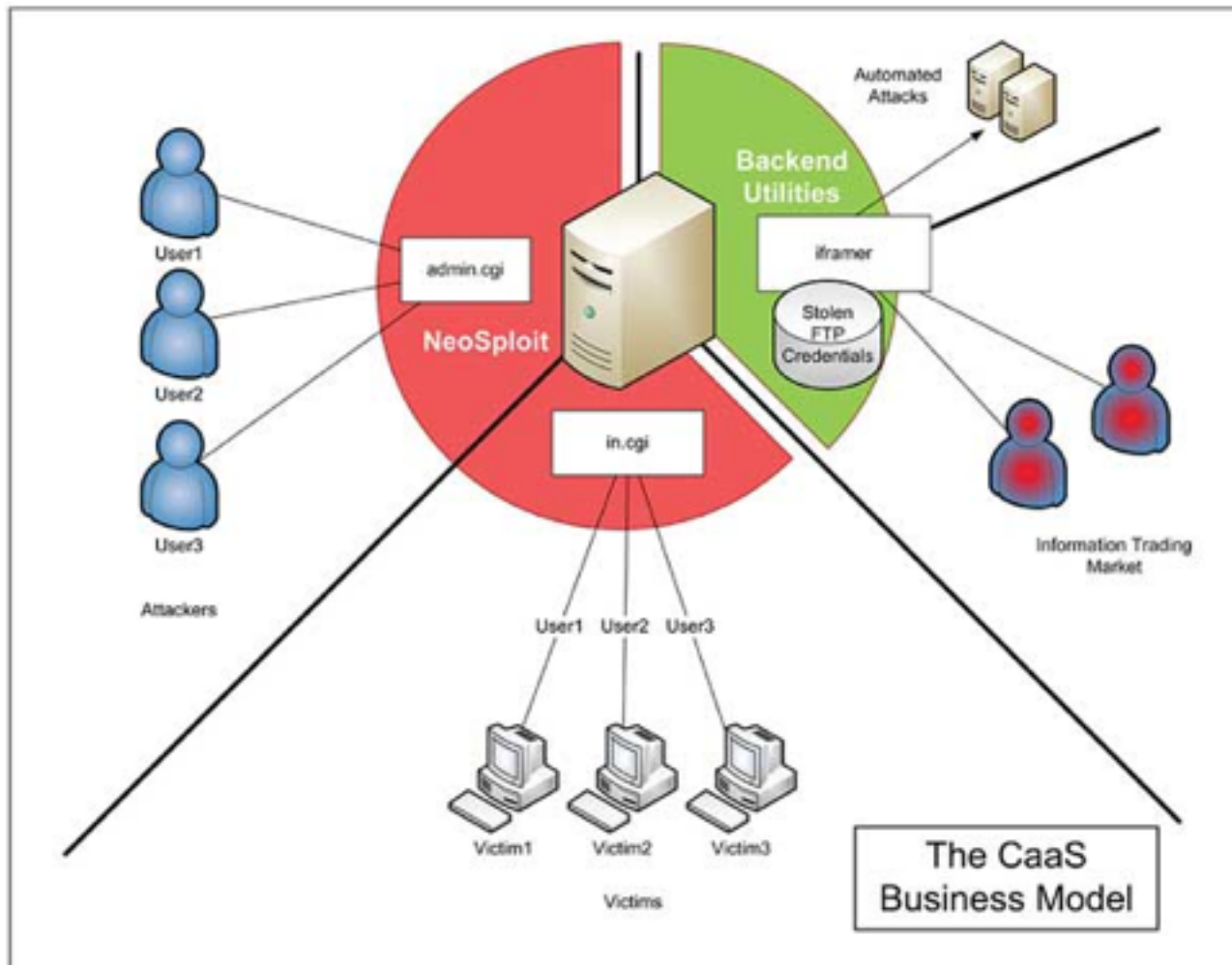


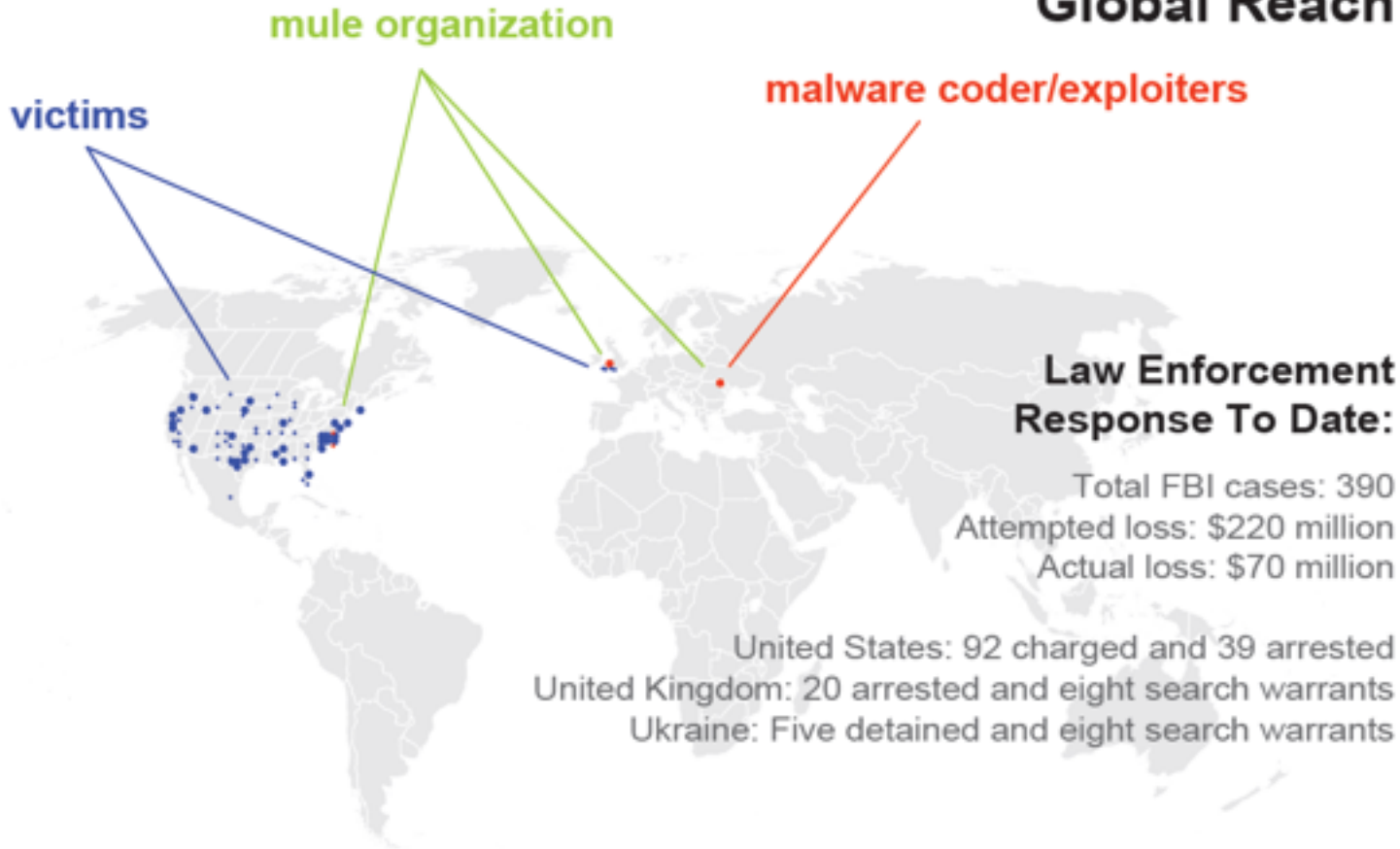
Malware Forensics (Virenforensik)

Dr. Morton Swimmer, FTR Team, Trend Micro Deutschland, GmbH





Global Reach



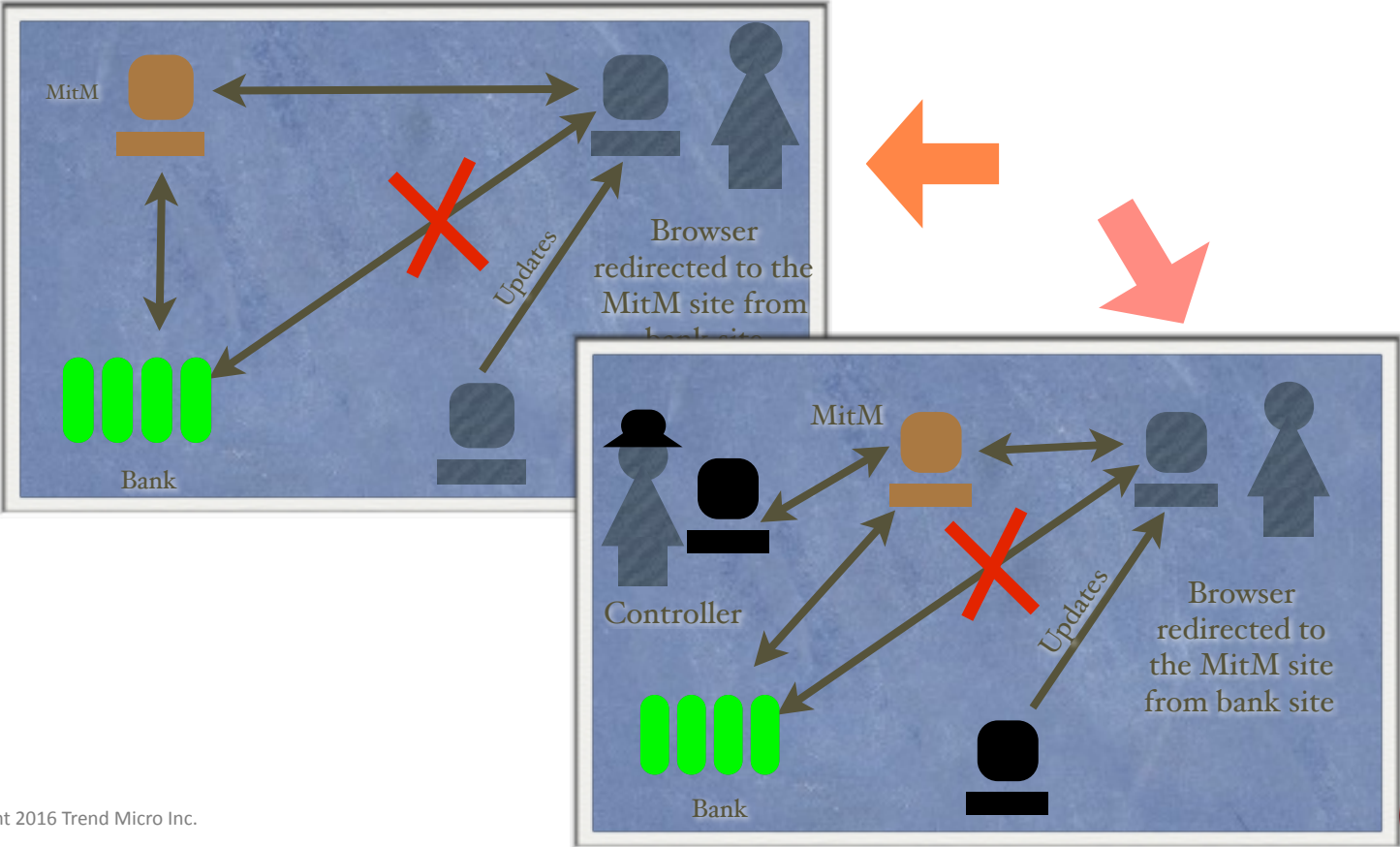
Source: <http://www.fbi.gov/news/stories/2010/october/cyber-banking-fraud/cyber-banking-fraud-graphic>

FTR

- Forward-Looking Threat Research
- 25 researchers in 6 geographies
- What are the threats in 5 years ... in 10 years time?



