2017-07-04 - MALSPAM WITH JAVA-BASED RAT

malware-traffic-analysis.net/2017/07/04/index.html

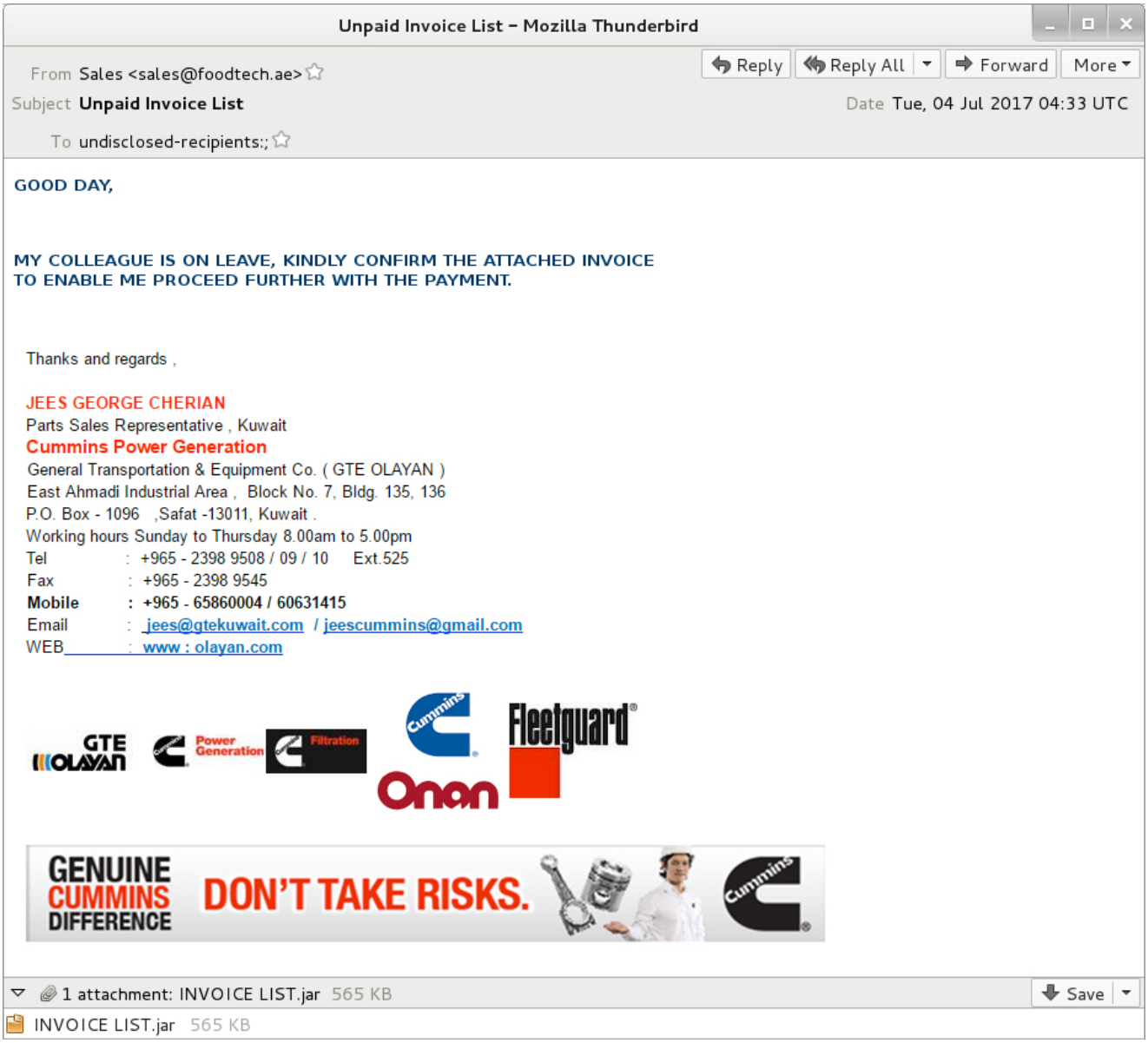
ASSOCIATED FILES:

Zip archive of the email and artifacts: 2017-07-04-Java-RAT-malspam-and-artifacts.zip
1.5 MB (1,506,426 bytes)

- 2017-07-04-malspam-0433-UTC.eml (946,555 bytes)
- INVOICE LIST.jar (578,829 bytes)
- _0.3253909458280891429470818100609952 33.class (247,088 bytes)

EMAIL

SCREENSHOT:



Shown above: Screenshot of the email.

