PureLogs Forensics

By Erik Hjelmvik

Published: 2025-07-02 · Archived: 2026-04-05 18:05:15 UTC

,

Wednesday, 02 July 2025 11:52:00 (UTC/GMT)

I analyzed some PureLogs Stealer malware infections this morning and found some interesting behavior and artifacts that I want to share.

PureLogs infections sometimes start with a dropper/downloader (PureCrypter) that retrieves a .pdf file from a legitimate website. The dropper I will demo here downloaded this file:

> hxxps://www.vastkupan[.]com/wp-admin/js/Daupinslenj.pdf

This file isn't really a PDF though, but more on that later. Here's a CapLoader screenshot with some interesting flows from the infection:

Server_IP	Server_	Trans	Protocol	Hostname	JA3	JA4
192.168.100.2	53	UDP	DNS			
185.15.121.100	443	TCP	TLS	www.vastkupan.com	3b5074...	t12d210...
91.92.120.101	65535	TCP	PureLogs			
91.92.120.101	65535	TCP	PureLogs			
91.92.120.101	65535	TCP	PureLogs			

The PCAP in the screenshot above comes from a sandbox execution on any.run of a file called BSN100357-HHGBM100002525.exe.

Here's a breakdown of what happens behind the scenes in this execution:

1. Dropper connects to www.vastkupan[.]com (DNS and TLS flows).
2. A fake PDF (Daupinslenj.pdf) is downloaded over HTTPS.
3. The fake PDF is decrypted to a DLL (PureLogs), which is stored in memory.
4. InstallUtil.exe is started.
5. The PureLogs DLL is injected into the running InstallUtil process.
6. PureLogs connects to C2 server at 91.92.120.101:65535

The same dropper has also been run on JoeSandbox, with almost identical behavior. The vastkupan.com website belongs to a legitimate company (Västkupan Fastigheter).

The PDF that Wasn't

This is what the downloaded "PDF" looks like:

```
xxd Daupinslenj.pdf | head
00000000: 7a6b a137 3231 3731 3537 3131 c8ce 3137  zk.721715711..17
00000010: 8931 3731 3137 3131 7731 3137 3131 3731  .1711711w1171171
00000020: 3137 3131 3731 3137 3131 3731 3137 3131  1711711711711711
00000030: 3731 3137 3131 3731 3137 3131 b731 3137  711711711711.117
00000040: 3f2e 8d3f 3183 38fc 1689 307b fc10 6359  ?..?1.8...0{..cY
00000050: 5844 1141 455e 5645 505c 1752 5059 5f5e  XD.AE^VEP\.RPY_^
00000060: 4311 5352 1143 425f 115e 5f11 737e 6217  C.SR.CB_.^_.s~b.
00000070: 5c5e 5354 1f3a 3c3b 1331 3137 3131 3731  \^ST.:<;.1171171
00000080: 6172 3131 7b30 3237 75af 6459 3137 3131  ar11{027u.dY1711
00000090: 3731 3137 d131 3910 3a36 0131 371f 0437  7117.19.:6.17..7
```

So, what's up with all that "171171" data? Let's XOR with "711" and see what we get.

```
xxd Daupinslenj.decoded | head
00000000: 4d5a 9000 0300 0000 0400 0000 ffff 0000  MZ..............
00000010: b800 0000 0000 0000 4000 0000 0000 0000  ........@.......
00000020: 0000 0000 0000 0000 0000 0000 0000 0000  ................
00000030: 0000 0000 0000 0000 0000 0000 8000 0000  ................
00000040: 0e1f ba0e 00b4 09cd 21b8 014c cd21 5468  ........!..L.!Th
00000050: 6973 2070 726f 6772 616d 2063 616e 6e6f  is program canno
00000060: 7420 6265 2072 756e 2069 6e20 444f 5320  t be run in DOS
00000070: 6d6f 6465 2e0d 0d0a 2400 0000 0000 0000  mode....$.......
00000080: 5045 0000 4c01 0300 449e 5368 0000 0000  PE..L...D.Sh....
00000090: 0000 0000 e000 0e21 0b01 3000 002e 3500  .......!..0...5.
```

The downloaded PDF turns out to be a .NET DLL file with MD5 38d29f5ac47583f39a2ff5dc1c366f7d. This is the file that was injected into the otherwise legitimate InstallUtil process. Some PureLogs droppers use RegAsm.exe instead of InstallUtil though (see JoeSandbox and any.run).

