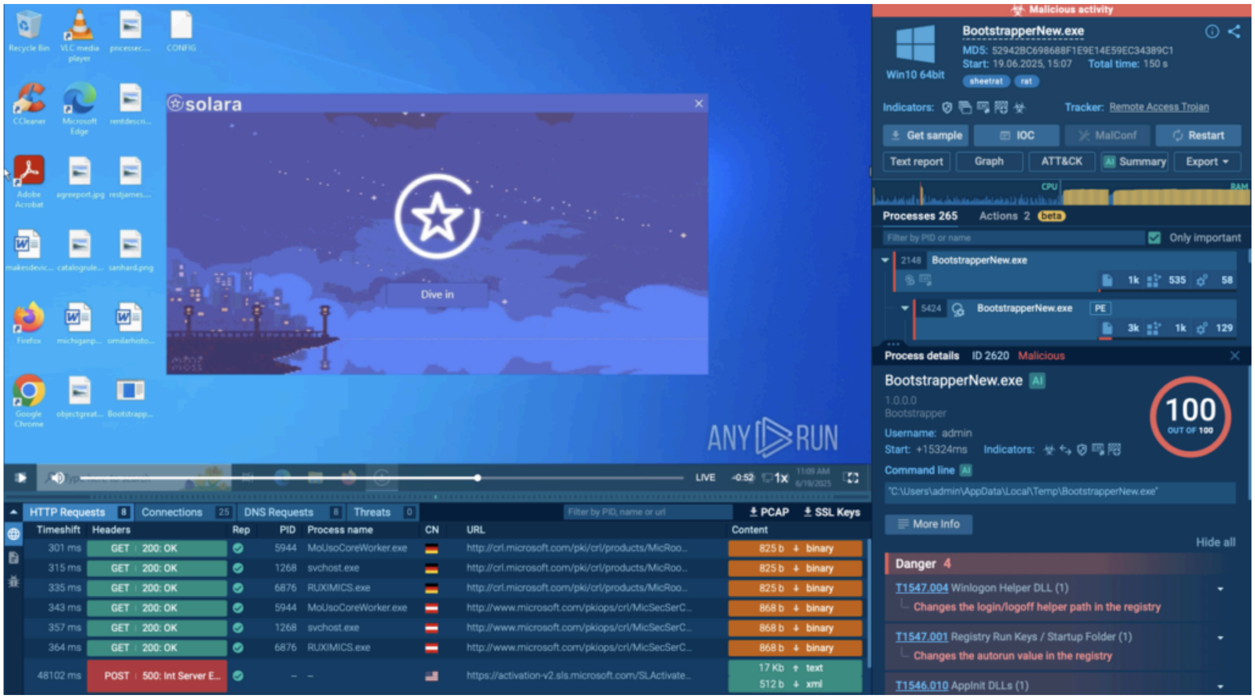
Real-World Examples of Registry Abuse in Malware

Now, let’s look at how malware abuses the registry in practice and how ANY.RUN makes it easy to detect.

1. Persistence via Autorun Key Modification

This sample shows how the malware (BootstrapperNew.exe) abuses the registry to ensure it launches automatically every time the system boots; a classic persistence mechanism.

View analysis session



BootstrapperNew.exe
MD5: 52942BC698688F1E9E14E59EC34389C1
Start: 19.06.2025, 15:07 Total time: 150 s
Tracker: Remote Access Trojan

2148 BootstrapperNew.exe 1k 535 58
5424 BootstrapperNew.exe 3k 1k 129

Process details ID 2620 Malicious

BootstrapperNew.exe
1.0.0.0
Bootstrapper
Username: admin
Start: +15324ms
100 OUT OF 100
Command line
"C:\Users\admin\AppData\Local\Temp\BootstrapperNew.exe"

Danger 4
T1547.004 Winlogon Helper DLL (1)
Changes the login/logoff helper path in the registry
T1547.001 Registry Run Keys / Startup Folder (1)
Changes the autorun value in the registry
T1546.010 AppInit DLLs (1)

Timeshift	Headers	Rep	PID	Process name	CN	URL	Content
301 ms	GET 200: OK	✓	5944	MoUsoCoreWorker.exe		http://crl.microsoft.com/pki/crl/products/MicRoo...	825 b binary
315 ms	GET 200: OK	✓	1268	svchost.exe		http://crl.microsoft.com/pki/crl/products/MicRoo...	825 b binary
335 ms	GET 200: OK	✓	6876	RUXIMICS.exe		http://crl.microsoft.com/pki/crl/products/MicRoo...	825 b binary
343 ms	GET 200: OK	✓	5944	MoUsoCoreWorker.exe		http://www.microsoft.com/pkiops/crl/MicSecSerC...	868 b binary
357 ms	GET 200: OK	✓	1268	svchost.exe		http://www.microsoft.com/pkiops/crl/MicSecSerC...	868 b binary
364 ms	GET 200: OK	✓	6876	RUXIMICS.exe		http://www.microsoft.com/pkiops/crl/MicSecSerC...	868 b binary
48102 ms	POST 500: Int Server E...	✓	–	–		https://activation-v2.sls.microsoft.com/SLActivate...	17 Kb text 512 b xml

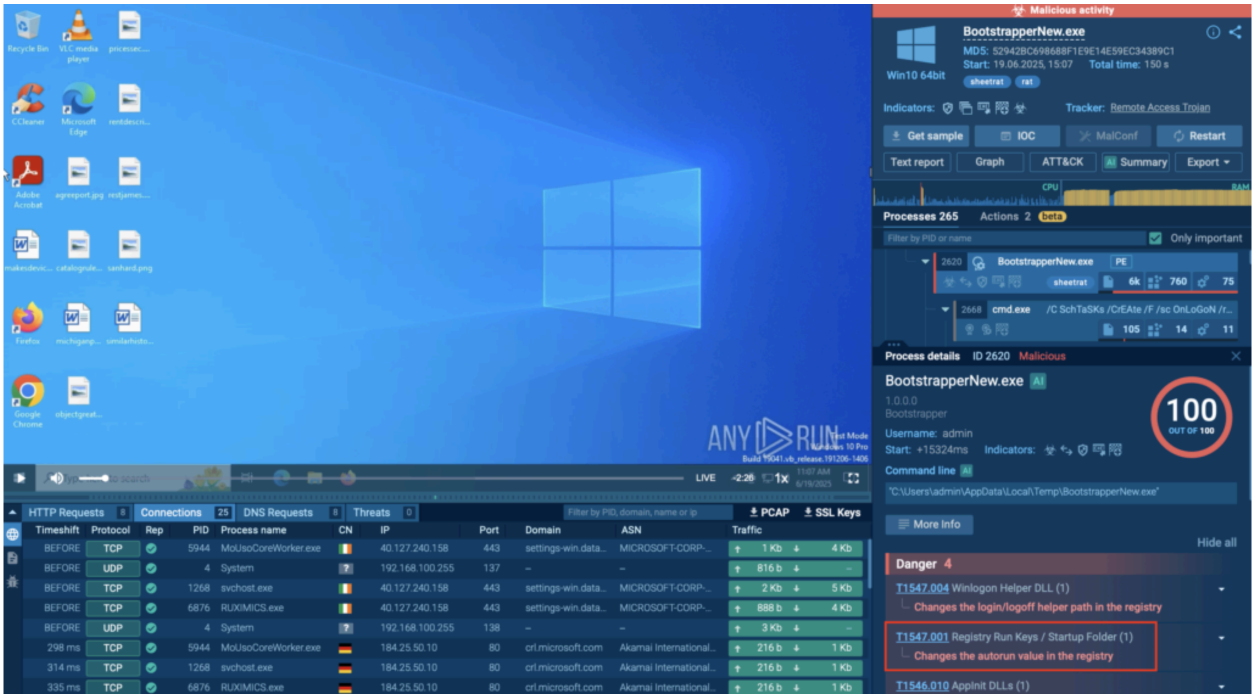
As shown in the analysis, the malware modifies the following registry key:

