UNCOVERING AND VISUALIZING MALICIOUS INFRASTRUCTURE
ABOUT US
ANDREA SCARFO
Security Research Manager & Security Researcher
Cisco Umbrella (formerly OpenDNS) in San Francisco.
Joined in 2015

Previously:
System Administrator for 12 years
JOSH PYORRE
Senior Security Research Analyst & Security Researcher
Cisco Umbrella (formerly OpenDNS) in San Francisco.
Joined in 2015

Previously:
NASA
MANDIANT

Consulting for Non-Profits:
Point Blue Conservation Science
Hamilton Families
SUMMARY

- Our Research
- Finding Maliciousness
- Why Build Visualizations
- Visualizations and Findings
OUR RESEARCH
CRIMINAL ACTIVITY

<iframe src="http://far.IAAS.NEWS/?biw=OMITTEDURI" width="263" height="257"></iframe>

1. Download the "Tor Browser" from http://www.torproject.org/ and install it.
2. In the "Tor Browser" open your personal page here:
   http://p27aehpzzn7wgr.onion/DC91-E730-12F8-0095-7496

Note! This page is available via "Tor Browser" only.

Click here!!

Click here!!

$\text{SPAM}$$

here!!

$\text{CERBER RANSOMWARE}$
Mrs. Collete Gullo <qpmeyqnu@forthnet.gr>

Be careful with this message. It contains a suspicious link that was used to steal people's personal information. Unless you trust the sender, don't click links or reply with personal information. Learn more

Pardon me my baby

h00kup now so send me msg
my screen name - Collete87 ..
My account is here: http://czhonh.dategs.ru
Click and see my xxx album-
Collete87
I have much more sexy pics in the album above for you, my sweet :-* Call me!
WEBSITE COMPROMISE

<iframe src="http://far.IAAS.NEWS/?biw=OMITTEDURI" width="263" height="257"></iframe>
RATS

Remote Access Trojans
## What is there to visualize?

<table>
<thead>
<tr>
<th>IP Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>95.31.22.193</td>
</tr>
<tr>
<td>185.90.61.36</td>
</tr>
<tr>
<td>185.90.61.37</td>
</tr>
<tr>
<td>62.112.8.34</td>
</tr>
<tr>
<td>87.229.111.163</td>
</tr>
<tr>
<td>188.126.94.79</td>
</tr>
<tr>
<td>82.118.242.158</td>
</tr>
<tr>
<td>217.195.60.211</td>
</tr>
<tr>
<td>84.124.94.11</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Client Hello</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="https://40259">https://40259</a> [ACK] Seq=1 Ack=199 Win=64248 Len=0</td>
</tr>
<tr>
<td>Server Hello, Certificate, Server Hello Done</td>
</tr>
<tr>
<td>40259 → https [ACK] Seq=190 Ack=970 Win=63271 Len=0</td>
</tr>
<tr>
<td>Client Key Exchange, Change Cipher Spec, Encrypted Handshake</td>
</tr>
<tr>
<td><a href="https://40259">https://40259</a> [ACK] Seq=979 Ack=548 Win=64248 Len=0</td>
</tr>
<tr>
<td>Change Cipher Spec, Encrypted Handshake Message</td>
</tr>
<tr>
<td>40259 → https [ACK] Seq=548 Ack=1861 Win=63180 Len=0</td>
</tr>
<tr>
<td>Application Data</td>
</tr>
<tr>
<td><a href="https://40259">https://40259</a> [ACK] Seq=1861 Ack=953 Win=64240 Len=0</td>
</tr>
<tr>
<td>Application Data</td>
</tr>
<tr>
<td><a href="https://40259">https://40259</a> [ACK] Seq=1861 Ack=1742 Win=64240 Len=0</td>
</tr>
<tr>
<td>[TCP segment of a reassembled PDU]</td>
</tr>
<tr>
<td>[TCP segment of a reassembled PDU]</td>
</tr>
</tbody>
</table>
COMPROMISED DOMAINS

DEPENDS ON THE TYPE OF ATTACK
DEPENDS ON THE TYPE OF ATTACK
PHISHING DOMAINS
DEPENDS ON THE TYPE OF ATTACK

COMMAND & CONTROL DOMAINS (DGAS)

SHA256 ("2015-7-416")

TLD [16 mod 8]

5b214d2b3366d88cfcbcbf0c2133551e40da981d759b88564f7e916b50ef3bdd

q14d2b3366d88cfcbcbf0c2133551e40da.cc:443

abc [16 mod 26]
DEPENDS ON THE INFECTION METHOD

SPAM

BUY QUALITY DRUGS FROM CANADA!

TOP Products

Viagra

Generic Viagra, containing Sildenafil Citrate, enable achieve or sustain an erect penis for sexual activity. The prime treatment for erectile dysfunction.

More Info »
DEPENDS ON THE INFECTION METHOD

WEBSITE COMPROMISE

Server HackeD

By

TIGER-M@TE

#Bangladeshi Hacker

HACKED

Greetz : aBu.HaLil.501 , w7sh.syria , Sy-Hacker , NmR.Hacker , Wa7sh Hacker , h31l c0d3
DEPENDS ON THE INFECTION METHOD

