



Cyber Intelligence Threat Briefing

Presented by: Ian Trump @ itSMF
17 Jan 12



Agenda

- Overview of Threat Environment
- Types of Threats & Definitions
- Response Tactics
- Managing the Risks
- Conclusion

...when **SUCCESS** matters



Advanced Persistent Threat (APT)

- **What is it?**

A group, such as a foreign nation state government, with both the capability and the intent to persistently and effectively target a specific entity.

- **What does it do?**

Long-term, sophisticated hacking attacks aimed at governments, companies, and political activists, and by extension also refers to the groups behind these attacks.

...when **success** matters



- **Operation ShadyRAT, Night Dragon, Aurora, Lurid, & Nitro**

Cyber attack which began in mid-2006 and continued through December 2009. Targeted Google, Adobe Systems, Juniper Networks, Rackspace, Yahoo, Symantec, Northrop Grumman, Morgan Stanley and Dow Chemical. Attributed to the People's Republic of China

- **Target:** Civilian, Military IP and Dissident Activity (Mitsubishi Heavy Industries)



Goal of APT Attacks

Information = competitive advantage

- Classified or sensitive software
- Classified, sensitive, emerging, or advanced industrial design breakthroughs
- Information to exploit a better protected system
- Mineral exploration data
- Information for a competitive advantage
- Disruption of business operations
- Destruction of brand reputation
- Credit card, social insurance, or medical information



APT Lurid 22 Sep 2011

- **What is it?**

An APT attack on the former Soviet Union region and other countries.

Who did it target?

50 victim organizations including government ministries and agencies, diplomatic missions, research institutions, and commercial entities in the former Soviet Union region and other countries. Russia, Kazakhstan, Ukraine, and Vietnam have been hit hardest.

What is affected?

1,465 computers in 61 countries with more than 300 targeted attacks. The attackers deployed a command-and-control (C&C) infrastructure of some 15 domain names and 10 IP addresses to keep their foothold in the victim machines.



APT Nitro 1 Nov 11

- **What is it?**

An APT attack which hit close to 50 companies, including 29 chemical firms and 19 firms mostly in the defense industry.

How did it work?

Phishing email sent to the targeted organizations the emails posed as security updates and meeting invitations contained an encrypted attachment with the PoisonIvy backdoor Trojan. The attackers went after administrator credentials and access to sensitive information at the targeted firm. (1989 - all over again Backorifice Attacks)

What is affected?

101 unique IP addresses representing 52 different ISPs or organizations in 20 countries. Symantec was able to trace the attacks to a virtual private server in the U.S., owned by a man nicknamed "Covert Grove," who appears to have a connection to a "hacking for hire" service.

...when **SUCCESS** matters



History of APT

- 2003 Gulf War (Aborted Attack on Iraqi Banking Infrastructure)
- 2003 Serbian War (US Army Spoofs Air Defense Systems)
- 2000 Israel/Palestine (Harmless University Students ?)
- 2005 Iraq/Afghanistan (US Army ECM/ELINT Operations)
- 2007 Cyber Attack on Estonia (POP Russian Hackers)
- 2007 Israel Attack on Syria (Spoof Greek, Turkish and Syrian ADS - BAE Software implicated)
- 2007 Counter-IED (NRO and attacks on ISP, Cell and Land-Line Infrastructure, Counter-Terrorism NSA Operations)
- **2008 Cyber Attack on Georgia** (Russian Government Sub-Contracts to Russian Organized Crime)

...when **success** matters



Military and Civilians Working Together



- 2009 Cyber Attack on Israel Palestine (23 Countries, Russian Organized Crime, Iranian Cyber Army, Israel's downloadable tool)
- 2010 Iran (Stuxnet - Germans, Israel, US)
- 2010 Wikileaks (LOIC Tool, Anonymous, Aaron Barr, HB Garry)
- 2011 The Canadian government reports a major cyber attack against its agencies, including Defense Research and Development Canada, a research agency for Canada's Department of National Defense. The attack forced the Finance Department and Treasury Board, to disconnect from the internet. Canadian sources attribute the attack to China.

http://csis.org/files/publication/110906_Significant_Cyber_Incidents_Since_2006.pdf (81 Since the Last Update in September 6, 2011)

...when **success** matters



APT For Rent or Free!

