Targeted Attacks: Then and Now

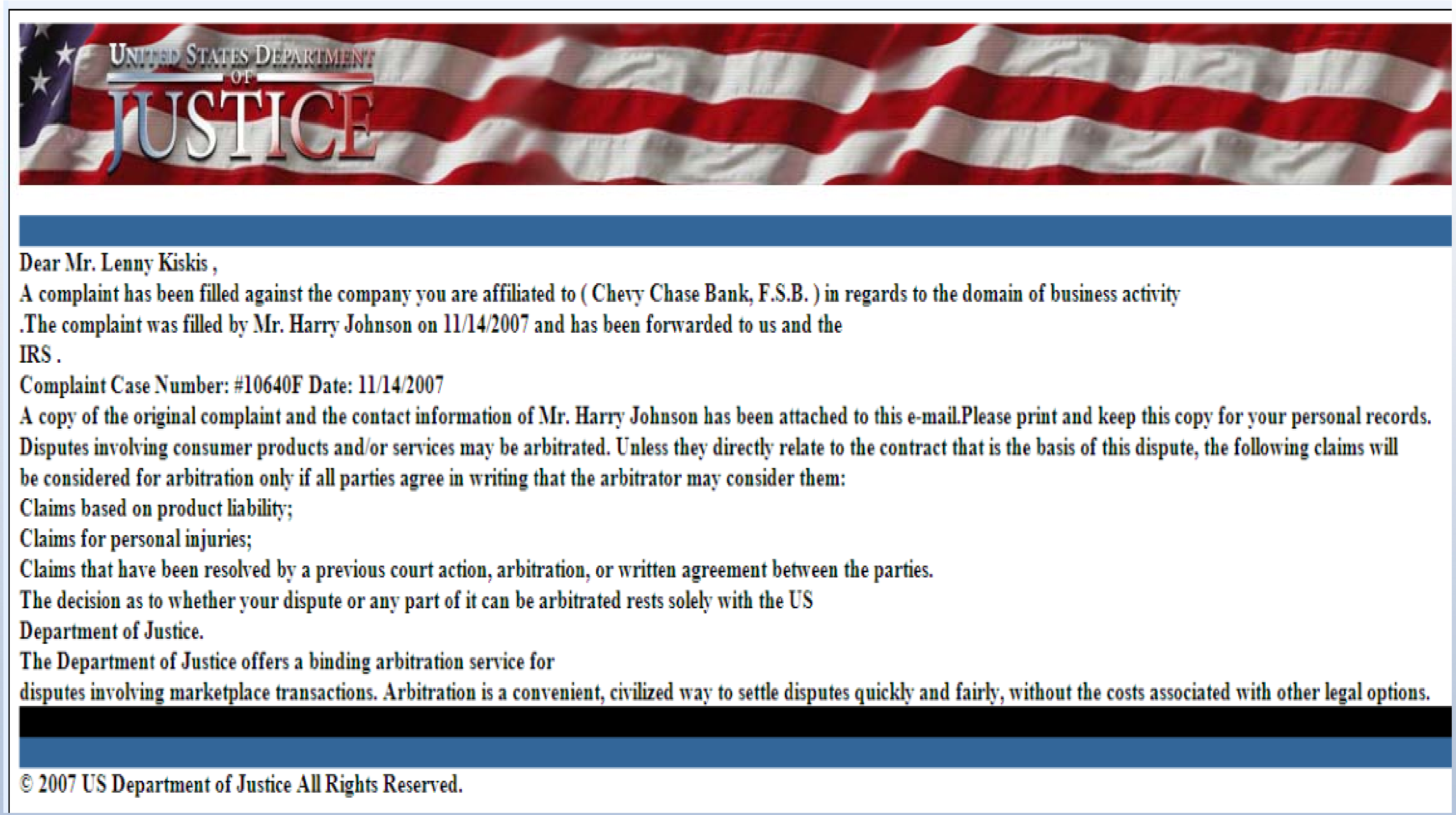
Ken Dunham, Director of Global Response
CISSP, GCIH Gold (Honors), GSEC, GCFA, GREM
kdunham@isightpartners.com

Kim Grillo, Engineer, kgrillo@isightparners.com

Introduction

- BBB Attacks of 2007-2008
- Eastern Europe Attacks
- Operation Aurora attacks
- Mitigation

BBB Attacks of 2007-2008



Dear Mr. Lenny Kiskis ,

A complaint has been filled against the company you are affiliated to (Chevy Chase Bank, F.S.B.) in regards to the domain of business activity .The complaint was filled by Mr. Harry Johnson on 11/14/2007 and has been forwarded to us and the IRS .