Internet Forensics



Threat Landscape

- Attacks
 - most are automated; indiscriminate
 - some are specific and targeted
- Spectrum
 - highly skilled and well resourced adversaries
 - opportunistic amateurs
 - individuals or groups
- Motivation
 - financial gain, politics or status
 - espionage and data theft

Targeted Malware Attacks

Targeted Attacks

- Attacks against
 - civil society organizations/ NGOs
 - business enterprises
 - government/military networks
- Attacks are typically part of a broader campaign
- Attackers use whatever is required based on reconnaissance
- Will adjust tactics in reaction to the defenses of the target
- In contrast with most Malware that aims for the masses
 - try variations against entire target population until something sticks

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

Stages of an attack

Reconnaissance

Delivery

Compromise

Command & Control

Persistence

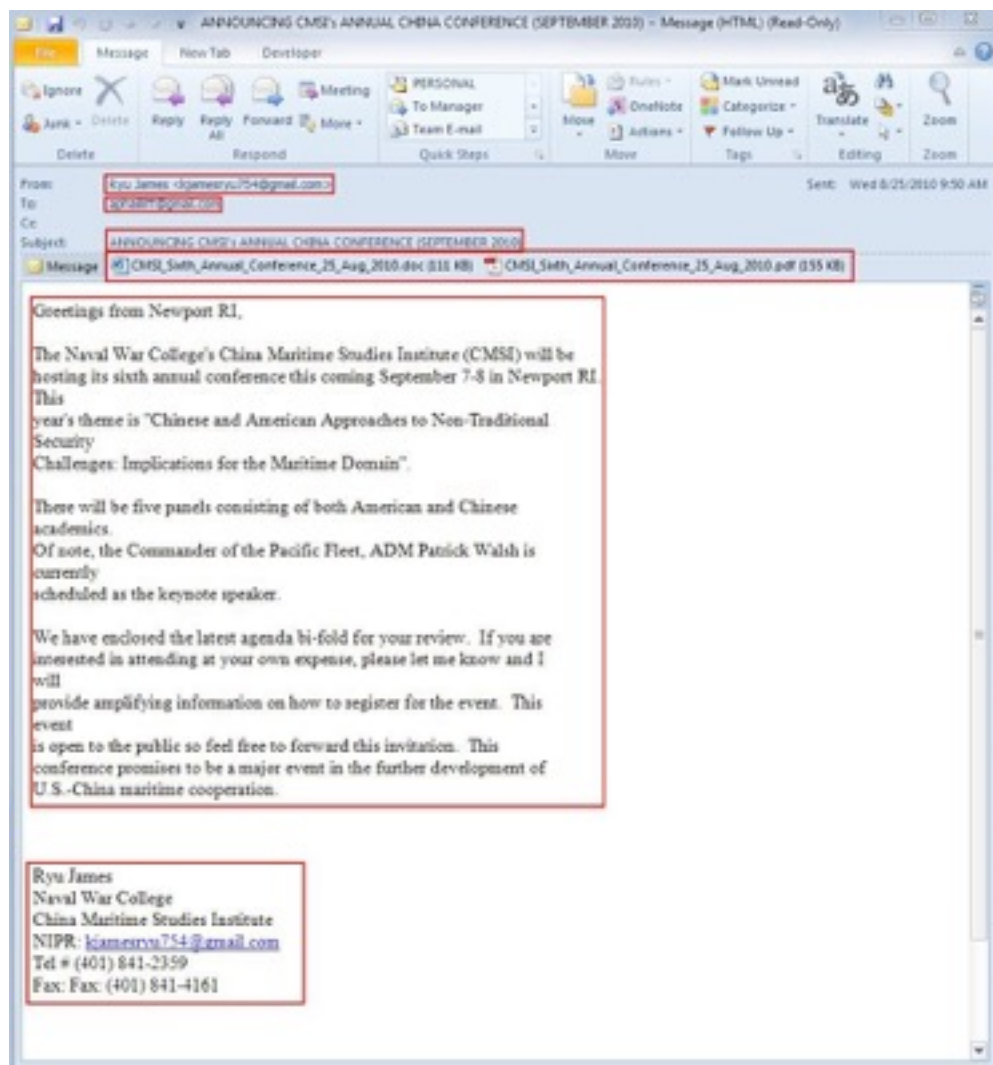
Data ex-filtration

Social Engineering

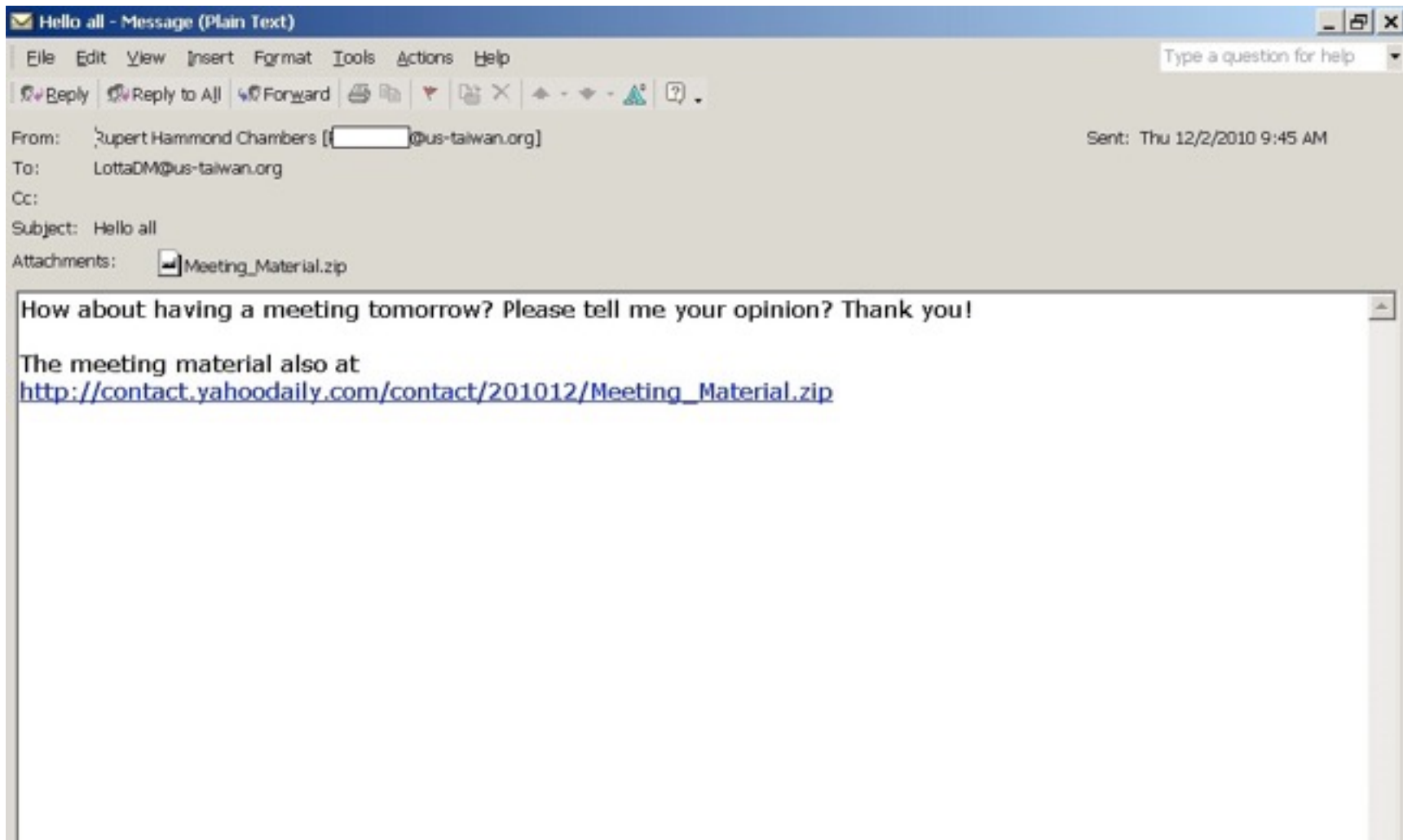
- Spoofed Email
 - From a “real” person
- Content of the message
 - Real events
- Document attachments?

Trends

- Forwarding 'legitimate' emails with malware
- Sending two or more attachments
 - the first clean, next malware
- Leveraging authority relationships
 - Spoofing governmental email addresses



Source: contagiodump.blogspot.com



Taiwan news media report of Dalai Lama(2010) - Message (HTML)

File Edit View Insert Format Tools Actions Help

Reply Reply to All Forward

You forwarded this message on 6/1/2010 9:29 AM. Click here to find all related messages.

From: [redacted] [danny2chy@hotmail.com] Sent: Mon 5/31/2010 4:05 AM

To: [redacted]@ceip.org; [redacted]@mail.house.gov; [redacted]@mail.house.gov; [redacted]@naswdc.org; [redacted]@asiasoc.org; [redacted]@microsicare.net; [redacted]@mail.house.gov; [redacted]@mail.house.gov; [redacted]@verizon.net; [redacted]@exchange.sba.miami.edu; [redacted]@yahoo.com; [redacted]@carnegieendowment.org; [redacted]@dudinskyassociates.com; [redacted]@law.upenn.edu; [redacted]@verizon.net; [redacted]@brookings.edu; [redacted]@imwithfred.com; [redacted]@aol.com; [redacted]@mindspring.com; [redacted]@americangaming.org; [redacted]@voanews.com; [redacted]@state.gov;

Cc:

Subject: Taiwan news media report of Dalai Lama(2010)

Attachments: Details.rar (84 KB)

Dear Friends,

Taiwan news media report that Dalai Lama, spiritual leader of Tibetan Buddhism is scheduled to arrive Taiwan in the afternoon of August 15, 2010.

President Ma approved the invitation on humanitarian and religious reasons. On the other hand, the Taiwan Affairs Office of Mainland China's State Council released a statement, opposing to Dalai Lama's visit.

Details are at Annex.

With best regards,

Jacob Chang

start: 0000-00-00 end: 0000-00-00

Hotmail 強大的垃圾郵件管理功能，值得你信賴。 [馬上註冊](#)

TREND MICRO

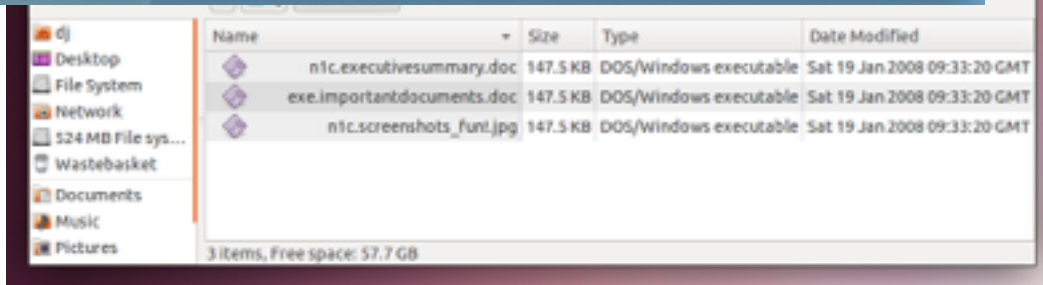
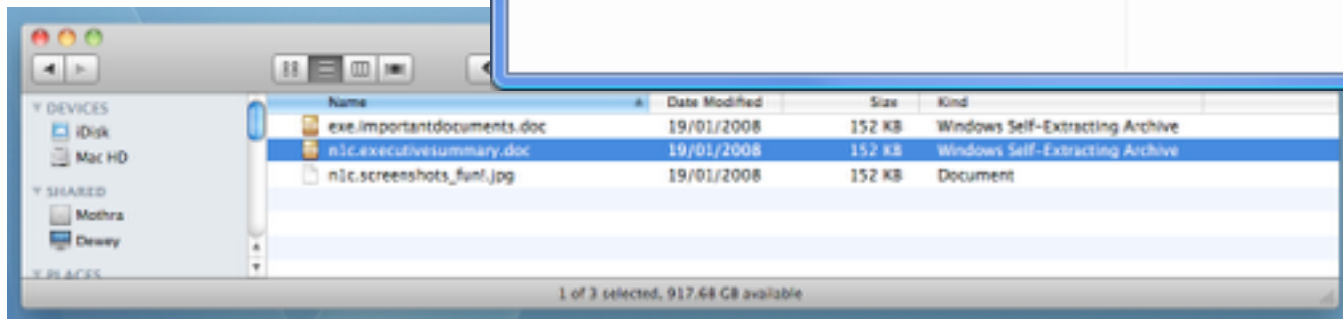
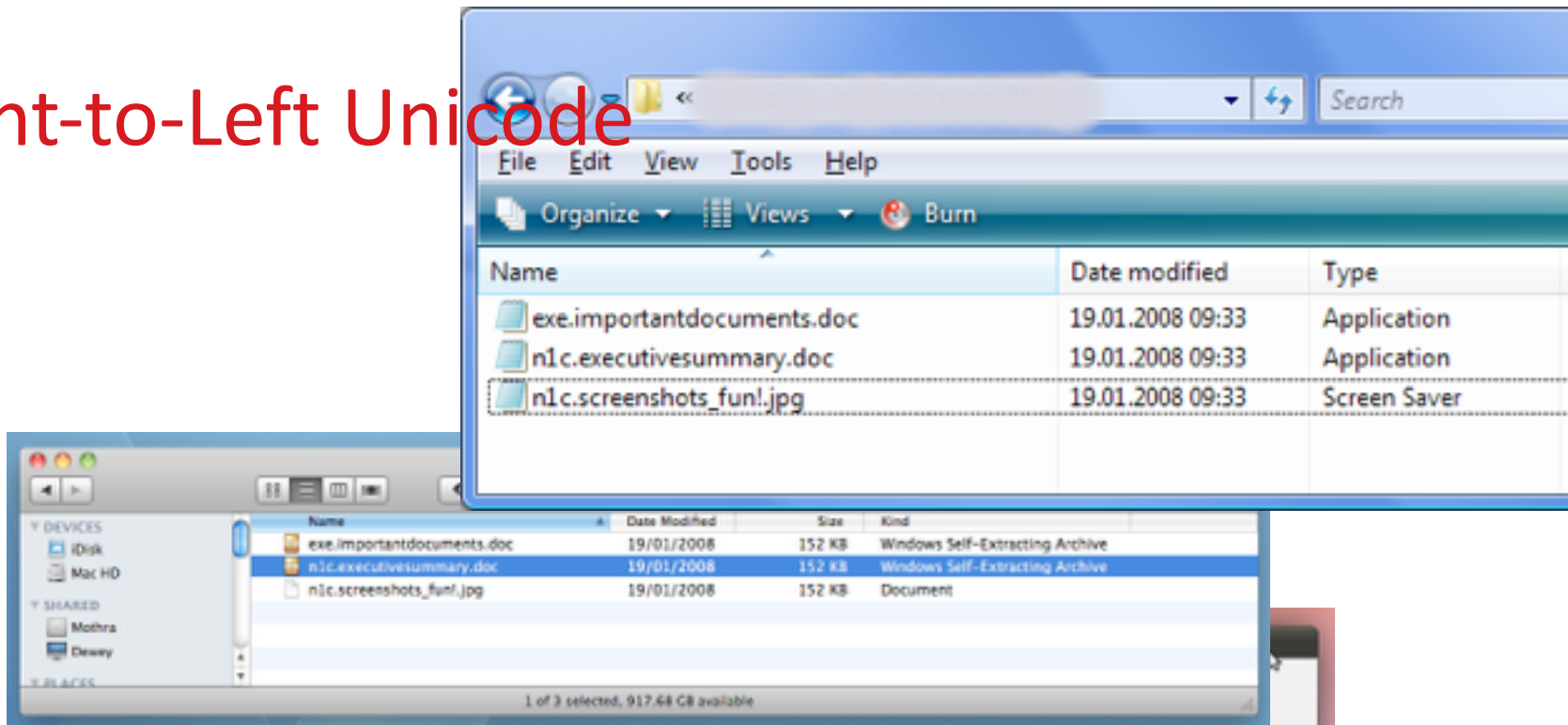
Delivery

