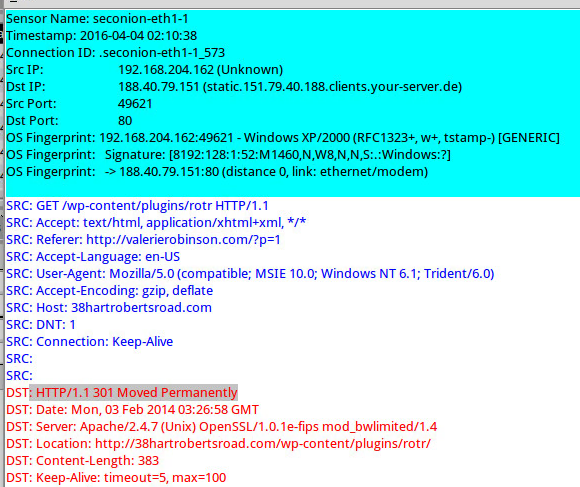
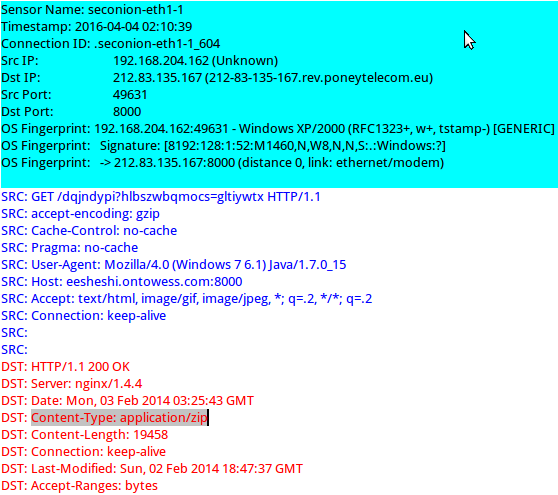
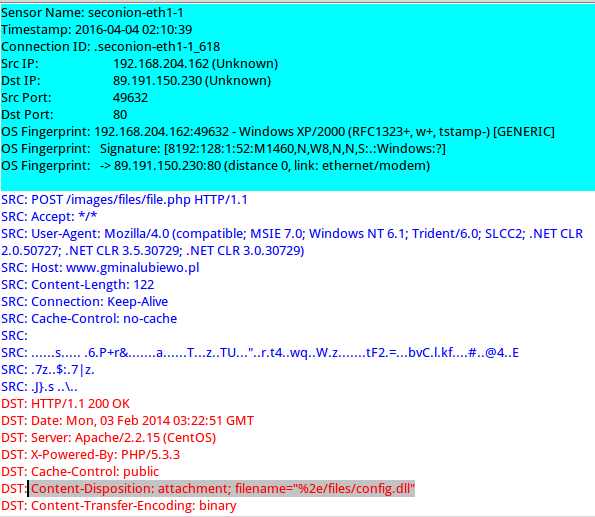
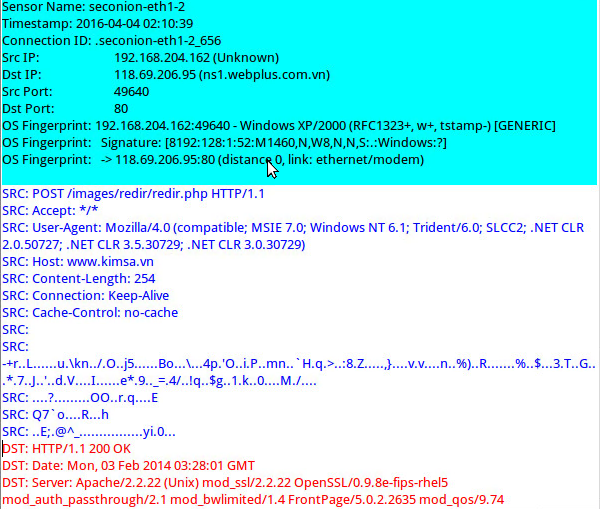
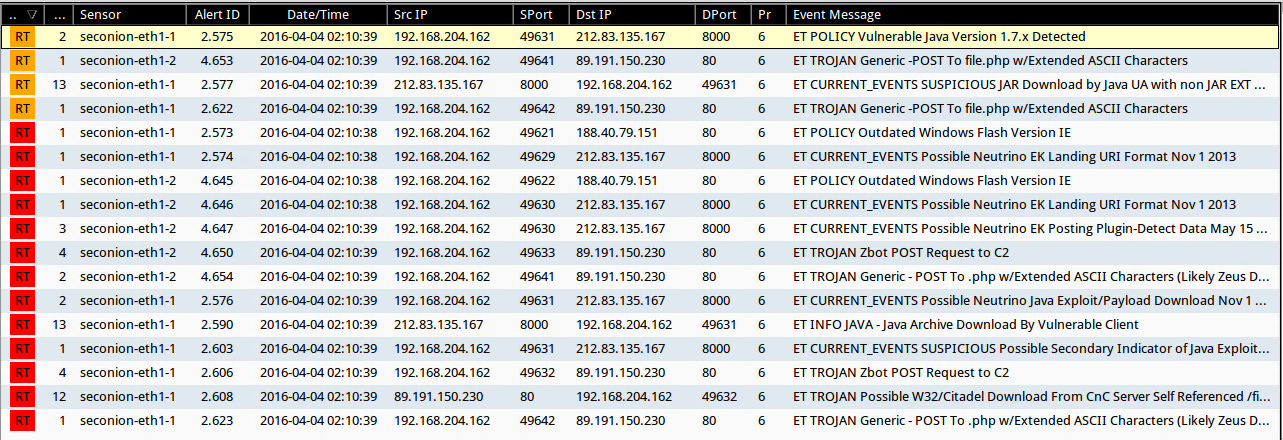
In this analysis, the victim host is 192.168.204.162 and the IPs from the attacker are 212.83.135.167, 89.191.150.230, 118.69.206.95 and 188.40.79.151.

