Malware-Traffic-Analysis.net - 2018-01-04 - PCRAT/Gh0st infection

Archived: 2026-04-05 15:27:40 UTC

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:

- 2018-01-04-PCRAT-Gh0st-traffic.pcap.zip 1.7 kB (1,681 bytes)

> - 2018-01-04-PCRAT-Gh0st-traffic.pcap (5,009 bytes)

- 2018-01-04-PCRAT-Gh0st-email-and-malware.zip 701.6 kB (701,577 bytes)

> - 2018-01-04-malspam-pushing-PCRAT-Gh0st-1813-UTC.eml (256,098 bytes)
> - RasTls.dat (149,816 bytes)
> - RasTls.dll (45,056 bytes)
> - RasTls.exe (107,848 bytes)
> - Very beautiful.exe (393,216 bytes)
> - Very beautiful.zip (185,607 bytes)

NOTES:

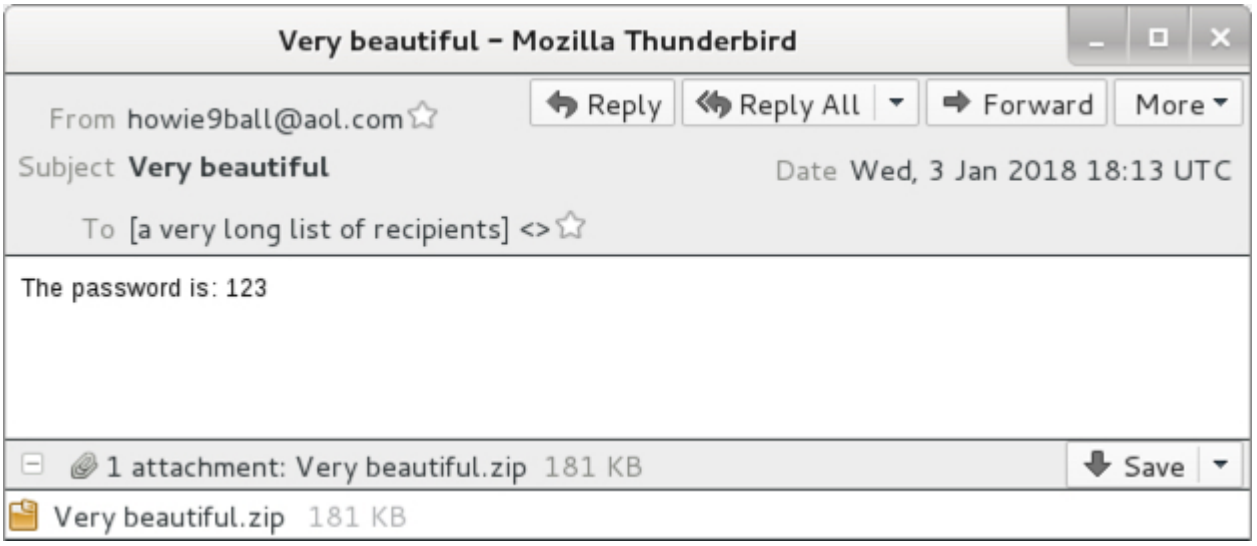
- The zip attachment is password-protected with ***123*** as stated in the malspam.
- Post-infection activity triggered an EmergingThreats alert for PCRAT/Gh0st CnC traffic

WEB TRAFFIC BLOCK LIST

Indicators are not a block list. If you feel the need to block web traffic, I suggest the following URLs and domain:

