Analysis of Pupy RAT Used in Attacks Against Linux Systems

By ATCP

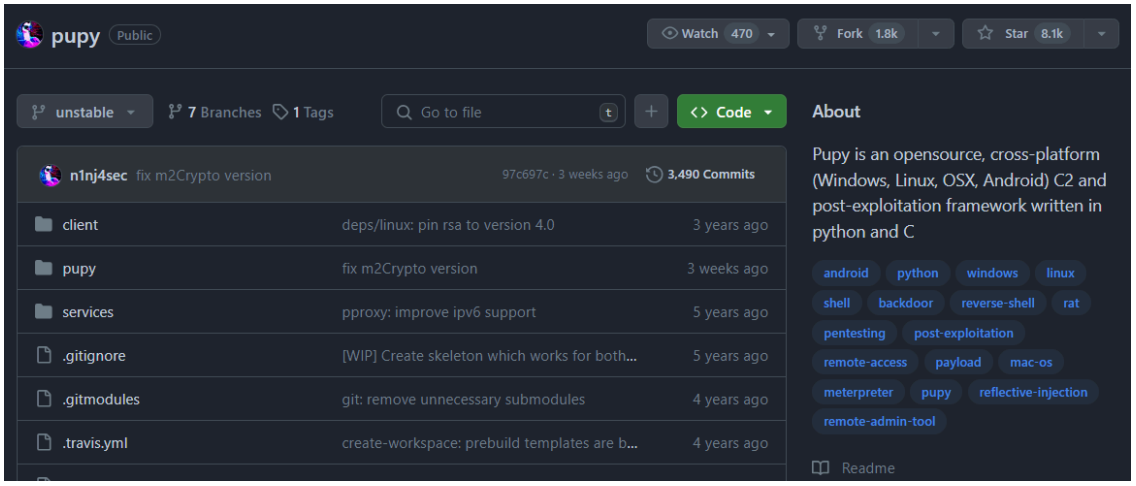
Published: 2024-04-10 · Archived: 2026-04-06 00:04:00 UTC

Pupy is a RAT malware strain that offers cross-platform support. Because it is an open-source program published on GitHub, it is continuously being used by various threat actors including APT groups. For example, it is known to have been used by APT35 (said to have ties to Iran) [1] and was also used in Operation Earth Berberoka [2] which targeted online gambling websites. Recently, a malware strain named Decoy Dog was discovered, which is an updated version of Pupy RAT. Decoy Dog was used in attacks against corporate networks in Russia and Eastern Europe. [3]

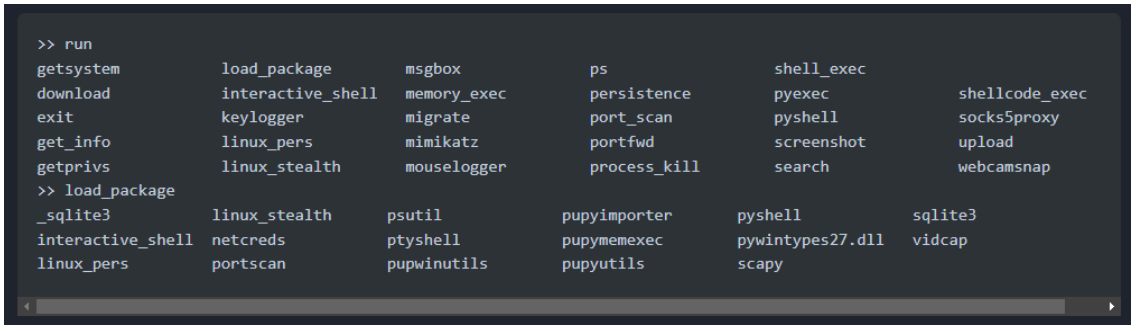
This post will provide a basic overview of Pupy RAT and cover attack cases identified during the analysis process. Major examples include attacks against Linux systems in South Korea and the Pupy RAT malware versions that have been distributed for several years to Asian countries.

1. PupyRAT

Published on GitHub, Pupy RAT was written based on C and Python. It supports Windows and Linux operating systems and can also support Mac OSX and Android, albeit to a limited degree.



Because it is a RAT malware type, it supports features such as command execution, handling files and processes, and uploading and downloading files. It also provides information theft features such as capturing screenshots and keylogging. Unlike ordinary RATs, Pupy RAT supports post-exploitation modules, which make follow-up attacks such as privilege escalation, account credential theft, and lateral movement possible.