- Decide on who/what to target
- Decide on Social Engineering approach
- Decide on delivery mechanism for malware
 - E.g. Email, IM, Twitter, other social media
 - E.g. via a PDF document

Trends

- Malicious attachments via socially engineered email
 - pdf, doc, xls, ppt
- Links to web pages hosting malware inside of compressed files via Email or IM
 - .zip, .rar,
 - sometimes password protected
- “folder” icons that are really executables
- Webinjects on legitimate webpages
 - often contextually relevant to the victim
- Use of right-to-left Unicode hole to disguise executables

Right-to-Left Unicode



Source: h-online.com

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>

Compromise/Exploit

- Goal: deliver control of system to attacker
- Tailor malware to target
- Execute the malware
- Take control

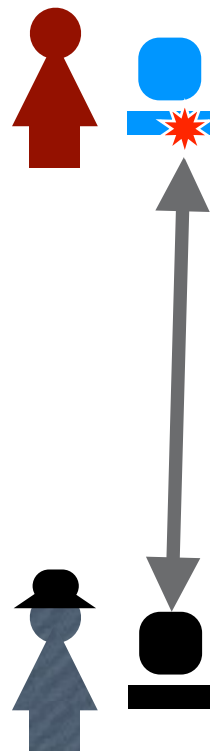
Trends

- Use exploits in
 - Gmail/IE (MHTML)
 - Yahoo! Mail (XSS)
 - Hotmail (XSS)
- Vulnerabilities exploited:
 - Adobe PDF Reader
 - Adobe Flash, embedded
 - MS DOC and XLS

Not always 0-days!

TA Command and Control

- Control acts as a 'phone-home'
- Command issues commands to the target machine
- Compromised machine is directly controlled
- C&C system informs remote access tool (RAT) where to connect to and when to lie dormant

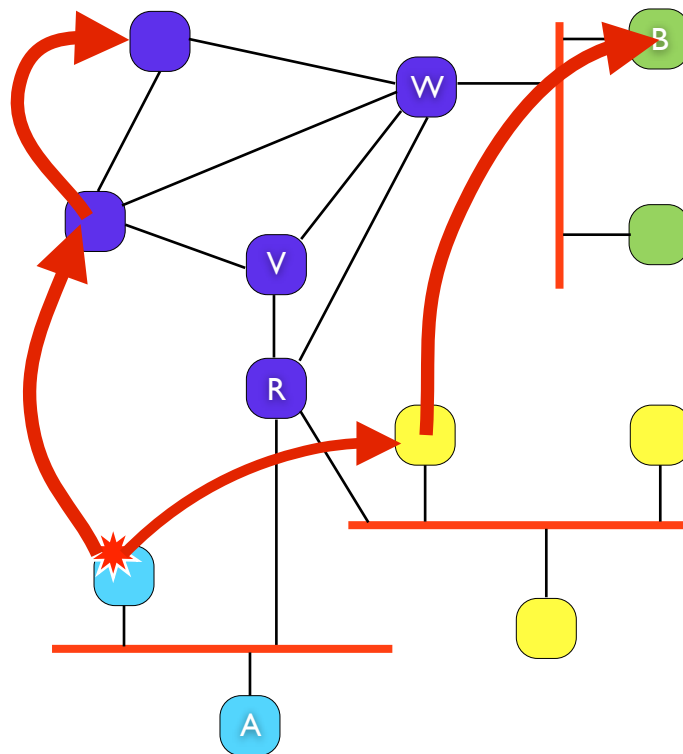


Flying under the radar

- Cloud-based command and control
- Use of intermediaries such as blogs
- SSL encrypted webmail services
- The use of stolen or forged SSL certificates
- Vetting Malware with CAVs (Criminal Antivirus Scanning services)

Persistence/Lateral Movement

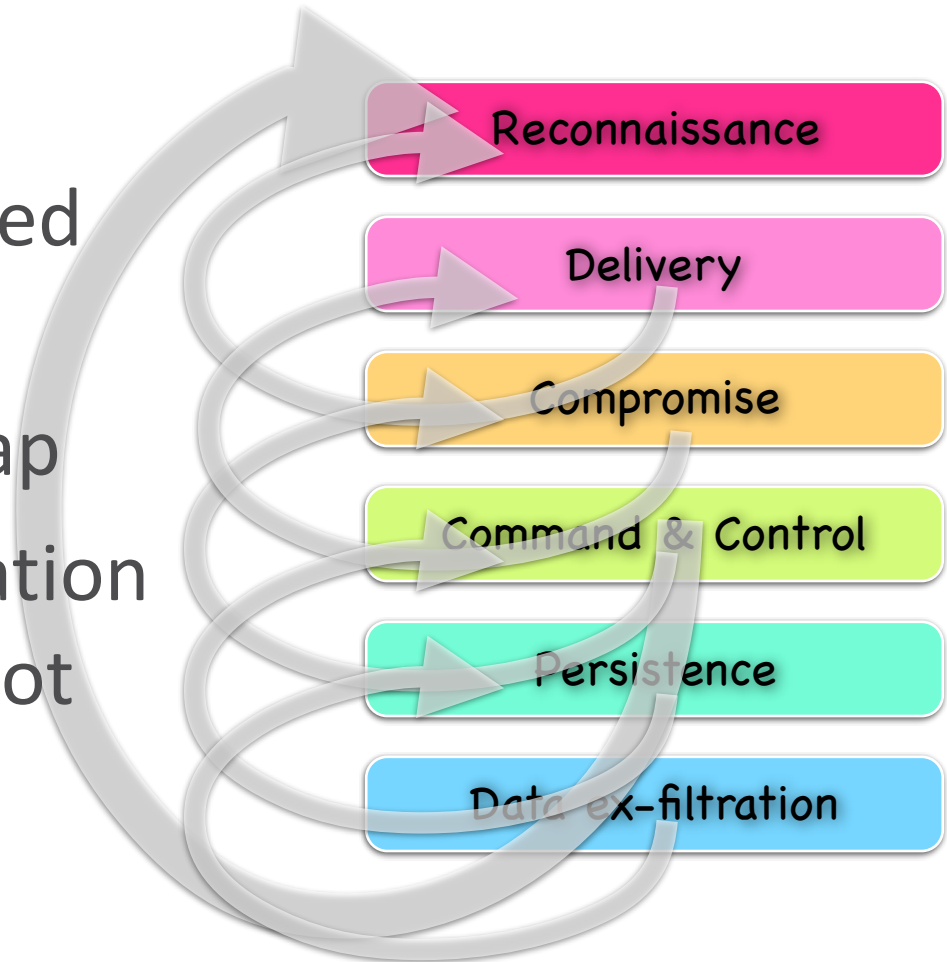
- Ensure malware survives a reboot
- Continued remote access
 - e.g. VPN credentials
 - e.g. More backdoors
- Explore and infect more machines:
 - more remote access
 - more access to sensitive information



Data ex-filtration

- Transmitting sensitive information
 - encryption
 - compression
 - chunking

- These stages feed on each other
- And they overlap
- A target occupation of 600 days is not that unusual



Ex: Ghostnet

GhostNet

- Targeted email
 - Word exploit
 - sent to members of the Dalai Lama's office
- Relevant enough to get redistributed by the victims
- Over time these emails got more sophisticated
 - Recycling legitimate email
 - Inserting email into active conversations
- 8 different trojans used!

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, "to share of the voluntary contribution into the Tibetan Freedom Movement Receipt book. This resolution was later reaffirmed by the 11th Tibetan People's 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	-	-	HW97:CVE-2006-2492
eTrust-Vet	-	-	V97H/SmartTags!exploit
F-Prot	-	-	CVE-2006-2492
Fortinet	-	-	MSWord/ObjPointer.At!exploit.M20062492
OData	-	-	HW97:CVE-2006-2492
Ikarus	-	-	Virus.HW97.CVE.2006.2492
Microsoft	-	-	Exploit:Win32/Wordjnp.gen
Sophos	-	-	Troj/MalDoc-Fan
Webwasher-Gateway	-	-	Exploit.Word.Dropper.Gen

source: Nart Villeneuve/Trend



Filter: tcp.stream eq 717

Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Info
32858	4195.032862	192.168.0.4	218.77.188.70	TCP	4284 > http [SYN] Seq=0 Win=32768 Len=0 MSS=1460
32859	4195.470873	218.77.188.70	192.168.0.4	TCP	http > 4284 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1452
32860	4195.470918	192.168.0.4	218.77.188.70	TCP	4284 > http [ACK] Seq=1 Ack=1 Win=32768 Len=0
32861	4195.470945	192.168.0.4	218.77.188.70	HTTP	GET /ld/queenfun/v1/onLine.php?c=RGVzYW50U11TVEVNSs=200712221103647R97025916p=HTKyLJE20C4wLj0=6Hl=2wsdf351 HTTP/1.0
32862	4196.085444	218.77.188.70	192.168.0.4	HTTP	HTTP/1.1 200 OK (text/html)
32863	4196.086194	218.77.188.70	192.168.0.4	TCP	http > 4284 [FIN, ACK] Seq=105 Ack=199 Win=65535 Len=0
32864	4196.086236	192.168.0.4	218.77.188.70	TCP	218.77.188.70 > 192.168.0.4 [ACK] Seq=199 Ack=105 Win=0 Len=0
32865	4196.015937	192.168.0.4	218.77.188.70	TCP	218.77.188.70 > 192.168.0.4 [ACK] Seq=199 Ack=105 Win=0 Len=0
32866	4196.452812	218.77.188.70	192.168.0.4	TCP	218.77.188.70 > 192.168.0.4 [ACK] Seq=105 Ack=199 Win=0 Len=0

Follow TCP Stream

Stream Content

```

GET /ld/queenfun/v1/onLine.php?c=RGVzYW50U11TVEVNSs=200712221103647R97025916p=HTKyLJE20C4wLj0=6Hl=2wsdf351 HTTP/1.0
User-Agent: Mozilla/4.0 (compatible; )
Accept: */*
Host: www.ibmunion.net

HTTP/1.1 200 OK
Date: Wed, 10 Sep 2008 07:18:57 GMT
Server: Apache/2.2.4 (Unix)
Content-Length: 15
Connection: close
Content-Type: text/html

```

04872000

Find Save As Print Entire conversation (362 bytes)

 ASCII
 EBCDIC
 Hex Dump
 C Arrays
 Raw

Help

Filter Out This Stream

Close

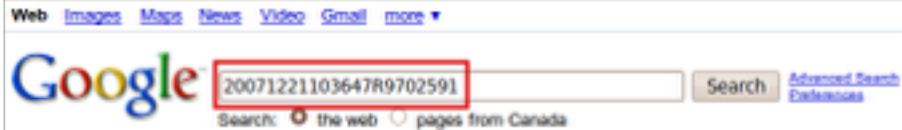
- Frame 32861 (252 bytes on wire, 252 bytes captured)
- Ethernet II, Src: AsustekC_02:0d:c1 (00:13:c2:02:0d:c1), Dst: 192.168.0.4
- Internet Protocol, Src: 192.168.0.4, Dst: 218.77.188.70
- Transmission Control Protocol, Src Port: 4284, Dst Port: 80
- Hypertext Transfer Protocol

```

0000 00 09 5b a8 b9 9e 00 13 04 02 0d c1 08 00 43 00  ..z0... (...M
0010 00 ee 7a 11 40 00 80 06 28 b8 c0 a8 00 04 da 4d  ..F..P).f..'.P.
0020 bc 46 10 bc 00 50 7d 0e 90 66 e4 c8 27 eb 50 18  ..X!..0E T /ld/qu
0030 00 00 50 21 00 00 47 45 54 20 2f 6c 64 2f 71 75  eenfun/v1/onLine
0040 65 65 6e 66 75 6e 2f 76 31 2f 6f 6e 6c 69 6e 65  _php?c=RGVzYW50
0050 2e 70 60 70 3f 63 3d 52 47 56 7a 59 57 35 6e 26  u=U11TVEVNSs=200
0060 75 30 55 31 6c 54 56 45 56 4e 26 73 3d 32 30 30  71221103 647R9702
0070 37 31 32 32 31 31 30 33 36 34 37 52 39 37 30 32  5916p=HTKyLJE20C
0080 35 39 31 26 70 3d 4d 54 6b 79 4c 6a 45 32 4f 43  4wLj0=6Hl=2wsdf3
0090 34 77 4c 6a 51 3d 26 68 69 3d 32 77 73 64 66 33  51 HTTP/1.0. Use
00a0 35 31 20 48 54 54 50 2f 31 2e 30 0d 0a 55 73 65  r-Agent: Mozilla
00b0 72 2d 41 67 65 6e 74 3a 20 4d 6f 7a 69 6c 6c 61  /4.0 (compatible;
00c0 2f 34 2e 30 20 28 63 6f 6d 70 61 74 69 62 6c 65  ;).Accept: */*
00d0 3b 20 29 0d 0a 41 63 63 65 70 74 3a 20 2a 2f 2a  ;).Accept: */*

```

Google is your friend!



