Malware-Traffic-Analysis.net - 2017-11-23 - Necurs Botnet malspam pushes "Scarab" ransomware

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.

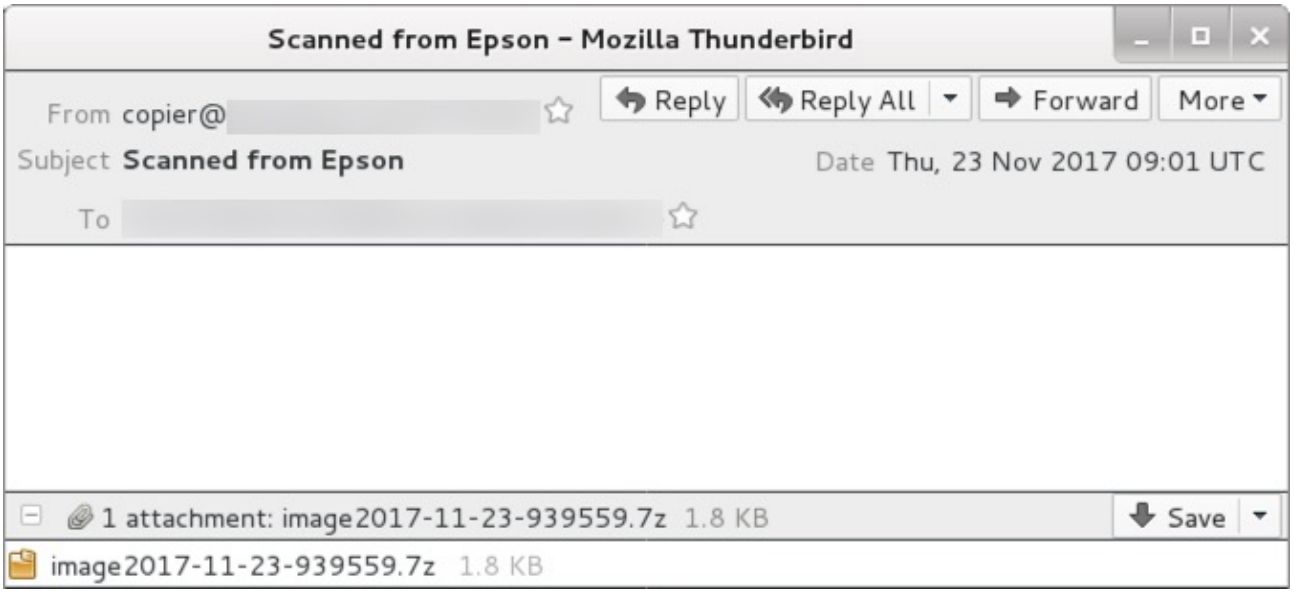
ASSOCIATED FILES:

- 2017-11-23-Necurs-Botnet-malspam-pushes-Scarab-ransomware.pcap.zip 164.2 kB (164,157 bytes)
- 2017-11-23-Necurs-Botnet-malspam-tracker.csv.zip 1.0 kB (996 bytes)
- 2017-11-23-files-from-Necurs-Botnet-malspam-and-Scarab-ransomware-infection.zip 282.6 kB (282,638 bytes)

NOTES:

- Necurs Botnet malspam pushing ransomware nicknamed "Scarab" because encrypted files all end with the file extension ***.scarab***
- More info at: https://www.bleepingcomputer.com/news/security/scarab-ransomware-pushed-via-massive-spam-campaign/

