Malware-Traffic-Analysis.net - 2017-11-02 - Adventures with Smoke Loader

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.

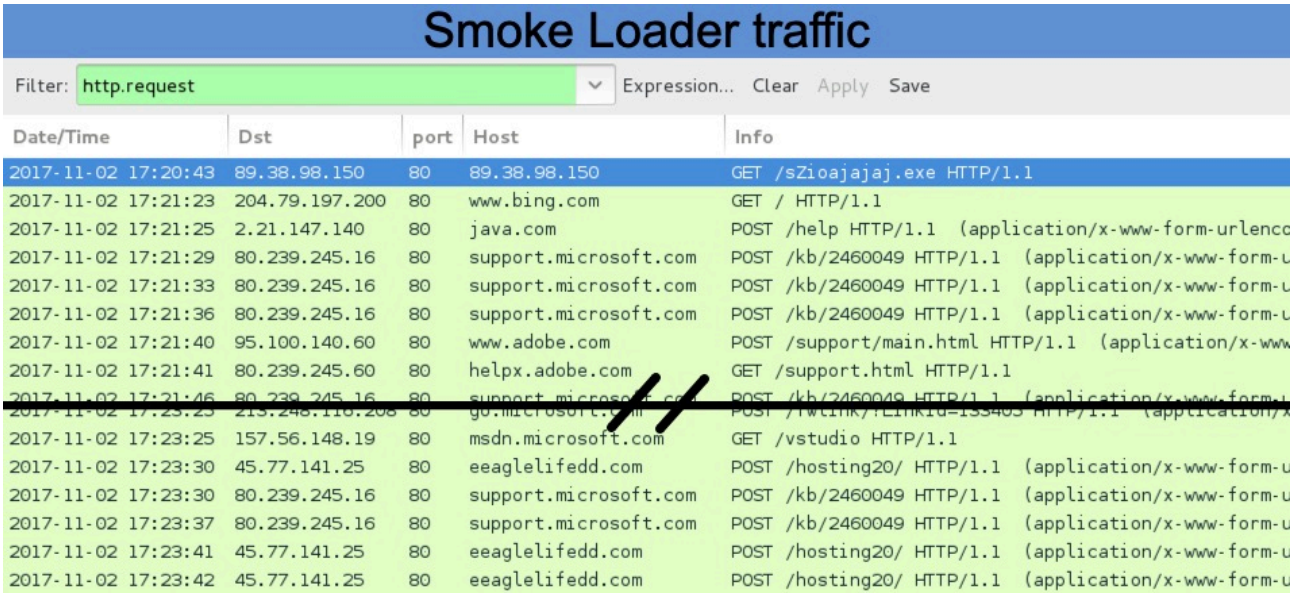
ASSOCIATED FILES:

- 2017-11-02-Smoke-Loader-infection-traffic.pcap.zip 712.0 kB (711,971 bytes)
- 2017-11-02-Neutrino-malware-infection-traffic.pcap.zip 4.4 MB (4,417,303 bytes)
- 2017-11-02-associated-malware-samples.zip 1.1 MB (1,089,242 bytes)

INFECTION SUMMARY

89.38.98[.]150/sZioajajaj.exe (Smoke Loader) --> Neutrino malware --> Lethic spambot infection

IMAGES



Shown above: Smoke Loader infection traffic filtered in Wireshark.

Smoke Loader alerts

RealTime Events | Escalated Events

ST	CNT	Date/Time	Src IP	SPort	Dst IP	DPort	Pr	Event Message
RT	1	2017-11-02...	10.11.2.101	49410	89.38.98.150	80	6	ET POLICY exe download via HTTP - Informational
RT	1	2017-11-02...	10.11.2.101	49410	89.38.98.150	80	6	ET INFO Executable Download from dotted-quad Host
RT	2	2017-11-02...	89.38.98.150	80	10.11.2.101	49410	6	ET POLICY PE EXE or DLL Windows file download
RT	2	2017-11-02...	89.38.98.150	80	10.11.2.101	49410	6	ET POLICY Binary Download Smaller than 1 MB Likely Hostile
RT	28	2017-11-02...	10.11.2.101	49415	80.239.245.16	80	6	ET TROJAN Sharik/Smoke Loader Microsoft Connectivity check
RT	2	2017-11-02...	10.11.2.101	49418	95.100.140.60	80	6	ET TROJAN Sharik/Smoke Loader Adobe Connectivity check
RT	36	2017-11-02...	89.38.98.150	80	10.11.2.101	49410	6	ET TROJAN VMProtect Packed Binary Inbound via HTTP - Likely Hostile
RT	4	2017-11-02...	10.11.2.101	49418	95.100.140.60	80	6	ET TROJAN Sharik/Smoke Loader Adobe Connectivity Check 3
RT	8	2017-11-02...	10.11.2.101	49429	213.248.116.208	80	6	ET TROJAN Sharik/Smoke Loader Microsoft Connectivity Check
RT	4	2017-11-02...	10.11.2.101	49437	95.100.140.60	80	6	ET TROJAN Sharik/Smoke Loader Adobe Connectivity Check 2
RT	3	2017-11-02...	45.77.141.25	80	10.11.2.101	49449	6	ET POLICY PE EXE or DLL Windows file download
RT	2	2017-11-02...	45.77.141.25	80	10.11.2.101	49449	6	ETPRO TROJAN Smoke/Sharik HTTP 404 Containing EXE

