HITCON Talk
金融資安科技研討會

技術解析 SWIFT Network 攻擊

張裕敏

gasgas4@gmail.com

ziv_chang@trend.com.tw

事件回顧

孟加拉央行被盜領8100萬美元

- 駭客集團是在今年2月入侵了孟加拉央行的系統，企圖從該行位於聯邦儲備銀行紐約分行的帳戶轉出9.51億美元，駭客原本打算分數十次盜轉上述基金，但在第五次要轉帳至偽造的斯里蘭卡非營利組織Shalika Foundation時，把Foundation誤打成Fandation，因而引起注意，使得孟加拉央行停止了之後的轉帳，最後駭客只成功轉出8100萬美元到菲律賓的偽造帳戶。

新聞來源: ITHOME http://www.ithome.com.tw/news/105463 (20160425)

越南先鋒銀行被駭 險轉走136萬美元

- 〔編譯楊芙宜／綜合報導〕繼孟加拉央行後，越南央行官員週二證實，越南先鋒銀行（Tien Phong Bank或TP Bank）也遭遇類似網路駭客攻擊，所幸並未成功；駭客都利用SWIFT（環球銀行金融電信協會）通訊系統，試圖詐騙且轉移120萬歐元（約136萬美元）至斯洛維尼亞銀行，但遭到攔阻。消息傳出後，新加坡和菲律賓央行都要求國內金融業者維持資安高度警戒狀態。

新聞來源: 自由時報 http://news.ltn.com.tw/news/business/paper/990745（20160518)

厄瓜多爾一家銀行 遭駭客盜提近1200萬美元

- 法院文件指出，這宗網路駭客攻擊竊盜案發生在2015年1月，和孟加拉國央行被盜走一樣，駭客取得Banco del Austro使用Swift的代碼，進而用以轉走存放在另一家銀行的資金。
- 根據報導，Banco del Austro今年向紐約聯邦法院提告，指控富國銀行沒有注意到去年1月間出現12次轉帳交易的「危險訊號」，且未在竊賊轉走約1200萬美元前就阻止這些交易，導致大部分資金被轉移至香港的銀行。

新聞來源: 自由時報 http://news.ltn.com.tw/news/business/breakingnews/1703513（20160520)

又見駭客攻擊銀行　一菲律賓銀行疑受害

- 孟加拉央行今年2月遭駭客攻擊，被竊走8100萬美元（26.3億元台幣），資訊安全業者指出，駭客用同一手法發動另一波攻擊，受害者是菲律賓一家銀行，如經證實，這將是環球銀行金融電信協會（SWIFT）第4起遭到網路攻擊的案件。

新聞來源: 蘋果日報 http://www.appledaily.com.tw/realtimenews/article/new/20160527/871953/