- www.etybh[.]com

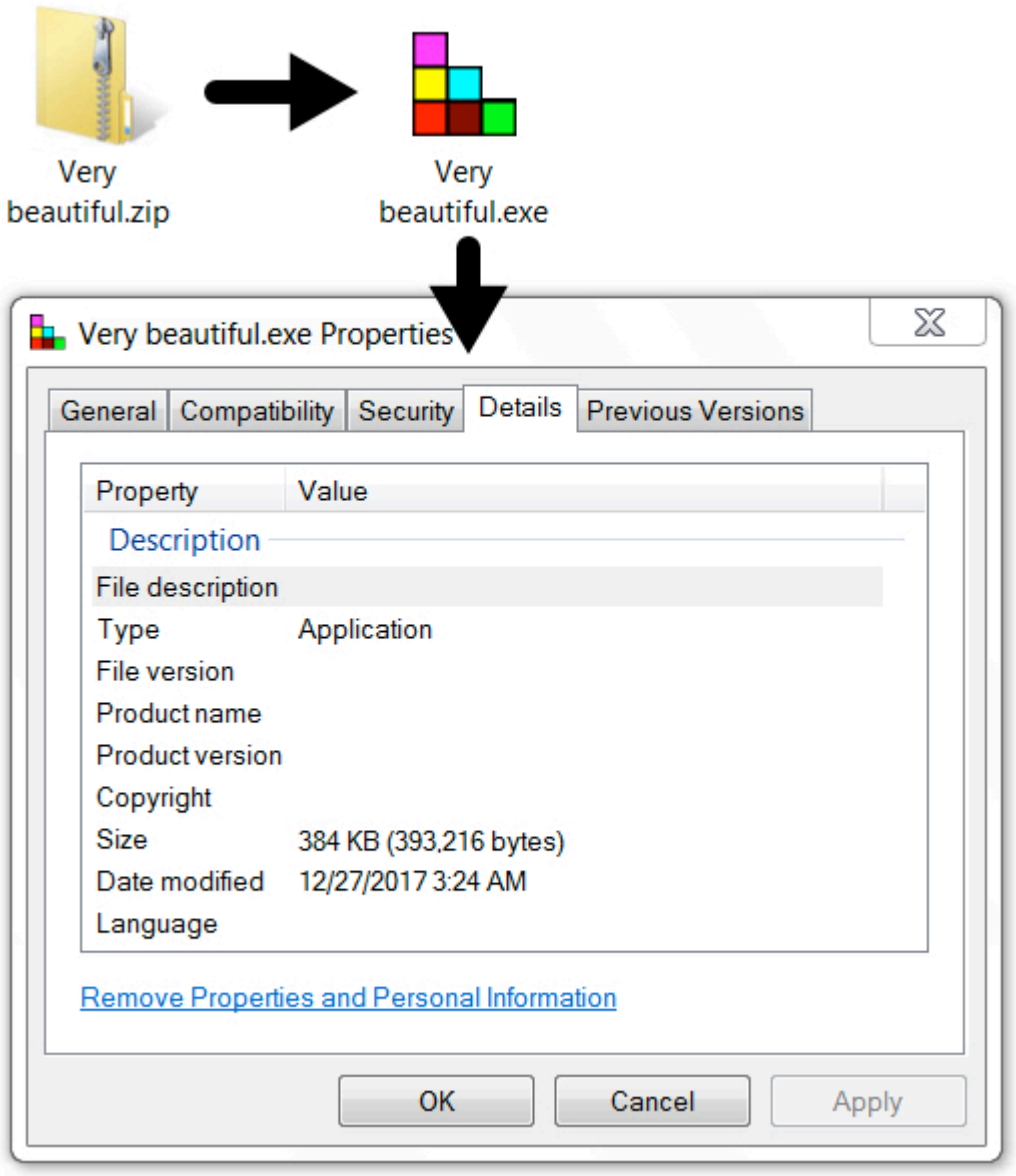
EMAIL



Shown above: Screenshot of the email.

EMAIL INFORMATION:

- Date: Wednesday, 2018-01-03 at 18:13 UTC
- Subject: Very beautiful
- From: howie9ball@aol[.]com
- To: [a very long list of recipients]
- Message-Id: <160bd3a471c-171d-2842@webjas-vac003.srv.aolmail.net>
- Attachment name: Very beautiful.zip



Shown above: Malware extracted from the zip attachment.

