"Reading" Ransomware and its Defence on Cloud

從雲端計算看勒索軟件及其解決方案

Mike Lo, Vice Chairman, CSA HKM Chapter

CISSP, CISM, CISA, PMP , CCSK Certified Trainer, CCNA, MCSE, MCNE, SAP Certified Consultant

Jul 12, 2016

Copyright © 2016 Cloud Security Alliance

Mike Lo (Vice Chairperson of CSA HKM)

Working Experience in IT Industry

Mike has been working in IS/IT sectors for over 15 years. He actively involves in Cyber Security and Risk Management projects and researches, which include SAP Security Practice implementation, Security Assessment on Web and Mobile Applications, Mobile Source Code Secure Review, Enterprise Information Security Maturity Gap Analysis, Global Systems Security Role Review, Data Encryption on Cloud Storage and Ransomware Incident Handling for Global and Asia Pacific clients in 11 countries.

Mike holds profession qualifications of CCSK, IPv6 Sage, CISSP, CISA, CISM, PMP, SAP Certified Consultant, MCSE, MCNE, and CCNA

Deloitte

- Cyber Security Manager
- Pent. Test / Secure Source Code Review / Cyber Security & Privacy Training / Security Maturity Gap Analysis / SAP Security Assessment
- IAM / DLP / SIEM / SOC / Security Assessment on Smart Device including Smart Car

NGO Security Association (PISA / CSA HKMC / ISC2 HKC) Executive Committee members

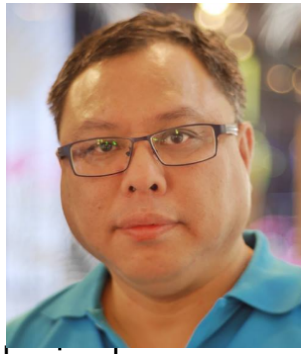
http://www.csahkm.org/

http://www.pisa.org.hk

http://www.isc2chapter.hk/

Copyright © 2016 Cloud Security Alliance

Co-Author
Frankie Leung
Vice President of ISC2 HK Chapter



Working Experience in IT Industry

Mr. Leung has over 29 years well-rounded IT management experience in Technical Product Marketing, Business Information Management, Software Development as well as Information Security Consulting in Greater China region and many Asian countries. As an independent Security Consultant, he has provided different security solutions, technical write up, defining Security policies, IT audit , Computer Forensic and Security Awareness Training to major government departments, High Education Collage and some large finance institutes in Asia, particularly for USB Device Controls, Encryption Technology, Network Security, PKI infra-structure, Multi-factor Authentication, Digital Rights Management, Data Leakage Prevention, IT Audit and Computer Forensic.

Frankie holds profession qualifications of CISSP, CISA, CISM, CRISC, ISO 27001 ISMS Implementation Specialist

1.勒索軟件的歷史
2.勒索軟件主要的感染途徑
3.勒索軟件相關是一盤生意？
4.常見勒索軟件種類及個案分享
5.勒索軟年的解決方案
6.如何從雲端計算減低勒索軟件入侵風險

勒索軟件 Ransomware (勒索病毒/綁架病毒)散播超過十年, 第一個版本早在2005年在俄羅斯現身, 有些冒充警察的勒索軟體會宣稱受害人違反法律, 進而鎖住系統,顯示繳交罰款的勒索頁面, 甚至播放聲音檔,催促繳款。

RANSOM_Cerbera加密勒索軟體則用電腦語音播放：

「注意！注意！注意！」「你的文件、照片、資料庫和其他重要檔案都已經被加密！」

http://blog.trendmicro.com.tw/?p=16660

2013年出現一個特別麻煩的勒索軟件當時被稱為**史上最狠毒的勒索軟件**「**Cryptolocker**」。它會加密重要的檔案，只有當你支付贖金後才提供解密方法。至此,加密勒索軟件開始大行其道，相關攻擊一直在持續升溫。

從 2013 年起，被偵測到的傳統勒索軟體件與加密勒索軟件的比例，已從過去的80/20 演變至今日的20/80,甚至還從一般電腦發展到Android系統上。起初加密勒索軟件主要鎖定歐美，到了2015年，勒索軟件開始出現簡/繁體中文介面，大中華爆發災情,受害者包含企業和個人。

http://blog.trendmicro.com.tw/?p=16660

第一隻針對Synology NAS 操作系統的勒索軟件

Aug 2014

http://sensorstechforum.com/synology-nas-devices-attacked-by-synolocker-ransomware/

Copyright © 2016 Cloud Security Alliance

2016-04-03 21:56

近月出現一種名為「Locky」的加密勒索電腦程式肆虐，多會透過垃圾電郵，入侵受害者的電腦，然後把電腦中的檔案加密，讓受害人不能開啟，並會在受害人電腦桌面登出勒索告示，索取l幾塊比特幣，即約數千至逾萬港元。

Locky雖並非電腦病毒，但亦為一種經加密的勒索程式，傳播途徑有兩種，一種是廣發垃圾郵件，若受害人開啟電郵，電腦便很可能被Locky軟件入侵；另一種途徑則是黑客先入侵部分網站，當受害人登入有關網站時，便會被引導至已植入Locky的網站，再入侵受害人電腦。

當Locky入侵受害人電腦後，便會迅速把電腦內的數據及檔案加密，受害人會因不能解密，而未能開啟檔案。若電腦連接至其他伺服器，Locky更會入內，把其他檔案加密

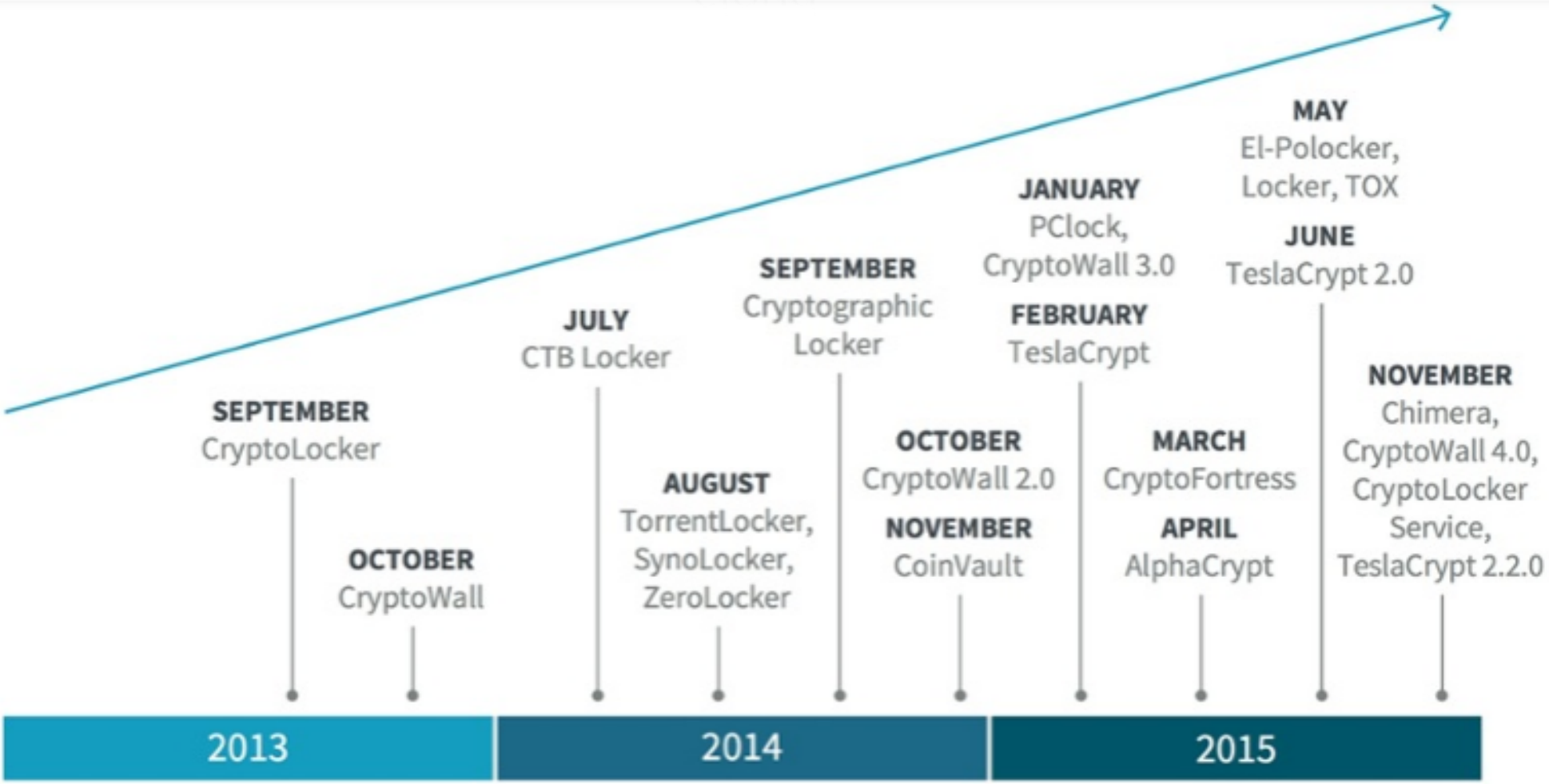
Copyright © 2016 Cloud Security Alliance

Locky

Mar 2016

Copyright © 2016 Cloud Security Alliance

勒索軟件發展史



https://blog.knowbe4.com/its-here.-new-ransomware-hidden-in-infected-word-files

Copyright © 2016 Cloud Security Alliance

勒索軟件Ransomwares有幾多種 ？

This service currently detects **133** different ransomwares as of Jul 11, 2016. Here is a complete, dynamic list of what is currently detected:

777, 7ev3n, 7h9r, 8lock8, **Alfa**, Alpha, AMBA, Apocalypse, ApocalypseVM, AutoLocky, AxCrypter, BadBlock, BankAccountSummary, Bart, BitCryptor, BitMessage, **BitStak**, Black Shades, Blocatto, Booyah, Brazilian Ransomware, **Bucbi**, BuyUnlockCode, Cerber, Chimera, **Coin Locker**, CoinVault, Coverton, CryFile, Crypren, Crypt0L0cker, Crypt38, CryptoDefense, **CryptoFinancial**, CryptoFortress, CryptoHasYou, CryptoHitman, CryptoJoker, CryptoMix, CryptoRoger, CryptoShocker, CryptoTorLocker, CryptoWall 2.0, CryptoWall 3.0, CryptoWall 4.0, **CryptXXX**, **CryptXXX 2.0, CryptXXX 3.0**, CrySiS, CTB-Locker, DEDCryptor, DMA Locker, DMA Locker 3.0, DMA Locker 4.0, ECLR Ransomware, EduCrypt,**El Polocker**, Encryptor RaaS, Enigma, GhostCrypt, Gomasom, Herbst, **Hi Buddy!**, HydraCrypt, Jigsaw, JobCrypter, JuicyLemon, KeRanger, KEYHolder, KimcilWare, Kozy.Jozy, KratosCrypt, Kriptovor, KryptoLocker, LeChiffre, **Locky**, Lortok, Magic, Maktub Locker, MirCop, MireWare, Mischa, Mobef, NanoLocker, NegoziI, Nemucod, Nemucod-7z, **ODCODC**, OMG! Ransomcrypt, PadCrypt, PClock, **PizzaCrypts**, PowerWare, Protected Ransomware, RAA-SEP, Radamant, Radamant v2.1, RemindMe, Rokku, Russian EDA2, SamSam, Sanction, Satana, SecureCryptor, Shade, Shujin, SNSLocker, Sport, SuperCrypt, Surprise, SZFLocker, TeslaCrypt 0.x, TeslaCrypt 2.x, TeslaCrypt 3.0, TeslaCrypt 4.0, TowerWeb, ToxCrypt, Troldesh, TrueCrypter, UCCU, UmbreCrypt, Unlock92, **Unlock92 2.0**, VaultCrypt, Vipasana, WildFire Locker, WonderCrypter, Xorist, Xort, XRTN, zCrypt, ZimbraCryptor, Zyklon

