

# M86 Security

## Cybercriminals Target Online Banking Customers

*Use Trojan and Exploit Kits to Steal Funds from Major UK Financial Institution*

August 2010

# Today's Speaker



- Bradley Anstis
- Vice President, Technical Strategy, M86 Security
- Speaker on security technology and malware trends
- Over 20 Years of IT industry experience

## Recent Press Coverage

- Latest Zeus Trojan discovered compromising 3000 accounts of one global financial institution, US\$1m stolen over 20 days
- 3 days of interviews resulting in:-
  - 134 press stories
  - Live interview on Fox Business News
  - Significant discussion and activity around this event



[http://video.foxbusiness.com/v/4309656/is-zeus-v3-virus-a-threat-to-us/?playlist\\_id=87185](http://video.foxbusiness.com/v/4309656/is-zeus-v3-virus-a-threat-to-us/?playlist_id=87185)

## Background

- In July 2010, an organized network of cybercriminals launched a complex, multi-level scheme that targeted online customers of a large UK financial institution
  - Close to £675,000 taken between July 5 and August 4<sup>th</sup>
  - Approximately 3000 customer accounts compromised
- M86 Security Labs detected this illegal operation after discovering a malicious code attack used to infect users' PCs with a Trojan
- The team then followed the trail to the Command & Control center
- According to our research, these cybercriminals used a combination of the new Zeus v3 Trojan and exploit toolkits to successfully avoid anti-fraud systems while robbing bank accounts

## How we uncovered the attack

- M86 Security labs takes in threat feed data from customers, 3<sup>rd</sup> party feeds and from Secure Browsing
- Analyzing the Secure Browsing feed identified a pattern of infected legitimate UK orientated sites
- We purposely infected ourselves with the Trojan and started tracking its command and control communication
- After identifying the actual C&C servers we were able to recover logging data from the active attack
- We handed the logging data to law enforcement and the institution involved

