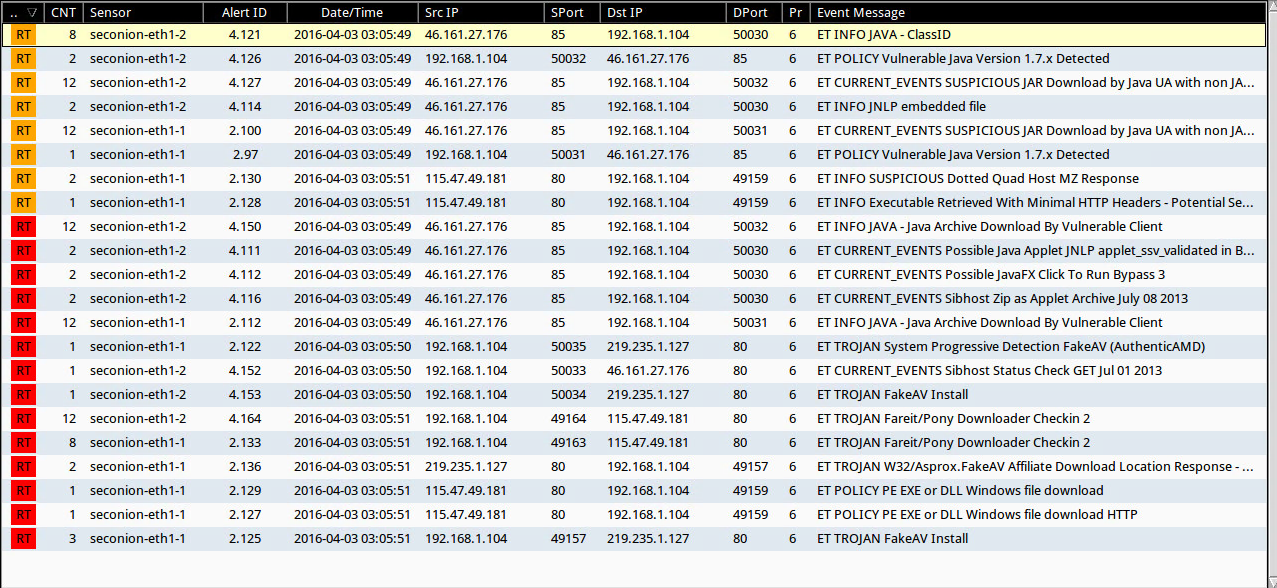
In this analysis, the victim host is 192.168.1.104 and the IPs from the attacker are 46.161.27.176, 219.235.1.127 and 115.47.49.181.

Here is the infection traffic in Sguil:



Infection traffic details:

1. **Event:** ET INFO JAVA – ClassID

**Content:** 8AD9C840-044E-11D1-B3E9-00805F499D93

**Explanation:** This is a Java classid. Internet Explorer can use the classid attribute OBJECT tag to load Java. This classid calls the latest installed version of Java Plug-in installed on the machine and tell the attacker the Java version.

**GET /MJ8BBSp4D3uZDSmbE91prhIGA4FmI6bVPLtYhYn5GFiSMda**

**Source IP:** 46.161.27.126 port 85

**URL:** http://robertsontrainingsystems.com/forum/showthread.php?95-Lumbar-Flexion-when-squatting

**Destination IP:** 192.168.1.104 port 50030

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

**Content:** Java/1.7.0\_

**Explanation:** the attacker get the java version and try to send a zip file.

**GET /MJ8BBSp4D3uZDSmbE91prhIGA4FmI6bVPLtYhYn5GFiSMda2.zip**

**Source IP:** 192.168.1.104 port 50032

**Destination IP:** 46.161.27.176 port 85

**URL:** bewarecommadelimited.org

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

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

**Explanation:** it shows JAR (MJ8BBSp4D3uZDSmbE91prhIGA4FmI6bVPLtYhYn5GFiSMda2.zip) is loaded and stored on the exploit site.