Complaint Case Number: #10640F Date: 11/14/2007

A copy of the original complaint and the contact information of Mr. Harry Johnson has been attached to this e-mail.Please print and keep this copy for your personal records.

Disputes involving consumer products and/or services may be arbitrated. Unless they directly relate to the contract that is the basis of this dispute, the following claims will be considered for arbitration only if all parties agree in writing that the arbitrator may consider them:

Claims based on product liability;

Claims for personal injuries;

Claims that have been resolved by a previous court action, arbitration, or written agreement between the parties.

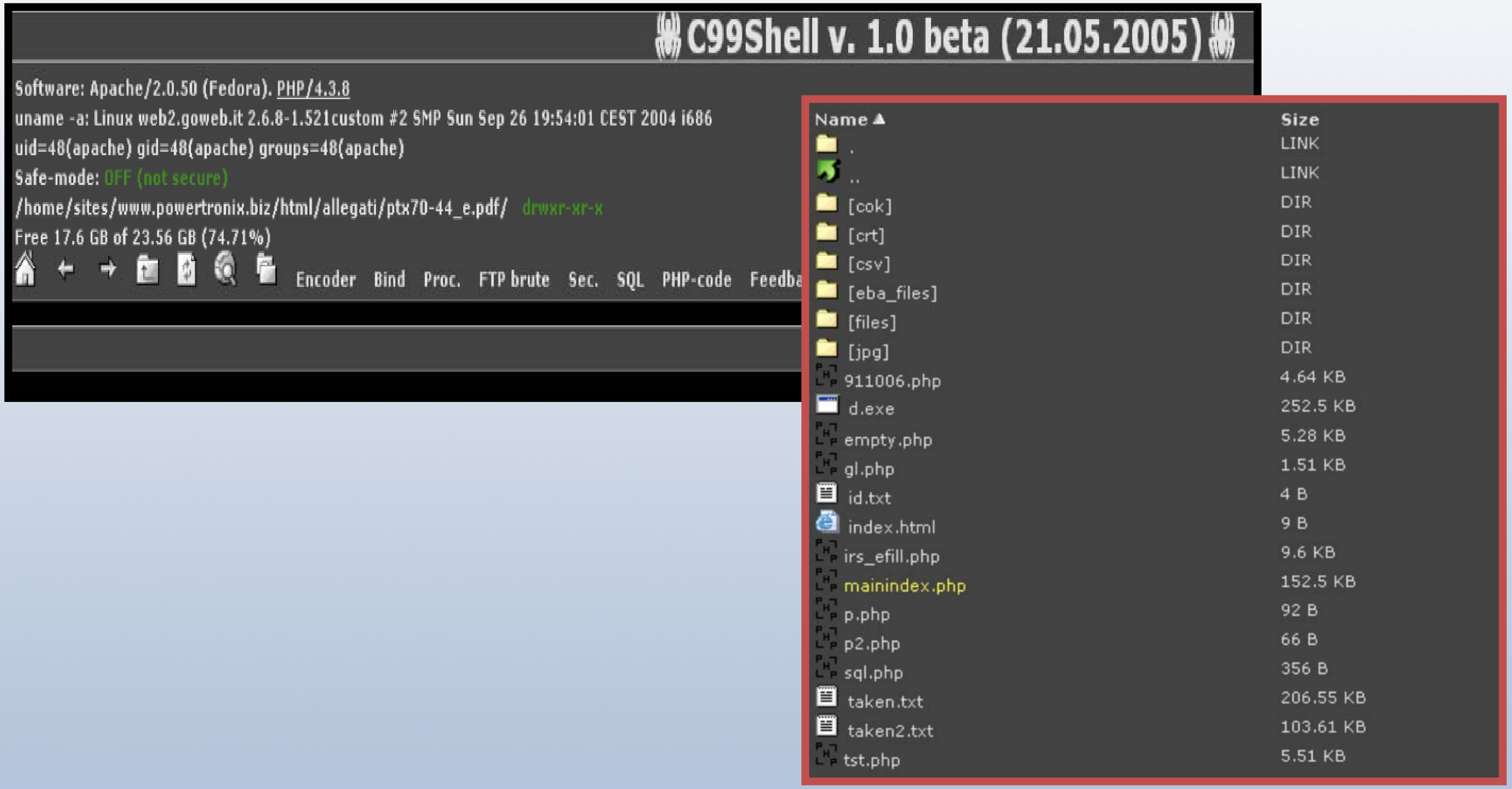
The decision as to whether your dispute or any part of it can be arbitrated rests solely with the US Department of Justice.