EMAIL HEADER INFO:

- Return-Path: <sales@foodtech.ae>
- X-Originating-Ip: [162.144.89.147]
- Authentication-Results: [removed]; iprev=pass policy.iprev="162.144.89.147"; spf=softfail smtp.mailfrom="sales@foodtech.ae" smtp.helo="server.joshmachines.com"; dkim=none (message not signed) header.d=none; dmarc=none (p=nil; dis=none) header.from=foodtech.ae
- Received: from [162.144.89.147] ([162.144.89.147:36560] helo=server.joshmachines.com)
  by [removed] (envelope-from <sales@foodtech.ae>)
  [removed]; Tue, 04 Jul 2017 01:42:30 -0400

- Received: from [127.0.0.1] (port=45926 helo=harshangzaveri.com)
  by server.joshmachines.com with esmtpa (Exim 4.89)
  (envelope-from <sales@foodtech.ae>)
  id 1dSFWO-0008CV-Tu; Tue, 04 Jul 2017 04:33:09 +0000
- MIME-Version: 1.0
- Date: Tue, 04 Jul 2017 04:33:08 +0000
- From: Sales <sales@foodtech.ae>
- To: undisclosed-recipients:;
- Subject: Unpaid Invoice List
- Reply-To: sales@foodtech.ae
- Mail-Reply-To: sales@foodtech.ae
- Message-ID: <a01dfe55b97e7efd3c75d28a9286ec40@foodtech.ae>
- X-Sender: sales@foodtech.ae
- User-Agent: Roundcube Webmail/1.2.4

Attachment: INVOICE LIST.jar

TRAFFIC

Date/Time	Src	port	Dst	port	Info
2017-07-04 14:53:54	10.7.4.101	49215	191.101.22.49	3020	49215→cifs [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=
2017-07-04 14:53:55	191.101.22.49	3020	10.7.4.101	49215	cifs→49215 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0
2017-07-04 14:53:55	10.7.4.101	49215	191.101.22.49	3020	[TCP Spurious Retransmission] 49215→cifs [SYN] Seq=0 Win=8192 Le
2017-07-04 14:53:55	191.101.22.49	3020	10.7.4.101	49215	cifs→49215 [RST, ACK] Seq=3572715275 Ack=1 Win=64240 Len=0
2017-07-04 14:53:56	10.7.4.101	49215	191.101.22.49	3020	[TCP Spurious Retransmission] 49215→cifs [SYN] Seq=0 Win=8192 Le
2017-07-04 14:53:56	191.101.22.49	3020	10.7.4.101	49215	cifs→49215 [RST, ACK] Seq=3374772087 Ack=1 Win=64240 Len=0
2017-07-04 14:53:58	10.7.4.101	49219	191.101.22.49	3020	49219→cifs [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=
2017-07-04 14:53:59	191.101.22.49	3020	10.7.4.101	49219	cifs→49219 [RST, ACK] Seq=1 Ack=1 Win=64240 Len=0
2017-07-04 14:53:59	10.7.4.101	49219	191.101.22.49	3020	[TCP Spurious Retransmission] 49219→cifs [SYN] Seq=0 Win=8192 Le
2017-07-04 14:53:59	191.101.22.49	3020	10.7.4.101	49219	cifs→49219 [RST, ACK] Seq=3683092035 Ack=1 Win=64240 Len=0
2017-07-04 14:54:00	10.7.4.101	49219	191.101.22.49	3020	[TCP Spurious Retransmission] 49219→cifs [SYN] Seq=0 Win=8192 Le
2017-07-04 14:54:00	191.101.22.49	3020	10.7.4.101	49219	cifs→49219 [RST, ACK] Seq=927571168 Ack=1 Win=64240 Len=0

Shown above: Traffic from an infection filtered in Wireshark.

POST-INFECTION TRAFFIC:

191.101.22.49 port 3020 - attempted TCP connections, but RST from the server.