https://id-ransomware.malwarehunterteam.com/

Copyright © 2016 Cloud Security Alliance

誘騙使用者連到看似真正銀行或政府機構網站的假網頁

輸入驗證碼（**CAPTCHA**，一種防止機器人的程序）

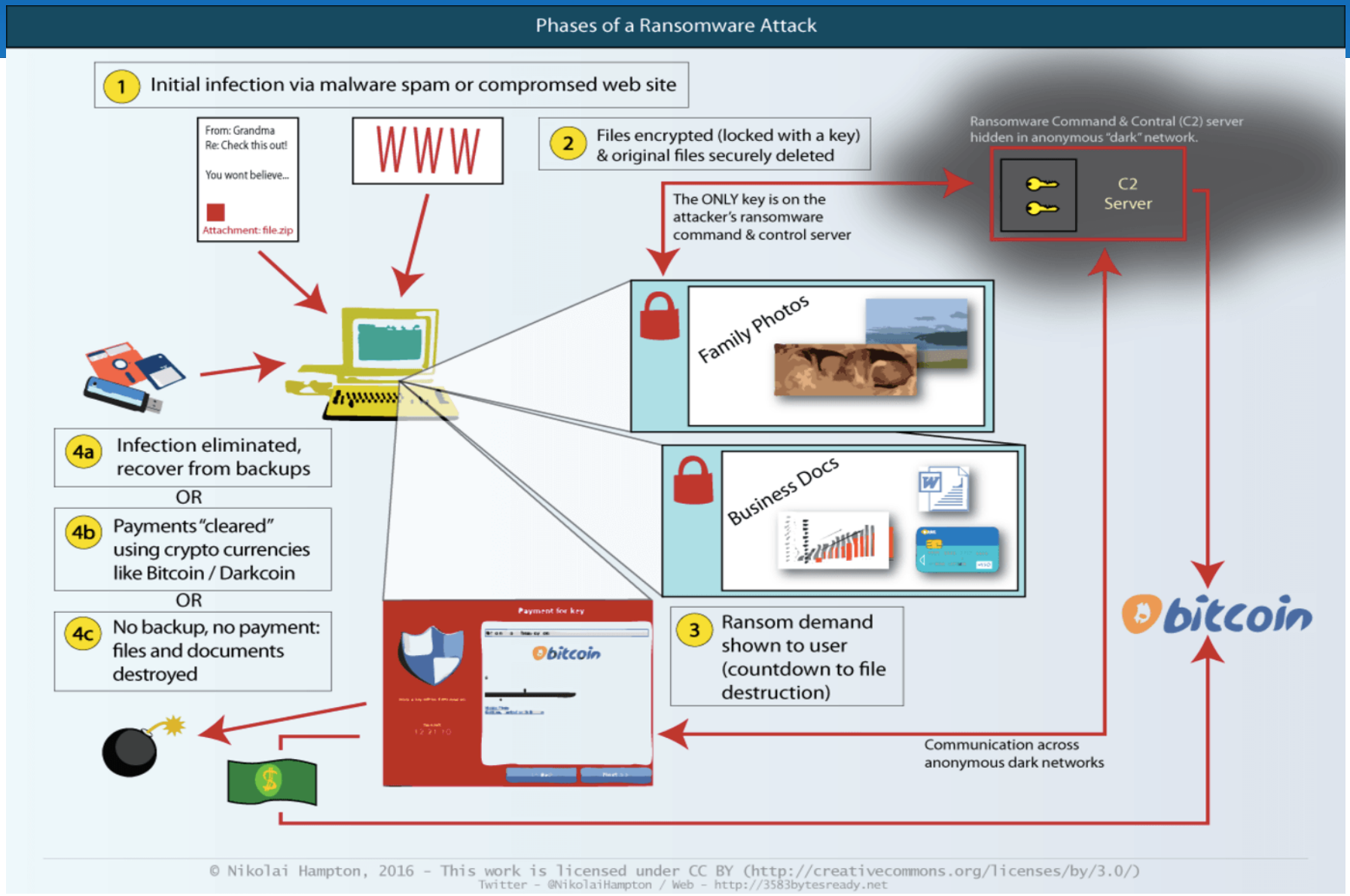
網路釣魚信件 針對瀏覽器、Windows作業系統、Adobe Flash Player等軟件的漏洞 內含惡意程式的網路廣告或是論壇文章

http://blog.trendmicro.com.tw/?p=17208

1.勒索軟件的歷史
2.勒索軟件主要的感染途徑及運作
3.勒索軟件相關是一盤生意？
4.常見勒索軟件種類及個案分享
5.勒索軟年的解決方案
6.如何從雲端計算減低勒索軟件入侵風險

http://blog.trendmicro.com.tw/?p=16660

勒索軟件的運作



http://cdn.phys.org/newman/gfx/news/hires/2016/whatisransom.png

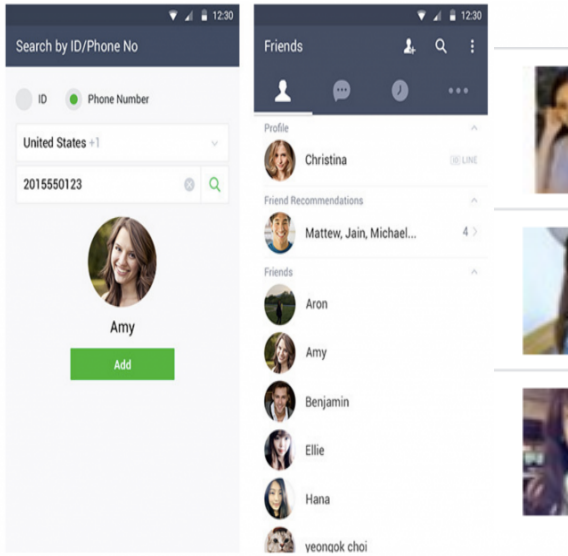
Copyright © 2016 Cloud Security Alliance

勒索軟件主要的感染途徑

A) 惡意郵件

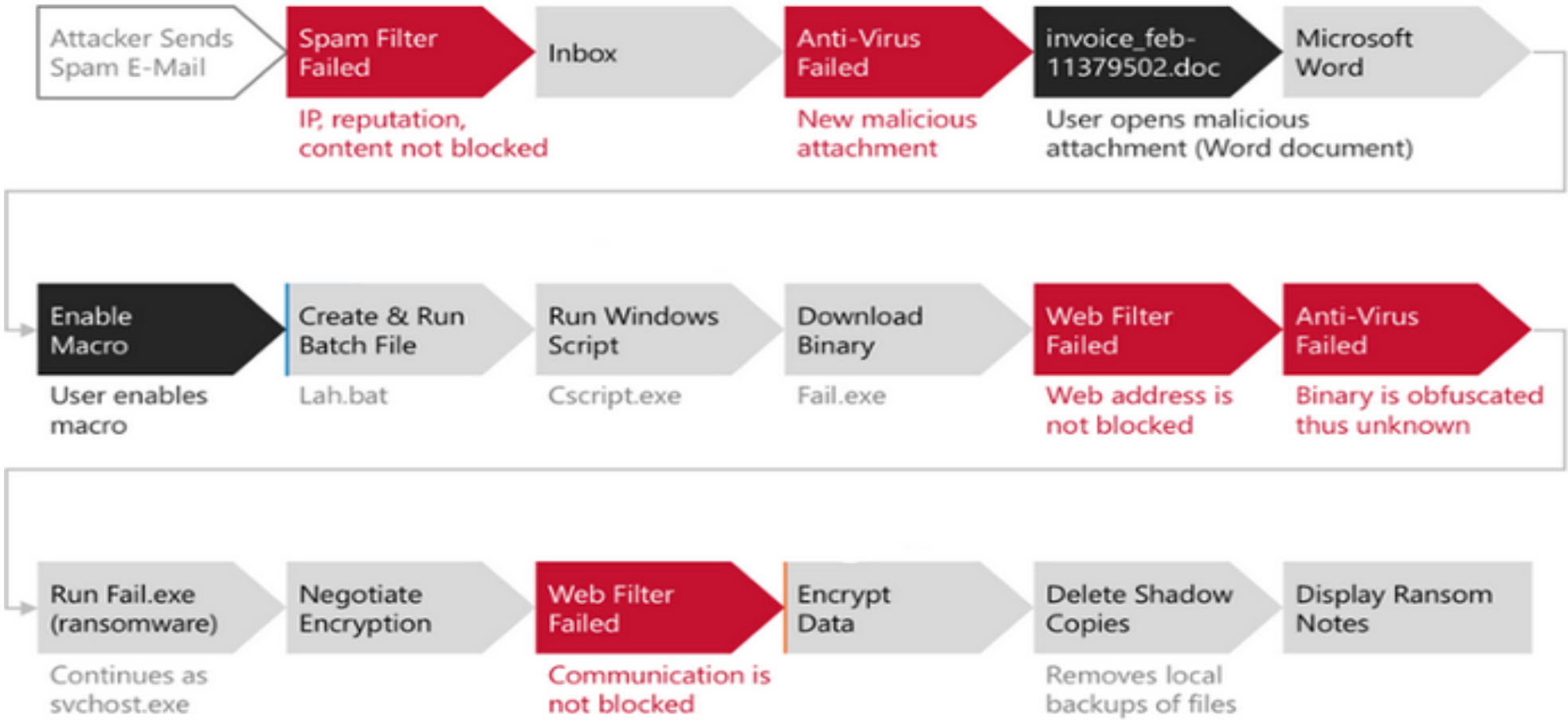
B) 社交網路廣告或連結

C) 入侵的網，針對使用過時或未修補的瀏覽器（如 IE）或插件（如 Flash Player）；



Copyright © 2016 Cloud Security Alliance

The Attack Flow



https://blog.knowbe4.com/its-here.-new-ransomware-hidden-in-infected-word-files

Copyright © 2016 Cloud Security Alliance

1.勒索軟件的歷史
2.勒索軟件主要的感染途徑
3.勒索軟件相關是一盤生意？
4.常見勒索軟件種類及個案分享
5.勒索軟年的解決方案
6.如何從雲端計算減低勒索軟件入侵風險

http://blog.trendmicro.com.tw/?p=16660

[勒索軟件]事業愈做愈大了:

1.成立技術支援團隊, 全天候 7 天 24 小時提供付款電話支援服務, 甚至對勒索本文提供翻譯

2.提供網路聊天的方式即時協助受害者進行付款流程

3.加密勒索軟件的成長,架設網站, 提供免費試用解密工具,甚至成立了技術支援團隊, 協助受害者進行付款流程

http://blog.trendmicro.com.tw/?p=16660

Copyright © 2016 Cloud Security Alliance

Ransomware as a Service (RaaS)

1) Ransomware authors are marketing on-demand versions of code, using traditional malware distributors in a classic affiliate model.

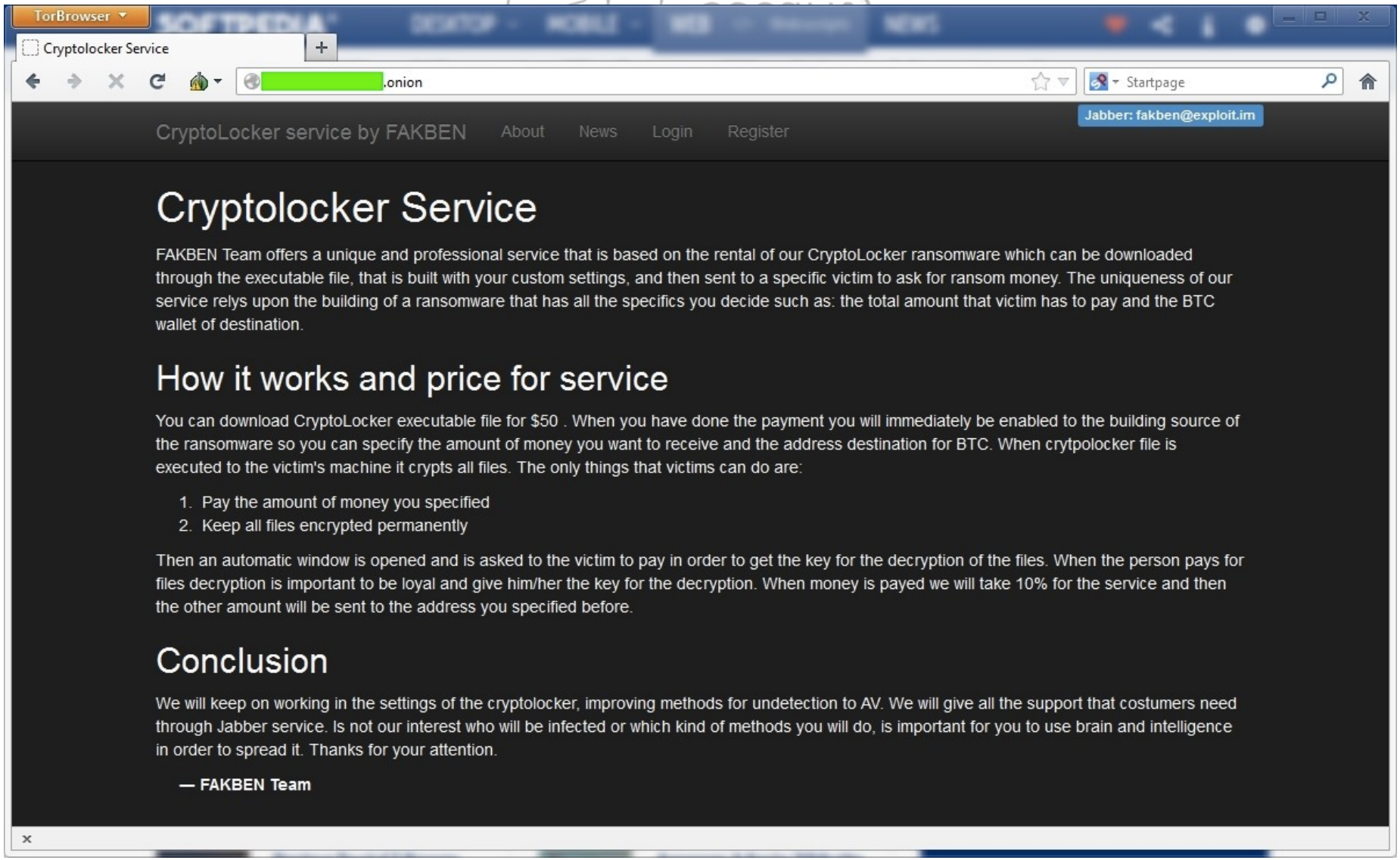
2) The ransomware author collects the ransom and shares it with the distributor.
Malware is distributed through spam email messages, malicious advertisements。

3) The ransomware author gets a small cut of the funds (5%-25%) while the rest goes to the distributor (affiliate)."

4) This model, based on TOR and Bitcoins, is designed to keep the identity of the author and the distributor hidden from law enforcement agencies."

http://www.techrepublic.com/article/ransomware-as-a-service-is-exploding-be-ready-to-pay/

Copyright © 2016 Cloud Security Alliance



Copyright © 2016 Cloud Security Alliance

Price List for Hacker Goods and Services

Credit Cards

	Price in 2013	Price in 2014	Recent Prices
Visa and MasterCard (U.S.)	$4	$4	$7
Visa Classic and MasterCard (U.S.) with Track 1 and Track 2 Data	$12	$12	$15
Visa Classic and MasterCard (Canada, Australia, and New Zealand) with Track 1 and Track 2 Data	$19 – $20	$19 – $20	$25
Visa Classic and MasterCard Standard (EU) with Track 1 and 2 Data	$28	$28	$40
Visa Classic and MasterCard Standard (U.K) with Track 1 and Track 2 Data	$19 – $20	$19 – $20	$40
Visa Classic and MasterCard Standard (Japan and Asia) with Track 1 and Track 2 Data	$28	$28	$50
Premium Visa and MasterCard (U.S.) with Track 1 and Track 2 Data		$23 (V); $35 (MC)	$30
Premium Visa and MasterCard (EU and U.K.) with Track 1 and 2 Data		$23 (V); $35 (MC)	$50 – $60
Premium Visa and MasterCard (Canada, Australia and New Zealand) with Track 1 and Track 2 Data		$23 (V); $35 (MC)	$35 for V and MC
Premium Visa and MasterCard (Japan and Asia) with Track 1 and Track 2 Data		$23 (V); $35 (MC)	$80 for V and MC
Premium American Express Card (U.S.) with Track 1 and Track 2 Data		$23 (V); $35 (MC)	$30
Premium Discover Card (U.S.) with Track 1 and Track 2 Data		$23 (V); $35 (MC)	$30
VBV (U.K., Australia, Canada, EU and Asia)	$17 – $25	$28	$25

Underground Hacker Markets ANNUAL REPORT—APRIL 2016
http://online.wsj.com/public/resources/documents/secureworks_hacker_annualreport.pdf

Copyright © 2016 Cloud Security Alliance

Price List for Hacker Goods and Services

Tools

	Price in 2013	Price in 2014	Recent Prices
Remote Access Trojans (RATs)	$50 – $250	$20 – $50	$5 – $10
Crypters		L50	$80 – $440
Angler Exploit Kit			$100 – $135

WHAT IS A CRYPTER?