The Department of Justice offers a binding arbitration service for disputes involving marketplace transactions. Arbitration is a convenient, civilized way to settle disputes quickly and fairly, without the costs associated with other legal options.

© 2007 US Department of Justice All Rights Reserved.

BBB Attacks of 2007-2008

Secondary payloads downloaded from compromised websites hosting c99 shells.



```
Software: Apache/2.0.50 (Fedora). PHP/4.3.8
uname -a: Linux web2.goweb.it 2.6.8-1.521custom #2 SMP Sun Sep 26 19:54:01 CEST 2004 i686
uid=48(apache) gid=48(apache) groups=48(apache)
Safe-mode: OFF (not secure)
/home/sites/www.powertronix.biz/html/allegati/ptx70-44_e.pdf/  drwxr-xr-x
Free 17.6 GB of 23.56 GB (74.71%)
```

```
Name ▲                Size
.                     LINK
..                    LINK
[cok]                 DIR
[crt]                 DIR
[csv]                 DIR
[eba_files]           DIR
[files]               DIR
[jpg]                 DIR
911006.php            4.64 KB
d.exe                 252.5 KB
empty.php             5.28 KB
gl.php                1.51 KB
id.txt                4 B
index.html            9 B
irs_efill.php         9.6 KB
mainindex.php         152.5 KB
p.php                 92 B
p2.php                66 B
sql.php               356 B
taken.txt             206.55 KB
taken2.txt            103.61 KB
tst.php               5.51 KB
```

BBB Attacks of 2007-2008

- July 2008 - a number of attackers were arrested by US and Romanian law enforcement.
- http://webtv.realitatea.net/actual/cei-19-hackeri-retinuti-au-fost-adusi-la-tribun for video.
- Investigation is ongoing in US.

Göteborg
Gotland
LATVIA
Riga
Baltic Sea
Öland
NMARK
enhagen
Malmö
Bornholm
Kaliningrad
RUSSIA
LITHUANIA
Vilnius
Vitsyebsk
Smolensk
Mahilyow
Minsk
BELARUS
Hrodna
Homyel'
Gdańsk
Hamburg
remen
Berlin
Poznań
POLAND
Warsaw
Brest
Łódź
Wrocław
Kiev
Rivne
Leipzig
RMANY
ankfurt
Main
Prague
CZECH REPUBLIC
Brno
Kraków
L'viv
UKRAINE
Chernivtsi
tuttgart
Munich
SLOVAKIA
Bratislava
Vienna
AUSTRIA
LIECH.
Vaduz
Budapest
HUNGARY
Cluj-Napoca
Iaşi
Chisinau
MOLDOVA
Mykolayiv
Odesa
ROMANIA
Ljubljana
SLOVENIA
Zagreb
ilan
Venice
Bucharest
Constanța
Black Sea
noa
SAN MARINO
Florence
CROATIA
BOSNIA AND HERZEGOVINA
Sarajevo
Belgrade
SERBIA AND MONTENEGRO
Varna
BULGARIA
Sofia
Danube
ITALY
Rome
VATICAN CITY
Adriatic Sea
Skopje
F.Y.R.O.M.
Istanbul
Tirana
ALB.
Naples
Thessaloniki
Bursa
TUR