EXPLOIT KITS

Phoenix Exploit's Kit 3.1 full

<table>
<thead>
<tr>
<th>Operation systems statistics</th>
<th>Advanced browsers statistics</th>
</tr>
</thead>
<tbody>
<tr>
<td>OS</td>
<td>Browser</td>
</tr>
<tr>
<td>Other</td>
<td>Other</td>
</tr>
<tr>
<td>Windows XP SP2</td>
<td>MSIE v6.0</td>
</tr>
<tr>
<td>Windows XP</td>
<td>MSIE v7.0</td>
</tr>
<tr>
<td>Windows 7</td>
<td>Firefox v11.0</td>
</tr>
<tr>
<td>Windows</td>
<td>Firefox v9.0-1</td>
</tr>
<tr>
<td>Linux</td>
<td>Opera v9.80</td>
</tr>
<tr>
<td>Windows 98</td>
<td>Safari</td>
</tr>
<tr>
<td>Windows Vista</td>
<td>MSIE v6.0</td>
</tr>
<tr>
<td>Windows 95</td>
<td>MSIE v7.01</td>
</tr>
<tr>
<td></td>
<td>Firefox v3.6.9</td>
</tr>
<tr>
<td></td>
<td>Opera v9.0</td>
</tr>
<tr>
<td></td>
<td>Firefox v1.5-0</td>
</tr>
<tr>
<td></td>
<td>Firefox v3.0-9</td>
</tr>
<tr>
<td></td>
<td>Firefox v3.6.23</td>
</tr>
<tr>
<td></td>
<td>MSIE v5.0</td>
</tr>
<tr>
<td></td>
<td>Opera v9.64</td>
</tr>
</tbody>
</table>

Menu:
- Simple statistics
- Advanced statistics
- Countries statistics
- Browsers statistics
- Sniffers statistics
- Clear statistics
- Upload log
- Exit
REACH
SIZE and SCALE
FEATURES FROM THE IOCS

2017-07-04 www.magicpharmacyinc.su

DNS queries

DNS queries/hour

DNS queries/hour

FINDING MALICIOUSNESS
ANALYZING DGAS TO FIND THE C&C
EXAMPLE OF C&C CONTACT

Layer 1
- BOTS
- Infected users/computers
- Accept and carry out commands

Layer 2
- Nodes
- More infected users act as HTTP proxies between bots and C&Cs

Layer 3
- Proxy

C&C
- Made up of compromised servers
- Act as proxy between Nodes & C&C Backend

Storage

C&C Backend Control Panel
C&C CONTACT - DOMAIN FLUX

- Large amount of changing DGA domains
- NX Domains
- Not all are registered - lots of noise to dig through
- One of the DGAs will be the C&C with a hosted IP address
PASSIVE DNS

- **DOMAIN NAMES:**
  - C&C communications
  - DGAs - resolving and NX domains

- **IP ADDRESSES:**
  - Hosting IPs

- **NAMSERVERS, EMAIL REGISTRANT:**
  - WHOIS Information

- **HASHES OF MALICIOUS BINARIES:**
  - Dropped by RATS
  - Contained in Spam
  - Dropped by compromised websites or malvertising
Tracking Hailstorm Spam
USING PASSIVE DNS

95.31.22.193
<table>
<thead>
<tr>
<th>Known domains hosted at this IP</th>
<th>857</th>
</tr>
</thead>
<tbody>
<tr>
<td>LD2 domains count</td>
<td>422</td>
</tr>
<tr>
<td>LD3 domains count</td>
<td>833</td>
</tr>
</tbody>
</table>
SELECT DOMAINS SHOW PHARMA-SPAM DOMAINS

- dcargile.denapamelina.trade
- deb.drusiloudianna.ru
- denapamelina.trade
- djejptlb.hotgenericsmart.ru
- dojwqexb.curingremedyelement.ru
- dppftabx.thesmartwebmart.ru
- dsxbetyq.medicalmedsgroup.ru
- dvcegnjy.firstdrugmall.ru
- eemxbxd.newremedyelement.ru
- ekjugnju.globalrxprogram.ru
- ekolluri.brendaalmira.trade
- elitalebbie.eu
- eqoqdmaa.thesmartwebmart.ru
- ernestinetanhya.ru
- fastherbsshop.ru
- fastmedshop.su
- fastsmartbargain.ru
- felicity.denapamelina.trade
- felizagustara.ru
- firstfirstdeal.ru
- firsthome.fullhouse.mycarequality.su
- gaeeweef.fastsmartbargain.ru
- globalpillssale.com
- globalsafegroup.ru
- goldiabrandais.ru
- goodpillscompany.su
- greg.jennylindi.eu
- gwennethjessika.ru
- homehealthvalue.su
- homeprivategroup.ru
- homeredemialnc.ru
- hotglobalquality.su
- hotgenericsmart.ru
- jcdwktvn.newremedyelement.ru
- jjudzkhq.curingbestmart.ru
- jqqzpyuh.newremedyelement.ru
- kbqobfhue.hotgenericsmart.ru
- kwwukygf.firstdrugmall.ru
- kznuxux.fastsmartbargain.ru
- lobbungy.medicalmedsgroup.ru
- londland.medicalmedsgroup.ru
- mail.bambyteriann.trade
- mail.pureaidvalue.ru
- mail.smartsecureinc.ru
- mail.xn.--b1ahtabi5ap.xn.--p1ai
- mail.xn.--b1akrmvz.xn.--p1ai
- mail.xn.--g1aii0c9b.xn.--p1ai
- medicaldrugsmall.su
- medicalhealthinc.su
- mlwndvrj.firstdrugmall.ru
- msilkryd.newremedyelement.ru
- mujsvqkh.firstdrugmall.ru
- mynbehvd.firstdrugmall.ru
- mywlenesswebmart.ru
- nestaerminia.ru
- newtabletshop.ru
- nick.dena
- ns1.blondelleevvy.ru
- ns1.brendaalmira.trade
- ns1.curingbestmart.ru
- ns1.curingremedyelement.ru
- ns1.decioldb.ru
- ns1.denapamenu.firstdrugmall.ru
- ns1.1stsmartwebmart.ru
- ns1.1stglobalprogram.ru
- ns1.goodgenericsmall.ru
- ns1.homerxwebmart.ru
- ns1.homesecondaryassist.su
- ns1.jumfzwgo.ru
- ns1.jzltets.ru
- ns1.kxibfipa.ru
- ns1.kyanpnoj.ru
- ns1.luckypillmall.su
- ns1.medicalmedsgroup.ru
- ns1.minns1.rou
- ns1.rygvnz.ru
- ns1.securepillsinc.com
- ns1.stfbrmmmg.com
- ns1.thesecurereward.ru
- ns1.thesmartwebmart.ru
- ns1.xjmqk
- ns1.brendaalmira.trade
- ns2.btsqwy.com
- ns2.curingremedyelement.ru
- ns2.curingremedygroup.ru
- ns2.denapamelina.trade
We can pivot and find even more data.