- Nation-state cyber espionage attackers are buying already-infected machines from cybercriminals as a more streamlined way to infiltrate a targeted organization, according to FireEye.
- Ashar Aziz, CEO and CTO of FireEye, says his firm has spotted such conspiracy between traditional cybercriminals who infect machines for profit, and so-called advanced persistent threat (APT)-type attackers who infiltrate targeted organizations to steal intellectual property or other intelligence.
- "We are seeing collusion between the criminal element and the nation-state. Rather than launch a targeted attack ... they choose to come back to an existing infection" to get inside more easily and faster, he says.

...when **SUCCESS** matters



Supervisory Control and Data Acquisition System & Stuxnet

- **SCADA, What is it?**

Computer systems designed and interfaced to sensors which measure or control automated process.

- **What does it do?**

Controls industrial process in refineries, pipelines, power plants, fabrication via network (Internet) connections. In place since the 1950's built with little security, authentication process and code review.

...when **SUCCESS** matters



Supervisory Control and Data Acquisition System & Stuxnet

- **Stuxnet, What is it?**

Computer worm discovered in July 2010. It targets Siemens industrial software and equipment running on Microsoft Windows.

- **What does it do?**

Designed to target only Siemens supervisory control and data acquisition. Targeted five Iranian organizations with the probable target widely suspected to be uranium enrichment infrastructure in Iran

...when **SUCCESS** matters



SCADA is Vulnerable

- September, 2011 - An Italian researcher has disclosed 13 vulnerabilities in a variety of supervisory control and data acquisition (SCADA) products. The same man, Luigi Ariemma, disclosed 34 flaws in SCADA products in March. DHS has released security advisories in response to the latest set of flaws, which was released with proof-of-concept exploit code.



Programmable Logic Controllers (PLC) are Vulnerable

Industrial-control modules manufactured by Schneider Electric

- In order to fully understand the PLC/Eth module, backplane and other protocols (i.e Unity's UMAS) we can reverse engineer the firmware, the java classes and vendor's software like Unity Loader.
 - You can remotely compromise Modicon PLCs exposed via Ethernet modules through ftp, telnet, modbus, WDB, snmp, web... by using the backdoor credentials exposed or even without using them.
 - You can load your own trojanized firmware.
 - There are non-documented hidden accounts that can be used to compromise a PLC.
 - There are non-documented functionalities with security implications.

...when **SUCCESS** matters



Duqu 19 Oct 11

What is it?

A new worm built on some Stuxnet virus components

- **What does it do?**

McAfee experts suggests that the worm was created "for espionage and targeted attacks against sites such as Certificate Authorities (CAs)."

- **Why?**

64 Bit Computing yah all, Pwnage is hard because:

64 bit kernel modules must carry a valid digital signature that can be checked by the operating system, or loading the module fails. Pwn the CA → Auth "New" kernel modules – Pwn the Box.

...when **success** matters



* Latest News*

Flaws in Siemens FactoryLink could be exploited remotely

06 January 2012

Two vulnerabilities in the Siemens FactoryLink industrial control system could enable a hacker to carry out remotely denial of service and arbitrary code execution attacks, warned the US Industrial

Control Systems Cyber Emergency Response Team (ICS-CERT).

...when **success** matters



MetaSploit

What is it?

