Distribution of SmartLoader Malware via Github Repository Disguised as a Legitimate Project

By ATCP

Published: 2025-08-07 · Archived: 2026-04-10 02:08:12 UTC

AhnLab SEcurity intelligence Center (ASEC) has recently discovered the massive distribution of SmartLoader malware through GitHub repositories. These repositories are carefully crafted to appear as legitimate projects and are attracting user interest by focusing on topics such as game cheats, software cracks, and automation tools. Each repository contains a README file and a compressed file, which in turn contains the SmartLoader malware.

- **SmartLoader Distribution URLs**
  hxxps://github[.]com/[Threat Actor Account]/Maple-Story-Menu/releases/download/v3.2.0/Maple.Story.Menu.v3.2.0.zip
  hxxps://github[.]com/[Threat Actor Account]/Minecraft-Vape-Client/releases/download/v1.3.1/Minecraft.Vape.Client.v1.3.1.zip
  hxxps://github[.]com/[Threat Actor Account]/ms-rewards-automation/releases/download/v1.8.1/ms-rewards-automation.v1.8.1.zip
  hxxp://github[.]com/[Threat Actor Account]/ddos-protection/releases/download/uncork/ddos-protection-uncork.zip
  hxxp://github[.]com/[Threat Actor Account]/strongvpn/releases/download/pseudobrotherly/strongvpn_pseudobrotherly.zip
  hxxp://github[.]com/[Threat Actor Account]/VSDC-Video-Editor-Pro-Crack/releases/download/2.3.3/vsdc-video-editor-pro-crack-2.3.3.zip
  hxxp://github[.]com/[Threat Actor Account]/Instagram-Followers-Booster-v2.4.5/releases/download/v1.3.6/instagram-followers-booster-v2.4.5-v1.3.6.zip
  hxxps://github[.]com/[Threat Actor Account]/Call-of-Duty-Modern-Warfare-3-MW3-Hack-Cheat-Aimbot-Esp-Unban-Hwid-Unlocks-GunLVL/releases/download/desertless/Desertless.zip
  hxxps://github[.]com/[Threat Actor Account]/MCP-Manager-GUI/releases/download/v1.6.1/MCP.Manager.GUI.v1.6.1.zip
  hxxp://github[.]com/[Threat Actor Account]/Project-Zomboid-Hack/releases/download/scholae/project-zomboid-hack-scholae.zip
  hxxps://github[.]com/[Threat Actor Account]/portfolio/raw/refs/heads/main/Software.zip

Upon searching for keywords such as game hacks, software crack, and automation tool, the GitHub repository containing the SmartLoader malware is displayed at the top of the search results, allowing users to easily access it.