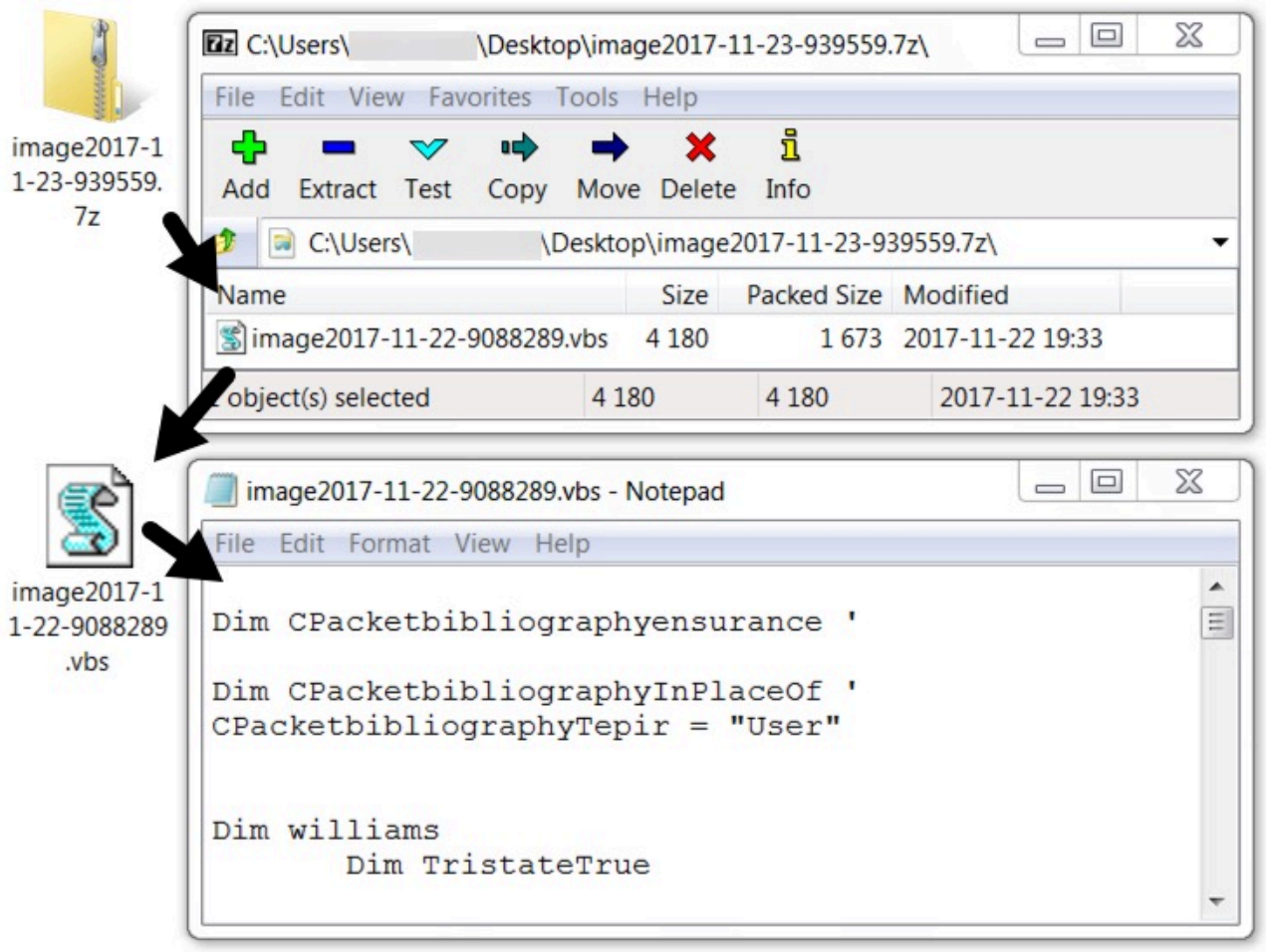
EMAILS



Shown above: Screenshot from one of the emails.

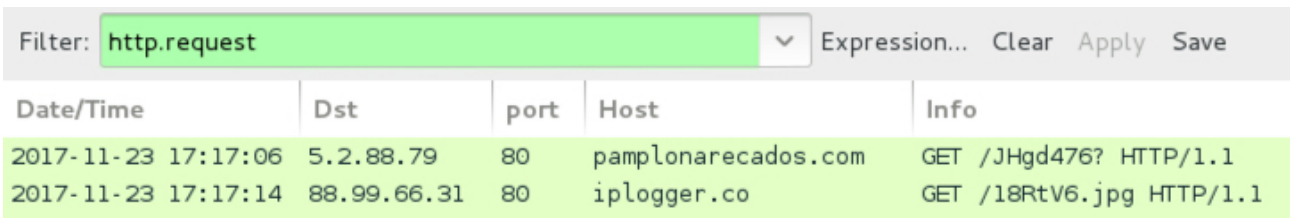
EMAIL HEADERS:

- Date/Time: Thursday 2017-11-23 as early as 08:05 UTC through at least 09:01 UTC
- Subject: Scanned from Canon
- Subject: Scanned from Epson
- Subject: Scanned from HP
- Subject: Scanned from Lexmark
- From (spoofed): copier@*[recipient's email domain]*
- Attachment name: image2017-11-23-*[random digits]*.7z



Shown above: Attachment and extracted VBS file from one of the emails.

