

# Recent Cyber Attack Cases in Taiwan

TWNCERT

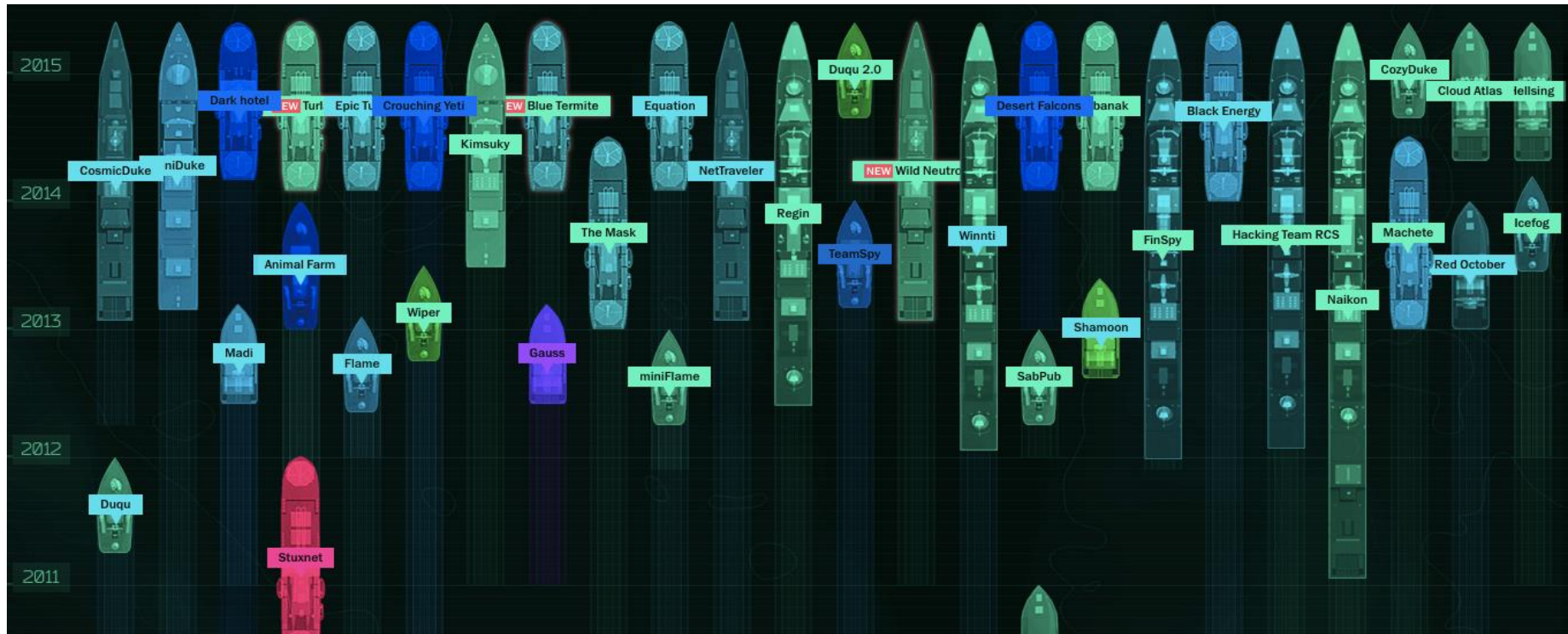
(National Center for Cyber Security Technology)

- Cyber Attack Trends in Taiwan
- Cyber Attack Cases Studies
  - Attack via Network Equipment
  - Attack via AD Golden Ticket
  - Attack via Third Party Software
- Conclusions

- Cyber Attack Trends in Taiwan
- Cyber Attack Cases Studies
  - Attack via Network Equipment
  - Attack via AD Golden Ticket
  - Attack via Third Party Software
- Conclusions

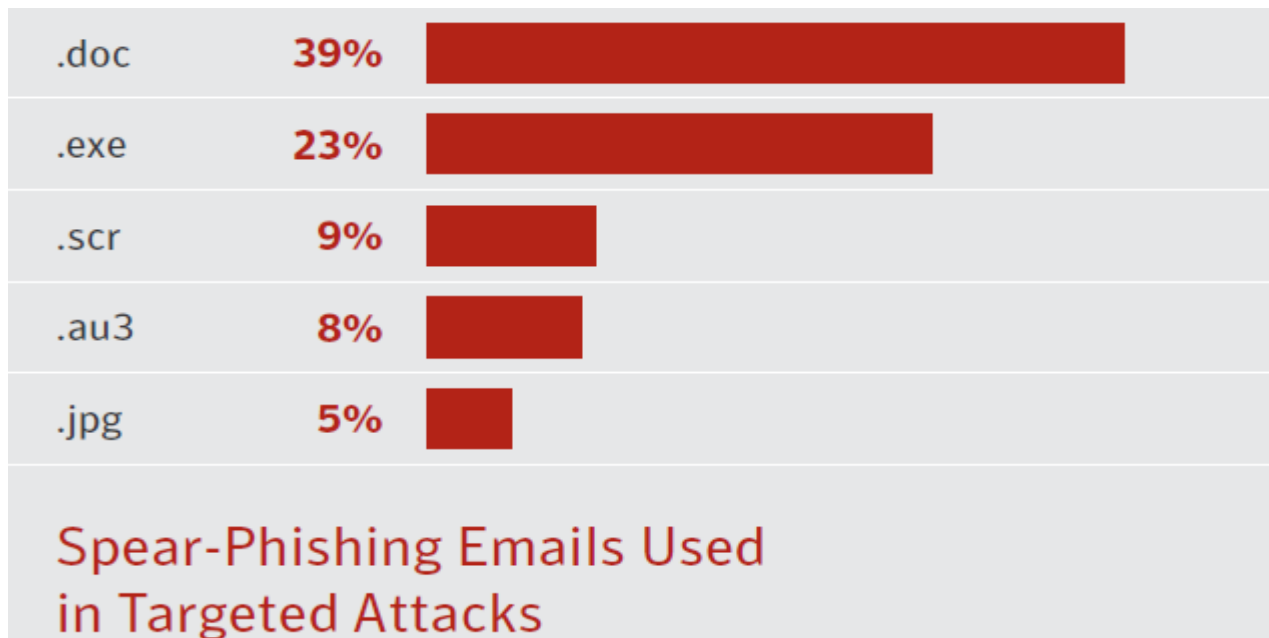
# APT Hackers Around the Globe

- There are over 20 APT hacker teams operates actively around the Globe during 2014 ~ 2015
- Besides the US, UK, China, Russia, and Israel, there are many new APT hacker teams come from North Korea and Middle East



