Targeted Attack

SC Leung
Senior Consultant

HKCERT

Agenda

- Recent News
- Case Study: Stuxnet
- Implications
- Mitigation Measures

News

SCMP
30 September 2010

Stuxnet virus attacks 'nearly 1,000' facilities using Siemens control systems; HK at risk

Cyber worm hits mainland industry

At risk? Infrastructure using Siemens systems and therefore possibly at risk from the Stuxnet virus

Under attack
Potential threat posed by Stuxnet to national security could be 'unprecedented'

The virus has infected this many computers in China over the past few days

6m

woman said the
d by companies
far it had not re-
an attack in the
s include Hong
irport, Disney-
Power and St
acowy Bay. The
hey had been
s and were told
t affected.
said the poten-
s to China's na-
nprecedented",
nly steals and
ata of the infect-
y but also leaves
remote control

been sounded
dustrial sector –

steel, energy, transport ... This has never happened before," said Wang Zhantao (王占濤), a network security engineer with antivirus service provider Beijing Rising International Software.

Beijing said it would closely monitor the situation and may order a nationwide assessment of Siemens systems. "If it is serious, we may reexamine the issuing of licences for Siemens products," an official from the Ministry of Industry and Information Technology said.

Siemens' headquarters in Munich refused to comment on the impact of the virus on its Chinese clients but said it was working to fix the problem. Neither Beijing nor Siemens would provide a full list of the industrial facilities affected by the virus.

Siemens' system is widely used by airports, railways, including the Shanghai maglev, nuclear power plants and the Three Gorges Dam.

Professor Sun Jianping (孫建平), a hydropower expert, said he was worried. Sun led a study on the reliability and stability of the generators at the Three Gorges Dam, which are controlled and monitored by a Siemens system vulnerable to the virus. "If someone hacks into the system and takes over, we will be blinded and disabled," he said. "It could cause more destruction than a bomb."

The Stuxnet virus attacking China is the same type found at Iran's first nuclear plant, Bushehr, this month. The plant suffered only slight damage from the Internet-based attacks but the virus alarmed security experts

Harry's View
A14

worldwide. The plant will begin supplying energy early next year after a delay of several months.

Stuxnet is a highly complex malware – malicious software – that has never been seen before. It is so advanced that experts believed that a state may have been involved in creating it. Unlike ordinary spyware that attack personal computers, Stuxnet targeted Siemens control systems. It uses personal computers as springboards to search and attack main computer systems installed with the Siemens programme.

It can be transferred by USB memory stick, or other flash memory such as digital cameras. A worker with an infected USB stick could unknowingly plug it into a company network, bypassing the firewall, transferring the virus to the system.

The virus uses four previously unknown security holes in Microsoft Windows to seek the database for Siemens' supervisory control and data acquisition software (SCADA), which is widely used to run factories, chemical, water supply and power plants around the world.

"An employee who plugs his MP3 player into a company computer can wreck the whole production plant without knowing it," Wang said.

A senior sales manager with Rockwell Automation, a direct competitor of Siemens', said the fact the company's codec was based on Microsoft Windows has turned out to be a fatal

• CONTINUED ON A2

Ming Pao
1 October 2010

超級電腦病毒Stuxnet恐襲港

肆虐全球 內地600萬電腦中招

【明報專訊】一種針對大型基建電腦系統的超級電腦病毒Stuxnet近日肆虐全球，中國官方媒體新華社亦證實內地600萬台電腦受感染。港府資訊科技總監辦公室已向各決策局及部門發出警報，促請他們留意病毒威脅。**電腦專家**表示，Stuxnet的傳播性低，但一旦基建受擾，會帶來嚴重破壞，不能掉以輕心，呼籲有關機構盡快與電腦系統生產商聯絡，做好防範措施。

部分受Stuxnet影響國家

德國
西門子發源地，西門子證實收到的大部分感染系統來自當地

美國 英國 阿塞拜疆 俄羅斯

中國
600萬個人電腦和企業系統受影響

南韓

印尼
全球第二大重災區，佔兩成

伊朗
全球近六成感染來自當地，其中包括核設施

巴基斯坦

印度 佔全球一成

明報製圖

專攻西門子系統 基建高危

資訊科技總監辦公室發言人表示，一直與香港電腦保安事故協調中心和警方密切留意Stuxnet的散播情況，以及在本港及海外造成的影響。如有需要，會加強監察、協調及通報措施。辦公室已發出警報，促請各部門留意Stuxnet的威脅，有需要情況下安裝修補程式，堵塞軟件保安漏洞。

新華社證實，Stuxnet於內地已侵襲600萬台個人電腦和重要企業電腦系統。Stuxnet針對西門子（Siemens）生產的監控和數據收集系統（SCADA），該系統主要用於發電、供水等基建和大型工業設施；伊朗原定11月投產的第一個核發電設施，亦因Stuxnet侵襲而被迫押後兩月。