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run

It adds a new value:

- Name: BootstrapperNew
- Value: C:\Users\admin\AppData\Roaming\Windows\BootstrapperNew.exe
- Operation: Write
- Type: REG_NONE

You can check all these details by checking the “BootstrapperNew.exe” process from the right part of the screen.



BootstrapperNew.exe
MD5: 52942BC698688F1E9E14E59EC34389C1
Start: 19.06.2025, 15:07 Total time: 150 s

Indicators: Tracker: Remote Access Trojan

2620 BootstrapperNew.exe sheetrat 6k 760 75

2668 cmd.exe /C SchTaSKs /CrEAte /F /sc OnLoGoN /r... 105 14 11

Timeshift	Protocol	Rep	PID	Process name	CN	IP	Port	Domain	ASN	Traffic
BEFORE	TCP	✓	5944	MoUsoCoreWorker.exe		40.127.240.158	443	settings-win.data...	MICROSOFT-CORP-...	↑ 1 Kb ↓ 4 Kb
BEFORE	UDP	✓	4	System	?	192.168.100.255	137	–	–	↑ 816 b ↓ –
BEFORE	TCP	✓	1268	svchost.exe		40.127.240.158	443	settings-win.data...	MICROSOFT-CORP-...	↑ 2 Kb ↓ 5 Kb
BEFORE	TCP	✓	6876	RUXIMICS.exe		40.127.240.158	443	settings-win.data...	MICROSOFT-CORP-...	↑ 888 b ↓ 4 Kb
BEFORE	UDP	✓	4	System	?	192.168.100.255	138	–	–	↑ 3 Kb ↓ –
298 ms	TCP	✓	5944	MoUsoCoreWorker.exe		184.25.50.10	80	crl.microsoft.com	Akamai International...	↑ 216 b ↓ 1 Kb
314 ms	TCP	✓	1268	svchost.exe		184.25.50.10	80	crl.microsoft.com	Akamai International...	↑ 216 b ↓ 1 Kb
335 ms	TCP	✓	6876	RUXIMICS.exe		184.25.50.10	80	crl.microsoft.com	Akamai International...	↑ 216 b ↓ 1 Kb

Process details ID 2620 Malicious

BootstrapperNew.exe AI
1.0.0.0
Bootstrapper
Username: admin
Start: +15324ms Indicators:

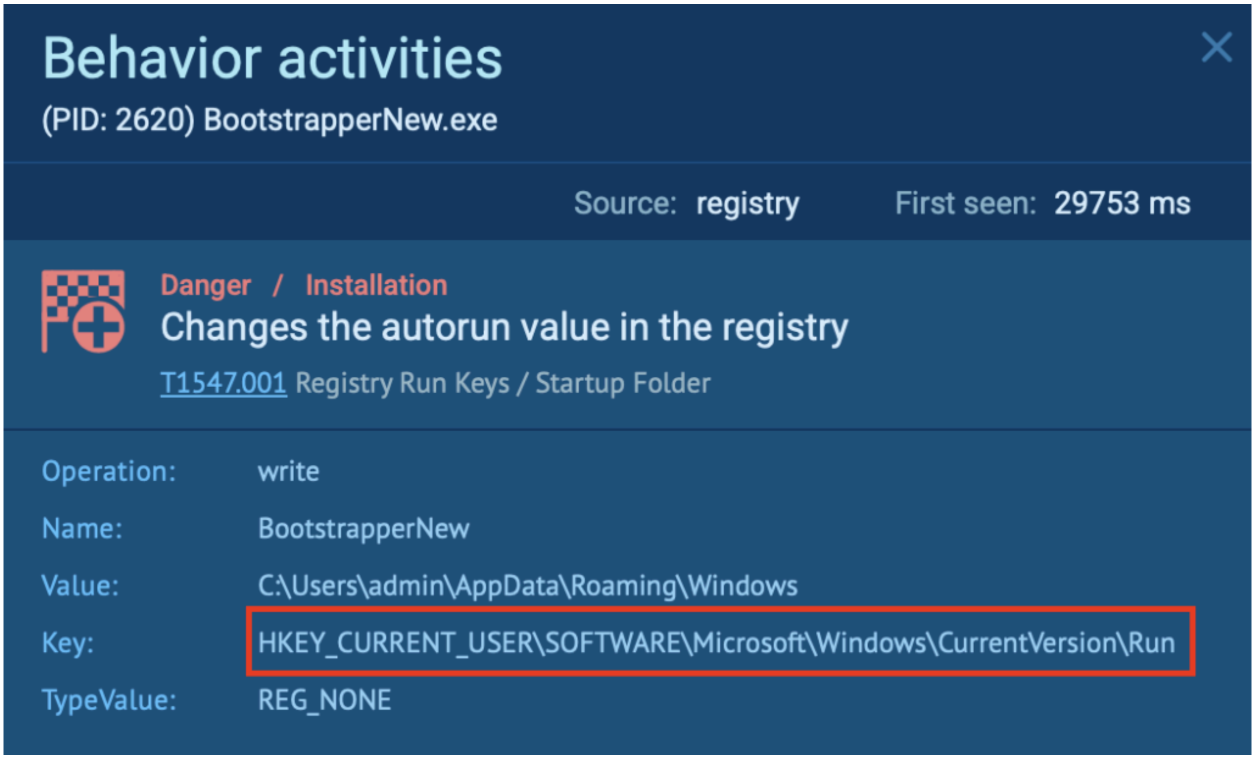
100 OUT OF 100

Command line AI
"C:\Users\admin\AppData\Local\Temp\BootstrapperNew.exe"

Danger 4
T1547.004 Winlogon Helper DLL (1)
Changes the login/logoff helper path in the registry
T1547.001 Registry Run Keys / Startup Folder (1)
Changes the autorun value in the registry
T1546.010 AppInit DLLs (1)

BootstrapperNew.exe process with its details demonstrated inside ANY.RUN sandbox

Click on the tactic to get all the details:



Behavior activities

(PID: 2620) BootstrapperNew.exe

Source: registry First seen: 29753 ms

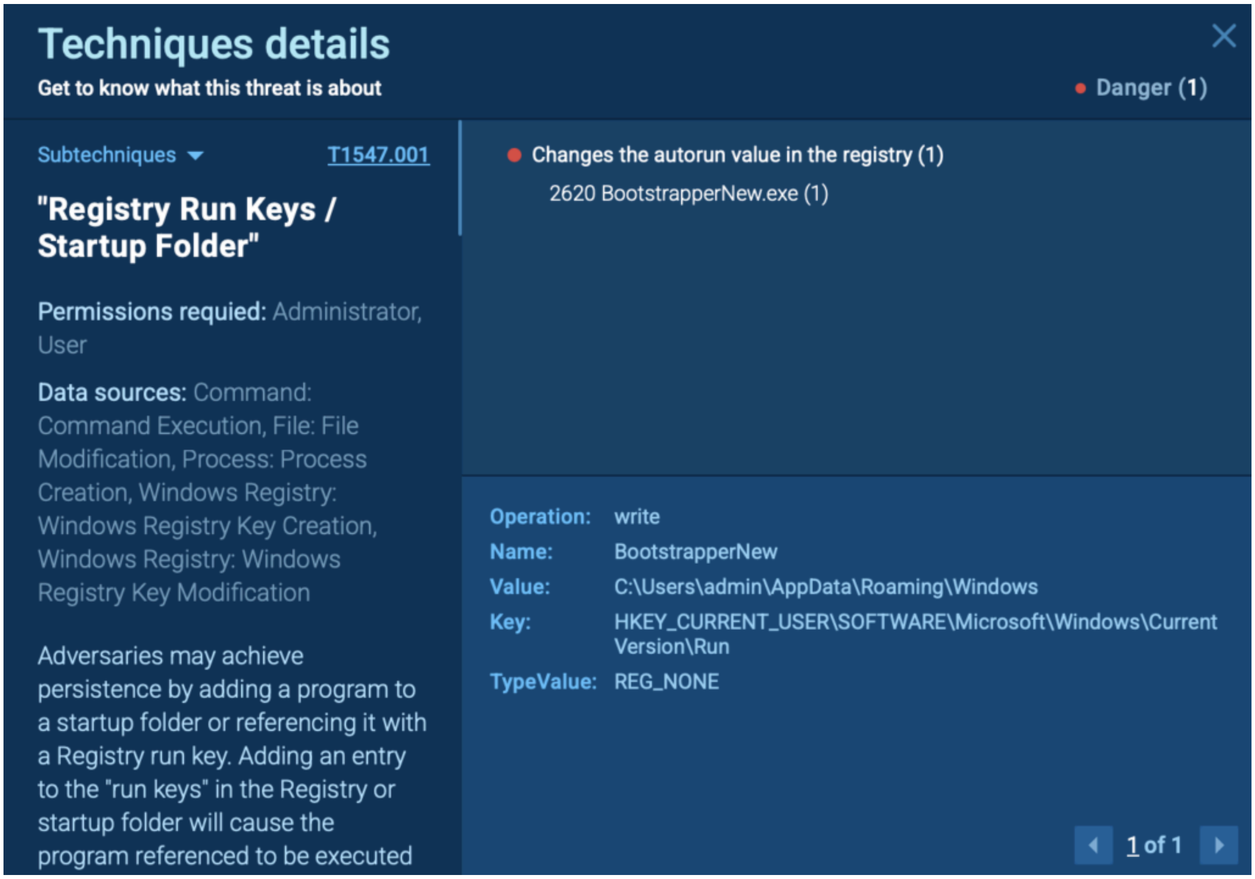
Danger / Installation
Changes the autorun value in the registry
T1547.001 Registry Run Keys / Startup Folder

Operation:	write
Name:	BootstrapperNew
Value:	C:\Users\admin\AppData\Roaming\Windows
Key:	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
TypeValue:	REG_NONE

Modification of the mentioned registry key

This modification triggers Windows to execute the malicious file at every user login, giving the attacker a reliable foothold on the system.

ANY.RUN also flags this behavior with the MITRE ATT&CK sub-technique T1547.001 (Registry Run Keys / Startup Folder), clearly highlighting the persistence mechanism used. The visual process tree further confirms the execution flow, registry operation, and background network activity.



Techniques details

Get to know what this threat is about

● Danger (1)

Subtechniques ▾ T1547.001

"Registry Run Keys / Startup Folder"

Permissions requied: Administrator, User

Data sources: Command: Command Execution, File: File Modification, Process: Process Creation, Windows Registry: Windows Registry Key Creation, Windows Registry: Windows Registry Key Modification

Adversaries may achieve persistence by adding a program to a startup folder or referencing it with a Registry run key. Adding an entry to the "run keys" in the Registry or startup folder will cause the program referenced to be executed

● Changes the autorun value in the registry (1)

2620 BootstrapperNew.exe (1)

Operation:	write
Name:	BootstrapperNew
Value:	C:\Users\admin\AppData\Roaming\Windows
Key:	HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\Current Version\Run
TypeValue:	REG_NONE

MITRE ATT&CK technique discovered inside ANY.RUN sandbox

With static detection tools, this behavior might go unnoticed. But in ANY.RUN's sandbox, the threat is immediately identified, tagged, and visually traceable in real time, from registry edit to scheduled task creation.

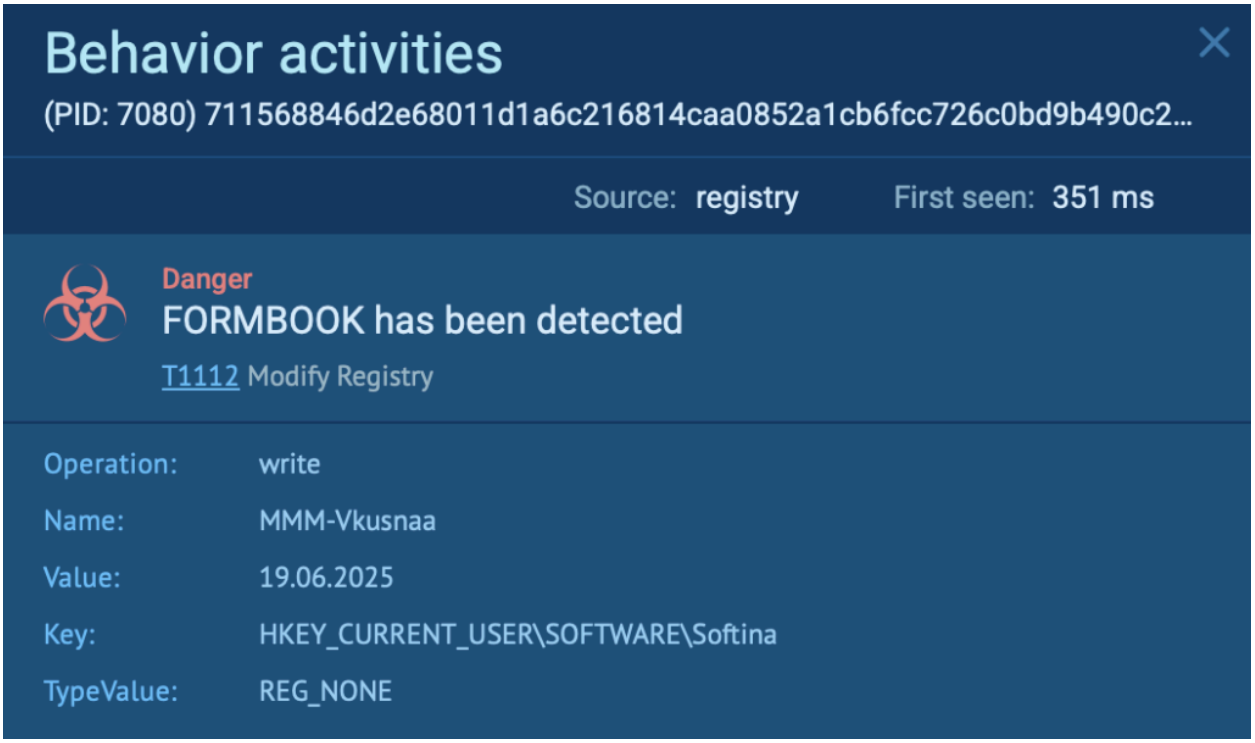
2. FormBook Stealer Using Registry for Stealth