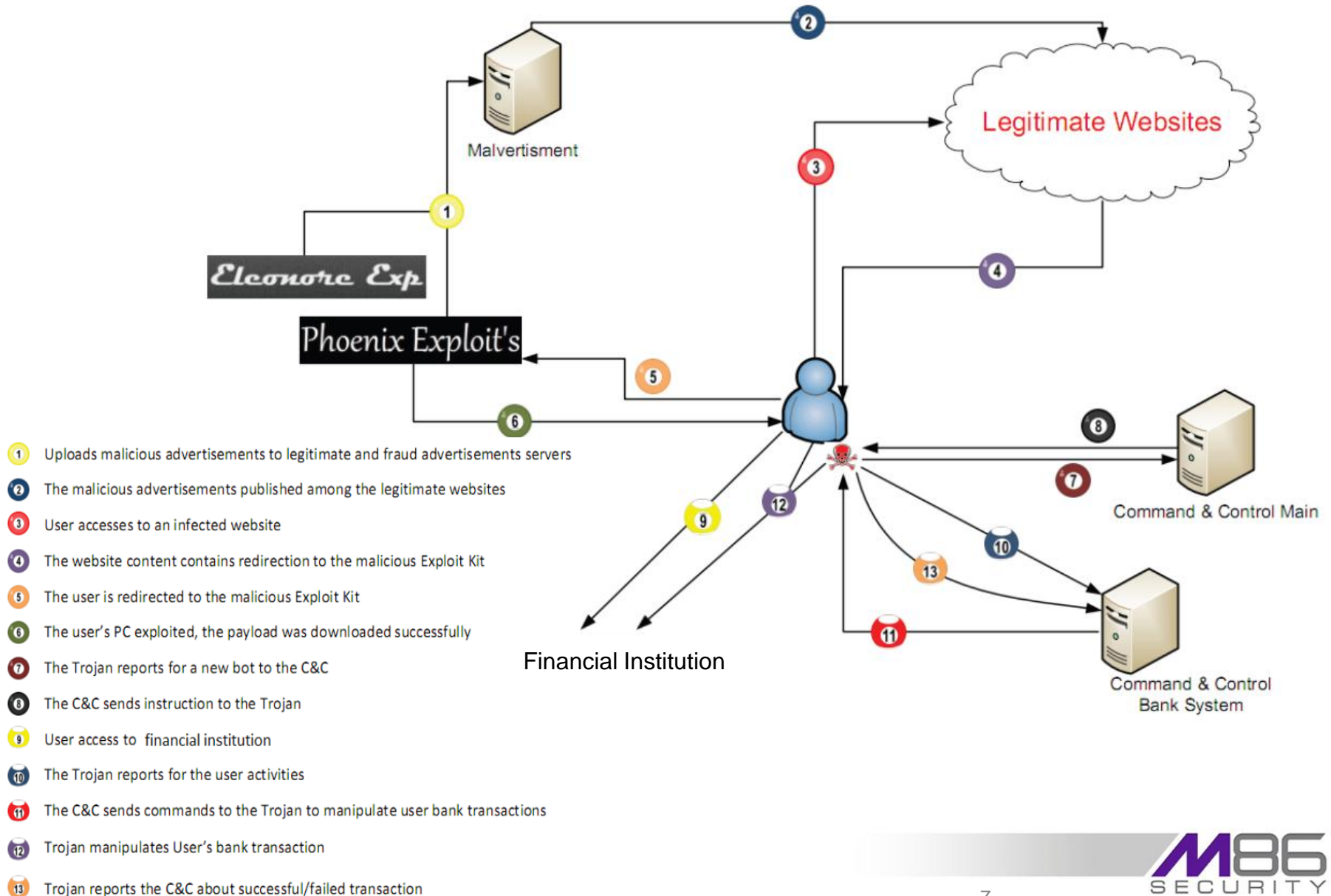


*Eleonore Exp* Eleonore Exploits pack version 1.4.1  
Please enter your login and password.

Operation Systems:	Totals:
Windows XP	121582
Windows Vista	106000
Windows 7	56826
Mac OS	3851
Linux	359
Power PC	312
PlayStation	308
Windows 2000	304
Windows 2003	265
Windows 98	80
Bots	53
Unknown OS :(	27
Symbian OS	22
Nintendo Wii	7
Windows NT 4	2
iPhone OS	1
SunOS	1
Windows ME	1

# The Stages of the Attack

# Overview of the attack



# Selecting the Exploit Kit

- Combination of Phoenix & Eleonore Exploit kits used in this attack
- Exploit kit is used to control the attack, provide reports, load vulnerability exploits and new malware samples
- Exploit kits can be purchased easily and cost just a few hundred dollars
- An exploit is a piece of code taking advantage of vulnerability in software in order to cause unanticipated or malicious behavior

Current version 2.2.1 prices:

\$400 - 1 License

1 License includes:

+ Domain locked one domain (subdomains unlimited)

+ 2 new domain builds if blacklisted

+ Support

+ Minor updates for free

+ Discount on new releases

Extras:

1. Domain re-build for other domain (50\$)

\*\*\* NOTE: YOU ARE NOT ALLOWED TO RESELL/SHARE, IF WE CATCH YOU DOING THIS YOUR LICENSE WILL BE REVOKED \*\*\*

2. AV-Cleaning (\$80 first time, \$50 after)

If you are interested in promoting/reselling, you will get a good offer

Screenshots can be found at:

<http://profile>

Contacts:

MSN: [crimepack@](mailto:crimepack@)

ICQ:



# Infecting Legitimate Websites

- Infecting legitimate websites with malware
- Creating fraudulent online advertisement websites
- Publishing malicious advertisements among legitimate websites
- Statistics show the individual URLs, how many hits in total and number of successful infections