西門子證實本港多間機構均有採用其產品，但暫未能確認政府部門是否有使用SCADA。公司已提供工具堵塞漏洞，目前西門子全球共受收到15宗報告，本港未有感染個案。

USB手指傳播 港未有電腦中招

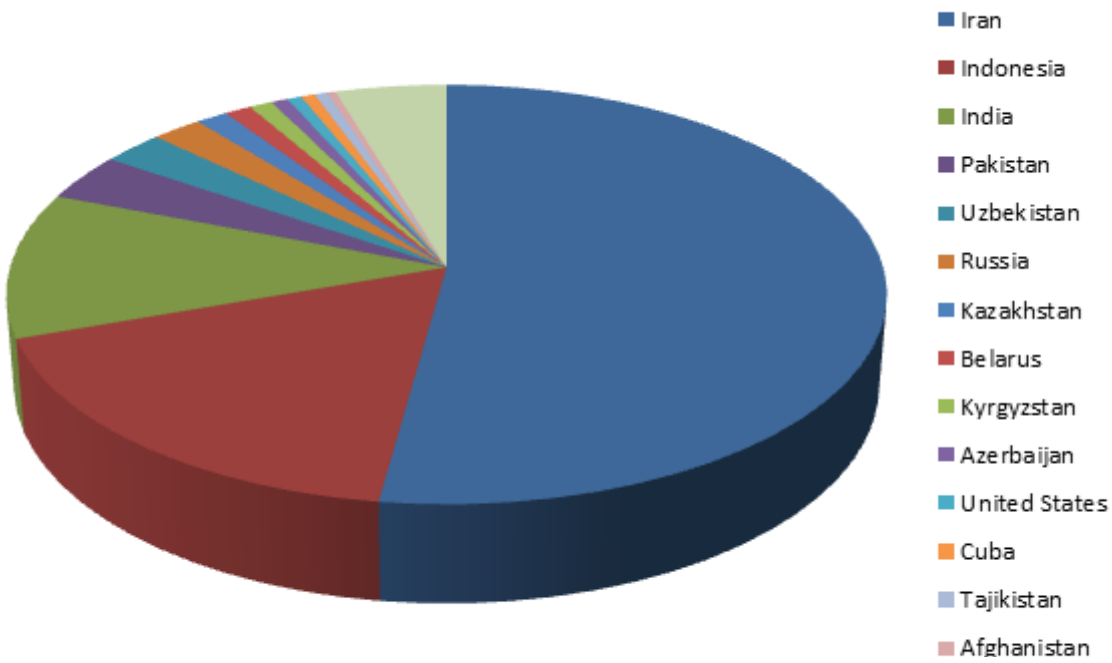
電腦保安事故協調中心經理古煒德表示，Stuxnet可入侵並控制基建電腦系統，一旦系統受破壞，市民日常生活會大受影響，不能掉以輕心。他補充，Stuxnet主要透過USB手指傳播，目前中心亦無收到本地感染個案。

編碼極複雜 疑國家設計攻伊朗

Stuxnet編碼異常複雜，有英國安全專家指它幾可肯定屬國家設計的病毒，由於攻擊目標明顯是伊朗的核設施，美國及以色列嫌疑最大。有電腦專家在Stuxnet的編碼中發現一個名為「Myrtus」（香桃木）的檔案，香桃木一詞出自《聖經》，源自猶太人先發制人，破壞了波斯軍隊的陰謀，有分析認為那代表以色列意圖藉散播Stuxnet，破壞伊朗核計劃，但亦有指有人插贓以色列。

鑑於Stuxnet已在內地爆發，立法會資訊科技界議員鄭偉豪擔心它很快會攻擊香港，促請港府留意相關基建、發電與機場等重要設施。他認為政府的電腦防衛意識較強，但提醒當局要特別留意由其他公私營機構監控的設施，同時要及早制定應變方案。

Distribution of Infection by Region



Iran	Indonesia	India	Pakistan	Uzbekistan	Russia	Kazakhstan	Belarus
52,2%	17,4%	11,3%	3,6%	2,6%	2,1%	1,3%	1,1%
Kyrgyzstan	**Azerbaijan**	**United States**	**Cuba**	**Tajikistan**	**Afghanistan**	**Rest of the world**	
1,0%	0,7%	0,6%	0,6%	0,5%	0,3%	4,6%	

Stuxnet Under the Microscope, ESET

HKCERT

News: Stuxnet attack on SCADA

Breaking News Yen surges, stocks fall as Japan cris_

JPost.com > Iranian Threat > News

'Stuxnet virus set back Iran's nuclear program by 2 years'

By YAAKOV KATZ
12/15/2010 05:15

Top German computer consultant tells 'Post' virus was as effective as military strike, a huge success; expert speculates IDF creator of virus.

Talkbacks (68)

Photo by: Associated Press

The Stuxnet virus, which has attacked Iran's nuclear facilities and which Israel is suspected of creating, has set back the Islamic Republic's nuclear program by two

The Jerusalem Post
15-December-2010

CSO SECURITY AND RISK Newsletters Dashboard RSS Solution Centers White Papers

NEWS

If Stuxnet was act of cyberwar, is the U.S. ready for a response?

The complex Stuxnet worm proved attacks on SCADA and other industrial control systems were possible. Are we ready if one comes our way?

By George V. Hulme

March 02, 2011 — CSO —

With Stuxnet setting back Iran's disputed nuclear program, that country has vowed against the powers it believes launched the attack, a recent news story in the Teh