In this example, the malware identified as **FormBook** manipulates the Windows Registry to aid in **stealth and persistence**.

View analysis session

Right after execution, FormBook writes a new registry entry under:

- Key: HKEY_CURRENT_USER\SOFTWARE\Softina
- Name: MMM-Vkusnaa
- Value: 19.06.2025



Behavior activities

(PID: 7080) 711568846d2e68011d1a6c216814caa0852a1cb6fcc726c0bd9b490c2...

Source: registry First seen: 351 ms

Danger

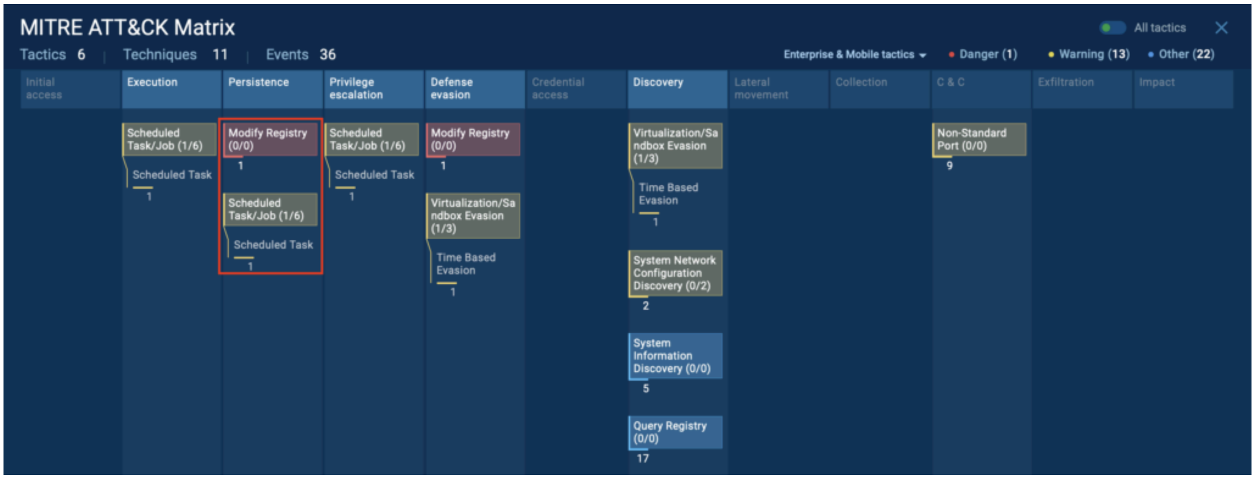
FORMBOOK has been detected

T1112 Modify Registry

Operation:	write
Name:	MMM-Vkusnaa
Value:	19.06.2025
Key:	HKEY_CURRENT_USER\SOFTWARE\Softina
TypeValue:	REG_NONE

Formbook detected with modified registry key

Custom registry values like this aren’t random. They’re typically placed in obscure subkeys (SOFTWARE\Softina in this case) to avoid detection and logging by standard monitoring tools, but in ANY.RUN’s sandbox, it’s instantly visible and tied to MITRE technique **T1112: Modify Registry**.



MITRE ATT&CK Matrix

Tactics 6 | Techniques 11 | Events 36

All tactics

Enterprise & Mobile tactics ● Danger (1) ● Warning (13) ● Other (22)

Initial access	Execution	Persistence	Privilege escalation	Defense evasion	Credential access	Discovery	Lateral movement	Collection	C & C	Exfiltration	Impact
	Scheduled Task/Job (1/6) Scheduled Task 1	Modify Registry (0/0) 1 Scheduled Task/Job (1/6) Scheduled Task 1	Scheduled Task/Job (1/6) Scheduled Task 1	Modify Registry (0/0) 1 Virtualization/Sandbox Evasion (1/3) Time Based Evasion 1		Virtualization/Sandbox Evasion (1/3) Time Based Evasion 1 System Network Configuration Discovery (0/2) 2 System Information Discovery (0/0) 5 Query Registry (0/0) 17			Non-Standard Port (0/0) 9		