Shown above: Alerts from Smoke Loader infection traffic on Security Onion using Sguil with Suricata and the EmergingThreats Pro (ETPRO) ruleset.

Neutrino malware infection traffic (HTTP requests)

Filter: http.request | Expression... | Clear | Apply | Save

Date/Time	Dst	port	Host	Info
2017-11-02 19:21:14	118.193.174.133	80	n31.smokemenowhhalala.bit	POST /newfiz31/logout.php HTTP/1.0 (application/
2017-11-02 19:21:24	118.193.174.133	80	n31.smokemenowhhalala.bit	POST /newfiz31/logout.php HTTP/1.0 (application/
2017-11-02 19:21:28	89.38.98.150	80	89.38.98.150	GET /85cZioajajaj.exe HTTP/1.1
2017-11-02 19:21:34	118.193.174.133	80	n31.smokemenowhhalala.bit	POST /newfiz31/logout.php HTTP/1.0 (application/
2017-11-02 19:21:38	89.38.98.150	80	89.38.98.150	GET /17Zioajajaj.exe HTTP/1.1
2017-11-02 19:21:42	118.193.174.133	80	n31.smokemenowhhalala.bit	POST /newfiz31/logout.php HTTP/1.0 (application/
2017-11-02 19:21:48	89.38.98.150	80	89.38.98.150	GET /74Zioajajaj.exe HTTP/1.1
2017-11-02 19:21:53	118.193.174.133	80	n31.smokemenowhhalala.bit	POST /newfiz31/logout.php HTTP/1.0 (application/
2017-11-02 19:21:58	89.38.98.150	80	89.38.98.150	GET /121Zioajajaj.exe HTTP/1.1
2017-11-02 19:22:05	118.193.174.133	80	n31.smokemenowhhalala.bit	POST /newfiz31/logout.php HTTP/1.0 (application/
2017-11-02 19:22:08	89.38.98.150	80	89.38.98.150	GET /123Zioajajaj.exe HTTP/1.1
2017-11-02 19:22:14	118.193.174.133	80	n31.smokemenowhhalala.bit	POST /newfiz31/logout.php HTTP/1.0 (application/
2017-11-02 19:22:18	89.38.98.150	80	89.38.98.150	GET /226Zioajajaj.exe HTTP/1.1
2017-11-02 19:22:23	118.193.174.133	80	n31.smokemenowhhalala.bit	POST /newfiz31/logout.php HTTP/1.0 (application/
2017-11-02 19:22:28	89.38.98.150	80	89.38.98.150	GET /38Zioajajaj.exe HTTP/1.1
2017-11-02 19:22:32	118.193.174.133	80	n31.smokemenowhhalala.bit	POST /newfiz31/logout.php HTTP/1.0 (application/
2017-11-02 19:22:38	89.38.98.150	80	89.38.98.150	GET /161Zioajajaj.exe HTTP/1.1
2017-11-02 19:22:44	118.193.174.133	80	n31.smokemenowhhalala.bit	POST /newfiz31/logout.php HTTP/1.0 (application/
2017-11-02 19:25:09	118.193.174.133	80	n31.smokemenowhhalala.bit	POST /newfiz31/logout.php HTTP/1.0 (application/
2017-11-02 19:28:59	118.193.174.133	80	n31.smokemenowhhalala.bit	POST /newfiz31/logout.php HTTP/1.0 (application/
2017-11-02 19:32:50	118.193.174.133	80	n31.smokemenowhhalala.bit	POST /newfiz31/logout.php HTTP/1.0 (application/

Shown above: Neutrino malware infection traffic filtered in Wireshark.