**GET /MJ8BBSp4D3uZDSmbE91prhIGA4FmI6bVPLtYhYn5GFiSMda2.zip**

**Source IP:** 46.161.27.176 port 85

**Destination IP:** 192.168.1.104 port 50032

**URL:** bewarecommadelimited.org

1. **Event:** ET INFO JNLP embedded file

**Content:** jnlp PD94bWwgdmVyc2lvbj0

**Explanation:** the attacker add a Java application, Java Network Launch Protocol (JNLP) which is used to deliver the malicious content.

**GET /MJ8BBSp4D3uZDSmbE91prhIGA4FmI6bVPLtYhYn5GFiSMda**

**Source IP:** 46.161.27.176 port 85

**Destination IP:** 192.168.1.104 port 50030

**URL:** http://robertsontrainingsystems.com/forum/showthread.php?95-Lumbar-Flexion-when-squatting

1. **Event:** ET INFO SUSPICIOUS Dotted Quad Host MZ Response

**Content:** MZ PE[00 00]

**Explanation:** it shows it is potentially bad traffic and the attacker is trying to send a file, qtcheck.exe.

**GET /qtcheck.exe?ts=6216d09f995d5e85c142f6378c611074365019c3&affid=76002**

**Source IP:** 115.47.49.181 port 80

**Destination IP:** 192.168.1.104 port 49159

1. **Event:** ET INFO Executable Retrieved With Minimal HTTP Headers - Potential Second Stage Download

**Content:** MZ PE[00 00]

**Explanation:** it shows it is potentially bad traffic and the victim is ready to download this file, qtcheck.exe.

**GET /qtcheck.exe?ts=6216d09f995d5e85c142f6378c611074365019c3&affid=76002**

**Source IP:** 115.47.49.181 port 80

**Destination IP:** 192.168.1.104 port 49159

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

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

**Explanation:** it shows the Archive file which will be downloaded is vulnerable.

**GET /MJ8BBSp4D3uZDSmbE91prhIGA4FmI6bVPLtYhYn5GFiSMda2.zip**

**Source IP:** 46.161.27.176 port 85

**Destination IP:** 192.168.1.104 port 50032

**URL:** bewarecommadelimited.org

1. **Event:** ET CURRENT\_EVENTS Possible Java Applet JNLP applet\_ssv\_validated in Base64

**Content:** X19hcHBsZXRfc3NZhbGlkYXRI

**Explanation:** it shows the JNLP uses the base-64 encoded configuration file.

**GET /MJ8BBSp4D3uZDSmbE91prhIGA4FmI6bVPLtYhYn5GFiSMda**

**Source IP:** 46.161.27.176 port 85

**Destination IP:** 192.168.1.104 port 50030

**URL:** bewarecommadelimited.org

1. **Event:** ET CURRENT\_EVENTS Possible JavaFX Click To Run Bypass 3

**Content:** ByZWxvYWRlci1jbGFzc

**Explanation:** it shows the downloaded file will run JNLP Bypass 3 through JavaFX.

**GET /MJ8BBSp4D3uZDSmbE91prhIGA4FmI6bVPLtYhYn5GFiSMda**

**Source IP:** 46.161.27.176 port 85

**Destination IP:** 192.168.1.104 port 50030

**URL:** bewarecommadelimited.org

1. **Event:** ET CURRENT\_EVENTS Sibhost Zip as Applet Archive July 08 2013

**Content:** jquery.js archive

**Explanation:** it shows the malware is Sibhost Toolkit and the downloaded file will use jquery.js.

**GET /MJ8BBSp4D3uZDSmbE91prhIGA4FmI6bVPLtYhYn5GFiSMda**

**Source IP:** 46.161.27.176 port 85

**Destination IP:** 192.168.1.104 port 50030

**URL:** bewarecommadelimited.org

1. **Event:** ET TROJAN System Progressive Detection FakeAV (AuthenticAMD)