* 188.40.79.151 - **38hartrobertsroad.com** - a redirect domain
* 212.83.135.167 - **eesheshi.ontowess.com** – an Exploit Kit domain over TCP port 8000
* 89.191.150.230 - **www.gminalubiewo.pl** - triggered Zeus/Zbot/Citadel events
* 118.69.206.95 - **www.kimsa.vn** - triggered Zeus/Zbot events

Here is the infection traffic in Sguil:



Infection traffic details:

1. **Event:** ET POLICY Vulnerable Java Version 1.7.x Detected

**Content:** Java/1.7.0\_ !99

**Explanation:** delivering the Java exploit

**GET /dqjndypi?hlbszwbqmocs=gltiywtx**

**Source IP:** 192.168.204.162 port 49631

**Destination IP:** 212.83.135.167 port 8000

**URL:** eesheshi.ontowess.com

1. **Event:** ET TROJAN Generic -POST To file.php w/Extended ASCII Characters

**Content:** POST /file.php !Referer:

**Explanation:** download a malware file which triggered event

**POST /images/files/file.php**

**Source IP:** 192.168.204.162 port 49641

**Destination IP:** 89.191.150.230 port 80

**URL:** [www.gminalubiewo.pl](http://www.gminalubiewo.pl)

1. **Event:** ET CURRENT\_EVENTS SUSPICIOUS JAR Download by Java UA with non JAR EXT matches various EKs

**Content:** !.jar PK .class

**Explanation:** delivering the Java exploit

**GET /dqjndypi?hlbszwbqmocs=gltiywtx**

**Source IP:** 192.168.204.162 port 49631

**Destination IP:** 212.83.135.167 port 8000

**URL:** eesheshi.ontowess.com

1. **Event:** ET POLUCY Outdated Windows Flash Version IE

**Content:** x-flash-version | 3a 20 | !18,0,0,333 | 0d 0a | !21,0,0,197 | 0d 0a | MSIE

**Explanation:** direct to another website

**GET /wp-content/plugins/rotr**

**Source IP:** 192.168.204.162 port 49621

**Destination IP:** 188.40.79.151 port 80

**URL:** 38hartrobertsroad.com

1. **Event:** ET CURRENT\_EVENTS Possible Neutrino EK Landing URI Format Nov 1 2013