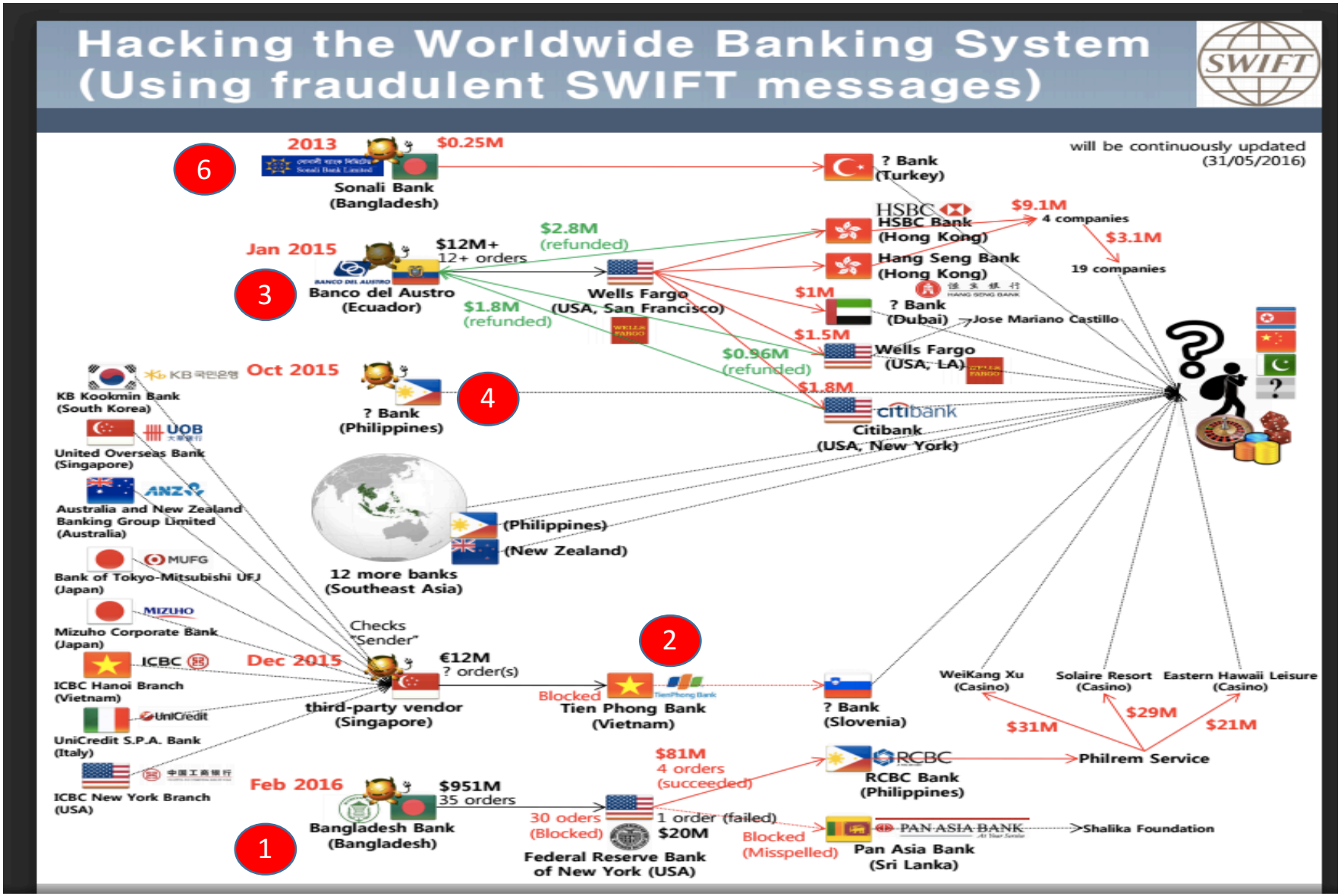
SWIFT黑客再現 烏克蘭銀行被盜一千萬美元

- 國際信息系統審計協會（ISACA）的專家近日證實『 SWIFT 黑客』再次現身，這一次他們再次通過 SWIFT 系統漏洞從一家烏克蘭銀行盜走了一千萬美元（約6650萬元人民幣）。

- 烏克蘭銀行僱傭了 ISACA 組織進行一起網絡攻擊的相關調查，但是就目前來看，已有多家銀行遭到了攻擊，損失達上千萬美元。
- 「目前，已經有數十家銀行（主要位於烏克蘭與俄羅斯）被攻擊，黑客從這些銀行中盜走了上千萬美元，」 ISACA 在一份新聞稿中說道。
-