FILE HASHES

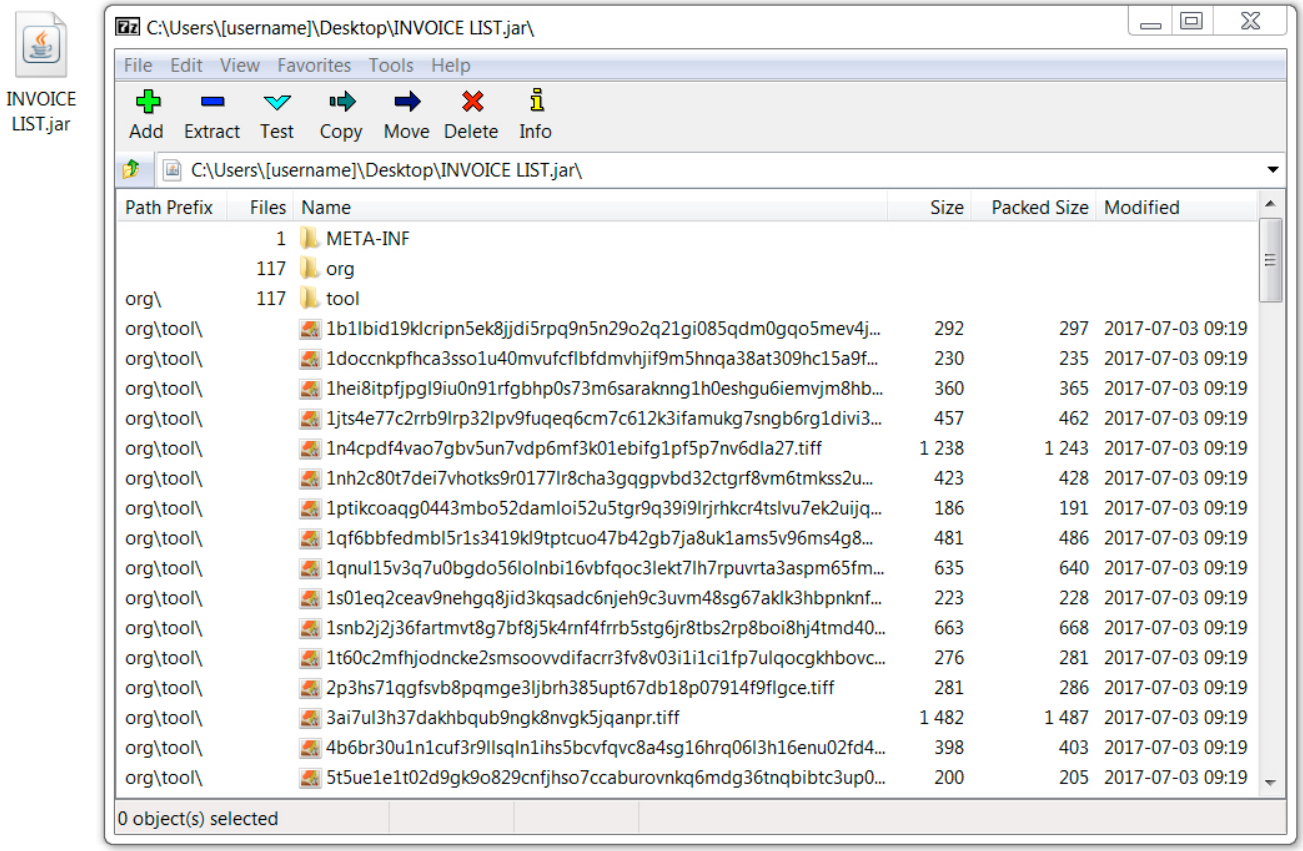
EMAIL ATTACHMENT:

SHA256 hash:
9863c850c213dee716dc5954bb0f28a1c480cf0435e93110824cb083fd4bdda5
File name: INVOICE LIST.jar
File size: 578,829 bytes

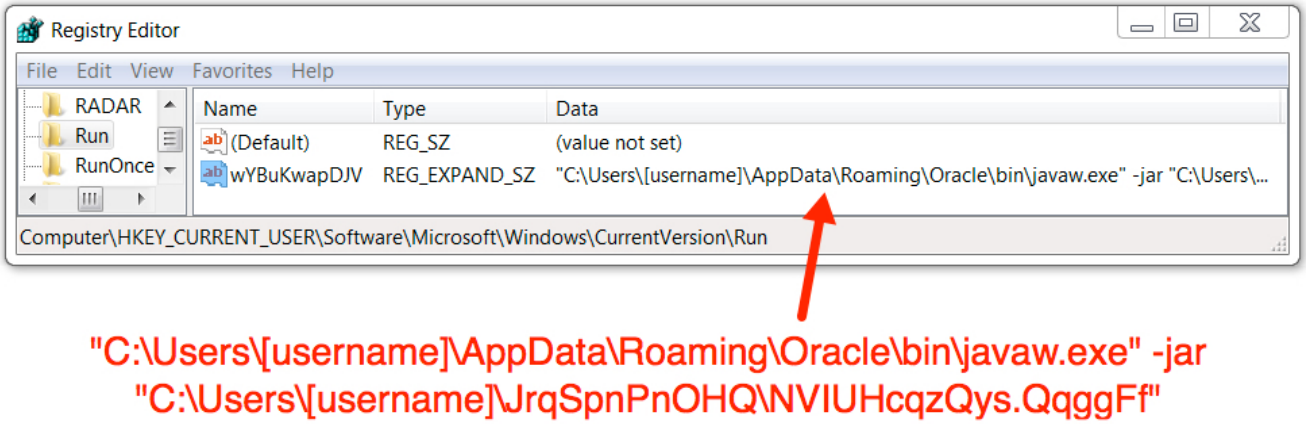
ARTIFACT FOUND IN USER'S APPDATA\LOCAL\TEMP DIRECTORY:

SHA256 hash:
97d585b6aff62fb4e43e7e6a5f816dcd7a14be11a88b109a9ba9e8cd4c456eb9
File name: _0.3253909458280891429470818100609952 33.class
File size: 247,088 bytes

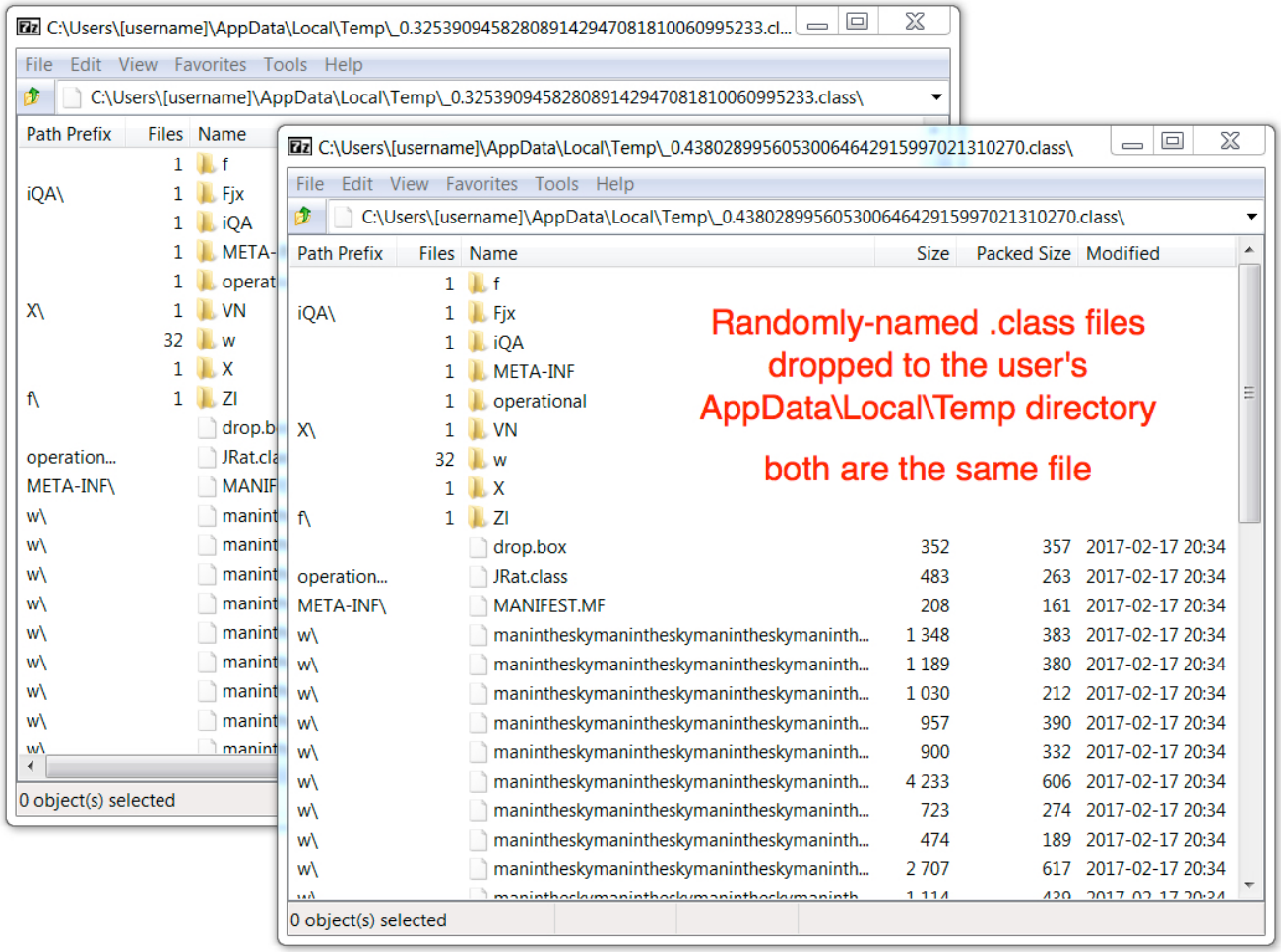
IMAGES



Shown above: Contents of the email attachment.



Shown above: Windows registry change to make the malware persistent after a reboot.



*Shown above: Two .class files with the same file hash found in the user's **AppData\Local\Temp** directory after this infection.*

FINAL NOTES

Once again, here are the associated files:

Zip archive of the email and artifacts: 2017-07-04-Java-RAT-malspam-and-artifacts.zip
1.5 MB (1,506,426 bytes)

Zip archives 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.