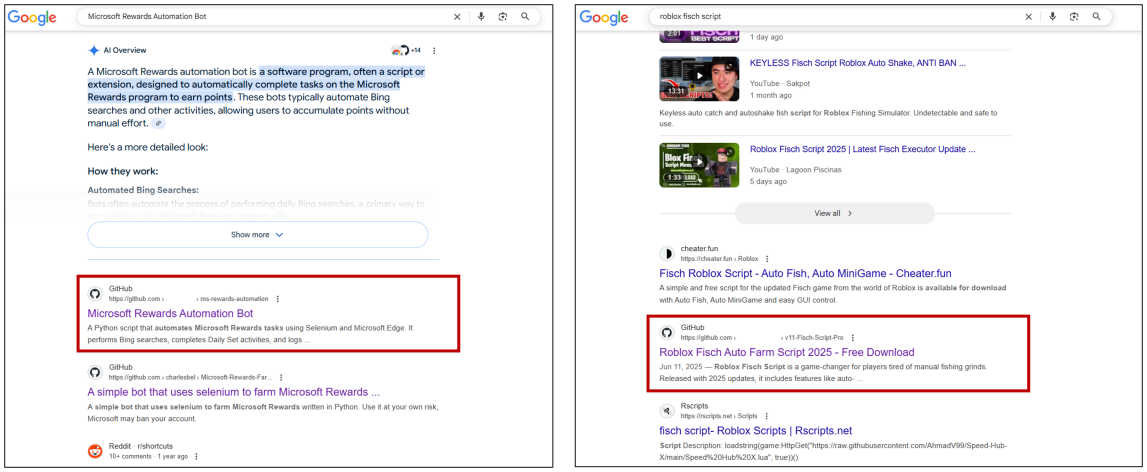


Figure 1. The SmartLoader distribution site being displayed at the top of Google search results

The GitHub repository disguised as a legitimate project contains a README file and other project-related files. The README file is well-written and includes an overview of the project, a table of contents, key features, and installation and usage instructions, making it difficult for regular users to recognize the repository as a malware distribution site. Users follow the provided installation instructions and download the compressed file, which contains the malware.

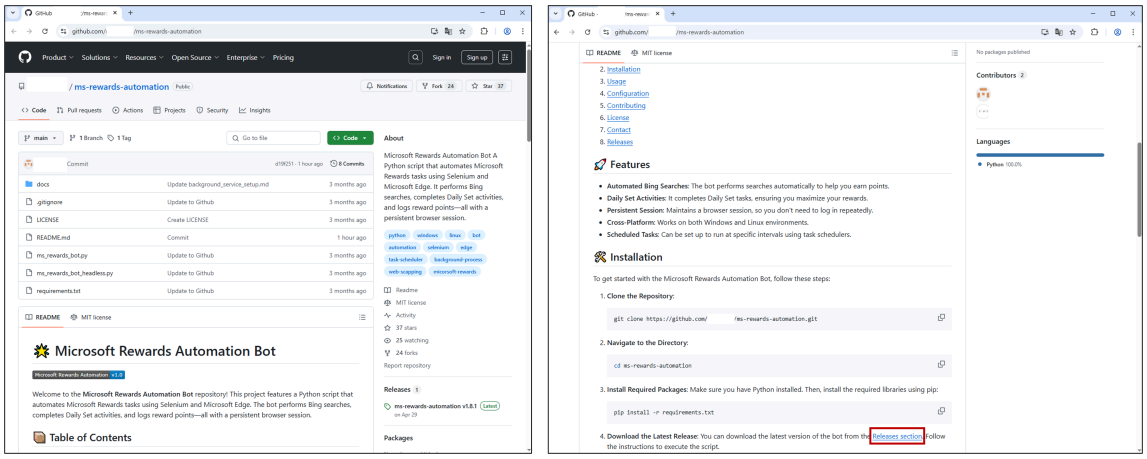


Figure 2. A GitHub repository disguised as a legitimate project (1)

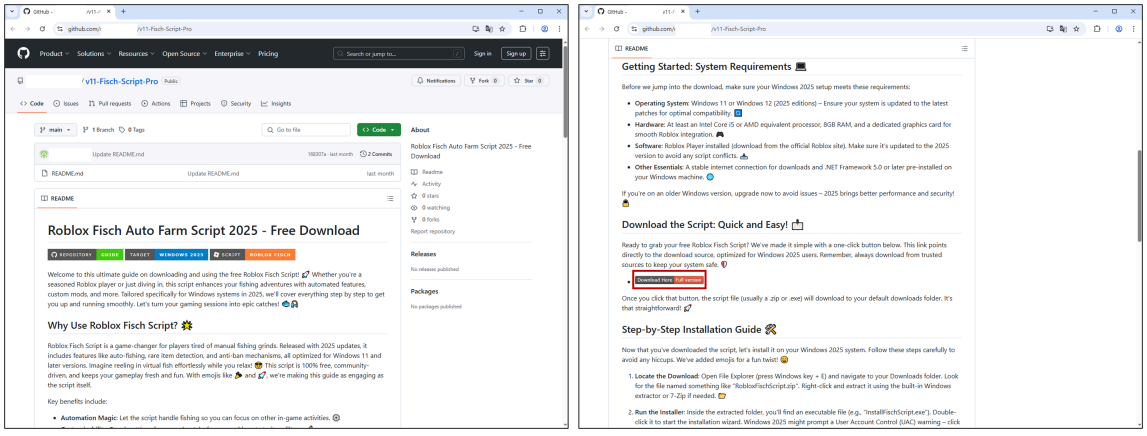


Figure 3. GitHub repository disguised as a legitimate project (2)

