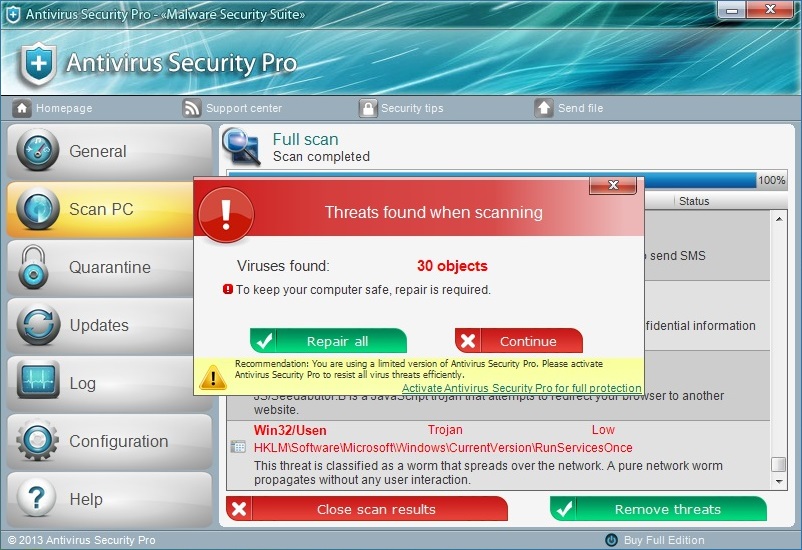
[](http://www.malware-traffic-analysis.net/index.html)

**2013-10-28 - FAKE ANTI-VIRUS AND PASSWORD STEALER**

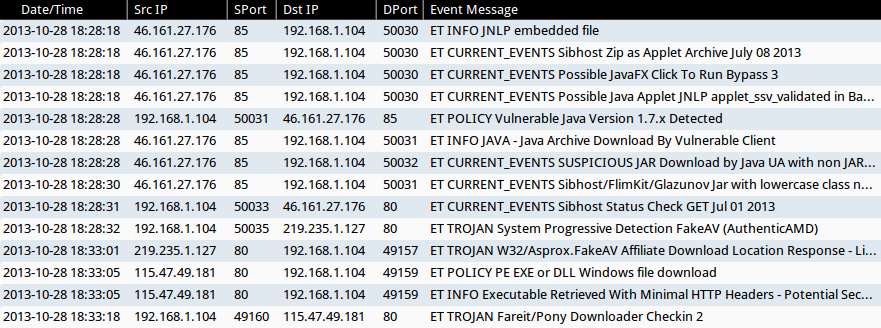
At this point, I've investigated several dozen infections, whether it's been at work or in my home lab.  In almost every case, the malware involved a **.JAR** file (Java exploit) followed a malicious **.EXE** for the initial infection.  However, this time the Java exploit and malicious binary were delivered together in a single **.ZIP** file.  The end result was an infected computer with a fake anti-virus and a Fareit password stealer.

  
*The fake anti-virus program, Antivirus Security Pro...  The Fareit password stealer is working behind the scenes.*

Let's look at the IDS events and chain of infection...

**SNORT EVENTS**

The compromised web page that kicked off the infection chain was a forum post on **robertsontrainingsystems.com**.  I used [Security Onion](http://code.google.com/p/security-onion/) to monitor a vulnerable Windows desktop running Java 7 update 17.  The infection traffic generated the following events in Sguil (all times GMT):