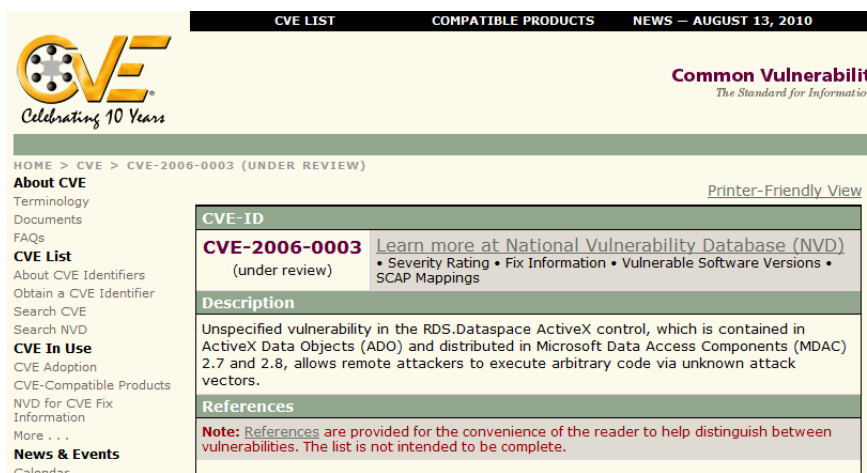


is an internet advertising and marketing service connecting advertisers (buyers of ad space), and webmasters (publishers of web sites), with one another in a fast and easy to use method. Publishers can set their own pricing per week, per month or at per click rates. What sets apart from other forms of internet advertising services are 3 distinct features: Any Ad Types, Human Placement Technology, SmartCache XML

HTTP Referrer:	Traffic:	Loads:	Percent:
www.cityofmedia.com	168966	18989	11.24%
ads2.newspaper.in	34444	4001	11.62%
servedby.adpower.com	23371	4881	20.86%
cr1.sparshlessons.net	15808	1742	11.02%
ads.myalplatform.com	15182	3230	21.28%
cr1.worldsoccerlive.name	11773	1306	11.09%
ads.sma.com	6004	1084	18.05%
ad1.streamdirectsports.in	5939	749	12.61%
ad.yieldmanager.com	5048	722	14.3%
cr1.worldsoccerlive.org	2195	220	10.02%
--	736	158	21.47%
ads.eye.com	223	31	13.9%

# Load the Exploit Kit with Exploits

- Exploits are pieces of code that have been developed to make use of a vulnerability to infect a computer
- All the vulnerabilities used in this attack have been patched



The screenshot shows the CVE website interface. At the top, there is a navigation bar with links for 'CVE LIST', 'COMPATIBLE PRODUCTS', and 'NEWS - AUGUST 13, 2010'. The CVE logo is on the left, with the text 'Celebrating 10 Years'. The main content area displays the details for CVE-2006-0003, which is currently 'UNDER REVIEW'. The page includes a sidebar with navigation links such as 'About CVE', 'Terminology', 'Documents', 'FAQs', 'CVE List', 'About CVE Identifiers', 'Obtain a CVE Identifier', 'Search CVE', 'Search NVD', 'CVE In Use', 'CVE Adoption', 'CVE-Compatible Products', 'NVD for CVE Fix Information', 'More . . .', and 'News & Events'. The main content area has a 'Printer-Friendly View' link and a table with the following information:

CVE-ID	
<b>CVE-2006-0003</b> (under review)	<a href="#">Learn more at National Vulnerability Database (NVD)</a> • Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings
Description	
Unspecified vulnerability in the RDS.Dataspace ActiveX control, which is contained in ActiveX Data Objects (ADO) and distributed in Microsoft Data Access Components (MDAC) 2.7 and 2.8, allows remote attackers to execute arbitrary code via unknown attack vectors.	
References	
<b>Note:</b> References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.	

1. IE MDAC Vulnerability [CVE-2006-0003](#)
2. Adobe Reader Collab GetIcon Vulnerability - [CVE-2009-0927](#)
3. Adobe Reader CollectEmailInfo Vulnerability - [CVE-2007-5659](#)
4. Adobe Reader newPlayer Vulnerability [CVE-2009-4324](#)
5. Java Development Kit Vulnerability [CVE-2008-5353](#)
6. Java Web Start Vulnerability - [CVE-2010-1423](#)

# Track the successful infections

- Top table shows the number of hits on the infected Web pages by OS
- Bottom table shows the number of successful exploit loads or completed infections
- This was a windows targeted attack, but all that would have been required in infect other platforms was an exploit for the platform and a piece of malware

Operation Systems:	Totals:
Windows XP	121582
Windows Vista	106000
Windows 7	56826
Mac OS	3851
Linux	359
Power PC	312
PlayStation	308
Windows 2000	304
Windows 2003	265
Windows 98	80
Bots	53
Unknown OS :(	27
Symbian OS	22
Nintendo Wii	7
Windows NT 4	2
iPhone OS	1
SunOS	1
Windows ME	1