TRAFFIC



Shown above: Traffic from the infection filtered in Wireshark.

URLS FROM THE EXTRACTED VBS FILES:

- 98.124.251[.]75 port 80 - **atlantarecyclingcenters[.]com** - GET /JHgd476?

- 66.36.173[.]111 port 80 - **hard-grooves[.]com** - GET /JHgd476?
- 66.36.165[.]149 port 80 - **hellonwheelsthemovie[.]com** - GET /JHgd476?
- 98.124.251[.]75 port 80 - **miamirecyclecenters[.]com** - GET /JHgd476?
- 5.2.77[.]79 port 80 - **pamplonarecados[.]com** - GET /JHgd476?
- 185.57.172[.]213 port 80 - **xploramail[.]com** - GET /JHgd476?

IP ADDRESS CHECK BY INFECTED HOST (NOT INHERENTLY MALICIOUS):

- 88.99.66[.]31 port 80 - **iplogger[.]co** - GET /18RtV6.jpg

EMAIL ADDRESS FROM THE DECRYPTION INSTRUCTIONS:

- **suupport@protonmail[.]com**

FILE HASHES

FILE HASHES FOR THE ATTACHMENTS:

- cae7d4fda96f11ce04cde669cfdfa818c9662b321368a98d7f7ce3e437e91589 - image2017-11-23-0292531.7z
- 1b15b60a7091223b766f7cc4868818b8e835a2301888272486a2d1ab2c427fb2 - image2017-11-23-030256.7z
- b2de2ea9bd7c1c1b10010f53d299564f6833d81aec7614859b4f67518fa565fb - image2017-11-23-043100.7z
- 3958f05bc95d4de0cb5e73b7cb3e6df65e9c6f12162b62b9fcc8770e1d877cad - image2017-11-23-9164504.7z
- e6215a0e9f9c30c43a453503e00acba44bd0f18eb52d187d00cadf6165e23fe6 - image2017-11-23-939559.7z