Web

[待发送指令列表](#)

20071221103647R9702591, 2009-02-14, 11-30-13, 20081111155839 ...

[good-blog.com/ZhINvDT202/showcmdinfo.php - 29k - Cached - Similar pages](#)

[待发送指令列表](#)

20071221103647R9702591, 2009-01-22, 22-10-29, 20081111155839 ...

[good-blog.com](#)

[More results for](#)

In order to show you
if you like, you can

Web [Images](#) [Maps](#) [News](#) [Video](#) [Gmail](#) [more](#) ▼

Google

[Advanced Search](#)
[Preferences](#)

Web

[Microsoft Corporation](#)

Microsoft = Silverlight delivers a new generation of high-quality audio and video, e= ngaging media experiences, and interactive applications for the Web. ...

[good-blog.com/ - 597k - Cached - Similar pages](#)

[服务端列表](#) - [[Translate this page](#)]

注册日期, 注册时间, 登录日期, 登录时间, 唯一标记, 外网IP, 内网IP, 主机名, 当前用户名, 发送指令地址, 开始时间, 2008-08-20, 17:09:02, 2008-12-18, 19:22:27 ...

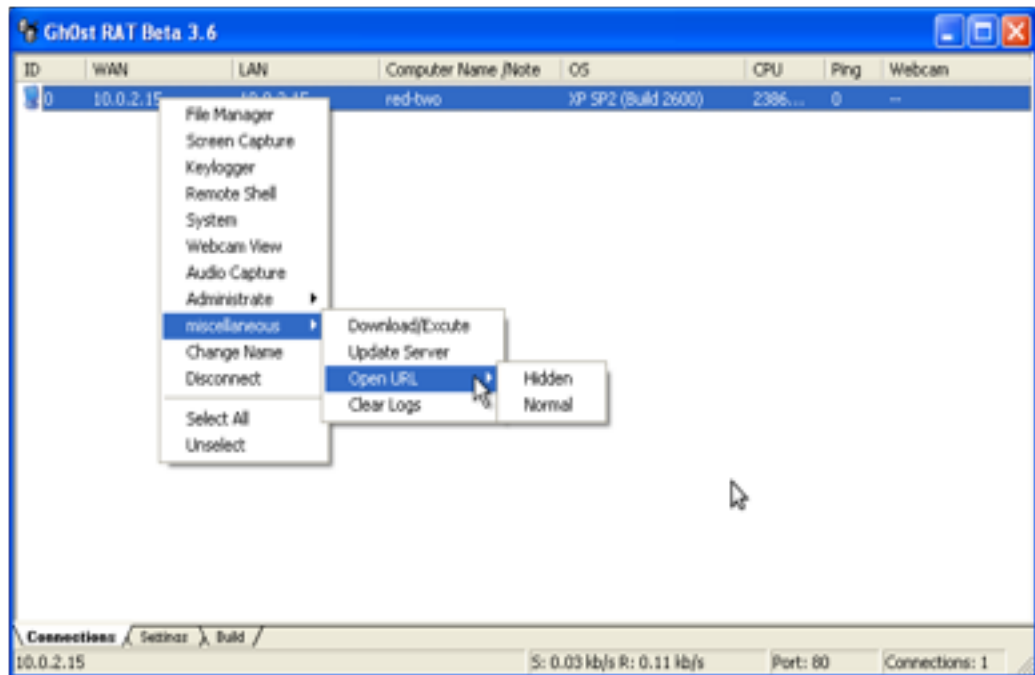
[good-blog.com/ZhINvDT201/Serverlist.php - 37k - Cached - Similar pages](#)

当前服务器时间: Sunday 08th of March 2009 08:28:22 AM 共有注册用户92

注册日期	注册时间	登录日期	登录时间	唯一标记	外网IP	内网IP	主机名	当前用户名	发送指令地址	开机时长
2008-08-24	18:30:03	2008-08-25	19:55:12	20080416110157R3753815				SYSTEM	Send Command	0
2008-08-26	20:23:04	2008-09-03	02:39:36	20080520085720R2050748				SYSTEM	Send Command	536
2008-08-24	18:34:18	2008-08-27	02:49:23	20080612002936R7867410				SYSTEM	Send Command	537
2008-08-26	20:36:38	2008-11-26	00:23:25	20080615184105R9914356				SYSTEM	Send Command	2
2008-08-26	20:19:04	2008-10-23	18:31:15	20071212172154R4299769				SYSTEM	Send Command	1
2008-08-25	07:17:19	2008-08-25	16:44:59	20080605170355R4980676				SYSTEM	Send Command	568
2008-10-27	09:40:55	2008-11-10	18:22:24	20081023130810R8994851				SYSTEM	Send Command	0
2008-11-13	21:38:46	2008-11-18	19:12:09	2008111103243R6675372				SYSTEM	Send Command	0
2008-08-31	01:48:45	2009-03-08	08:12:14	20071210082410R9814790				SYSTEM	Send Command	472
2008-09-04	23:43:25	2008-09-09	02:05:07	20080703232822R6552940				SYSTEM	Send Command	151
2008-08-26	20:20:09	2009-03-05	19:45:23	20080111091234R9085443				SYSTEM	Send Command	349
2008-08-26	22:40:33	2008-08-27	22:54:43	20080310205648R5877214				SYSTEM	Send Command	3
2008-08-20	17:18:38	2009-01-11	22:52:01	20071207170830R5666692				SYSTEM	Send Command	106
2009-01-14	19:08:10	2009-02-04	21:53:13	20080114165816R8595555				SYSTEM	Send Command	77
2008-08-26	22:01:31	2009-03-06	16:47:22	20080102114619R2089949				SYSTEM	Send Command	78
2008-09-18	07:43:43	2008-11-04	07:04:21	20080918063420R6130419				SYSTEM	Send Command	22
2008-09-09	02:59:00	2009-03-08	01:10:43	20080227151807R5907262				SYSTEM	Send Command	8
2008-09-04	01:47:33	2008-12-02	04:59:50	20080902210935R2341663				SYSTEM	Send Command	1
2008-12-02	05:21:19	2008-12-02	05:22:19	20081202052118R7082861				SYSTEM	Send Command	24
2008-09-11	19:30:54	2009-03-08	08:11:54	20080911190533R1727438				SYSTEM	Send Command	12181
2008-08-26	20:24:47	2008-10-06	01:57:18	20080403151159R8609279				SYSTEM	Send Command	171
2008-09-18	07:41:58	2009-03-06	10:11:30	20080918063335R4699286				SYSTEM	Send Command	263
2008-08-26	22:30:19	2008-09-15	03:45:34	20071212172958R4560900				SYSTEM	Send Command	128
2008-08-26	20:15:04	2008-11-03	12:10:09	20071221085134R4426370				SYSTEM	Send Command	4536
2008-09-21	23:30:03	2008-12-02	00:45:08	20080918072634R1160528				SYSTEM	Send Command	21
2008-09-18	07:47:17	2008-11-20	01:12:38	20080918072156R2712160				SYSTEM	Send Command	47
2008-08-26	20:33:10	2009-03-06	01:41:06	20080519082934R2793725				SYSTEM	Send Command	563
2008-08-27	02:05:46	2008-12-25	18:48:23	20080319104141R6977495				SYSTEM	Send Command	1
2008-09-08	18:30:11	2009-02-27	07:15:40	20080908174344R9839881				SYSTEM	Send Command	13166
2008-08-20	17:15:23	2009-01-12	18:32:01	20071210091020R4980211				SYSTEM	Send Command	352

81	2009-03-06	00:51:16	20080421075613R8923674		192.168.11.108			SYSTEM	Send Command	496
01	2009-03-06	02:37:21	20080114165935R9101265		172.19.8.151			SYSTEM	Send Command	426
11	2008-09-10	20:54:16	20071221103647R9702591		192.168.0.4			SYSTEM	Send Command	64
19	2009-03-06	06:56:34	20080310162314R9261967		192.168.0.15			SYSTEM	Send Command	460

sid	cmd
0720040208091558468070000000	ghv1.jpg@SystemRoot%\goroot.exe@67693128ad9ff8928ec4c81323692f8c@
0720040208091558468070000000	'sy.jpg@SystemRoot%\Soundriver.exe@672b73197f9524b36e9523454791463f@
0720040208091558468070000000	hqt.jpg@SystemRoot%\installer.exe@7ecf160082fb224829737231d1fdb436@
0720080428110239186070000000	l.jpg@SystemRoot%\winlogon.exe@5d1d85f6cd2012c2a83ffb7733e5f88@
0720080428110239186070000000	rdsdm.jpg@SystemRoot%\netdsd.exe@7c0a705f5976133da39656b94ca713f@
0720080428110239186070000000	rdsdm.jpg@SystemRoot%\netdsd.exe@7c0a705f5976133da39656b94ca713f@
0720080429092019500070000000	l.jpg@SystemRoot%\winlogon.exe@5d1d85f6cd2012c2a83ffb7733e5f88@
0720080508164004578070000000	l.jpg@SystemRoot%\winlogon.exe@5d1d85f6cd2012c2a83ffb7733e5f88@
0720080508164004578070000000	rdsdm.jpg@SystemRoot%\netdsd.exe@7c0a705f5976133da39656b94ca713f@
0720080508164004578070000000	rdsdm.jpg@SystemRoot%\netdsd.exe@7c0a705f5976133da39656b94ca713f@
0720080508164004578070000000	edit.jpg@SystemRoot%\gpedit.exe@65a3a52f14b2a2aae96e2722ad19899b@
0720080508164004578070000000	gh.jpg@SystemRoot%\ghost.exe@71c62ff0dd3ab02919a8b446193249f5@
0720080508164004578070000000	ost.jpg@SystemRoot%\winlogon.exe@73afd9c696ed161cab40eac130e98e8a@
0720080508164004578070000000	ost.jpg@SystemRoot%\winlogon.exe@73afd9c696ed161cab40eac130e98e8a@
0720080508164004578070000000	gh.jpg@SystemRoot%\ghost.exe@71c62ff0dd3ab02919a8b446193249f5@
0720080508164004578070000000	hqt.jpg@SystemRoot%\installer.exe@7ecf160082fb224829737231d1fdb436@
0720080508164004578070000000	gh.jpg@SystemRoot%\ghost.exe@71c62ff0dd3ab02919a8b446193249f5@
0720080508164004578070000000	'sy.jpg@SystemRoot%\Soundriver.exe@672b73197f9524b36e9523454791463f@
0720080508164004578070000000	hqt.jpg@SystemRoot%\installer.exe@7ecf160082fb224829737231d1fdb436@
0720080508164004578070000000	gh.jpg@SystemRoot%\ghost.exe@71c62ff0dd3ab02919a8b446193249f5@
0720080508164004578070000000	gh.jpg@SystemRoot%\ghost.exe@71c62ff0dd3ab02919a8b446193249f5@
0720080508164004578070000000	ghv1.jpg@SystemRoot%\goroot.exe@67693128ad9ff8928ec4c81323692f8c@
0720080508164004578070000000	ghv1.jpg@SystemRoot%\goroot.exe@67693128ad9ff8928ec4c81323692f8c@
0720080508164004578070000000	'sy.jpg@SystemRoot%\Soundriver.exe@672b73197f9524b36e9523454791463f@
0720080508164004578070000000	hqt.jpg@SystemRoot%\installer.exe@7ecf160082fb224829737231d1fdb436@
0720080508164004578070000000	hqt.jpg@SystemRoot%\installer.exe@7ecf160082fb224829737231d1fdb436@
0720080508164004578070000000	ghv1.jpg@SystemRoot%\goroot.exe@67693128ad9ff8928ec4c81323692f8c@
0720080508164004578070000000	'sy.jpg@SystemRoot%\Soundriver.exe@672b73197f9524b36e9523454791463f@
0720080508164004578070000000	hqt.jpg@SystemRoot%\installer.exe@7ecf160082fb224829737231d1fdb436@
0720080508164004578070000000	ghv1.jpg@SystemRoot%\goroot.exe@67693128ad9ff8928ec4c81323692f8c@



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?
- Botnets stand in contrast
 - no persistent, active control
 - no specific targeting

Challenges

Low Distribution / High Impact

Computer Spies Breach Fighter-Jet Project

By: **HOBAN GORMAN, AUGUST COLE and YOUNG BREAZEN**

WASHINGTON - Computer spies have broken into the Pentagon's \$300-million Joint Strike Fighter program - the Defense Department's costliest weapons program ever - according to current and former government officials familiar with the attacks.