* 18:28:18 - 46.161.27.176 port 85 - 192.168.1.104 port 50030 - ET INFO JNLP embedded file
* 18:28:18 - 46.161.27.176 port 85 - 192.168.1.104 port 50030 - ET CURRENT\_EVENTS Sibhost Zip as Applet Archive July 08 2013
* 18:28:18 - 46.161.27.176 port 85 - 192.168.1.104 port 50030 - ET CURRENT\_EVENTS Possible JavaFX Click To Run Bypass 3
* 18:28:18 - 46.161.27.176 port 85 - 192.168.1.104 port 50030 - ET CURRENT\_EVENTS Possible Java Applet JNLP applet\_ssv\_validated in Base64
* 18:28:28 - 192.168.1.104 port 50031 - 46.161.27.176 port 85 - ET POLICY Vulnerable Java Version 1.7.x Detected
* 18:28:28 - 46.161.27.176 port 85 - 192.168.1.104 port 50031 - ET INFO JAVA - Java Archive Download By Vulnerable Client
* 18:28:28 - 46.161.27.176 port 85 - 192.168.1.104 port 50032 - ET CURRENT\_EVENTS SUSPICIOUS JAR Download by Java UA with non JAR EXT matches various EKs
* 18:28:30 - 46.161.27.176 port 85 - 192.168.1.104 port 50031 - ET CURRENT\_EVENTS Sibhost/FlimKit/Glazunov Jar with lowercase class names
* 18:28:31 - 192.168.1.104 port 50033 - 46.161.27.176 port 80 - ET CURRENT\_EVENTS Sibhost Status Check GET Jul 01 2013
* 18:28:32 - 192.168.1.104 port 50035 - 219.235.1.127 port 80 - ET TROJAN System Progressive Detection FakeAV (AuthenticAMD)
* 18:33:01 - 219.235.1.127 port 80 - 192.168.1.104 port 49157 - ET TROJAN W32/Asprox.FakeAV Affiliate Download Location Response - Likely Pay-Per-Install For W32/Papras.Spy or W32/ZeroAccess
* 18:33:05 - 115.47.49.181 port 80 - 192.168.1.104 port 49159 - ET POLICY PE EXE or DLL Windows file download
* 18:33:05 - 115.47.49.181 port 80 - 192.168.1.104 port 49159 - ET INFO Executable Retrieved With Minimal HTTP Headers - Potential Second Stage Download
* 18:33:18 - 192.168.1.104 port 49160 - 115.47.49.181 port 80 - ET TROJAN Fareit/Pony Downloader Checkin 2

**INFECTION CHAIN OF EVENTS**

INITIAL INFECTION CHAIN (times below in CDT)

* 13:28:17 - 192.168.1.104 port 50023 - 108.162.192.118 port 80 (robertsontrainingsystems.com) - GET /forum/showthread.php?95-Lumbar-Flexion-when-squatting
* 13:28:18 - 192.168.1.104 port 50030 - 46.161.27.176 port 85 (bewarecommadelimited.org) - GET /MJ8BBSp4D3uZDSmbE91prhIGA4FmI6bVPLtYhYn5GFiSMda
* 13:28:18 - 192.168.1.104 port 50030 - 46.161.27.176 port 85 (bewarecommadelimited.org) - GET /jquery.js
* 13:28:28 - 192.168.1.104 port 50031 - 46.161.27.176 port 85 (bewarecommadelimited.org) GET /MJ8BBSp4D3uZDSmbE91prhIGA4FmI6bVPLtYhYn5GFiSMda2.zip  *[ZIP file of malware, requested twice]*