**Content:** ts= affid= AuthenticAMD | 3b |

**Explanation:** it shows the malware is using FakeAV.

**GET /api/dom/no\_respond/?ts=6216d09f995d5e85c142f6378c611074365019c3&token=sysdocx1&group=asp&nid=25AC56D0&lid=0057&ver=0057&affid=76002&dx=0**

**Source IP:** 192.168.1.104 port 50035

**Destination IP:** 219.235.1.127 port 80

**URL:** bewarecommadelimited.org

1. **Event:** ET CURRENT\_EVENTS Sibhost Check GET Jul 01 2013

**Content:** GET | 29 20 |Java/1

**Explanation:** it shows the malware is Sibhost Toolkit and the version is Jul 01 2013.

**GET /MJ8BBSp4D3uZDSmbE91prhIGA4FmI6bVPLtYhYn5GFiSMda?id=2&text=899**

**Source IP:** 192.168.1.104 port 50033

**Destination IP:** 46.161.27.176 port 80

**URL:** bewarecommadelimited.org

1. **Event**: ET TROJAN Fareit/Pony Downloader Checkin 2

**Content:** POST | 0d 0a | Content-Encoding | 3a | binary | 0d 0a | MSIE !Referer | 3a 20 | HTTP/1.0 | 0d 0a |

**Explanation:** check the downloaded file, k3JRL75YXw.php.

**POST /twXEsyUTli71/k3JRL75YXw.php**

**Source IP:** 192.168.1.104 port 50034

**Destination IP:** 115.47.49.181 port 80

1. **Event**: ET TROJAN W32/Asprox.FakeAV Affiliate Download Location Response - Likely Pay-Per-Install For W32/Papras.Spy or W32/ZeroAccess

**Content:** http | 3A | // .exe?ts= &affid=

**Explanation:** event want to check this malware is Papras.Spy or ZeroAccess.

**GET /api/stats/debug/2/?ts=6216d09f995d5e85c142f6378c611074365019c3&token=sysdocx1&group=asp&nid=25AC56D0&lid=0057&ver=0057&affid=76002**

**Source IP:** 219.235.1.127 port 80

**Destination IP:** 192.168.1.104 port 50034

1. **Event**: ET POLICY PE EXE or DLL Windows file download

**Content:** MZ PE | 00 00|

**Explanation:**

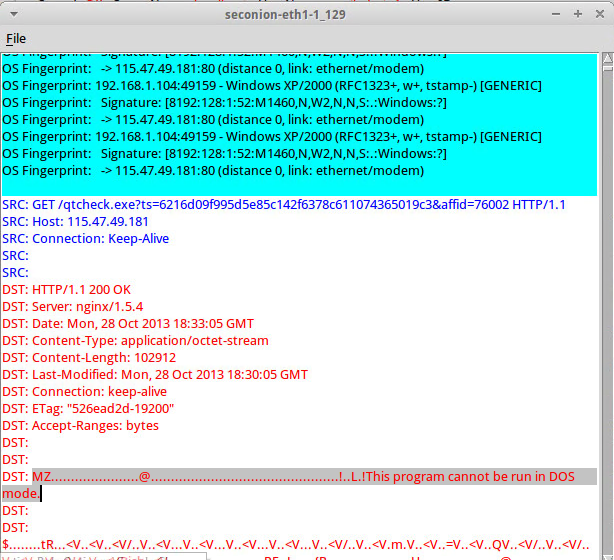
**GET /qtcheck.exe?ts=6216d09f995d5e85c142f6378c611074365019c3&affid=76002**