Crypters are software tools that use a combination of encryption, obfuscation, and code manipulation of malware to make them FUD (Fully Undetectable) by legacy security products.

Hacking Services

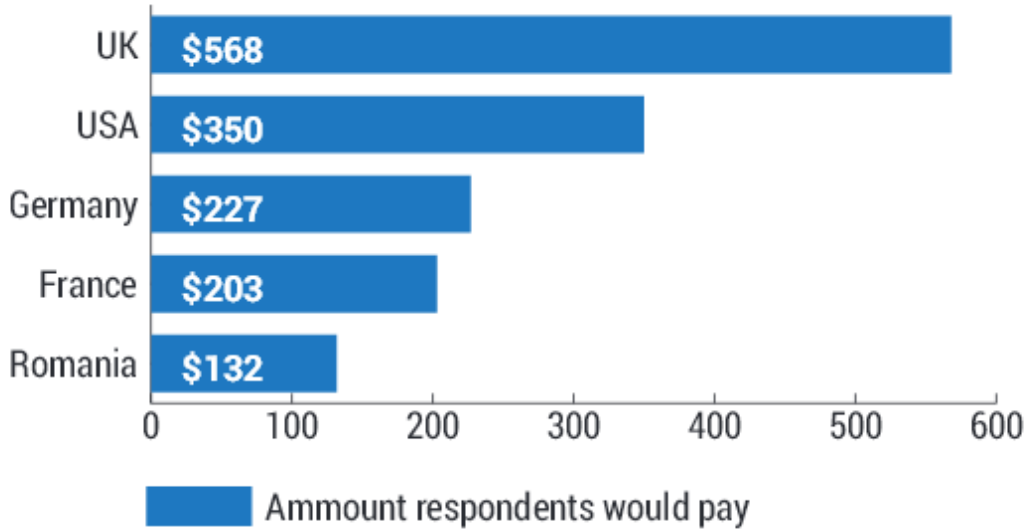
	Price in 2013	Price in 2014	Recent Prices
Hacking Tutorials	N/A	$1 each to $30 for 10 (depending on the tutorial)	$20 to $40 for multiple tutorials
Hacking Website (stealing data)	$100 – $300	$100 – $200	$350
DDoS Attacks	Per Hour: $3 – $5 Per Day: $90 – $100 Per Week: $400 – $600	Per Hour: $3 – $5 Per Day: $60 – $90 Per Week: $350 – $600	Per hour: $5 – $10 Per Day: $30-$55 Per Week: $200 – $555
Doxing	$25-$100	$25-$100	$19.99

Underground Hacker Markets ANNUAL REPORT—APRIL 2016

Copyright © 2016 Cloud Security Alliance

Ransomware is Good Business

A Bitdefender study conducted in November 2015 revealed that ransomware victims would be willing to pay up to **$500 to recover their data**.



Regardless of whether it is Android / PC ransomware, or even Linux ransomware, **malware-as-a-service** has become a financially driven industry that's willing and able to supply malware to anyone who will pay for it.

For instance, the **Cryptolocker/Cryptowall ransomware** kit for PCs is being Reportedly sold for as little as **$3,000**, and with various business models that favor both the customer and the malware developers. The return on investment could be stellar if an effective distribution method is found and many victims are infected

http://download.bitdefender.com/resources/files/News/CaseStudies/study/85/Android-Malware-Threat-Report-H2-2015.pdf

Copyright © 2016 Cloud Security Alliance

How Victims React to Ransomware

A study conducted by Bitdefender revealed that 50 percent of US ransomware victims have actually paid the extortionists. While Americans are the ones most willing to pay, French and Romanian are close behind, with 44 percent and 48 percent, respectively, showing the same behavior.

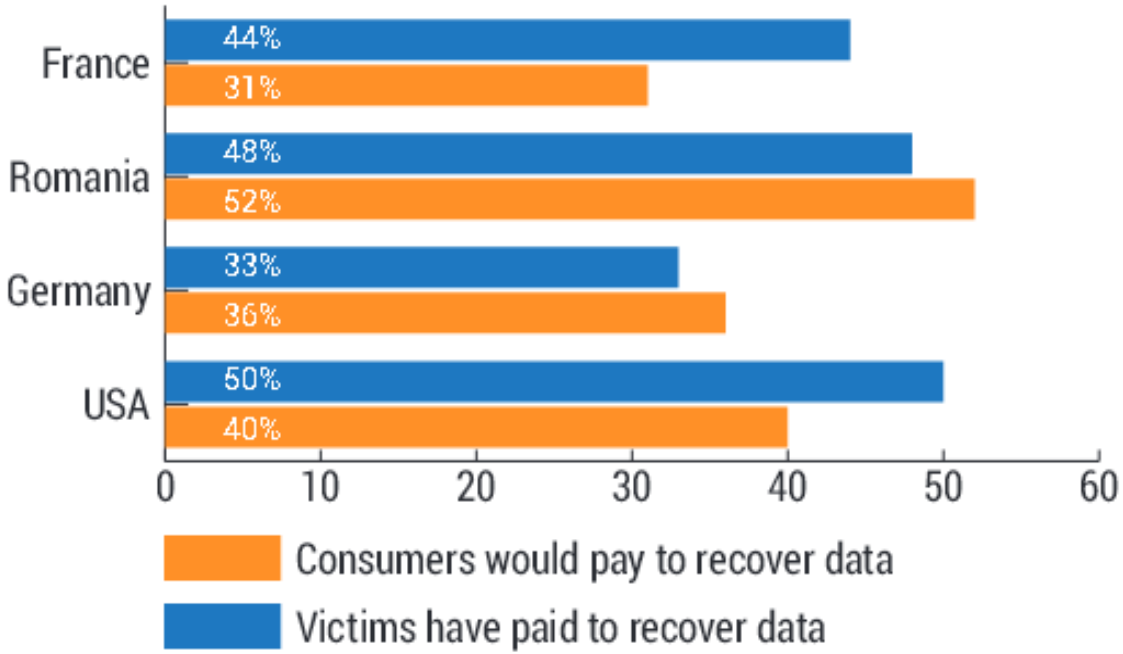


Fig. 10 – How victims react to ransomware

http://download.bitdefender.com/resources/files/News/CaseStudies/study/85/Android-Malware-Threat-Report-H2-2015.pdf

Copyright © 2016 Cloud Security Alliance

1.勒索軟件的歷史
2.勒索軟件主要的感染途徑
3.勒索軟件相關是一盤生意？
4.常見勒索軟件種類及個案分享
5.勒索軟年的解決方案
6.如何從雲端計算減低勒索軟件入侵風險

http://blog.trendmicro.com.tw/?p=16660

Widespread Attack on Office 365 Corporate Users with Zero-day Ransomware Virus (Jul 1st, 2016)

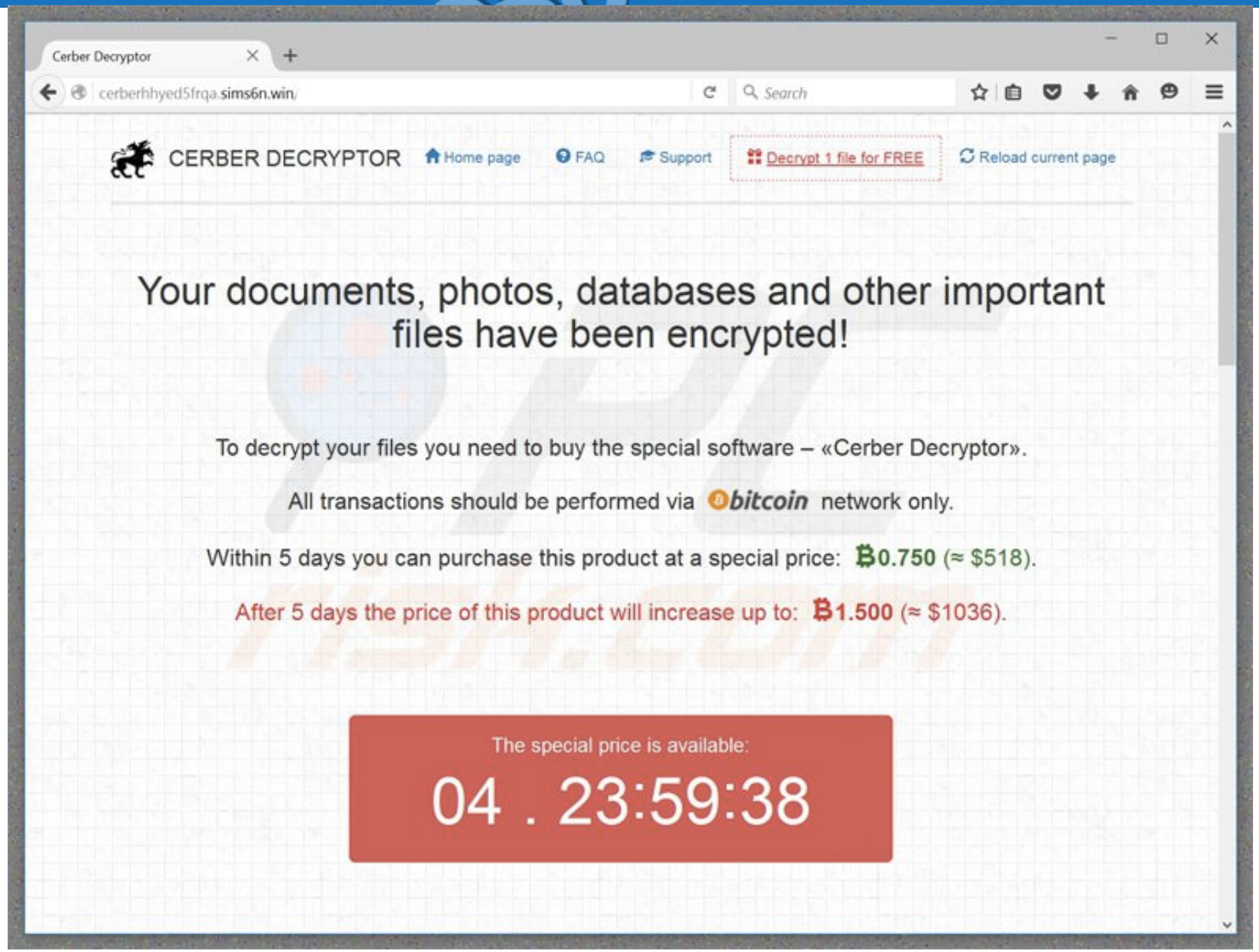
Millions of Microsoft Office 365 users were potentially exposed to a massive zero-day Cerber ransomware attack last week that **not only included a ransom note, but an audio warning informing victims that their files were encrypted.**

The attacker asked for a ransom totaling 1.4 bitcoin, or about $500 (£375), for the decryption key.

"This attack seems to be a variation of a virus originally detected on network mail servers back in early March of this year," and is confirm that the virus was able to bypass the Office 365 built-in security tools through a private Office 365 mail account."

http://www.scmagazineuk.com/microsoft-office-365-hit-with-massive-cerber-ransomware-attack-report/article/505928/

Copyright © 2016 Cloud Security Alliance



https://www.pcrisk.com/images/stories/screenshots201603/cerber-ransomware-wallpaper.jpg

Copyright © 2016 Cloud Security Alliance

Chinese-language Ransomware 'SHUJIN' Makes An Appearance

Posted on: May 12, 2016 at 8:03 am **Posted in:** Deep Web, Malware, Ransomware
Author: Jasen Sumalapao (Threat Response Engineer)