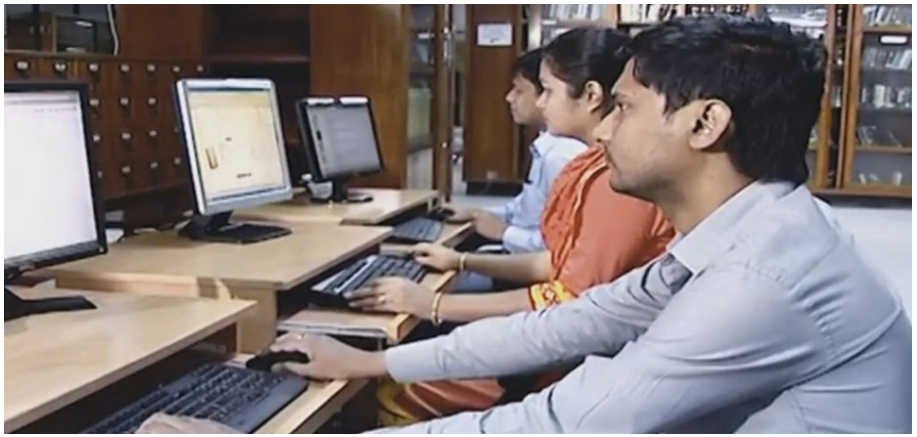
新聞來源: 每日頭條 https://kknews.cc/news/jvgyll.html （2016 06 27)

攻撃分析


Hacking the Worldwide Banking System
(Using fraudulent SWIFT messages)
SWIFT
will be continuously updated
(31/05/2016)
6
2013
$0.25M
Sonali Bank
(Bangladesh)
? Bank
(Turkey)
HSBC
HSBC Bank
(Hong Kong)
$9.1M
4 companies
$3.1M
19 companies
Hang Seng Bank
(Hong Kong)
Jan 2015
$12M+
12+ orders
$2.8M
(refunded)
3
Banco del Austro
(Ecuador)
Wells Fargo
(USA, San Francisco)
$1.8M
(refunded)
$1M
? Bank
(Dubai)
Jose Mariano Castillo
$1.5M
Wells Fargo
(USA, LA)
$0.96M
(refunded)
$1.8M
citibank
Citibank
(USA, New York)
Oct 2015
KB Kookmin Bank
(South Korea)
? Bank
(Philippines)
4
United Overseas Bank
(Singapore)
Australia and New Zealand
Banking Group Limited
(Australia)
(Philippines)
(New Zealand)
12 more banks
(Southeast Asia)
Bank of Tokyo-Mitsubishi UFJ
(Japan)
Mizuho Corporate Bank
(Japan)
Checks
"Sender"
2
ICBC Hanoi Branch
(Vietnam)
Dec 2015
€12M
? order(s)
third-party vendor
(Singapore)
Blocked
Tien Phong Bank
(Vietnam)
? Bank
(Slovenia)
UniCredit S.P.A. Bank
(Italy)
ICBC New York Branch
(USA)
WeiKang Xu
(Casino)
Solaire Resort
(Casino)
Eastern Hawaii Leisure
(Casino)
$29M
$31M
$21M
$81M
4 orders
(succeeded)
RCBC
RCBC Bank
(Philippines)
Philrem Service
Feb 2016
$951M
35 orders
Bangladesh Bank
(Bangladesh)
1
30 oders
(Blocked)
1 order (failed)
$20M
Federal Reserve Bank
of New York (USA)
Blocked
(Misspelled)
PAN ASIA BANK
Pan Asia Bank
(Sri Lanka)
Shalika Foundation

孟加拉央行 (Bangladesh Central Bank) 攻擊分析

- 至少32台電腦被佔領
- Accounts and Budgeting Department 的內部系統中, 有一台電腦專門用來與SWIFT系統連線, 這電腦有三個終端機可供登入使用
- 稽核記錄分析發現, 1月24日可能為第一次駭客登入,1月29日駭客用管理權限安裝 “SysMon in SWIFTLIVE” , 接著駭客每天登入直到2月6日為止