IOC List

Droppers (MD5):

- 711d9cbf1b1c77de45c4f1b1a82347e6
- 6ff95e302e8374e4e1023fbec625f44b
- e6d7bbc53b718217b2de1b43a9193786
- a9bc0fad0b1a1d6931321bb5286bf6b7
- 09bb5446ad9055b9a1cb449db99a7302

Dropper TLS handshake signatures:

- JA3: 3b5074b1b5d032e5620f69f9f700ff0e
- JA4: t12d210700_76e208dd3e22_2dae41c691ec

Payload URLs:

- hxxps://www.vastkupan[.]com/wp-admin/js/Cicdwkknms.pdf
- hxxps://www.vastkupan[.]com/wp-admin/js/Daupinslenj.pdf

- hxxps://www.new.eventawardsrussia[.]com/wp-includes/Ypeyqku.pdf

Payloads (MD5):

- ab250bb831a9715a47610f89d0998f86 (Cicdwkknms.pdf)
- cec53e8df6c115eb7494c9ad7d2963d4 (Daupinslenj.pdf)
- eedc8bb54465bd6720f28b41f7a2acf6 (Ypeyqku.pdf)

Decrypted payloads:

- MD5: 38d29f5ac47583f39a2ff5dc1c366f7d
- SHA1: fc8b0ee149027c4c02f7d44cc06cade3222bb6b6
- SHA256: 8d7729ca0b25a677287076b4461304a21813e6f15053e190975512e58754988f

PureLogs C2:

- 91.92.120.101:62520 (old)
- 91.92.120.101:65535 (new)

Update 2025-07-16

Additional PureLogs payloads have been found on vastkupan.com.

Payload URLs:

- hxxps://www.vastkupan[.]com/wp-admin/js/Cxqyoub.dat
- hxxps://www.vastkupan[.]com/wp-admin/js/Qlwxqgsag.dat

Cxqyoub.dat is decrypted by XOR-ing with "414".

```
$ curl -s https://www.vastkupan.com/wp-admin/js/Cxqyoub.dat | xxd | head
00000000: 796b a434 3234 3431 3034 3134 cbce 3434  yk.424410414..44
00000010: 8934 3431 3434 3134 7431 3434 3134 3431  .4414414t1441441
00000020: 3434 3134 3431 3434 3134 3431 3434 3134  4414414414414414
00000030: 3431 3434 3134 3431 3434 3134 b431 3434  414414414414.144
00000040: 3f2b 8e3f 3480 38f9 1589 3578 fc15 6059  ?+.?4.8...5x..`Y
00000050: 5d47 1144 465e 5346 5059 1452 555a 5f5b  ]G.DF^SFPY.RUZ_[
00000060: 4011 5651 1146 415f 145d 5f14 707e 6714  @.VQ.FA_.]_.p~g.
00000070: 5c5b 5054 1a39 3c3e 1031 3434 3134 3431  \[PT.9<>.1441441
00000080: 6471 3134 7830 3734 60a1 4059 3434 3134  dq14x074`.@Y4414
00000090: 3431 3434 d134 3a10 3f35 0134 3419 0134  4144.4:.?5.44..4
```

Qlwxqgsag.dat is a DLL with reversed content.

```
$ curl -s https://www.vastkupan.com/wp-admin/js/Qlwxqgsag.dat | xxd | tail
00352760: 0035 2000 0030 010b 210e 00e0 0000 0000  .5 ..0..!.......
00352770: 0000 0000 686e dba3 0003 014c 0000 4550  ....hn.....L..EP
00352780: 0000 0000 0000 0024 0a0d 0d2e 6564 6f6d  .......$....edom
00352790: 2053 4f44 206e 6920 6e75 7220 6562 2074   SOD ni nur eb t
003527a0: 6f6e 6e61 6320 6d61 7267 6f72 7020 7369  onnac margorp si
003527b0: 6854 21cd 4c01 b821 cd09 b400 0eba 1f0e  hT!.L..!........
003527c0: 0000 0080 0000 0000 0000 0000 0000 0000  ................
003527d0: 0000 0000 0000 0000 0000 0000 0000 0000  ................
003527e0: 0000 0000 0000 0040 0000 0000 0000 00b8  .......@........
003527f0: 0000 ffff 0000 0004 0000 0003 0090 5a4d  ..............ZM
```

Payloads (MD5):