The *Metasploit*® Framework is a free, open source penetration testing solution, (breaks networked systems)

- **What does it do?**

Uses a library of Exploits to compromise systems, SCADA
Exploits available since 2008

Database currently has 12 exploits covering dozens of
software implementations

Network reconnaissance is already ongoing (Iranian Cyber
Army)

SCADA = Power Generation = Military Bases

...when **SUCCESS** matters



Certificates and TLS/SSL

- **What is it?**
Used to confirm identity and encrypt connections between computer systems
- **What is the problem?**
 - Broken in multiple ways
 - 128 bit encryption will be done (cloud computing)
 - Cert authorities compromised (DigiNotar and three others, Iran, EFF)
 - Man-in-the-middle attack: Browser Exploit Against SSL/TLS tool, dubbed BEAST
 - Cookies, Expired Certificates, Spoofed Certificates
 - Upgrading TLS is proving surprisingly difficult, mostly because almost every fix breaks widely used applications or technologies.
- **Target:** Steal your \$, listen to your conversations

...when **SUCCESS** matters



Incident Management & Reality

- IT Security/IT OPS need to be part of the conversation, need to educate Upper Management
- A compromise or un-authorized disclosure is coming to a theatre near you (HB Garry)
- Stay off of the radar (LuzSec, Anti-Sec, Cyber crime Gangs, Anonymous)
- Have plan for when the s&t hits the fan (BP)
- 2 factor authentication FTW
- Ask for help and call in experts (Sony example)

...when **SUCCESS** matters



Manage the Risk



- Don't believe the hype
- Been going on for a really long time
(World's 2nd oldest profession)
- User education, policies and process are the only answers to social engineering attacks
- Be aware when using social networks
- Treat all your business information like it is your credit card number
- If a person is super-hot, talking to you and you work in IT, be suspicious

...when **SUCCESS** matters



It's 10 Bucks & Comes With Support

URL: http://

Intervall: 180

Mutex: [blurred]

Registry Name: MSN 2011

ActiveX: { [blurred] }

Drop Name: MSN_2011

Firewall deaktivieren (XP + Vista)

Packen mit UPX

Stub wurde nicht gefunden!

- Requires minimal configuration beyond entering the name of a command-and-control server, which comes with the tool
- Capable of extracting saved passwords from the browser cache of compromised machines
- Based on the recently leaked ZeuS source code, is also capable of running distributed denial of service attacks on targeted websites
- Compromised machines might also be used as a proxy for anonymous surfing
- Tool might be employed by perverts hunting for child abuse images on the net

...when **success** matters



Response Tactics

- Don't be arrogant, plan for a failure, learn from mistakes
- Network and build a circle of friends smarter than you
- Manage risks, communicate and call for help
- Get back to the basics
- Physical security is as important as IT security
- Be the hard target, casual hackers will go someplace else

...when **success** matters



Conclusions for ISP/Telcos

- **Beware of new legal requirements like those found in:**
C-50, Access to Investigative Tools for Serious Crimes Act
C-51, Investigative Powers for the 21st Century Act
C-52, Investigating and Preventing Criminal Electronic Communications Act and Canadian Copy Write Act

The Harford Insurance Company - “Your Failure is Our Profit”

- Introduces such new terms as: Due Diligence, 3rd Party Liability, Reasonable Precautions and potentially:
- **ISP liability:** Internet service providers can be liable for failing to take down offensive, defamatory or IPR-infringing content. In such circumstances, corporate customers should seek an indemnity (\$) for any loss suffered as a result of material being unnecessarily deleted or moved and should insist on being notified in advance if any content is to be removed.

Remedy: A robust, signed and customer understood TOS on file.

New Word: Subrogation

...when **SUCCESS** matters



Conclusions

- Business decisions have real world implications for IT Security – layoffs, strike, disasters, etc.
- Work with business and support the change management process.
- Good will in the IT Community is your most important tool
- Manage for inconvenience, Prepare for disaster
- Sophisticated Cyber attacks are for rent, don't draw fire.
- It may not be a deliberate attack, just an accident

...when **SUCCESS** matters

Questions ?



...when **success** matters