MITRE technique T1112: Modify Registry inside ANY.RUN sandbox

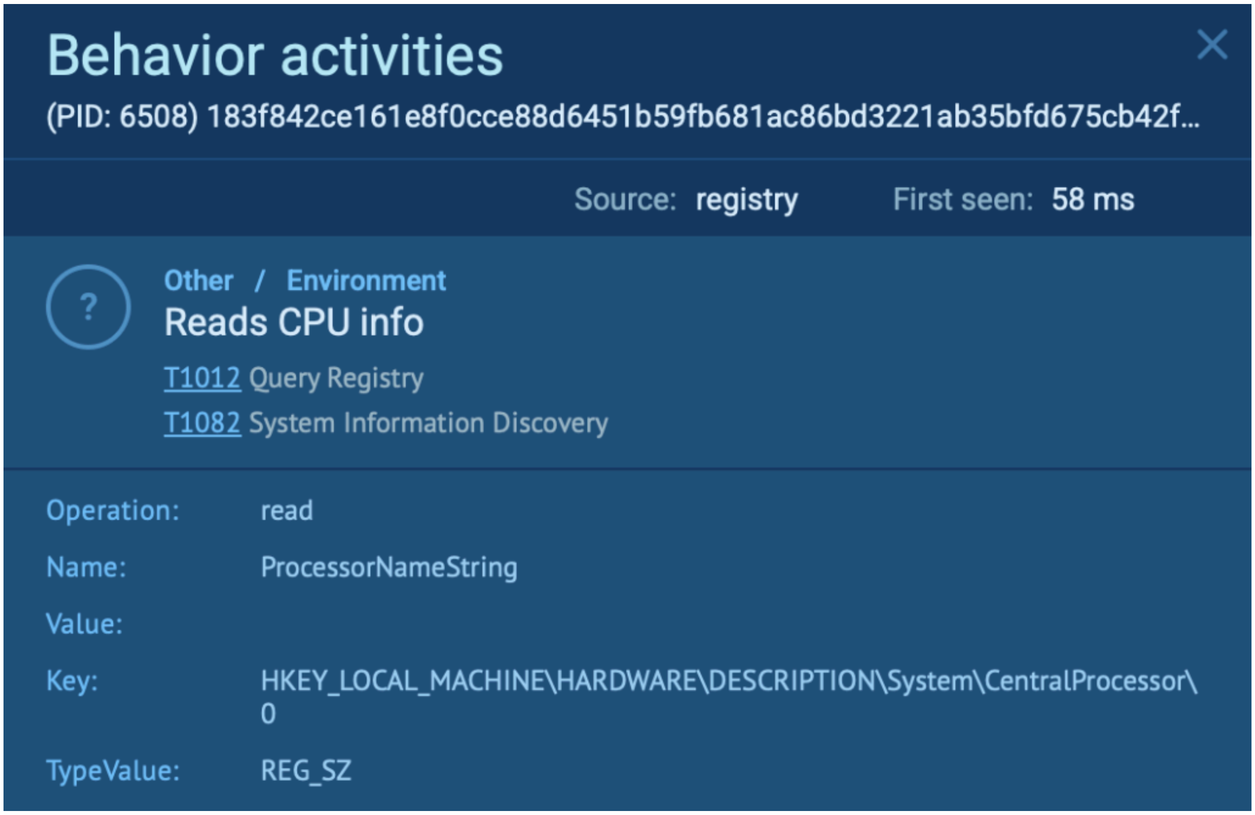
3. System Profiling Through Registry Access

Some malware doesn’t act immediately. Instead, it quietly profiles the environment to decide **how (or whether)** to execute. That’s exactly what we see in this sample, where the malware queries the registry to gather detailed system information.

View analysis session

One of the first actions taken is a read operation targeting:

- Key: HKEY_LOCAL_MACHINE\HARDWARE\DESCRIPTION\System\CentralProcessor\0
- Name: ProcessorNameString



Behavior activities

(PID: 6508) 183f842ce161e8f0cce88d6451b59fb681ac86bd3221ab35bfd675cb42f...

Source: registry First seen: 58 ms

Other / Environment

Reads CPU info

T1012 Query Registry

T1082 System Information Discovery

Operation:	read
Name:	ProcessorNameString
Value:	
Key:	HKEY_LOCAL_MACHINE\HARDWARE\DESCRIPTION\System\CentralProcessor\0
TypeValue:	REG_SZ

Malware reading CPU info exposed inside ANY.RUN sandbox

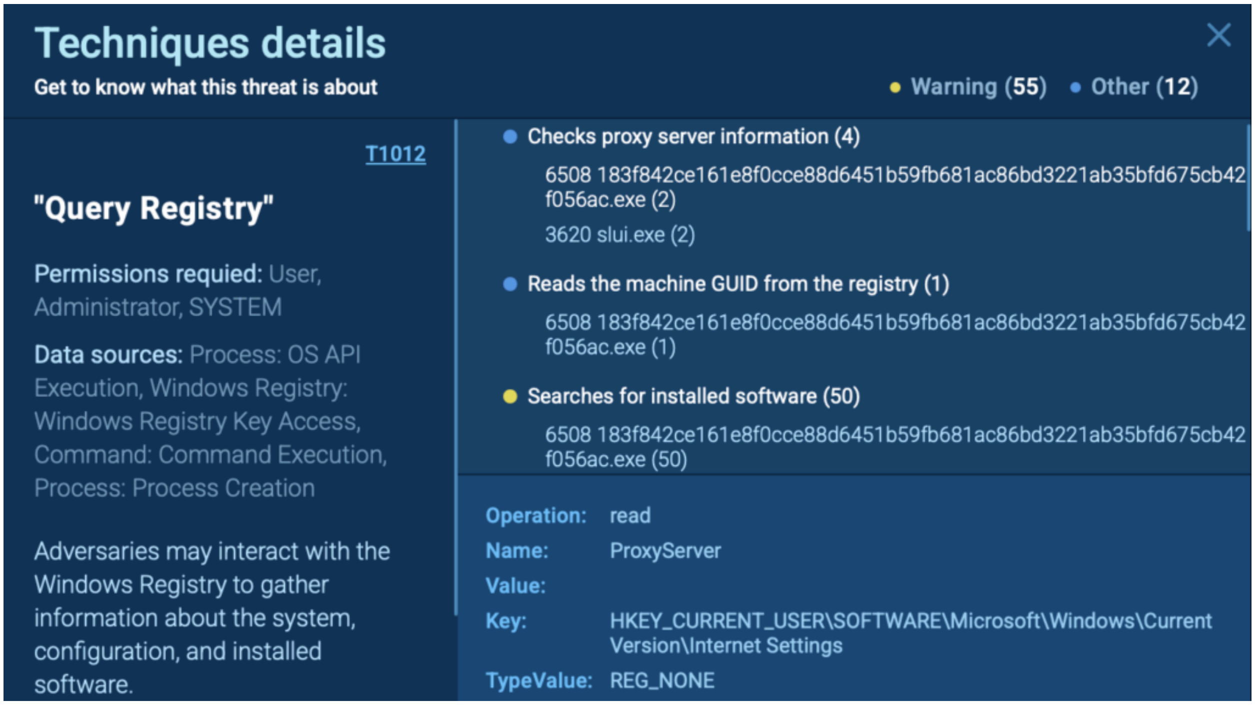
This query fetches **CPU information**, such as model name and vendor. While this might seem benign, it plays a crucial role in **anti-analysis** and **evasion tactics**.

Why malware reads CPU info:

- **Environment validation**: Malware may use CPU data to check if it’s running on a real machine or a virtual one (e.g., commonly used by sandboxes or researchers).

- **Tailored payloads**: Some threats adapt their behavior based on system specs, avoiding execution if they detect low-end CPUs or virtual environments.
- **Fingerprinting the target**: CPU info is often collected alongside other system data to create a unique victim profile.

But this is just the beginning. According to the MITRE ATT&CK technique **T1012: Query Registry**, this sample retrieves a wide range of values:



Techniques details

Get to know what this threat is about

● Warning (55) ● Other (12)

T1012

"Query Registry"

Permissions requied: User, Administrator, SYSTEM

Data sources: Process: OS API Execution, Windows Registry: Windows Registry Key Access, Command: Command Execution, Process: Process Creation

Adversaries may interact with the Windows Registry to gather information about the system, configuration, and installed software.