**Content:** GET ? ; =

**Explanation:** the Java exploit landed on Nov 1 2013.

**GET /fdoufeipqrxkf?zxchqtevykm=2404448**

**GET /ilmcdsiekgu.js**

**Source IP:** 192.168.204.162 port 49629

**Destination IP:** 212.83.135.167 port 8000

**URL:** eesheshi.ontowess.com

1. **Event:** ET CURRENT\_EVENTS Possible Neutrino EK Posting Plugin-Detect Data May 15 2013

**Content:** POST XMLHttpRequest

**Explanation:** the Java exploit was post on May 15 2013.

**GET /fjiqivykkrno?zpowtxqkxm=2404448**

**GET /bspxisnw**

**POST /sgphmsawu**

**Source IP:** 192.168.204.162 port 49630

**Destination IP:** 212.83.135.167 port 8000

**URL:** eesheshi.ontowess.com

1. **Event:** ET TROJAN Zbot POST Request to C2

**Content:** POST .php HTTP/1. | 0D 0A | Accept | 3a | !Referer | 3a |

**Explanation:** the download malware file want to control the victim and it should be Zeus.

**POST /images/files/file.php**

**Source IP:** 192.168.204.162 port 49641

**Destination IP:** 89.191.150.230 port 80

**URL:** [www.gminalubiewo.pl](http://www.gminalubiewo.pl)

1. **Event:** ET TROJAN Generic -POST To file.php w/Extended ASCII Characters (Likely Zeus Derivative)

**Content:** POST .php !Referer | 3a | Content-Type | 3a | MSIE

**Explanation:** the download malware file should be Zeus deriavative.

**POST /images/redir/redir.php**

**Source IP:** 192.168.204.162 port 49641

**Destination IP:** 118.69.206.95 port 80

**URL:** www.kimsa.vn

1. **Event:** ET INFO JAVA - Java Archive Download By Vulnerable Client

**Content:** | 0D 0A 0D 0A | PK PK

**Explanation:** delivering the Java exploit

**GET /dqjndypi?hlbszwbqmocs=gltiywtx**

**GET /META-INF/services/javax.xml.datatype.DatatypeFactory**

**GET /kkmohtafl?hnvhxikvyt=gltiywtx**

**Source IP:** 192.168.204.162 port 49630

**Destination IP:** 212.83.135.167 port 8000

**URL:** eesheshi.ontowess.com

1. **Event:** ET CURRENT\_EVENTS SUSPICIOUS Possible Secondary Indicator of Java Exploit (Artifact Observed mostly in EKs/a few mis-configured apps)

**Content:** /java.xml.datatype.DatatypeFactory Java/1.

**Explanation:**

**GET /dqjndypi?hlbszwbqmocs=gltiywtx**

**GET /META-INF/services/javax.xml.datatype.DatatypeFactory**

**GET /kkmohtafl?hnvhxikvyt=gltiywtx**

**Source IP:** 192.168.204.162 port 49631

**Destination IP:** 212.83.135.167 port 8000

**URL:** eesheshi.ontowess.com

1. **Event:** ET TROJAN Possible W32/Citadel Download From CnC Server Self Referenced /files/ attachment