藏在SWIFT網路的惡意程式

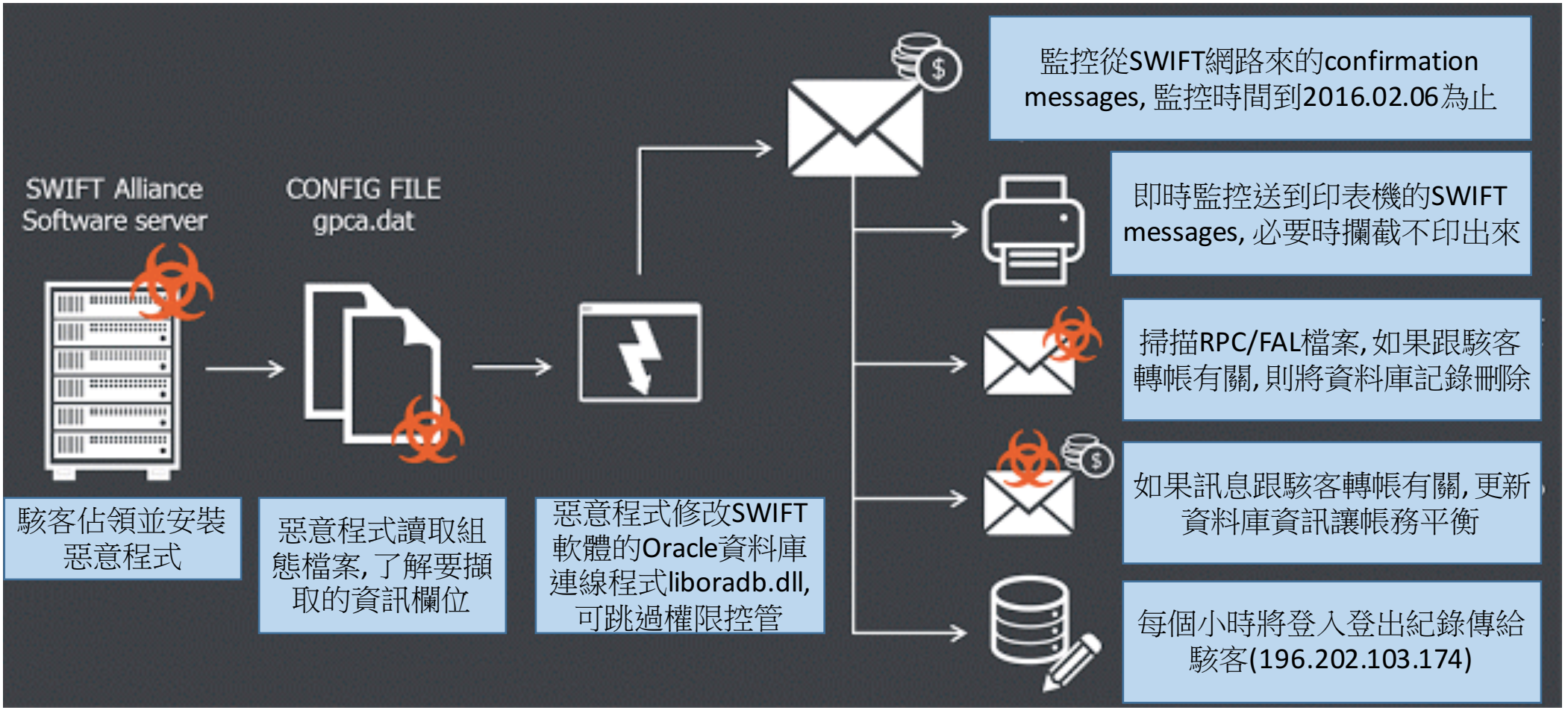
主要惡意程式, 程式總指揮 2016-02-05 11:46:20

程式清道夫 2016-02-04 13:45:39

組態檔案, 駭客轉帳資訊存在此處

印表機控制主程式 2016-02-05 08:55:19

孟加拉央行惡意程式運作方式



越南先鋒銀行(Tien Phong)攻擊分析

- 攻擊可能時間: 2015-12-04
- 資安公司樣本發現時間: 2015-12-22
- 銀行調查時間: 2016.02 (孟加拉銀行新聞出來之後)
- 銀行調查回報時間: 2016.05
- 攻擊手法: 換掉 PDF reader: Foxit (FoxItReader.exe Foxlt_Reader.exe)
- 這個惡意程式會攔截8個銀行傳來的SWIFT messages, 然後刪除交易紀錄, 交易歷史紀錄, 系統紀錄, 阻擋印表機列印交易