merln.ndu.edu

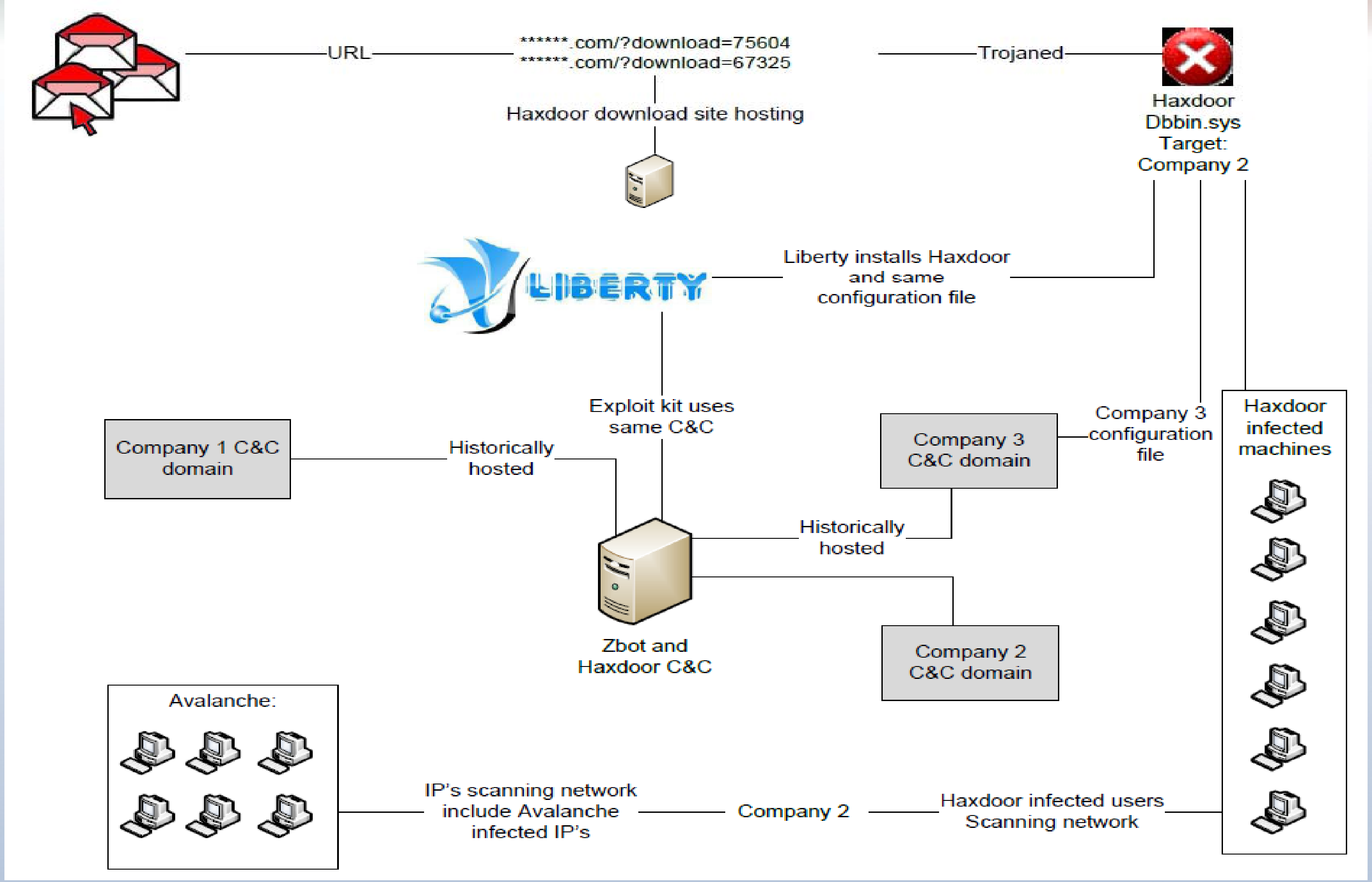
Eastern Europe Attacks

- 2009 – 3 companies victims of malware attacks with links based on attack characteristics
- **Company 1** – Zeus variant targeting customers, keylogged data used to setup fraudulent accounts that would be used to transfer money to mules.
- **Company 2** – Haxdoor variant, C&C hosted at IP address that historically hosted Company 1 attacks.
- **Company 3** – Haxdoor variant, same configuration file (MD5) as Company 2.
- All three attacks only install malware if correct URL and parameters are used and only once, otherwise downloads non malicious notepad.exe.

Eastern Europe Attacks

- September 2009 – Liberty Exploit Kit
  - Installed Haxdoor variant, same MD5 as Company 2 and 3 attacks.
  - Connected to same IP address as Company 2 attacks.
- Haxdoor attack from May 2009 used same MD5, C&C hosted on IP with money mule recruitment domains.

