BankSlip Keylogger Malware Report

Executive Summary

This report documents a comprehensive artifact-driven static and dynamic analysis of the Windows PE sample identified by SHA256

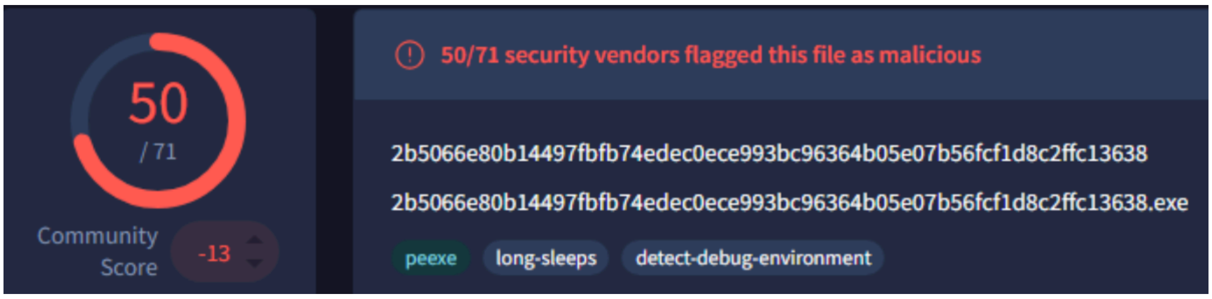
`2b5066e80b14497fbfb74edec0ece993bc96364b05e07b56fcf1d8c2ffc13638`

Analysis of the provided RegShot snapshot shows the sample was executed from C:\Users\windows\Downloads\ during the capture window and that many registry values were added or modified as a result of execution. UserAssist and AppCompat entries corroborate interactive launch. Memory and crash artifacts were provided and are suitable for deeper forensics (process lists, open sockets, loaded modules, and strings). This report contains findings, confirmed indicators of compromise (IOCs), recommended next steps, and detection/remediation guidance.

Static Analysis

The static analysis begins by opening the malware in VirusTotal to see what existing information there is on this malware. The findings are as follows:

The analysis begins by seeing that the malware is obviously well known, with 50 out of 71 scanners knowing about it:


50 / 71

Community Score -13

50/71 security vendors flagged this file as malicious

2b5066e80b14497fbfb74edec0ece993bc96364b05e07b56fcf1d8c2ffc13638

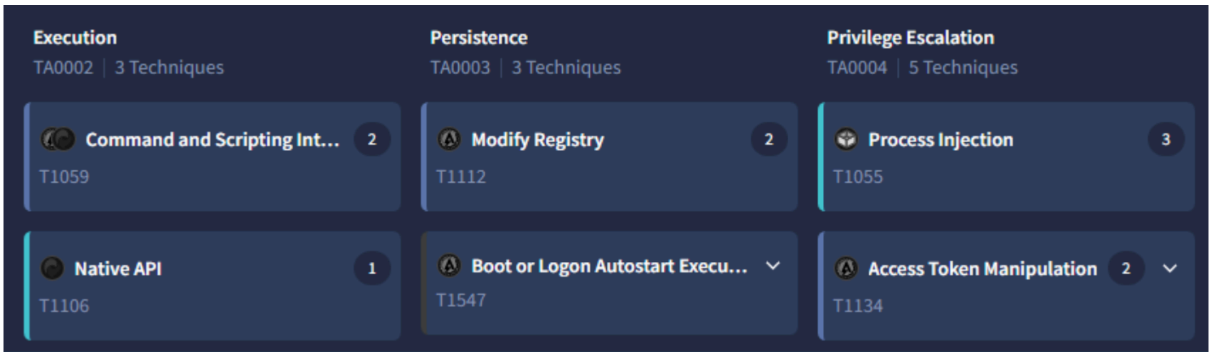
2b5066e80b14497fbfb74edec0ece993bc96364b05e07b56fcf1d8c2ffc13638.exe

peexe long-sleeps detect-debug-environment

It can also be seen that this malware can detect a debugging environment. One of the names this malware has been seen as is **BankSlip.exe** which shows that it has probably been used on banks in the past.