TRAFFIC

Date/Time	Src	port	Dst	port	Info
2018-01-04 19:19:32	10.1.4.101	64186	10.1.4.1	53	Standard query 0x77c3 A www.etybh.com
2018-01-04 19:19:32	10.1.4.1	53	10.1.4.101	64186	Standard query response 0x77c3 A 98.126.223.218
2018-01-04 19:19:34	10.1.4.101	49221	98.126.223.218	900	49221→omginitialrefs [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256
2018-01-04 19:19:34	98.126.223.218	900	10.1.4.101	49221	omginitialrefs→49221 [SYN, ACK] Seq=0 Ack=1 Win=16384 Len=0 MSS=
2018-01-04 19:19:34	10.1.4.101	49221	98.126.223.218	900	49221→omginitialrefs [ACK] Seq=1 Ack=1 Win=65536 Len=0
2018-01-04 19:19:34	10.1.4.101	49221	98.126.223.218	900	49221→omginitialrefs [PSH, ACK] Seq=1 Ack=1 Win=65536 Len=95
2018-01-04 19:19:35	98.126.223.218	900	10.1.4.101	49221	omginitialrefs→49221 [PSH, ACK] Seq=1 Ack=96 Win=65440 Len=27
2018-01-04 19:19:35	10.1.4.101	49221	98.126.223.218	900	49221→omginitialrefs [ACK] Seq=96 Ack=28 Win=65536 Len=0
2018-01-04 19:22:35	10.1.4.101	49221	98.126.223.218	900	[TCP Keep-Alive] 49221→omginitialrefs [ACK] Seq=95 Ack=28 Win=65
2018-01-04 19:22:35	98.126.223.218	900	10.1.4.101	49221	[TCP Keep-Alive ACK] omginitialrefs→49221 [ACK] Seq=28 Ack=96 Wi
2018-01-04 19:22:35	98.126.223.218	900	10.1.4.101	49221	[TCP Keep-Alive] omginitialrefs→49221 [ACK] Seq=27 Ack=96 Win=65
2018-01-04 19:22:35	10.1.4.101	49221	98.126.223.218	900	[TCP Keep-Alive ACK] 49221→omginitialrefs [ACK] Seq=96 Ack=28 Wi
2018-01-04 19:25:35	10.1.4.101	49221	98.126.223.218	900	[TCP Keep-Alive] 49221→omginitialrefs [ACK] Seq=95 Ack=28 Win=65
2018-01-04 19:25:35	98.126.223.218	900	10.1.4.101	49221	[TCP Keep-Alive] omginitialrefs→49221 [ACK] Seq=27 Ack=96 Win=65
2018-01-04 19:25:35	10.1.4.101	49221	98.126.223.218	900	[TCP Keep-Alive ACK] 49221→omginitialrefs [ACK] Seq=96 Ack=28 Wi

Shown above: Infection traffic filtered in Wireshark.

ASSOCIATED TRAFFIC:

- 98.126.223[.]218 port 900 - **www.etybh[.]com** - PCRAT/Gh0st CnC traffic

MALWARE

ZIP ARCHIVE FROM THE MALSPAM:

- SHA256 hash: 067d5729b4787fc667c061b027625be4273806c64beacfb6877fc7f182f9ed37
  File size: 185,607 bytes
  File name: Very beautiful.zip

MALICIOUS EXECUTABLE EXTRACTED FROM THE ZIP ARCHIVE:

- SHA256 hash: 423f4c1f9ba4f184ff6e82db4f01420feb7b76693bdece6402fc2157c0c2f946
  File size: 393,216 bytes
  File name: Very beautiful.exe

EXECUTABLE FROM THE INFECTED WINDOWS HOST:

- SHA256 hash: f9ebf6aeb3f0fb0c29bd8f3d652476cd1fe8bd9a0c11cb15c43de33bbce0bf68
  File size: 107,848 bytes
  File location: C:\Microsoft\TEMP\Networks\Connections\Sementech\sementech\RasTls.exe
  NOTE: This is apparently a legitimate file abused by various Trojans for DLL side-loading.