Spoit:	Loads:
3D3Dmdac	1
3Dmdac	2
	2
_new	53
_geticon	155
_email	259
mdac	1468
_pack	7492
java_gsb	10053
x1YY	17657

## Also track by country

- Targeting a specific country is as easy as infecting websites orientated towards that country
- Here you see the number of hits on the website from which country and how many were successfully infected
- The loads you get outside of your targeted country are just considered collateral damage

Country:	Traffic:	Loads:	Percent:
GB	287685	36802	12.79 %
--	2153	307	14.26 %
RU	75	5	6.67 %
US	37	14	37.84 %
IE	22	4	18.18 %
DE	7	5	71.43 %
NL	5	1	20 %
JP	5	3	60 %
CN	4	0	0 %
FR	2	0	0 %
BR	1	0	0 %
PE	1	0	0 %
PS	1	0	0 %
SA	1	0	0 %
SG	1	0	0 %
NG	1	1	100 %

# Local Anti-virus detecting the malware samples?



- Two different samples uploaded to VirusTotal
- 2.39% detection rate for one and 14.64% for the other
- Feeling lucky?

File **eleonore.html** received on **2010.07.27 13:46:40 (UTC)**  
Current status: **finished**  
Result: **1/42 (2.39%)**

[Compact](#) [Print results](#)

Antivirus	Version	Last Update	Result
AhnLab-V3	2010.07.27.00	2010.07.26	-
AntiVir	8.2.4.26	2010.07.27	-
Antiy-AVL	2.0.3.7	2010.07.26	-
Authentium	5.2.0.5	2010.07.27	-
Avast	4.8.1351.0	2010.07.27	-
Avast5	5.0.332.0	2010.07.27	-
AVG	9.0.0.851	2010.07.27	JS/Downloader.Agent
BitDefender	7.2	2010.07.27	-
CAT-QuickHeal	11.00	2010.07.27	-
ClamAV	0.96.0.3-git	2010.07.27	-
Comodo	5556	2010.07.27	-
DrWeb	5.0.2.03300	2010.07.27	-
Emsisoft	5.0.0.34	2010.07.27	-
eSafe	7.0.17.0	2010.07.26	-
eTrust-Vet	36.1.7742	2010.07.27	-
F-Prot	4.6.1.107	2010.07.27	-
F-Secure	9.0.15370.0	2010.07.27	-
Fortinet	4.1.143.0	2010.07.24	-

File **1.html** received on **2010.07.27 13:35:12 (UTC)**  
Current status: **finished**  
Result: **6/41 (14.64%)**

[Compact](#) [Print results](#)

Antivirus	Version	Last Update	Result
AhnLab-V3	2010.07.27.00	2010.07.26	-
AntiVir	8.2.4.26	2010.07.27	JS/Ag.13173
Antiy-AVL	2.0.3.7	2010.07.26	-
Authentium	5.2.0.5	2010.07.27	-
Avast	4.8.1351.0	2010.07.27	HTML:Downloader-H
Avast5	5.0.332.0	2010.07.27	HTML:Downloader-H
AVG	9.0.0.851	2010.07.27	-
BitDefender	7.2	2010.07.27	-
CAT-QuickHeal	11.00	2010.07.27	-
ClamAV	0.96.0.3-git	2010.07.27	-
Comodo	5556	2010.07.27	-
DrWeb	5.0.2.03300	2010.07.27	-
Emsisoft	5.0.0.34	2010.07.27	-
eSafe	7.0.17.0	2010.07.26	-
eTrust-Vet	36.1.7742	2010.07.27	-
F-Prot	4.6.1.107	2010.07.27	JS/Crypted.CV.gen
F-Secure	9.0.15370.0	2010.07.27	-
Fortinet	4.1.143.0	2010.07.24	-