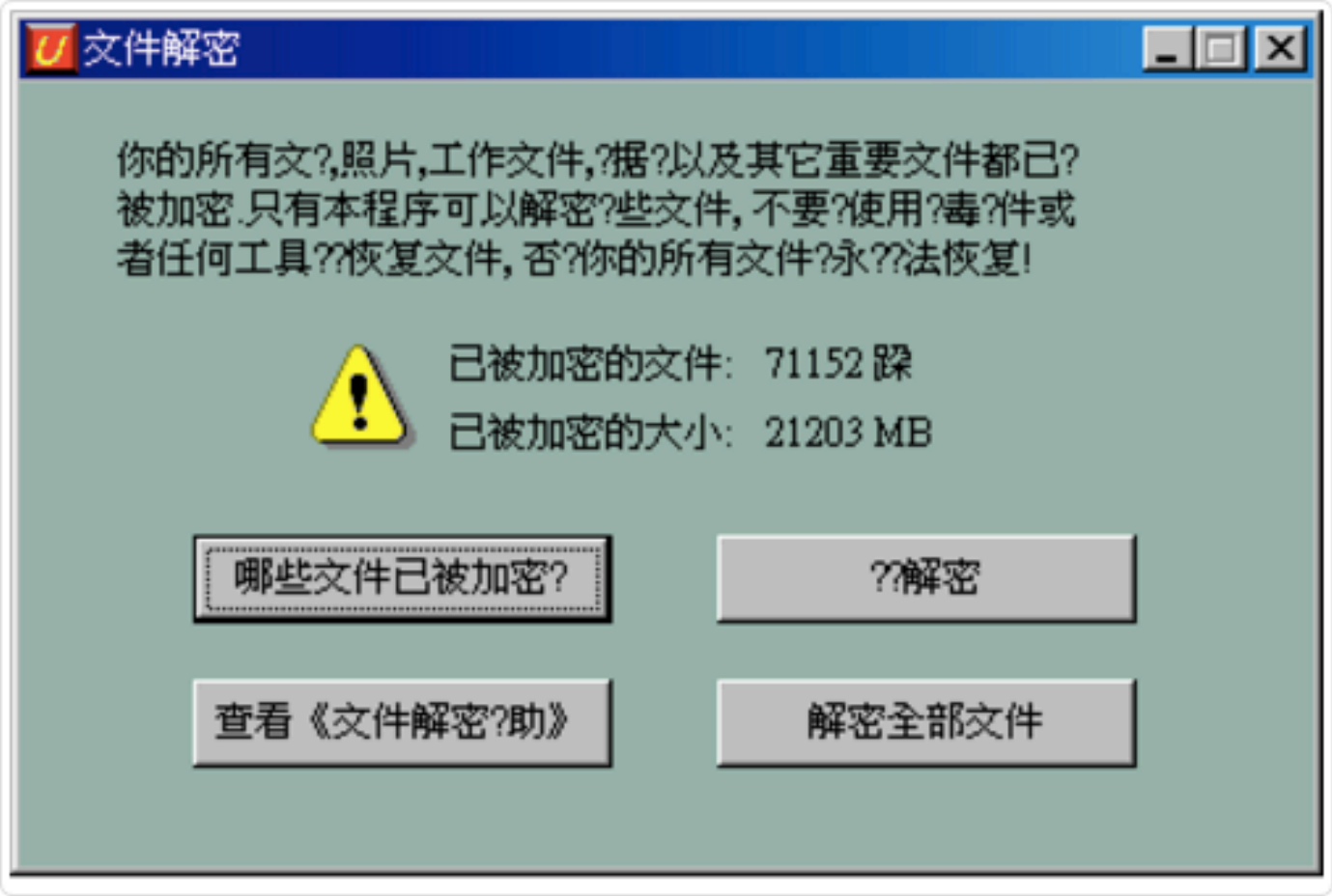
Additional analysis by Lion Gu

Whenever a threat is "localized" to a specific region, it's a sign that attackers believe there is money to be made. Ransomware has made millions of dollars around the world, and it looks like it's poking its nose into a new part of the world: China. However, the initial foray into this market made several mistakes.

We recently came across multiple samples of what appeared to be Chinese-language ransomware. We detect this as Ransom_SHUJIN.A. All of these samples could be decompressed into the same executable file. While this is not the first time that Chinese-language ransomware has been found, this may be the first time that one used simplified Chinese characters. This character set is favored for use in mainland China. As of this writing, the infection vector of this attack is not yet known.

Copyright © 2016 Cloud Security Alliance

Once this ransomware is run, it displays the following message:



Copyright © 2016 Cloud Security Alliance

Ransomware Recap: New Families and Updated Variants in June 2016

CryptXXX

Aside from the usual ransomware routine of locking its victims files with encryption, **CryptXXX has also been discovered to possess Bitcoin-stealing capabilities**.

After the "embarrassment" brought about by the fast release of a "free decryption tool" made available online, CryptXXX was updated with stronger encryption. The development continued into June with an overhaul of its interface, ransom note, and payment site. Labeled as *CryptXXX 3.0*, the updated version also implemented a new encryption algorithm that prevented the use of free decrypter tools widely available online. After infection, the ransomware redresses its desktop wallpaper to an image similar to its revamped Tor payment site. The victim is given a 90-hour deadline to pay the ransom. Failure to do so would then double the ransom to two Bitcoins.

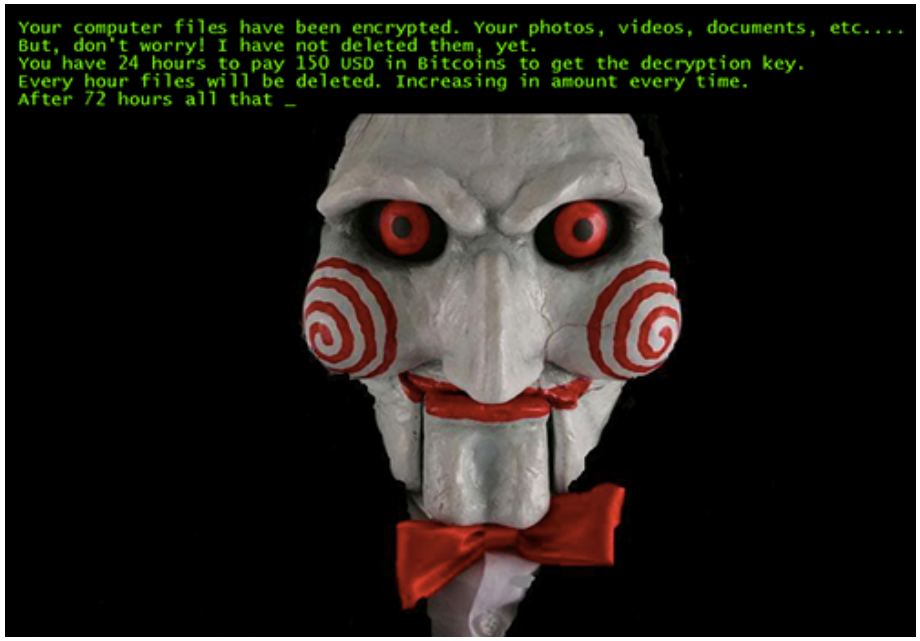
http://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/ransomware-recap-new-families-updated-variants-in-june

Copyright © 2016 Cloud Security Alliance

Ransomware Recap: New Families and Updated Variants in June 2016

Jigsaw

Jigsaw played games with its victims—fitting for extortion malware named after the famous Hollywood slasher flick, *Saw.* Bannering a ransom note in English and Portuguese with the image of the villainous character, Billy, **Jigsaw threatened to delete chunks of the files it encrypted every hour that the ransom (ranging from US$20 – 150) has not been paid.** The mean streak does not end as the ransom actually increases per hour.



Copyright © 2016 Cloud Security Alliance

Ransomware Recap: New Families and Updated Variants in June 2016

MIRCOP

As of June 23rd, the ransomware has been demanding a ransom of 48.48 bitcoins (around $28,730.70) from its users.

Further, at the end of the note, the cybercriminals involved simply included a bitcoin address, unlike other ransomware families that provide step-by-step instructions.

MIRCOP is known to be delivered by spam emails with a poisoned macro-enabled document masquerading as a Thai customs form. Apart from its file-encrypting capabilities, **this ransomware is also capable of mining credentials from several programs like Mozilla Firefox, Google Chrome, Opera, Filezilla, and Skype.**

Copyright © 2016 Cloud Security Alliance

RANSOMWARE PLAGUES KENTUCKY HOSPITAL, FORCES TOTAL SYSTEM SHUTDOWN

By **Gabe Carey** — March 23, 2016

21 Subscribe to this topic

In yet another large-scale ransomware attack, Henderson, Kentucky-based Methodist Hospital has announced an "internal state of emergency," according to Krebs on Security, after numerous files on its computer systems were savaged by encryption. The way ransomware works, all of the documents involved will be held for ransom, awaiting the hospital's payment, hence the name.

DON'T FALL BEHIND

Stay current with a recap of today's **Tech News** from Digital Trends.

Enter your Email

Sign Up

http://www.digitaltrends.com/computing/kentucky-hospital-subjected-to-ransomware/

Copyright © 2016 Cloud Security Alliance

Computer Forensic on “Locky”

Locky encrypts your data and completely changes the filenames

When Locky is started it will create and assign a unique 16 hexadecimal number to the victim and will look like F67091F1D24A922B. Locky will then scan all local drives and **unmapped** network shares for data files to encrypt. When encrypting files it will use the AES encryption algorithm and only encrypt those files that match the following extensions:

```
.mid, .wma, .flv, .mkv, .mov, .avi, .asf, .mpeg, .vob, .mpg, .wmv, .fla, .swf, .wav, .qcow2, .vdi, .vmdk, .vmx, .gpg
, .aes, .ARC, .PAQ, .tar.bz2, .tbk, .bak, .tar, .tgz, .rar, .zip, .djv, .djvu, .svg, .bmp, .png, .gif, .raw, .cgm, .
jpeg, .jpg, .tif, .tiff, .NEF, .psd, .cmd, .bat, .class, .jar, .java, .asp, .brd, .sch, .dch, .dip, .vbs, .asm, .pas
, .cpp, .php, .ldf, .mdf, .ibd, .MYI, .MYD, .frm, .odb, .dbf, .mdb, .sql, .SQLITEDB, .SQLITE3, .asc, .lay6, .lay, .m
s11 (Security copy), .sldm, .sldx, .ppsm, .ppsx, .ppam, .docb, .mml, .sxm, .otg, .odg, .uop, .potx, .potm, .pptx, .p
ptm, .std, .sxd, .pot, .pps, .sti, .sxi, .otp, .odp, .wks, .xltx, .xltm, .xlsx, .xlsm, .xlsb, .slk, .xlw, .xlt, .xlm
, .xlc, .dif, .stc, .sxc, .ots, .ods, .hwp, .dotm, .dotx, .docm, .docx, .DOT, .max, .xml, .txt, .CSV, .uot, .RTF, .p
df, .XLS, .PPT, .stw, .sxw, .ott, .odt, .DOC, .pem, .csr, .crt, .key, wallet.dat
```

Furthermore, Locky will skip any files where the full pathname and filename contain one of the following strings:

```
tmp, winnt, Application Data, AppData, Program Files (x86), Program Files, temp, thumbs.db, $Recycle.Bin, System Vol
ume Information, Boot, Windows
```

http://www.bleepingcomputer.com/news/security/the-locky-ransomware-encrypts-local-files-and-unmapped-network-shares/

Copyright © 2016 Cloud Security Alliance

一個名為「Petya」的惡意程式（RANSOM_PETYA.A）利用加密勒索軟體進行一波新的攻擊，此惡意程式透過發送電郵來散布一封看似要應徵某項 工作的電郵，信件內含一個連向 Dropbox 雲端空間的連結，點選連結後會發現內含兩個檔案：一個是偽裝成履歷表的解除壓縮執行檔，另一個是冒充「求職者」的照片檔可讓收件人用來下載求職者的履歷表。

但用戶一旦下載及開啟連結中的執行檔時，電腦將被植入一個木馬程式，此木馬程式會先讓電腦系統中所安裝的防毒軟件失效，然後再下載並執行 Petya 勒索軟體，進一步修改電腦硬碟的主要開機磁區 （MBR），讓 Windows 當機並出現藍色畫面。接著，當用戶重新開機時，電腦就會載入歹徒寫入的主要開機磁區，此時電腦不會進入 Windows 系統，而是在螢幕上顯示一個骷髏頭畫面以及勒索指示，用戶必須透過比特幣（Bitcoin）支付一定的贖金來救回電腦和檔案。

Copyright © 2016 Cloud Security Alliance

有關 Petya 的消息於兩星期前出現。Petya 藉著假冒履歷表來入侵電腦，然後把所有檔案加密。這款勒索軟件最大的特色是會修改開機磁區，使受害人連 Windows 也無法進入。

不過已有人破解了 Petya 並發布工具幫受害人解密檔案。只要把被加密的硬碟放至另一部完好的電腦，把 sector 55 (0x37h) offset 0(0x0) 的 512 bytes 資料，以及在 sector 54 (0x36) offset: 33 (0x21)的8 bytes nonce 的資料抽出，然後轉至 Base64 編碼，把資料貼到網上，就會產生用作解密的字串。連結如下：

- https://petya-pay-no-ransom.herokuapp.com/ 或
- https://petya-pay-no-ransom-mirror1.herokuapp.com/

不過一般人難以抽取資料，所以又有人制作 Petya Sector Extractor 讓受害人更方便地抽取資料。同樣要把被加密的硬碟放至另一部電腦方可抽取。

http://unwire.pro/2016/04/13/petya-has-been-cracked/news/

Copyright © 2016 Cloud Security Alliance

圖說：加密勒索軟體 PETYA 的解密與付款指示架設在深層網路(Deep Web)上的網站

Copyright © 2016 Cloud Security Alliance

1.勒索軟件的歷史
2.勒索軟件主要的感染途徑
3.勒索軟件相關是一盤生意？
4.常見勒索軟件種類及個案分享
5.勒索軟件的解決方案
6.如何從雲端計算減低勒索軟件入侵風險