**Content:** filename= | 22 | %2e/files/

**Explanation:** it shows the file.php is downloaded.

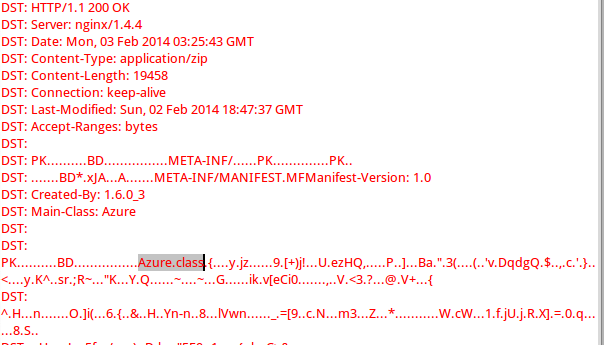
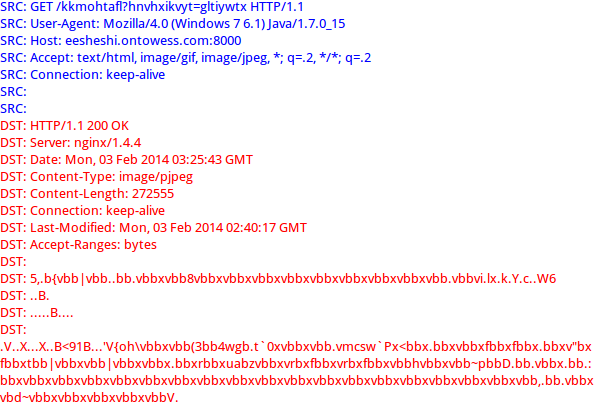
**POST /images/files/file.php**

**Source IP:** 192.168.204.162 port 49632

**Destination IP:** 89.191.150.230 port 80

**URL:** [www.gminalubiewo.pl](http://www.gminalubiewo.pl)

There are three downloaded files. One is a zip file, some kind of Exploit Kit. This EK is from 212.83.135.167 port 8000(eesheshi.ontowess.com). Its function is to load a Exploit Kit. The webpage, eesheshi.ontowess.com:8000/dqjndypi?hlbszwbqmocs=gltiywtx delivers the Java exploit kit. The webpage, eesheshi.ontowess.com:8000/kkmohtafl?hnvhxikvyt=gltiywtx delivers its EXE payload.

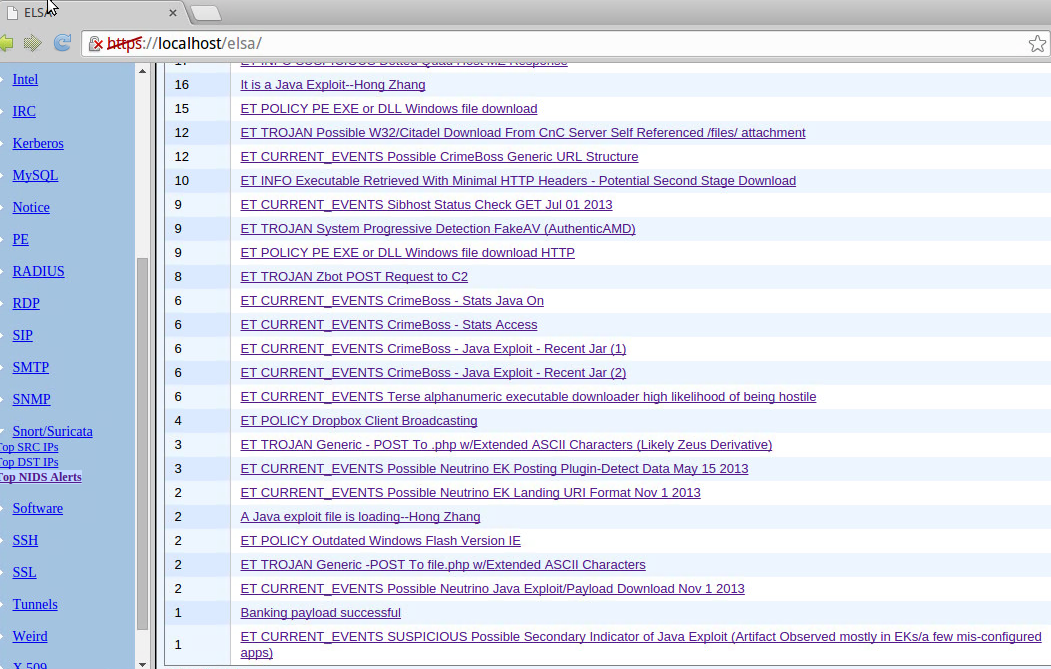
 

The second file is file.php which attaches a dll file, config.dll. It is downloaded from 89.191.150.230 port 80 (www.gminalubiewo.pl). Its functions is to trigger Zeus/Zbot/Citadel events.