Malware strains that target Linux systems generally have their process names changed to resemble normal processes to conceal themselves. One of the characteristics of Pupy RAT is that it changes the process name to “/usr/sbin/atd” at runtime by default. Of course, some threat actors may use different path names. The different names can be used as one of the factors for distinguishing threat actors alongside the first 8 digits of the Revision number that is saved when building Pupy RAT.

```
334     BOOL init_pupy(void)
335     {
336             PyObject *pupy = Py_InitModule3("_pupy", methods, module_doc);
337             if (!pupy) {
338                     return FALSE;
339             }
340
341             PyModule_AddStringConstant(pupy, "revision", GIT_REVISION_HEAD);
342             ExecError = PyErr_NewException("_pupy.error", NULL, NULL);
```

```
27      #ifndef DEFAULT_ARGV0
28      #define DEFAULT_ARGV0 "/usr/sbin/atd"
29      #endif
```

2. Cases of Attacks Against Asian Countries

The following are cases where the malware is believed to be created and distributed by the same threat actor. Based on the information on VirusTotal, the malware strains are distributed with the names being variants of “nptd” or “kworker”. They were mainly collected in Asian regions including not only Taiwan, Hong Kong, and Singapore, but also Japan and Thailand.

Date	Region	Name
2023-12-09 12:41:00 UTC	HONG KONG	kworker
2023-12-09 15:28:06 UTC	SINGAPORE	kworker

Date	Region	Name
2022-07-04 07:28:31 UTC	HONG KONG	ntpd
2022-11-13 08:21:12 UTC	TAIWAN	ntpd

Date	Region	Name
2021-12-10 17:20:28 UTC	TAIWAN	kworkers0id

The attacks have been continuing from 2021 to recent times, and the malware strain is still available for download even as of right now. The threat actor used several addresses over many years to upload the malware and use them as C&C servers.

Note that Cobalt Strike is one of the malware strains that share the same download and C&C server URL. Thus, the threat actor probably targeted Linux systems as well as Windows systems using Cobalt Strike. Seeing from the malware icons and file names such as “ChromeSetup.exe” and “刘中盛—运维工程师-大型企业内网运维-个人简历.docx.exe”, they are believed to have been distributed via web pages disguised as download pages for legitimate software or through spear phishing attacks.

```
BeaconType                      - HTTPS
Port                            - 443
SleepTime                       - 45000
MaxGetSize                      - 1403644
Jitter                          - 37
MaxDNS                          - Not Found
PublicKey_MD5                   - 9a9550a4b2acebe24a502c69a4396e1b
C2Server                        - api1-cdn.com,/jquery-3.3.1.min.js
UserAgent                       - Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
HttpPostUri                     - /jquery-3.3.2.min.js
Malleable_C2_Instructions       - Remove 1522 bytes from the end
                                  Remove 84 bytes from the beginning
                                  Remove 3931 bytes from the beginning
                                  Base64 URL-safe decode
                                  XOR mask w/ random key
HttpGet_Metadata                - ConstHeaders
                                       Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
                                       Referer: http://code.jquery.com/
                                       Accept-Encoding: gzip, deflate
                                  Metadata
                                       base64url
                                       prepend "__cfduid="
                                       header "Cookie"
HttpPost_Metadata               - ConstHeaders
                                       Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
                                       Referer: http://code.jquery.com/
                                       Accept-Encoding: gzip, deflate
                                  SessionId
```

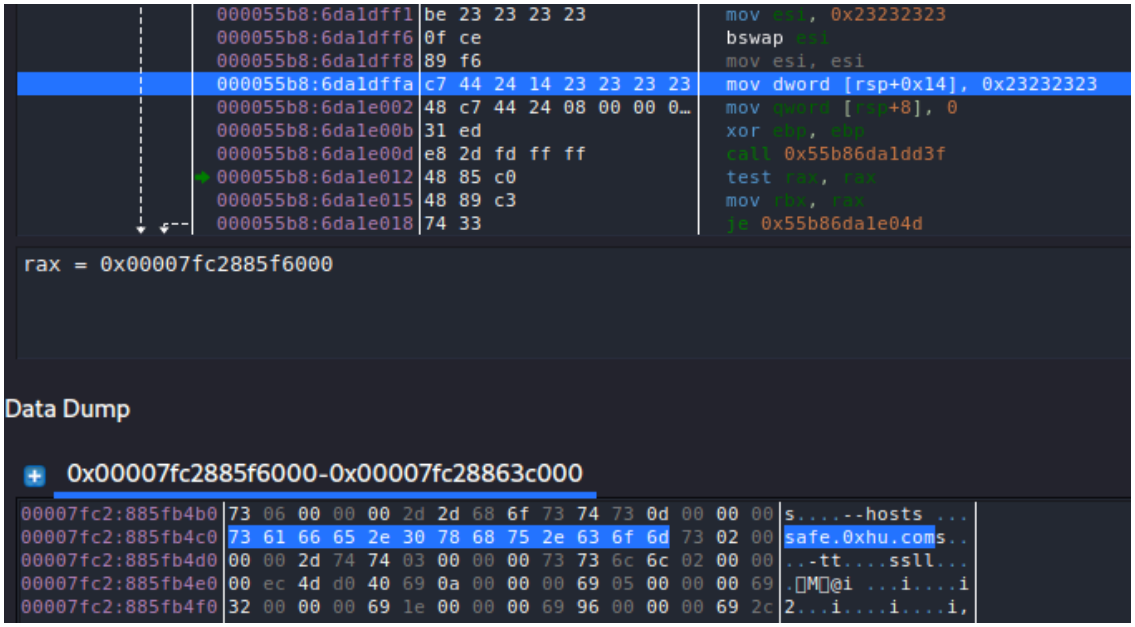
3. Analysis of Attacks Against South Korea