CSO Online
02-March-2011

HKCERT

Case Study: Stuxnet

Case: Stuxnet

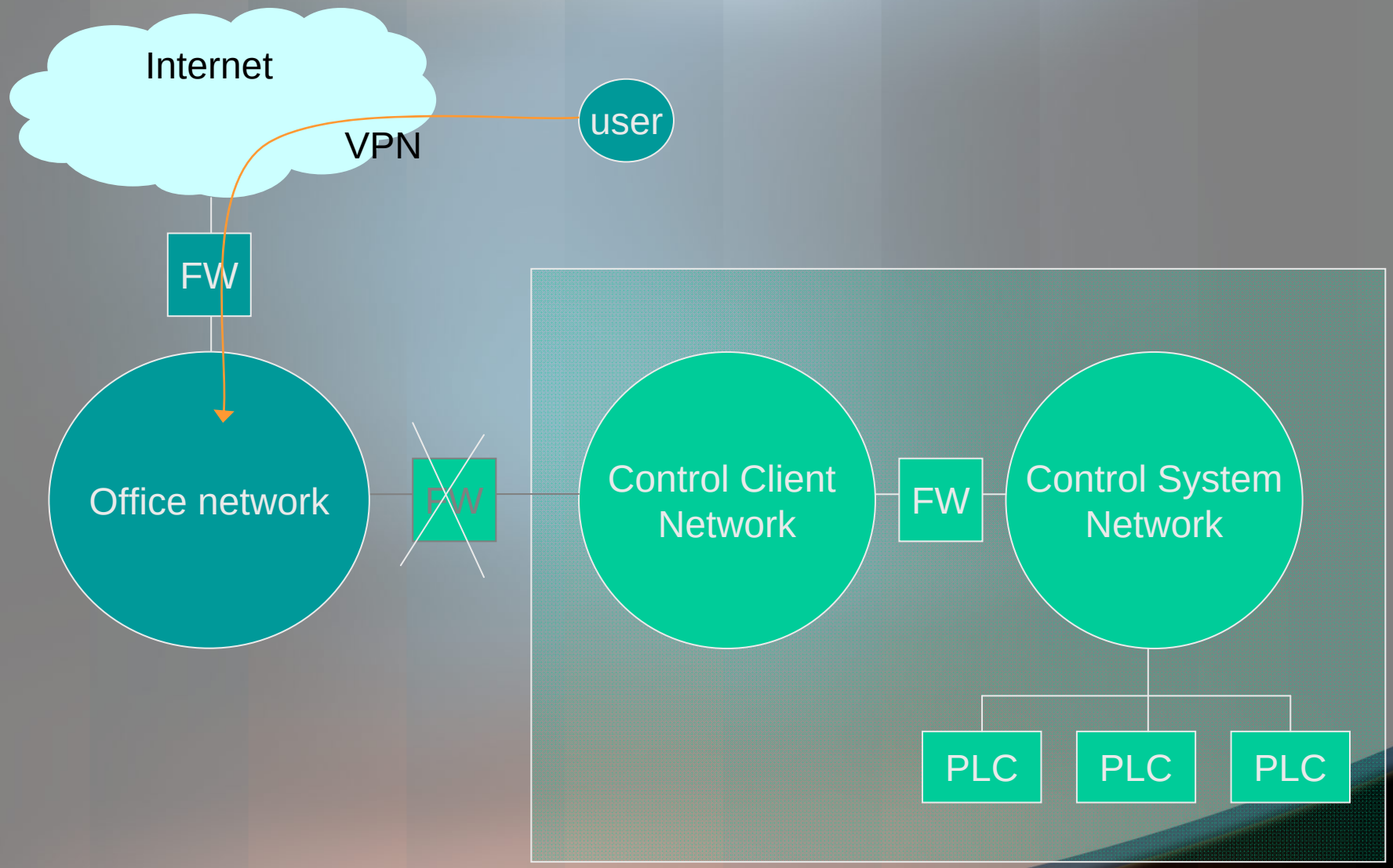
- Target:
  - Siemens SIMATIC WinCC Programmable Logic Controllers (PLC)
  - Obtain information from the database
- Impact:
  - Not collecting sensitive data, but bringing down the SCADA facility
- Filesize: 1.2MB

What is SCADA?

- Supervisory Control and Data Acquisition
  - computerized control system that automates many infrastructures such as oil and gas pipelines, power grids, communication networks, etc.

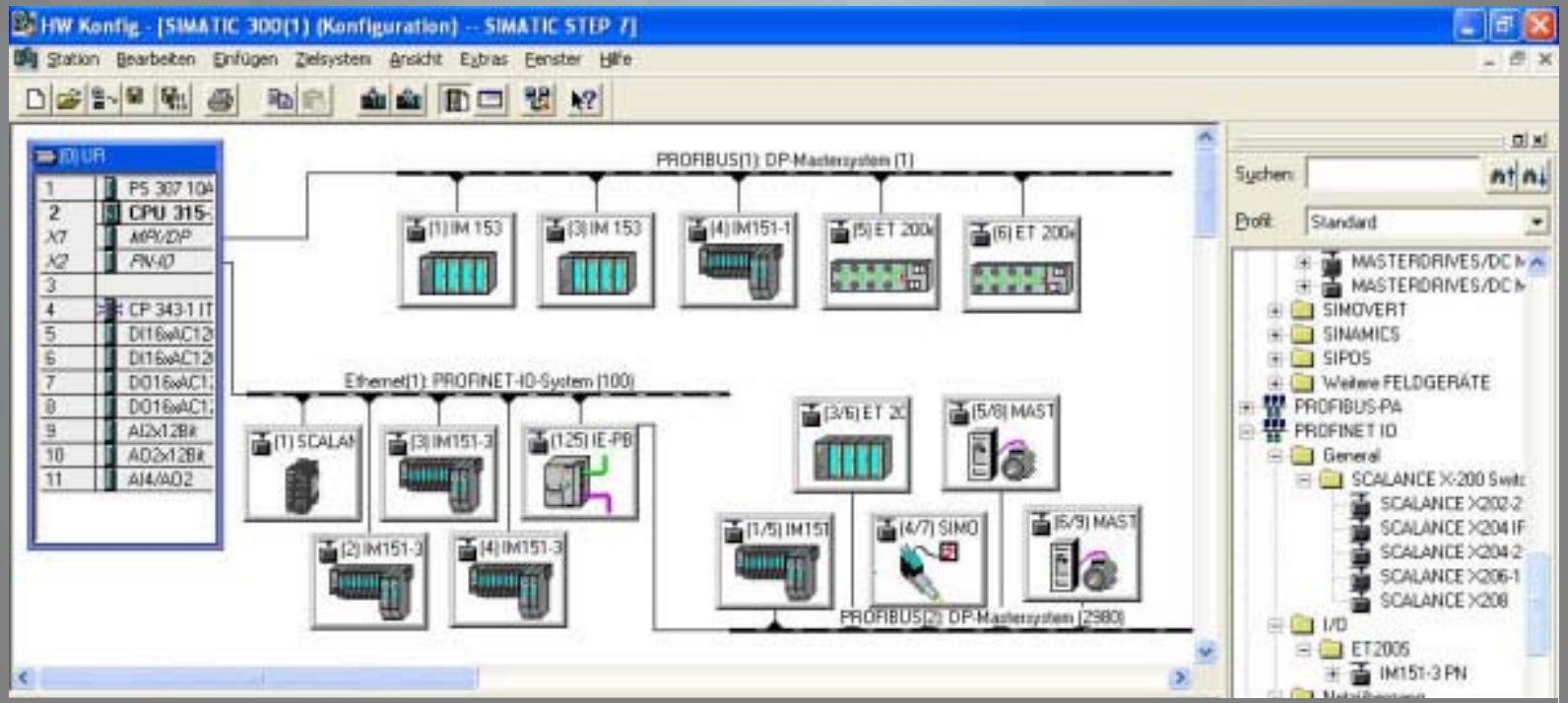
- Security of SCADA
  - Trend: towards commercial-over-the-shelf (COTS) platforms
  - Network segregation, Physical isolation
  - Change Control
  - Consequence of Security Breach
    - Steal information
    - Disable system safeguards
    - Trigger action outside normal operations
    - Cause permanent damage to system
    - Cause danger to human life

Security of SCADA



HKCERT

What did Stuxent do?