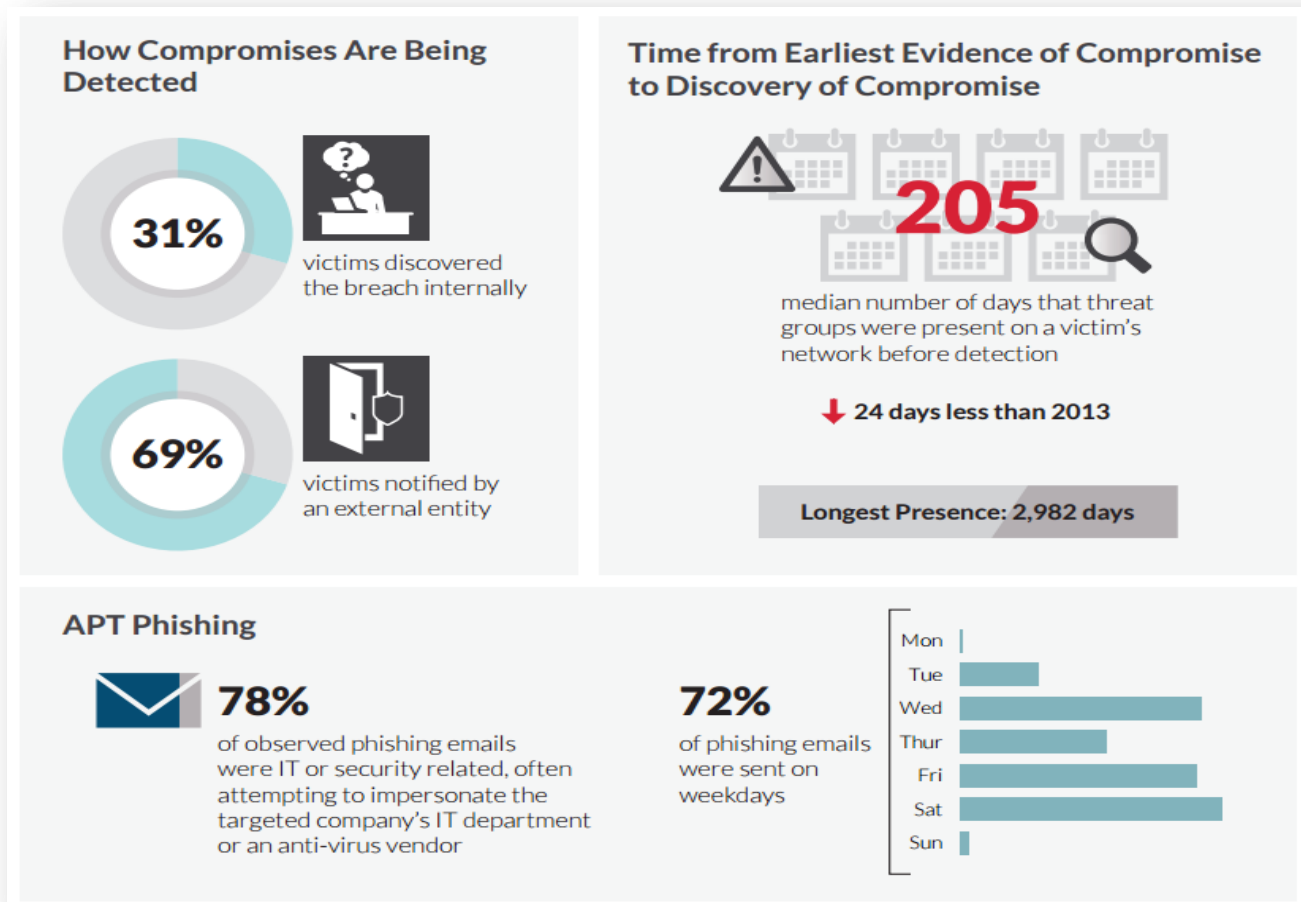
Source : <https://apt.securelist.com/>

- APT still is the main cyber threats of Taiwan government agencies, via vulnerabilities plus phishing mails
- APT Attack Analysis
  - 91% of APT Attacks started from a spear phishing e-mail
    - 94% of spear phishing e-mails have attachment files
    - Most common file types are .doc 、 .exe 、 .scr 、 .au3 、 .jpg 、 .pdf

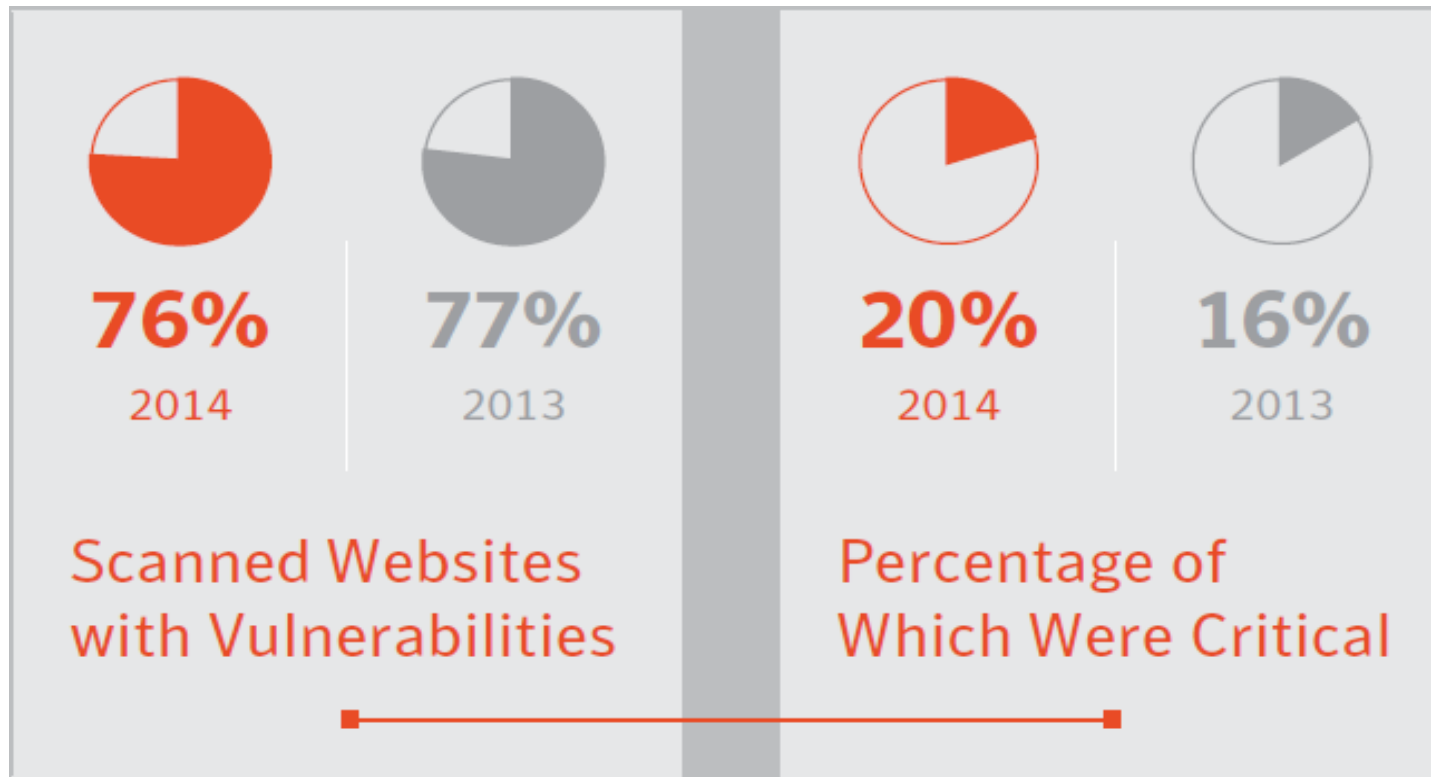


# Hard to Detect

- APT attacks are very hard to detect
  - It took average of **205** days before APT attacks were being detected !!!