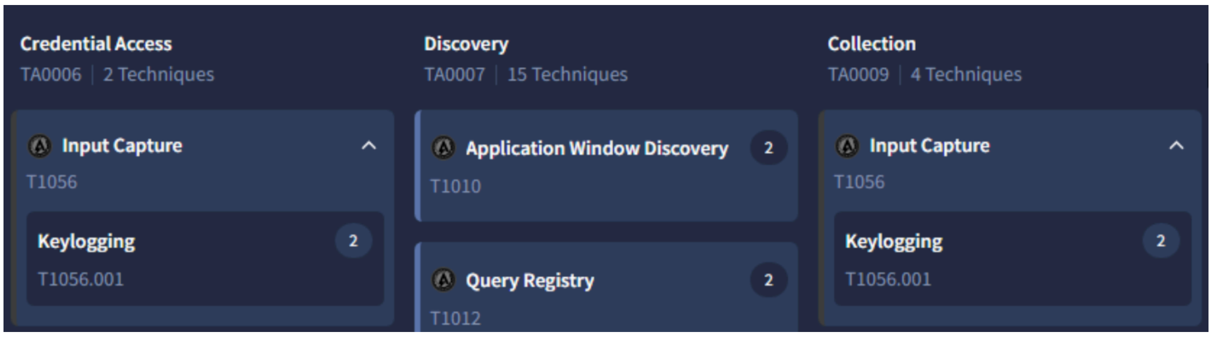
Bank slip.exe

Moving on to detections it can be seen that this malware attempts persistence by injecting itself into auto start registries.


Execution — TA0002 | 3 Techniques
- Command and Scripting Int... (2) T1059
- Native API (1) T1106

Persistence — TA0003 | 3 Techniques
- Modify Registry (2) T1112
- Boot or Logon Autostart Execu... T1547

Privilege Escalation — TA0004 | 5 Techniques
- Process Injection (3) T1055
- Access Token Manipulation (2) T1134


Credential Access — TA0006 | 2 Techniques
- Input Capture T1056
  - Keylogging (2) T1056.001

Discovery — TA0007 | 15 Techniques
- Application Window Discovery (2) T1010
- Query Registry (2) T1012

Collection — TA0009 | 4 Techniques
- Input Capture T1056
  - Keylogging (2) T1056.001

Here a big clue was found with the detection of Input Capture and **Keylogging**. For an analyst this gives big input because now the type of malware being dealt with is understood.

IDA and PEstudio Analysis

From here, the analysis moves on to IDA and PEstudio to look at strings and imports to see what can be found there:

1. Keylogging and Stealing

- *GetAsyncKeyState, GetKeyboardState, SetKeyboardState* - Captures keystrokes
- *GetForegroundWindow, GetWindowTextW* - Gets the active window titles

2. Information Gathering

- *GetComputerNameW, GetUserNameW* - Identifies victim machine
- *GetProcessMemoryInfo, Process32FirstW* - Monitors system processes
- *GetDiskFreeSpaceW, GetVolumeInformationW* - System information gathering

3. Exporting of the Data

- Network functions: *InternetOpenW, InternetConnectW, HttpSendRequestW*
- FTP capabilities: *FtpOpenFileW, FtpGetFileSize*
- Email through SMTP (implied by mail-related strings)

4. Persistence & Evasion

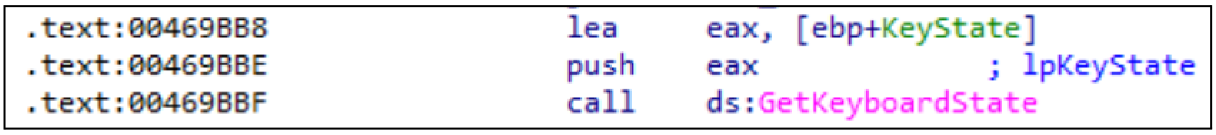
- Registry functions: *RegCreateKeyExW, RegSetValueExW* - Installs itself
- *CreateProcessW, ShellExecuteW* - Executes other programs
- *IsDebuggerPresent* - Anti-analysis check

After some static analysis, a conclusion can be made about the malware: this is probably a professional grade information stealer (keylogger) and is probably used by threat actors for financial gain or espionage of some sort. Finally here are some findings found through the assembly itself where a lot of these findings are reinforced. These functions are called multiple times around the assembly:

Assembly Code Analysis

The following key functions were identified throughout the assembly code:

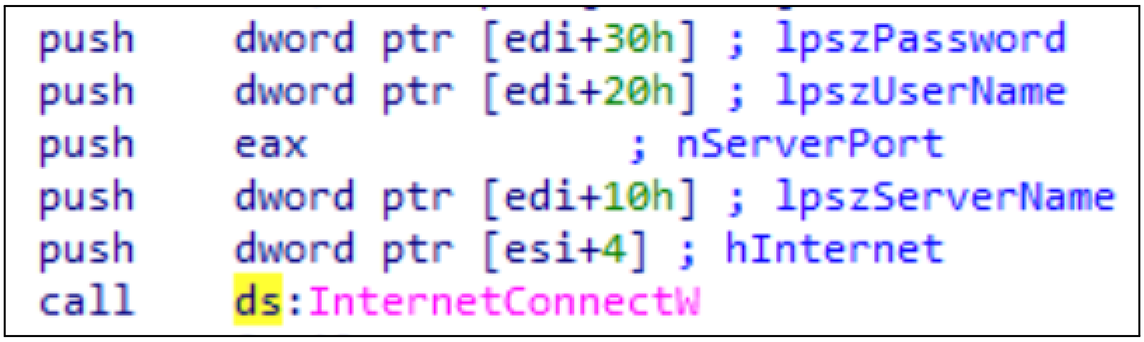
Keyboard State Monitoring



```
.text:00469BB8                 lea     eax, [ebp+KeyState]
.text:00469BBE                 push    eax             ; lpKeyState
.text:00469BBF                 call    ds:GetKeyboardState
```

The assembly shows repeated calls to `GetKeyboardState`, confirming keystroke capture capabilities.

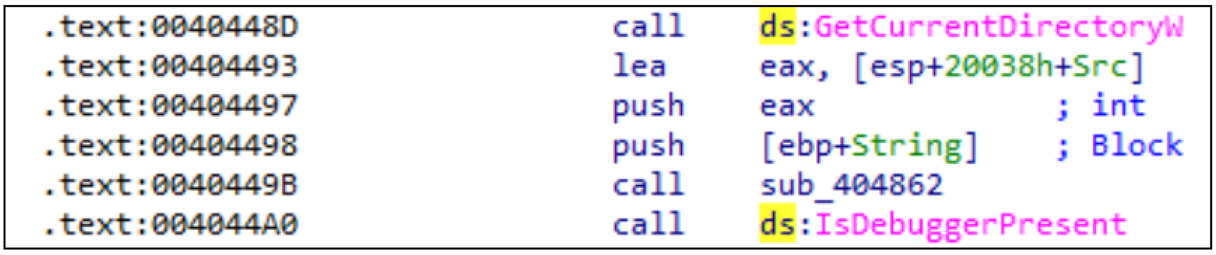
Network Communication Setup



```
push    dword ptr [edi+30h] ; lpszPassword
push    dword ptr [edi+20h] ; lpszUserName
push    eax                 ; nServerPort
push    dword ptr [edi+10h] ; lpszServerName
push    dword ptr [esi+4] ; hInternet
call    ds:InternetConnectW
```

The code shows *InternetConnectW* being called with parameters for server name (lpszServerName), username (lpszPassword), password (lpszPassword), and port (nServerPort). This shows command-and-control communication for moving data.

Anti-Debugging Checks



```
.text:0040448D          call    ds:GetCurrentDirectoryW
.text:00404493          lea     eax, [esp+20038h+Src]
.text:00404497          push    eax             ; int
.text:00404498          push    [ebp+String]    ; Block
.text:0040449B          call    sub_404862
.text:004044A0          call    ds:IsDebuggerPresent
```

The malware calls *IsDebuggerPresent* to detect analysis environments and evade reverse engineering.

Dynamic Analysis

Objectives

- Verify whether the supplied sample executed and altered system state.
- Extract concrete artifacts (execution path, timestamps, registry changes, UserAssist/AppCompat entries).
- Produce a concise IOC table suitable for class submission.
- Recommend containment, detection, and follow-up forensic actions.

File Identification and Hash Verification

File name:

`2b5066e80b14497fbfb74edec0ece993bc96364b05e07b56fcf1d8c2ffc13638.exe`

Location:

`C:\Users\windows\Downloads\`

Algorithm and Hash Value

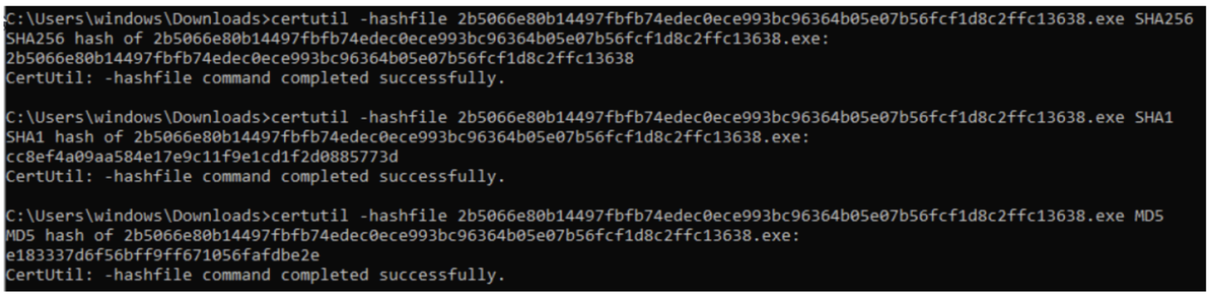
SHA256: `2b5066e80b14497fb7b74edec0ece993bc96364b05e07b56fcf1d8c2ffc13638`