POST INFECTION CALLBACK TRAFFIC

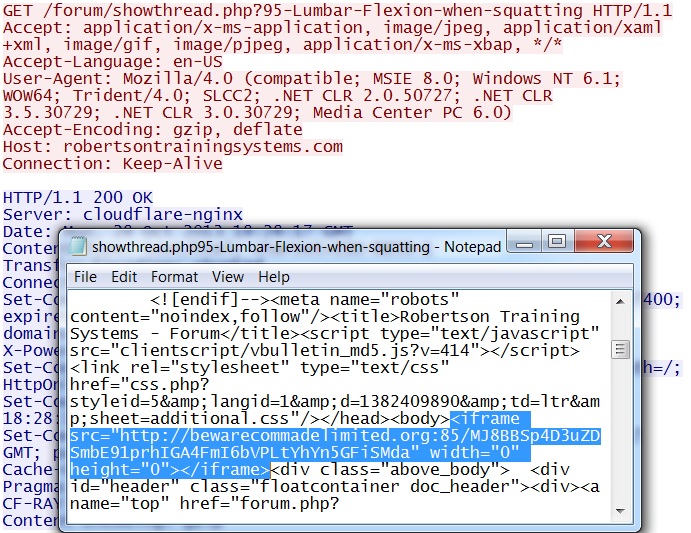
* 13:28:31 - 192.168.1.104 port 50033 - 46.161.27.176 port 80 (bewarecommadelimited.org) - GET /MJ8BBSp4D3uZDSmbE91prhIGA4FmI6bVPLtYhYn5GFiSMda?id=2&text=899
* 13:28:32 - 192.168.1.104 port 50034 - 219.235.1.127 port 80 (219.235.1.127) - GET /api/stats/debug/1/?ts=6216d09f995d5e85c142f6378c611074365019c3&token=sysdocx1&group=asp&nid=25AC56D0&lid=0057&ver=0057&affid=76002
* 13:28:32 - 192.168.1.104 port 50035 - 219.235.1.127 port 80 (219.235.1.127) - GET /api/dom/no\_respond/?ts=6216d09f995d5e85c142f6378c611074365019c3&token=sysdocx1&group=asp&nid=25AC56D0&lid=0057&ver=0057&affid=76002&dx=0
* 13:32:58 - 192.168.1.104 port 49157 - 219.235.1.127 port 80 (219.235.1.127) - GET /api/stats/debug/2/?ts=6216d09f995d5e85c142f6378c611074365019c3&token=sysdocx1&group=asp&nid=25AC56D0&lid=0057&ver=0057&affid=76002
* 13:33:00 - 192.168.1.104 port 49157 - 219.235.1.127 port 80 (219.235.1.127) - GET /api/urls/?ts=6216d09f995d5e85c142f6378c611074365019c3&affid=76002  *[repeated later]*
* 13:33:02 - 192.168.1.104 port 49157 - 219.235.1.127 port 80 (219.235.1.127) - GET /api/stats/debug/3/?ts=6216d09f995d5e85c142f6378c611074365019c3&token=sysdocx1&group=asp&nid=25AC56D0&lid=0057&ver=0057&affid=76002
* 13:33:05 - 192.168.1.104 port 49159 - 115.47.49.181 port 80 (115.47.49.181) - GET /qtcheck.exe?ts=6216d09f995d5e85c142f6378c611074365019c3&affid=76002  *[Second malicious EXE, the Fareit password stealer]*
* 13:33:18 - 192.168.1.104 port 49160 - 115.47.49.181 port 80 (115.47.49.181) - POST /twXEsyUTli71/k3JRL75YXw.php  *[repeated several times]*
* 13:34:13 - 192.168.1.104 port 49165 - 219.235.1.127 port 80 (219.235.1.127) - GET /api/stats/debug/4/?ts=6216d09f995d5e85c142f6378c611074365019c3&token=sysdocx1&group=asp&nid=25AC56D0&lid=0057&ver=0057&affid=76002

**INFECTION TRAFFIC DETAILS**

**GET /forum/showthread.php?95-Lumbar-Flexion-when-squatting**  
IP address: **108.162.192.118 port 80**  
domain name: **robertsontrainingsystems.com**

Sguil events: None

Screenshot of traffic:

  
*There's a hidden iframe right after the body of the HTML file.*

**GET /MJ8BBSp4D3uZDSmbE91prhIGA4FmI6bVPLtYhYn5GFiSMda**  
IP address: **46.161.27.176 port 85**  
domain name: **bewarecommadelimited.org**

Sguil events:

* **ET INFO JNLP embedded file**
* **ET CURRENT\_EVENTS Sibhost Zip as Applet Archive July 08 2013**
* **ET CURRENT\_EVENTS Possible JavaFX Click To Run Bypass 3**
* **ET CURRENT\_EVENTS Possible Java Applet JNLP applet\_ssv\_validated in Base64**