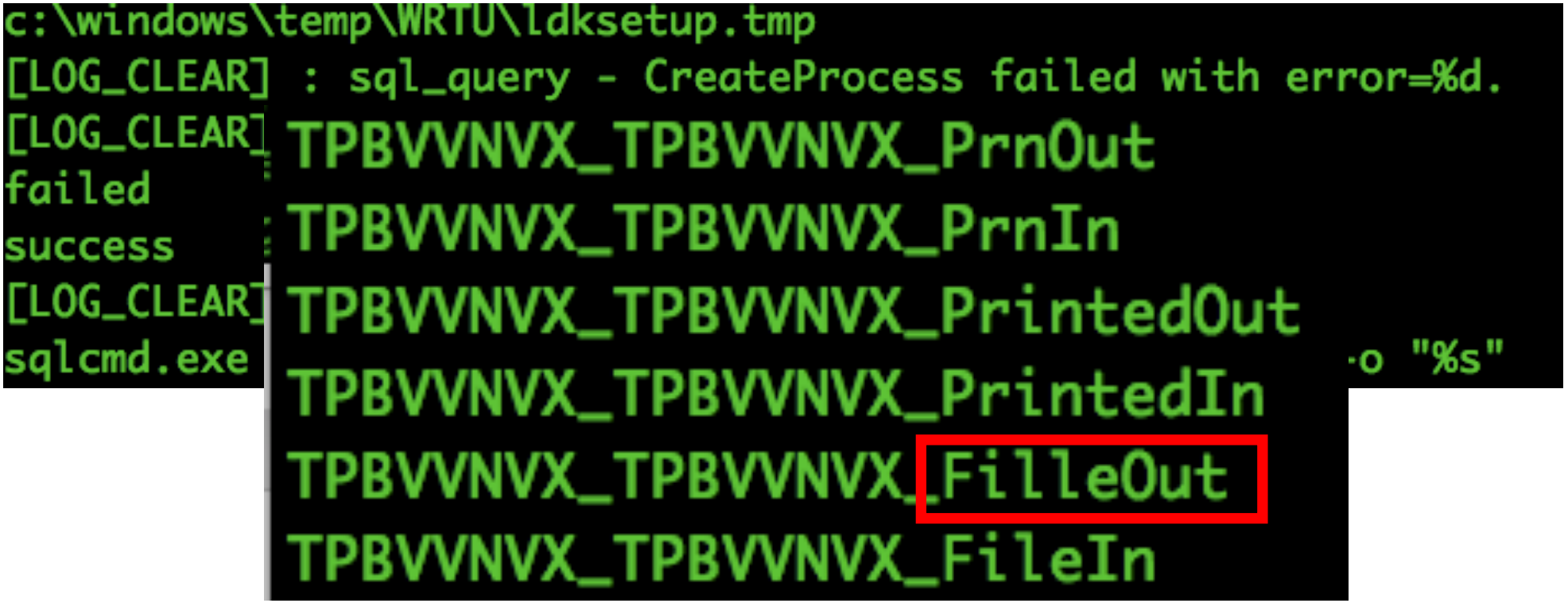
惡意程式(I): 攔截的8家銀行資訊

Foxit_Reader.exe_ab9031e553b439290b9852ad39651c03bde00c300ea54bd61279fb9ae9f9434d