Similar incidents have also breached the Air Force's stealthy combat system in recent months, these people say. In the case of the fighter jet program, the intruders were able to copy and upload all several terabytes of data related to design and electronics systems, officials say, potentially making it easier to defend against the cost.

The latest intrusions provide new evidence that a battle is heating up between the U.S. and potential adversaries over the data networks that tie the world together. The intrusions follow a recent Wall Street Journal report that computers used to control the U.S. electrical distribution

Open Letter to RSA Customers

Like any large company, EMC experiences and successfully repels multiple cyber attacks on its IT infrastructure every day. As a result, we have developed an extremely sophisticated and robust system designed to continuously update and defend against RSA. We have a variety of approaches that we employ to protect our business and our customers, all backed up by our IT infrastructure. We also receive intelligence on the attacks and are working closely to address them.

Your investigation has led us to believe that the other advanced threat actors (APT) that are targeting RSA are also targeting RSA customers. We are recommending the advice to RSA customers and providing guidance and information that is useful to you.

GREG WESTON: Foreign hackers attack Canadian government

Computer systems at 3 key departments probed

An unprecedented intrusion on the Canadian government this spring led to a "major" security review, says a senior government official, according to a report by CBC News.

The attack, apparently from China, also gave foreign hackers access to highly sensitive information, including the names of the

EU institutions hit by 'major' cyber attack

The institutions have taken action to prevent the spread of sophisticated information (APT) attacks.

LEADER ANALYSIS

23/05/2014 @ 16:24 CEST

STRASBOURG - (EPA) - The European Commission and the External Action Service have been hit by a "major" cyber attack ahead of a key EU summit - which critical decisions on the future structure of the bloc, possible accession strategies and the ongoing war in Libya are to be discussed.

The commission will not comment on the nature of the attacks but to security officials, the confirmed the institutions are indeed the focus of a serious strike. Meanwhile officials are comparing the attack to an assault on the French finance ministry last year ahead of a G20 meeting.

"We're regularly hit by cyber attacks, but this one's a bit different. It's a bit more sophisticated than the others that we did not want to comment on."

The cyber attack was by "hackers" and used to get at sensitive information that both the commission and EU member states are working to protect.

The commission is currently attempting to assess the impact to prevent the "leakage of sensitive information" and to "ensure the continuity of the institution's services."

All staff have been asked to change their passwords and to ensure

A new approach to China

2/12/2010 03:00:00 PM

Like many other well-known organizations, we face cyber attacks of varying degrees of regularity. In mid-December, we detected a highly sophisticated and targeted attack against infrastructure originating from China that resulted in the theft of intellectual property from Google. However, it soon became clear that what at first appeared to be solely a data incident - about a significant one-way something gone awry.

First, this attack was not just on Google. As part of our investigation we have discovered at least twenty other large companies from a wide range of businesses - including the IT finance, technology, media and chemical sectors - have been similarly targeted. We are currently in the process of notifying these companies, and we are also working with the relevant U.S. authorities.

Second, we have evidence to suggest that a primary goal of the attackers was access to Gmail accounts of Chinese human rights activists. Based on our investigation to date we believe these attacks did not achieve that objective. Only two Gmail accounts appear to have been accessed, and that activity was limited to account information (such as the date the account was created) and subject line, rather than the contents of emails themselves.

French gov't gives more details of hack: 150 PCs compromised

150 French National IT Systems Security Agency computers further details of the recent attack on French government computers, saying they were targeted by cyberattacks.

Around 100 IT staff spent the weekend on a mission-critical operation to undo the effects of the attack on computers at the French Ministry of

Chinese hackers stole S. Korean documents on spy drone

SEOUL, South Korea - Chinese hackers allegedly broke into a computer network early last week, stealing sensitive South Korean government documents on a spy drone, according to the United States, an opposition newspaper has reported.

The alleged hacking occurred in June last year, and the South Korean government has not said the state with the Chinese government because of a pending dispute, the Yonhap news outlet said.



Challenges

- Traditional anti-virus solutions not well adapted to the targeted threat
- The onus is on the defender to analyze it
- More comprehensive defense mechanisms!

Let's back up a little...

1928



1931



Entscheidungsproblem
is unsolvable

1936



Halting Problem

1984



Virus Property

Entscheidungsproblem

*Wir müssen wissen.
Wir werden wissen.*

Limits of computer security

- Much early security research focussed on mainframes in a Malware-free world
- The security models are not applicable to our world
- No alternatives have come to light
- Security becomes a trade-off

Why do we care?

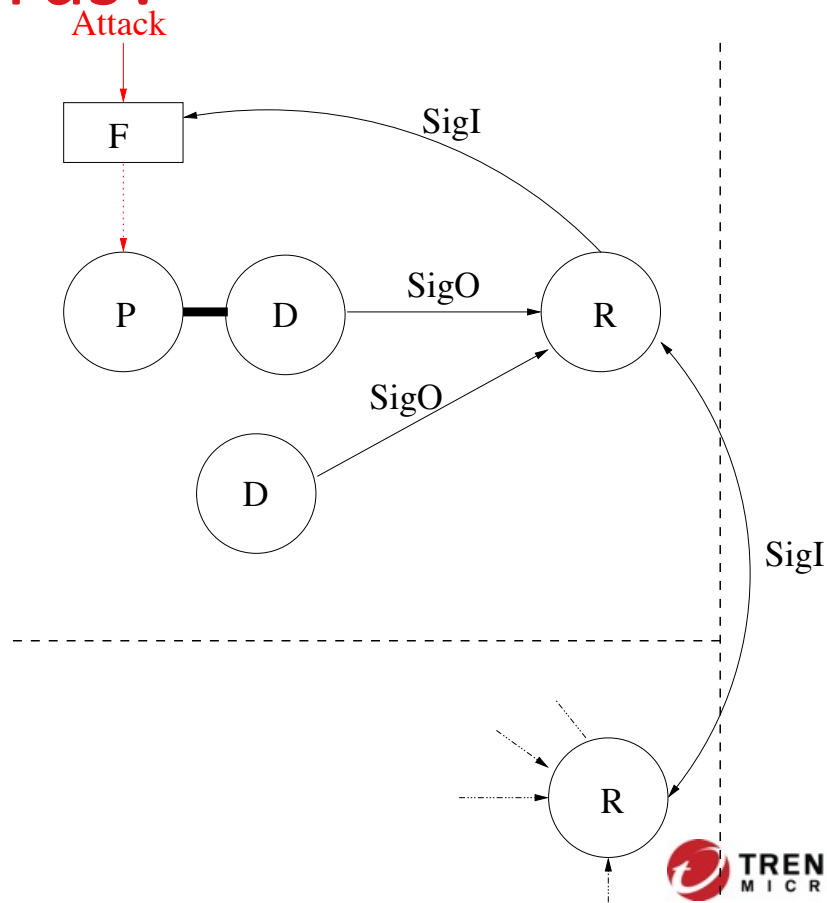
- Can't create universal Malware detection
- In practice, we can't create the security we crave and still do business
- Confidentiality, Integrity, Availability and Safety in conflict

Knowing this, what can we do?

- Heuristics
- Apply our knowledge
 - Productize our knowledge
- You need to be able to use the tools provided

What is a modern Antivirus?

- A detection engine
- An ecosystem
- A comprehensive solution



Reversing

Looking at Malware

- Why?
 - Detection alone is not enough
 - Sometimes understanding is vital
- Where does manual analysis fit in?

Disassembling/reversing

- Take the binary machine code
- Produce something humans can understand
- Extract information to use in threat analysis

```

crackme0x00.exe
0  4D5A9000 03000000 04000000 FFFF0000  MZé  --
16 B8000000 00000000 40000000 00000000  ||  e
32 00000000 00000000 00000000 00000000
48 00000000 00000000 00000000 80000000  Å
64 0E1FBA0E 00B409CD 21B8014C CD215468  f  ¥  Ö!|| LÖ!Th
80 69732070 726F6772 616D2063 616E6E6F  is program canno
96 74206265 2072756E 20696E20 444F5320  t be run in DOS
112 6D6F6465 2E0D0D0A 24000000 00000000  mode. $
128 50450000 4C010500 191D6347 002E0000  PE L  cG .
144 22020000 E0000703 0B010238 00200000  "  †  §
160 002A0000 00020000 60120000 00100000  +
176 00300000 00004000 00100000 00020000  0  e
192 04000000 01000000 04000000 00000000
208 00700000 00040000 179C0000 03000000  p  ú
224 00002000 00100000 00001000 00100000
240 00000000 10000000 00000000 00000000
256 00600000 80030000 00000000 00000000  Å
272 00000000 00000000 00000000 00000000
288 00000000 00000000 00000000 00000000
304 00000000 00000000 00000000 00000000
320 00000000 00000000 00000000 00000000
336 00000000 00000000 00000000 00000000
352 00000000 00000000 00000000 00000000
368 00000000 00000000 2E746578 74000000  .text
384 781E0000 00100000 00200000 00040000  x
400 00000000 00000000 00000000 60000060
416 2E646174 61000000 40000000 00300000  .data  @  @

Signed Int  big  (select some data)
0 out of 24440 bytes

```

```

2. makers_admin@FTR-01:~ (radare2)
[0x00401260]> pdf @ sym._main
/ (fcn) sym._main 141
; var int local_18h @ ebp-0x18
; var int local_1ch @ ebp-0x1c
; CALL XREF from 0x00401222 (sym._main)
0x00401310 55          push ebp
0x00401311 89e5       mov ebp, esp
0x00401313 83ec38    sub esp, 0x38
0x00401316 83e4f0    and esp, 0xffffffff
0x00401319 b0000000  mov eax, 0
0x0040131e 83c00f    add eax, 0xf
0x00401321 83c00f    add eax, 0xf
0x00401324 c1e804    shr eax, 4
0x00401327 c1e004    shl eax, 4
0x0040132a 8945e4    mov dword [ebp - local_1ch], eax
0x0040132d 8b45e4    mov eax, dword [ebp - local_1ch]
0x00401330 e83b190000 call fcn.00402c70
0x00401335 e836010000 call sym.__main
0x0040133a c7042404040. mov dword [esp], str.IOLI_Crackme_Level_0x00_n ; [0x40000:4]=0x494c4f49 LEA section.rdata ; "IOLI Crackme Level 0x00." @ 0x404000
0x00401341 e8ea190000 call sym.printf
0x00401346 c70424194040. mov dword [esp], str.Password: ; [0x404019:4]=0x73736
150 LEA str.Password: ; "Password: " @ 0x404019
0x0040134d e0de190000 call sym.printf
0x00401352 8d45e8    lea eax, [ebp - local_18h]
0x00401355 89442404 mov dword [esp + 4], eax
0x00401359 c70424244040. mov dword [esp], 0x404024 ; [0x404024:4]=0x32007325
; "%s" 0x00404024 ; "%s" @ 0x404024
0x00401360 e8bb190000 call sym.scanf
0x00401365 8d45e8    lea eax, [ebp - local_18h]
0x00401368 c74424042740. mov dword [esp + 4], str.250382 ; [0x404027:4]=0x3338
3532 LEA str.250382 ; "250382" @ 0x404027
0x00401370 890424    mov dword [esp], eax
0x00401373 e898190000 call sym.strcmp
0x00401376 85c0     test eax, eax
0x0040137a 740e     je 0x40138a
0x0040137c c704242e4040. mov dword [esp], str.Invalid_Password__ ; [0x40402e:
4]=0x61706e49 LEA str.Invalid_Password_n ; "Invalid Password!." @ 0x40402e
0x00401383 e8a8190000 call sym.printf
0x00401388 eb0c     jmp 0x401396
; JMP XREF from 0x0040137a (sym._main)
-> 0x0040138a c70424414040. mov dword [esp], str.Password_OK;__n ; [0x404041:4]=
0x73736150 LEA str.Password_OK;__n ; "Password OK :)." @ 0x404041
0x00401391 e89a190000 call sym.printf
; JMP XREF from 0x00401388 (sym._main)
-> 0x00401396 b0000000 mov eax, 0
0x0040139b c9       leave
0x0040139c c3       ret
[0x00401260]>