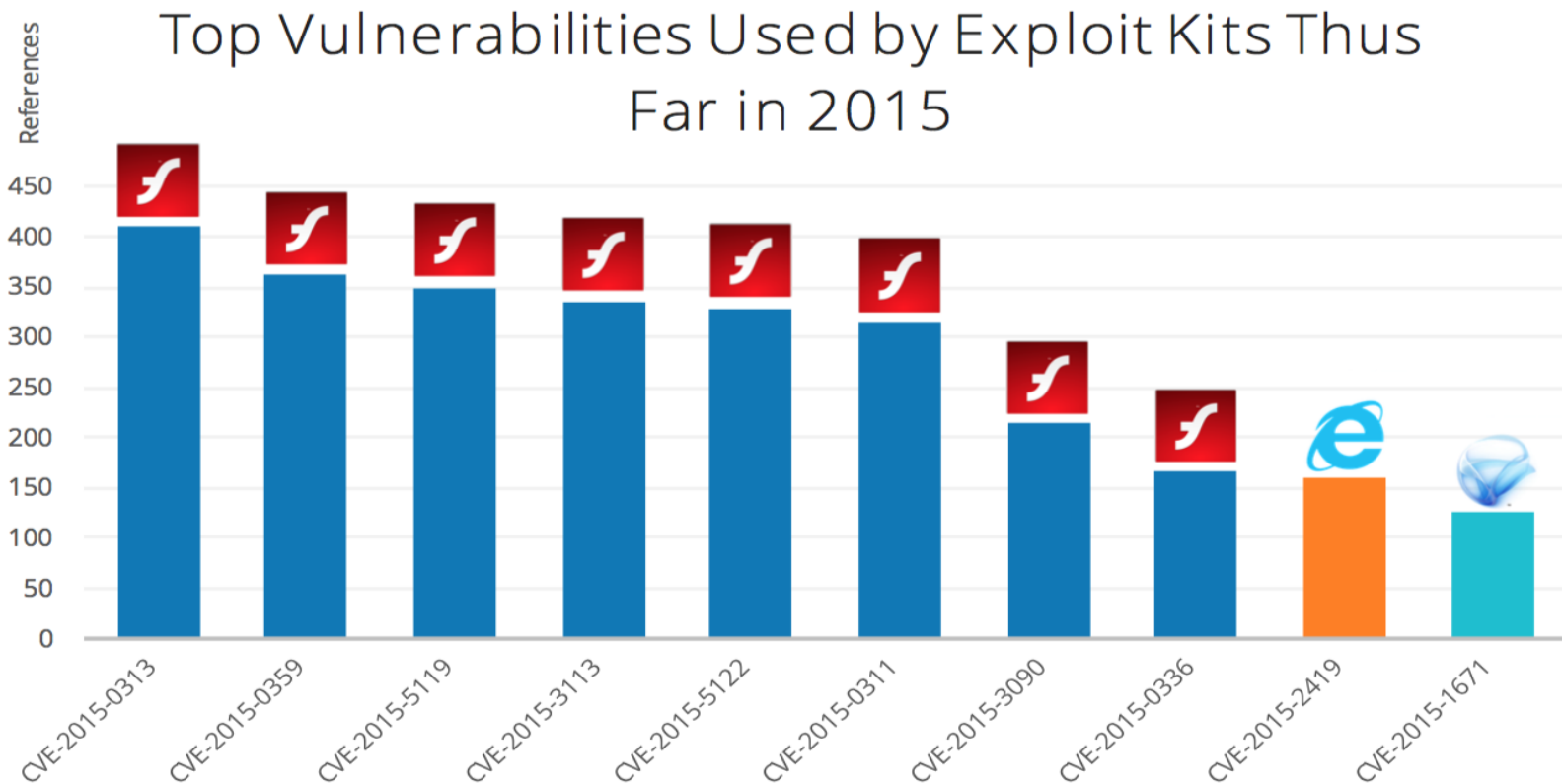


- So far, most websites around the globe still have vulnerabilities
  - It is not easy to update some web third-party applications, plus many web developers lack cyber security awareness, so there are still vulnerabilities exist in many websites



# Top 10 Vulnerabilities in 2015

- The top 10 most often used vulnerabilities
  - These vulnerabilities are triggered easily and have greater effects





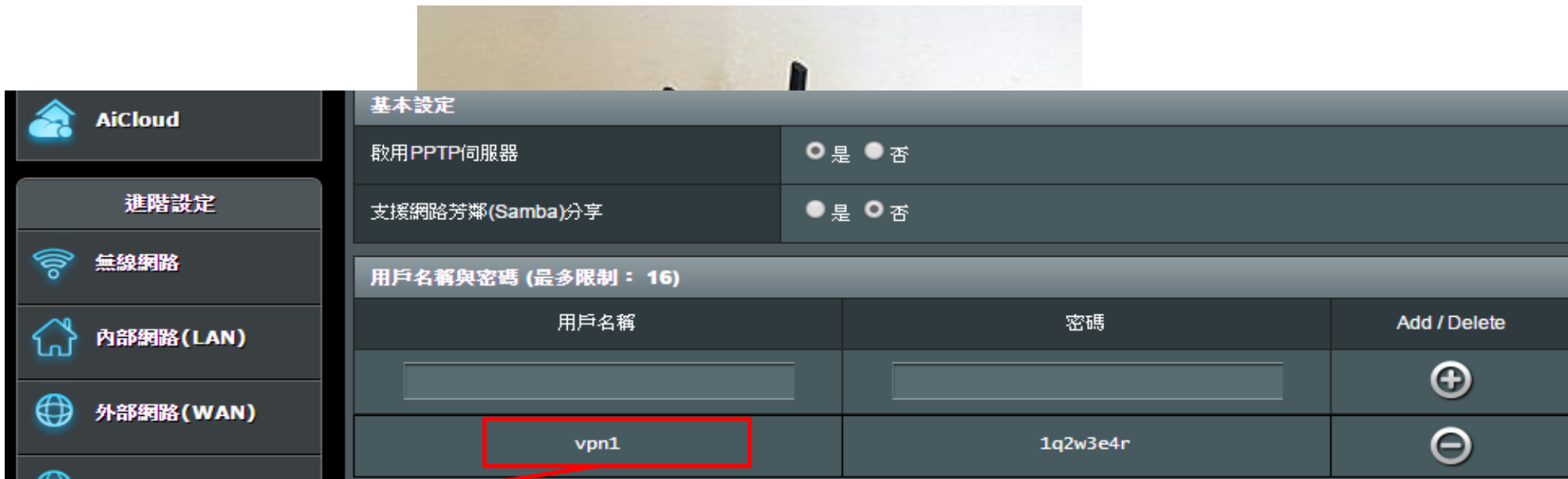
- Cyber Attack Trends in Taiwan
- Cyber Attack Cases Studies
  - Attack via Network Equipment
  - Attack via AD Golden Ticket
  - Attack via Third Party Software
- Conclusions

- Network equipment are hard to manage, and very easily get hacked
  - Network equipment has many varieties, and manufacturers usually do not have proper patch management or update process, plus the users neglects on setup(ex. use default password), thus hackers can hack into network equipments very easily
  - Network equipment has vulnerabilities just like PCs, if there are no proper updates, it will be hard to defend the invasion of hackers
- Hacking network equipment is old news, but hackers continue to do so because it relatively easy
  - Since 2011, there are cases of hackers invade network equipments and use as C&C every year in Taiwan

- We were collecting phishing mails and analyzed them
  - We extracted the malware from attachments and links
  - We found a C&C IP within the malware
- We traced this C&C IP, and found it was located in a civilian household
  - According to the owner, he would shut down the computer when it was not in use. It was not on 24 hours
  - But hackers usually would pick computers which operates 24 hours to be the C&C

# It is a Wireless Router

- The C&C actually is a wireless router
  - After careful investigation, we found out that the C&C is actually a wireless router. The hacker got into the router easily because the default password was still in use.
  - The hacker got in and turned on the built-in VPN function



The account created by hacker

- Router transferred packets automatically
  - By looking at the setting, the hacker transferred all packets came from port 80, 443 to 192.168.10.2
  - 192.168.10.2 is the VPN IP, so when the hacker connected to the VPN service of this router, he would continuously receive victims' reporting packets sending through port 80, 443



服務名稱	通訊埠範圍	本地 IP	本地通訊埠	通訊協定	Add / Delete
				TCP	+
https	443	192.168.10.2	443	TCP	-
http	80	192.168.10.2	80	TCP	-