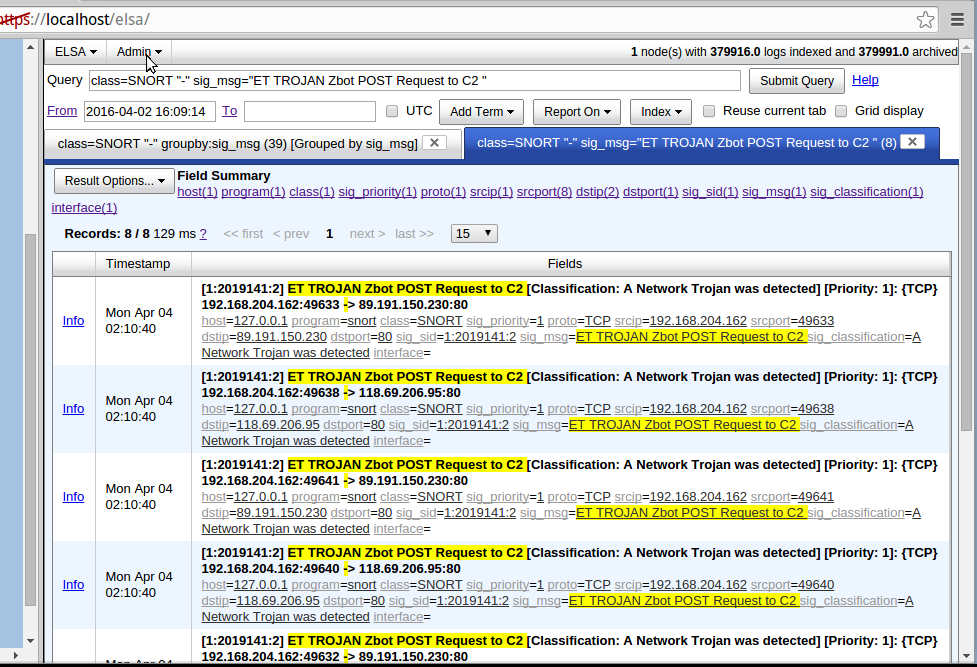
The third file is redir.php.It is downloaded from 118.69.206.95 port 80 (www.kimsa.vn). Its functions is to trigger Zeus/Zbot events.

The “PK”, “.class” and “.php” in the content of the packet will cause to fire. There are six events, “ET TROJAN Generic -POST To file.php w/Extended ASCII Characters”, “ET CURRENT\_EVENTS SUSPICIOUS JAR Download by Java UA with non JAR EXT matches various EKs”, “ET TROJAN Zbot POST Request to C2”, “ET TROJAN Generic -POST To file.php w/Extended ASCII Characters (Likely Zeus Derivative)”, “ET INFO JAVA - Java Archive Download By Vulnerable Client” and “ET TROJAN Possible W32/Citadel Download From CnC Server Self Referenced /files/ attachment” contain these contents. Hence, these six events are the main malicious snort rules/events that fired based on traffic or downloads.