Screenshot of traffic:



**GET /MJ8BBSp4D3uZDSmbE91prhIGA4FmI6bVPLtYhYn5GFiSMda2.zip**  
IP address: **46.161.27.176 port 85**  
domain name: **bewarecommadelimited.org**

Sguil events:

* **ET POLICY Vulnerable Java Version 1.7.x Detected**
* **ET INFO JAVA - Java Archive Download By Vulnerable Client**
* **ET CURRENT\_EVENTS Sibhost/FlimKit/Glazunov Jar with lowercase class names**
* **ET CURRENT\_EVENTS SUSPICIOUS JAR Download by Java UA with non JAR EXT matches various EKs**

Screenshot of traffic:

  
*In this case, the java exploit and malicious binary (the fake anti-virus) are packaged in a single ZIP file.*

**GET /MJ8BBSp4D3uZDSmbE91prhIGA4FmI6bVPLtYhYn5GFiSMda?id=2&text=899**  
IP address: **46.161.27.176 port 80**  
domain name: **bewarecommadelimited.org**

Sguil event:

* **ET CURRENT\_EVENTS Sibhost Status Check GET Jul 01 2013**

Screenshot of traffic:

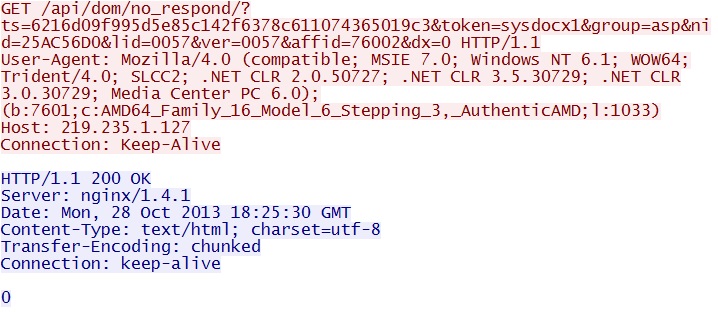
  
*This is the infected host reporting that it got the malware.*

**GET /api/dom/no\_respond/?ts=6216d09f995d5e85c142f6378c611074365019c3&token=sysdocx1&group=asp&nid=25AC56D0&lid=0057&ver=0057&affid=76002&dx=0**  
IP address: **219.235.1.127 port 80**  
domain name: none

Sguil event:

* **ET TROJAN System Progressive Detection FakeAV (AuthenticAMD)**

Screenshot of traffic:

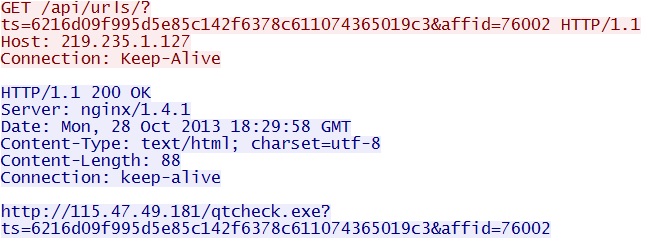


**GET /api/urls/?ts=6216d09f995d5e85c142f6378c611074365019c3&affid=76002**  
IP address: **219.235.1.127 port 80**  
domain name: none

Sguil event:

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

Screenshot of traffic:

  
*The response sets up the next HTTP GET request shown below...*

**GET /qtcheck.exe?ts=6216d09f995d5e85c142f6378c611074365019c3&affid=76002**  
IP address: **115.47.49.181 port 80**  
domain name: none

Sguil events:

* **ET POLICY PE EXE or DLL Windows file download**
* **ET INFO Executable Retrieved With Minimal HTTP Headers - Potential Second Stage Download**

Screenshot of traffic:

  
*Here, the infected computer downloads a second piece of malware, the Fareit password stealer.*

**POST /twXEsyUTli71/k3JRL75YXw.php**  
IP address: **115.47.49.181 port 80**  
domain name: none

Sguil event:

* **ET TROJAN Fareit/Pony Downloader Checkin 2**

Screenshot of traffic:

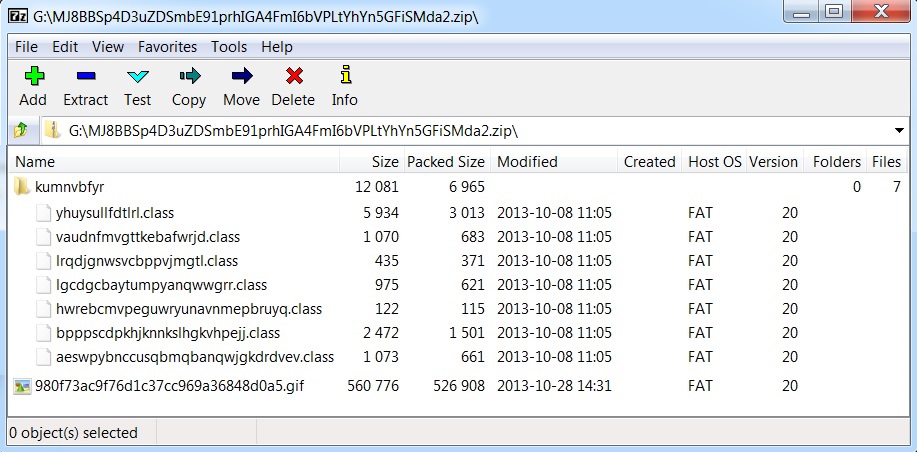
  
*The second piece of malware is calling back, but not getting a response.*

**PRELIMINARY MALWARE ANALYSIS**

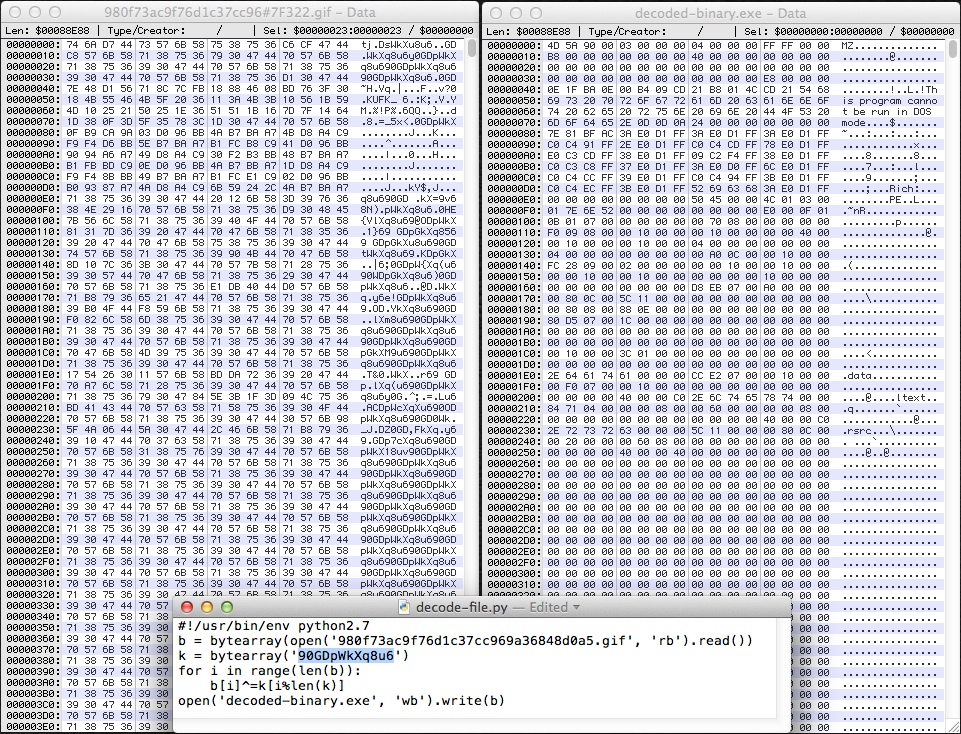
First piece of malware: ZIP file from 46.161.27.176 port 85 (bewarecommadelimited.org):