● Checks proxy server information (4)

6508 183f842ce161e8f0cce88d6451b59fb681ac86bd3221ab35bfd675cb42f056ac.exe (2)

3620 slui.exe (2)

● Reads the machine GUID from the registry (1)

6508 183f842ce161e8f0cce88d6451b59fb681ac86bd3221ab35bfd675cb42f056ac.exe (1)

● Searches for installed software (50)

6508 183f842ce161e8f0cce88d6451b59fb681ac86bd3221ab35bfd675cb42f056ac.exe (50)

Operation: read
Name: ProxyServer
Value:
Key: HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings
TypeValue: REG_NONE

MITRE ATT&CK technique T1012: Query Registry with a wide range of values

- Proxy configuration: Determines whether the system uses a proxy and may hijack it
- Machine GUID: A unique identifier, useful for tracking infected hosts
- Installed software (50 reads): Likely for reconnaissance or to check for security tools
- Internet Explorer security settings: May suggest preparation for exploit delivery via browser
- System language & locale: Used to avoid infecting machines in certain countries
- Computer name & Windows product ID: Adds more detail to the fingerprint
- Software policy settings: Used to detect restrictions or protections enabled by admins

This shows how malware can treat the registry as a rich source of system intelligence. Each value queried helps build a clearer picture of the host environment, guiding the next malicious action.

Learn to analyze cyber threats

Follow along a detailed guide to using ANY.RUN's Interactive Sandbox for malware and phishing analysis

Read full guide

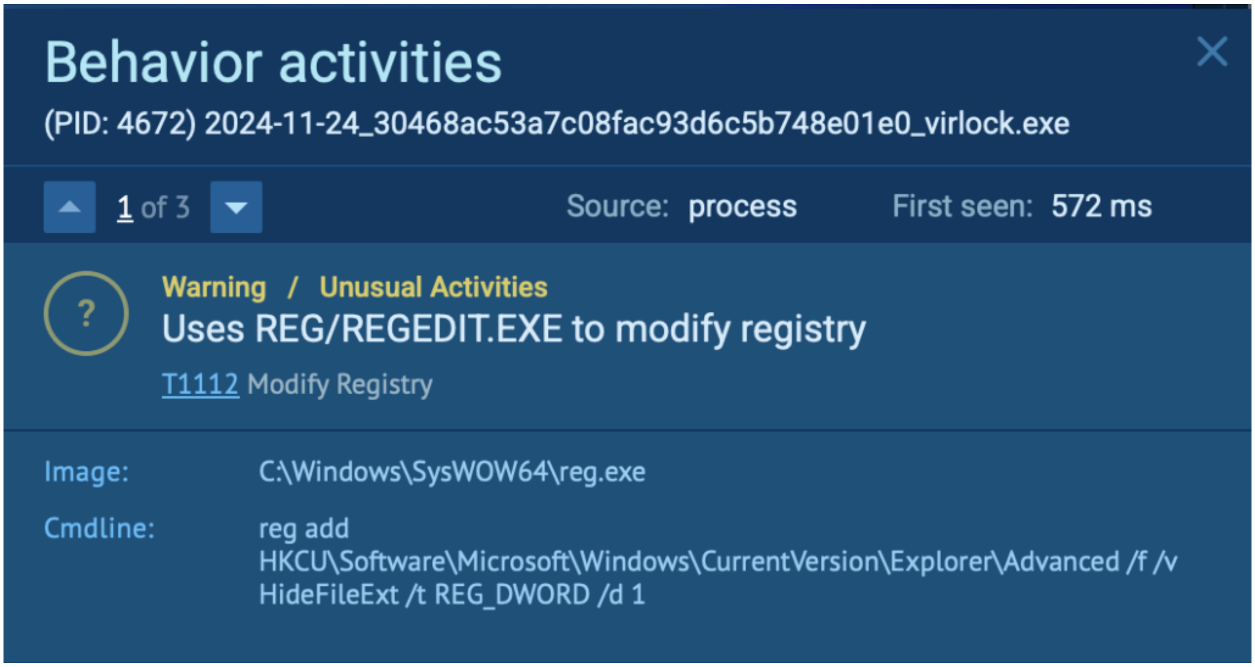
4. Suspicious Registry Modification via REG.EXE

This sample involves a process (_virlock.exe) that uses reg.exe, a legitimate Windows utility, to modify the registry. This kind of activity isn't inherently malicious, but in the context of malware execution, it often signals stealthy post-infection behavior.

View analysis session

Shortly after execution, the malware launches a command: reg add HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced /v HideFileExt /t REG_DWORD /d 1

This command modifies the registry to hide file extensions for known file types, a well-documented trick used by malware to disguise malicious executables (e.g., invoice.pdf.exe appears as invoice.pdf).



Behavior activities

(PID: 4672) 2024-11-24_30468ac53a7c08fac93d6c5b748e01e0_virlock.exe

1 of 3 Source: process First seen: 572 ms

Warning / Unusual Activities

Uses REG/REGEDIT.EXE to modify registry

T1112 Modify Registry

Image: C:\Windows\SysWOW64\reg.exe

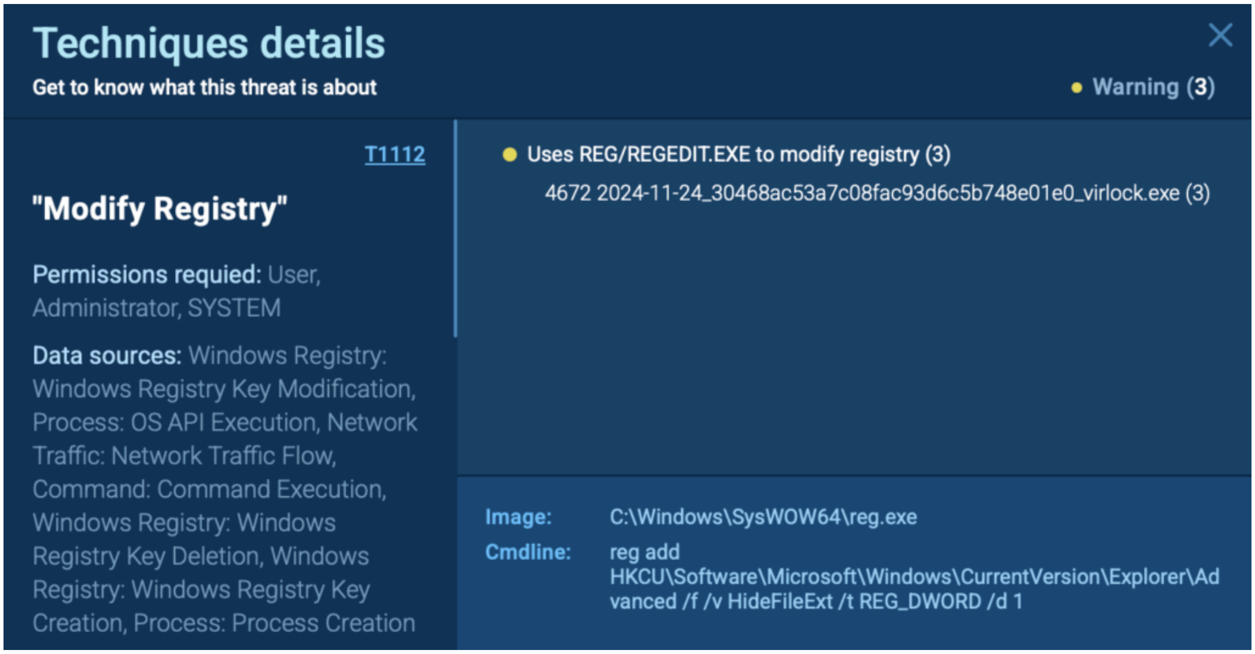
Cmdline:

```
reg add
HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced /f /v
HideFileExt /t REG_DWORD /d 1
```

Registry modification details demonstrated inside ANY.RUN sandbox

Why it’s suspicious:

- This change is frequently used in **social engineering attacks**, where victims are tricked into running malware that looks like a harmless document.
- The behavior is executed via reg.exe, which is a living-off-the-land binary (LOLBIN); a legitimate tool abused by attackers to avoid detection.
- ANY.RUN flags this activity under **T1112: Modify Registry**, and classifies it as a **Warning / Unusual Activity**.