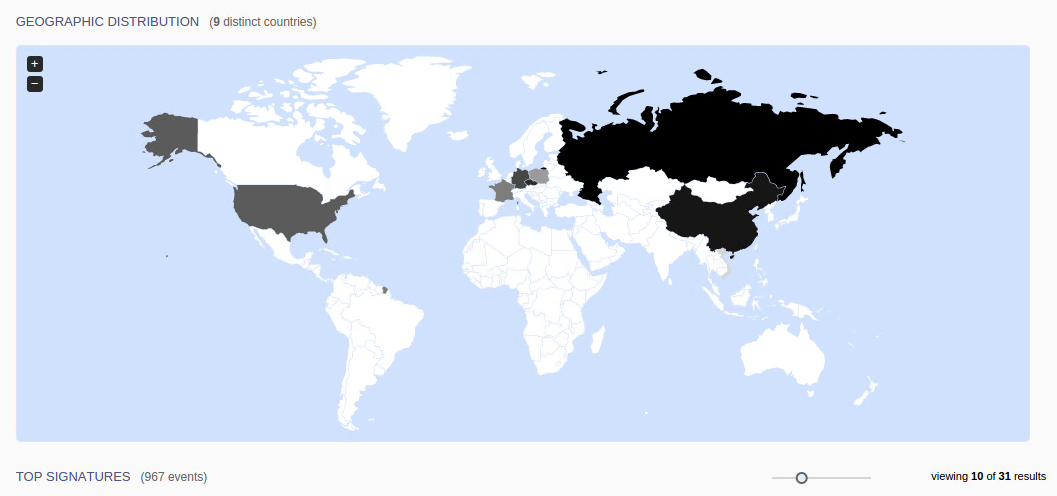
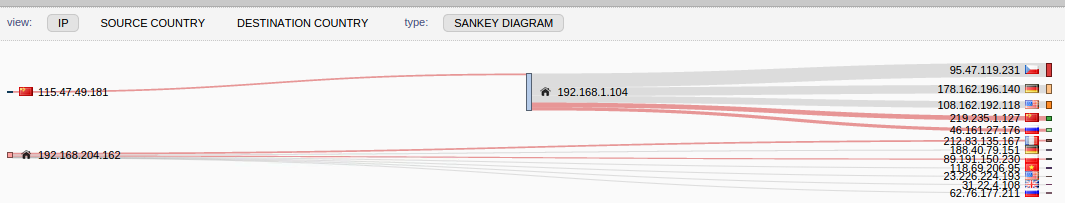
Here is a screenshot from ELSA. It shows all infected events.



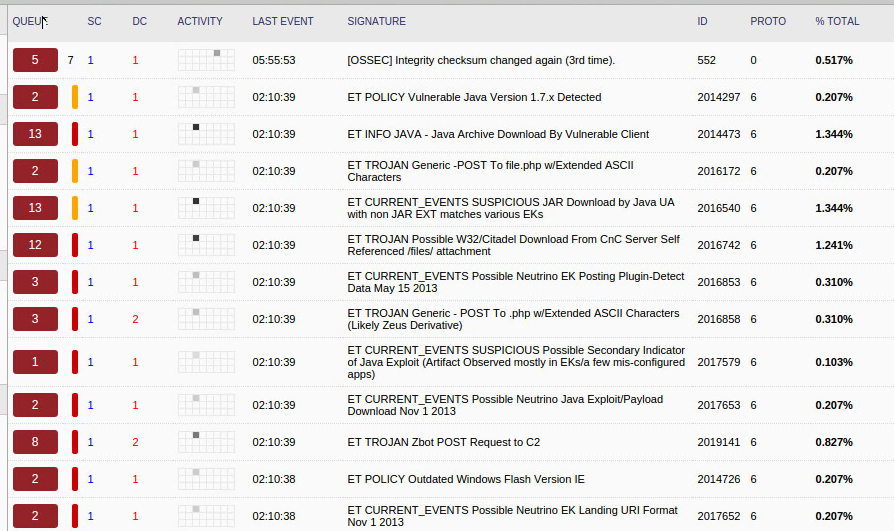
When I click the event of “ET TROJAN Zbot POST Request to C2” and it shows more details about this event.



Here is the screenshot form Squert. It shows the geographic distribution.

Here is another sceernshot. it shows the top dangerous events.



Here is the screenshot from Snorby.