- Spread itself via different channels
- Connect to C&C to get command and send data
- Search for Siemens Simatic WinCC and PCS 7 SCADA systems. Try to gain access to backend database

Spread of Stuxnet

- 3 channels
  - USB drive & removable media (slow)

Copy of Copy of Copy of Copy of Shortcut to.lnk
Copy of Copy of Copy of Shortcut to.lnk
Copy of Copy of Shortcut to.lnk
Copy of Shortcut to.lnk
~wtr4132.tmp (worm)
~wtr4141.tmp (worm)

    - you may see the files briefly displayed in Windows Explorer, and then disappear a few seconds later (rootkit installed)
  - LAN (fast)
  - infected Siemens project files (WinCC & STEP 7)

Spread of Stuxnet

- Removable device
  - Exploit a vulnerability that Windows display icons of shortcut files (.LNK) - MS10-046, 0-day
- LAN
  - Copy to print servers - MS10-061, 0-day
  - Attack an old (used by Conficker) RPC vulnerability - MS08-067
- Escalation of privilege
  - Win2000/XP - MS10-073, 0-day
  - Vista/Win7.Win2008 - MS10-0xx, 0-day
- (Earlier version) use autorun.inf to infect USB drives

- Contact Siemens WinCC SQLServer and installs itself on those servers via database calls (CVE-2010-2772) 0-day
  - Siemens Simatic WinCC and PCS 7 SCADA system (hard-coded password)
- Puts copies of itself into Siemens STEP 7 project files to auto-execute whenever the files are loaded.

Spread of Stuxnet : the birth

- Can you suggest possible ways the first instance of Stuxnet got started?
  - Pass an infected USB to factory employee who have access to the PLC
    - Exchange of technical document
    - Trade show free USB drive gift
  - Targeted email → client side attack
    - PDF or MS Office document
  - Supply infected PLC project file (contractor/client channel)

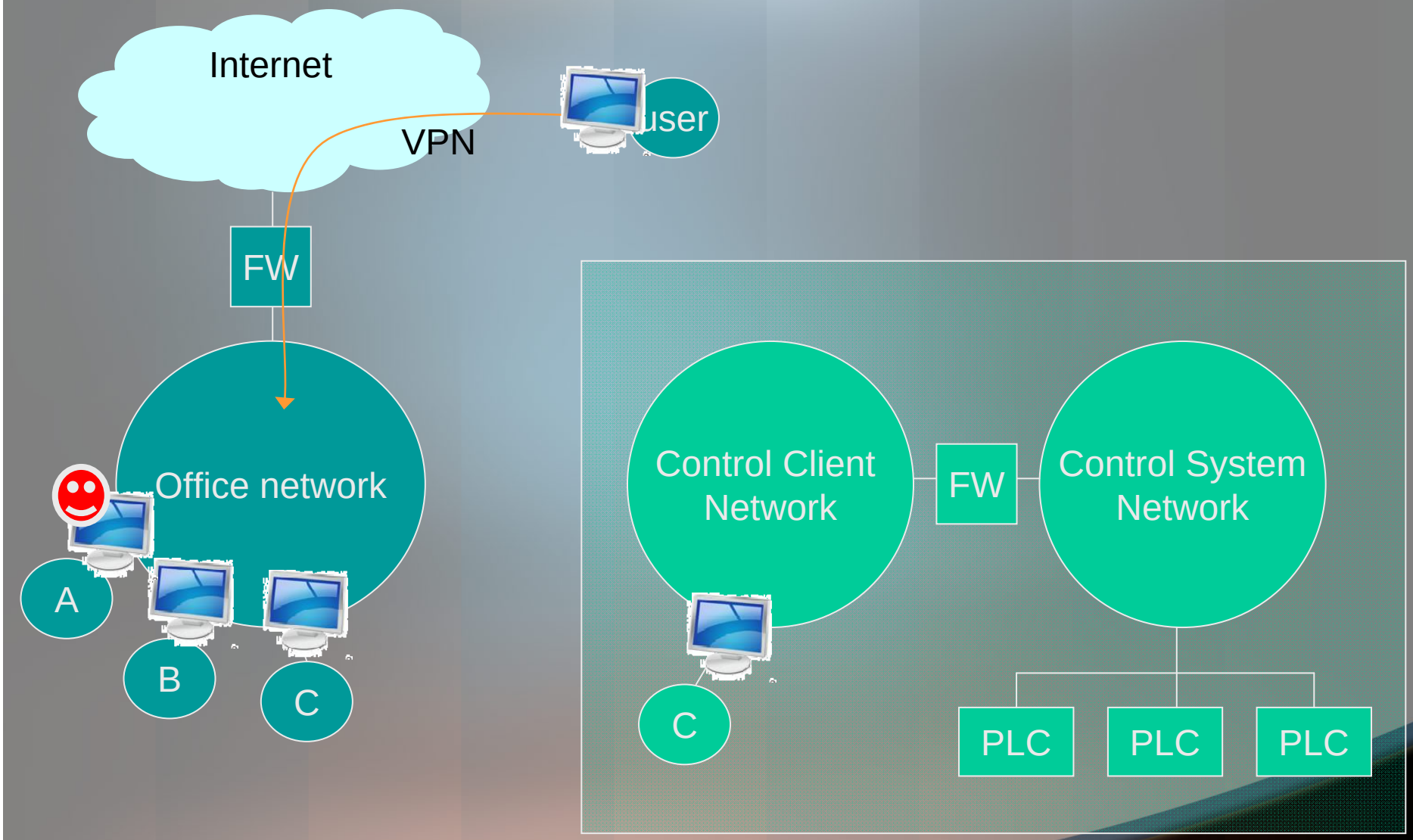
Stuxnet: break the silent rule

- It is a worm! It breaks the silent rule of targeted attacks

- Controversy: why spread via USB
  - This arouse attention!
  - Some said “excellent technology failing in implementation”