Techniques details

Get to know what this threat is about

● Warning (3)

T1112

"Modify Registry"

Permissions requied: User, Administrator, SYSTEM

Data sources: Windows Registry: Windows Registry Key Modification, Process: OS API Execution, Network Traffic: Network Traffic Flow, Command: Command Execution, Windows Registry: Windows Registry Key Deletion, Windows Registry: Windows Registry Key Creation, Process: Process Creation

● Uses REG/REGEDIT.EXE to modify registry (3)

4672 2024-11-24_30468ac53a7c08fac93d6c5b748e01e0_virlock.exe (3)

Image: C:\Windows\SysWOW64\reg.exe

Cmdline: reg add HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced /f /v HideFileExt /t REG_DWORD /d 1

T1112: Modify Registry inside MITRE ATT&CK section

This case is a good reminder that not all registry abuse is about persistence. Some changes are purely meant to deceive the user, reduce visibility, or mask malicious actions.

With ANY.RUN's behavioral analysis, this tactic becomes immediately visible, showing which registry key was changed, how, when, and by what process, including full command-line context.

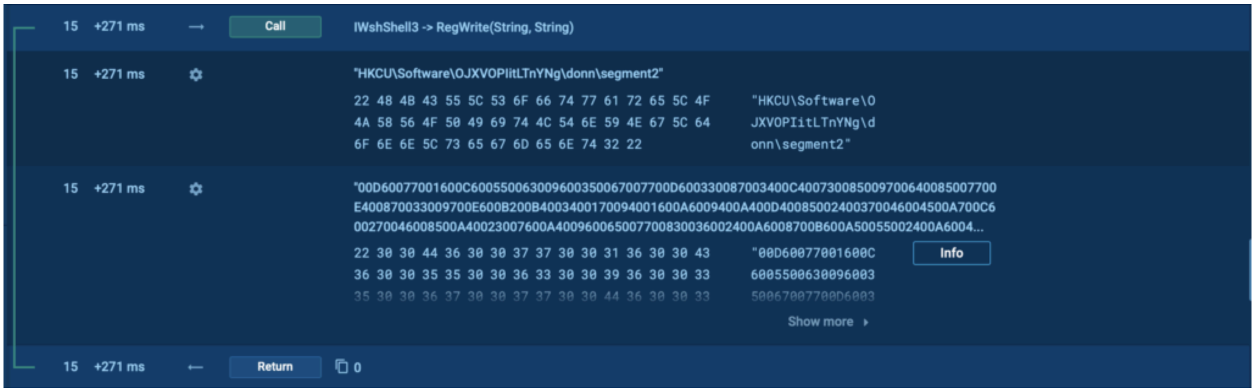
5. Script-Based Registry Modification

In this sample, we see a Windows Script Host process (wscript.exe) modifying the registry, not through a typical executable, but via script-based interaction. This kind of behavior is harder to detect, especially if you're relying on traditional static analysis.

View analysis session

Thanks to ANY.RUN's Script Tracer, we can observe the exact call and parameters used:

- Key: HKCU\Software\OJXVOPIitLTnYNg\donn\segment2
- Value: (Hex-encoded string payload)
- Process: wscript.exe
- Operation: RegWrite via WshShell3



```
15  +271 ms  →  Call  IWshShell3 -> RegWrite(String, String)

15  +271 ms        "HKCU\Software\OJXVOPIitLTnYNg\donn\segment2"
                   22 48 4B 43 55 5C 53 6F 66 74 77 61 72 65 5C 4F    "HKCU\Software\O
                   4A 58 56 4F 50 49 69 74 4C 54 6E 59 4E 67 5C 64    JXVOPIitLTnYNg\d
                   6F 6E 6E 5C 73 65 67 6D 65 6E 74 32 22             onn\segment2"

15  +271 ms        "00D60077001600C6005500630096003500670077 00D600330087003400C4007300850097006400850077 00
                   E400870033009700E600B200B40034001700940016 00A6009400A400D4008500240037004600450 0A700C6
                   00270046008500A40023007600A4009600650077008300360024 00A6008700B600A50055002400A6004...
                   22 30 30 44 36 30 30 37 37 30 30 31 36 30 30 43    "00D60077001600C
                   36 30 30 35 35 30 30 36 33 30 30 39 36 30 30 33    6005500630096003
                   35 30 30 36 37 30 30 37 37 30 30 44 36 30 30 33    50067007700D6003
                                                        Show more ▸

15  +271 ms  ←  Return  0
```

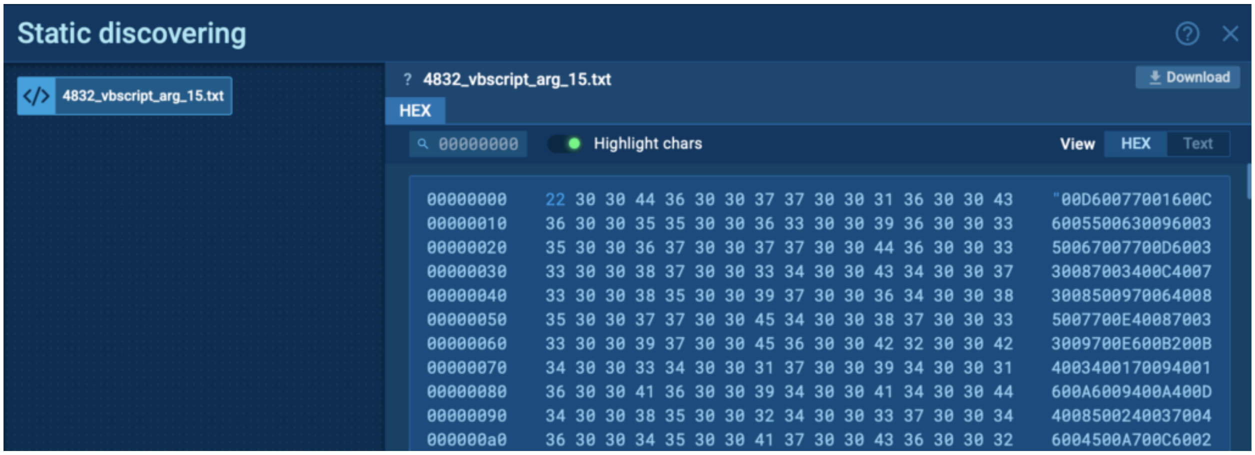
ANY.RUN’s Script Tracer observing calls and parameters

This script creates a new key and writes what appears to be an obfuscated or encoded payload into the registry; a technique commonly used to:

- Store secondary payloads or shellcode
- Evade file-based detection mechanisms
- Delay execution until a later stage (fileless persistence)

The registry key name (OJXVOPIitLTnYNg) is randomly generated and meaningless, a common trait of **obfuscated malware activity**.