Pupy RAT is continuously being collected in South Korea as well. Based on the provided IoCs, there is a case where Pupy RAT was distributed alongside PlugX around 2019. PlugX is one of the major backdoors used by APT threat groups that are based in China. It is known to have been distributed from around 2008. Mustang Panda, Winnti, APT3, and APT41 are the main APT threat groups that have used PlugX in their attacks, most of them being known to be based in China.

```
10002EB7   81FE 380A0000   CMP ESI,0A38
10002EBD ^ 7C D4           JL SHORT 10002E93
10002EBF   813D 9C930210   CMP DWORD PTR DS:[1002939C],12345678
10002EC9 v 0F84 CD010000   JE 1000309C
10002ECF   A1 24A30210     MOV EAX,DWORD PTR DS:[1002A324]
10002ED4   85C0            TEST EAX,EAX
10002ED6 v 75 16           JNE SHORT 10002EEE
10002ED8   A1 342B0210     MOV EAX,DWORD PTR DS:[10022B34]
10002EDD   68 9CF90110     PUSH 1001F99C                    ASCII "MessageBoxA"
10002EE2   50              PUSH EAX
10002EE3   FF15 402B0210   CALL DWORD PTR DS:[10022B40]
10002EE9   A3 24A30210     MOV DWORD PTR DS:[1002A324],EAX
10002EEE   68 40002000     PUSH 200040
10002EF3   6A 00           PUSH 0
10002EF5   68 F0910110     PUSH 100191F0                    ASCII "CONFIG-ERR!"
10002EFA   6A 00           PUSH 0
Imm=12345678
[1002939C]=12345678
```

```
Address   Hex dump                                          ASCII
10029398  0E 60 4D 2C 78 56 34 12 E8 03 00 00 40 0D 03 00  ♫`M,xV4‼è└ @ └
100293A8  01 00 BB 01 34 35 2E 33 32 2E 38 2E 31 34 33 00  ┌ »┌45.32.8.143
100293B8  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
100293C8  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
100293D8  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
100293E8  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
100293F8  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
10029408  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
10029418  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
10029428  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
10029438  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
10029448  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
10029458  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
10029468  00 00 00 00 00 00 16 00 31 32 37 2E 30 2E 30 2E      ┬ 127.0.0.
10029478  31 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  1
```

There was also a case where Pupy RAT was uploaded on a currently closed Korean Windows utility-sharing website around 2023, although the specific infection route has not been ascertained.



4. Conclusion

Pupy RAT is a malware strain that can receive commands from the C&C server and control the infected system. It not only supports basic commands but also provides information extortion and proxy features among various others. Aside from these features provided by ordinary RAT malware, it also has various other features for follow-up attacks such as privilege escalation, account credential theft, and lateral movement.

Because the malware is an open-source program and supports various platforms, it is used by various threat actors including APT groups. While most of the known attacks target Windows systems, it is constantly used in attacks targeting Linux servers as well. Most of the recently identified malware variants that target Linux systems were collected in Asian countries, with cases also reported from Korea.

To prevent such security threats, users must check their vulnerable environment configuration or credentials and always update relevant systems to the latest versions to defend systems from threats. Also, V3 should be updated to the latest version so that malware infection can be prevented.

File Detection

– Malware/Win32.Generic.C3121812 (2019.03.24.09)
– Backdoor/Win.CobaltStrike.C5611386 (2024.04.11.03)
– Downloader/Win.CobaltStrike.C5611385 (2024.04.11.03)
– Backdoor/Linux.PupyRAT.3414160 (2024.04.08.02)
– Backdoor/Linux.PupyRAT.3700880 (2024.04.08.02)
– Backdoor/Linux.PupyRAT.3713536 (2021.07.09.02)
– Linux/Agent.2652544 (2019.08.04.00)

MD5

1358d7f17b0882a38a3cfa88df256fc1

16b088b75442e247a8c53161a8a130b0

1738429d3737b22d52b442c4faef50a1

2c802c1fac3b0035b2a79cbd56510caa

2f378559b835cbe9ec9874baec73a578

Additional IOCs are available on AhnLab TIP.

URL

http[:]//45[.]32[.]16[.]248/adobe[.]dll

http[:]//45[.]32[.]16[.]248/lvmetad

http[:]//api[.]api-alipay[.]com/kworker0ytj

http[:]//api[.]api-alipay[.]com/kworker37yu

http[:]//api[.]api-alipay[.]com/kworker54c8

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/64258/