DLL FROM THE INFECTED WINDOWS HOST:

- SHA256 hash: a392f8f96ffc53978b177d844ef17adb09c6329997f29334e5c2029e8f5f18e8
  File size: 45,056 bytes
  File location: C:\Microsoft\TEMP\Networks\Connections\Sementech\sementech\RasTls.dll

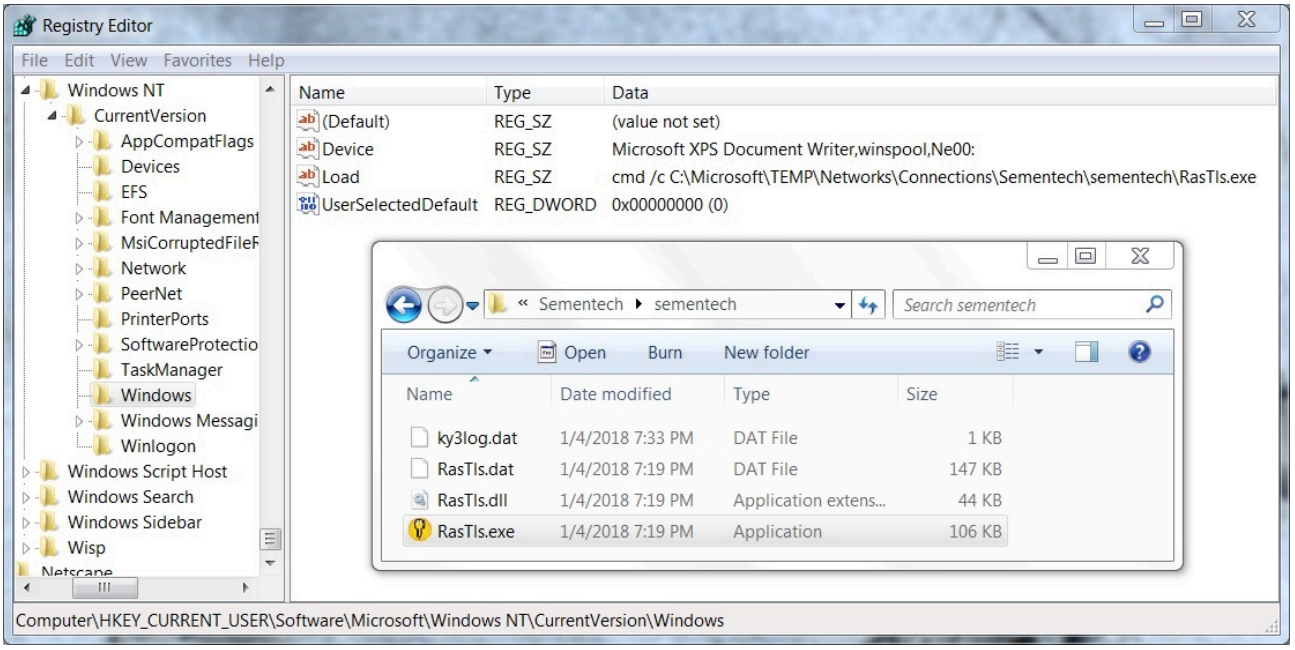
WINDOWS REGISTRY ENTRY FOR PERSISTENCE:

- Registry Key: HKCU\Software\Microsoft\Windows NT\CurrentVersion\Windows
- Value name: Load
- Value Type: REG_SZ
- Value Data: cmd /c C:\Microsoft\TEMP\Networks\Connections\Sementech\sementech\RasTls.exe

