LINKS ABOUT THE MALWARE

* [http://en.wikipedia.org/wiki/Zeus\_(Trojan\_horse)](http://en.wikipedia.org/wiki/Zeus_%28Trojan_horse%29)
* <http://nakedsecurity.sophos.com/2012/12/05/the-citadel-crimeware-kit-under-the-microscope/>
* <http://blog.trendmicro.com/trendlabs-security-intelligence/zeuszbot-malware-shapes-up-in-2013/>

**CHAIN OF EVENTS**

ASSOCIATED DOMAINS

* 23.226.224.193 - **valerierobinson.com** - Comrpomised website
* 188.40.79.151 - **38hartrobertsroad.com** - First redirect domain
* 62.76.177.211 - **62.76.177.211** - Second redirect
* 31.22.4.108 - **30oct2007.com** - Final redirect
* 212.83.135.167 - **eesheshi.ontowess.com** - Neutrino EK domain over TCP port 8000
* 89.191.150.230 - **www.gminalubiewo.pl** - Post-infection callback domain - triggered Zeus/Zbot/Citadel events
* 118.69.206.95:80 - **www.kimsa.vn** - Post-infection callback domain - triggered Zeus/Zbot events

INFECTION CHAIN OF EVENTS

* 03:26:57 UTC - 192.168.204.162:49610 - 23.226.224.193:80 - www.valerierobinson.com - GET /?p=1
* 03:26:57 UTC - 192.168.204.162:49612 - 23.226.224.193:80 - valerierobinson.com - GET /?p=1
* 03:26:57 UTC - 192.168.204.162:49612 - 23.226.224.193:80 - valerierobinson.com - GET /wp-content/themes/twentytwelve/js/navigation.js?ver=1.0
* 03:26:58 UTC - 192.168.204.162:49621 - 188.40.79.151:80 - 38hartrobertsroad.com - GET /wp-content/plugins/rotr
* 03:26:58 UTC - 192.168.204.162:49622 - 188.40.79.151:80 - 38hartrobertsroad.com - GET /wp-content/plugins/rotr
* 03:26:58 UTC - 192.168.204.162:49622 - 188.40.79.151:80 - 38hartrobertsroad.com - GET /wp-content/plugins/rotr/
* 03:26:58 UTC - 192.168.204.162:49621 - 188.40.79.151:80 - 38hartrobertsroad.com - GET /wp-content/plugins/rotr/
* 03:26:59 UTC - 192.168.204.162:49622 - 188.40.79.151:80 - 38hartrobertsroad.com - HEAD /wp-content/plugins/rotr/load.swf?sid=28949
* 03:26:59 UTC - 192.168.204.162:49621 - 188.40.79.151:80 - 38hartrobertsroad.com - HEAD /wp-content/plugins/rotr/load.swf?sid=66025
* 03:26:59 UTC - 192.168.204.162:49622 - 188.40.79.151:80 - 38hartrobertsroad.com - GET /wp-content/plugins/rotr/load.swf?sid=28949
* 03:26:59 UTC - 192.168.204.162:49621 - 188.40.79.151:80 - 38hartrobertsroad.com - GET /wp-content/plugins/rotr/load.swf?sid=66025
* 03:26:59 UTC - 192.168.204.162:49621 - 188.40.79.151:80 - 38hartrobertsroad.com - GET /wp-content/plugins/rotr/load.swf?sid=28949&ref=http://valerierobinson.com/?p=1
* 03:26:59 UTC - 192.168.204.162:49622 - 188.40.79.151:80 - 38hartrobertsroad.com - GET /wp-content/plugins/rotr/load.swf?sid=66025&ref=http://valerierobinson.com/?p=1
* 03:26:59 UTC - 192.168.204.162:49625 - 62.76.177.211:80 - 62.76.177.211 - GET /sleev/?10
* 03:26:59 UTC - 192.168.204.162:49626 - 62.76.177.211:80 - 62.76.177.211 - GET /sleev/?10
* 03:27:00 UTC - 192.168.204.162:49627 - 31.22.4.108:80 - 30oct2007.com - GET /wp-content/rotr/
* 03:27:00 UTC - 192.168.204.162:49628 - 31.22.4.108:80 - 30oct2007.com - GET /wp-content/rotr/
* 03:27:01 UTC - 192.168.204.162:49629 - 212.83.135.167:8000 - eesheshi.ontowess.com:8000 - GET /fdoufeipqrxkf?zxchqtevykm=2404448
* 03:27:01 UTC - 192.168.204.162:49630 - 212.83.135.167:8000 - eesheshi.ontowess.com:8000 - GET /fjiqivykkrno?zpowtxqkxm=2404448
* 03:27:01 UTC - 192.168.204.162:49629 - 212.83.135.167:8000 - eesheshi.ontowess.com:8000 - GET /ilmcdsiekgu.js
* 03:27:02 UTC - 192.168.204.162:49629 - 212.83.135.167:8000 - eesheshi.ontowess.com:8000 - GET /bfduw
* 03:27:02 UTC - 192.168.204.162:49630 - 212.83.135.167:8000 - eesheshi.ontowess.com:8000 - GET /bspxisnw
* 03:27:07 UTC - 192.168.204.162:49630 - 212.83.135.167:8000 - eesheshi.ontowess.com:8000 - POST /sgphmsawu
* 03:27:23 UTC - 192.168.204.162:49631 - 212.83.135.167:8000 - eesheshi.ontowess.com:8000 - GET /dqjndypi?hlbszwbqmocs=gltiywtx
* 03:27:23 UTC - 192.168.204.162:49631 - 212.83.135.167:8000 - eesheshi.ontowess.com:8000 - GET /META-INF/services/javax.xml.datatype.DatatypeFactory
* 03:27:24 UTC - 192.168.204.162:49631 - 212.83.135.167:8000 - eesheshi.ontowess.com:8000 - GET /kkmohtafl?hnvhxikvyt=gltiywtx