<table>
<thead>
<tr>
<th>First Seen</th>
<th>Host</th>
<th>qType</th>
<th>Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>2017-06-29 18:11:03</td>
<td>eboemghfvblqtx.thesmartvalue.ru</td>
<td>A</td>
<td>188.126.94.79</td>
</tr>
<tr>
<td>2017-06-22 00:54:48</td>
<td>eboemghfvblqtx.thesmartvalue.ru</td>
<td>A</td>
<td>62.112.8.24</td>
</tr>
<tr>
<td>2017-06-20 05:07:20</td>
<td>eboemghfvblqtx.thesmartvalue.ru</td>
<td>A</td>
<td>87.229.111.163</td>
</tr>
<tr>
<td>2017-06-20 12:35:04</td>
<td>eboemghfvblqtx.thesmartvalue.ru</td>
<td>A</td>
<td>95.31.22.193</td>
</tr>
</tbody>
</table>
We can pivot again and find even more data.

<table>
<thead>
<tr>
<th>Date</th>
<th>Website Link</th>
</tr>
</thead>
<tbody>
<tr>
<td>2017-08-01</td>
<td><a href="http://www.ytqudyxq.ru">www.ytqudyxq.ru</a></td>
</tr>
<tr>
<td>2017-08-01</td>
<td><a href="http://www.zptcuhed.ru">www.zptcuhed.ru</a></td>
</tr>
<tr>
<td>2017-08-01</td>
<td>youraidwebmart.ru</td>
</tr>
<tr>
<td>2017-08-01</td>
<td>yourmedicalinc.ru</td>
</tr>
<tr>
<td>2017-08-01</td>
<td>yourrxquality.com</td>
</tr>
<tr>
<td>2017-08-01</td>
<td>zonnyasheelagh.eu</td>
</tr>
<tr>
<td>2017-08-01</td>
<td>zptcuhed.ru</td>
</tr>
<tr>
<td>2017-07-09</td>
<td>magicmedsprogram.ru</td>
</tr>
<tr>
<td>2017-07-09</td>
<td><a href="http://www.magicmedsprogram.ru">www.magicmedsprogram.ru</a></td>
</tr>
<tr>
<td>2017-07-04</td>
<td>magicpharmacyinc.su</td>
</tr>
<tr>
<td>2017-07-04</td>
<td><a href="http://www.magicpharmacyinc.su">www.magicpharmacyinc.su</a></td>
</tr>
<tr>
<td>2017-06-29</td>
<td>yourfirsteshop.win</td>
</tr>
<tr>
<td>2017-06-19</td>
<td>eboemghfblqtx.thesmartvalue.ru</td>
</tr>
<tr>
<td>2017-06-19</td>
<td><a href="http://www.eboemghfblqtx.thesmartvalue.ru">www.eboemghfblqtx.thesmartvalue.ru</a></td>
</tr>
<tr>
<td>2017-06-18</td>
<td>goodherbvalue.ru</td>
</tr>
</tbody>
</table>
This domain is currently in the Umbrella block list

Classifier prediction: suspicious

Umbrella risk score: 90

This domain may have been created using a domain generation algorithm (DGA)

DNS queries

WHOIS Record Data

Registrar Name: MarkMonitor Inc.  IANAID: 292

Created: October 26, 2017  Updated: October 26, 2017  Expires: October 26, 2018

Email Address: admin@dnstinations.com  Associated Domains: Greater than 500 Total  Email Type: Administrative, Registrant, Technical  Last Observed: Current
This domain is currently in the Umbrella block list.

Classifier prediction: suspicious
Umbrella risk score: -90

This domain may have been created using a domain generation algorithm (DGA)

DNS queries

<table>
<thead>
<tr>
<th>Date</th>
<th>DNS queries/hour</th>
</tr>
</thead>
<tbody>
<tr>
<td>12 Oct</td>
<td></td>
</tr>
<tr>
<td>14 Oct</td>
<td></td>
</tr>
<tr>
<td>16 Oct</td>
<td></td>
</tr>
<tr>
<td>18 Oct</td>
<td></td>
</tr>
<tr>
<td>20 Oct</td>
<td></td>
</tr>
<tr>
<td>22 Oct</td>
<td></td>
</tr>
<tr>
<td>24 Oct</td>
<td></td>
</tr>
<tr>
<td>26 Oct</td>
<td></td>
</tr>
<tr>
<td>28 Oct</td>
<td></td>
</tr>
<tr>
<td>30 Oct</td>
<td></td>
</tr>
<tr>
<td>1 Nov</td>
<td></td>
</tr>
<tr>
<td>3 Nov</td>
<td></td>
</tr>
<tr>
<td>5 Nov</td>
<td></td>
</tr>
<tr>
<td>7 Nov</td>
<td></td>
</tr>
<tr>
<td>9 Nov</td>
<td></td>
</tr>
</tbody>
</table>

IP Addresses

<table>
<thead>
<tr>
<th>First seen</th>
<th>Last seen</th>
<th>IPs</th>
</tr>
</thead>
<tbody>
<tr>
<td>1/1/17</td>
<td>11/8/17</td>
<td>255.192.197.93 (TTL: 86400)</td>
</tr>
</tbody>
</table>
This domain is currently in the Umbrella block list