  - I do think they make sense.
  - It is a balance of “security” and “effectiveness” → a need to jump over the “air gap”

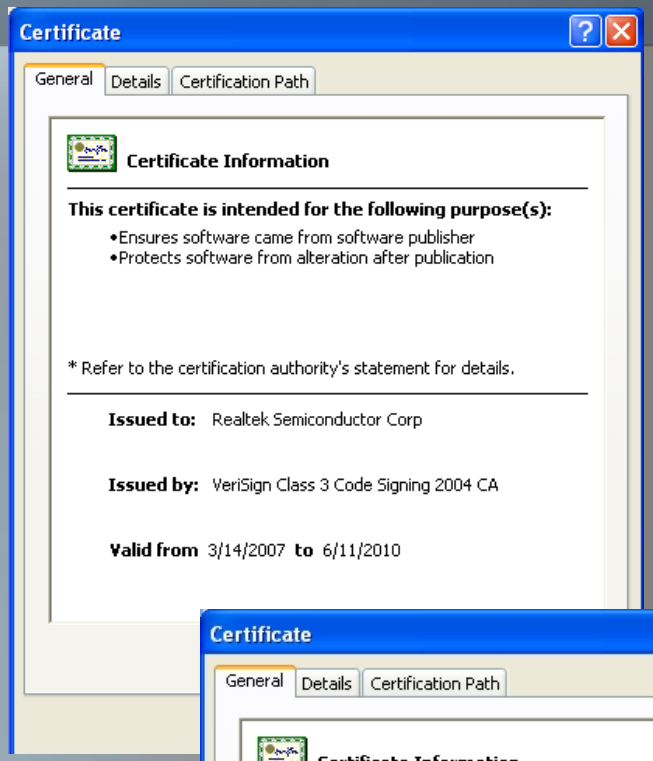
Security of SCADA

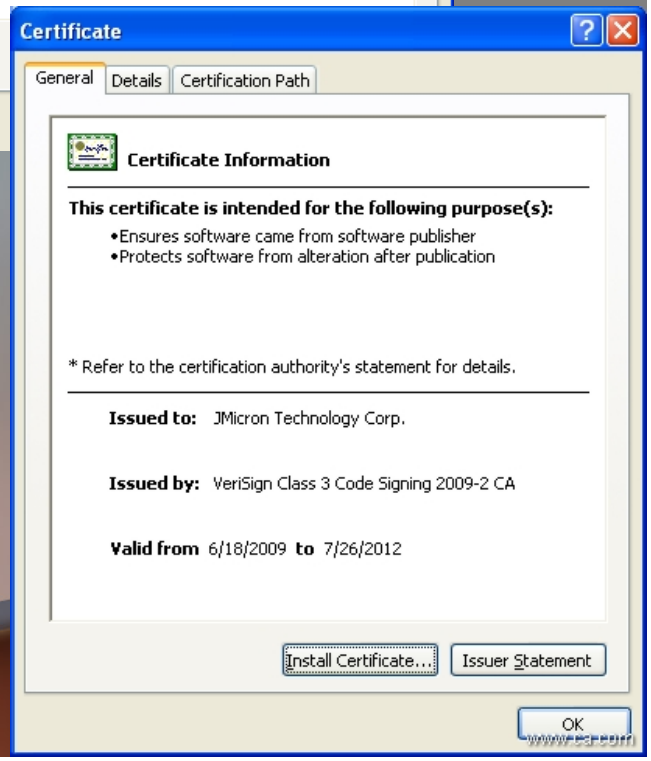


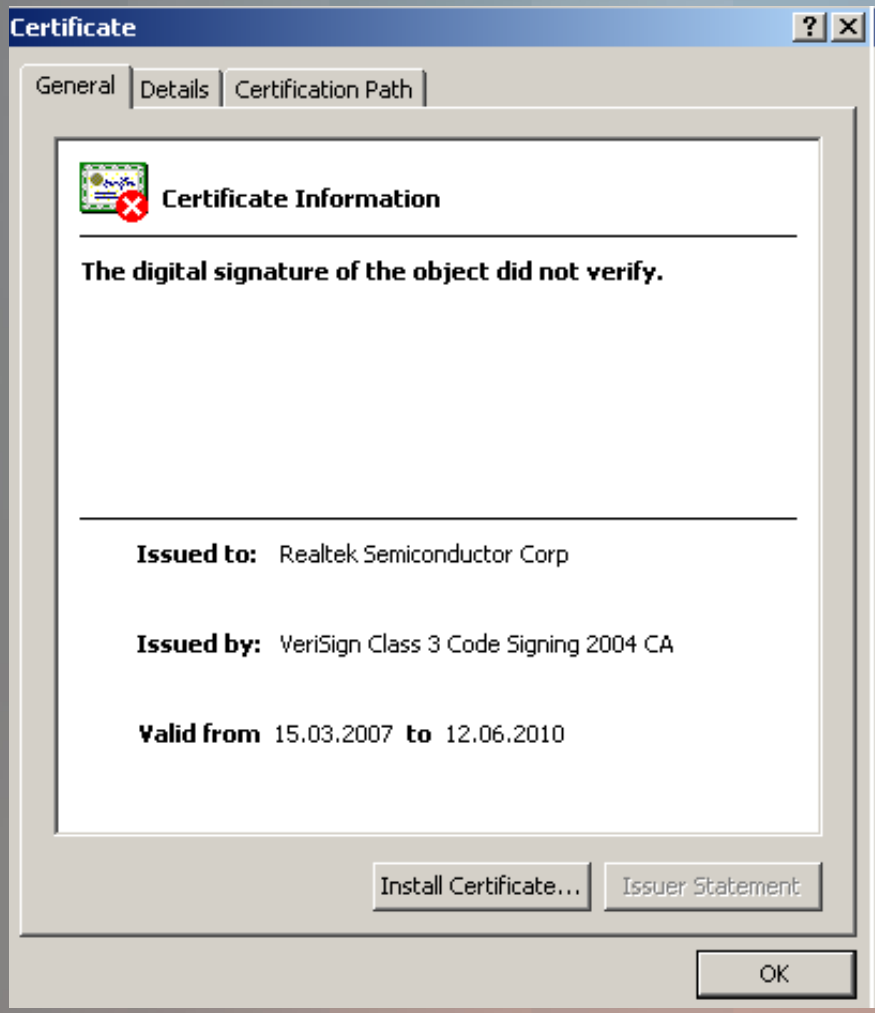
HKCERT

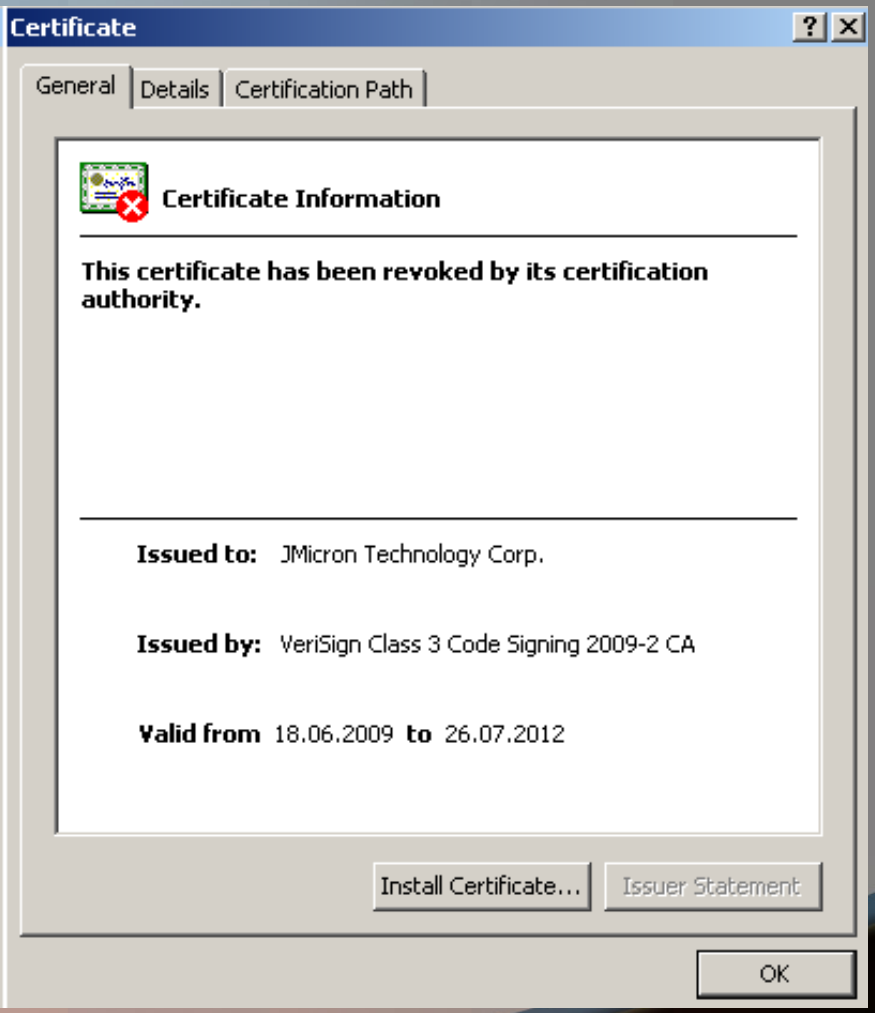
Install Stuxnet

- Create 2 services
  - MRXCLS.sys
  - MRXNET.sys
- Files signed by stolen digital certificates
  - Realtek Semiconductor
    - informed 24-Jun, cert revoked 17-Jul;
  - JMicron Technology
    - cert appeared 14-Jul
- MRXCLS.sys
  - compiled 01-01-2009
  - signed 25-01-2010
  - Inject code into current process
- Install a rootkit to hide Stuxnet
- If Siemens SIMATIC WinCC is found, replace the S7OTXDX.dll with a wrapper and intercept all commands