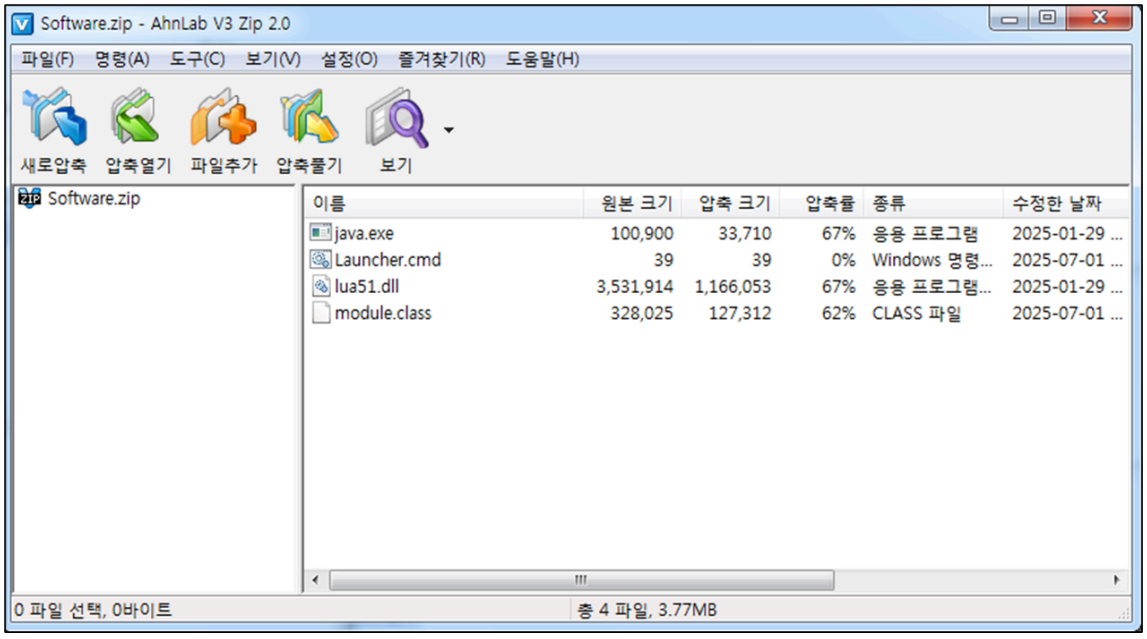


Figure 4. Files inside the compressed file

The downloaded compressed file contains a total of 4 files, each with the following functions.

- **File Features**
  java.exe: The legitimate Lua loader executable luajit.exe
  Launcher.cmd: A malicious batch file that executes java.exe with module.class as an argument (malicious)
  lua51.dll: Luajit runtime interpreter (legitimate)
  module.class: Obfuscated Lua script (malicious)

When a user executes the Launcher.cmd file to install it, the obfuscated malicious Lua script is loaded through luajit.exe (Lua loader), and SmartLoader is ultimately activated. To maintain persistence, SmartLoader copies the luajit.exe (ODE3.exe), module.class, and lua51.dll files to the “%AppData%\ODE3” path and registers it in the Task Scheduler as “SecurityHealthService_ODE3”.