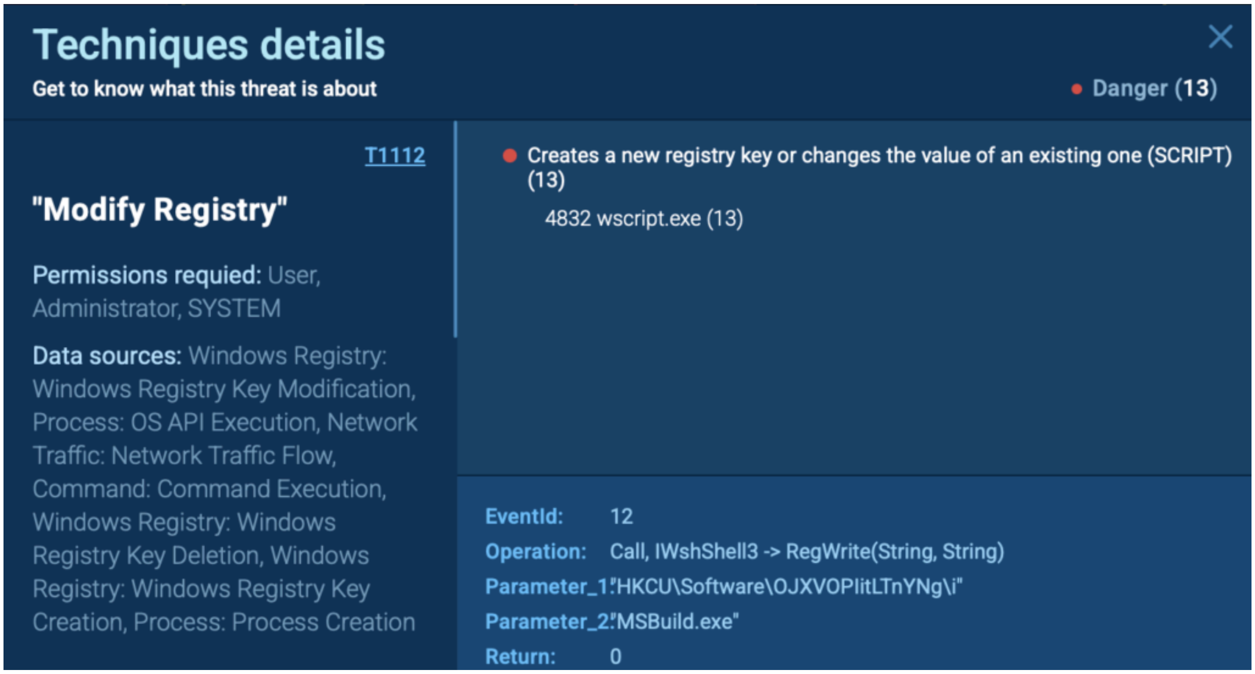
We can see how the script writes a long block of hexadecimal content, which may later be decoded and executed, without ever dropping a traditional file on disk.



```
00000000    22 30 30 44 36 30 30 37 37 30 30 31 36 30 30 43    "00D60077001600C
00000010    36 30 30 35 35 30 30 36 33 30 30 39 36 30 30 33    6005500630096003
00000020    35 30 30 36 37 30 30 37 37 30 30 44 36 30 30 33    50067007700D6003
00000030    33 30 30 38 37 30 30 33 34 30 30 43 34 30 30 37    30087003400C4007
00000040    33 30 30 38 35 30 30 39 37 30 30 36 34 30 30 38    3008500970064008
00000050    35 30 30 37 37 30 30 45 34 30 30 38 37 30 30 33    5007700E40087003
00000060    33 30 30 39 37 30 30 45 36 30 30 42 32 30 30 42    3009700E600B200B
00000070    34 30 30 33 34 30 30 31 37 30 30 39 34 30 30 31    4003400170094001
00000080    36 30 30 41 36 30 30 39 34 30 30 41 34 30 30 44    600A6009400A400D
00000090    34 30 30 38 35 30 30 32 34 30 30 33 37 30 30 34    4008500240037004
000000a0    36 30 30 34 35 30 30 41 37 30 30 43 36 30 30 32    6004500A700C6002
```

Long block of hexadecimal content displayed inside ANY.RUN sandbox

These modifications fall under MITRE ATT&CK technique **T1112: Modify Registry**, and ANY.RUN labels this behavior as **Dangerous (13 instances)**.



Techniques details

Get to know what this threat is about

● Danger (13)

T1112

"Modify Registry"

Permissions requied: User, Administrator, SYSTEM

Data sources: Windows Registry: Windows Registry Key Modification, Process: OS API Execution, Network Traffic: Network Traffic Flow, Command: Command Execution, Windows Registry: Windows Registry Key Deletion, Windows Registry: Windows Registry Key Creation, Process: Process Creation

● Creates a new registry key or changes the value of an existing one (SCRIPT) (13)

4832 wscript.exe (13)

```
EventId:     12
Operation:   Call, IWshShell3 -> RegWrite(String, String)
Parameter_1:"HKCU\Software\OJXVOPlitLTnYNg\i"
Parameter_2:"MSBuild.exe"
Return:      0
```

The technique “Modify Registry” with all its details inside ANY.RUN sandbox

Without behavioral analysis, this kind of registry manipulation would be nearly invisible, but with Script Tracer, security analysts can follow every step the script takes, down to the exact method calls and values.

Spotting Registry Abuse is Easy with ANY.RUN

Registry modifications are a common and powerful tactic used by malware to stay hidden, persist through reboots, and weaken your defenses. But with the right tools, these threats become much easier to spot, investigate, and respond to.

ANY.RUN’s interactive sandbox doesn’t just show you what malware is doing, it **visually breaks down every behavior**, from registry edits to process injection and data exfiltration, in real time.

- **Faster threat detection**
  Catch malicious registry changes and system tampering before damage is done; no need to wait for traditional tools to catch up.
- **Improved incident response**
  With clear visual evidence and behavior chains, your team can respond to threats with greater accuracy and speed.
- **Reduced investigation time**
  Analysts can immediately see what’s been changed, what triggered the behavior, and which malware family is involved.
- **Stronger defenses across the board**
  By identifying how threats abuse the registry, you can harden your endpoints, update rules, and block similar attacks in the future.

- **Better collaboration and reporting**
  Export detailed analysis reports, share IOCs with teams, and make smarter security decisions faster.