SHA1: `c8f4fa049a5847fec1f119e41df2d885737d`

MD5: `e1b337d15ef69ff7165ffdfadfbe4ee2`

Computed hashes via certutil

Command used:



```
C:\Users\windows\Downloads>certutil -hashfile 2b5066e80b14497fbfb74edec0ece993bc96364b05e07b56fcf1d8c2ffc13638.exe SHA256
SHA256 hash of 2b5066e80b14497fbfb74edec0ece993bc96364b05e07b56fcf1d8c2ffc13638.exe:
2b5066e80b14497fbfb74edec0ece993bc96364b05e07b56fcf1d8c2ffc13638
CertUtil: -hashfile command completed successfully.

C:\Users\windows\Downloads>certutil -hashfile 2b5066e80b14497fbfb74edec0ece993bc96364b05e07b56fcf1d8c2ffc13638.exe SHA1
SHA1 hash of 2b5066e80b14497fbfb74edec0ece993bc96364b05e07b56fcf1d8c2ffc13638.exe:
cc8ef4a09aa584e17e9c11f9e1cd1f2d0885773d
CertUtil: -hashfile command completed successfully.

C:\Users\windows\Downloads>certutil -hashfile 2b5066e80b14497fbfb74edec0ece993bc96364b05e07b56fcf1d8c2ffc13638.exe MD5
MD5 hash of 2b5066e80b14497fbfb74edec0ece993bc96364b05e07b56fcf1d8c2ffc13638.exe:
e183337d6f56bff9ff671056fafdbe2e
CertUtil: -hashfile command completed successfully.
```

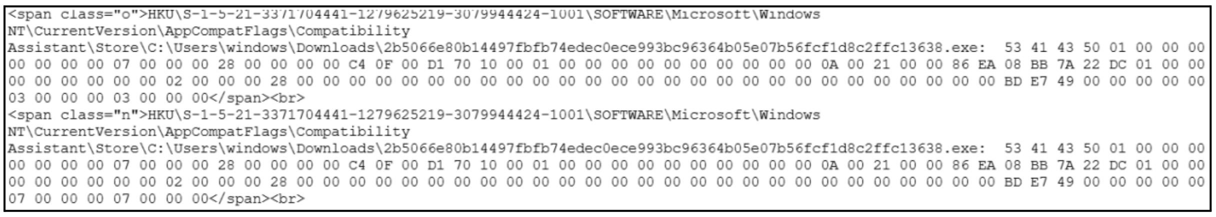
Figure 2: Commands Used

Analysis Environment & Methodology

- **Approach:** artifact-driven. Analysis relied on the RegShot comparison output, the provided crash dump, and the .i64 memory image.
- **Timestamps:** RegShot captured a before/after window of **2025-10-31 19:58:09** → **2025-10-31 20:33:48**; all changes referenced use that timeframe.
- **Artifacts parsed:** RegShot HTML (registry diffs, UserAssist and AppCompat entries), DMP (crash dump — summary parsing), memory image (process/modules/strings where extractable).

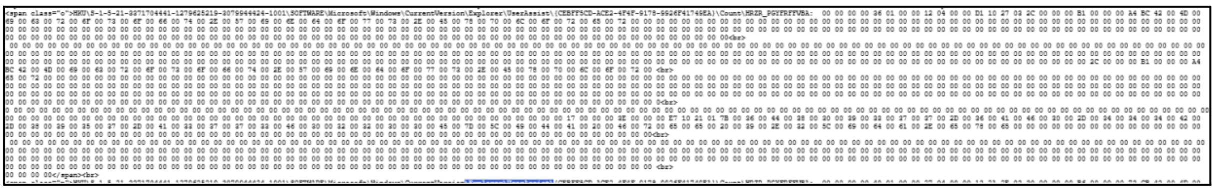
Chronological Findings & Behavioral Summary