Lethic spambot traffic in Neutrino pcap

Filter: !(tcp.port eq 80) and !(tcp.port eq 443) and tcp.flags e Expression... Clear Apply Save

Dst	port	Info
109.236.87.85	5500	49164→fcp-addr-srvr1 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
89.248.174.17	5500	49167→fcp-addr-srvr1 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
80.82.65.74	5500	49169→fcp-addr-srvr1 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
65.54.188.94	25	49171→smtp [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
65.55.37.120	25	49172→smtp [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
98.138.112.32	25	49174→smtp [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
98.138.112.38	25	49176→smtp [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
91.232.105.121	5500	49177→fcp-addr-srvr1 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
109.236.87.85	5500	49178→fcp-addr-srvr1 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
182.22.12.247	25	49179→smtp [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
89.248.174.17	5500	49182→fcp-addr-srvr1 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
217.23.14.123	5500	49183→fcp-addr-srvr1 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
66.218.85.139	25	49184→smtp [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
66.196.118.240	25	49187→smtp [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
93.190.137.226	5500	49188→fcp-addr-srvr1 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
182.22.12.247	25	49189→smtp [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
104.44.194.237	25	49191→smtp [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
217.23.15.38	6600	49193→mshvlm [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
109.236.87.85	5500	49194→fcp-addr-srvr1 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
133.139.20.60	25	49195→smtp [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
217.23.14.123	5500	49196→fcp-addr-srvr1 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1

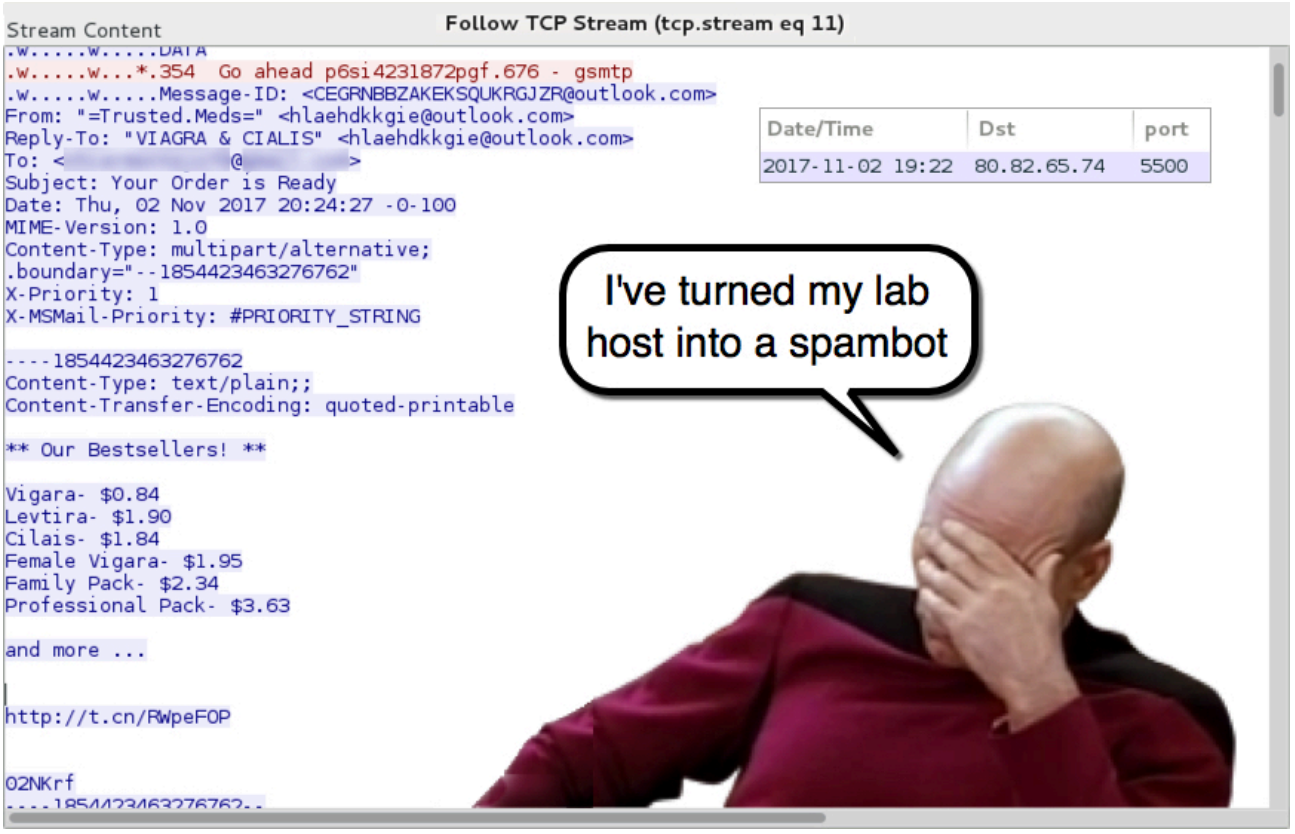
Shown above: Neutrino pcap filtered to show some of the post-infection IPs/ports for Lethic spambot activity,