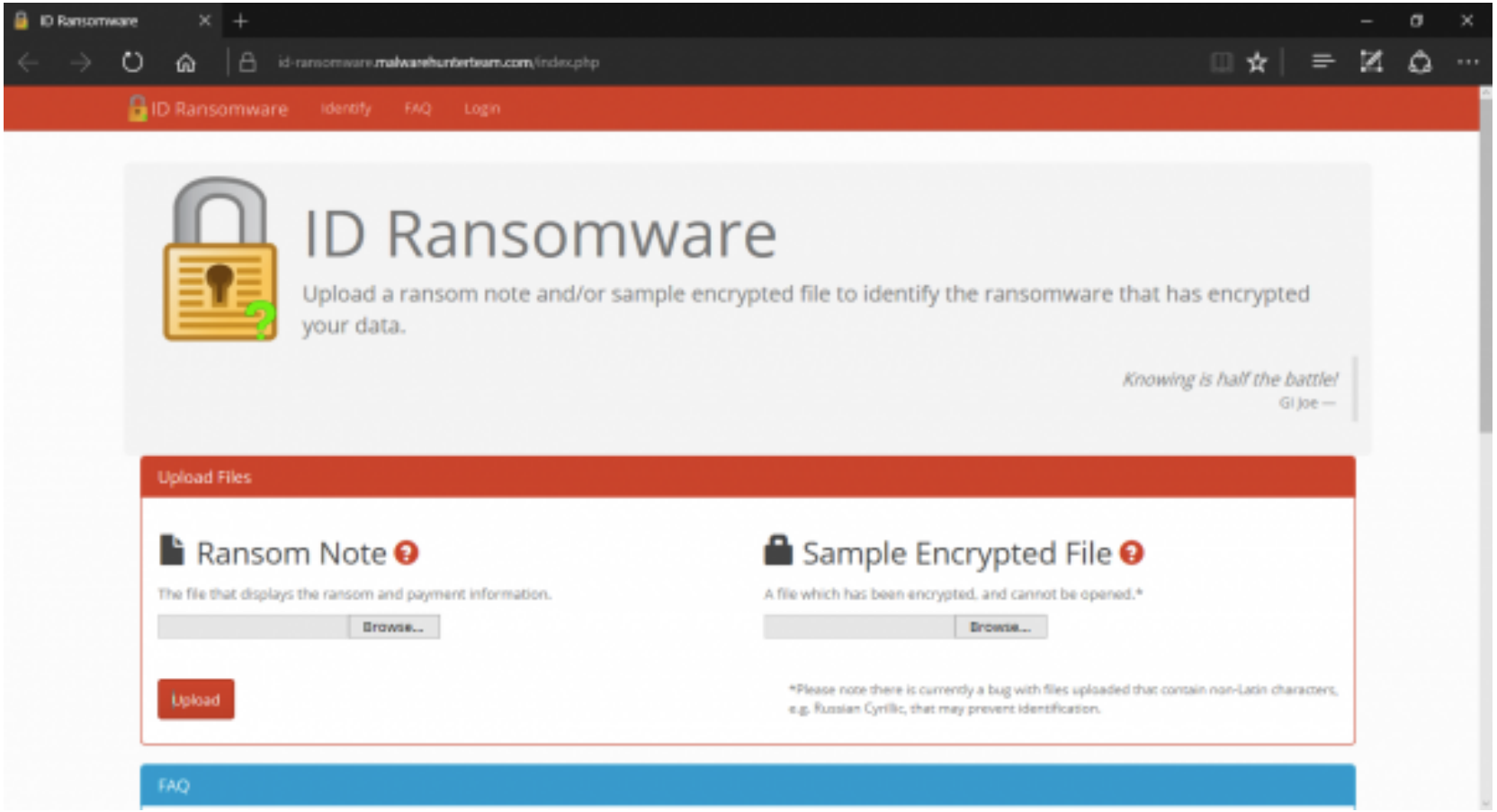
http://blog.trendmicro.com.tw/?p=16660

成功破解勒索軟件、真的可以嗎？

勒索軟件成為資訊保安新聞，連電視台新聞都有報導，亦有報導各種「勒索軟件成功破解方法」或是「安裝勒索軟件剋星一勞永逸」訊息。

誠然不少廠商都推出應付勒索軟件的方法，不過誰也不敢說「一勞永逸」，而就算能防範勒索軟件入侵或解密的程式，其實也只限於特定版本的勒索軟件，正所謂「勒索軟件有很多種」，只要變種了或是有全新的勒索軟件出現，這些方法也沒有辦法的。

如何知道被植入的何種勒索軟件



http://thewindowsclub.thewindowsclubco.netdna-cdn.com/wp-content/uploads/2016/04/ransomware-600x326.png

Copyright © 2016 Cloud Security Alliance

直至現時，未有任何有效方法確保為受脅持的檔案解鎖。因此，為保障你的電腦，請記：

A）慎防可疑郵件
請勿開啟附件，尤其壓縮檔（.zip、.7zip、.rar）或執行檔（.exe）。
請勿按郵件內的可疑網站連結。
B）停用 Office 檔案中的巨集。
C）定期為檔案備份，並將備份檔案儲存至安全地方，如離線，避免受惡意軟件攻擊。
D）定期為操作系統及電腦軟件安裝最新補丁。
E）安裝及定期更新防毒軟件。。

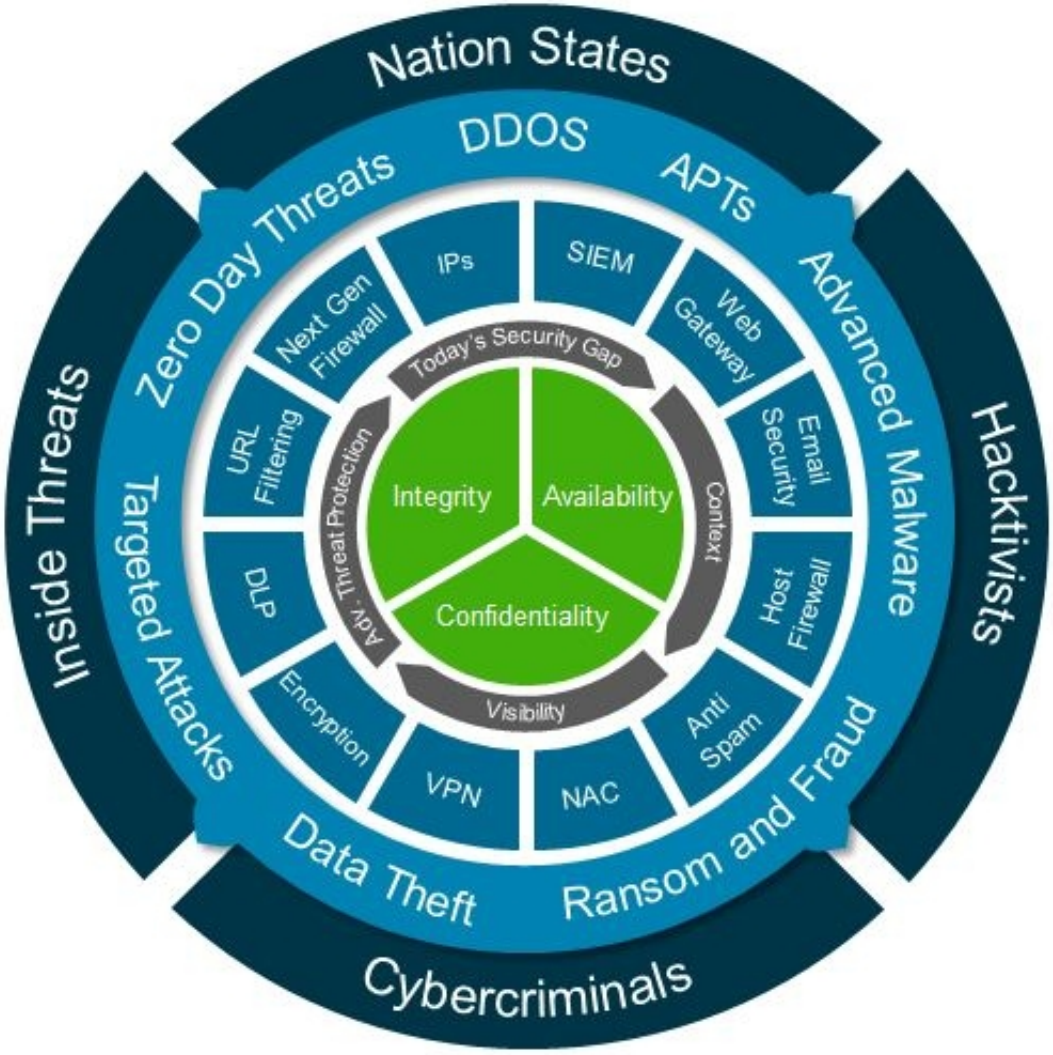
若不幸受害...

若你的電腦已遭 勒索軟件入侵...

1) 請**立即**中斷任何有線或無線連網，並拔除所有 USB 裝（避免進一步危害相關資料夾）。
2) 如被入侵的電腦內存有你的密碼資料（電郵、網上理財戶口等），請使用未受惡意軟件感染及可信的電腦更改所有相關密碼資料。
3) 不要即時回覆付款要求，儘量了解攻擊的勒索軟件種類，立即聯絡資訊科技服務處及報警求助跟進。
4) 如有良好可信備份，可考慮重新安裝電腦作業系統，並從備份檔案中修覆原有的資料。

() https://www.cuhk.edu.hk/itsc/chinese/security/gpis/ransomwarealert.html

多層防禦（Multi-layer Defense）



1. Firewall/VPN
2. IDS/IDP/DDOS/APT Gatewy
3. Anti-virus for Email Sever
4. Anti-Spam for Email Server
5. Web Filtering Gateway
6. Server Anti-Virus
7. Client Anti-Virus
8. Patch Management
9. USB Port Control
10. Application Control (White List)
11. Client Side APT
12. Deploy OpenDNS
13. SIEM
14. Awareness Training
15. Security Police/Framework

網上預防勒索軟體病毒免費工具

多間 公司推出一款能夠抵擋勒索病毒的工具，使用者可以免費下載使用，由於近年來的勒索病毒越來越多，不管是公家機關、中小企業、個人電腦等…都是勒索病毒的目 標可以預防Locky、TeslaCrypt、CTB-Locker勒索病毒；在這之前或許很多人使用　工具來預防病毒，不過 也因為病毒的變化方式導致沒有辦法有效預防，

有一些更有預防Ransomware 版本可以免費下載使用，對於目前主流勒索病毒也是可以有效預防，所以使用者多一層預防防護勒索病毒也是一個不錯的選擇。

Copyright © 2016 Cloud Security Alliance

https://labs.bitdefender.com/2016/03/combination-crypto-ransomware-vaccine-released/

Copyright © 2016 Cloud Security Alliance

KASPERSKY lab

RANSOMWARE DECRYPTOR

Welcome to NoRansom, your home for decryption tools and education on ransomware.

Ransomware is malware that locks your computer or encrypts your files. You can't get the data back unless you pay a ransom, and even if you do, there's no guarantee that you'll get your data back.

Before downloading and starting the solution, read the how-to guide. Make sure you remove the malware (you can use Kaspersky Internet Security) from your system first, otherwise it will repeatedly lock your system or encrypt files.

DESTROY COINVAULT

CoinVaultDecryptor tool is designed to decrypt files affected by **CoinVault and Bitcryptor.** The National High Tech Crime Unit (NHTCU) of the Netherlands' police, Netherlands' National Prosecutors & Kaspersky helped create this tool.

For more information please see this how-to guide.

SMASH RANNOH & CO

RannohDecryptor tool is designed to decrypt files affected by **Rannoh, AutoIt, Fury, Crybola, Cryakl, CryptXXX versions 1 and 2 (files encrypted by Trojan-Ransom.Win32.CryptXXX version 3 are detected, but not decrypted).**

For more information please see this how-to guide.

FIGHT RAKHNI & FRIENDS

RakhniDecryptor tool is designed to decrypt files affected by **Rakhni, Agent.iih, Aura, Autoit, Pletor, Rotor, Lamer, Lortok, Cryptokluchen, Democry, Bitman (TeslaCrypt) version 3 and 4.**

For more information please see this how-to guide.

https://noransom.kaspersky.com/

Copyright © 2016 Cloud Security Alliance

Obtaining and Executing the Tool(s)

1. Click the **Download** button below to obtain the latest version(s) of the Trend Micro Ransomware File Decryptor tool. Decompress (unzip) and then launch either the included RansomwareFileDecryptor or TeslacryptDecryptor exe file.

   Download RansomwareFileDecryptor

   Download TeslacryptDecryptor

2. Upon launch, users will be required to accept the End User License Agreement (EULA) to proceed.

3. After accepting the EULA, the tool will proceed to the main user interface (UI). From here, users will be presented with a step-by-step guide to perform the file decryption.

http://esupport.trendmicro.com/solution/en-us/1114221.aspx

Copyright © 2016 Cloud Security Alliance

Supported Ransomware Families

The following list describes the known ransomware-encrypted files types can be handled by the latest version of the tool.

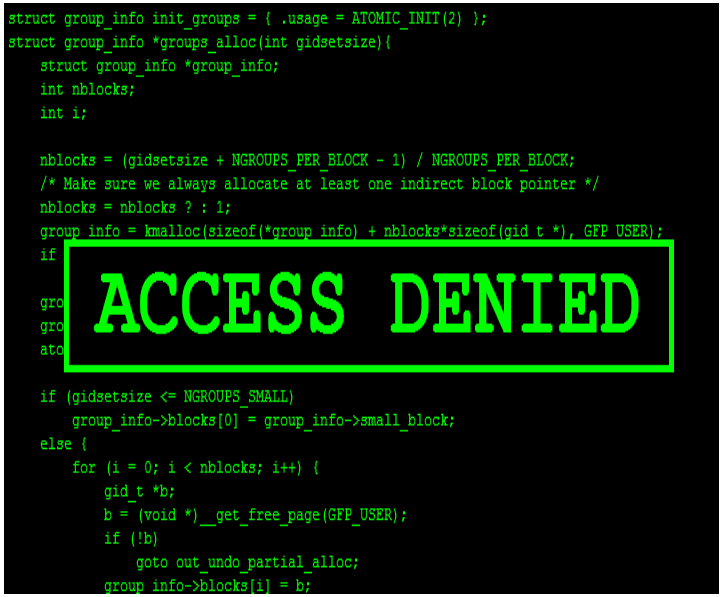
Ransomware	File name and extension
CryptXXX V1, V2, V3*	{original file name}.crypt, crypz, or 5 hexadecimal characters
TeslaCrypt V1**	{original file name}.ECC
TeslaCrypt V2**	{original file name}.VVV, CCC, ZZZ, AAA, ABC, XYZ
TeslaCrypt V3	{original file name}.XXX or TTT or MP3 or MICRO
TeslaCrypt V4	File name and extension are unchanged
SNSLocker	{Original file name}.RSNSLocked
AutoLocky	{Original file name}.locky
BadBlock	{Original file name}
777	{Original file name}.777
XORIST	{Original file name}.xorist or random extension
XORBAT	{Original file name}.crypted

http://esupport.trendmicro.com/solution/en-us/1114221.aspx

Copyright © 2016 Cloud Security Alliance

CISCO OpenDNS Home or VIP Home

- To block Ransomware's ability to phone home (C2) to botnets.
- Big Data Delivers Protection Before Malware Analysis