Classifier prediction: suspicious
Umbrella risk score: 48

This domain may have been created using a domain generation algorithm (DGA)

### DNS queries

<table>
<thead>
<tr>
<th>Date</th>
<th>DNS queries/hour</th>
</tr>
</thead>
<tbody>
<tr>
<td>12. Oct</td>
<td>0</td>
</tr>
<tr>
<td>14. Oct</td>
<td>0</td>
</tr>
<tr>
<td>16. Oct</td>
<td>0</td>
</tr>
<tr>
<td>18. Oct</td>
<td>0</td>
</tr>
<tr>
<td>20. Oct</td>
<td>0</td>
</tr>
<tr>
<td>22. Oct</td>
<td>0</td>
</tr>
<tr>
<td>24. Oct</td>
<td>0</td>
</tr>
<tr>
<td>26. Oct</td>
<td>0</td>
</tr>
<tr>
<td>28. Oct</td>
<td>0</td>
</tr>
<tr>
<td>30. Oct</td>
<td>0</td>
</tr>
<tr>
<td>1. Nov</td>
<td>0</td>
</tr>
<tr>
<td>3. Nov</td>
<td>0</td>
</tr>
<tr>
<td>5. Nov</td>
<td>0</td>
</tr>
<tr>
<td>7. Nov</td>
<td>0</td>
</tr>
<tr>
<td>9. Nov</td>
<td>0</td>
</tr>
</tbody>
</table>

**TTLs**

<table>
<thead>
<tr>
<th>Metric</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>TTLs min</td>
<td>86,400</td>
</tr>
<tr>
<td>TTLs max</td>
<td>86,400</td>
</tr>
<tr>
<td>TTLs mean</td>
<td>86,400</td>
</tr>
<tr>
<td>TTLs median</td>
<td>86,400</td>
</tr>
</tbody>
</table>
This domain is currently in the Umbrella block list.

Classifier prediction: suspicious

Umbrella risk score: 98

This domain may have been created using a domain generation algorithm (DGA)

### DNS queries

<table>
<thead>
<tr>
<th>Date</th>
<th>DNS queries/hour</th>
</tr>
</thead>
<tbody>
<tr>
<td>12. Oct</td>
<td></td>
</tr>
<tr>
<td>13. Oct</td>
<td></td>
</tr>
<tr>
<td>14. Oct</td>
<td></td>
</tr>
<tr>
<td>15. Oct</td>
<td></td>
</tr>
<tr>
<td>16. Oct</td>
<td></td>
</tr>
<tr>
<td>17. Oct</td>
<td></td>
</tr>
<tr>
<td>18. Oct</td>
<td></td>
</tr>
<tr>
<td>19. Oct</td>
<td></td>
</tr>
<tr>
<td>20. Oct</td>
<td></td>
</tr>
<tr>
<td>21. Oct</td>
<td></td>
</tr>
<tr>
<td>22. Oct</td>
<td></td>
</tr>
<tr>
<td>23. Oct</td>
<td></td>
</tr>
<tr>
<td>24. Oct</td>
<td></td>
</tr>
<tr>
<td>25. Oct</td>
<td></td>
</tr>
<tr>
<td>26. Oct</td>
<td></td>
</tr>
<tr>
<td>27. Oct</td>
<td></td>
</tr>
<tr>
<td>28. Oct</td>
<td></td>
</tr>
<tr>
<td>29. Oct</td>
<td></td>
</tr>
<tr>
<td>30. Oct</td>
<td></td>
</tr>
<tr>
<td>31. Oct</td>
<td></td>
</tr>
<tr>
<td>1. Nov</td>
<td></td>
</tr>
<tr>
<td>2. Nov</td>
<td></td>
</tr>
<tr>
<td>3. Nov</td>
<td></td>
</tr>
<tr>
<td>4. Nov</td>
<td></td>
</tr>
<tr>
<td>5. Nov</td>
<td></td>
</tr>
<tr>
<td>6. Nov</td>
<td></td>
</tr>
<tr>
<td>7. Nov</td>
<td></td>
</tr>
<tr>
<td>8. Nov</td>
<td></td>
</tr>
<tr>
<td>9. Nov</td>
<td></td>
</tr>
</tbody>
</table>

| Popularity | 11.37 |

<table>
<thead>
<tr>
<th>Requester geo distribution</th>
</tr>
</thead>
<tbody>
<tr>
<td>NG (15.79 %)</td>
</tr>
<tr>
<td>ID (15.79 %)</td>
</tr>
<tr>
<td>PS (10.53 %)</td>
</tr>
<tr>
<td>TR (10.53 %)</td>
</tr>
<tr>
<td>VE (6.26 %)</td>
</tr>
<tr>
<td>EG (5.26 %)</td>
</tr>
<tr>
<td>RO (5.26 %)</td>
</tr>
<tr>
<td>BA (5.26 %)</td>
</tr>
<tr>
<td>TH (5.26 %)</td>
</tr>
<tr>
<td>PH (5.26 %)</td>
</tr>
<tr>
<td>IR (5.26 %)</td>
</tr>
<tr>
<td>IT (5.26 %)</td>
</tr>
<tr>
<td>?? (5.26 %)</td>
</tr>
</tbody>
</table>
CO-OCCURRING DOMAINS ARE QUERIED JUST BEFORE OR AFTER A DOMAIN

Co-occurrences

fvioskxw.sc.lan (43.64)  nbhlwkrqggogyv.ac (15.22)  scrffgmsgituwwcfxx.org (6.90)  uxymnoackmgvdvlix.in (4.52)  tsxgfpoxpcnjk.xxx (3.53)
kbjxwwwxhesn.su (2.59)  evujuwheciodovlfkif.im (2.37)  poectwbq.co (2.34)  yjsvrgtibbemk.eu (1.80)  vpfpuktj.eu (1.50)  nbsqgxblmcldxfyf.sx (1.48)
qljnvxsvwnv.mu (1.44)  yenlleiywigmdu.su (1.42)  bslruyyawqgslufc.sh (1.37)  jbsppvjkdlqpfamm.com (1.37)  celpdahujm.la (1.28)  kqhragsn.ru (1.26)
emaebjksxhewetf.to (1.19)  c1qcqjflfvmavnxkcifyi.ga (1.01)  hxmlkxnl.co (0.73)  qnblqffluurnqjlm.ms (0.70)  wtturri.tv (0.70)  kqenycuytwvrfq.su (0.69)
snbqalraojexqv.ug (0.66)
OSINT

WHERE DO YOU GET DATA TO LOOK AT?

