Malware-Traffic-Analysis.net - 2017-04-03 - Ursnif and Pushdo infection

NOTICE:

- The zip archives on this page have been updated, and they now use the new password scheme. For the new password, see the "about" page of this website.

ASSOCIATED FILES:

- 2017-04-03-Ursnif-and-Pushdo-infection.pcap.zip 9.2 MB (9,156,400 bytes)

> - 2017-04-03-Ursnif-and-Pushdo-infection.pcap (10,643,014 bytes)

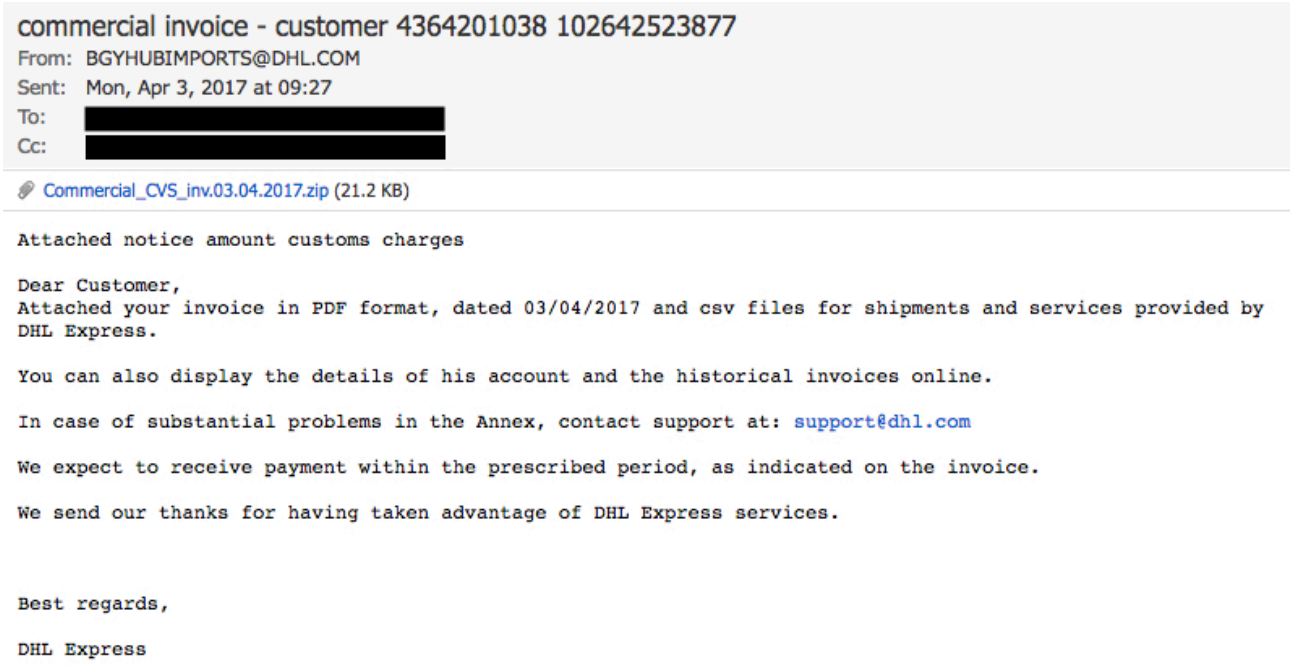
- 2017-04-03-Ursnif-and-Pushdo-emails-and-malware.zip 685.7 kB (685,705 bytes)

> - 2017-04-03-DHL-themed-malspam-0928-UTC.eml (22,764 bytes)
> - 2017-04-03-DHL-themed-malspam-1117-UTC.eml (22,746 bytes)
> - 2017-04-03-DHL-themed-malspam-1220-UTC.eml (22,812 bytes)
> - 2017-04-03-image-themed-malspam-1357-UTC.eml (22,126 bytes)
> - 2017-04-03-image-themed-malspam-1546-UTC.eml (22,646 bytes)
> - 2017-04-03-image-themed-malspam-1646-UTC.eml (22,391 bytes)
> - 33521.exe (353,965 bytes)
> - 462137.exe (295,936 bytes)
> - Balt.dll (49,152 bytes)
> - Commercial_CVS_inv.03.04.2017.cvs.js (25,273 bytes)
> - Commercial_CVS_inv.03.04.2017.zip (15,870 bytes)
> - img-20170403-0014,jpeg.zip (15,446 bytes)
> - img-20170403-0054.jpeg.js (24,464 bytes)