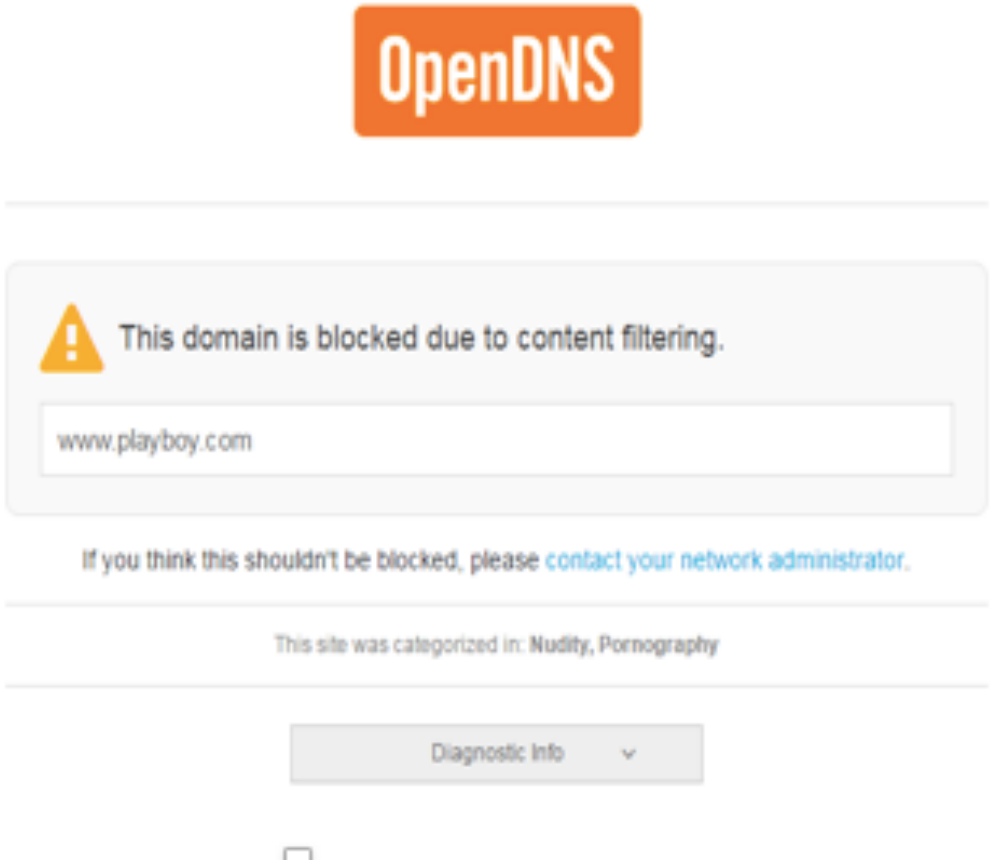
OpenDNS Home (Free) and OpenDNS VIP Home (USD19.9 per year)

Restrict Internet access to specific white-listed domain environment

OpenDNS

Copyright © 2016 Cloud Security Alliance

CISCO OpenDNS Home or VIP Home

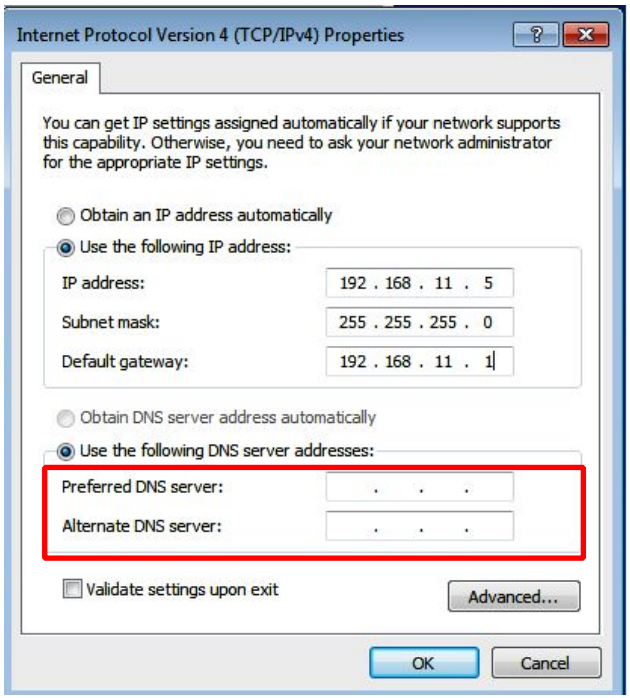


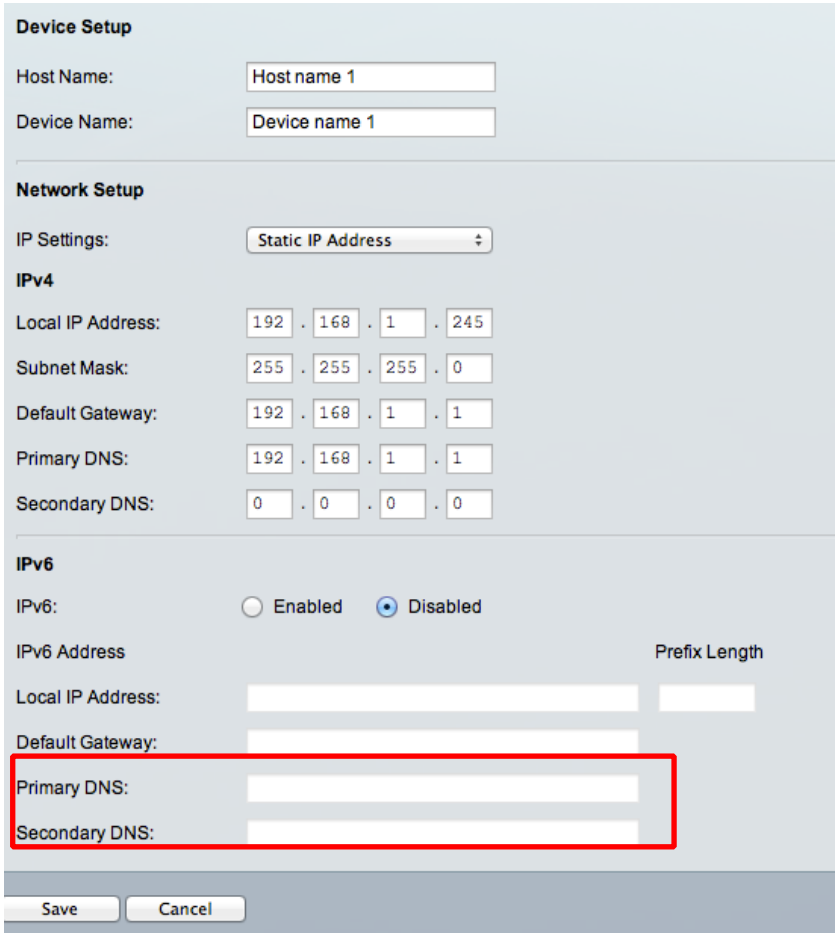
Copyright © 2016 Cloud Security Alliance

CISCO OpenDNS Home or VIP Home

DNS for OpenDNS Home

- 208.67.222.123
- 208.67.220.123

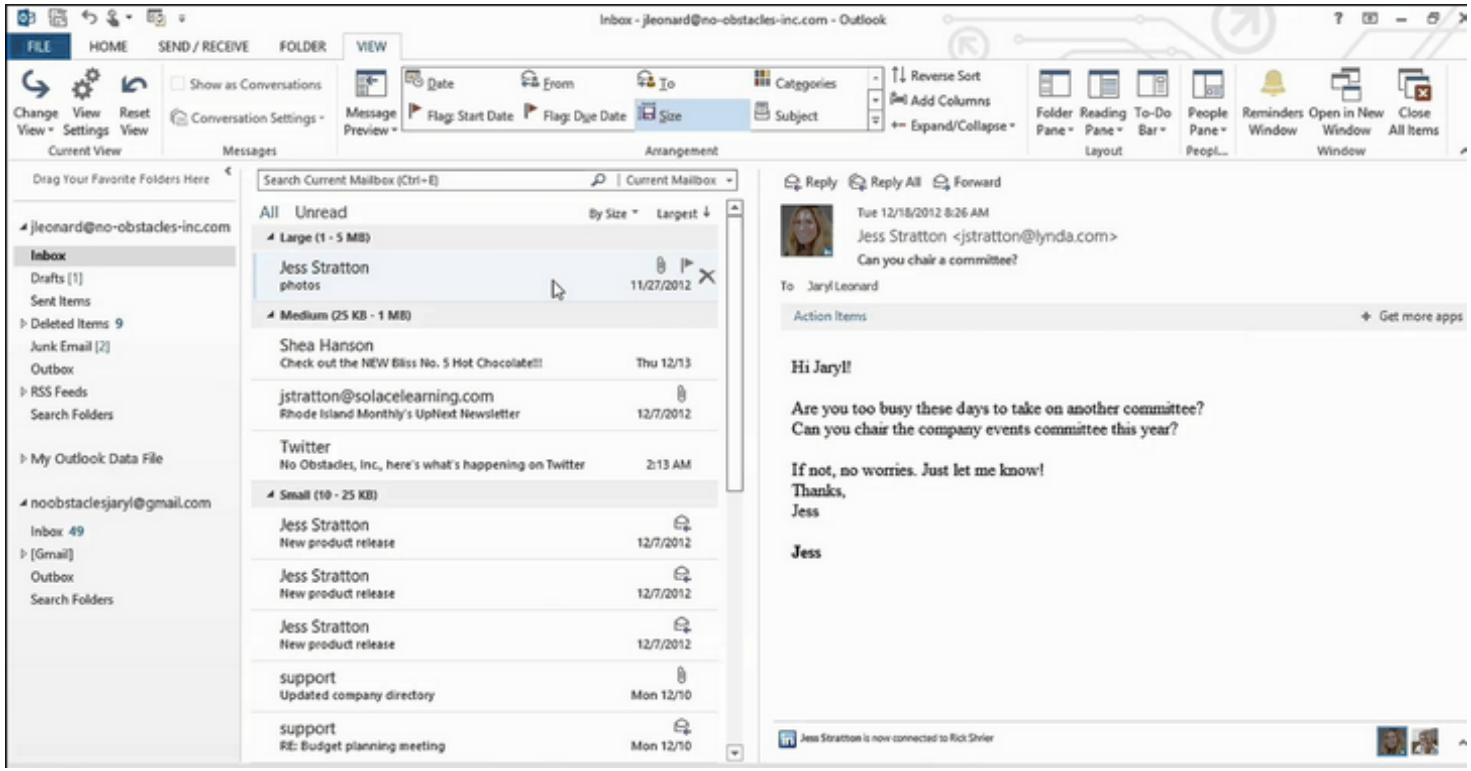




Copyright © 2016 Cloud Security Alliance

使用雲端Gmail 作 Email Filtering

- Forward all your email to a Gmail Account
- Using IMAP to get email using Gmail Account with your email client
- Gmail will filter suspicious email malware attachment



Copyright © 2016 Cloud Security Alliance

Android N equips with Anti-Ransomware

Android N plugs one ransomware attack vector

by **Martin Brinkmann** on July 11, 2016 in **Google Android** - Last Update:July 11, 2016 1

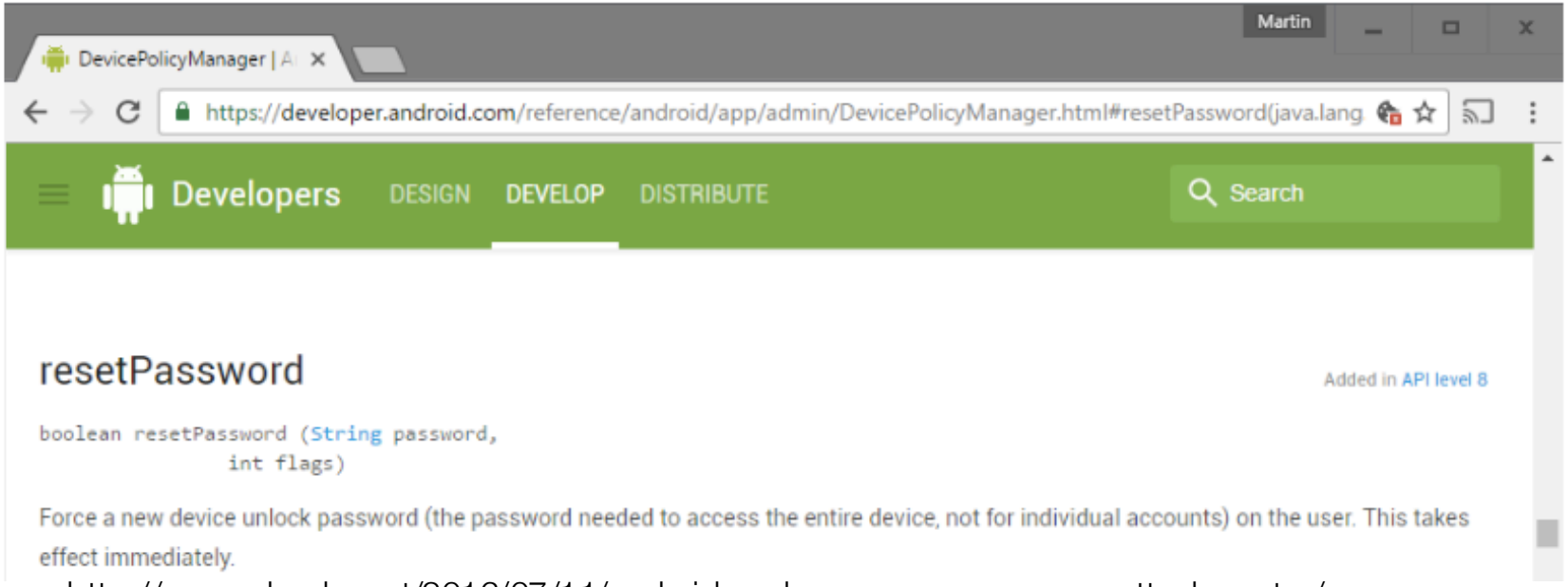
The upcoming Android N (Nougat) operating system ships with a security change that will prevent ransomware attacks from succeeding that target the unlock password.