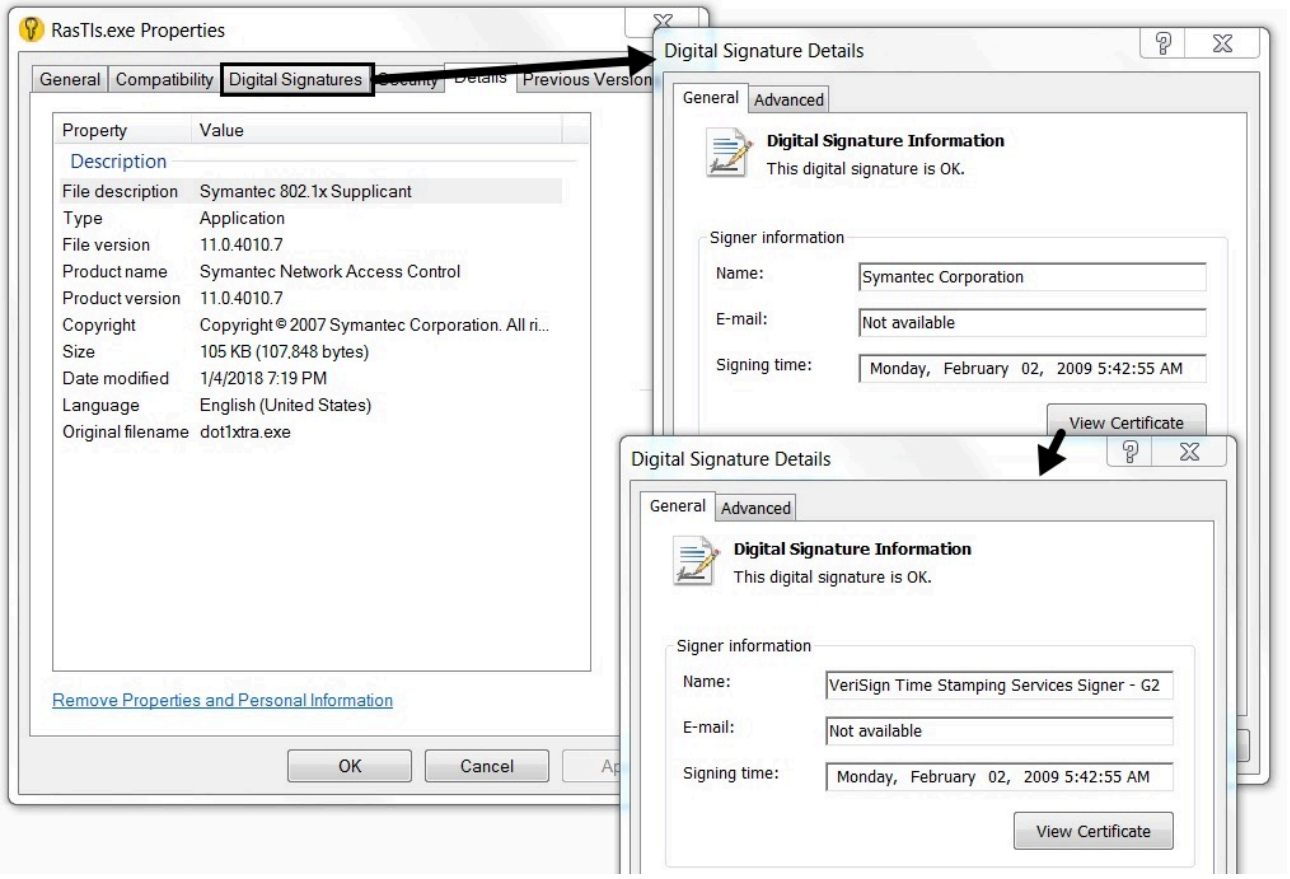
IMAGES

Shown above: TCP stream from the post-infection traffic.

Shown above: Alert from Sguil on the post-infection traffic in Security Onion using Suricata and the EmergingThreats ruleset.



Shown above: Registry key and associated files on the infected Windows host



Shown above: Apparently, a legitimate file abused by various malware families for DLL side-loading.

Click here to return to the main page.

Source: http://www.malware-traffic-analysis.net/2018/01/04/index.html