# Looking at the Log

- From the router log we could find the record of the hacker activities
  - An outside IP (111.175.\*.\*) was using the VPN service
  - That IP used VPN IP 192.168.10.2

```
Jul 23 08:13:31 pptpd[3533]: CTRL: Starting call (launching pppd, opening GRE)
Jul 23 08:13:31 pptp[3534]: Plugin pptp.so loaded.
Jul 23 08:13:31 pptp[3534]: PPTP plugin version 0.8.5 compiled for pppd-2.4.5, linux-2.6.22.19
Jul 23 08:13:31 pptp[3534]: pppd 2.4.5 started by admin, uid 0
Jul 23 08:13:31 pptp[3534]: Using interface ppp10
Jul 23 08:13:31 pptp[3534]: Connect: ppp10 <--> pptp (111.175. )
Jul 23 08:13:34 pptpd[3533]: CTRL: Ignored a SET LINK INFO packet with real ACCMs!
Jul 23 08:13:35 pptp[3534]: MPPC/MPPE 128-bit stateless compression enabled
Jul 23 08:13:35 pptp[3534]: Cannot determine ethernet address for proxy ARP
Jul 23 08:13:35 pptp[3534]: local IP address 192.168.1.1
Jul 23 08:13:35 pptp[3534]: remote IP address 192.168.10.2
```

The hacker used the VPN service

The VPN IP that hacker used

- This wireless router was set to transfer packets automatically
  - The hacker only needed to connect to the VPN service, then it will receive all packets automatically
  - After further investigation, victims were not only the Taiwan government agencies, there are other countries IP such as U.S., France, U.K., and Germany, reported to this C&C
  - We have sent alert info to CERTs of these countries

# Recommendations

---

- Make sure all network equipments within the organization are under security supervisions
  - Need to know all network equipments with in the organization
  - Check for security patches and updates regularly
  - Change the default password
  - Set the firewall rule to deny outside connection to network equipments



- Cyber Attack Trends in Taiwan
- Cyber Attack Cases Studies
  - Attack via Network Equipment
  - Attack via AD Golden Ticket
  - Attack via Third Party Software
- Conclusions

- Unusual login record in the log
  - One agency reported, one of the users had unusual login record on AD (using other user's PC to login), so it asked us to investigate



Mary's PC



Using Peter's account  
to login



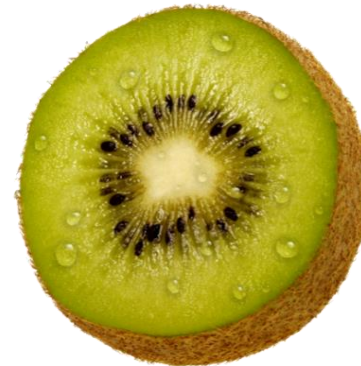
Try to access  
John's PC

# New Hacker Tool

- After initial investigation we found:
  - Mary's PC has been hacked for two years and the hacker planted Trojan into her PC
  - Peter's PC and the Domain Controller were also checked, but **no problem was found**
  - Further analysis, a hacker tool named Mimikatz was found on Mary's PC



Mary's PC



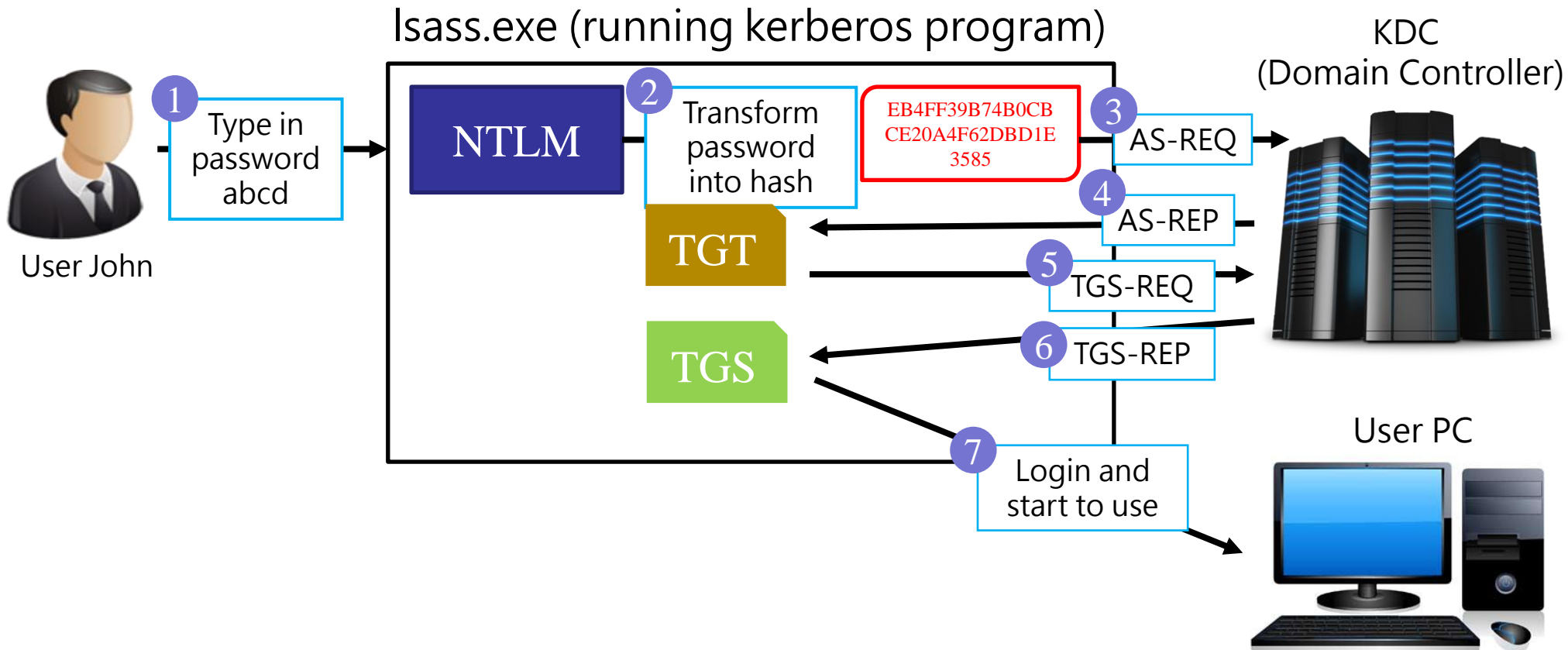
Mimikatz

- Hacker Tool : Mimikatz
  - Primarily used for **Pass-The-Ticket attack**
- Pass-The-Ticket Attack
  - Currently the Active Directory uses Kerberos to Authenticate, which the Pass-The-Ticket attack aims. If the attack is able to gain **TGT(Ticket Granting Ticket)** access, it does not need the password of the user, and **use the identity of the user** to login
  - The user's TGT is valid for 10 hours