<https://www.virustotal.com/en/file/c6dd592695370539578b967b0f78199519c7c8754fe6b2264b9c6d6d1b26d8f7/analysis/1383424137/>  
  
File name:  **MJ8BBSp4D3uZDSmbE91prhIGA4FmI6bVPLtYhYn5GFiSMda2.zip**  
File size:  522.6 KB ( 535119 bytes )   
MD5:  2c5ae7b00d4a157361b64eb7c6596b59  
Detection ratio:  11 / 45   
Microsoft calls this:  Exploit:Java/Urains.A   
Microsoft link:  <http://www.microsoft.com/security/portal/threat/encyclopedia/Entry.aspx?Name=Exploit%3AJava%2FUrains.A#tab=1>

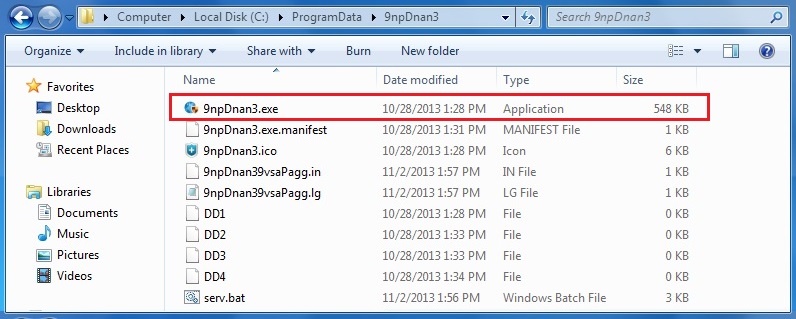
As stated earlier, this ZIP file has the Java exploit code and the malicious EXE included.  Here's what's in the archive:



The **.class** files contain Java exploit code.  The only other item is a 560K file with a **.gif** extension.  If you view this **.gif** file in a hex editor, it looks like an EXE file that's been encoded with an XOR string.  The image below shows this XOR-encoded file, the decoded file, and the Python script used to decode it.  The ASCII string used to XOR the file was: **90GDpWkXq8u6**



The infected machine has a file with the same MD5 hash as the decoded binary, which is located at **C:\ProgramData\9npDnan3\9npDnan3.exe**



Here's the Virus Total results on this malicious executable:

<https://www.virustotal.com/en/file/a55c16f3b1ea89e43c15387a368d8d75ca489c6cc44d95c434de7c13825112be/analysis/1383425334/>  
  
File name:  **9npDnan3.exe**  
File size:  547.6 KB ( 560776 bytes )  
MD5:  d972acf66a6752662d732819f5dfaa42  
Detection ratio:  23 / 47  
Microsoft calls this:  Rogue:Win32/Winwebsec   
Microsoft link:  <http://www.microsoft.com/security/portal/threat/encyclopedia/Entry.aspx?Name=Rogue%3AWin32%2FWinwebsec#tab=2>

Second piece of malware downloaded from 115.47.49.181 port 80 (no domain name):

<https://www.virustotal.com/en/file/712acf837afb83296cff0411c51fa0f2bbeb7f512406b8377a06219608361286/analysis/1383424159/>  
  
File name:  **qtcheck.exe**  
File size:  100.5 KB ( 102912 bytes )  
MD5:  45912f23c915fa3719601375521c8088  
Detection ratio:  30 / 47  
Microsoft calls this:  PWS:Win32/Fareit.gen!J  
Microsoft link:  [http://www.microsoft.com/security/portal/threat/encyclopedia/entry.aspx?name=PWS:WIN32/FAREIT.GEN!J#tab=1](http://www.microsoft.com/security/portal/threat/encyclopedia/entry.aspx?name=PWS:WIN32/FAREIT.GEN%21J#tab=1)