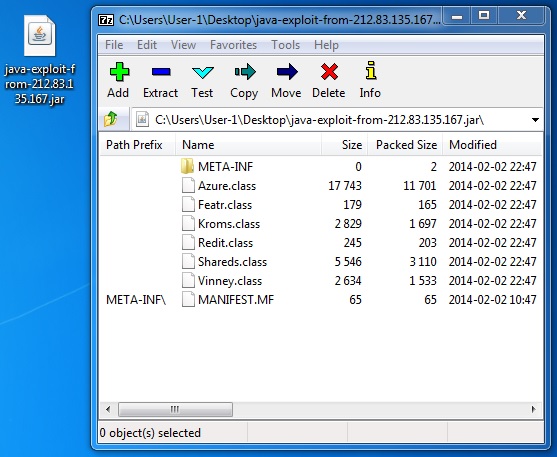
POST INFECTION CALLBACK TRAFFIC

* 03:27:27 UTC - 192.168.204.162:49632 - 89.191.150.230:80 - www.gminalubiewo.pl - POST /images/files/file.php
* 03:27:27 UTC - 192.168.204.162:49633 - 89.191.150.230:80 - www.gminalubiewo.pl - POST /images/files/file.php
* 03:27:28 UTC - 192.168.204.162:49634 - 89.191.150.230:80 - www.gminalubiewo.pl - POST /images/files/file.php
* 03:27:57 UTC - 192.168.204.162:49638 - 118.69.206.95:80 - www.kimsa.vn - POST /images/redir/redir.php
* 03:27:58 UTC - 192.168.204.162:49639 - 118.69.206.95:80 - www.kimsa.vn - POST /images/redir/redir.php
* 03:27:59 UTC - 192.168.204.162:49641 - 89.191.150.230:80 - www.gminalubiewo.pl - POST /images/files/file.php
* 03:27:59 UTC - 192.168.204.162:49640 - 118.69.206.95:80 - www.kimsa.vn - POST /images/redir/redir.php
* 03:28:00 UTC - 192.168.204.162:49642 - 89.191.150.230:80 - www.gminalubiewo.pl - POST /images/files/file.php

**PRELIMINARY MALWARE ANALYSIS**

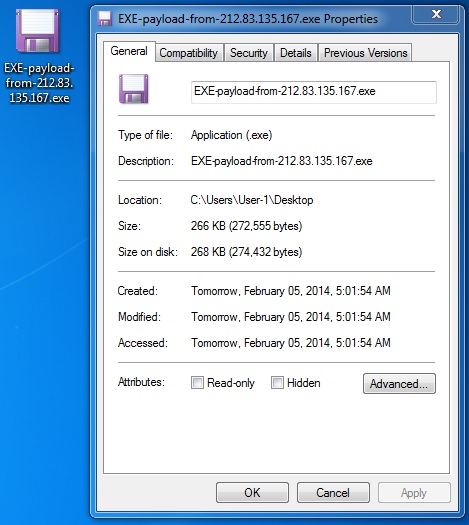
JAVA EXPLOIT

File name:  **java-exploit-from-212.83.135.167.jar**  
File size:  19.0 KB ( 19458 bytes )  
MD5 hash:  71cb847f10e45acf7d58ddef2ed43303  
Detection ratio:  1 / 51  
First submission:  2014-02-04 00:42:31 UTC  
VirusTotal link: <https://www.virustotal.com/en/file/5fac4c4670e9e8eac55974a3f366dbf57f675b624301a64b1707e047380b5cf1/analysis/>