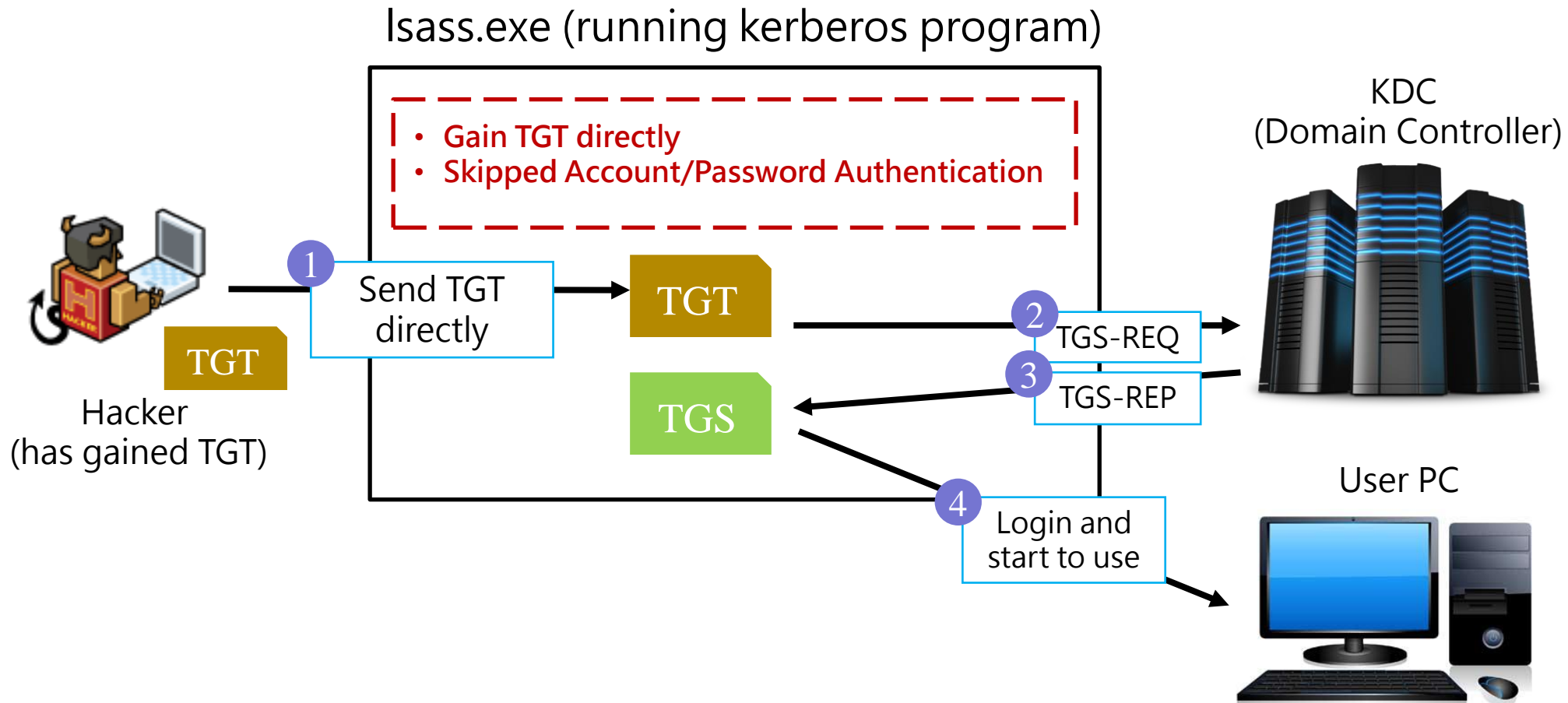


# Kerberos Authentication

- Normal Authentication Process (with Active Directory)



## • Pass-The-Ticket Attack



# The Golden Ticket

- Use System TGT to generate User TGT
  - Except the User TGTs, there is a **System built-in TGT (The Golden Ticket)**. Its function is to generate user TGTs. So if the Hacker has gained the System TGT, he can login as **any user** !!!
- The GoldenTicket
  - The System TGT is stored at account **krbtgt's password hash** (NTLM hash). This system account is automatically created after the AD setup is completed
  - The password of the account krbtgt is only stored in the Domain Controller, the hacker has to hack into the Domain Controller to get it !!!

- HOW?

- After careful investigation, only Mary's PC was hacked in this incident, no other PCs or systems were hacked
- So how did the hacker gain the krbtgt's password hash?
  - krbtgt's password hash (NTLM hash) is only stored in the Domain Controller

- After we looked through the incident handling record, this agency was hacked two years ago

- This agency reinstalled Domain Controller, built the new network infrastructure, enhanced security management process, purchased new defensive devices, started SOC services, and forced all users to change their passwords periodically
- But the password of krbtgt account did not change, the password of this account default expires in 10 years



# How to Detect This Attack?

- Check **Domain** System Security Log

–1. Account and source IP does not match (Event ID : 4624)

Type	Date	Time	Event	Source	Category
Audit Success	2015/9/8	上午 07:36:43	4624	Microsoft-Windows-Sec	登入



  

Description	
帳戶成功登入。	
主旨:	
安全性識別碼:	S-1-0-0
帳戶名稱:	-
帳戶網域:	-
登入識別碼:	0x0
登入類型:	3
新登入:	
安全性識別碼:	S-1-5-21-705273604-3707611877-3454562850-1000
帳戶名稱:	ART
帳戶網域:	CSI
登入識別碼:	0xf557c13
登入 GUID:	{A384ADBB-8955-6555-0B85-36A67A396DE7}
處理程序資訊:	
處理程序識別碼:	0x0
處理程序名稱:	-
網路資訊:	
工作站名稱:	
來源網路位址:	192.168.124.2
來源連接埠:	49601

The user's PC does not use this IP

# How to Detect This Attack?

- Check **Local or Domain** System Security Log
  - 2. SID does not match the account name (Event ID : 4624)

Type	Date	Time	Event	Source	Category
 Audit Success	2015/9/7	下午 05:53:37	4624	Microsoft-Windows-Sec	登入
 Audit Success	2015/9/7	下午 05:52:46	4624	Microsoft-Windows-Sec	登入

**Description**

帳戶成功登入。

主旨:

安全性識別碼: S-1-0-0

帳戶名稱: -

帳戶網域: -

登入識別碼: 0x0

登入類型: 3

新登入:

安全性識別碼: **S-1-5-21-705273604-3707611877-3454562850-1111**

帳戶名稱: administrator

帳戶網域: csi

登入識別碼: 0x2d654


登入 GUID: {9375A84D-52B1-0F41-F682-06CA9EAD2E93}

The SID of Administrator should end with 500, not 1111

# How to Detect This Attack?

- Check **Local or Domain** System Security Log

- 3. Account Domain is in wrong format (Event ID : 4624 、 4672)

Type	Date	Time	Event	Source	Category
 Audit Success	2015/9/7	下午 05:04:41	4624	Microsoft-Windows-Sec	登入

Description	
帳戶成功登入。	
主旨:	
安全性識別碼:	S-1-0-0
帳戶名稱:	-
帳戶網域:	-
登入識別碼:	0x0
登入類型:	3
新登入:	
安全性識別碼:	S-1-5-21-705273604-3707611877-3454562850-500
帳戶名稱:	administrator
帳戶網域:	<3 eo.oe ~ ANSSI E>
登入識別碼:	0x5b185
登入 GUID:	{D7E857AA-E29A-7FDD-E6E5-A672FED6B030}

Account Domain is weird string, FQDN or empty. The proper format should be the domain abbreviation