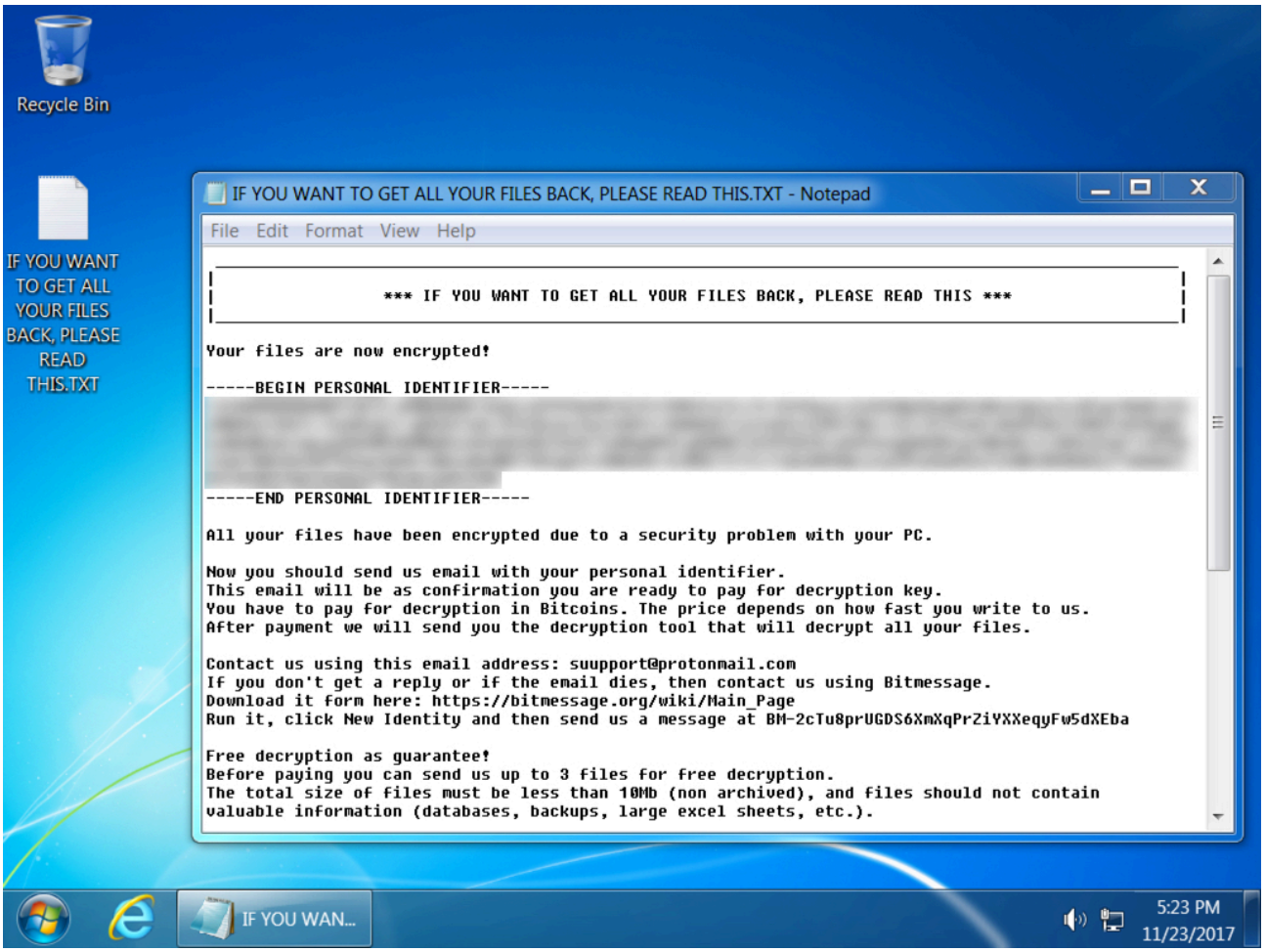
FILE HASHES FOR THE EXTRACTED VBS FILES:

- fd072a6c2fe9187f799a27e21c27fc67dd2f145ccbc0faa917f37469d0d26974 - image2017-11-22-5379282.vbs
- 25ee9aaf6fd29574f3b897c85286a201b0ba4f946956bf0ea6ec0a9c29c6b248 - image2017-11-22-6133563.vbs
- 39e61f8fff8b7b6a36aa54b4046df218d87ab370edf457b75d6c2547577c6b78 - image2017-11-22-7374139.vbs
- 9bd4009931ca1182763ca0acacd74fc11917d04fe7c2459bc4e1e3b3d88eae5d - image2017-11-22-9088289.vbs
- 281c8ccf6b1a0d983b696c656883da14a43fc4408c92d8012f08fba144de121a - image2017-11-22-9603833.vbs