Neutrino malware alerts

RealTime Events | Escalated Events

ST	CNT	Date/Time	Src IP	SPort	Dst IP	DPort	Pr	Event Message
RT	13	2017-11-02...	10.11.2.102	49158	118.193.174.133	80	6	ETPRO TROJAN Win32/Neutrino checkin 4
RT	8	2017-11-02...	10.11.2.102	49160	89.38.98.150	80	6	ET POLICY exe download via HTTP - Informational
RT	8	2017-11-02...	10.11.2.102	49160	89.38.98.150	80	6	ET INFO Executable Download from dotted-quad Host
RT	16	2017-11-02...	89.38.98.150	80	10.11.2.102	49160	6	ET POLICY PE EXE or DLL Windows file download
RT	16	2017-11-02...	89.38.98.150	80	10.11.2.102	49160	6	ET POLICY Binary Download Smaller than 1 MB Likely Hostile
RT	61	2017-11-02...	89.38.98.150	80	10.11.2.102	49160	6	ET INFO SUSPICIOUS Dotted Quad Host MZ Response
RT	2	2017-11-02...	89.38.98.150	80	10.11.2.102	49165	6	ET SHELLCODE Possible TCP x86 JMP to CALL Shellcode Detected
RT	27	2017-11-02...	10.11.2.102	57216	10.11.1.1	53	17	ET CURRENT_EVENTS DNS Query Domain .bit
RT	41	2017-11-02...	10.11.2.102	49169	80.82.65.74	5500	6	ET TROJAN Lethic Spambot CnC Initial Connect Bot Response
RT	85	2017-11-02...	10.11.2.102	49169	80.82.65.74	5500	6	ET TROJAN Lethic Spambot CnC Bot Command Confirmation
RT	6	2017-11-02...	10.11.2.102	49169	80.82.65.74	5500	6	ET TROJAN Lethic - Client Alive
RT	1869	2017-11-02...	10.11.2.102	49169	80.82.65.74	5500	6	ET TROJAN Lethic Spambot CnC Bot Transaction Relay

Shown above: Alerts from the Neutrino & Lethic spambot traffic on Security Onion using Sguil with Suricata and the EmergingThreats Pro (ETPRO) ruleset.



Shown above: TCP stream of Lethic spambot traffic.

DETAILS

NOTES:

- Saw a malicious HTTP request to 89.38.98[.]150 led to Sharik/Smoke Loader.
- When I tested it in my lab, it retrieved Neutrino malware, which then retrieved Lethic spambot malware.
- About an hour I tried this, 89.38.98[.]150/sZioajajaj.exe returned a different file hash that was still Sharik/Smoke Loader.

DOMAINS OR URLS TO BLOCK:

- hxxp[:]//89.38.98[.]150/sZioajajaj.exe
- hxxp[:]//89.38.98[.]150/85cZioajajaj.exe
- hxxp[:]//89.38.98[.]150/17Zioajajaj.exe
- hxxp[:]//89.38.98[.]150/74Zioajajaj.exe
- hxxp[:]//89.38.98[.]150/121Zioajajaj.exe
- hxxp[:]//89.38.98[.]150/123Zioajajaj.exe
- hxxp[:]//89.38.98[.]150/226Zioajajaj.exe
- hxxp[:]//89.38.98[.]150/38Zioajajaj.exe
- hxxp[:]//89.38.98[.]150/161Zioajajaj.exe
- eeaglelifedd.com
- n31.smokemenowhhalala.bit

INITIAL MALWARE - SHARIK/SMOKE LOADER:

- SHA256 hash: 6401c4de903ec06a5493adf7a9dd45e123c9ce3033b44e1083e10bc5709c3964
  File size: 122,880 bytes
  Online location: 89.38.98[.]150/sZioajajaj.exe
  On infected host at: C:\Users\[username]\AppData\Roaming\Microsoft\ujwbersj\gresctab.exe
  Associated Windows registry update: HKCU\Software\Microsoft\Windows\CurrentVersion\Run

- SHA256 hash: 035f394168da1c15cf98792f12b0292fefdb7dd29538c3b1e019d2fb09d3dfa6
  File size: 118,272 bytes
  Online location: 89.38.98[.]150/sZioajajaj.exe
  On infected host at: C:\Users\[username]\AppData\Roaming\Microsoft\ujwbersj\gresctab.exe
  Associated Windows registry update: HKCU\Software\Microsoft\Windows\CurrentVersion\Run

SHARIK/SMOKE LOADER TRAFFIC:

Start date/time: 2017-11-02 at 17:20 UTC

- 89.38.98[.]150 port 80 - 89.38.98[.]150 - GET /sZioajajaj.exe
- www.bing[.]com - GET /
- java[.]com - POST /help
- java[.]com - GET /en/download/help/index.html
- java[.]com - GET /en/download/help/
- support.microsoft[.]com - POST /kb/2460049
- www.adobe[.]com - POST /
- www.adobe[.]com - POST /go/flashplayer_support/
- www.adobe[.]com - POST /support/flashplayer
- www.adobe[.]com - POST /support/main.html
- helpx.adobe[.]com - GET /flash-player.html
- helpx.adobe[.]com - GET /support.html
- go.microsoft[.]com - POST /fwlink/?LinkId=133405
- go.microsoft[.]com - POST /fwlink/?LinkId=164164
- msdn.microsoft[.]com - GET /vstudio
- www.microsoft[.]com - GET /
- 45.77.141[.]25 port 80 - eeaglelifedd[.]com - POST /hosting20/

ASSOCIATED EMERGING THREATS (ET) AND ETPRO ALERTS:

- ET TROJAN Sharik/Smoke Loader Microsoft Connectivity Check
- ET TROJAN Sharik/Smoke Loader Adobe Connectivity Check
- ET TROJAN Sharik/Smoke Loader Adobe Connectivity Check 2
- ET TROJAN Sharik/Smoke Loader Adobe Connectivity Check 3
- ETPRO TROJAN Smoke/Sharik HTTP 404 Containing EXE

FOLLOW-UP MALWARE - NEUTRINO MALWARE:

- SHA256 hash: 517e92c585449b75d6b8a5e5f00323fb5f3b125972cd1442b1251ca7087107fc
  File size: 255,488 bytes
  File returned from HTTP POST to: eeaglelifedd[.]com/hosting20/
  On infected host at: C:\Users\[username]\AppData\Roaming\Xl5jVVxcVWIx\jevgr.exe

NEUTRINO MALWARE INFECTION TRAFFIC:

- DNS queries for ns.dotbit[.]me - resolved to 107.161.16[.]236
- 107.161.16[.]236 port 53 - DNS queries (UDP) for n31.smokemenowhhalala[.]bit
- 118.193.174[.]133 port 80 - n31.smokemenowhhalala[.]bit - POST /newfiz31/logout.php
- 89.38.98[.]150 port 80 - 89.38.98[.]150 - GET /85cZioajajaj.exe
- 89.38.98[.]150 port 80 - 89.38.98[.]150 - GET /17Zioajajaj.exe
- 89.38.98[.]150 port 80 - 89.38.98[.]150 - GET /74Zioajajaj.exe
- 89.38.98[.]150 port 80 - 89.38.98[.]150 - GET /121Zioajajaj.exe
- 89.38.98[.]150 port 80 - 89.38.98[.]150 - GET /123Zioajajaj.exe
- 89.38.98[.]150 port 80 - 89.38.98[.]150 - GET /226Zioajajaj.exe
- 89.38.98[.]150 port 80 - 89.38.98[.]150 - GET /38Zioajajaj.exe
- 89.38.98[.]150 port 80 - 89.38.98[.]150 - GET /161Zioajajaj.exe

ASSOCIATED EMERGING THREATS (ET) AND ETPRO ALERTS:

- ETPRO TROJAN Win32/Neutrino checkin 4 (118.193.174[.]133 port 80)