SWIFT Codes	Banks
UOVBSGSGXXX	United Overseas Bank Ltd, Singapore
ANZBAU3MXXX	Australia and New Zealand Banking Group Ltd, Melbourne, Australia
BOTKJPJTXXX	Bank of Tokyo-Mitsubishi UFJ Ltd, Tokyo, Japan
MHCBJPJTXXX	Mizuho Bank Ltd, Tokyo, Japan
CZNBKRSEXXX	Kookmin Bank, Seoul, South Korea
UNCRITMMXXX	Unicredit S.P.A., Milan, Italy
ICBKVNVNXXX	Industrial and Commercial Bank of China, Hanoi branch, Vietnam
ICBKUS33XXX	Industrial and Commercial Bank of China, New York branch, United States

惡意程式(II): 清除稽核紀錄

mspdclr.exe_764189cf2707175251df6837da12797420ae4c482ad70f50cc0ec4acd21e4dff



Ecuadorian bank(Banco del Austro (BDA))

- 發生時間: 2015.01
- 惡意程式先佔領銀行內部網路
- 攻佔 SWIFT network網路
- 透過SWIFT, 偽造交易訊息從大銀行把錢轉出來
- 錢轉入 Hong Kong, Dubai(Mashreq bank), New York and Los Angeles.

烏克蘭多家銀行透過SWIFT方式被盜

- 2016.06.27
- 受害區域: 烏克蘭, 俄羅斯
- 家數: 12家(以上)
- 金額: 有一家 1M USD, 總數 10M USD

Взломщикам SWIFT повезло на Украине

01.07.2016 774

Очередной банк стал жертвой взломщиков системы SWIFT — на этот раз на Украине. Манипулируя сообщениями межбанковской информационной платформы, мошенники похитили 10 млн долларов.

Киевский филиал международной ассоциации специалистов в области IT-консалтинга и аудита Information Systems Audit and Control Association (ISACA) сообщил о краже денежных средств в размере 10 млн долларов из украинского банка посредством манипулирования командами в системе SWIFT. Об этом сообщило местное издание Kyiv Post.

Представители ISACA не стали уточнять название банка. По их словам, банк нанял их для расследования инцидента. К выводу о том, что хищение было совершено через SWIFT, они пришли в ходе работы. Специалисты не сообщили предполагаемую страну пребывания взломщиков.