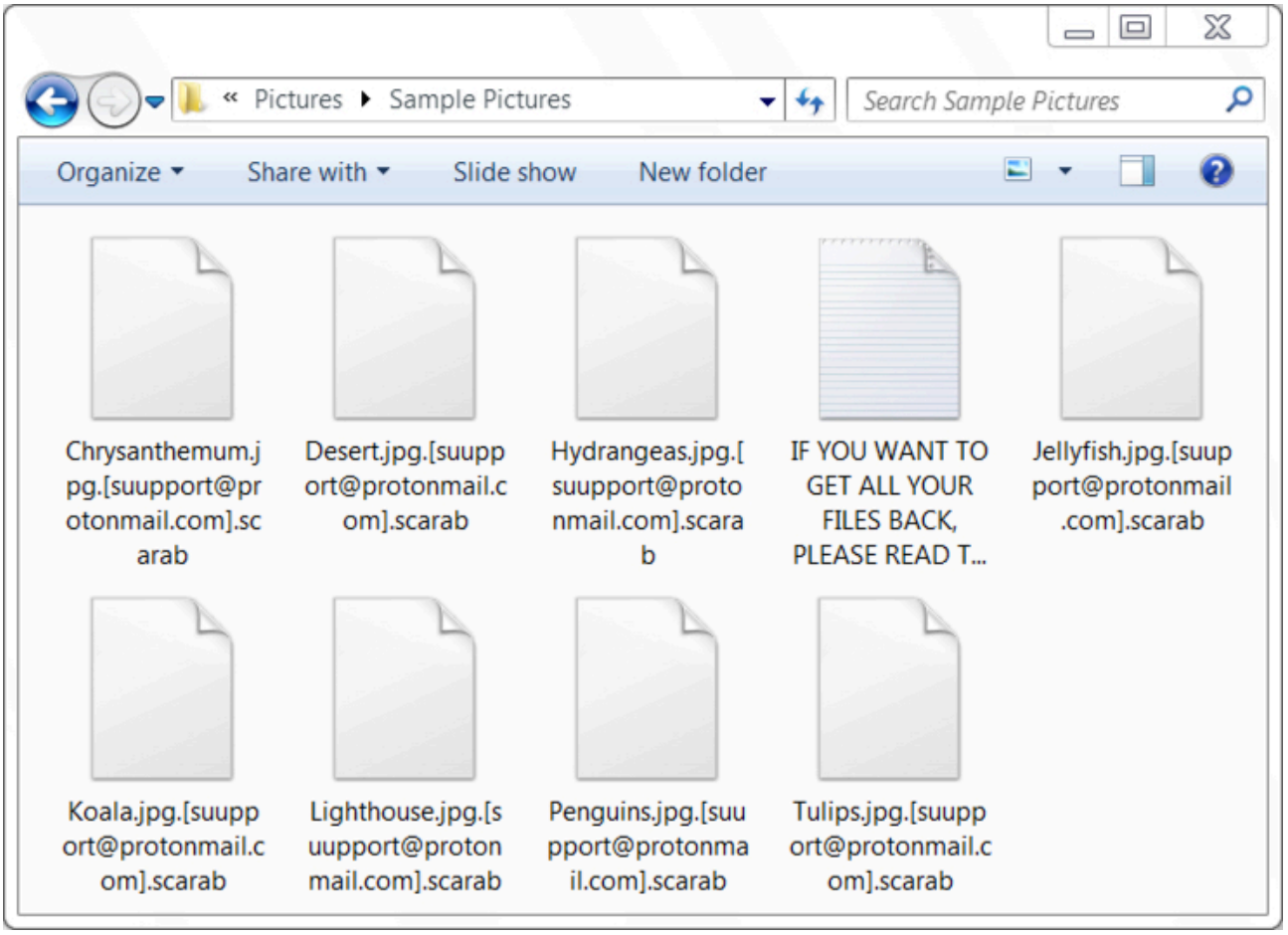
DOWNLOADED "SCARAB" RANSOMWARE:

- SHA256 hash: 7a60e9f0c00bcf5791d898c84c26f484b4c671223f6121dc3608970d8bf8fe4f
  File size: 365,056 bytes
  File location: C:\Users*[username]*\AppData\Local\Temp*[random string]*.exe

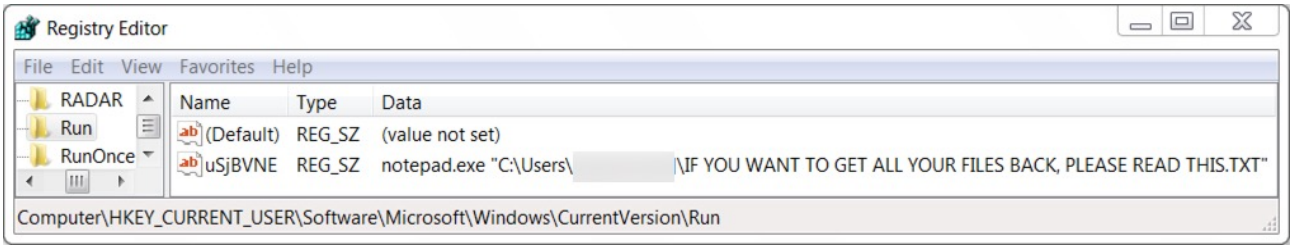
IMAGES



Shown above: Desktop of an infected Windows host.



Shown above: An example of the encrypted files.



Shown above: Registry key updated to display the ransom note on reboot.

Click here to return to the main page.

Source: http://malware-traffic-analysis.net/2017/11/23/index.html