- 2017-11-07 -- A Day in the Life (of a Researcher)
- 2017-11-06 -- Hancitor malspam - Subject: Delivery failed
- 2017-11-03 -- malspam pushing Nymaim
- 2017-11-03 -- Brazil malspam pushes Banload malware
- 2017-11-02 -- Adventures with Smoke Loader
- 2017-11-01 -- Hancitor malspam (fake RingCentral fax)
- 2017-11-01 -- Necurs Botnet malspam continues pushing Locky

- 2017-10-31 -- Quick post: Hancitor malspam (Payment notice for invoice)
- 2017-10-31 -- Necurs Botnet malspam stops using DDE, still uses Word docs
- 2017-10-30 -- Hancitor malspam (View your Office 365 Business billing statement)
- 2017-10-30 -- Necurs Botnet malspam uses DDE attack to push Locky
- 2017-10-27 -- malspam pushing Remcos RAT
- 2017-10-26 -- Hancitor malspam (missed delivery/shipment/shipping notification)
- 2017-10-26 -- EITest campaign sends HoeflerText popups or fake AV page
- 2017-10-24 -- Necurs Botnet malspam uses DDE attack to push Locky
- 2017-10-24 -- Compromised site has EITest fake AV, also has colinminer javascript
- 2017-10-24 -- Phishing email, Subject: BAHL Internet Banking - Update
- 2017-10-23 -- Brazil malspam pushes Banload
- 2017-10-23 -- malspam pushes a RAT's nest of malware
- 2017-10-19 -- Pcap & malware for an ISC diary (Necurs Botnet malspam uses DDE attack)
- 2017-10-18 -- Pcap and malware for an ISC diary (Loki Bot malspam)
- 2017-10-17 -- Terror EK sends Smoke Loader, Smoke Loader sends more malware
- 2017-10-16 -- pcap and malware for an ISC diary (Hancitor malspam)
- 2017-10-13 -- Blank Slate malspam stops pushing Locky, starts pushing Sage 2.2
- 2017-10-11 -- WhatsApp-themed Brazil malspam pushes Banload malware
- 2017-10-11 -- FTFY: Necurs Botnet malspam pushing "asasin" variant Locky ransomware
- 2017-10-11 -- Phishing email - Subject: Completed Title Work - Please DocuSign
2018-08-24 - QUICK POST: EMOTET INFECTIONS WITH ZEUS PANDA BANKER

ASSOCIATED FILES:


- 2018-08-24-Emotet-infection-traffic-with-Zeus-Panda-Banker.pcap.zip 1.3 MB (1,250,753 bytes)
- 2018-08-24-malware-from-Emotet-and-Zeus-Panda-Banker-infection.zip 350 KB (349,531 bytes)

NOTES:

- Zip archives are password-protected with the standard password. If you don't know it, look at the "about" page of this website.
DOMAINS FROM A PCAP

- astraclinic.com
- trustsoft.ro
- tailbackuisback.xyz
- mykeeptake.xyz
- kermain-valley.com
- tonyssmarineservice.co.uk
- canevaszzi.com.br
- fufu.com.mx
- cranmorelodge.co.uk
- veliketomoveit.ca
- fundacionafanian.com
- humoronoff.top
- www.kirk666.top
- nebula-ent.com

IT’S FASTER TO PROGRAMMATICALLY PULL DATA OUT OF A PCAP

- gator3110.hostgator.com
- www.thesocialindian.in
- abovecreative.com
- gmokkasd.website
- alberguetaulill.com
- melissakiss.com
- grupoembatec.com
- amedion.net
- vuoshakar123123.website
- eedolewnia.pl
- simcon.ca
- sano.ir
- organicprom.ru
- akademia.gnatyshyn.pl
- soportek.cl
Malformed emails from Necurs botnet try to deliver Locky using word doc with embedded OLE objects

Another Locky ransomware campaign that is trying to use Embedded OLE Objects is hitting the UK again (and probably other countries at the same time) with an email with a subject of Emailing: JXF53 – 08.11.2017, (random characters and numbers) pretending to come from random senders. Some have a ...
Continue reading →

ANOTHER EXAMPLE OF A SITE WITH INTEL YOU COULD USE

Fake You have a new highly encrypted secure fax from eFax! malspam delivers Trickbot banking Trojan

An email with the subject of You have a new fax pretending to come from eFax Corporate but actually coming from a look-a-like domain <message@efax-secure.com> with a malicious word doc attachment is today's latest spoof of a well-known company, bank or public authority delivering Trickbot banking Trojan You can now ...
Continue reading →
Malware Families

The following is a listing of the malware families currently included in DGArchive.

