

2017-06-12 - LOKI BOT MALSPAM - SUBJECT: RE: PURCHASE ORDER 457211

malware-traffic-analysis.net/2017/06/12/index.html

ASSOCIATED FILES:

ZIP archive of the pcap: [2017-06-12-Loki-Bot-malspam-traffic.pcap.zip](#) 2.5 kB (2,543 bytes)

| [2017-06-12-Loki-Bot-malspam-traffic.pcap](#) (9,334 bytes)

ZIP archive of the malware: [2017-06-12-Loki-Bot-malspam-and-artifacts.zip](#) 486 kB (485,562 bytes)

- [2017-06-12-Loki-bot-malspam-0137-UTC.eml](#) (213,873 bytes)
- [PO12062017.ace](#) (157,430 bytes)
- [PO12062017.exe](#) (327,680 bytes)

NOTES:

- Somewhat similar to the Loki Bot malspam I documented last week on [2017-06-07](#)
- Today the email had a ZIP archive attachment containing was a Word document with an embedded .js file that downloaded Loki Bot.
- This time it was an ACE archive attachment that contained the Loki Bot binary.

EMAILS

Re: PURCHASE ORDER 457211 - Mozilla Thunderbird

Reply Reply All Forward More

From Amina Diab <dxboman@emirates.net.ae> ☆

Subject Re: PURCHASE ORDER 457211 Date Mon, 12 Jun 2017 01:37 UTC

To [REDACTED] ☆

Sales:

Please quote 2000 pcs asap.
Awaiting for your feedback.

Amina Diab

Dubai & Oman General Trading Co LLC
Suite # 302 B, P 114 Building
P.O. Box - 28280
Deira, Dubai - UAE

Tel: + 9714 -2278910
Fax: + 9714-2278911
Email: dxboman@emirates.net.ae
Website: <http://www.dubaioman.com/>

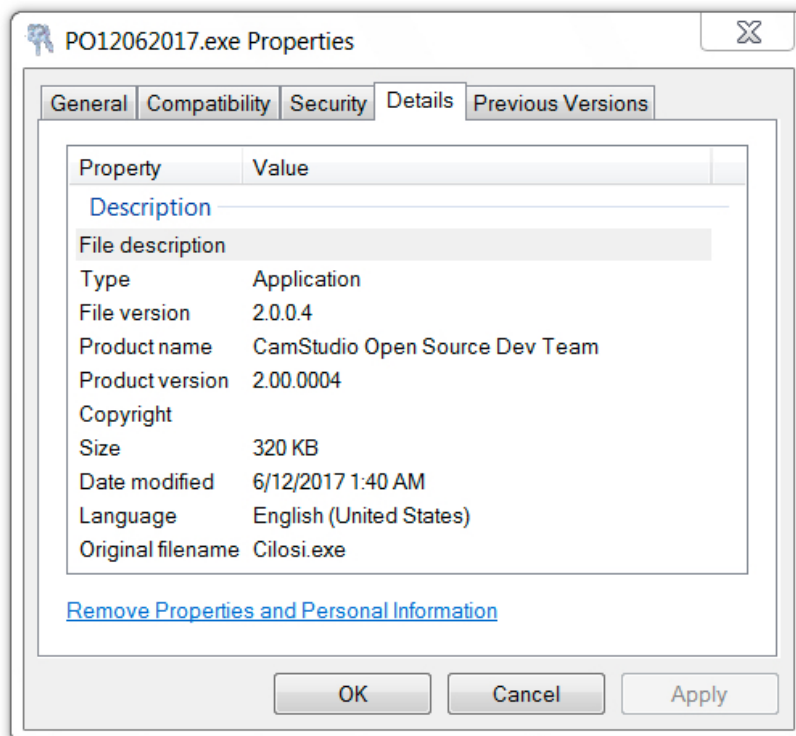
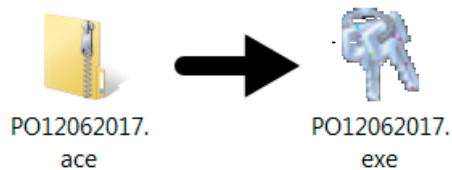
1 attachment: PO12062017.ace 154 KB Save

PO12062017.ace 154 KB

Shown above: Screen shot from the email.

EMAIL HEADERS:

- Date: Monday 2017-06-12 at 01:37 UTC
- From: "Amina Diab" <dxboman@emirates.net.ae>
- Subject: Re: PURCHASE ORDER 457211
- Attachment: PO12062017.ace



Shown above: Malicious executable in ACE archive from the malspam.

TRAFFIC

Filter: **http.request** Expression... Clear Apply Save Filter Filter Filt

Date/Time	Dst	port	Host	Info
2017-06-12 02:36:04	192.99.2.94	80	192.99.2.94	POST /~sadrenam/mmt/Panel/five/fre.php HTTP/1.0
2017-06-12 02:36:04	192.99.2.94	80	192.99.2.94	POST /~sadrenam/mmt/Panel/five/fre.php HTTP/1.0
2017-06-12 02:36:04	192.99.2.94	80	192.99.2.94	POST /~sadrenam/mmt/Panel/five/fre.php HTTP/1.0
2017-06-12 02:37:05	192.99.2.94	80	192.99.2.94	POST /~sadrenam/mmt/Panel/five/fre.php HTTP/1.0
2017-06-12 02:38:05	192.99.2.94	80	192.99.2.94	POST /~sadrenam/mmt/Panel/five/fre.php HTTP/1.0
2017-06-12 02:39:06	192.99.2.94	80	192.99.2.94	POST /~sadrenam/mmt/Panel/five/fre.php HTTP/1.0

Shown above: Traffic from the infection filtered in Wireshark.