FOLLOW-UP MALWARE FROM NEUTRINO MALWARE INFECTION - ALL LETHIC SPAMBOT MALWARE BINARIES:

- SHA256 hash: e324c63717a4c2011fde7d1af0d8dbe8ddb0897fe4e7f80f3147a7498e2166fe
  File size: 185,344 bytes
  Location: 89.38.98[.]150/161Zioajajaj.exe
  Location: C:\RECYCLER\S-1-5-21-0243556031-888888379-781862338-196818750\backwindow32.exe
  Associated Windows registry update: HKCU\Software\Microsoft\Windows\CurrentVersion\Run

- SHA256 hash: f55be01c217b2ec9be0aa45a007661adb1365a9651e306329679a6ba2d5b119d
  File size: 192,512 bytes
  Location: 89.38.98[.]150/85cZioajajaj.exe
  Location: C:\RECYCLER\S-1-5-21-0243556031-888888379-781862338-196818750\backwindow132.exe
  Associated Windows registry update: HKCU\Software\Microsoft\Windows\CurrentVersion\Run

- SHA256 hash: 701a2461d31b1a717fc9dad4fd61458c3484836bb89b4c72c0841ce9b3948d52
  File size: 186,880 bytes
  Location: 89.38.98[.]150/17Zioajajaj.exe
  Location: C:\RECYCLER\S-1-5-21-0243556031-888888379-781862338-196818750\backwindow232.exe
  Associated Windows registry update: HKCU\Software\Microsoft\Windows\CurrentVersion\Run

- SHA256 hash: eacbc0588d0e8fc22daf80479598cfb49a6bdc7155efd2bd3c24740a22716d17
  File size: 191,488 bytes

Location: 89.38.98[.]150/74Zioajajaj.exe
Location: C:\RECYCLER\S-1-5-21-0243556031-888888379-781862338-1968138750\backwindow332.exe
Associated Windows registry update: HKCU\Software\Microsoft\Windows\CurrentVersion\Run

- SHA256 hash: 8b57e7424e305a87cb55ff69c1454855341e5b138cec648b3b3a96df53d1076a
File size: 186,368 bytes
Location: 89.38.98[.]150/121Zioajajaj.exe
Location: C:\RECYCLER\S-1-5-21-0243556031-888888379-781862338-1968138750\backwindow432.exe
Associated Windows registry update: HKCU\Software\Microsoft\Windows\CurrentVersion\Run

- SHA256 hash: f3eadfd04bdf3615afb5f4b9b3b7386579846a834a389585cbbee6a3c7640ca3
File size: 188,928 bytes
Location: 89.38.98[.]150/123Zioajajaj.exe
Location: C:\RECYCLER\S-1-5-21-0243556031-888888379-781862338-1968138750\backwindow532.exe
Associated Windows registry update: HKCU\Software\Microsoft\Windows\CurrentVersion\Run

- SHA256 hash: 2de7e6763fd895757e4504e72389a8aee9f2f63f651d02efc22b1865bbd4f1b0
File size: 193,024 bytes
Location: 89.38.98[.]150/226Zioajajaj.exe
Location: C:\RECYCLER\S-1-5-21-0243556031-888888379-781862338-1968138750\backwindow632.exe
Associated Windows registry update: HKCU\Software\Microsoft\Windows\CurrentVersion\Run

- SHA256 hash: b7137c65b7c8884329c252d14fe32d4ffa96fd1a9886f895b39b1d3419c01895
File size: 187,392 bytes
Location: 89.38.98[.]150/38Zioajajaj.exe
Location: C:\RECYCLER\S-1-5-21-0243556031-888888379-781862338-1968152800\systimwindow32.exe
Associated Windows registry update: HKCU\Software\Microsoft\Windows\CurrentVersion\Run

LETHIC SPAMBOT INFECTION TRAFFIC:

- Various IP addresses over TCP port 25 - attempted SMTP traffic
- Various IP addresses over TCP port 25, 5500, 6600, and 7700 - SMTP and similar spambot traffic
- Possibly other IP addresses over similar ports that didn't establish a full TCP connection

ASSOCIATED EMERGING THREATS (ET) AND ETPRO ALERTS:

- ET TROJAN Lethic Spambot CnC Initial Connect Bot Response
- ET TROJAN Lethic Spambot CnC Bot Command Confirmation
- ET TROJAN Lethic Spambot CnC Bot Transaction Relay
- ET TROJAN Lethic Client Alive

Click here to return to the main page.