**Source IP:** 115.47.49.181 port 80

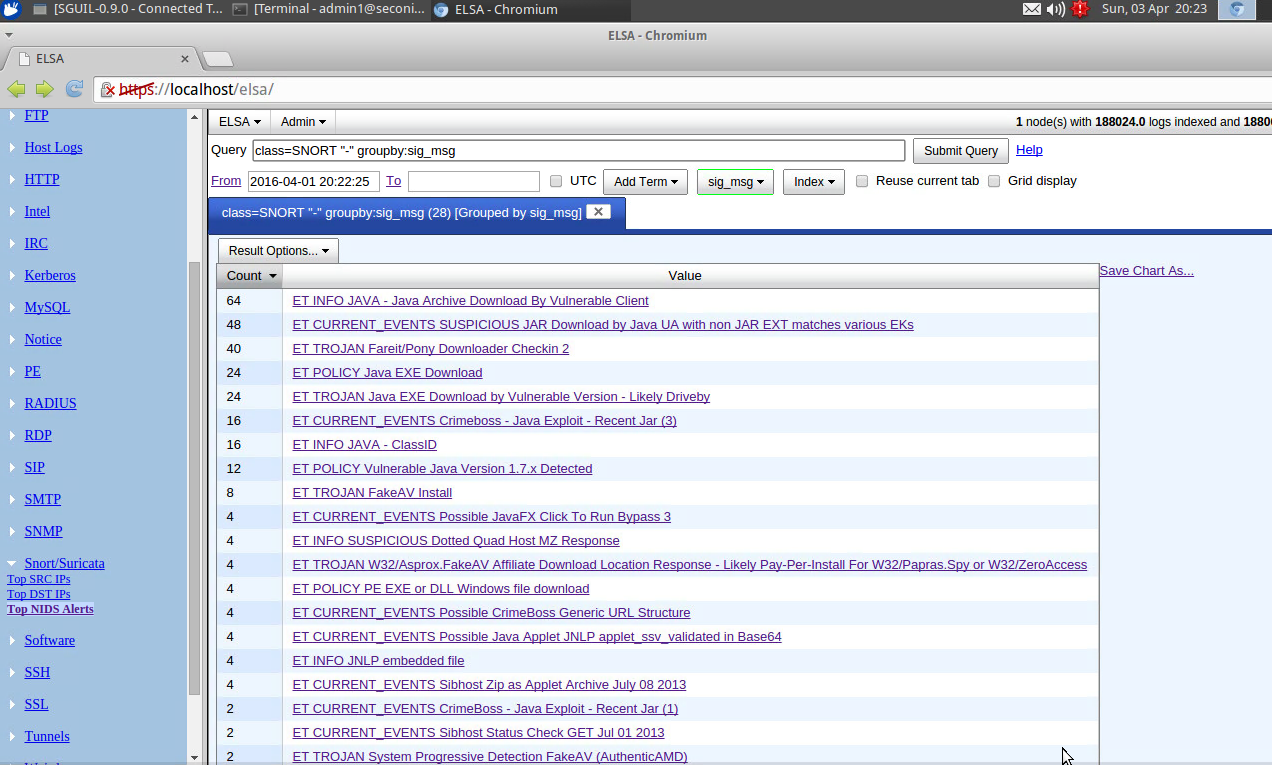
**Destination IP:** 192.168.1.104 port 49159

There are two downloaded files. One is MJ8BBSp4D3uZDSmbE91prhIGA4FmI6bVPLtYhYn5GFiSMda2.zip, a zip file of malware. This file is from 46.161.27.176 port 85 (bewarecommadelimited.org). Its function is to install a FakeAV. The second file is qtcheck.exe, a malicious EXE. It is downloaded from 115.47.49.181 port 80 (no domain name). Its functions is to steal the victim’s password.