1. Execution confirmed: AppCompat and UserAssist entries in the RegShot indicate the sample was launched from C:\Users\windows\Downloads\2b5066e8...13638.exe during the capture window. This supports interactive or user-triggered execution.



```
<span class="o">HKU\S-1-5-21-3371704441-1279625219-3079944424-1001\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\AppCompatFlags\Compatibility
Assistant\Store\C:\Users\windows\Downloads\2b5066e80b14497fbfb74edec0ece993bc96364b05e07b56fcf1d8c2ffc13638.exe:  53 41 43 50 01 00 00 00
00 00 00 00 07 00 00 00 28 00 00 00 00 C4 0F 00 D1 70 10 00 01 00 00 00 00 00 00 00 00 00 0A 00 21 00 00 86 EA 08 BB 7A 22 DC 01 00 00
00 00 00 00 00 00 02 00 00 00 28 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 BD E7 49 00 00 00 00 00
03 00 00 00 03 00 00 00</span><br>
<span class="n">HKU\S-1-5-21-3371704441-1279625219-3079944424-1001\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\AppCompatFlags\Compatibility
Assistant\Store\C:\Users\windows\Downloads\2b5066e80b14497fbfb74edec0ece993bc96364b05e07b56fcf1d8c2ffc13638.exe:  53 41 43 50 01 00 00 00
00 00 00 00 07 00 00 00 28 00 00 00 00 C4 0F 00 D1 70 10 00 01 00 00 00 00 00 00 00 00 00 0A 00 21 00 00 86 EA 08 BB 7A 22 DC 01 00 00
00 00 00 00 00 00 02 00 00 00 28 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 BD E7 49 00 00 00 00 00
07 00 00 00 07 00 00 00</span><br>
```

Figure 3: RegShot AppCompatFlags Compatibility Assistant “Store” entry for C:\Users\windows\Downloads\2b5066e80b14497fbfb74edec0ece993bc96364b05e07b56fcf1d8c2ffc13638.exe. The before (top) and after (bottom) registry values show the key was created or updated during execution, confirming the sample ran on the system

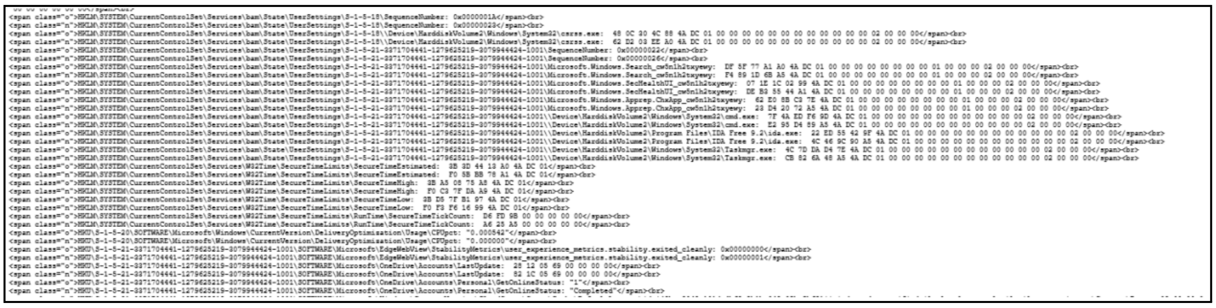


```
<span class="o">HKU\S-1-5-21-3371704441-1279625219-3079944424-1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}\Count\HRZR_PGYFRFFVBA:  00 00 00 00 36 01 00 00 12 04 00 00 D1 10 27 03 2C 00 00 00 B1 00 00 00 A4 BC 42 00 4D 00
69 00 63 00 72 00 6F 00 73 00 6F 00 66 00 74 00 2E 00 57 00 69 00 6E 00 64 00 6F 00 77 00 73 00 2E 00 45 00 78 00 70 00 6C 00 6F 00 72 00 65 00 72 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00<br>
 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 2C 00 00 00 B1 00 00 00 A4
BC 42 00 4D 00 69 00 63 00 72 00 6F 00 73 00 6F 00 66 00 74 00 2E 00 57 00 69 00 6E 00 64 00 6F 00 77 00 73 00 2E 00 45 00 78 00 70 00 6C 00 6F 00 72 00 <br>
65 00 72 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 0<br>
0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 17 00 00 00 2E 00 00 00 E7 10 21 01 7B 00 36 00 44 00 38 00 30 00 39 00 33 00 37 00 37 00 2D 00 36 00 41 00 46 00 30 00 2D 00 34 00 34 00 34 00 42 00
2D 00 38 00 39 00 35 00 37 00 2D 00 41 00 33 00 37 00 37 00 33 00 46 00 30 00 32 00 32 00 30 00 30 00 45 00 7D 00 5C 00 49 00 44 00 41 00 20 00 46 00 72 00 65 00 65 00 20 00 39 00 2E 00 32 00 5C 00 69 00 64 00 61 00 2E 00 65 00 78 00 65 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00<br>
 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 <br>
00 00 00 00</span><br>
```

Figure 4: RegShot UserAssist entry under HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}\Count. This entry records interactive

launches through Windows Explorer, confirming that the sample was manually executed by a user during the capture window.