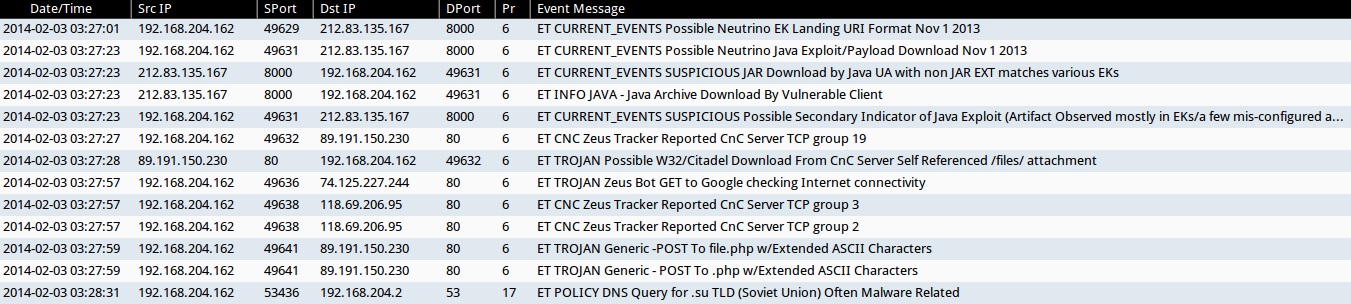
EXE PAYLOAD - came over the network XOR-ed with the ASCII string: **xvbb**

File name:  **EXE-payload-from-212.83.135.167.exe**  
File size:  266.2 KB ( 272555 bytes )  
MD5 hash:  9114cd6411e9164631d6953e290c3b45  
Detection ratio:  26 / 51  
First submission:  2014-02-05 05:04:01 UTC  
VirusTotal link: <https://www.virustotal.com/en/file/656b3886f4214bc986d68cd6bf753be2ad2acd8741176349c1335272caa765fa/analysis/>



**SNORT EVENTS**

SNORT EVENTS FOR NEUTRINO EK TRAFFIC (FROM [SECURITY ONION](http://code.google.com/p/security-onion/))



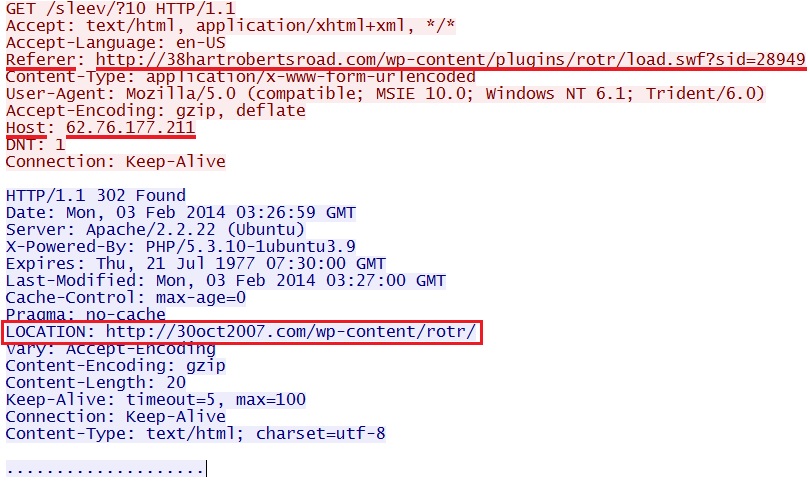
* ET CURRENT\_EVENTS Possible Neutrino EK Landing URI Format Nov 1 2013
* ET CURRENT\_EVENTS Possible Neutrino Java Exploit/Payload Download Nov 1 2013
* ET CURRENT\_EVENTS SUSPICIOUS JAR Download by Java UA with non JAR EXT matches various EKs
* ET INFO JAVA - Java Archive Download By Vulnerable Client
* ET CURRENT\_EVENTS SUSPICIOUS Possible Secondary Indicator of Java Exploit (Artifact Observed mostly in EKs/a few mis-configured apps)
* ET CNC Zeus Tracker Reported CnC Server TCP group 19
* ET TROJAN Possible W32/Citadel Download From CnC Server Self Referenced /files/ attachment
* ET TROJAN Zeus Bot GET to Google checking Internet connectivity
* ET CNC Zeus Tracker Reported CnC Server TCP group 3
* ET CNC Zeus Tracker Reported CnC Server TCP group 2
* ET TROJAN Generic -POST To file.php w/Extended ASCII Characters
* ET TROJAN Generic - POST To .php w/Extended ASCII Characters
* ET POLICY DNS Query for .su TLD (Soviet Union) Often Malware Related

**HIGHLIGHTS FROM THE TRAFFIC**

Embedded iframe in the infected web page - **www.valerierobinson.com/?p=1**



Part of the redirect chain - **62.76.177.211/sleev/?10**



Final redirect to the Neutrino EK domain - **30oct2007.com/wp-content/rotr/**



Neutrino EK domain delivering the Java exploit - **eesheshi.ontowess.com:8000/dqjndypi?hlbszwbqmocs=gltiywtx**



Neutrino EK domain delivering the EXE payload - **eesheshi.ontowess.com:8000/kkmohtafl?hnvhxikvyt=gltiywtx** - which is XOR-ed with the ASCII string: **xvbb**



Post-infection callback returns more malware which triggered event on possible Citadel download - **www.gminalubiewo.pl/images/files/file.php**