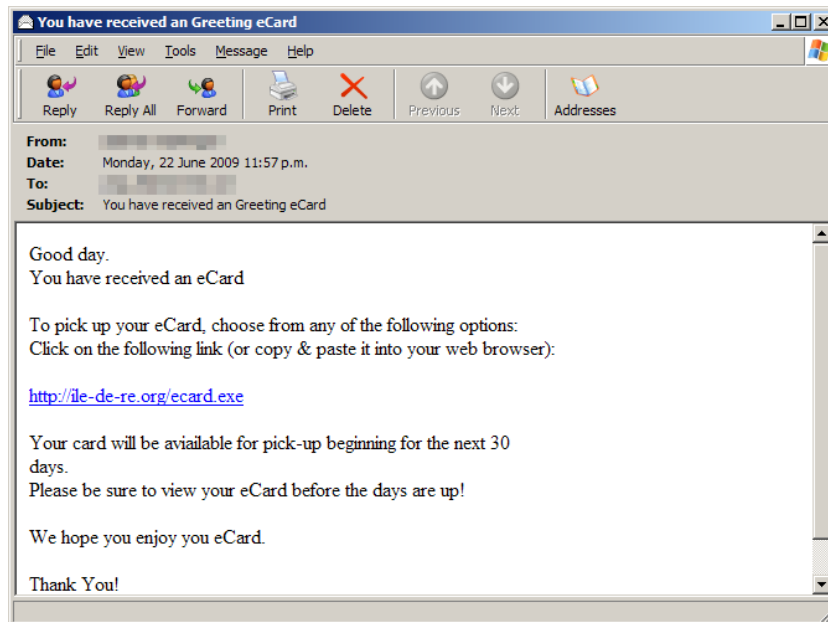
**The payload:-**

**Zeus Trojan...  
(Aka Zbot)**



# Origins...

- Zeus family first appeared in 2007
- Back then it was a password stealing Trojan targeting a specific list of sites...
- Sending any collected information back to its C&C every hour



- !\*livejournal.com\*
- !\*facebook.com\*
- !\*myspace.com\*
- !\*youtube.com\*
- !\*blogger.com\*
- !\*amazon.com\*
- !\*.microsoft.com/\*
- !\*flickr.com\*
- !http://\*myspace.com\*
- @\*/www.svbconnect.com/security/challengeVerify.do
- https://chsec.wellsfargo.com/login/login.fcc
- http://ultrex.info/webstat/03/03x.htm
- https://wellsfargo.com/portal/signon/index.jsp?UpdateProfileInfo
- \*/my.ebay.com/\*CurrentPage=MyeBayPersonalInfo\*
- \*.ebay.com/\*eBayISAPI.dll?\*
- https://www.us.hsbc.com/\*
- https://online.wellsfargo.com/das/cgi-bin/session.cgi\*
- https://www.paypal.com/\*/webscr?cmd=\_account
- https://www.paypal.com/\*/webscr?cmd=\_login-done\*
- https://www.usbank.com/internetBanking/LoginRouter
- https://www#.citizensbankonline.com/\*/index-wait.jsp
- https://onlinebanking.nationalcity.com/OLB/secure/AccountList.aspx
- https://www.suntrust.com/portal/server.pt\*parentname=Login\*
- https://www.53.com/servlet/efsonline/index.html\*
- https://web.da-us.citibank.com/\*BS\_Id=MemberHomepage\*
- https://onlineeast#.bankofamerica.com/cgi-bin/ias\*/GotoWelcome
- https://online.wamu.com/Servicing/Servicing.aspx?targetPage=AccountSummary
- https://businessonline.tdbank.com/CorporateBankingWeb/Core/Login.aspx\*
- https://online.citibank.com/\*
- https://webexpress.tdbanknorth.com/wcmfd/wcmpw/CustomerLogin
- https://onb.webcashmgmt.com/wcmfd/wcmpw/CustomerLogin
- https://www.sterlingwires.com/
- https://ffce.webcashmgmt.com/wcmfd/wcmpw/CustomerLogin
- https://web3.secureinternetbank.com/ebc\_etc1961/ebc1961.aspx\*
- https://trading.scottrade.com/home/default.aspx
- https://www.svbconnect.com/security/integratedLoginAuth.do
- https://www.svbconnect.com/useraccess/Login.jsp
- https://www.svbconnect.com/\*
- https://chaseonline.chase.com/MyAccounts.aspx
- https://www.securechemicalbankmi.com/onlineserv/CM/