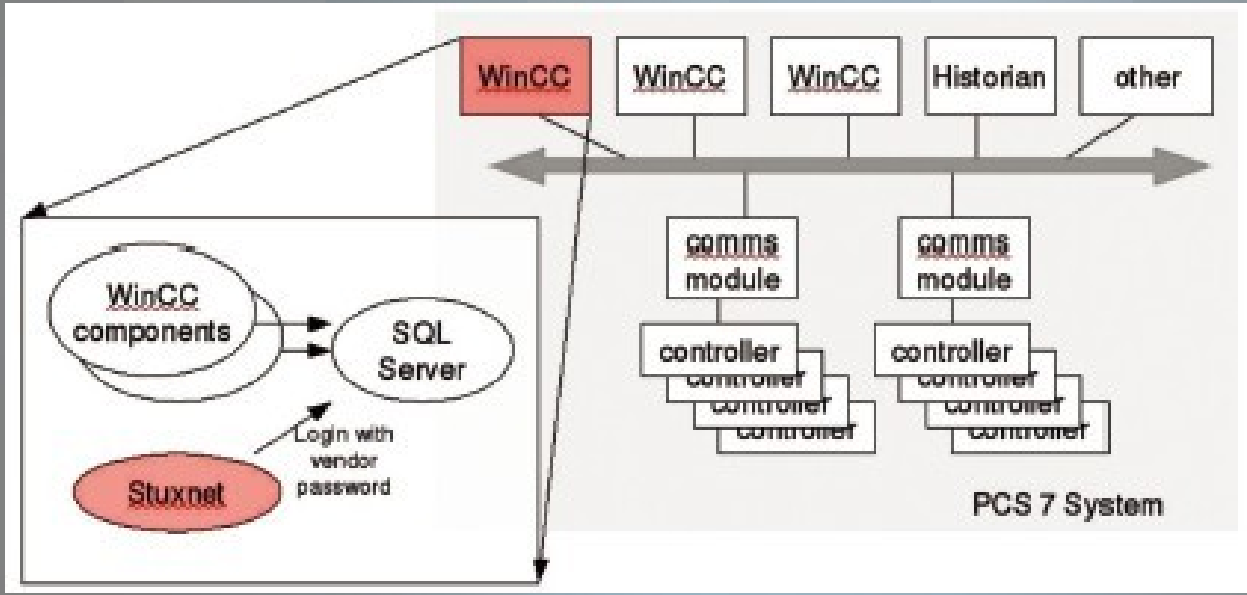




Targeted Attack

HKCERT

Attack Siemens PLC



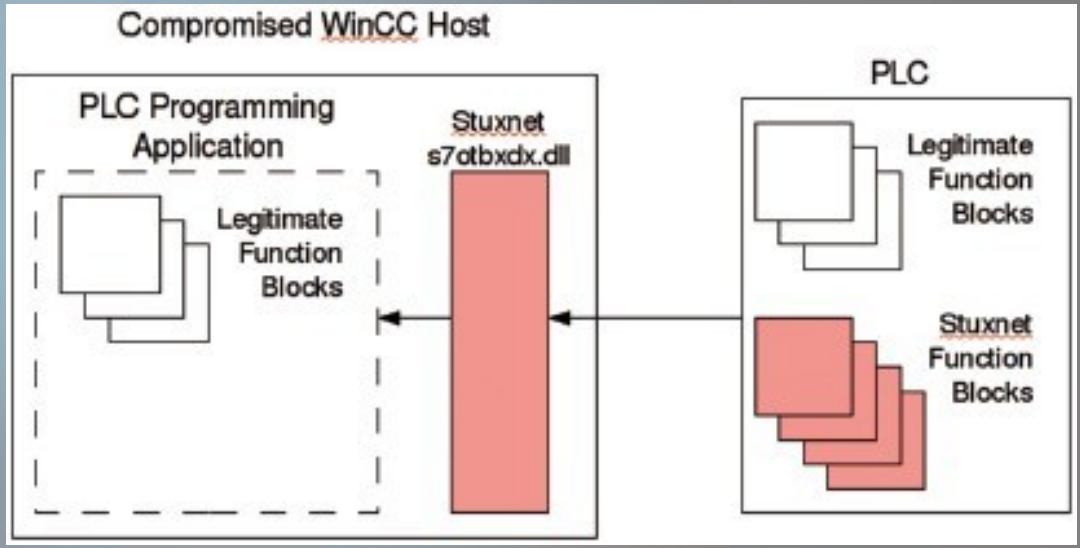
http://www.iebmedia.com/index.php?id=7409&parentid=63&themeid=255&hft=61&showdetail=true&bb=1

- Attempt to connect to the WinCC SCADA visualization system, using the default password from Siemens.
  - Stuxnet.dll contains code (uid=WinCCConnect;pwd=(removed)########) to connect to database server to dump database tables to disk, and possibly inject/execute a binary on the database server
- The Stuxnet version of S7OTXDX.dll act as a wrapper to connect to WinCC, intercept commands and modify data, while redirecting the rest of the functions to the original dll.
- Can delete the database to remove traces of commands issued

Attack Siemens PLC

- The Stuxnet version of S7OTXDX.dll act as a wrapper to connect to WinCC, intercept commands and modify data, while redirecting the rest of the functions to the original dll.

s7db_open
s7blk_write
s7blk_findfirst
s7blk_findnext
s7blk_read
s7_event
s7ag_test
s7ag_read_szl
s7blk_delete
s7ag_link_in
s7db_close
s7ag_bub_cycl_read_create
s7ag_bub_read_var
s7ag_bub_write_var
s7ag_bub_read_var_seg
s7ag_bub_write_var_seg



Network behaviour

- C&C
  - Connect to two URLs to get commands
    - www.mypremierfutbol.com
    - www.todaysfutbol.com
  - Send encrypted information to the URL:
    - http://<c&c>/index.php?data=<data>
- P2P
  - installed an RPC server and client
  - Any other infected computer on the network can connect to the RPC server and exchange version number and software

Timeline

- Jan 2009 Stuxnet complied

- Jan Stuxnet MRXCLS.sys signed
- Jun Stuxnet discovered
- Jun-24 Realtek informed of stolen cert
- Jul-14 Siemens acknowledge knowledge
- Jul-15 US-CERT advisories
- Jul-16 Microsoft advisory
- Jul-16 JMicron certificate appeared
- Jul-17 Verisign revoked Realtek cert
- Aug 2 MS patched LNK vulnerability
- Sep 14 MS patched print spooler vulnerability

After Stuxnet

- Most AV can detect Stuxnet worm
- Some Stuxnet cleaning tools appeared
- Microsoft released patches to 0-day vulnerabilities
- Microsoft closed Autorun 2011-Feb
- *** Systems with hardcoded password can hardly be revamped without very great effort

Implications

What are the implications?

- SCADA security issues
  - Weak default configuration, slow patch
  - Awareness of plant engineer focused on safety and availability but less on security. Some don't believe this is a threat or don't' believe their systems are sufficiently exposed to that threat.
    - By Walt Sikora, Industrial Defender's VP of Security Solutions,
- Current AV, IDS, etc. are not sufficient to deter targeted attack.
- If system cannot be patched it can be disastrous

What are the implications?

- New era of SCADA attack
  - First rootkit in SCADA
  - Success (or failure?) or semi-targeted attack
  - Botnet successful getting into SCADA network
- Professional and determined attacker out there
  - Several 0-day vulnerabilities
  - Two real digital certificates
  - Able to bypass the front door, able to climb over the wall if you have no door
- State sponsored cyber attacks surface?
- Progress of Advanced Persistent Threat (APT)?