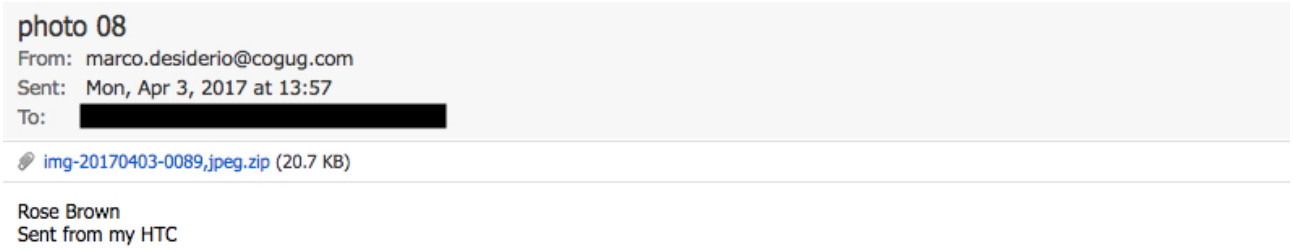
NOTES:

- Saw two waves of malspam with zip attachments containing .js files that generated the same infection traffic.
- Post-infection traffic generated alerts for Ursnif and Pushdo.

EMAIL



Shown above: Screen shot of an email from the first wave.



Shown above: Screen shot of an email from the second wave.

EMAIL HEADERS - FIRST WAVE:

- Date: Monday 2017-04-03 at 09:27 UTC
- From: <BGYHUBIMPORTS@DHL[.]COM>
- Subject: commercial invoice - customer 4364201038 102642523877
- Attachment name: Commercial_CVS_inv.03.04.2017.zip
- Extracted file name: Commercial_CVS_inv.03.04.2017.cvs.js

- Date: Monday 2017-04-03 at 11:17 UTC
- From: <BGYHUBIMPORTS@DHL[.]COM>
- Subject: NOTICE CUSTOMS CHARGES 0094793224 767285436700
- Attachment name: Commercial_CVS_inv.03.04.2017.zip
- Extracted file name: Commercial_CVS_inv.03.04.2017.cvs.js

- Date: Monday 2017-04-03 at 12:20 UTC
- From: <ebillingcmfs.ddi@DHL[.]COM>
- Subject: Dhl Commercial Invoices 6807164709 856884589470
- Attachment name: Commercial_CVS_inv.03.04.2017.zip