Eastern Europe Attacks

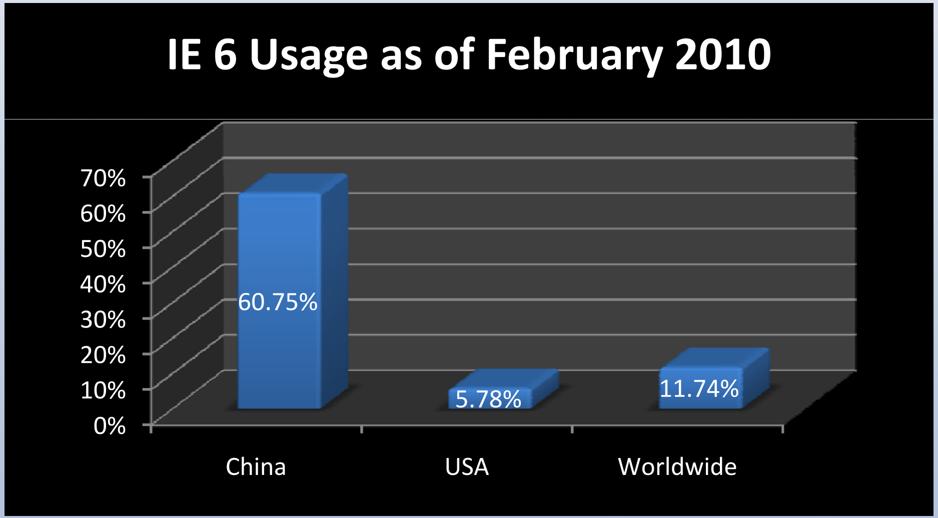


URL
******.com/?download=75604
******.com/?download=67325
Trojaned
Haxdoor download site hosting
Haxdoor
Dbbin.sys
Target:
Company 2
LIBERTY
Liberty installs Haxdoor and same configuration file
Exploit kit uses same C&C
Company 1 C&C domain
Historically hosted
Company 3 C&C domain
Company 3 configuration file
Haxdoor infected machines
Historically hosted
Zbot and Haxdoor C&C
Company 2 C&C domain
Avalanche:
IP's scanning network include Avalanche infected IP's
Company 2
Haxdoor infected users Scanning network

http://images.astronet.ru/pubd/2007/04/09/0001221491/aurora1_wikipedia.jpg

Operation Aurora Attacks

- The attacker's social engineer a victim into opening a malicious website. The malicious email may have been delivered to an oversea employee, likely in China, from one of their trusted contacts.
- Link to a website which hosts a zero day exploit (CVE-2010-0249), vulnerability in Internet Explorer (IE) 6.



Operation Aurora Attacks

- Once installed and executed, the malware connects to C&C servers using dynamic DNS services.
- The attackers escalated privileges to gain access to the corporate network where they can search for, collect, and exfiltrate data of interest.

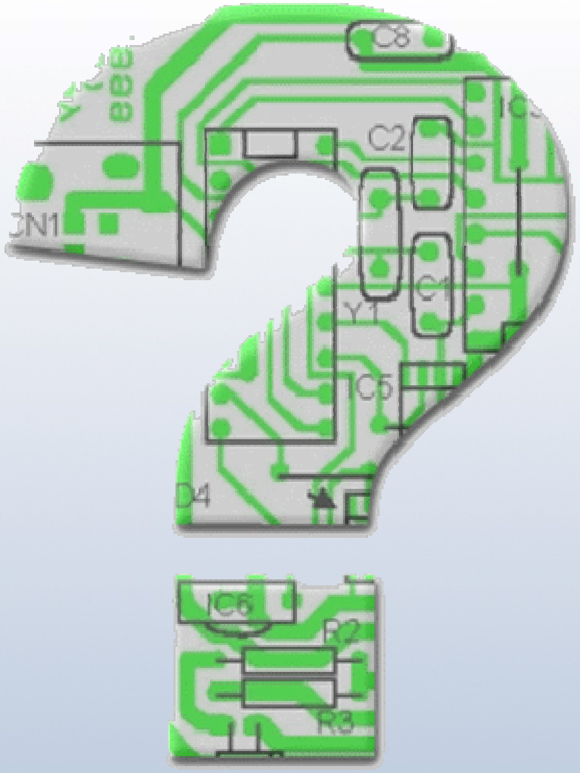
Mitigation

- Network
  - Access Control
  - Blacklisting
  - Monitoring
- Application
  - Enable DEP for Windows and IE
  - Use an alternative PDF reader
  - Application Policies
  - Patching
- Users
  - Education and Training

Key Trends

- All attacks involve highly targeted attacks against specific individuals of interest within companies of interest.

- Attacks are becoming increasingly sophisticated.
- Attacks are also becoming sector specific.



kdunham@isightpartners.com