<table>
<thead>
<tr>
<th>#</th>
<th>Name</th>
<th>#Seeds</th>
<th>#Domains (unique)</th>
<th>MinLen</th>
<th>MaxLen</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>bobax_dga</td>
<td>1</td>
<td>300 (300)</td>
<td>9</td>
<td>19</td>
</tr>
<tr>
<td>2</td>
<td>banjori_dga</td>
<td>32</td>
<td>452,115 (438,949)</td>
<td>7</td>
<td>26</td>
</tr>
<tr>
<td>3</td>
<td>bamital_dga</td>
<td>1</td>
<td>271,128 (271,128)</td>
<td>32</td>
<td>35</td>
</tr>
<tr>
<td>4</td>
<td>blackhole_dga</td>
<td>1</td>
<td>4,380 (732)</td>
<td>16</td>
<td>16</td>
</tr>
<tr>
<td>5</td>
<td>cryptoclocker_dga</td>
<td>1</td>
<td>1,824,000 (1,824,000)</td>
<td>12</td>
<td>18</td>
</tr>
<tr>
<td>6</td>
<td>conficker_dga</td>
<td>2</td>
<td>1,537,000 (1,536,783)</td>
<td>5</td>
<td>11</td>
</tr>
<tr>
<td>7</td>
<td>chinad_dga</td>
<td>1</td>
<td>729,000 (186,624)</td>
<td>16</td>
<td>16</td>
</tr>
<tr>
<td>8</td>
<td>corebot_dga</td>
<td>2</td>
<td>426,660 (151,320)</td>
<td>12</td>
<td>28</td>
</tr>
<tr>
<td>9</td>
<td>darkshell_dga</td>
<td>1</td>
<td>49 (49)</td>
<td>6</td>
<td>6</td>
</tr>
<tr>
<td>10</td>
<td>dyre_dga</td>
<td>1</td>
<td>1,308,000 (1,308,000)</td>
<td>34</td>
<td>34</td>
</tr>
<tr>
<td>11</td>
<td>dircrypt_dga</td>
<td>20</td>
<td>600 (600)</td>
<td>8</td>
<td>20</td>
</tr>
</tbody>
</table>
VirusTotal

Analyze suspicious files and URLs to detect types of malware including viruses, worms, and trojans.

ANOTHER EXAMPLE OF A SITE WITH INTEL YOU COULD USE

Upload and scan file

By using VirusTotal you consent to our Terms of Service and Privacy Policy and allow us to share your submission with the security community. Learn more.
YOU CAN WRITE YARA RULES TO AUTOMATICALLY HUNT FOR THINGS
AND YOU CAN DOWNLOAD AND PROCESS FILES, GETTING USEFUL INFO
In addition to static/historical maliciousness, there are live feeds.
WHY VISUALS?

▸ Turn Messy Data into Meaningful Information
▸ Help Us Quickly Analyze Threat Hunting Data
Assessments of change, dynamics, and cause and effect are at the heart of thinking and explanation. To understand is to know...

What cause provokes what effect, by what means, at what rate.

How then is such knowledge to be represented?

~Edward Tufte
VISUALS THAT WE LIKE TO USE

Data-Driven Documents

WE PROCESS WITH PYTHON AND THEN VISUALIZE USING D3 AND MATPLOTLIB
VISUALS WE LIKE TO USE

▸ Force-Directed Graph
▸ Timelines of First Seen Queries VS Domain Registration
▸ Timelines of Domain Queries
▸ Timelines of Queries From Network Captures
▸ Signature Patterns Built From Queries In Network Capture Files
SOME OF THE BEAUTIFUL THINGS YOU CAN CREATE WITH FORCE-DIRECTED GRAPHS
GAMEOVER ZEUS
QUERY TIMELINES

Query Volume for google.com
LOOKING AT THE TIMES OF POSTS AND GETS IN PCAPS
WHAT MAKES A VISUAL USEFUL?
QUESTIONS WE ASK OURSELVES

When showing quantities, what will make the visual clear?
QUESTIONS WE ASK OURSELVES

Am I placing the data in an appropriate context?

force directed graphs: intuitive for networks
QUESTIONS WE ASK OURSELVES

How can I …

• reduce visual clutter?
• clarify primary information?
• highlight notable content?
QUESTIONS WE ASK OURSELVES

How can I assess change and rates of change?

- Queries on Different Days to Same Domain Reveal Patterns, Assessed Change, and Rates of Change.
- We See This On Domains Which Show a Sudden Spike (the assessed change) and How Many Queries There Were On The Spike (or if it ever happened)

![Query Volume for vodaless.net](image)
VISUAL EXAMPLES OF ATTACK CAMPAIGNS
EMOTET

**Arrival**

1. Malware with URL. Subject is Invoice / Payment notification
   - User clicking the URL in malware leads to download

2. Doc with malicious macro
   - Executes powershell command line to download payload

**Installation**

3. EMOTET

   (4) Drops copy
   a. `%system%\<file name>.exe`
   b. `%appdata%\Local\Microsoft\Windows\<file name>.exe`

   (5) Delete Zone.Identifier ADS

   (6) Creates Service (if with admin rights)

   a. With admin rights
   b. Without admin rights
   Service name / Regrun value is same as `<file name>`

**Routines**

7. List running processes
8. Get System and OS info

9. Send info to CnC

10. Create Auto-start registry
    - HKCU\%regrun%
    (if without admin rights)

Send modules to perform other routines

11. Execute modules received from CnC
    a. Update copy
    b. Spammer module
    c. Credential Stealer module
    d. Network propagation module
OFTEN, YOU JUST HAVE A LIST OF DOMAINS AND IPS