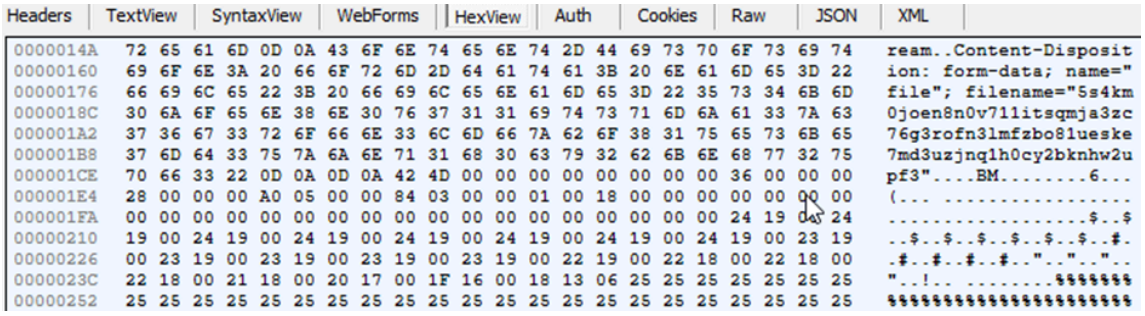


Figure 5. Sending a screenshot (BMP file)

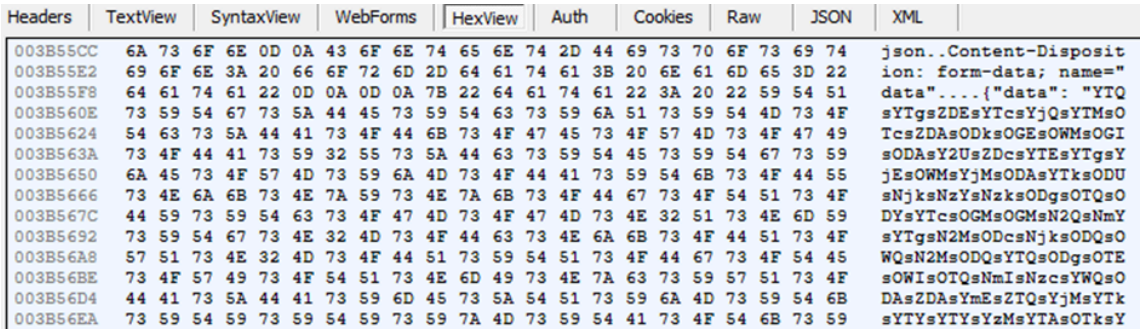


Figure 6. Transmission of system information (encoded form)

Afterward, a screenshot of the infected PC and its system information are transmitted to the C2 server. Additional malicious behaviors are then performed based on the response value received from the server. The data exchanged with the C2 server is transmitted in an encrypted form through Base64 encoding and byte operations. The key value used in this process exists in an obfuscated form within the Lua script, and the key could be obtained in the dynamic memory.

- **C2**
  hxxp://89.169.13[.]215/api/YTAsODYsODIsOWQsYTEsODgsOTAsOTUsNjUsN2Qs

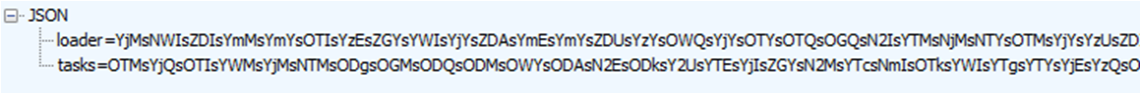


Figure 7. C2 response value

The response value is delivered in JSON format and contains two data: loader and tasks. Loader is a configuration value that controls the behavior of the malware, while tasks is a list of tasks to download and execute additional payloads. The following is the result of decoding this data using the obtained key.