## Zeus now...

- This Zbot/Zeus v3 version is an evolved mutation of Zbot 2
  - The versions we discuss are related to changes in behavior of the malware not actual software versions
- Now in addition to collecting credentials, also actively participating as a Man-in-the-Browser attack
  - Reassembling partial credentials supplied by the victim
  - Injecting its own transactions into a users banking session
  - Re-writing on-screen account balances & hiding its transactions
  - Re-generating pdf delivered statements
- Unlike older versions, this one focused specifically on online banking
  - This particular attack targeted just one financial institution
  - Waited for a minimum account balance ~US\$1000
  - Communicated with C&C using SSL, based on a legitimate certificate
  - Each transfer between US\$500-\$2500

# Man-in-the-Browser attacks

- Subset of Man-in-the-middle attacks
- Attack is running inside the victims computer
- Generally used to collect advanced credentials or take over transactions to web based applications
- Most seen in Internet banking attacks, example of configuration screen...
- Recent M86 whitepaper:-  
<http://www.m86security.com/labs/resources.asp>

NAME:	POST1
DROPSTATUS:	ENABLED <input type="button" value="v"/>
IF ACC BALANS "<":	-1
MIN_AMOUNT:	4000
MAX_AMOUNT:	15000
LEAVE % (default 23):	5
CORRECT (default 100):	0
DROPNAME:	VIKTOR KLOSE
KONTONUMMER:	1(009706
BLZ:	6(0070
C1:	Ref Num 995345
C2:	Ref Num 995345
C3:	Ref Num 995345
C4:	Ref Num 995345
COMMENT:	Tigr
BROWSER:	iexplore: <input checked="" type="checkbox"/> firefox: <input checked="" type="checkbox"/> mozilla: <input checked="" type="checkbox"/> avant: <input checked="" type="checkbox"/> maxthon: <input checked="" type="checkbox"/> MyIE: <input checked="" type="checkbox"/>

\*Example from another Internet Banking attack

# Hijacked Transaction Sequence

The malware began reporting to a different C&C server once the user accessed the desired bank.



After the user logged in to his personal banking account, it appears the Trojan transferred the login ID, date of birth, and a security number to the C&C server



Once the user accessed the transactional section of the site, the Trojan reported to the C&C. It then received new JavaScript code to replace the original bank JavaScript that was used for the transaction form.



After the user submitted the transaction form, the relevant data was sent to the C&C system instead of the bank



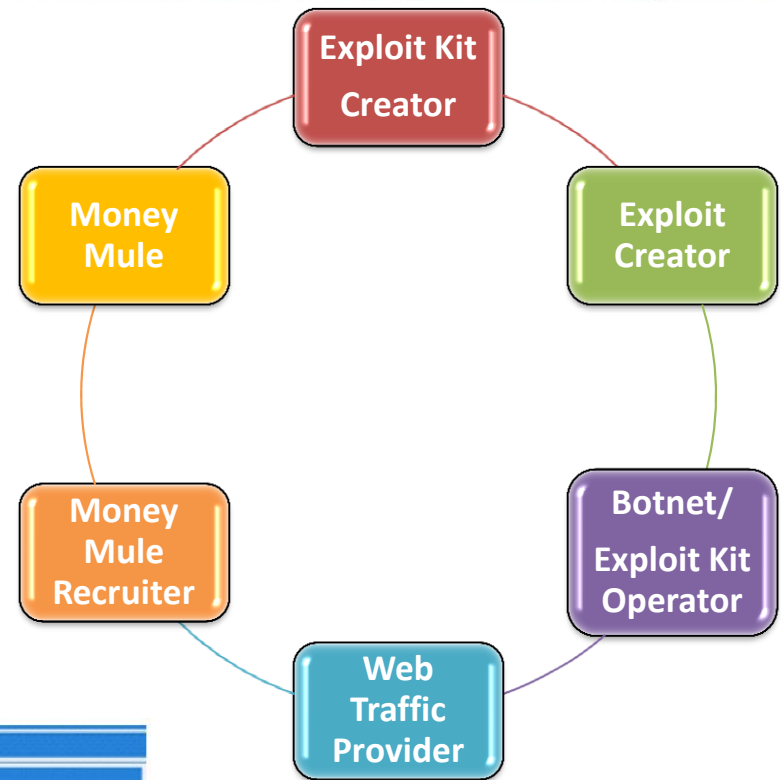
After analyzing the data, the system determined whether the user had enough money in the account. It selected the most appropriate mule account to retrieve the money, wrapped all the data, and sent it back to the Trojan installed on the victim's machine.