<table>
<thead>
<tr>
<th>Emotet_domains.txt</th>
<th>Emotet_ips.txt</th>
</tr>
</thead>
<tbody>
<tr>
<td>atakentegitimkurumlari.com</td>
<td>12.182.146.226</td>
</tr>
<tr>
<td>gadanie-lidia.ru</td>
<td>186.71.61.91</td>
</tr>
<tr>
<td>vodaless.net</td>
<td>181.142.74.233</td>
</tr>
<tr>
<td>eclatpro.com</td>
<td>71.202.205.235</td>
</tr>
<tr>
<td>weliketomoveit.ca</td>
<td>185.159.131.55</td>
</tr>
<tr>
<td>fundacionafanic.com</td>
<td>37.120.175.15</td>
</tr>
<tr>
<td>eeodlewnia.pl</td>
<td>69.17.170.58</td>
</tr>
<tr>
<td>simcon.ca</td>
<td>24.217.117.217</td>
</tr>
<tr>
<td>ownhive.com</td>
<td>60.192.109.50</td>
</tr>
<tr>
<td>gnatyshyn.pl</td>
<td>143.216.147.70</td>
</tr>
<tr>
<td>soportek.cl</td>
<td>79.78.160.225</td>
</tr>
<tr>
<td>ipinfo.io</td>
<td>73.178.169.180</td>
</tr>
<tr>
<td>goprorent.pl</td>
<td>129.89.95.241</td>
</tr>
<tr>
<td>irontech.com.tr</td>
<td>73.27.38.128</td>
</tr>
<tr>
<td>msftncsi.com</td>
<td>129.89.95.110</td>
</tr>
<tr>
<td>krugsp.com</td>
<td>96.95.159.237</td>
</tr>
<tr>
<td>collectorsway.com</td>
<td>24.40.239.62</td>
</tr>
<tr>
<td>webmounts.co.ke</td>
<td>71.8.1.188</td>
</tr>
<tr>
<td>brokbutcher.com</td>
<td>71.71.3.84</td>
</tr>
<tr>
<td>ocyoungactors.com</td>
<td>199.120.92.245</td>
</tr>
<tr>
<td>misico.com</td>
<td>186.71.61.91</td>
</tr>
<tr>
<td>181.142.74.233</td>
<td>71.202.205.235</td>
</tr>
</tbody>
</table>
FORCE-DIRECTED GRAPH : EMOTET IPS AND DOMAINS

PUT THAT LIST INTO A FORCE GRAPH
FORCE-DIRECTED GRAPH: EMOTET IPS AND DOMAINS

FIND THE THINGS THAT STAND OUT
FORCE-DIRECTED GRAPH: EMOTET IPS AND DOMAINS

FIND THE THINGS THAT STAND OUT
ENRICH THAT WITH ADDITIONAL PASSIVE DNS DATA AND TURN LABELS ON TO GET MORE INFO
THIS DOMAIN, ASSOCIATED WITH EMOTET WILL BE SEEN AGAIN LATER
2018-08-16 - EMOTET INFECTIONS WITH ZEUS PANDA BANKER ON 2018-08-15 & 2018-08-16

ASSOCIATED FILES:

- 2018-08-14-thru-16-Emotet-malspam-9-email-examples.zip  420 KB (420,063 bytes)

NOTES:

- Still seeing Zeus Panda Banker caused by Emotet, very similar to what I posted earlier this week on 2018-08-14.
- This ties into a recent Unit 42 blog I wrote last month, Malware Team Up: Malspam Pushing Emotet + Trickbot.

**EMOTET LINK INFECTION CHAIN**

- GRABBING JUST SOME PCAPS TO LOOK AT

**EMOTET ATTACHMENT INFECTION CHAIN**

Shown above: Flow chart typical Emotet malspam infections.
GET /WellsFargo/Smallbusiness/Aug-15-2018 HTTP/1.1
Accept: text/html, application/xhtml+xml, */*
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko
Accept-Encoding: gzip, deflate
Host: akademia.gnatyshyn.pl
DNT: 1
Connection: Keep-Alive
<table>
<thead>
<tr>
<th>No.</th>
<th>Time</th>
<th>Source</th>
<th>Destination</th>
<th>Protocol</th>
<th>Length</th>
<th>Info</th>
</tr>
</thead>
</table>

duncanfalk.com
psycchedelicsociety.org.au
gnatyshyn.pl
soportek.cl

PULL OUT THE DOMAINS WITH PYTHON
FROM ONE NETWORK CAPTURE

BUILD A TIMELINE, SHOWING THE TIMES EMAILS WERE RECEIVED

AND WHEN DOMAINS WERE FIRST-SEEN IN DNS
Looking at information on the domains in those PCAPs.
LOOKING AT INFORMATION ON THE DOMAINS IN THOSE PCAPS
<table>
<thead>
<tr>
<th>Date</th>
<th>Time</th>
<th>URL</th>
</tr>
</thead>
</table>
The Australian Psychedelic Society is an organisation seeking to connect Australia’s psychedelic community to benefit, enjoy and contribute to their culture in a safe and supportive environment.
VIEWING ALL THE EMOTET DOMAINS FROM A LOT OF PCAPS ON A TIMELINE TO FIND PATTERNS
PATTERNS
LOOKING AT THE TIMES IN BETWEEN POSTS AND GETS IN PCAPS
Looking at the times in between posts and GETs in PCAPs