Item	Decoded data
loader	{“bypass_defender”: 0, “autorun”: 0, “relaunch”: {“time”: 3600, “status”: false}, “tablet”: {“text”: “An error occurred”, “status”: false}, “hide”: 0, “persistence”: 1}
tasks	[{“id”: 814, “link”: “hxxps://github[.]com/kishoq123/Netrunner-Os-Abiy/releases/download/nasosubnasal/log.txt”, “file_path”: “AppData”, “file_name”: “Adobe**adobe.lua**“, “start”: 1, “autorun”: 0, “relaunch”: 0, “hide”: 0, “pump”: {“size”: 100, “status”: false}, “dll_loader”: {“func”: null, “type”: “LoadLibrary”}, “delivery”: “new”}, {“id”: 819, “link”: “hxxps://github[.]com/ngochoan1991/host/raw/ed0b087203fbe99717f2be9e93abc0cf9a4200c9/64.log”, “file_path”: “Temp”, “file_name”: “**_x64.bin**“, “start”: 1, “autorun”: 0, “relaunch”: 0, “hide”: 0, “pump”: {“size”: -1, “status”: false}, “dll_loader”: {“func”: null, “type”: “LoadLibrary”}, “delivery”: “new”}, {“id”: 820, “link”: “hxxps://github[.]com/ngochoan1991/host/raw/ed0b087203fbe99717f2be9e93abc0cf9a4200c9/86.log”, “file_path”: “Temp”, “file_name”: “**_x86.bin**“, “start”: 1, “autorun”: 0, “relaunch”: 0, “hide”: 0, “pump”: {“size”: -1, “status”: false}, “dll_loader”: {“func”: null, “type”: “LoadLibrary”}, “delivery”: “new”}]

Table 1. Decoded loader and tasks data

At the time of analysis, the tasks item had a total of three payloads, and after each payload is executed, the task ID and the country code of the infected PC are sent to the C2 server. The downloaded files are encoded in the same manner as described above and are decoded and executed in the memory. The functions of each file are as follows:

- **C2**
  hxxp://89.169.13[.]215/tasks/YTAsODYsODIsOWQsYTEsODgsOTAsOTUsNjUsN2Qs

1. adobe.lua

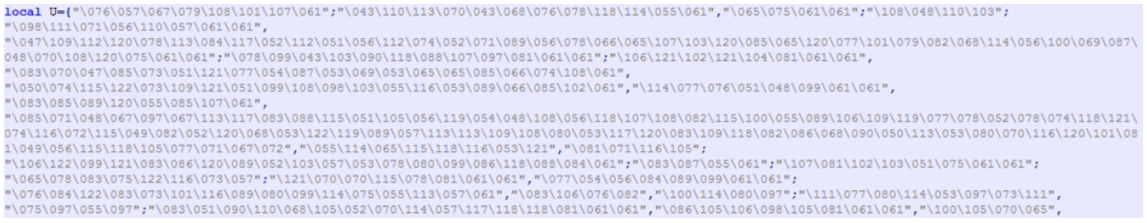


Figure 8. Decoded adobe.lua

This file is a obfuscated malicious Lua script that performs the same function as module.class. To maintain persistence, it is registered in the task scheduler under the name “WindowsErrorRecovery_ODE4”. It sends a screenshot of the infected PC and system information to the C2 server, then performs additional malicious behaviors based on the response received from the server. At the time of analysis, the tasks item was empty, so the additional malicious behavior could not be identified.