```


Address	Hex	Hex	Hex	Hex	Disassembly
0	4D5A9000	03000000	04000000	FFFF0000	MZé
16	B8000000	00000000	40000000	00000000	Π e
32	00000000	00000000	00000000	00000000	
48	00000000	00000000	00000000	80000000	Ä
64	0E1FBA0E	00B409CD	21B8014C	CD215468	ÿ ¥ Ô!Π LÔ!Th
80	69732070	726F6772	616D2063	616E6E6F	is program canno
96	74206265	2072756E	20696E20	444F5320	t be run in DOS
112	6D6F6465	2E0D0D0A	24000000	00000000	mode. \$
128	50450000	4C010500	191D6347	002E0000	PE L cG .
144	22020000	E0000703	0B010238	00200000	" † §
160	002A0000	00020000	60120000	00100000	* ' .
176	00300000	00004000	00100000	00020000	0 e
192	04000000	01000000	04000000	00000000	
208	00700000	00040000	179C0000	03000000	p ú
224	00002000	00100000	00001000	00100000	
240	00000000	10000000	00000000	00000000	
256	00600000	80030000	00000000	00000000	' Ä
272	00000000	00000000	00000000	00000000	
288	00000000	00000000	00000000	00000000	
304	00000000	00000000	00000000	00000000	
320	00000000	00000000	00000000	00000000	
336	00000000	00000000	00000000	00000000	
352	00000000	00000000	00000000	00000000	
368	00000000	00000000	2E746578	74000000	.text
384	781E0000	00100000	00200000	00040000	x
400	00000000	00000000	00000000	60000060	
416	2E646174	61000000	40000000	00300000	.data @ @

Signed Int big (select some data) - +

0 out of 24440 bytes

```

function sym._main () {
loc_0x401310:
push ebp
ebp = esp
esp -= 0x38
esp &= 0xfffffff0
eax = 0
eax += 0xf
eax += 0xf
eax >>= 4
eax <<= 4
dword [ebp - local_1ch] = eax
eax = dword [ebp - local_1ch]
fcn.00402c70 ()
sym.__main ()
dword [esp] = str.IOLI_Crackme_Level_0x00_n
sym._printf ()
dword [esp] = str.Password:
sym._printf ()
eax = [ebp - local_18h]
dword [esp + 4] = eax
dword [esp] = 0x404024
sym._scanf ()
eax = [ebp - local_18h]
dword [esp + 4] = str.250382
dword [esp] = eax
sym._strcmp ()
if (eax == eax
isZero 0x40138a) {
loc_0x40138a:
dword [esp] = str.Password_OK:__n
sym._printf () do {
loc_0x401396:
eax = 0
}
loc_0x401396:
eax = 0
} else {
goto loc_0x40137c
loc_0x40137c:
dword [esp] = str.Invalid_Password_n
sym._printf ()
goto 0x401396
}
}

```

Information we need

- Files/File patterns
- Internet resources
 - URLs, IP addresses, Domains
- System functions/Imports
- Strings

Understanding intent

- This is where a disassembly is required
- We need to be expert in
 - Assembler/CPU architecture
 - Operating System functionality
 - Other APIs

<http://www.eicar.org/download/eicar.com>

```
eicar.com
0 58354F21 50254041 505B345C 505A5835 X50!P%@AP[4\PZX5
16 3428505E 29374343 29377D24 45494341 4(P^)7CC)7}$EICA
32 522D5354 414E4441 52442D41 4E544956 R-STANDARD-ANTIV
48 49525553 2D544553 542D4649 4C452124 IRUS-TEST-FILE!$
64 482B482A H+H*
```

Signed Int big (select some data)

0 out of 68 bytes

```

0000:0100      58      pop ax
0000:0101     354f21  xor ax, @x214f
0000:0104      50      push ax
0000:0105     254041  and ax, @x4140
0000:0108      50      push ax
0000:0109     5b      pop bx
0000:010a     345c   xor al, @x5c
0000:010c      50      push ax
0000:010d     5a      pop dx
0000:010e     58      pop ax
0000:010f     353428  xor ax, @x2834
0000:0112      50      push ax
0000:0113     5e      pop si
0000:0114     2937   sub word [bx], si
0000:0116     43      inc bx
0000:0117     43      inc bx
0000:0118     2937   sub word [bx], si
< 0000:011a     7d24   jge @x140
| 0000:011c     45      inc bp
| 0000:011d     49      dec cx
| 0000:011e     43      inc bx
| 0000:011f     41      inc cx
| 0000:0120     52      push dx
| 0000:0121     2d5354  sub ax, @x5453
| 0000:0124     41      inc cx
| 0000:0125     4e      dec si
| 0000:0126     44      inc sp
| 0000:0127     41      inc cx
| 0000:0128     52      push dx
| 0000:0129     44      inc sp
| 0000:012a     2d414e  sub ax, @x4e41
| 0000:012d     54      push sp
| 0000:012e     49      dec cx
| 0000:012f     56      push si
| 0000:0130     49      dec cx
| 0000:0131     52      push dx
| 0000:0132     55      push bp
| 0000:0133     53      push bx
| 0000:0134     2d5445  sub ax, @x4554
| 0000:0137     53      push bx
| 0000:0138     54      push sp
| 0000:0139     2d4649  sub ax, @x4946
| 0000:013c     4c      dec sp
| 0000:013d     45      inc bp
| 0000:013e     2124   and word [si], sp
-> 0000:0140     48      dec ax
0000:0141     2b482a  sub cx, word [bx + si + 0x2a]

```

COM files were loaded to 0x100 in memory and just run (MS-DOS)

Computer science again

- There is a limit to what we can know
- Encryption/Packing
- Second stage files
- Environment-specific behavior

- And we haven't considered other file types

Sandboxing

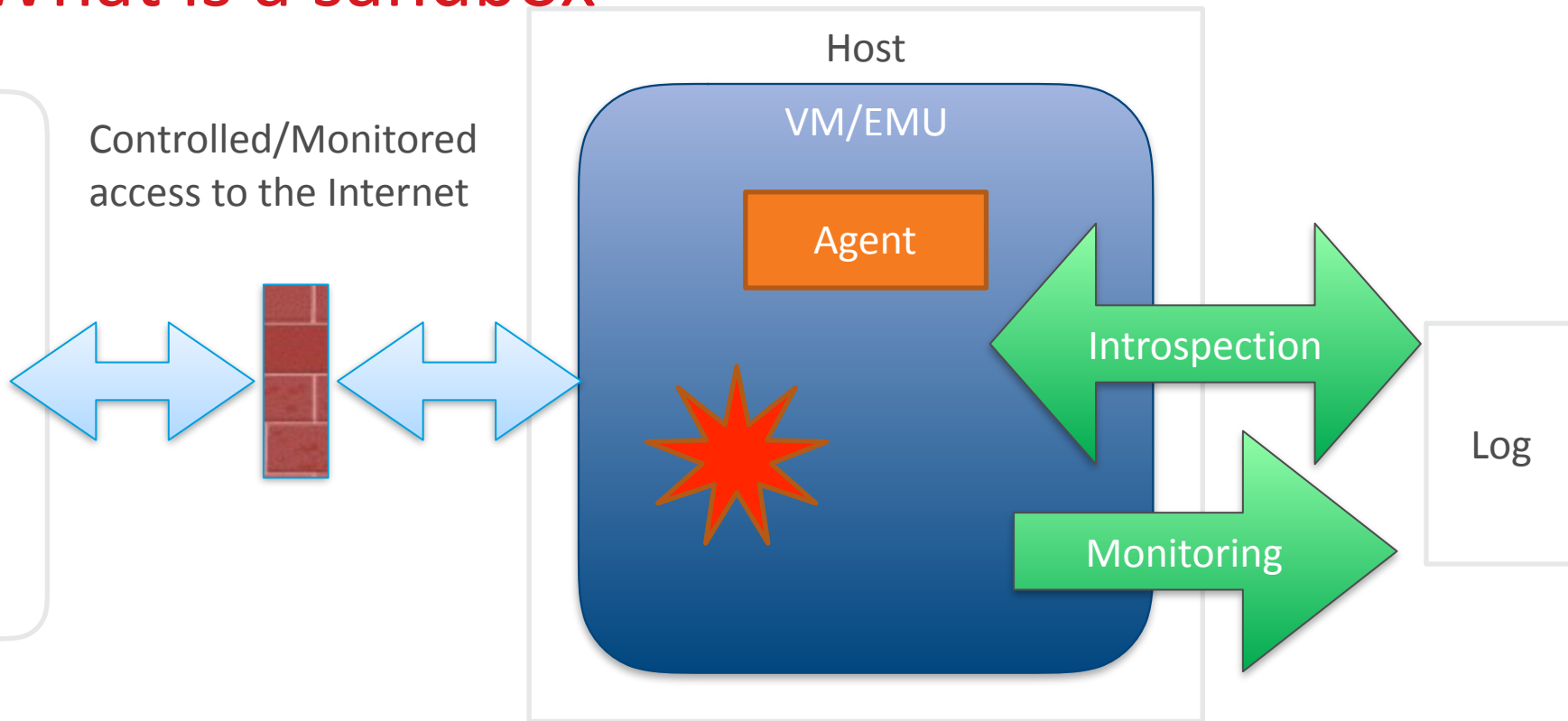
The Petri-dish idea

- Theory: we can understand Malware by observing it
- 1990: apply IDS ideas to low-level operations
- Later, encapsulated&instrumented environment built on an emulator

Sandboxes

- Usually VM-based
- Sometimes emulation-based
- Great selection
- But best if customizable

What is a sandbox



Analysis

CATEGORY	STARTED	COMPLETED	DURATION
FILE	2016-06-14 01:26:05	2016-06-14 01:35:22	557 seconds

File Details

FILE NAME	vv.exe
FILE SIZE	347136 bytes
FILE TYPE	PE32 executable (GUI) Intel 80386, for MS Windows
MD5	c49771018fbaae4bee8bd3bd3a2be169
SHA1	2335a5f8ebe8ee224373a84dac368e7a342a852a
SHA256	a615aaa82b091730662039982f66637a14e3ec079c2a07acd8f09a0bd3af84de
SHA512	583225b2be46e8a55c884ef446180acdee07bcd2e237fcd12a297bd4e18e07b5babfa1389fe1dc81b6f8c232f6825a38117e5919999ab98330e764b9497bb526
CRC32	B3A6B823
SSDEEP	6144:dda07CV/DBqjQLGdgN4soCo6i10ib+rBhez37rQ8v4nbXA:dR7CV/DBqjQasbb7mb+rBhezgXrv4
YARA	None matched

Hosts

IP
8.8.8.8
103.7.30.86
98.126.216.51

Domains

DOMAIN	IP
users.qzone.qq.com	103.7.30.86

Files

Registry Keys

Mutexes

C:\WINDOWS\Registration\R0000000000007.clb

C:\WINDOWS\system32\msscript.ocx

Summary

Files

Registry Keys

Mutexes

```
HKEY_LOCAL_MACHINE\Software\Microsoft\COM3
HKEY_USERS\S-1-5-21-1547161642-507921405-839522115-1004_Classes
HKEY_LOCAL_MACHINE\Software\Classes
\REGISTRY\USER
HKEY_LOCAL_MACHINE\Software\Classes\CLSID
HKEY_CLASSES_ROOT\ScriptControl
HKEY_CLASSES_ROOT\ScriptControl\CLSID
CLSID\{0E59F1D5-1FBE-11D0-8FF2-00A0D10038BC}
CLSID\{0E59F1D5-1FBE-11D0-8FF2-00A0D10038BC}\TreatAs
\CLSID\{0E59F1D5-1FBE-11D0-8FF2-00A0D10038BC}
\CLSID\{0E59F1D5-1FBE-11D0-8FF2-00A0D10038BC}\InprocServer32
\CLSID\{0E59F1D5-1FBE-11D0-8FF2-00A0D10038BC}\InprocServerX86
\CLSID\{0E59F1D5-1FBE-11D0-8FF2-00A0D10038BC}\LocalServer32
\CLSID\{0E59F1D5-1FBE-11D0-8FF2-00A0D10038BC}\InprocHandler32
\CLSID\{0E59F1D5-1FBE-11D0-8FF2-00A0D10038BC}\InprocHandlerX86
\CLSID\{0E59F1D5-1FBE-11D0-8FF2-00A0D10038BC}\LocalServer
HKEY_CLASSES_ROOT\CLSID\{0E59F1D5-1FBE-11D0-8FF2-00A0D10038BC}
HKEY_CLASSES_ROOT\CLSID\{0E59F1D5-1FBE-11D0-8FF2-00A0D10038BC}\TreatAs
HKEY_CLASSES_ROOT\TypeLib
HKEY_CLASSES_ROOT\TypeLib\{0E59F1D2-1FBE-11D0-8FF2-00A0D10038BC}
HKEY_CLASSES_ROOT\TypeLib\{0E59F1D2-1FBE-11D0-8FF2-00A0D10038BC}\1.0
HKEY_CLASSES_ROOT\TypeLib\{0E59F1D2-1FBE-11D0-8FF2-00A0D10038BC}\1.0\0
HKEY_CLASSES_ROOT\TypeLib\{0E59F1D2-1FBE-11D0-8FF2-00A0D10038BC}\1.0\0\win32
HKEY_CLASSES_ROOT\VBScript
HKEY_CLASSES_ROOT\VBScript\CLSID
CLSID\{B54F3741-5B07-11CF-A4B0-00AA004A55E8}
CLSID\{B54F3741-5B07-11CF-A4B0-00AA004A55E8}\TreatAs
```

Files

Registry Keys

Mutexes

```
CTF.TimListCache.FMPDefaultS-1-5-21-1547161642-507921405-839522115-1004MUTEX.DefaultS-1-5-21-1547161642-507921405-839522115-1004  
M_Test
```

Customization

- A customized sandbox is a key element in your defenses
- Must reflect your environment

Malware detecting VMs

- Generic VM detection rare
- More common
 - Detecting drivers unique to VMs
 - Installed as optimizations
 - Sometimes can be avoided
- Dedicated sandboxes avoid detection

Sandbox conclusions

- Much easier to automate
 - = cheaper, faster
- Can miss behaviors
 - Customization!
- May be 'impatient'

Indicators

Sandboxes and Reversing just the beginning

- Indicators as the result of reversing & sandboxing
- Each is a question that needs an answer

What sort of indicators?