Ransomware is not only a problem on desktop computer systems but also increasingly problematic on mobile devices.

Depending on what users do on the mobile device, it may be easy to have it infected with a ransomware variant.

Typically, this involves downloading apps from outside of the Google Play store.

Reset Password



http://www.ghacks.net/2016/07/11/android-n-plugs-one-ransomware-attack-vector/

Copyright © 2016 Cloud Security Alliance

1.勒索軟件的歷史
2.勒索軟件主要的感染途徑
3.勒索軟件相關是一盤生意？
4.常見勒索軟件種類及個案分享
5.勒索軟年的解決方案
6.如何從雲端計算減低勒索軟件入侵風險

http://blog.trendmicro.com.tw/?p=16660

傳統方案

NAS 檔案快照功能　瞬間還原受害檔案

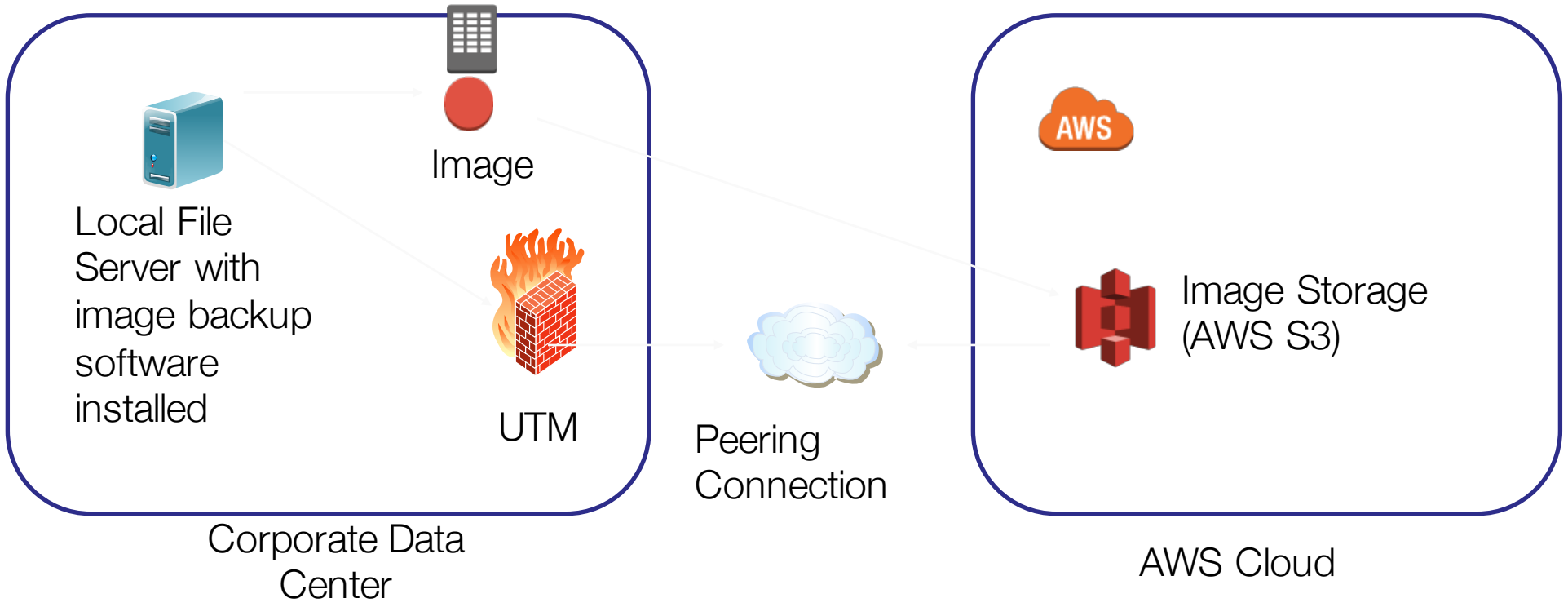
考量點：SnapShot – 硬盤容量的大小， 中距時間
NAS – 是被攻擊的目標之一， 且常設置在公共 IP地址

Copyright © 2016 Cloud Security Alliance

雲端計算如何助你減低遭到勒索軟件的威脅

Copyright © 2016 Cloud Security Alliance

Traditional Cloud Image backup solution

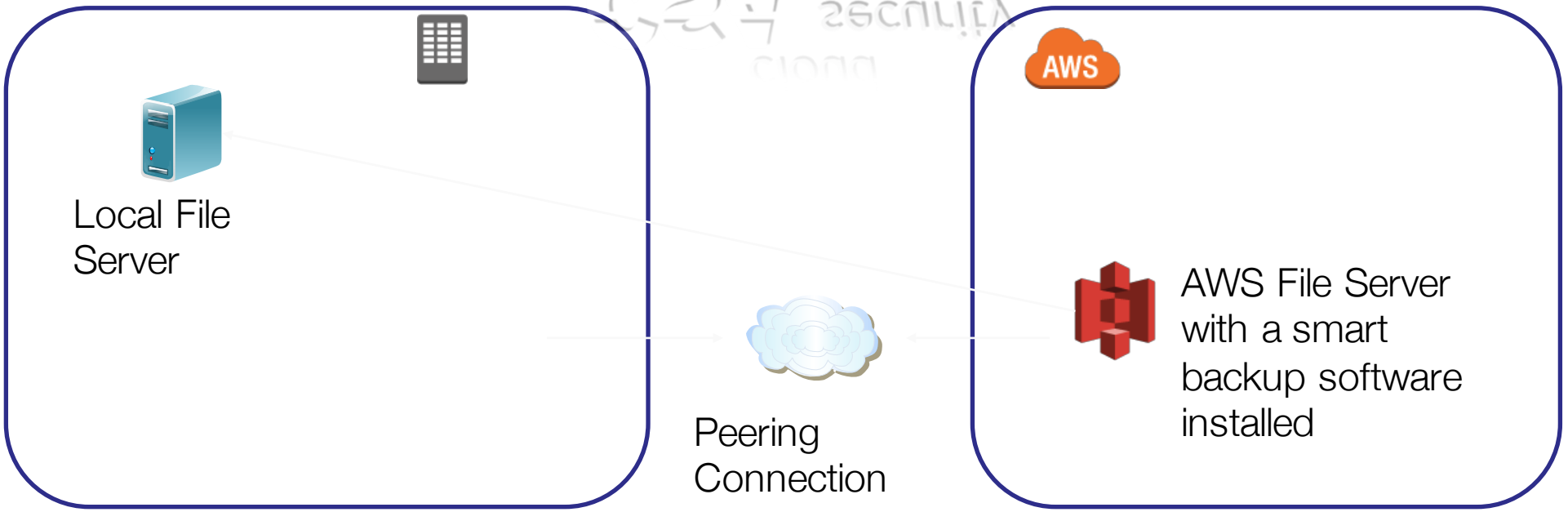


- Install image backup software(e.g. Acronis Backup) on local file server
- Admin can specific a path to create backup image
- Store the backup image to cloud
- In case of restore is needed, admin can retrieve the backup image from cloud storage

Copyright © 2016 Cloud Security Alliance

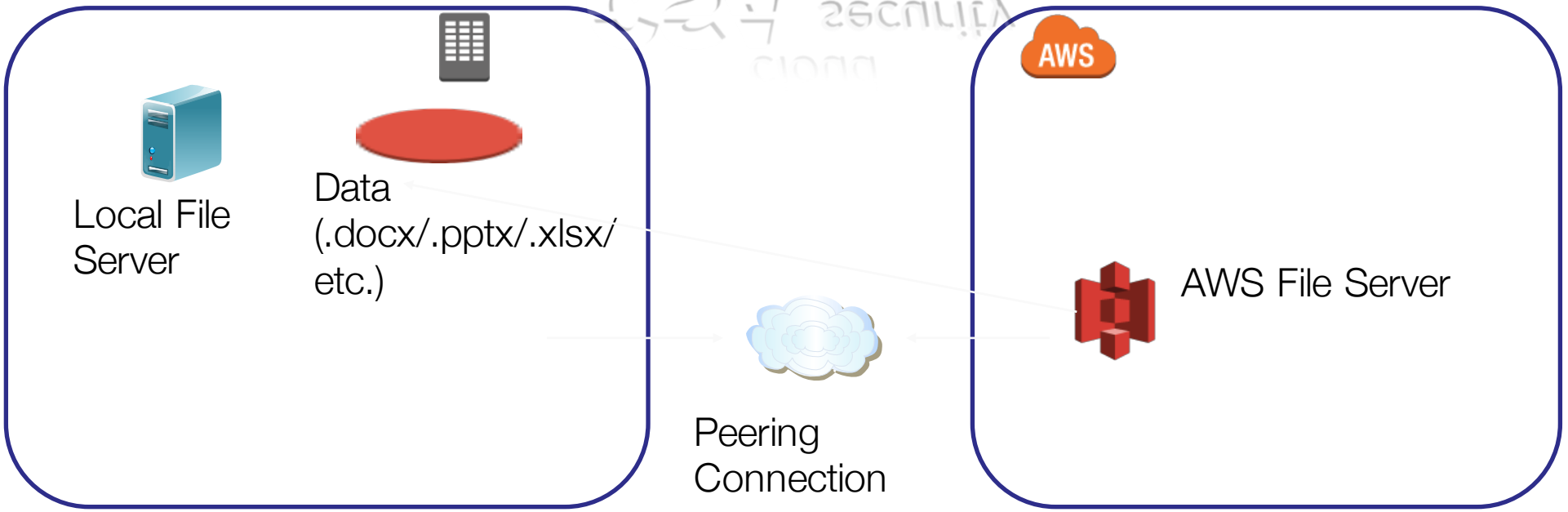
雲端計算只是個備份方案？

Copyright © 2016 Cloud Security Alliance



AWS File server will take the initiative to ask the local server to backup their files to AWS. Instead of waiting the local server to push every thing to cloud.

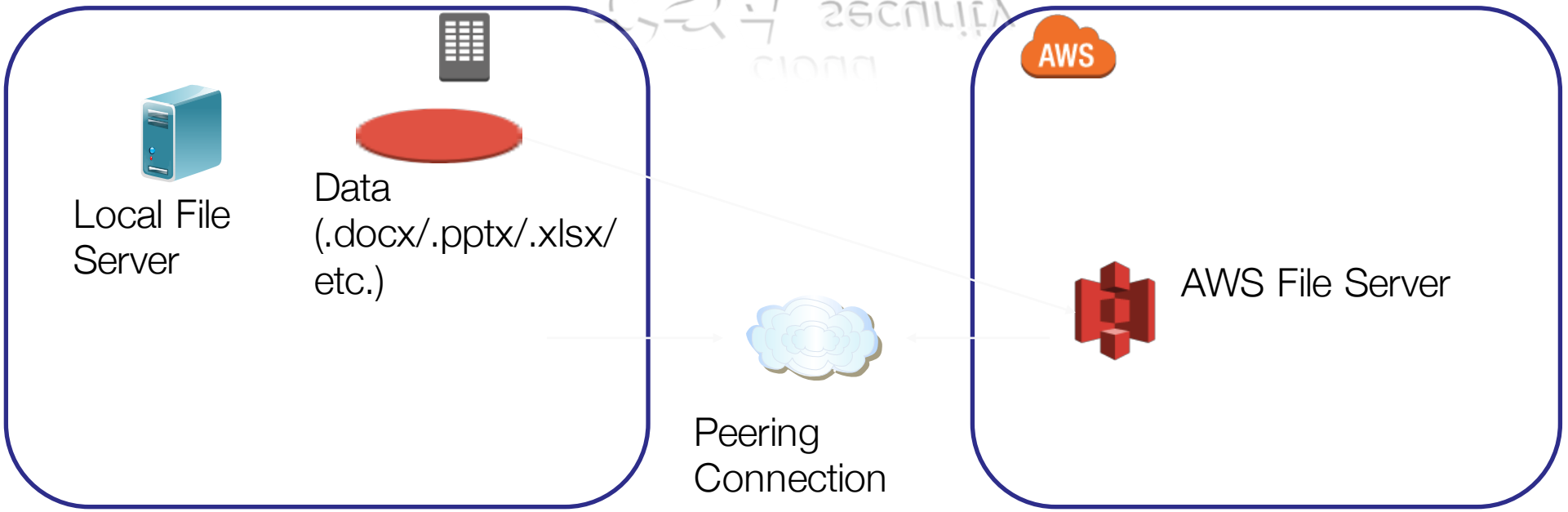
Copyright © 2016 Cloud Security Alliance



When new data is available, cloud server will check the extension of the local data. Only some user defined extension's file will be allowed to upload.

It can prevent upload some encrypted files to cloud server.

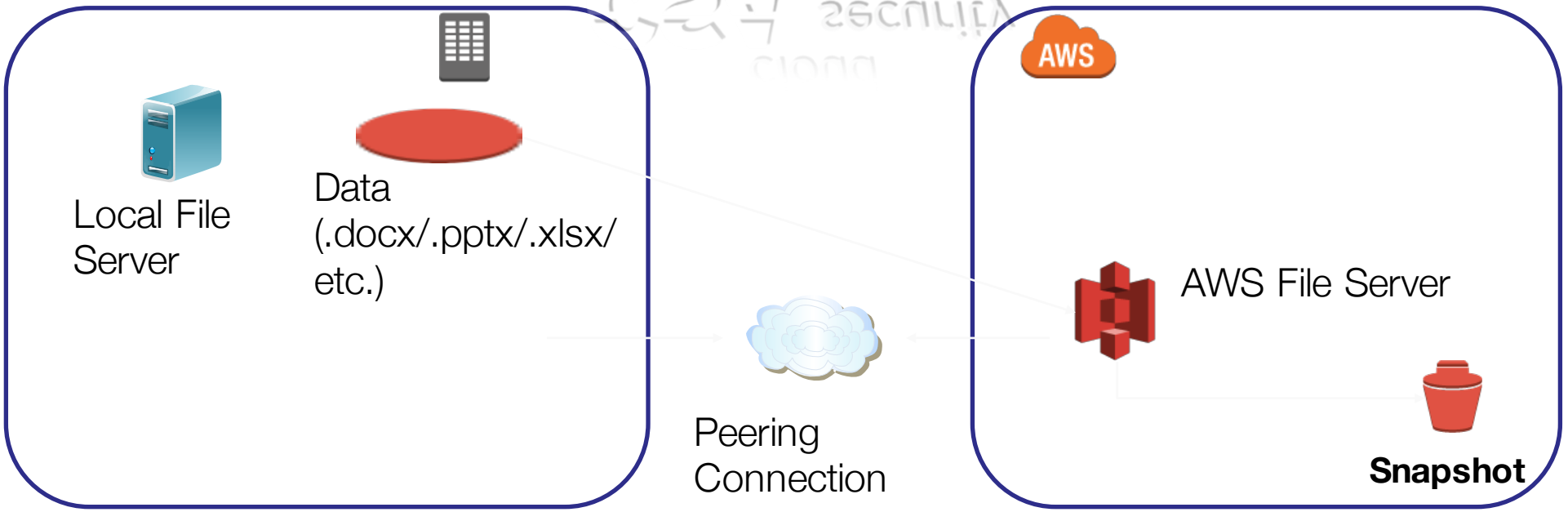
Copyright © 2016 Cloud Security Alliance



Check the local file server's file extension, select only those allowed extension file.