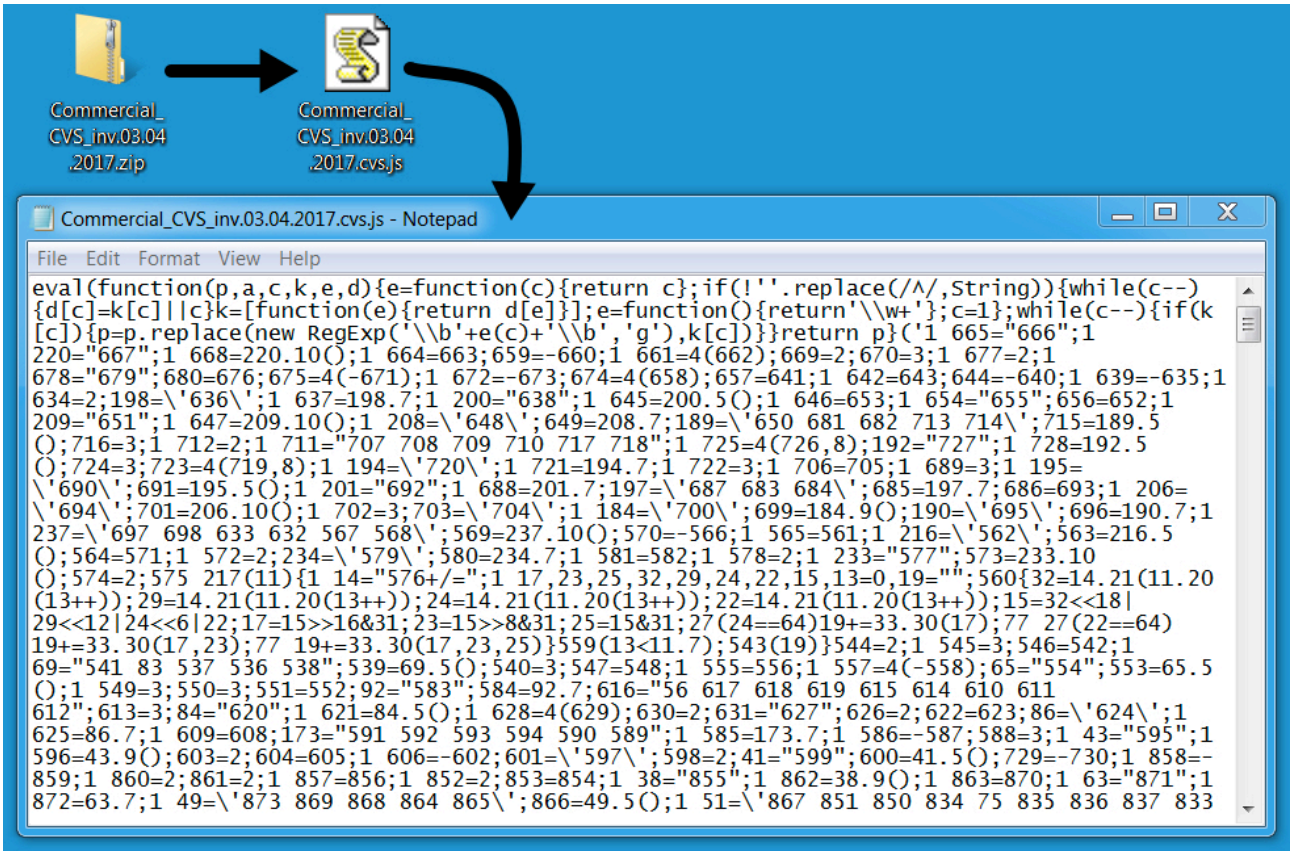
- Extracted file name: Commercial_CVS_inv.03.04.2017.cvs.js

EMAIL HEADERS - SECOND WAVE:

- Date: Monday 2017-04-03 at 13:57 UTC
- From: marco.desiderio@cogug[.]com
- Subject: photo 08
- Attachment name: img-20170403-0089,jpeg.zip
- Extracted file name: img-20170403-0054.jpeg.js