<table>
<thead>
<tr>
<th>Time</th>
<th>Source</th>
<th>Destination</th>
<th>Protocol</th>
<th>Length</th>
<th>Info</th>
</tr>
</thead>
<tbody>
<tr>
<td>6</td>
<td>10.6.5.102</td>
<td>193.18.246.76</td>
<td>HTTP</td>
<td>353</td>
<td>GET /ups.com/WebTracking/px-5748789735663/ HTTP/1.1</td>
</tr>
<tr>
<td>135</td>
<td>103.18.246.76</td>
<td>10.6.5.102</td>
<td>HTTP</td>
<td>2885</td>
<td>HTTP/1.1 200 OK (application/msword)</td>
</tr>
<tr>
<td>146</td>
<td>103.18.246.76</td>
<td>10.6.5.102</td>
<td>HTTP</td>
<td>2885</td>
<td>HTTP/1.1 200 OK (application/msword)</td>
</tr>
<tr>
<td>304</td>
<td>31.536961</td>
<td>10.6.5.102</td>
<td>HTTP</td>
<td>733</td>
<td>POST / HTTP/1.1</td>
</tr>
<tr>
<td>311</td>
<td>48.066116</td>
<td>10.6.5.102</td>
<td>HTTP</td>
<td>1053</td>
<td>HTTP/1.1 200 OK (text/html)</td>
</tr>
<tr>
<td>378</td>
<td>63.733795</td>
<td>10.6.5.102</td>
<td>HTTP</td>
<td>325</td>
<td>GET /whoami.php HTTP/1.1</td>
</tr>
<tr>
<td>1506</td>
<td>429.760962</td>
<td>138.68.13.161</td>
<td>HTTP</td>
<td>224</td>
<td>HTTP/1.1 200 OK (text/html)</td>
</tr>
<tr>
<td>1514</td>
<td>429.262788</td>
<td>10.6.5.102</td>
<td>HTTP</td>
<td>525</td>
<td>POST / HTTP/1.1</td>
</tr>
<tr>
<td>1516</td>
<td>429.760962</td>
<td>138.68.13.161</td>
<td>HTTP</td>
<td>358</td>
<td>HTTP/1.1 200 OK (text/html)</td>
</tr>
</tbody>
</table>
LOOKING AT THE TIMES IN BETWEEN POSTS AND GETS IN PCAPS

Times In Between Events
Are there patterns?
LOOKING AT THE TIMES IN BETWEEN POSTS AND GETS IN PCAPS
ACCOUNT CHECKING ACTIVITY FROM TRICKBOT BACKCONNECT PROXY

1. TRICKBOT BANKING TROJAN GANG
2. INITIAL INFECTION VICTIM
3. PAYLOAD SERVER
4. MODULE SERVER
5. BACKCONNECT SERVER
6. ACCOUNT CHECKING VIA LOGIN FORMS

GRAPHS
ENRICHING THOSE SMALL CONNECTIONS TO FIND ADDITIONAL RELATIONSHIPS
TURN LABELS ON TO ELABORATE THE RELATIONSHIPS
VIEWING ALL THE TRICKBOT DOMAINS FROM A LOT OF PCAPS ON A TIMELINE TO FIND PATTERNS
LOOKING AT THE TIMES IN BETWEEN POSTS AND GETS IN PCAPS
1. Target victims with malspam campaigns which includes the Hancitor document as attachment

2. Hancitor downloads The main payload (Vawtrack, Pony) from the C2
VIEWING ALL THE HANCITOR DOMAINS FROM A LOT OF PCAPS ON A TIMELINE TO FIND PATTERNS
FORCE DIRECTED GRAPH
TURN LABELS ON TO ELABORATE THE RELATIONSHIPS
WE SEE MYKEEPTAKE.XYZ, FROM EMOTET IN HANCITOR TOO
PATTERNS
LOOKING AT THE TIMES IN BETWEEN POSTS AND GETS IN PCAPS
RELATIONSHIPS BETWEEN ATTACK INFRASTRUCTURE
VIEWING TRICKBOT, EMOTET, AND HANCITOR ALL TOGETHER TO FIND SHARED INFRASTRUCTURE
COMPARING THE TIMES OF DOMAINS BEING USED

- chamber
- foothills.com
- thousand-india
- walkazamovet.com
- edate.com
- kiconsulting.net
- brkluther.com
- gspely.png.pl
- kozion cave.com
- amedion.net
- kerman-valley.com
- simon.ca
- tonyshaikhouseservice.co.uk
- eliobszobracsek.com
- sanor.is
- duncantalk.com
- portfoliochip.com
- vpd.imagas.net
- anyany.net
- nebrakent.com
- toxendis.net
- targa.com
- misco.com
- pubvoices.nl.t.
- idemtrust.com
- invokre.com
- ytfamily.com
- nikonphotosgroup.net
- xportal.pl
- altorganzatw.com
- turricolodiv.net
- tracaelit.tv
- positivebusinessimages.com
- abovecreative.com
- healthdataknowledge.com
- iras.com
- amoxextr.k
- aclovelmaa.pl
- igpco.com
- planeiq.com.net
- inovone.com.br
- lexneply.com.br
- cmnm marketed.net
- ipinfo.io
- lfy.org
- santalahis.com
- goorent.pl
- shopthepcmonograpos.com
- sandearth.com
- gadanie-lida.ru
- stewartandgreenltd.com
- ipsoft.es
- lnnf.org
- lpy.org
- miasakisa.com
- owmhk.com
- asmaritico.com
- hiakentteam.com
- organoptom.ru
- primersiana.org
- sawamoto bangdju.web.id
- objyounggations.com
- kikera66.top
- webmournis.cor
- collectorsway.com
- gpremipokwaalysportal.club
- psyaneslessonerry.org.us
- pynｵﾑｋ.com
- thyent24.com
COMPARING THE TIMES OF DOMAINS BEING USED

Hancitor
### Comparing the times of domains being used

<table>
<thead>
<tr>
<th>Emotet</th>
<th>Hancitor</th>
<th>Trickbot</th>
</tr>
</thead>
<tbody>
<tr>
<td>Oct 2016</td>
<td>Jan 2017</td>
<td>Apr 2018</td>
</tr>
<tr>
<td>Nov 2016</td>
<td>Feb 2017</td>
<td>May 2018</td>
</tr>
<tr>
<td>Dec 2016</td>
<td>Mar 2017</td>
<td>Jun 2018</td>
</tr>
</tbody>
</table>
COMPARING THE QUERIES OF DOMAINS BEING USED

Multiple Domains

Aug 2, 2018
- kirk666.top - 3
- eoodlewnia.pl - 6
- goprorent.pl - 0
- humoronoff.top - 478

Aug 05 2018, Aug 12, Aug 19, Aug 26
QUESTIONS?

CODE: https://pyosec.com

@AScarf0   @joshpyorre