- **C2**
  hxxp://95.164.53[.]26/api/YTAsODYsODIsOWQsYTEsODgsOTAsOTUsNjUsN2Qs

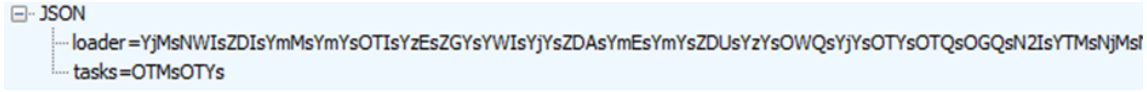
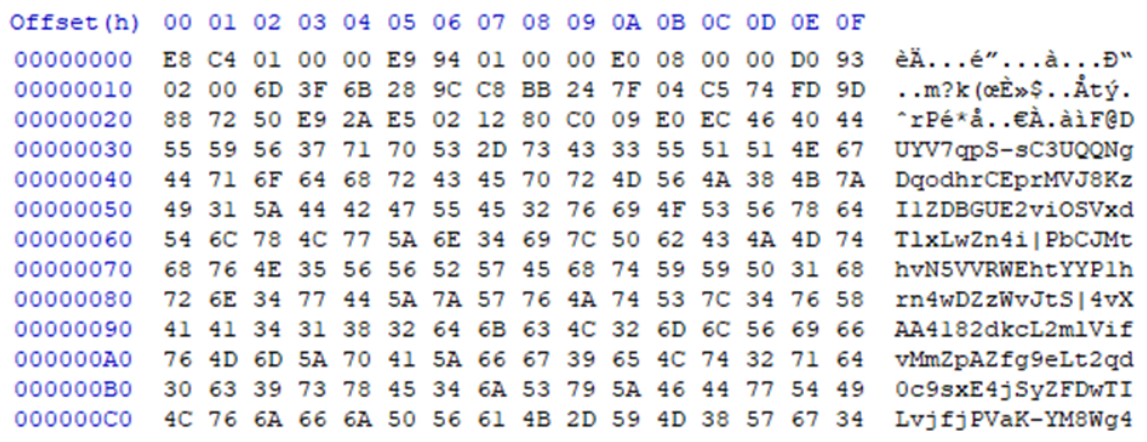


Figure 9. C2 response value

2. _x64.bin



Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	
00000000	E8	C4	01	00	00	E9	94	01	00	00	E0	08	00	00	D0	93	èÄ...é”...à...Ð“
00000010	02	00	6D	3F	6B	28	9C	C8	BB	24	7F	04	C5	74	FD	9D	..m?k(œÈ»$..Åtý.
00000020	88	72	50	E9	2A	E5	02	12	80	C0	09	E0	EC	46	40	44	ˆrPé*å..€À.àìF@D
00000030	55	59	56	37	71	70	53	2D	73	43	33	55	51	51	4E	67	UYV7qpS-sC3UQQNg
00000040	44	71	6F	64	68	72	43	45	70	72	4D	56	4A	38	4B	7A	DqodhrCEprMVJ8Kz
00000050	49	31	5A	44	42	47	55	45	32	76	69	4F	53	56	78	64	I1ZDBGUE2viOSVxd
00000060	54	6C	78	4C	77	5A	6E	34	69	7C	50	62	43	4A	4D	74	TlxLwZn4i|PbCJMt
00000070	68	76	4E	35	56	56	52	57	45	68	74	59	59	50	31	68	hvN5VVRWEhtYYP1h
00000080	72	6E	34	77	44	5A	7A	57	76	4A	74	53	7C	34	76	58	rn4wDZzWvJtS|4vX
00000090	41	41	34	31	38	32	64	6B	63	4C	32	6D	6C	56	69	66	AA4182dkcL2mlVif
000000A0	76	4D	6D	5A	70	41	5A	66	67	39	65	4C	74	32	71	64	vMmZpAZfg9eLt2qd
000000B0	30	63	39	73	78	45	34	6A	53	79	5A	46	44	77	54	49	0c9sxE4jSyZFDwTI
000000C0	4C	76	6A	66	6A	50	56	61	4B	2D	59	4D	38	57	67	34	LvjfjPVaK-YM8Wg4

Figure 10. Decoded _x64.bin

The file is a ShellCode that operates in a 64-bit environment and has been identified as the Infostealer malware, Rhadamanthys. Rhadamanthys performs injection into normal processes in Windows systems, and ultimately exfiltrates sensitive information related to email, FTP, and online banking services to the threat actor’s server.