-----Example-----  
 FQDN : abc.gov.tw  
 domain abbreviation : abc

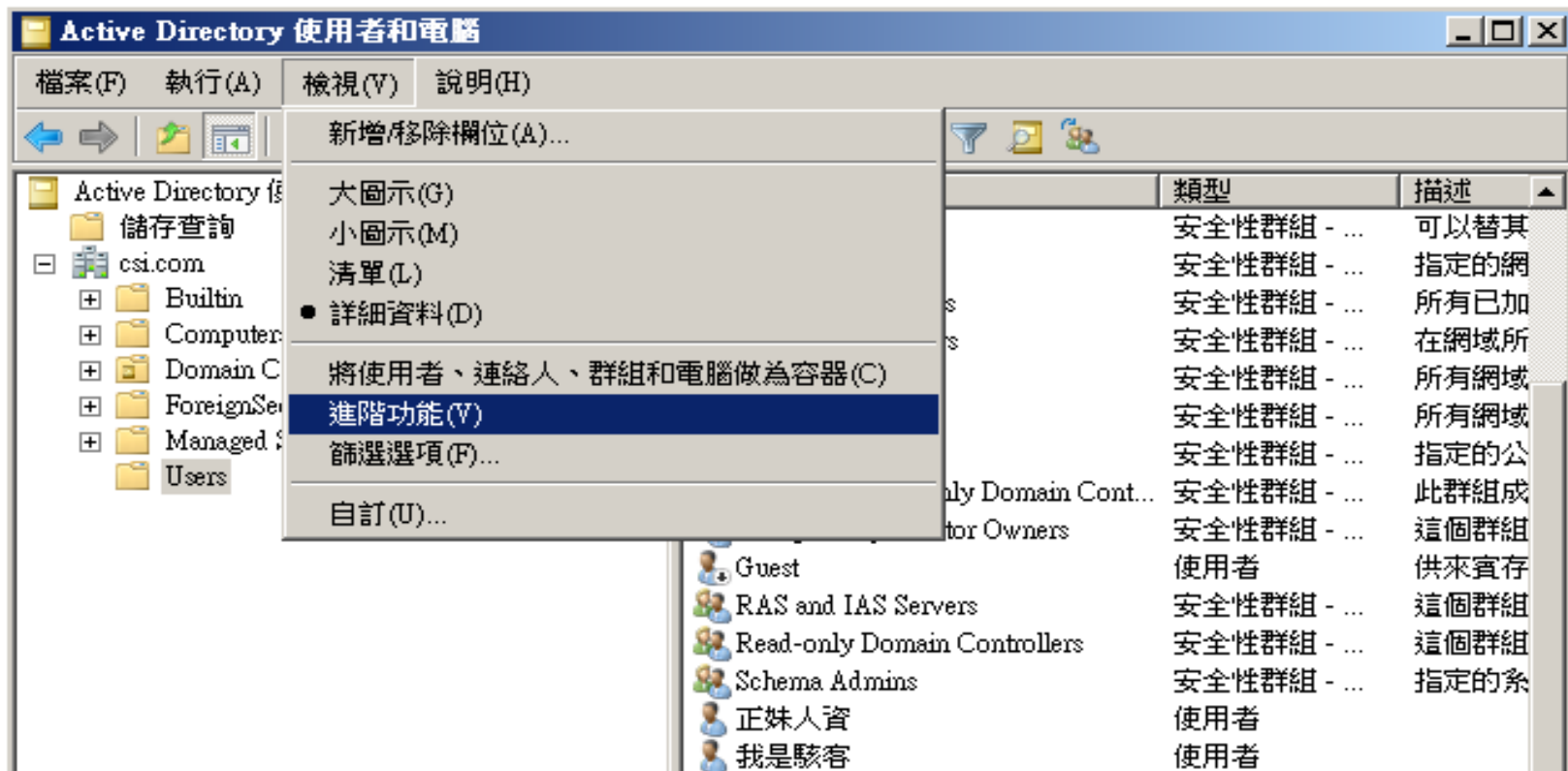
# How to Detect This Attack?

- Check **Local or Domain** System Security Log
  - 3. Account Domain is in wrong format (Event ID : 4624 、 4672)
    - The malware Mimikatz is open-sourced, so there are many various versions, and some versions will leave weird account domain names in the security log, while others will leave the field empty



# Recommendations

- If hit by this attack for sure, you need to change krbtgt account password **twice**
  - In Active Directory Users and Computer MMC, open 「view」 → 「advanced」




# Recommendations

- If hit by this attack for sure, you need to change krbtgt account password **twice**
  - Right click account 「krbtgt」 → 「reset password」 and restart



# Recommendations

- The error might occur in the System Security Log after password is changed (Event ID : 4769)
  - Error code **0x1f** means someone tried to login with the old hash and failed, it is normal to have these errors within **10** hours after password has changed

Type	Date	Time	Event	Source	Category
 Audit Failure	2015/11/11	下午 05:05:30	4769	Microsoft-Windows-Sec	Kerberos 服務票證操作

Description	
已要求 Kerberos 服務票證。	
帳戶資訊:	
帳戶名稱:	
帳戶網域:	
登入 GUID:	{00000000-0000-0000-0000-0
服務資訊:	
服務名稱:	
服務識別碼:	S-1-0-0
網路資訊:	
用戶端位址:	::ffff:192.168.1.7
用戶端連接埠:	52314
其他資訊:	
票證選項:	0x40810000
票證加密類型:	0xffffffff
錯誤碼:	0x1f
轉送的服務:	-

The hacker used IP 192.168.1.7 to perform attack again

0x1f means the authentication failed, the attack was stopped

- Cyber Attack Trends in Taiwan
- Cyber Attack Cases Studies
  - Attack via Network Equipment
  - Attack via AD Golden Ticket
  - Attack via Third Party Software
- Conclusions



- Third-Party Applications using in websites
  - Many organizations use third-party applications or modules when building up the websites
  - Third-party applications are great because they are often very easy to learn, to use, and FREE
    - Apache · PHP · OpenSSL · JBOSS · JAVA Struct2 · PhpMyAdmin · CKEditor.....
  - But the down side is, they are not easy to update
    - Most of them do not update automatically, and the new versions are usually not completely compatible with the old versions



CKEditor™

NEWS

## Hackers exploit JBoss

iThome 新聞 產品評測 CIO DevOps 技術 專題 專欄 主題頻道 · 研討會 社群 ·

新聞

### OpenSSL重大漏洞Heartbleed 全球網路加密傳輸安全拉警報

iThome 新聞 產品評測 CIO DevOps 技術 專題 專欄 主題頻道 · 研討會 社群 ·

搜尋

OpenSSL  
使用  
OpenSSL  
1.0.1

新聞

### Struts 2漏洞沒補好，Apache軟體基金會緊急重新釋出更新

ASF發現，今年3月2日釋出的Struts 2.3.16.1未能正確修補零時差攻擊漏洞，並於週日緊急釋出Struts 2.3.16.2。ASF強烈建議所有的開發人員進行版本更新。