- 22a304ea9c006e2ccb2f6110c4d3f53f (Cxqyoub.dat)
- d5b6607ee4718506eb4970c02cf286cd (XOR decrypted DLL from Cxqyoub.dat)
- 062d2a5906fac4c2ef07c6b43141e19c (Qlwxqgsag.dat)
- 40624de03bc3c53331b6e903d9e3860f (DLL from reversed Qlwxqgsag.dat)

C2 server:

- 91.92.120.102:62050

See JoeSandbox and any.run for sandbox executions of the dropper aa06d06ddb6d3801c70cc1991f393112 (retrieves Cxqyoub.dat), and JoeSandbox and any.run for c45a95dc7ebc8c78217cd996a8f6dda7 (gets Qlwxqgsag.dat).

Update 2025-07-21

Yet another PureLogs payload found on vastkupan.com.

- Dropped by: 031a9c2f44881f4db1c6f6d88a540206
- URL of encrypted DLL: hxxp://www.vastkupan[.]com/wp-admin/js/Kplbc.pdf
- Encrypted DLL MD5: 6ed3c9b70ca02d1c558d1ef9a8aaab77
- C2: 65.108.24.103:62050

Sandbox executions are available on JoeSandbox and any.run.

Update 2025-07-30

Additional encrypted PureLogs DLLs found on vastkupan.com

- Dropped by: 67861615d765d0c59d65e8d4454e5ffc
- URL of encrypted DLL: hxxps://www.vastkupan[.]com/wp-admin/js/Qytqk.pdf
- Encrypted DLL MD5: 668a42bdfd253e0d54716cd115479b9f
- C2: 91.92.120.102:62050 (same as Cxqyoub.dat and (Qlwxqgsag.dat)

- Dropped by: 031a9c2f44881f4db1c6f6d88a540206
- URL of encrypted DLL: hxxps://www.vastkupan[.]com:443/wp-admin/js/Kplbc.pdf

- Encrypted DLL MD5: 6ed3c9b70ca02d1c558d1ef9a8aaab77
- C2: 65.108.24.103:62050

- Dropped by: 07ff4006101f117aa4f198c984a45137
- URL of encrypted DLL: hxxps://www.vastkupan[.]com/wp-admin/js/Pnnvrpjewlq.vdf
- Encrypted DLL MD5: 98cf831688941cc8bccfe1e8a33c9c16

- Dropped by: a1fd8053b49442028d66e3adea550d19
- URL of encrypted DLL: hxxps://www.vastkupan[.]com/wp-admin/js/Niose.wav
- Encrypted DLL MD5: 067086aff11080357b92931e96ecebae

- Dropped by: 3cf704e64cbba6560663ec45ce2dabc2
- URL of encrypted DLL: hxxps://www.vastkupan[.]com:443/wp-admin/js/Frfkft.vdf
- Encrypted DLL MD5: c9bac721c9b6f2900fd3d8ed922bc759
- C2: 91.92.120.101:7705

- Dropped by: 486d6c9cbdb638f9d574c58459676ed9
- URL of encrypted DLL: hxxps://www.vastkupan[.]com/wp-admin/js/Skrcygatz.dat
- Encrypted DLL MD5: a3cf5108315a06d564c97c8367994fd1
- C2: 216.250.252.231:2080

Update 2025-07-31

Turns out the whole /wp-admin/js/ directory on Västkupan's website allows directory listing. Among the files in that directory is "New PO 102456688.exe", which drops PureLogs.

Name	Last Modified	Size
Parent Directory		
Irtnuo.vdf	2025-07-30 19:23	1386k
Ugylek.dat	2025-07-30 19:12	1387k
Thxyp.vdf	2025-07-30 19:07	1387k
New PO 102456688.exe	2025-07-30 10:38	85k
Kvoswopqpy.vdf	2025-07-30 10:32	1382k
Extbsasoude.pdf	2025-07-30 06:27	1388k

- Filename: New PO 102456688.exe
- MD5: b2647b263c14226c62fe743dbff5c70a
- C2: 147.124.219.201:65535

See executions on Tria.ge and any.run for details.

Posted by Erik Hjelmvik on Wednesday, 02 July 2025 11:52:00 (UTC/GMT)

Tags: #PureLogs#PureCoder#3b5074b1b5d032e5620f69f9f700ff0e#JoeSandbox

Short URL: https://netresec.com/?b=257eead
