Project 1 Report

Reporter: Yucheng Liu Date: 09/09/2013

===============================

1. Which (February 2012) top-ranked domain was initially visited? (Hint: look for the first use of the DNS) What host (domain or IP address) served the post-exploitation malware download?

Initially Visited Domain: gametug.com (70.32.100.154)

Post-exploitation Malware Host: imagedumper.su (78.159.112.13)

===============================

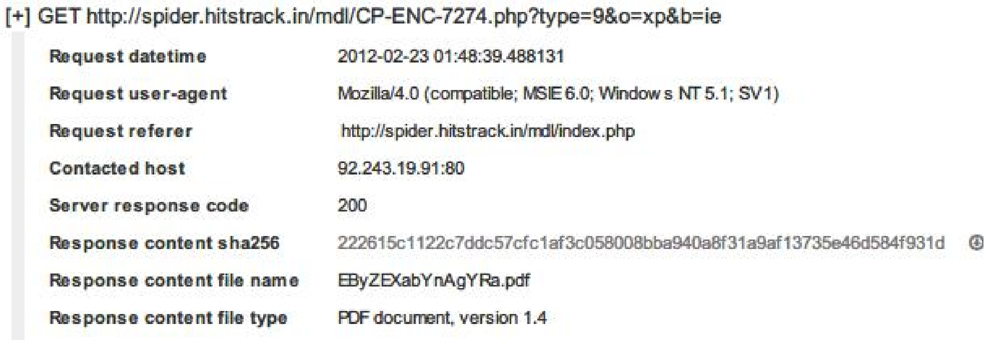
2. Which domains or hosts comprise the intermediate chain of includes or redirects that connect the top-ranked domain to the malware distribution site? Was an ad network involved? If so, specify which one.

Visit Sequence: gametug.com -> **www.google-analytics.com** -> spider.hitstrack.in -> imagedumper.su

Yes, an ad network was involved: www.google-analytics.com

===============================

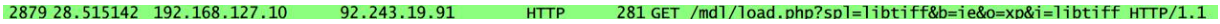
3. What software component targeted during the event resulted in successful exploitation? Upload the corresponding threat artifact you extract from the PCAP to VirusTotal and provide a link to its detections. Which CVE does this artifact target?



[+] GET http://spider.hitstrack.in/mdl/CP-ENC-7274.php?type=9&o=xp&b=ie

Request datetime	2012-02-23 01:48:39.488131
Request user-agent	Mozilla/4.0 (compatible; MSIE 6.0; Window s NT 5.1; SV1)
Request referer	http://spider.hitstrack.in/mdl/index.php
Contacted host	92.243.19.91:80
Server response code	200
Response content sha256	222615c1122c7ddc57cfc1af3c058008bba940a8f31a9af13735e46d584f931d
Response content file name	EByZEXabYnAgYRa.pdf
Response content file type	PDF document, version 1.4

Packet No. 2879



```
2879 28.515142  192.168.127.10       92.243.19.91          HTTP       281 GET /mdl/load.php?spl=libtiff&b=ie&o=xp&i=libtiff HTTP/1.1
```

Software Component Targeted: Adobe Reader and Acrobat

Link: https://www.virustotal.com/en/file/222615c1122c7ddc57cfc1af3c058008bba940a8f31a9af13735e46d584f931d/analysis/

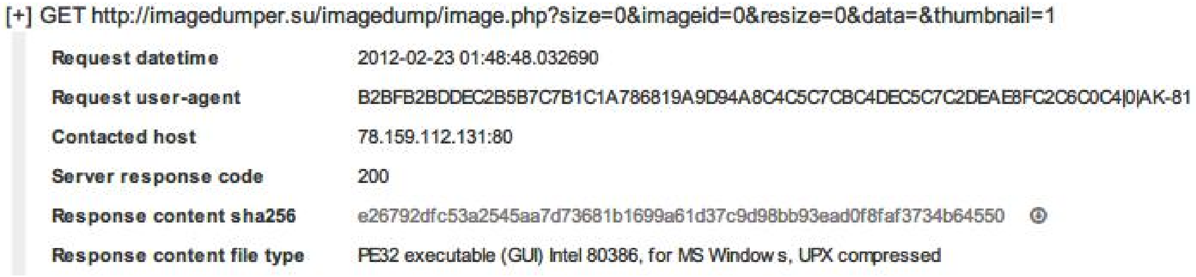
CVE Targeted: CVE-2010-0188 (labeled by Avast)

CVE Description: http://www.adobe.com/support/security/bulletins/apsb10-07.html

A critical vulnerability has been identified in Adobe Reader 9.3 for Windows, Macintosh and UNIX, Adobe Acrobat 9.3 for Windows and Macintosh, and Adobe Reader 8.2 and Acrobat 8.2 for Windows and Macintosh.

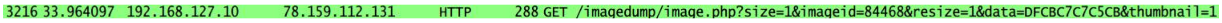
==============================

4. What malware instance was pushed to the exploited system? To answer this question, use reports from sandbox (e.g., Anubis, Malwr, ThreatExpert) and threat labeling (e.g., VirusTotal) systems.



```
[+] GET http://imagedumper.su/imagedump/image.php?size=0&imageid=0&resize=0&data=&thumbnail=1
    Request datetime             2012-02-23 01:48:48.032690
    Request user-agent           B2BFB2BDDEC2B5B7C7B1C1A786819A9D94A8C4C5C7CBC4DEC5C7C2DEAE8FC2C6C0C4|0|AK-81
    Contacted host               78.159.112.131:80
    Server response code         200
    Response content sha256      e26792dfc53a2545aa7d73681b1699a61d37c9d98bb93ead0f8faf3734b64550
    Response content file type   PE32 executable (GUI) Intel 80386, for MS Window s, UPX compressed
```

Packet No. 3216



```
3216 33.964097  192.168.127.10      78.159.112.131      HTTP       288 GET /imagedump/image.php?size=1&imageid=84468&resize=1&data=DFCBC7C7C5CB&thumbnail=1
```

VirusTotal: https://www.virustotal.com/en/file/e26792dfc53a2545aa7d73681b1699a61d37c9d98bb93ead0f8faf3734b64550/analysis/

ThreatExpert Report:

http://www.threatexpert.com/report.aspx?md5=b3fb20eba5b8e1d3be7f343b2ded7bd1

Brief Information: http://www.microsoft.com/security/portal/threat/encyclopedia/entry.aspx?name=TROJAN:WIN32/CHEBRI.A#tab=1

Win32/Chebri.A is a malicious program that is unable to spread of its own accord. It may perform a number of actions of an attacker's choice on an affected computer.

Detail

- A new process (%AppData%\regsrv64.exe) is created in system

- A new registry value is created:
    - [HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run] Microsoft DLL Registration = "%AppData%\regsrv64.exe"
    - So that %AppData%\regsrv64.exe runs every time Windows starts
- The following ports were opened:
    - 1033 TCP
    - 1034 TCP
- The following Host Name was requested from a host database:
    - 1852251819549311.com
- A registered attempt to establish connection with the remote host. The connection details are
    - Remote Host: 1852251819549311.com
    - Port Number: 20001