2. Registry modifications: RegShot reports **67 values added** and **136 values modified** across HKU and HKLM hives during the run window. The diffs include AppCompat and UserAssist entries referencing the sample, plus numerous other value changes consistent with a program making system and user-level modifications.



```
<span class="o">HKLM\SYSTEM\CurrentControlSet\Services\bam\State\UserSettings\S-1-5-18\SequenceNumber: 0x0000001A</span><br>
<span class="n">HKLM\SYSTEM\CurrentControlSet\Services\bam\State\UserSettings\S-1-5-18\SequenceNumber: 0x00000023</span><br>
<span class="o">HKLM\SYSTEM\CurrentControlSet\Services\bam\State\UserSettings\S-1-5-18\\Device\HarddiskVolume2\Windows\System32\csrss.exe:  48 0C 30 4C 88 4A DC 01 00 00 00 00 00 00 00 00 00 00 00 00 02 00 00 00</span><br>
<span class="n">HKLM\SYSTEM\CurrentControlSet\Services\bam\State\UserSettings\S-1-5-18\\Device\HarddiskVolume2\Windows\System32\csrss.exe:  62 D2 03 EE A0 4A DC 01 00 00 00 00 00 00 00 00 00 00 00 00 02 00 00 00</span><br>
<span class="o">HKLM\SYSTEM\CurrentControlSet\Services\bam\State\UserSettings\S-1-5-21-3371704441-1279625219-3079944424-1001\SequenceNumber: 0x00000022</span><br>
<span class="n">HKLM\SYSTEM\CurrentControlSet\Services\bam\State\UserSettings\S-1-5-21-3371704441-1279625219-3079944424-1001\SequenceNumber: 0x00000026</span><br>
<span class="o">HKLM\SYSTEM\CurrentControlSet\Services\bam\State\UserSettings\S-1-5-21-3371704441-1279625219-3079944424-1001\Microsoft.Windows.Search_cw5n1h2txyewy:  DF 5F 77 A1 A0 4A DC 01 00 00 00 00 00 00 00 00 01 00 00 00 02 00 00 00</span><br>
<span class="n">HKLM\SYSTEM\CurrentControlSet\Services\bam\State\UserSettings\S-1-5-21-3371704441-1279625219-3079944424-1001\Microsoft.Windows.Search_cw5n1h2txyewy:  F4 89 1D 6B A5 4A DC 01 00 00 00 00 00 00 00 00 01 00 00 00 02 00 00 00</span><br>
<span class="o">HKLM\SYSTEM\CurrentControlSet\Services\bam\State\UserSettings\S-1-5-21-3371704441-1279625219-3079944424-1001\Microsoft.Windows.SecHealthUI_cw5n1h2txyewy:  07 1E 1C 02 99 4A DC 01 00 00 00 00 00 00 00 00 01 00 00 00 02 00 00 00</span><br>
<span class="n">HKLM\SYSTEM\CurrentControlSet\Services\bam\State\UserSettings\S-1-5-21-3371704441-1279625219-3079944424-1001\Microsoft.Windows.SecHealthUI_cw5n1h2txyewy:  DE B3 55 44 A1 4A DC 01 00 00 00 00 00 00 00 00 01 00 00 00 02 00 00 00</span><br>
<span class="o">HKLM\SYSTEM\CurrentControlSet\Services\bam\State\UserSettings\S-1-5-21-3371704441-1279625219-3079944424-1001\Microsoft.Windows.Apprep.ChxApp_cw5n1h2txyewy:  62 E0 8B C3 7E 4A DC 01 00 00 00 00 00 00 00 00 01 00 00 00 02 00 00 00</span><br>
<span class="n">HKLM\SYSTEM\CurrentControlSet\Services\bam\State\UserSettings\S-1-5-21-3371704441-1279625219-3079944424-1001\Microsoft.Windows.Apprep.ChxApp_cw5n1h2txyewy:  23 D4 20 72 A5 4A DC 01 00 00 00 00 00 00 00 00 01 00 00 00 02 00 00 00</span><br>
<span class="o">HKLM\SYSTEM\CurrentControlSet\Services\bam\State\UserSettings\S-1-5-21-3371704441-1279625219-3079944424-1001\\Device\HarddiskVolume2\Windows\System32\cmd.exe:  7F 4A ED F6 9D 4A DC 01 00 00 00 00 00 00 00 00 00 00 00 00 02 00 00 00</span><br>
<span class="n">HKLM\SYSTEM\CurrentControlSet\Services\bam\State\UserSettings\S-1-5-21-3371704441-1279625219-3079944424-1001\\Device\HarddiskVolume2\Windows\System32\cmd.exe:  E2 95 D4 89 A5 4A DC 01 00 00 00 00 00 00 00 00 00 00 00 00 02 00 00 00</span><br>