文/ 陳曉莉 | 2014-04-29 發表

讚 1.9萬 按讚加入iThome粉絲團 讚 分享 12 G+ 6



圖片來源: 維基共享資源; 作者: U.S. Air Force photo/Capt. Carrie Kessler

iThome 電腦報  
按讚追蹤 iThome 最新報導

讚 1.9萬

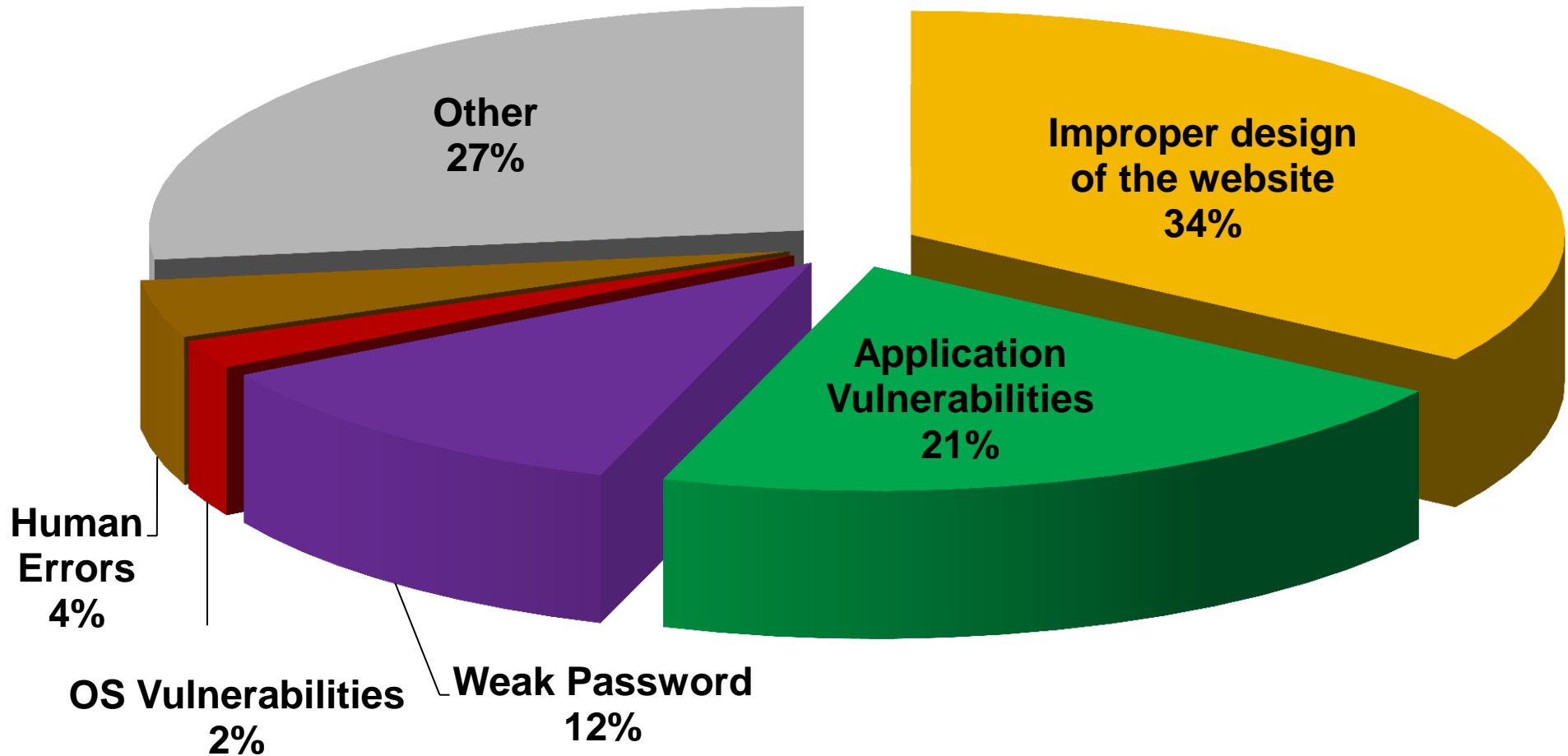
### 熱門新聞

最強大勒索軟體CryptoWall  
進化到4.0版，更難偵測，連  
權名都加密！  
2015-11-10

網管注意！勒索軟體已盯上  
Linux網站！  
2015-11-10

防事軟體主管竟上社群網站大  
爆顧客個資，日本E-Secure

- Incident Reports from Taiwan government agencies :



- Incident Reported

- We received the incident report from one agency, its website was hacked, and needed us to help investigate this incident

- We analyzed the logs and found out that this website had been hacked twice already

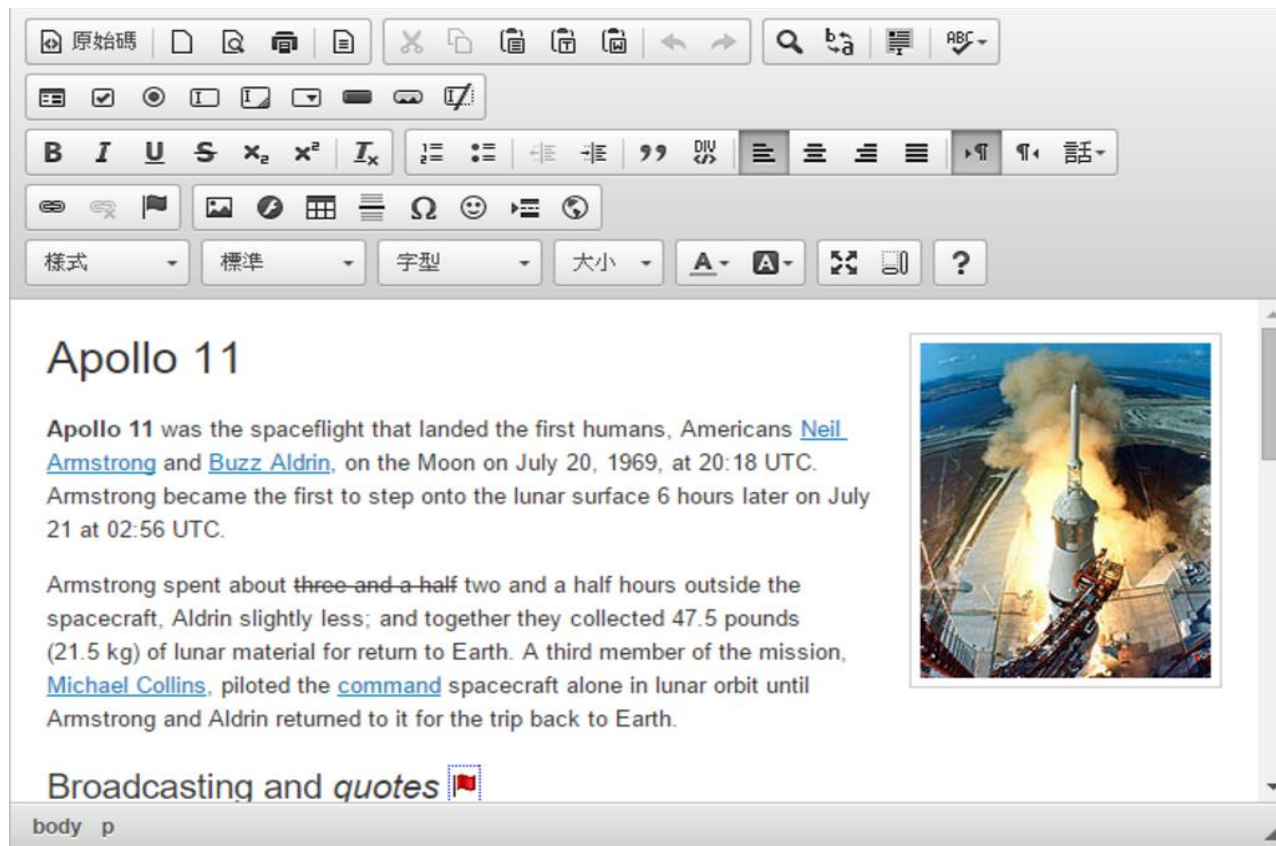
- Although the agency told us that its website backstage management page uses a strong password, but we found out that the Chinese and the English version of backstage management pages were separate, and the English version page used a very simple password

- English version backstage management page was CKEditor, the hacker was able to use it to upload malware

- Moreover, the website has FCKEditor testing page, the hacker could use it to upload malware also