Advanced Persistent Threat (APT)

- Very targeted to victim
- Good knowledge of victim and leverage on which to compromise
- Most targets are high level leaders in organization, or key persons with access to critical infrastructure components
- Maintain their presence in victim organization
- Repeated seek to regain presence

- Non-scalable: cost is high
- More sophisticated
- More knowledge of target

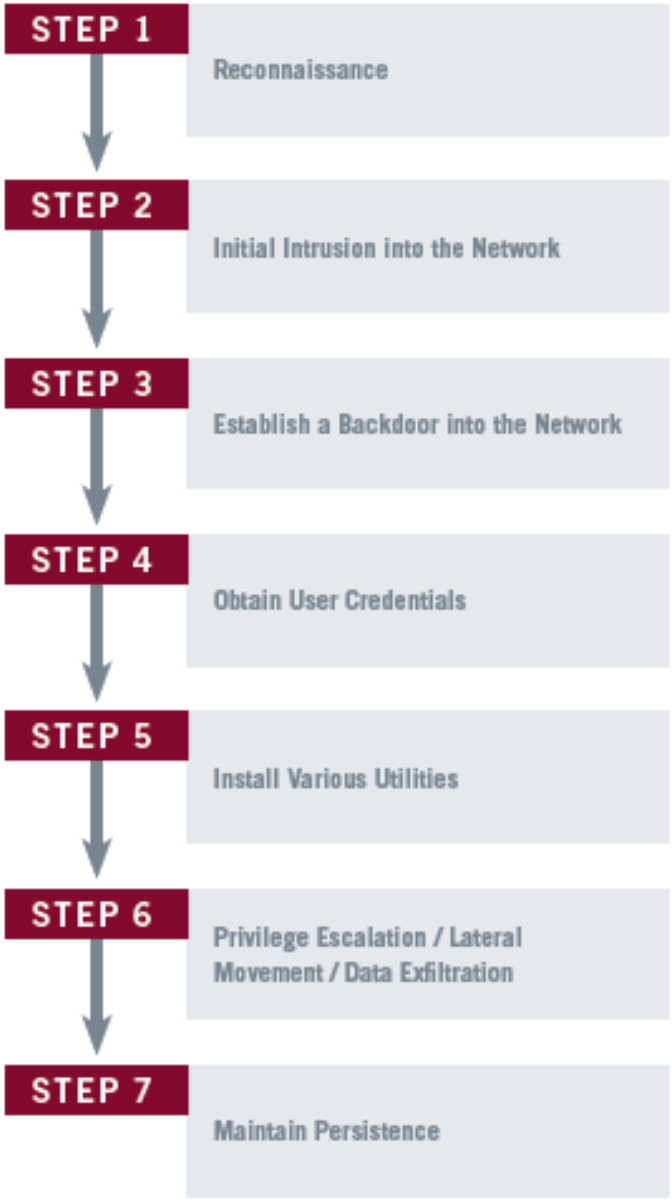
APT experts comment

- Mandiat Report
  - Only 24% malware used in attack are detected by security software
  - APT is reality … not just government and defense … at commercial level as well
  - Sometimes more than one teams. They do not even know other's existence
  - They usually use outbound HTTP, process inject to hide
  - Very slim: average 121.85KB
- Verizon Data Breach Report 2010
  - 87% had evidence of breach in log files, yet missed it

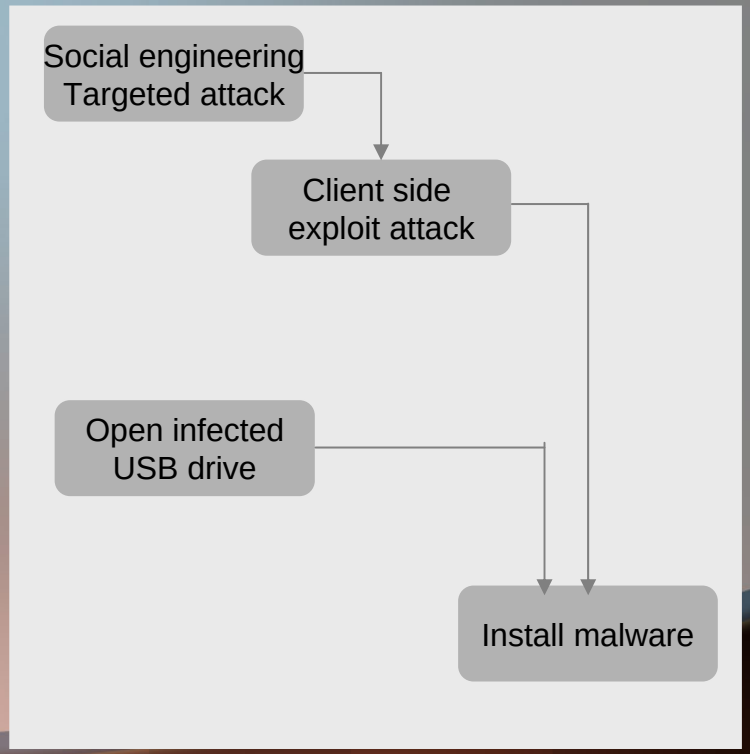
Why is it more dangerous?

- Commercial
  - Target CxOs at financial institution who have access to confidential information like trade secret, financial data, banking information
- Critical Infrastructure
  - Disrupt operation of organization which is essential to the living (utilities, communication, transport) or life of citizens

APT exploitation life cycle



- Reconnaissance
  - Get into the circle and listen (FB, physical contact), get familiarize with the language and tone used
  - Research and identify individuals they will target in the attacks, using public search or other methods to get their contact



Source: Mandiant M-Trends

HKCERT

Mitigation Measures

APT Risk Mitigation Highlights

- Control both inbound and outbound traffic
- Log Management
  - Monitor Dynamic DNS names via log
  - Log aggregation
- Build up internal network surveillance capability
- End-point security
  - Disable local administrative access
- Audit VPN access
- Awareness Education

Ref: ISEC Partners on “Aurora Response Recommendation”

APT Incident Response

- Richard Bejtlich [CIRT level response to APT]:
  - Not just to prevent compromise, but
    - Track the attacker tactics, tools and process to preempt attacks
    - Intrusion suppression
    - Increase the cost of the adversary
  - During 1st hour of APT incident
    - Document, change communication pattern
  - During 1st day
    - Alternate computing infrastructure, trusted communication among IR members
  - During 1st week
    - Source help
    - Initial briefing

Thank You

scleung@hkcert.org