- File accesses, file downloads
- System objects
- Network accesses
 - HTTP, FTP, DNS, SMTP, ...

Files and OS Objects

What files were accessed

- Could be an indicator of data leakage
- Understanding what's in file is important



Registry Keys

- OS run DB for application variables

Summary

Files

Registry Keys

Mutexes

```
HKEY_LOCAL_MACHINE\Software\Microsoft\COM3
HKEY_USERS\S-1-5-21-1547161642-507921405-839522115-1004_Classes
HKEY_LOCAL_MACHINE\Software\Classes
\REGISTRY\USER
HKEY_LOCAL_MACHINE\Software\Classes\CLSID
HKEY_CLASSES_ROOT\ScriptControl
HKEY_CLASSES_ROOT\ScriptControl\CLSID
CLSID\{0E59F1D5-1FBE-11D0-8FF2-00A0D10038BC}
CLSID\{0E59F1D5-1FBE-11D0-8FF2-00A0D10038BC}\TreatAs
\CLSID\{0E59F1D5-1FBE-11D0-8FF2-00A0D10038BC}
\CLSID\{0E59F1D5-1FBE-11D0-8FF2-00A0D10038BC}\InprocServer32
\CLSID\{0E59F1D5-1FBE-11D0-8FF2-00A0D10038BC}\InprocServerX86
\CLSID\{0E59F1D5-1FBE-11D0-8FF2-00A0D10038BC}\LocalServer32
\CLSID\{0E59F1D5-1FBE-11D0-8FF2-00A0D10038BC}\InprocHandler32
\CLSID\{0E59F1D5-1FBE-11D0-8FF2-00A0D10038BC}\InprocHandlerX86
\CLSID\{0E59F1D5-1FBE-11D0-8FF2-00A0D10038BC}\LocalServer
HKEY_CLASSES_ROOT\CLSID\{0E59F1D5-1FBE-11D0-8FF2-00A0D10038BC}
HKEY_CLASSES_ROOT\CLSID\{0E59F1D5-1FBE-11D0-8FF2-00A0D10038BC}\TreatAs
HKEY_CLASSES_ROOT\TypeLib
HKEY_CLASSES_ROOT\TypeLib\{0E59F1D2-1FBE-11D0-8FF2-00A0D10038BC}
HKEY_CLASSES_ROOT\TypeLib\{0E59F1D2-1FBE-11D0-8FF2-00A0D10038BC}\1.0
HKEY_CLASSES_ROOT\TypeLib\{0E59F1D2-1FBE-11D0-8FF2-00A0D10038BC}\1.0\0
HKEY_CLASSES_ROOT\TypeLib\{0E59F1D2-1FBE-11D0-8FF2-00A0D10038BC}\1.0\0\win32
HKEY_CLASSES_ROOT\VBScript
HKEY_CLASSES_ROOT\VBScript\CLSID
CLSID\{B54F3741-5B07-11CF-A4B0-00AA004A55E8}
CLSID\{B54F3741-5B07-11CF-A4B0-00AA004A55E8}\TreatAs
```


What Registry keys

- Can tell us
 - What programs Malware is trying to manipulate
 - How to be persistent on the system
 - How it self-IDs

File hashes

- Useful correlation method
- VirusTotal can give us more insights
- Approximate hashes
 - SSDEEP - most common
 - TLSH - most useful, but not common
 - <https://github.com/trendmicro/tlsh>

Virustotal

- Scanning and analysis server
- Run by Alphabet (Google)
- Upload file/search for hash
- Be careful!
 - Information leakage
 - Not an AV comparison tool

SHA256: a615aea82b091730662039982f66637a14e3ec079c2a07acd8f09a0bd3af84de

File name: npp.exe

Detection ratio: 30 / 55

Analysis date: 2016-06-15 02:02:27 UTC (2 hours, 54 minutes ago)



Analysis

File detail

Additional information

Comments 0

Votes

Behavioural information

Antivirus	Result	Update
ALYac	Trojan.Generic.AD.041911032	20160615
AVG	Generic_r.IWX	20160614
AVware	Trojan.Win32.Generic!BT	20160615
Ad-Aware	Gen:Heur.Kelios.1	20160615
AegisLab	Virtool.W32.Generic!c	20160615
Arcabit	Trojan.Kelios.1	20160615
Avast	Win32:Trojan-gen	20160615

📁 Opened files

C:\WINDOWS\Registration\R000000000007.clb (successful)

C:\WINDOWS\system32\msscript.ocx (successful)

\\PIPE\lsrpc (successful)

C:\WINDOWS\system32\wbem\wbemdisp.TLB (successful)

C:\WINDOWS\system32\stdole2.tlb (successful)

C:\WINDOWS\system32\drivers\etc\hosts (successful)

C:\WINDOWS\system32\rsaenh.dll (successful)

\\WMI\DataDevice (successful)

C:\WINDOWS\system32\WINHTTP.dll (successful)

📄 Read files

C:\WINDOWS\Registration\R000000000007.clb (successful)

C:\WINDOWS\system32\msscript.ocx (successful)

C:\WINDOWS\system32\wbem\wbemdisp.TLB (successful)

C:\WINDOWS\system32\stdole2.tlb (successful)

C:\WINDOWS\system32\drivers\etc\hosts (successful)

C:\WINDOWS\system32\rsaenh.dll (successful)

C:\WINDOWS\system32\WINHTTP.dll (successful)

🔑 Created mutexes

M_Test (successful)

📁 Runtime DLLs

kernel32.dll (successful)

user32.dll (successful)

ntdll (successful)

advapi32.dll (successful)

ole32.dll (successful)

ws2_32.dll (successful)

shlwapi.dll (successful)

dnsapi.dll (successful)

shell32.dll (successful)

msvcrt.dll (successful)

Show all

🌐 HTTP requests

URL: http://users.qzone.qq.com/fcg-bin/cgi_get_portrait.fcg?uins=2135988505

TYPE: GET

USER AGENT: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.154

URL: http://98.126.216.51/ca.php?m=4D4467744D4441744D6A63744D446B744E6A41745254513D&h=437

TYPE: GET

USER AGENT: Mozilla/4.0 (compatible; Win32; WinHttp.WinHttpRequest.5)

🌐 DNS requests

users.qzone.qq.com (103.7.30.86)

🌐 TCP connections

103.7.30.86:80

98.126.216.51:80

🌐 UDP communications

<MACHINE_DNS_SERVER>:53

Yara rules

- Like a little AV
- Supported in many systems
- Useful to check vulnerable systems
- Be careful!
 - F.P. prone

```
rule Malware_Cridex_Generic {
meta:
    description
        = "Rule matching Cridex-C Malware
        distributed in a German Campaign, January
        2014 (Vodafone, Telekom, Volksbank bills)"
    author = "F. Roth"
    date = "2014-01-15"
    reference
        = "https://www.virustotal.com/en/file/
        519120e4ff6524353247dbac3f66e6ddad711d384e3
        17923a5bb66c16601743e/analysis/"
    hash = "86d3e008b8f5983c374a4859739f7de4"
strings:
    $c1 = "NEWDEV.dll" fullword
    $b2a = "COMUID.dll" fullword
    $b2b = "INSENG.dll" fullword
condition:
    $c1 and 1 of ($b*)
}
```

Network objects

URLs

- Can refer to
 - second-stage Malware
 - Command and Control
 - Monetization
 - Data leakage

HTTP Requests

URI	DATA
<code>http://users.qzone.qq.com/fcg-bin/cgi_get_portrait.fcg?uins=2135988505</code>	<pre>GET /fcg-bin/cgi_get_portrait.fcg?uins=2135988505 HTTP/1.1 Host: users.qzone.qq.com Connection: keep-alive User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.154 Safari/537.36</pre>
<code>http://98.126.216.51/ca.php?m=4D4467744D4441744D6A6374526B55744F4559745245593D&h=437</code>	<pre>GET /ca.php?m=4D4467744D4441744D6A6374526B55744F4559745245593D&h=437 HTTP/1.1 Accept: */* User-Agent: Mozilla/4.0 (compatible; Win32; WinHttp.WinHttpRequest.5) Host: 98.126.216.51 Connection: Keep-Alive</pre>

```
$ curl -v http://users.qzone.qq.com/fcg-bin/cgi_get_portrait.fcg?uins=2135988505
*   Trying 103.7.30.86...
* Connected to users.qzone.qq.com (103.7.30.86) port 80 (#0)
> GET /fcg-bin/cgi_get_portrait.fcg?uins=2135988505 HTTP/1.1
> Host: users.qzone.qq.com
> User-Agent: curl/7.43.0
> Accept: */*
>
< HTTP/1.1 200 OK
< X-Powered-By: TSW/Node.js
< Cache-Control: max-age=86400
< Connection: close
< Keep-Alive: timeout=10
< Mod-Map: nodeproxy_index:photo.v7/nodejs/module/nodeproxy/index.js
< Content-Type: text/html
< Cache-Offline: false
< Content-Length: 124
< Server: QZHTTP-2.37.1
< Date: Wed, 15 Jun 2016 07:17:21 GMT
<
* Closing connection 0
portraitCallBack({"2135988505":["http://qlogo2.store.qq.com/qzone/2135988505/2135988505/100",
0,-1,0,0,0,"98.126.216.52",0]})
$
```

```
$ wget -v -O 2135988505.bin http://qlogo2.store.qq.com/qzone/2135988505/2135988505/100
--2016-06-15 09:20:21-- http://qlogo2.store.qq.com/qzone/2135988505/2135988505/100
Resolving qlogo2.store.qq.com... 174.35.71.14, 151.249.89.196
Connecting to qlogo2.store.qq.com|174.35.71.14|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 2055 (2.0K) [image/jpeg]
Saving to: '2135988505.bin'

2135988505.bin      100%[=====>]      2.01K  --.-KB/s    in 0s

2016-06-15 09:20:21 (131 MB/s) - '2135988505.bin' saved [2055/2055]
$ file 2135988505.bin
2135988505.bin: JPEG image data, JFIF standard 1.02
$
```

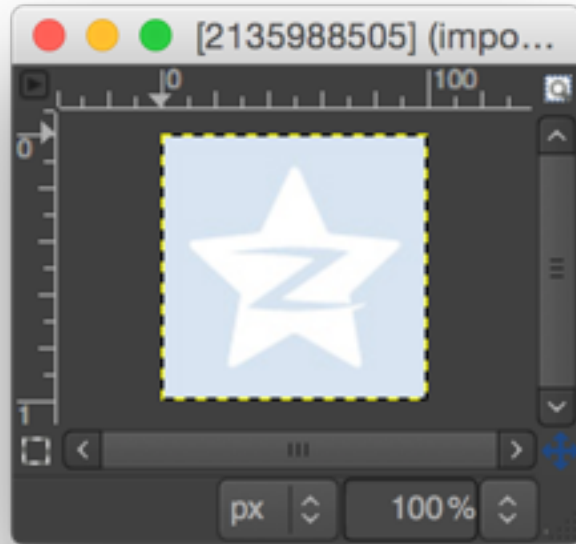
```

2135988505.bin
0  FFD8FFE0 00104A46 49460001 02000064  "y`± JFIF  d
16 00640000 FFEC0011 4475636B 79000100  d `I Ducky
32 04000000 500000FF EE000E41 646F6265  P `Ó Adobe
48 0064C000 000001FF DB008400 02020202  d¿ `e Ñ
64 02020202 02020302 02020304 03020203
80 04050404 04040405 06050505 05050506
96 06070708 07070609 090A0A09 090C0C0C
112 0C0C0C0C 0C0C0C0C 0C0C0C0C 01030303
128 05040509 0606090D 0B09080D 0F0E0E0E
144 0E0F0F0C 0C0C0C0C 0F0F0C0C 0C0C0C0C
160 0F0C0C0C 0C0C0C0C 0C0C0C0C 0C0C0C0C
176 0C0C0C0C 0C0C0C0C 0C0C0C0C 0CFFC000
192 11080064 00640301 11000211 01031101  " d d `¿
208 FFC4008C 00010002 03010101 00000000  `f á
224 00000000 00000106 04050703 02090101
240 00030101 00000000 00000000 00000000
256 02030401 05100001 03030204 010A0307
272 05000000 00000100 02031104 05311221
288 51610641 718191B1 C1223213 3314A172  Qa AqAë±j"2 3 `r
304 23425262 92C24416 D1437334 15110100  #BRb!~D -Cs4
320 02020104 03010101 00000000 00000001
336 02110321 31411204 51711361 1422FFDA  !1A Qq a ""/
352 000C0301 00021103 11003F00 FD8824D4  ? `d$'

```

Unsigned Int little (select some data)