<span class="o">HKLM\SYSTEM\CurrentControlSet\Services\bam\State\UserSettings\S-1-5-21-3371704441-1279625219-3079944424-1001\\Device\HarddiskVolume2\Program Files\IDA Free 9.2\ida.exe:  22 ED 55 42 9F 4A DC 01 00 00 00 00 00 00 00 00 00 00 00 00 02 00 00 00</span><br>
<span class="n">HKLM\SYSTEM\CurrentControlSet\Services\bam\State\UserSettings\S-1-5-21-3371704441-1279625219-3079944424-1001\\Device\HarddiskVolume2\Program Files\IDA Free 9.2\ida.exe:  4C 46 9C 90 A5 4A DC 01 00 00 00 00 00 00 00 00 00 00 00 00 02 00 00 00</span><br>
<span class="o">HKLM\SYSTEM\CurrentControlSet\Services\bam\State\UserSettings\S-1-5-21-3371704441-1279625219-3079944424-1001\\Device\HarddiskVolume2\Windows\System32\Taskmgr.exe:  4C 7D DA D4 7E 4A DC 01 00 00 00 00 00 00 00 00 00 00 00 00 02 00 00 00</span><br>
<span class="n">HKLM\SYSTEM\CurrentControlSet\Services\bam\State\UserSettings\S-1-5-21-3371704441-1279625219-3079944424-1001\\Device\HarddiskVolume2\Windows\System32\Taskmgr.exe:  CB 82 6A 48 A5 4A DC 01 00 00 00 00 00 00 00 00 00 00 00 00 02 00 00 00</span><br>
<span class="o">HKLM\SYSTEM\CurrentControlSet\Services\W32Time\SecureTimeLimits\SecureTimeEstimated:  3B 3D 44 13 A0 4A DC 01</span><br>
<span class="n">HKLM\SYSTEM\CurrentControlSet\Services\W32Time\SecureTimeLimits\SecureTimeEstimated:  F0 5B BB 78 A1 4A DC 01</span><br>
<span class="o">HKLM\SYSTEM\CurrentControlSet\Services\W32Time\SecureTimeLimits\SecureTimeHigh:  3B A5 08 75 A8 4A DC 01</span><br>
<span class="n">HKLM\SYSTEM\CurrentControlSet\Services\W32Time\SecureTimeLimits\SecureTimeHigh:  F0 C3 7F DA A9 4A DC 01</span><br>
<span class="o">HKLM\SYSTEM\CurrentControlSet\Services\W32Time\SecureTimeLimits\SecureTimeLow:  3B D6 7F B1 97 4A DC 01</span><br>
<span class="n">HKLM\SYSTEM\CurrentControlSet\Services\W32Time\SecureTimeLimits\SecureTimeLow:  F0 F3 F6 16 99 4A DC 01</span><br>
<span class="o">HKLM\SYSTEM\CurrentControlSet\Services\W32Time\SecureTimeLimits\RunTime\SecureTimeTickCount:  D6 FD 9B 00 00 00 00 00</span><br>
<span class="n">HKLM\SYSTEM\CurrentControlSet\Services\W32Time\SecureTimeLimits\RunTime\SecureTimeTickCount:  A6 25 A5 00 00 00 00 00</span><br>
<span class="o">HKU\S-1-5-20\SOFTWARE\Microsoft\Windows\CurrentVersion\DeliveryOptimization\Usage\CPUpct: "0.000542"</span><br>
<span class="n">HKU\S-1-5-20\SOFTWARE\Microsoft\Windows\CurrentVersion\DeliveryOptimization\Usage\CPUpct: "0.000000"</span><br>
<span class="o">HKU\S-1-5-21-3371704441-1279625219-3079944424-1001\SOFTWARE\Microsoft\EdgeWebView\StabilityMetrics\user_experience_metrics.stability.exited_cleanly: 0x00000000</span><br>
<span class="n">HKU\S-1-5-21-3371704441-1279625219-3079944424-1001\SOFTWARE\Microsoft\EdgeWebView\StabilityMetrics\user_experience_metrics.stability.exited_cleanly: 0x00000001</span><br>
<span class="o">HKU\S-1-5-21-3371704441-1279625219-3079944424-1001\SOFTWARE\Microsoft\OneDrive\Accounts\LastUpdate:  28 12 05 69 00 00 00 00</span><br>
<span class="n">HKU\S-1-5-21-3371704441-1279625219-3079944424-1001\SOFTWARE\Microsoft\OneDrive\Accounts\LastUpdate:  82 1C 05 69 00 00 00 00</span><br>
<span class="o">HKU\S-1-5-21-3371704441-1279625219-3079944424-1001\SOFTWARE\Microsoft\OneDrive\Accounts\Personal\GetOnlineStatus: "1"</span><br>
<span class="n">HKU\S-1-5-21-3371704441-1279625219-3079944424-1001\SOFTWARE\Microsoft\OneDrive\Accounts\Personal\GetOnlineStatus: "Completed"</span><br>
```