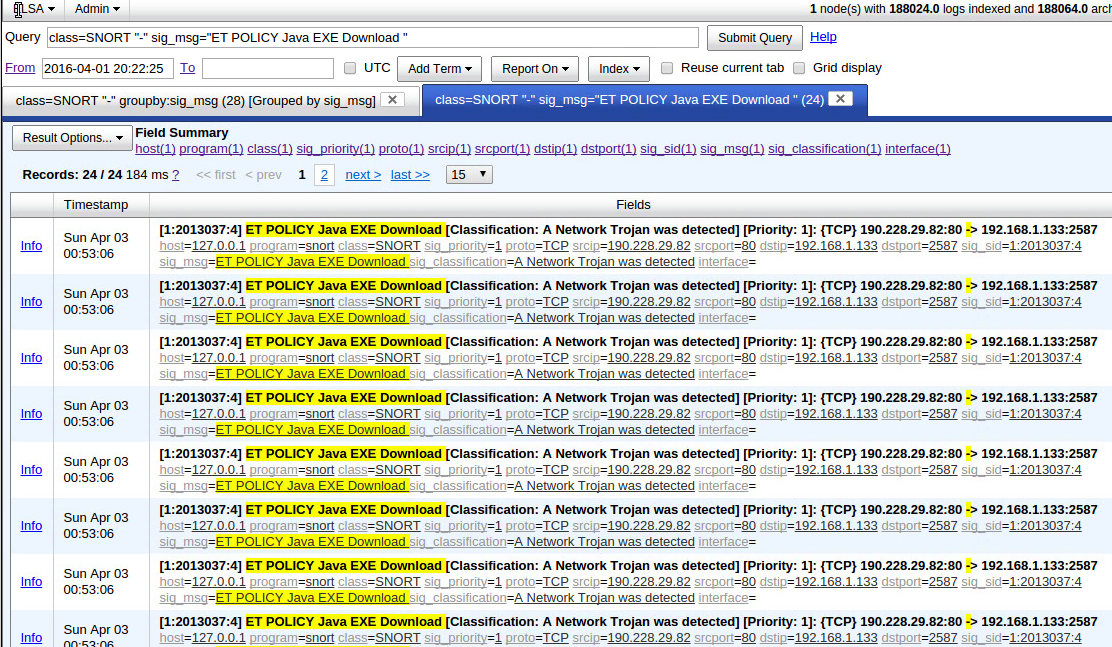
As we learned in the class, the “MZ” and “PE” in the content of the packet will cause to fire as a Windows EXE. There are three events, “ET INFO SUSPICIOUS Dotted Quad Host MZ Response”, “ET INFO Executable Retrieved With Minimal HTTP Headers - Potential Second Stage Download”, “ET POLICY PE EXE or DLL Windows file download” contain the content of “MZ” and “PE.” Hence, these three events are the main malicious snort rules/events that fired based on traffic or downloads.



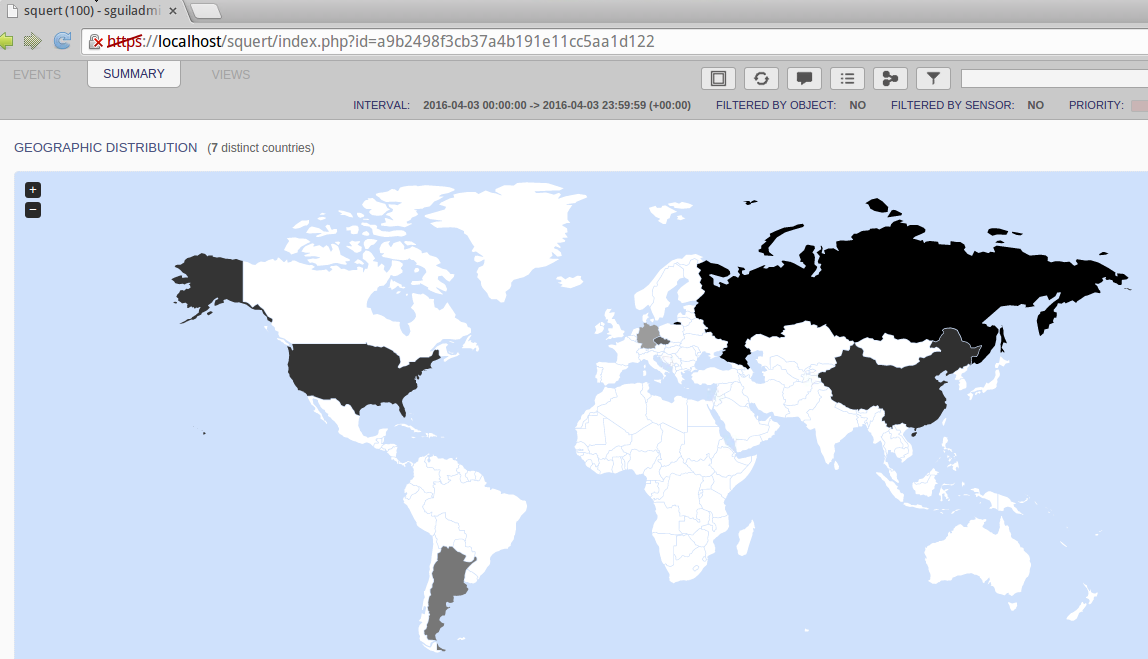
Here is a screenshot from ELSA. It shows all infected events.