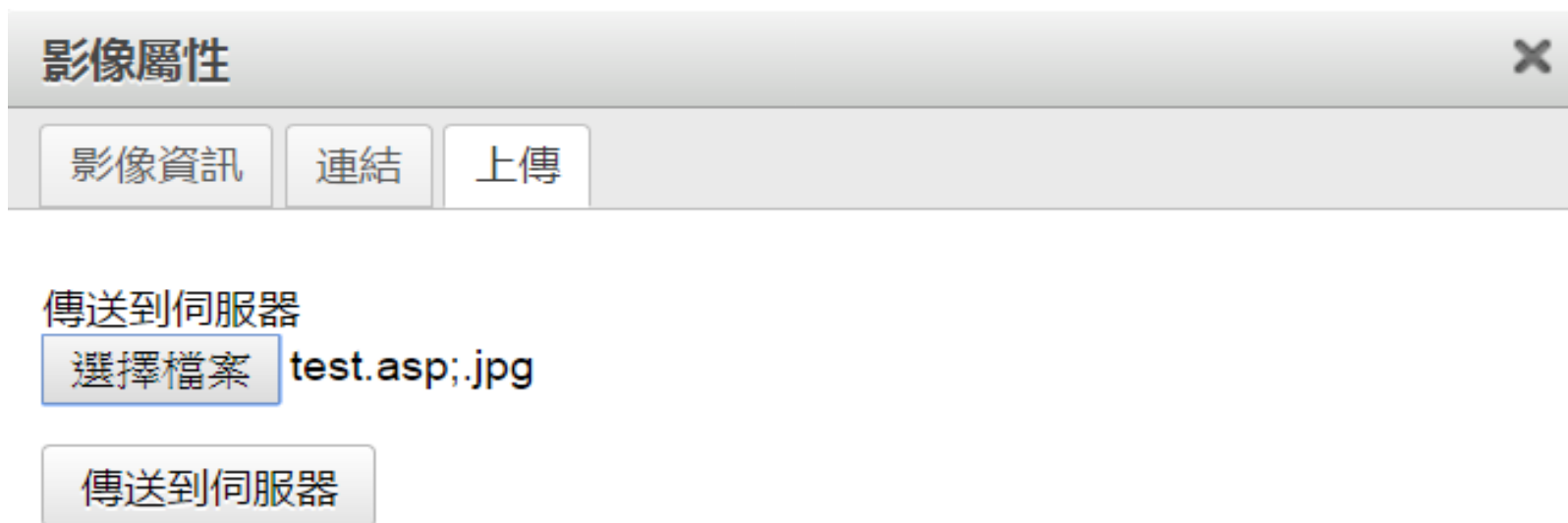
- CKEditor

- Common HTML Editor, What You See Is What You Get (WYSIWYG), users can easily update and maintain the website



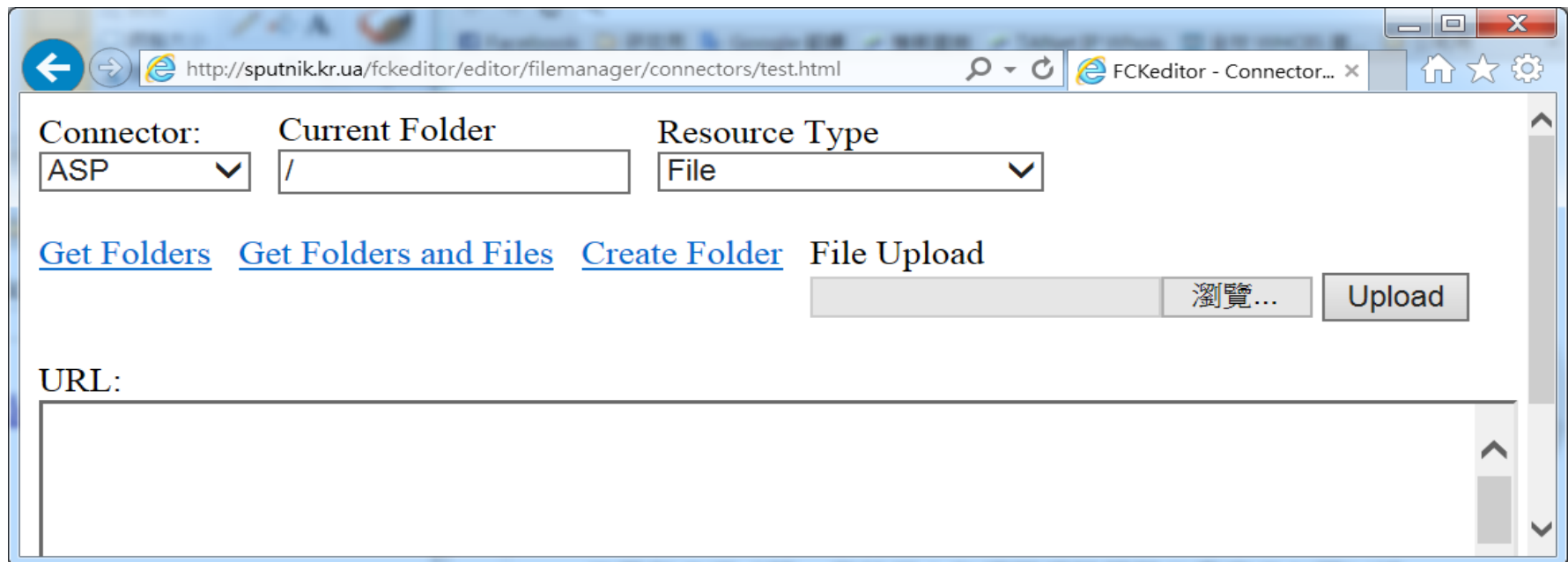
- CKEditor

- The page is in the backstage, after login with the account and password, the user can then upload pictures
- Although it can only upload pictures, but the hacker renamed the malware to **test.asp;.jpg**, and uploaded it successfully (a CKEditor vulnerability), and even executed it (an IIS6 Vulnerability)



- FCKEditor

- FCKEditor is the previous version of CKEditor, the subcontractor used it to test the web pages, but did not delete it after testing
- Only the subcontractor knew about this page, so the agency did not know the existence of this test page



- How did the hacker know about the existence of this test page?
  - Because FCKeditor is a well known third-party application, the hacker used Google Search to search backstage management pages and found its link
  - The subcontractor did not even set an account and password authentication, the hacker found the link and uploaded malware right away



The screenshot shows a Google search interface. The search bar contains the query `inurl:/fckeditor/editor/filemanager/connectors/test.html`. Below the search bar, there are navigation links for "網頁", "影片", "圖片", "新聞", "更多", and "搜尋工具". The search results section shows approximately 5,030 results in 0.34 seconds. The top result is titled "FCKeditor - Connectors Tests" and includes a snippet: "sputnik.kr.ua/fckeditor/editor/filemanager/connectors/test... 翻譯這個網頁 Connector: ASP, ASP.Net, ColdFusion, Lasso, Perl, PHP, Python. Current Folder, Resource Type. File, Image, Flash, Media, Invalid Type (for testing) ...".



- Better Website Management
  - All passwords need to be strong
  - When using the backstage management page such as CKEditor, be sure to turn on account/password authentication mechanism
  - When outsourcing the website development, make sure all testing pages are deleted before go online
  - Ask your website developers provide a list of third-party applications used, and check for updates regularly

- Taiwan Government has developed National Software Asset Management System (NSA) to better manage systems and software for government agencies
  - The agencies login to the NSA and register versions of their systems' OS, application software, and program libraries used
  - NSA compares the registered info with National Vulnerability Database (NVD) daily, if critical vulnerabilities were found, NSA will send the alerts to the agencies, remind them to update
  - After the updates, government agencies will update the register info
- By using the NSA, Taiwan Government is able to grasp not only third-party applications, but all software used in agencies, mitigating threats early and effectively

- Cyber Attack Trends in Taiwan
- Cyber Attack Cases Studies
  - Attack via Network Equipment
  - Attack via AD Golden Ticket
  - Attack via Third Party Software
- Conclusions

# Conclusions

---

- The security standard of network equipments should be treated as same as servers and PCs, do not let them to become the weakest link of your network
- Avoid using remote login to manage servers, especially domain controllers, to mitigate the possibilities of password leaks, and be sure to change administrator password periodically
- Be sure to know all third-party applications used in your websites, and perform security updates and weakness scans regularly to reduce threats

Thank You