Figure 5: RegShot comparison showing modified Background Activity Moderator (BAM) UserSettings keys under HKLM\SYSTEM\CurrentControlSet\Services\bam\State. The updated sequence numbers and per-process entries (e.g., cmd.exe, Taskmgr.exe) indicate new or recently executed processes during the capture window

3. No single clear Run autorun key found in examined excerpt: In the partial regshot snippets reviewed, an obvious HKCU\...\Run entry was not present; however, the full regshot contains many entries that should be searched for other persistence methods (scheduled tasks, service creation, Image File Execution Options, WMI event consumers, etc.).

4. Crash & memory artifacts present: The uploaded crash dump and .i64 memory image are expected to contain process stacks, module lists, and possibly network artifacts (sockets, DNS queries) and strings—these should be parsed with Volatility/Volatility3 to recover runtime indicators and possible C2 artifacts.

Confirmed Artifacts & IOCs

Execution Path

- `C:\Users\windows\Downloads\2b5066e80b14497fbfb74edec0ece993bc96364b05e07b56fcf1d8c2ffc13638.exe` (RegShot/AppCompat/UserAssist).

Timestamps

- RegShot "before→after" window: **2025-10-31 19:58:09 → 2025-10-31 20:33:48**

Registry

- Values added: **67** (RegShot summary).
- Values modified: **136** (RegShot summary).
- AppCompat and UserAssist entries referencing the sample were created/updated (evidence of execution and application compatibility logging).

Hashes

- SHA256, SHA1, MD5 as listed in File Identification section (useful for cross-referencing with threat feeds).

Notes

- The regshot contains many more individual registry keys and values; the assignment typically requires enumerating those keys — see Appendix A (below) for a suggested CSV-ready format. The full RegShot HTML can be parsed to list every added/modified key/value for submission.

Memory & Crash-Dump Findings (Summary / Planned Extraction)

Available artifacts: fakenet (6).DMP (crash dump) and .i64 memory image were uploaded. These are suitable for:

- listing running processes and threads at capture time,
- enumerating loaded modules and DLLs for suspicious modules or injections,
- extracting network sockets, DNS queries, and possible C2 endpoints,
- recovering strings, potential plaintext config, or embedded URLs.

Recommendation: run Volatility3 (or Volatility) plugins:

- `windows.pslist / windows.pstree` for process enumeration,
- `windows.netstat` for sockets,
- `windows.dlllist / windows.modscan` for modules,
- `strings` and `yarascan` for indicators inside memory,
- `windows.malfind` & `windows.injscan` for injected code.

Risk Assessment

The sample executed and produced numerous registry changes, which indicates capacity to modify system configuration and potentially persist. Without parsed memory/network artifacts, it's not yet possible to classify full capabilities (exfiltration, credential theft, lateral movement), but the evidence supports a **moderate to high risk profile** pending further analysis.

Detection, Containment, and Remediation Recommendations

Immediate

- Isolate the host (network disconnect) if this occurred on a production machine. Preserve memory and disk images for forensics; DO NOT power off before collecting memory.
- If the host cannot be isolated immediately, block egress at the network perimeter to suspected C2 indicators (if discovered).

Host Detection

- Deploy a host-based rule to alert on execution from user Downloads directories, e.g.:

```
ProcessCreate where ImagePath like '%\Users\%\Downloads\%2b5066e8%.exe'
```

- Monitor and alert on registry modifications in the same timeframe and on keys commonly used for persistence (Run, Scheduled Tasks, Services, IFEO, WMI).

Network Detection

- After extracting any domains/IPs from memory/pcap, block and sink them in a controlled environment; monitor for DNS lookups matching those domains on other hosts.

Long-term

- Sweep environment for the SHA256/MD5/SHA1 across endpoints and storage, and run YARA rules derived from recovered strings or memory signatures.
- Harden user behavior policies to avoid executing downloads from untrusted sources and use email/web protections to reduce click-through risk.

Conclusion

Ultimate Goal: The malware's primary objective is to silently monitor user activity, capture credentials, and move sensitive information to remote command-and-control servers.