- **Injection Target Processes**
  %Systemroot%\system32\openwith.exe
  %Systemroot%\system32\dialer.exe
  %Systemroot%\system32\dllhost.exe
  %Systemroot%\system32\rundll32.exe

3. _x86.bin

```
Offset(h)  00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F
00000000   E8 AB 01 00 00 E9 94 01 00 00 60 07 00 00 50 8C  è«...é”...`...PŒ
00000010   02 00 6D 3F 6B 28 9C C8 BB 24 7F 04 C5 74 FD 9D  ..m?k(œÈ»$..Åtý.
00000020   88 72 50 E9 2A E5 02 12 80 C0 09 E0 EC 46 40 71  ˆrPé*å..€À.àìF@q
00000030   76 6D 41 62 42 52 4E 54 4E 32 68 54 6E 79 34 33  vmAbBRNTN2hTny43
00000040   42 45 53 45 65 38 69 66 4D 75 79 57 2D 66 5A 4B  BESEe8ifMuyW-fZK
00000050   68 51 63 63 71 79 58 66 5A 71 34 4E 70 65 75 4A  hQccqyXfZq4NpeuJ
00000060   75 58 44 76 32 65 6B 74 46 64 43 63 57 70 4C 45  uXDv2ektFdCcWpLE
00000070   49 61 6A 70 61 43 4F 7A 68 6D 44 58 66 7A 41 4F  IajpaCOzhmDXfzAO
00000080   51 56 6D 4D 50 65 75 7A 59 4E 46 52 49 78 53 54  QVmMPeuzYNFRIxST
00000090   4B 30 55 4E 57 69 48 6B 70 74 45 52 46 74 36 59  K0UNWiHkptERFt6Y
000000A0   73 4F 77 77 68 62 78 73 49 78 38 69 70 5A 56 4B  sOwwhbxsIx8ipZVK
000000B0   79 6E 53 75 79 43 39 45 55 71 68 31 4B 42 51 65  ynSuyC9EUqh1KBQe
000000C0   51 6F 51 6B 6F 37 71 63 58 34 65 36 48 41 43 70  QoQko7qcX4e6HACp
```

Figure 11. Decoded _x86.bin

This file is a ShellCode that operates in a 32-bit environment, performing the same functions as the _x64.bin file. It is the Rhadamanthys malware.

SmartLoader is mainly used to download InfoStealer malware, and there have been many cases of it being used to execute other malware such as Rhadamanthys, Redline, and Lumma Stealer. As paths searched using illegal or unofficial keywords such as game hacks, cracks, and automation tools are highly likely to lead to malware, software must be downloaded from official sources. Even if a README file is meticulously written, the repository may still be malicious, so the source of the repository, the credibility of the author, and the commit and activity history must be checked.

MD5

2ed91e48a8a0b731ca3a3f6a7708256d

4d744f3e77a4cb86a676da9c0a28b186

952065a30e60fb71a5a27e0b78233cf1

bd48378e8370372f1c59e404bcb5c840

e5c783b9c1a70bd10efb66a79ff55ea1

Additional IOCs are available on AhnLab TIP.

URL

http[:]//150[.]241[.]108[.]62/api/YTAsODYsODIsOWQsYTEsODgsOTAsOTUsNjUsN2Qs

http[:]//77[.]105[.]164[.]178/api/YTAsODYsODIsOWQsYTEsODgsOTAsOTUsNjUsN2Qs

http[:]//89[.]169[.]12[.]179/api/YTAsODYsODIsOWQsYTEsODgsOTAsOTUsNjUsN2Qs

http[:]//89[.]169[.]13[.]215/api/YTAsODYsODIsOWQsYTEsODgsOTAsOTUsNjUsN2Qs

http[:]//89[.]169[.]13[.]215/tasks/YTAsODYsODIsOWQsYTEsODgsOTAsOTUsNjUsN2Qs

Additional IOCs are available on AhnLab TIP.

Gain access to related IOCs and detailed analysis by subscribing to **AhnLab TIP**. For subscription details, click the banner below.

Source: https://asec.ahnlab.com/en/89551/