The Trojan then updated the data in the form and sent it to the bank to complete the transaction. The bank received the requested operation and sent back the transaction result as the Trojan continued to listen to the bank response, reporting it to the C&C system.

# The Cyber-crime gang

- Each role has a specific function
- Some Individuals do multiple roles
- Money mules are typically innocent bystanders with accounts in the country being targeted



id	time	Блокировка	zaitNraz	priority	min_sum	max_sum	DrName	AccNum	sort	ref	isDeleted	Дронвод	Действие
62	12 Jul 2010 11:57:17	Да	2	0	1122	3999	...	...	...	...	1	...	Edit
65	12 Jul 2010 12:23:19	Да	1	0	1222	2555	...	...	...	...	1	...	Edit
67	12 Jul 2010 13:31:47	Нет	0	2	1333	1520	...	...	...	...	1	...	Edit
70	12 Jul 2010 14:02:12	Да	2	0	888	2999	...	...	...	...	1	...	Edit
72	12 Jul 2010 18:17:12	Да	1	0	800	1400	...	...	...	...	0	...	Edit
75	13 Jul 2010 10:18:11	Да	2	0	799	2999	...	...	...	...	1	...	Edit
76	13 Jul 2010 10:20:19	Да	2	0	666	2222	...	...	...	...	1	...	Edit
77	13 Jul 2010 10:21:49	Да	1	3	3155	4111	...	...	...	...	1	...	Edit
78	13 Jul 2010 11:49:06	Да	1	0	999	1755	...	...	...	...	1	...	Edit
80	13 Jul 2010 13:35:08	Да	1	0	999	2999	...	...	...	...	1	...	Edit
82	13 Jul 2010 15:48:28	Да	1	0	2499	3599	...	...	...	...	1	...	Edit
83	13 Jul 2010 15:51:16	Да	1	2	2399	3999	...	...	...	...	1	...	Edit
84	13 Jul 2010 18:55:36	Да	1	4	2999	4199	...	...	...	...	1	...	Edit

# How do you defend yourself? (For individuals)

- Keep all your applications and operating system up to date with security patches
- Make sure your AV product is up to date, consider running multiple products, some banks offer them for free, M86 Security also offers SecureBrowsing
- Consider using less popular applications for web browsing, pdf viewing etc., these are less targeted with vulnerability exploits
- Be suspicious of any web link in email, any 3<sup>rd</sup> party plug-in or codec update
- Know what your bank balance should be at all times, and validate with means other than Internet Banking
  - ATM balance
  - Telephone banking
  - Visit a branch
- Do you need to have the ability to transfer to 3<sup>rd</sup> party external accounts active?

# How do you defend yourself? (For Businesses)

- Review all currently deployed Internet security products:-
  - Ensure you are running reactive controls like AV scanning/URL Filtering from reputable vendors
  - Also layer in with newer innovative technologies like M86 Securities Real-time code analysis
  - Ensure these solutions are scanning all web content, from all websites (This attack was based on legitimate sites never previously infected)
- Educate all staff to the perils of Internet use
- Look to tighten up access to:-
  - Executable files needed by all staff?
  - All staff need access to all types of websites?
  - How are remote/mobile staff protected?

These measures will not guarantee protection but will raise your security posture