ASSOCIATED DOMAINS:

192.99.2.94 port 80 - **192.99.2.94** - POST /~sadrenam/mmt/Panel/five/fre.php

FILE HASHES

ACE ARCHIVE FROM THE EMAIL:

SHA256 hash:

42306a26580cf29068f1a716aaa61d1a4921b2206f3e8234d86d6fcc607d7be8

File size: 157,430 bytes

File name: PO12062017.ace

MALICIOUS BINARY EXTRACTED FROM THE ACE ARCHIVE (LOKI BOT):

SHA256 hash:

7e9c05cff0e0ac10640100c801c3f56470fb6166bbf4e67fa28c63af683458e4

File size: 327,680 bytes

File name: PO12062017.exe

File location on the infected host: C:\Users\
[username]\AppData\Roaming\subfolder\filename.exe

SUSPICIOUS FILE NOTED ON THE INFECTED HOST:

SHA256 hash:

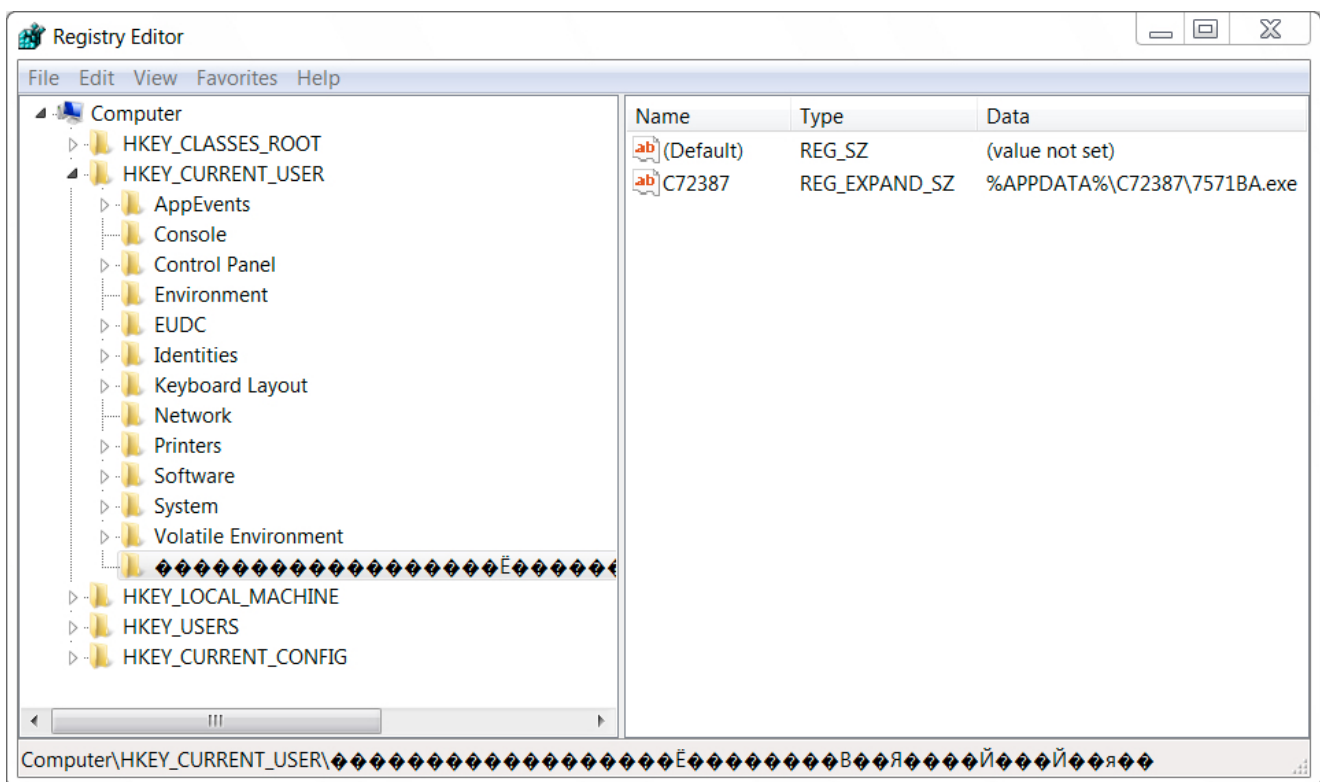
121118a0f5e0e8c933efd28c9901e54e42792619a8a3a6d11e1f0025a7324bc2

File location: C:\Users\[username]\AppData\Roaming\C72387\7571BA.exe

File size: 20,992 bytes

File description: Appears to be a legitimate Microsoft file named svchost.exe

IMAGES



Shown above: Updated Windows registry with the same file as last time.

FINAL NOTES

Once again, here are the associated files:

- ZIP archive of the pcap: [2017-06-12-Loki-Bot-malspam-traffic.pcap.zip](#) 2.5 kB (2,543 bytes)
- ZIP archive of the malware: [2017-06-12-Loki-Bot-malspam-and-artifacts.zip](#) 486 kB (485,562 bytes)

ZIP files are password-protected with the standard password. If you don't know it, look at the "about" page of this website.

[Click here](#) to return to the main page.