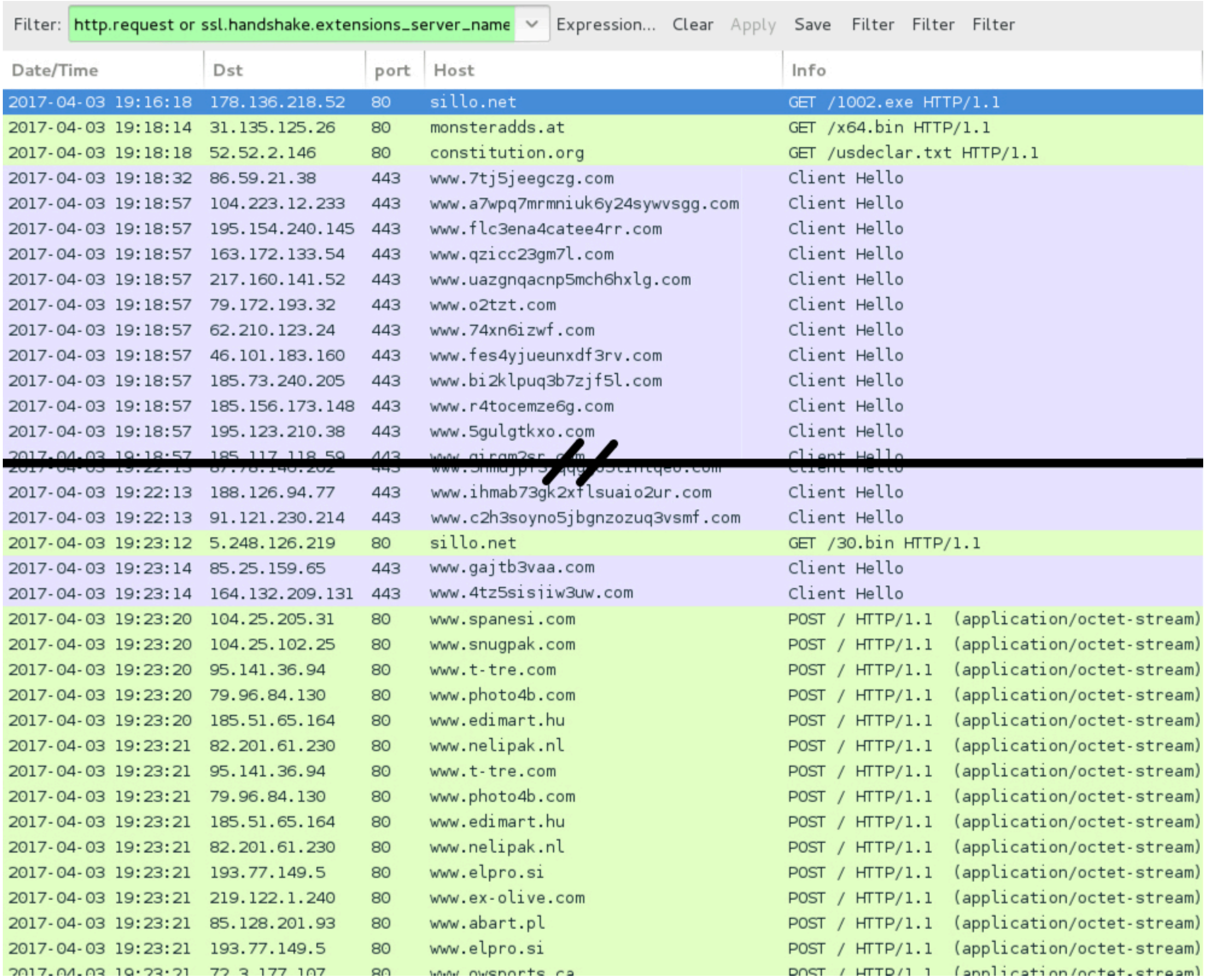
- Date: Monday 2017-04-03 at 15:46 UTC
- From: direzione@nyloq[.]com
- Subject: img_2550
- Attachment name: img-20170403-0014,jpeg.zip
- Extracted file name: img-20170403-0054.jpeg.js

- Date: Monday 2017-04-03 at 16:46 UTC
- From: marzia.berghella@yahoo[.]com[.]hk
- Subject: photo 2DNXAY
- Attachment name: img-20170403-0015,jpeg.zip
- Extracted file name: img-20170403-0054.jpeg.js



Shown above: Attachment taken from the malspam.