0 out of 2055 bytes



Traffic Direction Systems

- URLs lead to other URLs
- Each decision point is a TDS that looks at
 - Browser/Machine attributes
 - referer ID
 - Opportunities for monetizations

Domains

- FQDN (Fully Qualified Domain Name)
 - is mapped to an address
 - Sometimes the FQDN already tells us a lot
- DNS can tell us a few things more

For example

```
{
  "@eventID": "909",
  "Details": "URL: http://loslokos.com.br/invoice.exe Threat Name: WEB-THREAT_RAREWARE.WRS",
  "Event": "Attempts to connect to malicious URL"
},|
```

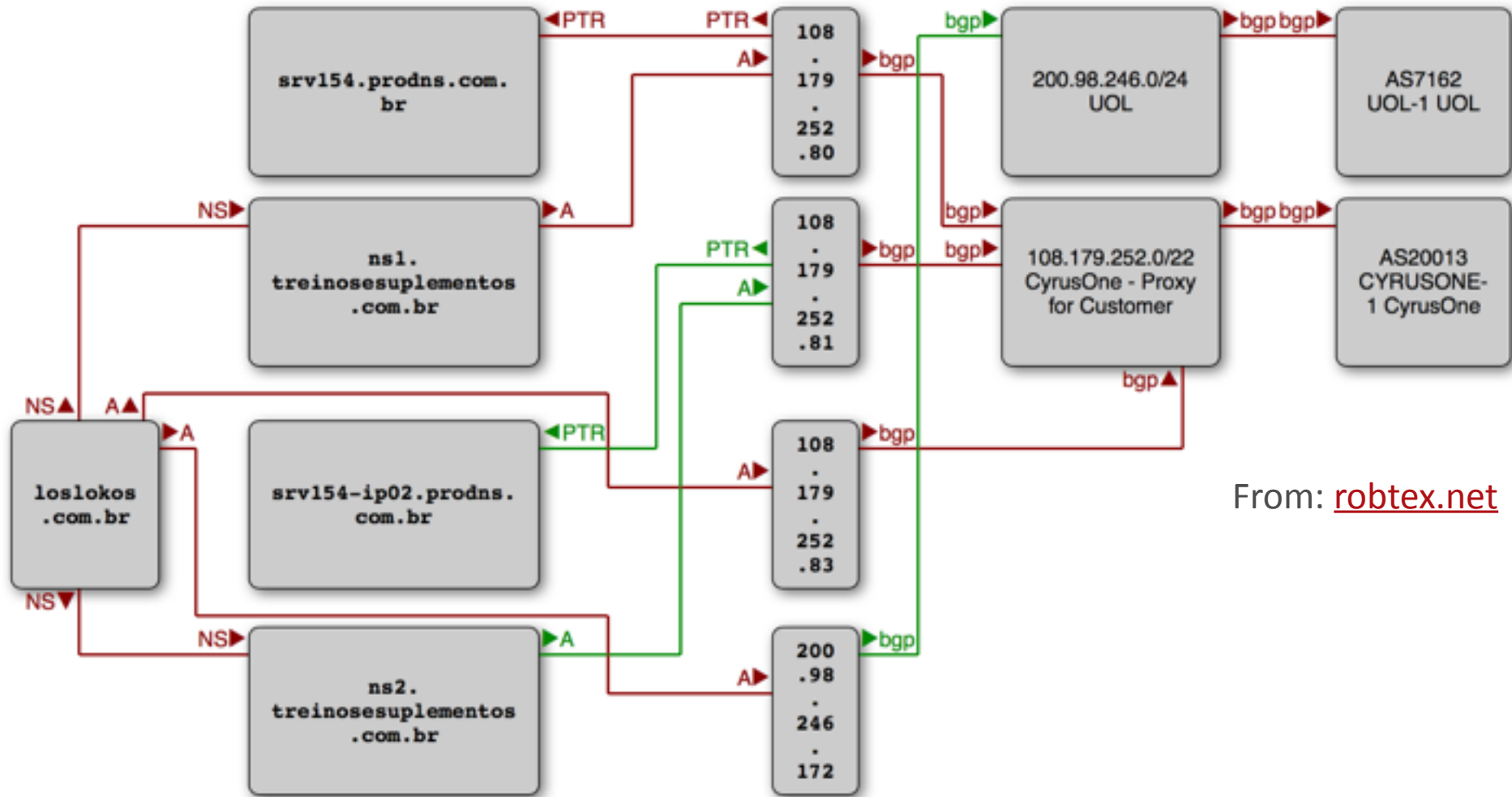
What can we tell by looking at loslokos.com.br?

loslokos.com.br

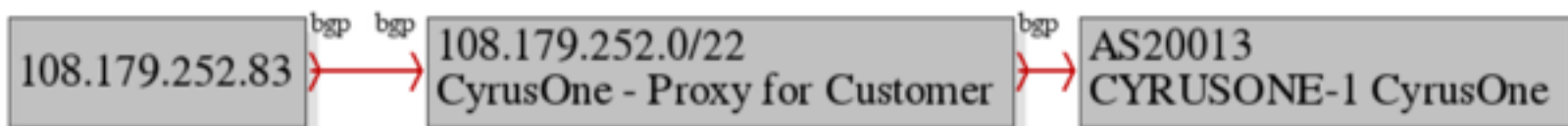
- Brazilian ccTLD
 - Country Code Top Level Domain
- COM.BR
 - “Commercial websites in general and individuals”

dig loslokos.com.br ANY

```
loslokos.com.br. 14400 IN A 108.179.252.83
loslokos.com.br. 86400 IN SOA ns1.treinosesuplementos.com.br. contato.etiketa.com.br.
2016013100 86400 7200 3600000 86400
loslokos.com.br. 14400 IN MX 0 loslokos.com.br.
loslokos.com.br. 14400 IN TXT "v=spf1 a mx include:websitewelcome.com ~all"
loslokos.com.br. 72019 IN NS ns1.treinosesuplementos.com.br.
loslokos.com.br. 72019 IN NS ns2.treinosesuplementos.com.br.
```



From: robtex.net



Pointing to 108.179.252.83 (100 shown)

```
atenasimoveis.com  
brunomigotto.com  
chaitosoft.com  
consultrt.com  
easybuildersite.com  
gamesgeral.com  
gceduacao.com  
germanobona.com  
gloriaeventos.com  
guiapalhoca.com  
ivoryboots.com  
loupbr.com  
musculacaoeficaz.com  
petroleumplatform.com  
portadosucesso.com  
ranassamir.com  
rdcomunicacao.com  
stawfer.com  
umpassarinhomecontou.com
```

whois loslokos.com.br

```
domain:      loslokos.com.br          changed:      20160315
owner:       MARCUS VINCIUS SARTORI
country:     BR
owner-c:     MAS3319
admin-c:     EDBSE5
tech-c:      EDBSE5
billing-c:   EDBSE5
nserver:     ns1.treinosesuplementos.com.br
nsstat:      20160614 AA
nslastaa:    20160614
nserver:     ns2.treinosesuplementos.com.br
nsstat:      20160614 AA
nslastaa:    20160614
saci:        yes
created:     20110103 #7740857
expires:     20170103
changed:     20160308
status:      published

nic-hdl-br:  EDBSE5
person:      Eduardo Brandao Secco
created:     20081018
```

IP addresses

- Sometimes we only get the IP address
- Or we have resolved the FQDN
- This can help us get the AS (Autonomous System) number

When CURL fails

```
$ curl -v http://98.126.216.51/ca.php?m=4D4467744D4441744D6A6374526B55744F4559745245593D\&h=437
* Trying 98.126.216.51...
* connect to 98.126.216.51 port 80 failed: Operation timed out
* Failed to connect to 98.126.216.51 port 80: Operation timed out
* Closing connection 0
curl: (7) Failed to connect to 98.126.216.51 port 80: Operation timed out
```

whois "n 98.126.216.51"

```
NetRange:      98.126.0.0 - 98.126.255.255
CIDR:          98.126.0.0/16
NetName:       VPLSNET
NetHandle:     NET-98-126-0-0-1
Parent:        NET98 (NET-98-0-0-0-0)
NetType:       Direct Allocation
OriginAS:      AS35908
Organization:  Krypt Technologies (VPLSI)
RegDate:       2008-06-10
Updated:       2012-03-02
Comment:
Comment:       For legal requests/assistance
please use the
Comment:       following contact information:
Comment:       VPLS Subpoena Phone: 213-406-9088
Comment:       VPLS Abuse Fax: 213-406-9001
Comment:       VPLS AUP, Terms of Service and
DMCA/Copyright notices info:
Comment:       http://www.vpls.net/privacy/
Ref:           https://whois.arin.net/rest/net/
NET-98-126-0-0-1

OrgName:       Krypt Technologies
OrgId:         VPLSI
Address:       1744 W. Katella Avenue.
Address:       Suite 200
City:          Orange
StateProv:    CA
PostalCode:   92867
Country:      US
RegDate:      2005-03-25
Updated:      2014-08-12
...
```


ASNs

- Autonomous System numbers
- Tell you who owns the IP space
- There are some 'bad' ASs

IDS/IPS

Inbound connections

- IDS typically sits at some gateway
- Monitor inbound traffic
- Match against known bad traffic
- Potential for statistical profiling

Outbound connections

- Often ignored
- Vital to track Malware inside a company
- Can often detect data leakage
 - But hard to write rules for this

In practice

- Alone, too many false positives to be useful
- Good for forensics
- Can help diagnose and measure extent of attack

Pulling it all together

Know yourself

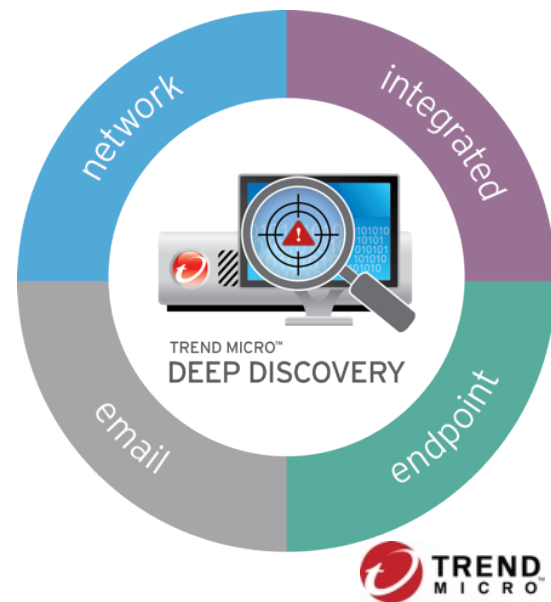
- Inventory!
 - Hardware
 - Software
 - Update schedule/budgeting
- Regular scans
 - devices
 - vulnerabilities

Know the enemy

- Sandboxes are great but they need to be fed
- Malware management systems needed
 - eg. Aleph
- Keep up to date with new threat models
 - (but don't freak out)

Central analysis and correlation

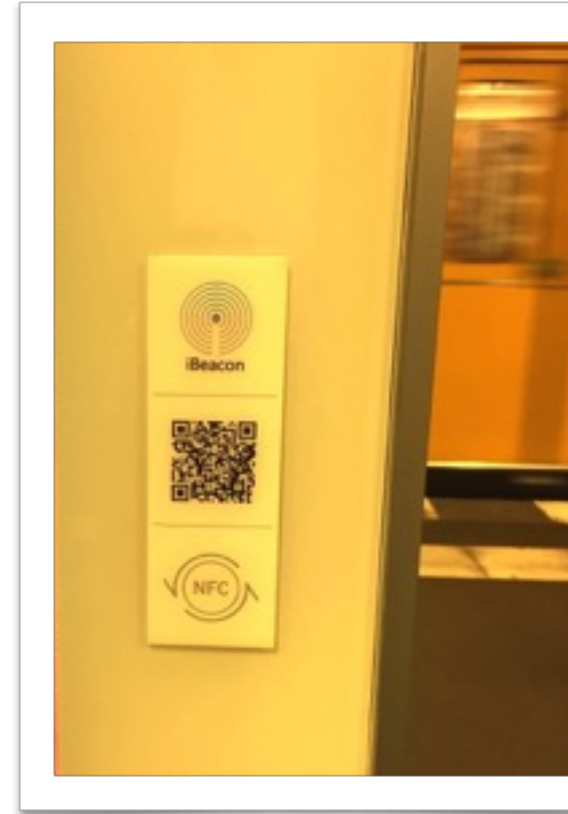
- Centralized handling of all your security data
- Correlate, analyze, explore
 - then tune your security stance
- Elasticsearch is becoming popular
- Vendors (like us) offer complete solutions



What to expect

Me, Cyborg

- Connected devices exploding in numbers
- Dependence on technology increases
- There is no 'inside'
 - Meet the PAN in the LAN in the WAN
 - Assume you are already compromised



Two sides of Snowflakes

- Homogeneity is your friend
- And your enemy
- Keep snowflake PCs under control



Legacy will kill you

- If you can't update, you will be exploited
 - Eg, MD5 and SHA1
 - Old protocols, machines, OSes
- Define an upgrade path before you install anything

Think holistically

- You will be attacked at your weakest point
- So, know yourself well
- Always challenge assumptions



Thank you

MORTON_SWIMMER@TRENDMICRO.DE