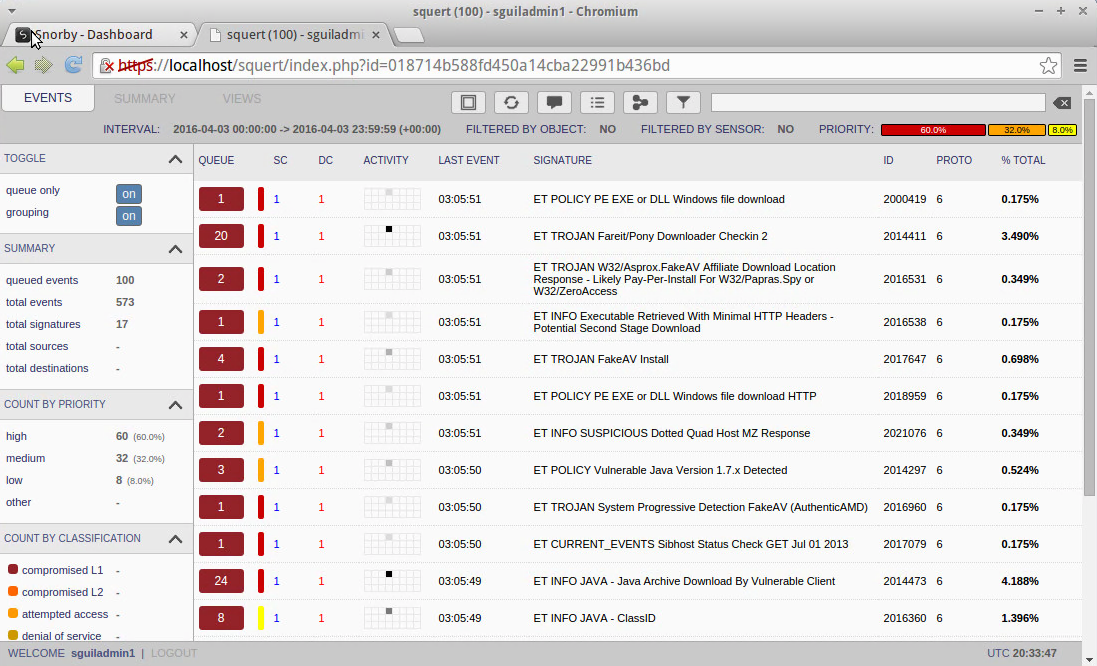
When I click the event of “ET POLICY Java EXE Download” and it shows more details about this event.



Here is the screenshot form Squert. It shows the geographic distribution which include China, Russia, America, Czech, German, Brazil and Argentina.



Here is another sceernshot. it shows the top dangerous event is “ET POLICY PE EXE or DLL Windows file download” which fire the exe.



Here is the screenshot from Snorby.