TRAFFIC



Filter: http.request or ssl.handshake.extensions_server_name
Expression... Clear Apply Save Filter Filter Filter
Date/Time Dst port Host Info
2017-04-03 19:16:18 178.136.218.52 80 sillo.net GET /1002.exe HTTP/1.1
2017-04-03 19:18:14 31.135.125.26 80 monsteradds.at GET /x64.bin HTTP/1.1
2017-04-03 19:18:18 52.52.2.146 80 constitution.org GET /usdeclar.txt HTTP/1.1
2017-04-03 19:18:32 86.59.21.38 443 www.7tj5jeegczg.com Client Hello
2017-04-03 19:18:57 104.223.12.233 443 www.a7wpq7mrmniuk6y24sywvsgg.com Client Hello
2017-04-03 19:18:57 195.154.240.145 443 www.flc3ena4catee4rr.com Client Hello
2017-04-03 19:18:57 163.172.133.54 443 www.qzicc23gm7l.com Client Hello
2017-04-03 19:18:57 217.160.141.52 443 www.uazgnqacnp5mch6hxlg.com Client Hello
2017-04-03 19:18:57 79.172.193.32 443 www.o2tzt.com Client Hello
2017-04-03 19:18:57 62.210.123.24 443 www.74xn6izwf.com Client Hello
2017-04-03 19:18:57 46.101.183.160 443 www.fes4yjueunxdf3rv.com Client Hello
2017-04-03 19:18:57 185.73.240.205 443 www.bi2klpuq3b7zjf5l.com Client Hello
2017-04-03 19:18:57 185.156.173.148 443 www.r4tocemze6g.com Client Hello
2017-04-03 19:18:57 195.123.210.38 443 www.5gulgtkxo.com Client Hello
2017-04-03 19:22:13 188.126.94.77 443 www.ihmab73gk2xflsuaio2ur.com Client Hello
2017-04-03 19:22:13 91.121.230.214 443 www.c2h3soyno5jbgnzozuq3vsmf.com Client Hello
2017-04-03 19:23:12 5.248.126.219 80 sillo.net GET /30.bin HTTP/1.1
2017-04-03 19:23:14 85.25.159.65 443 www.gajtb3vaa.com Client Hello
2017-04-03 19:23:14 164.132.209.131 443 www.4tz5sisiiw3uw.com Client Hello
2017-04-03 19:23:20 104.25.205.31 80 www.spanesi.com POST / HTTP/1.1 (application/octet-stream)
2017-04-03 19:23:20 104.25.102.25 80 www.snugpak.com POST / HTTP/1.1 (application/octet-stream)
2017-04-03 19:23:20 95.141.36.94 80 www.t-tre.com POST / HTTP/1.1 (application/octet-stream)
2017-04-03 19:23:20 79.96.84.130 80 www.photo4b.com POST / HTTP/1.1 (application/octet-stream)
2017-04-03 19:23:20 185.51.65.164 80 www.edimart.hu POST / HTTP/1.1 (application/octet-stream)
2017-04-03 19:23:21 82.201.61.230 80 www.nelipak.nl POST / HTTP/1.1 (application/octet-stream)
2017-04-03 19:23:21 95.141.36.94 80 www.t-tre.com POST / HTTP/1.1 (application/octet-stream)
2017-04-03 19:23:21 79.96.84.130 80 www.photo4b.com POST / HTTP/1.1 (application/octet-stream)
2017-04-03 19:23:21 185.51.65.164 80 www.edimart.hu POST / HTTP/1.1 (application/octet-stream)
2017-04-03 19:23:21 82.201.61.230 80 www.nelipak.nl POST / HTTP/1.1 (application/octet-stream)
2017-04-03 19:23:21 193.77.149.5 80 www.elpro.si POST / HTTP/1.1 (application/octet-stream)
2017-04-03 19:23:21 219.122.1.240 80 www.ex-olive.com POST / HTTP/1.1 (application/octet-stream)
2017-04-03 19:23:21 85.128.201.93 80 www.abart.pl POST / HTTP/1.1 (application/octet-stream)
2017-04-03 19:23:21 193.77.149.5 80 www.elpro.si POST / HTTP/1.1 (application/octet-stream)

Shown above: Traffic from the infection filtered in Wireshark.

ASSOCIATED DOMAINS:

- 178.136.218[.]52 port 80 - **sillo[.]net** - GET /1002.exe
- 31.135.125[.]26 port 80 - **monsteradds[.]at** - GET /x64.bin -- *[Ursnif module download]*
- 52.52.2[.]146 port 80 - **constitution[.]org** - GET /usdeclar.txt -- *[Gozi/Ursnif/Papras connectivity check]*
- 5.248.126[.]219 port 80 - **sillo[.]net** - GET /30.bin -- *[Zbot Generic URI/header struct .bin]*
- Various IP addresses on port TCP 80 - various domains - POST / -- *[Pushdo.s checkin]*
- Various IP addresses on various TCP ports - various domains - Tor traffic
- Various IP addresses on various ports - attempted TCP connections and non-Tor traffic