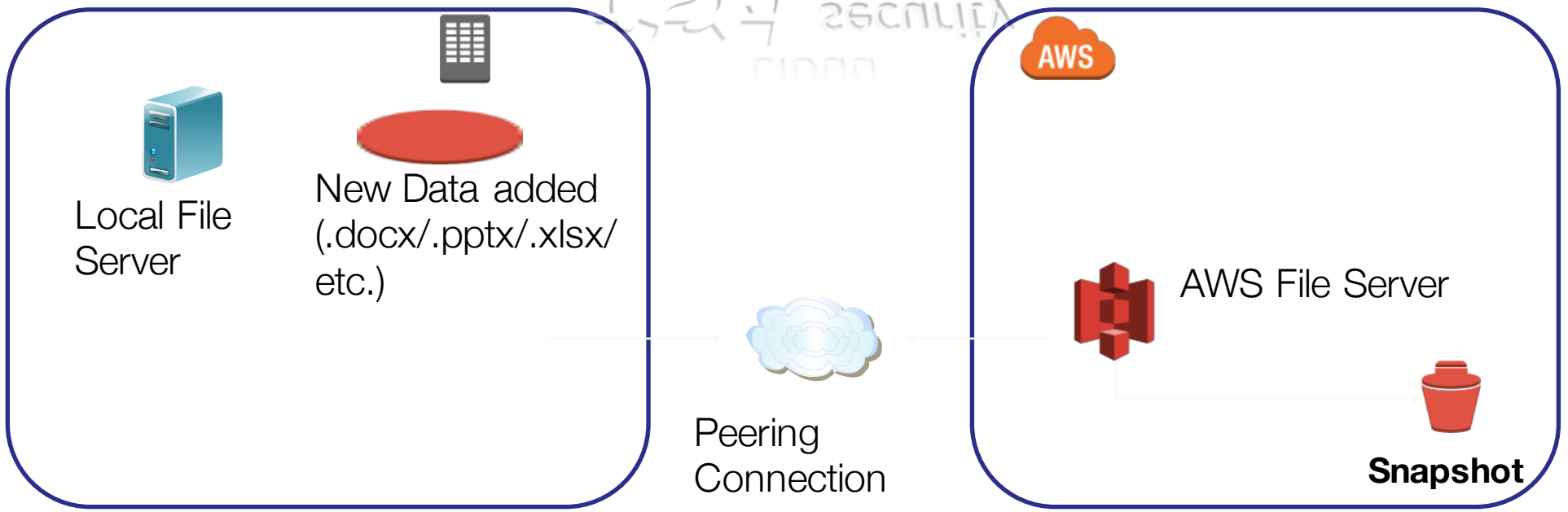
After Checking, cloud server will start to download those allowed data.

Copyright © 2016 Cloud Security Alliance



Once the backup job completed, cloud server will take a snapshot for it.

Copyright © 2016 Cloud Security Alliance



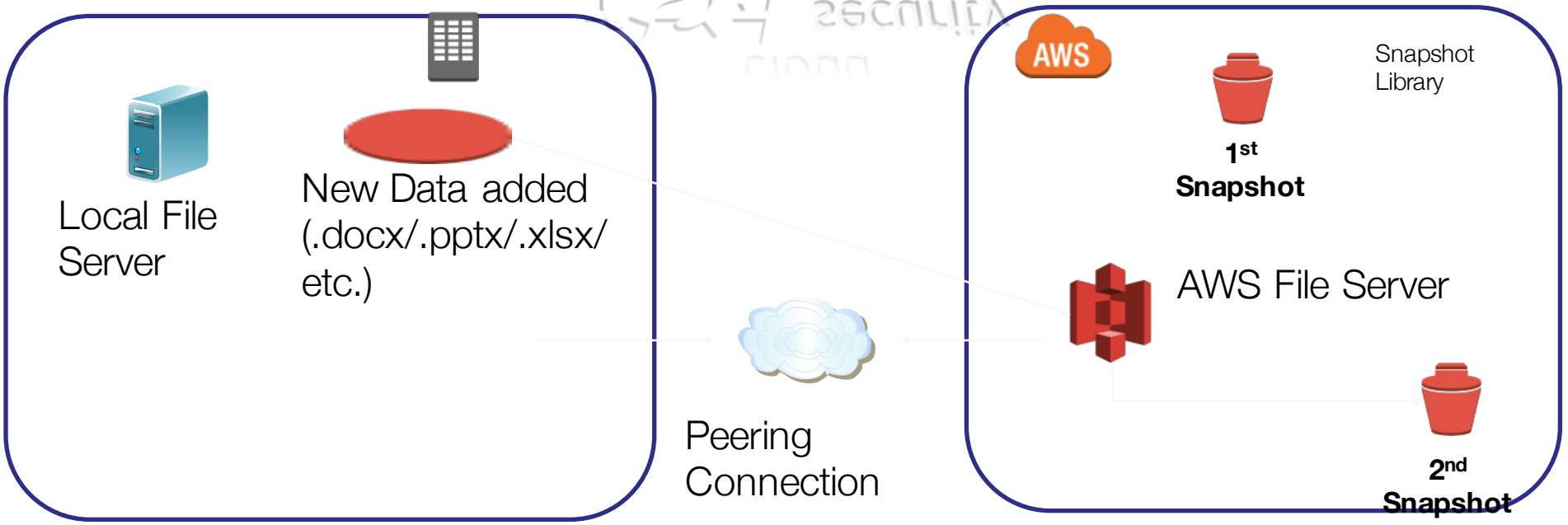
If new data is added, cloud server will load the snapshot and check the data between cloud and local.

Only new or modified data will be uploaded to cloud this time.

It can reduce transfer a large amount of data each time.

Cloud server will compare the difference between local data and the snapshot

Copyright © 2016 Cloud Security Alliance

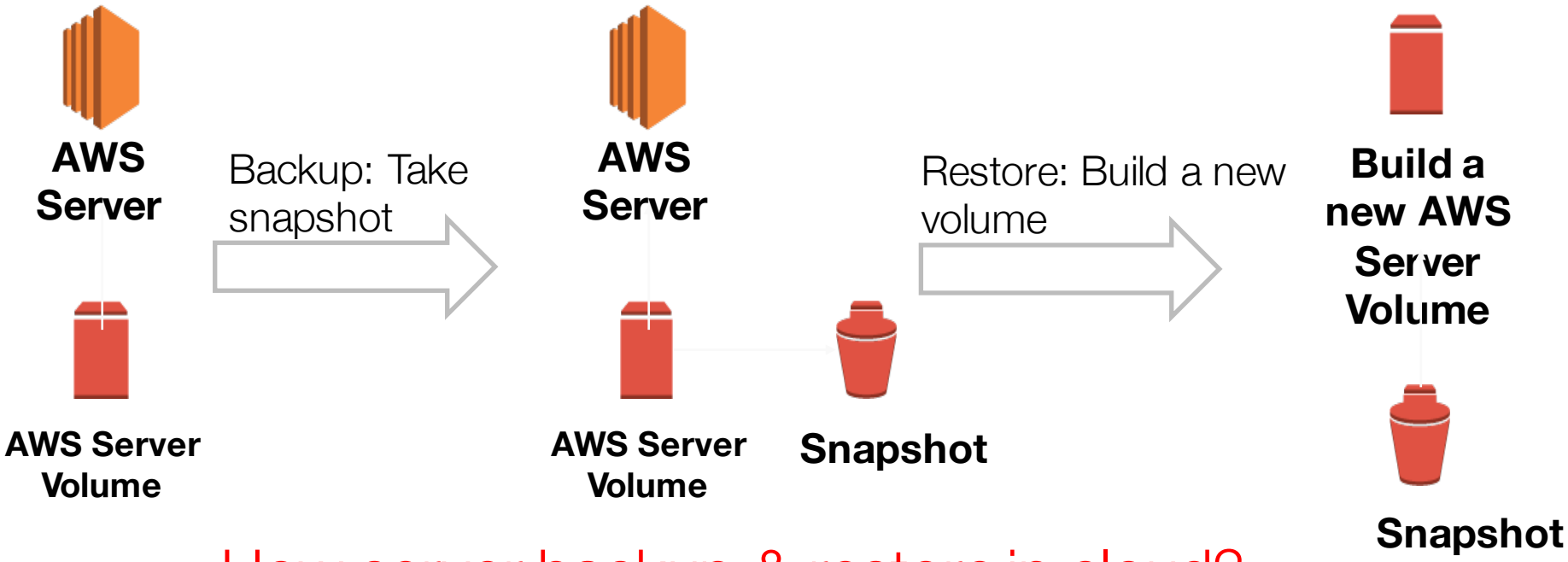


Cloud server download new or modified data to cloud and take a snapshot again

User can define to keep how many version of snapshot.

Copyright © 2016 Cloud Security Alliance

使用Cloud Service Provider

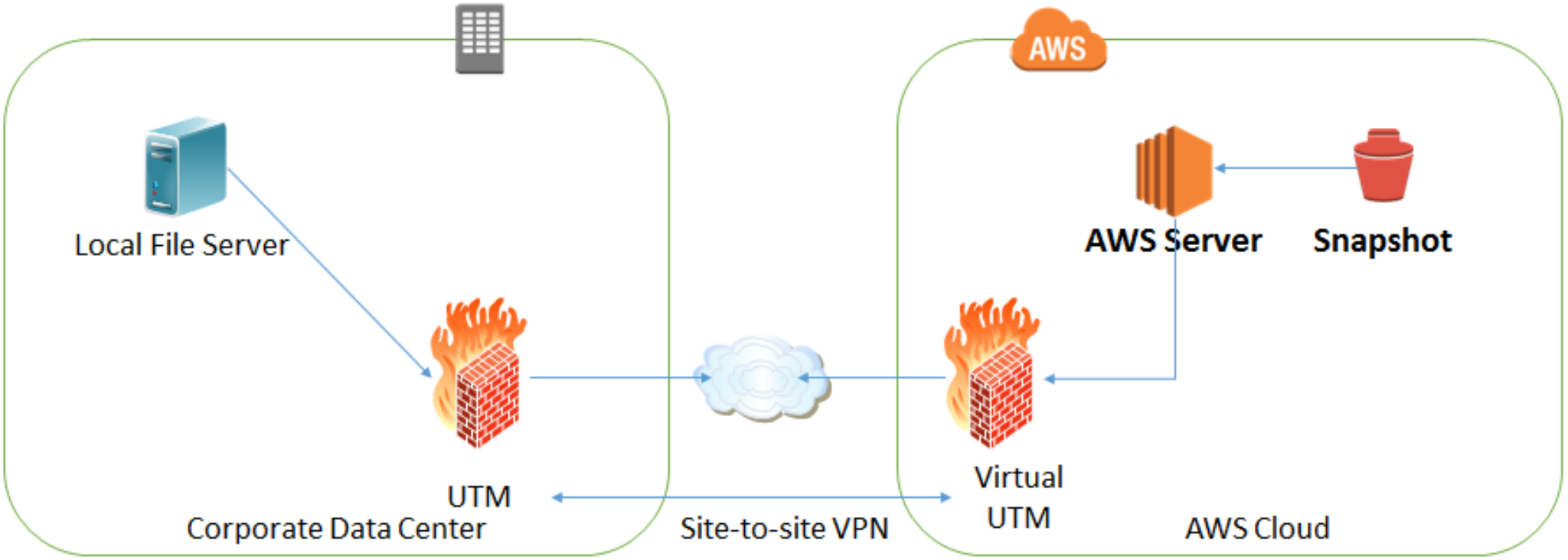


How server backup & restore in cloud?

Cloud snapshot's benefit

- Backup server volume as snapshot in five mins
- No time limit for snapshot
- No concern on storage for snapshot

Stand-by Server in cloud



- When local server is affected by ransomware
- Enable site-to-site VPN between local data center and cloud
- Resume file server service in cloud
- Cloud file server will take snapshot hourly to keep latest version of data

Copyright © 2016 Cloud Security Alliance

勒索軟件發展總結

1. 組織企業化
2. 版本多元化
3. 對象全球化
4. 介面中文化
5. 交收虛擬化
6. 系統多樣化

Mac OS X

ANDROID

UNIX®

Linux

Windows Server

Copyright © 2016 Cloud Security Alliance

Takeaway
利用雲端計算相關技術及預演部署作為減低被勒索軟件攻擊機會

1. 預防勝於治療
2. 智能雲端備份軟件
3. 使用信任DNS過慮服務
4. 網釣攻擊模擬演練
5. 使用公信知名的雲端電郵服務
6. 事故反應(IR)計劃

Copyright © 2016 Cloud Security Alliance

Copyright © 2016 Cloud Security Alliance

Thank You

Mike Lo, mlo@deloitte.com.hk

Copyright © 2016 Cloud Security Alliance