**How did our customers fare?**

# Exploit Vulnerability – Zeus Attack

Secunia Advisory SA37690



Adobe Reader newPlayer Vulnerability - CVE-2009-4324

Secunia Advisory	SA37690
Release Date	2009-12-15
Last Update	2010-01-14
Popularity	47,563 views
Comments	<a href="#">0 comments</a>
Criticality level	<b>Extremely critical</b>
Impact	Cross Site Scripting System access
Where	From remote
Authentication level	<i>Available in Customer Area</i>
Report reliability	<i>Available in Customer Area</i>
Solution Status	<b>Vendor Patch</b>
Secunia PoC	<i>Available in Customer Area</i>
Secunia analysis	<i>Available in Customer Area</i>
3rd party PoC/exploit	<i>Link available in Customer Area</i>
Systems affected	<i>Available in Customer Area</i>
Approve distribution	<i>Available in Customer Area</i>

```
if (isset($_REQUEST['ini']) && !empty($_REQUEST['ini'])) {  
    if ($cc=='GB' || $cc=='IE' || $cc=='NL') {  
        if($_REQUEST['ini'] == 'd'){  
            header("Location: get_dr.php?e=".$_REQUEST['e']);  
            exit;  
        }  
        if($_REQUEST['ini'] == 'i'){  
            header("Location: get_inf.php?e=".$_REQUEST['_eexw']);  
            exit;  
        }  
        if(preg_match("/https?:\/\//.*/", $_REQUEST['ini']) ||  
            if($_REQUEST['ini'] == 'j'){  
                if($browser == 'IE') include("./resour...");  
                if($browser == 'FF') include("./resour...js");  
                exit;  
            } else {  
                include("404.html");  
                exit;  
            }  
        }  
    }  
}
```

Code snippet, Zeus injecting its own transaction

Adobe Vulnerability from 2009 still being used for successful attacks

# Exploit Vulnerability – Zeus Attack

Users Policies Logs and Reports Administration Help

Logout

M86 SWG M86 SECURITY

Active real-time code analysis combined with behavioral analysis is essential to detect and stop stealthy crimeware that targets unknown and un-patched vulnerabilities

Crashing Internet Clients Remote Script Remote ActiveX Cross-Site and Spoofing

Buffer Overflows 3rd Parties

Select/Deselect all

<input checked="" type="checkbox"/>	<a href="#">AOL TGPVWZ ActiveX Buffer Overflow Vulnerability</a>
<input checked="" type="checkbox"/>	<a href="#">Acrobat reader XSS vulnerability</a>
<input checked="" type="checkbox"/>	<a href="#">Adobe Acrobat 9 ActiveX Vulnerability</a>
<input checked="" type="checkbox"/>	<a href="#">Adobe Reader media.newPlayer Vulnerability</a>
<input type="checkbox"/>	<a href="#">Adobe Reader media.newPlayer Vulnerability Type II</a>
<input checked="" type="checkbox"/>	<a href="#">Akamai Download Manager ActiveX Stack Buffer Overflow Vulnerability</a>
<input checked="" type="checkbox"/>	<a href="#">Akamai Download Manager Arbitrary File Download Vulnerability</a>
<input checked="" type="checkbox"/>	<a href="#">Anzio Web Print ActiveX Vulnerability</a>
<input checked="" type="checkbox"/>	<a href="#">AskJeeves Toolbar ActiveX Remote Code Execution Vulnerability</a>

Incoming Incoming

**Behavior Profile (Script)**  
Default Profile - Script Behavior  
[Generic Shellcode detection](#)  
[Suspected Malicious String Content](#)

**Rule Action**  
Block  
Blocked

# All vulnerabilities exploited successfully detected

1. IE MDAC Vulnerability [CVE-2006-0003](#)
2. Adobe Reader Collab GetIcon Vulnerability - [CVE-2009-0927](#)
3. Adobe Reader CollectEmailInfo Vulnerability - [CVE-2007-5659](#)
4. Adobe Reader newPlayer Vulnerability [CVE-2009-4324](#)
5. Java Development Kit Vulnerability [CVE-2008-5353](#)
6. Java Web Start Vulnerability - [CVE-2010-1423](#)



# Conclusions

- Demonstrated yet again the importance of Real-time code analysis
- Organizations need to be effectively layering reactive & proactive controls
- Application security patches still not being installed in a timely manner
- Financial Institutions have very secure applications and websites but now their customers are the ones being targeted, an area they have much less control over, and this has an impact on reputation
- Man-in-the-middle attacks take sophistication to a whole new level
- User education can go a long way to staying safe

# Questions?

[http://www.m86security.com/documents/pdfs/security\\_labs/cybercriminals\\_target\\_online\\_banking.pdf](http://www.m86security.com/documents/pdfs/security_labs/cybercriminals_target_online_banking.pdf)