FILE HASHES

EMAIL ATTACHMENTS:

- SHA256 hash: 1b402c3ccfe5380425023022614abc4af53369536bda9c70b3074e50484bb340
  File name: Commercial_CVS_inv.03.04.2017.zip

- SHA256 hash: ef3bbbace6eeaf06c2101612d45d694f734b6759ec89b83db0e3d07ea5c49f57
  File name: img-20170403-0014,jpeg.zip
  File name: img-20170403-0015,jpeg.zip
  File name: img-20170403-0089,jpeg.zip

EXTRACTED JS FILES:

- SHA256 hash: faad4f8730db9825cfc5fd29f105a16849c83e61e836d68b2e3eff55fe0f1ec5
  File name: Commercial_CVS_inv.03.04.2017.cvs.js

- SHA256 hash: a62712ff422477b15e512d3d83285d61c760c468e8f8bae26a7e5f0174e57db9
  File name: img-20170403-0054.jpeg.js

FILES RETRIEVED FROM THE INFECTED HOST:

- SHA256 hash: 94380803ac48bec2ca431f968240f4444fdc3a30bd04dbc62bf099bf0ece01f8
  File location: C:\Users\[username]\AppData\Local\Temp\33521.exe
  File location: C:\Users\[username]\AppData\Roaming\Microsoft\Cmcfspex\admpptsp.exe

- SHA256 hash: d26161bc381625ade7fb51db987f2e69c244acc642911948b1507860e90fd3f9
  File location: C:\Users\[username]\AppData\Local\Temp\462137.exe
  File location: C:\Users\[username]\bsebegfabe.exe

- SHA256 hash: 7b1bcab8e3aa932c6ebac8df67d0797b0c8aaa3a78704080853415006877 20a6
  File location: C:\Users\[username]\AppData\Local\Temp\Balt.dll

IMAGES

RealTime Events | Escalated Events

ST	CNT			Date/Time	Src IP	SPort	Dst IP	DPort	Pr	Event Message
RT	1			2017-04-03...	10.4.3.102	49158	178.136.218.52	80	6	ET POLICY exe download without User Agent
RT	1			2017-04-03...	10.4.3.102	49158	178.136.218.52	80	6	ET POLICY exe download via HTTP - Informational
RT	2			2017-04-03...	178.136.218.52	80	10.4.3.102	49158	6	ET POLICY PE EXE or DLL Windows file download
RT	2			2017-04-03...	178.136.218.52	80	10.4.3.102	49158	6	ET POLICY Binary Download Smaller than 1 MB Likely Hostile
RT	1			2017-04-03...	10.4.3.102	49159	31.135.125.26	80	6	ETPRO TROJAN Ursnif Module Download
RT	2			2017-04-03...	10.4.3.102	54723	208.67.222.222	53	17	ET POLICY OpenDNS IP Lookup
RT	1			2017-04-03...	10.4.3.102	49160	52.52.2.146	80	6	ET TROJAN Gozi/Ursnif/Papras Connectivity Check
RT	1			2017-04-03...	10.4.3.102	49328	5.248.126.219	80	6	ET CURRENT_EVENTS Zbot Generic URI/Header Struct .bin
RT	113			2017-04-03...	10.4.3.102	49336	104.25.205.31	80	6	ET TROJAN Backdoor.Win32.Pushdo.s Checkin
RT	1			2017-04-03...	10.4.3.102	49336	104.25.205.31	80	6	ET POLICY Internet Explorer 6 in use - Significant Security Risk
RT	1			2017-04-03...	10.4.3.102	49358	95.211.174.92	80	6	ET CNC Ransomware Tracker Reported CnC Server group 198
RT	1			2017-04-03...	10.4.3.102	49392	193.166.255.171	80	6	ET TROJAN Connection to Fitsec Sinkhole IP (Possible Infected Host)

Shown above: Some alerts on the traffic from the Emerging Threats Pro (ETPRO) rulesets using Sguil on Security Onion.

Click here to return to the main page.

Source: http://malware-traffic-analysis.net/2017/04/03/index2.html