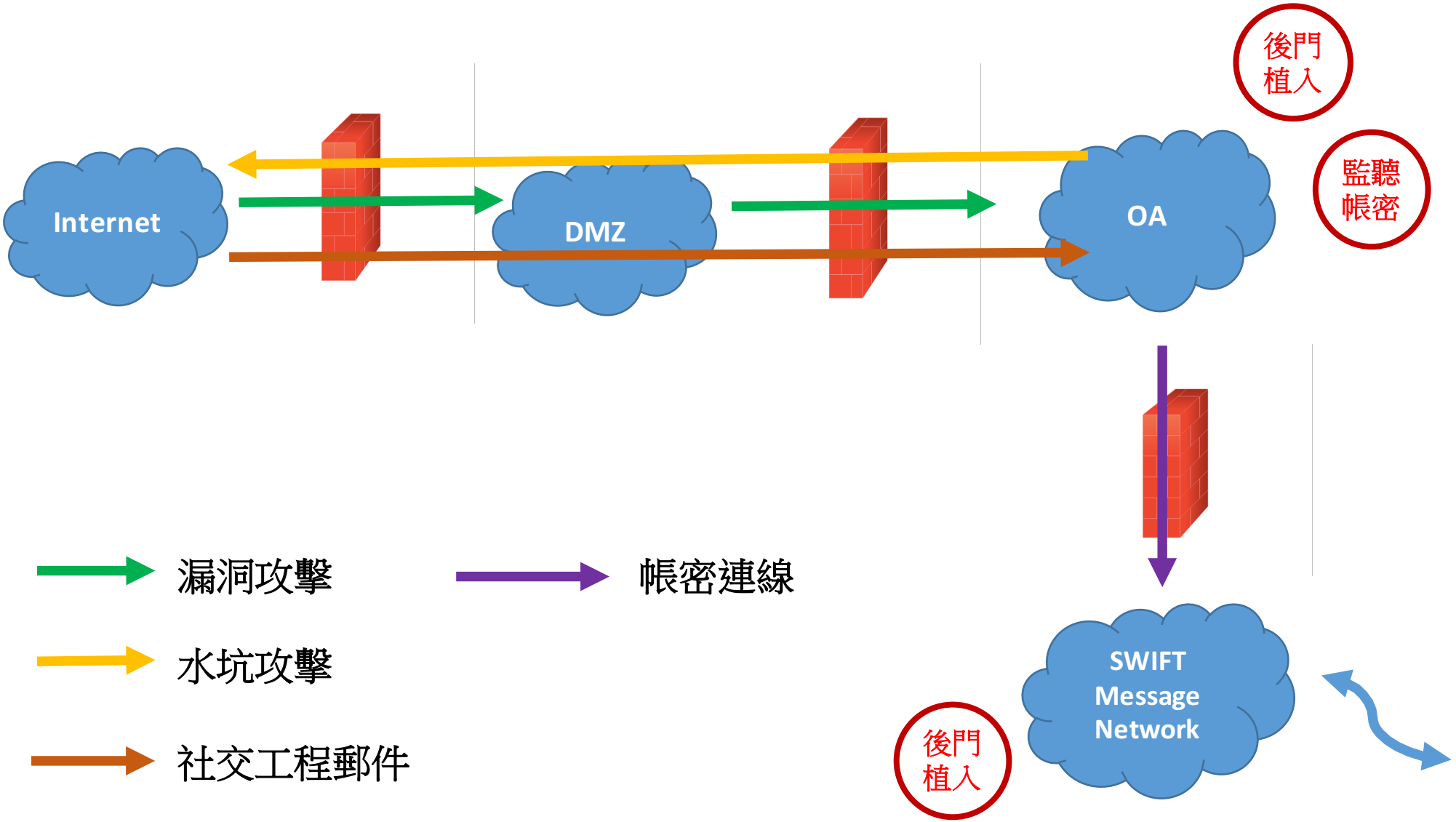
«К настоящему моменту хакеры проникли в десятки банков и похитили из них сотни миллионов долларов. Главным образом это банки на Украине и в России», — заявили в ISACA без уточнения подробностей.

事件共通點

- 銀行內部網路被佔領
- SWIFT network 伺服器被佔領
- 駭客可以從Internet遠端進入SWIFT伺服器
- 駭客對於SWIFT messages type很熟(對整個SWIFT系統**Alliance Access軟體**也很熟)
- 兩個案件中, 惡意程式內的英文字都會拼錯.....

Vietnam case	Attacker code featured the string 'FilleOut' instead of 'FileOut'
Bangladesh case	Attacker code featured the string 'alreay' instead of 'already'
	Attacker mis-spelled 'foundation' as 'fandation'

駭客如何進來的!???


Internet
DMZ
OA
後門
植入
監聽
帳密
漏洞攻擊
帳密連線
水坑攻擊
社交工程郵件
SWIFT
Message
Network
後門
植入

防範未來

如何防範後續的攻擊

- 各國銀行的提議
  - SWIFT 交易需要Fingerprint scanner confirm
  - SWIFT 交易需要啟動雙因子認證 (2016.05.28)
  - SWIFT 交易採用USB傳遞資訊
- 資安強化
  - Application Control (應用程式控管)
  - Integration check(檔案整合性測試, 系統整合性測試)
  - Access Control (連線控管, 存取控制, 帳密管制, 特權帳號管理)
  - Auditing log and record(稽核紀錄與監控)
  - 不該出現警示的地方, 就算只出現一次警示, 就應詳查