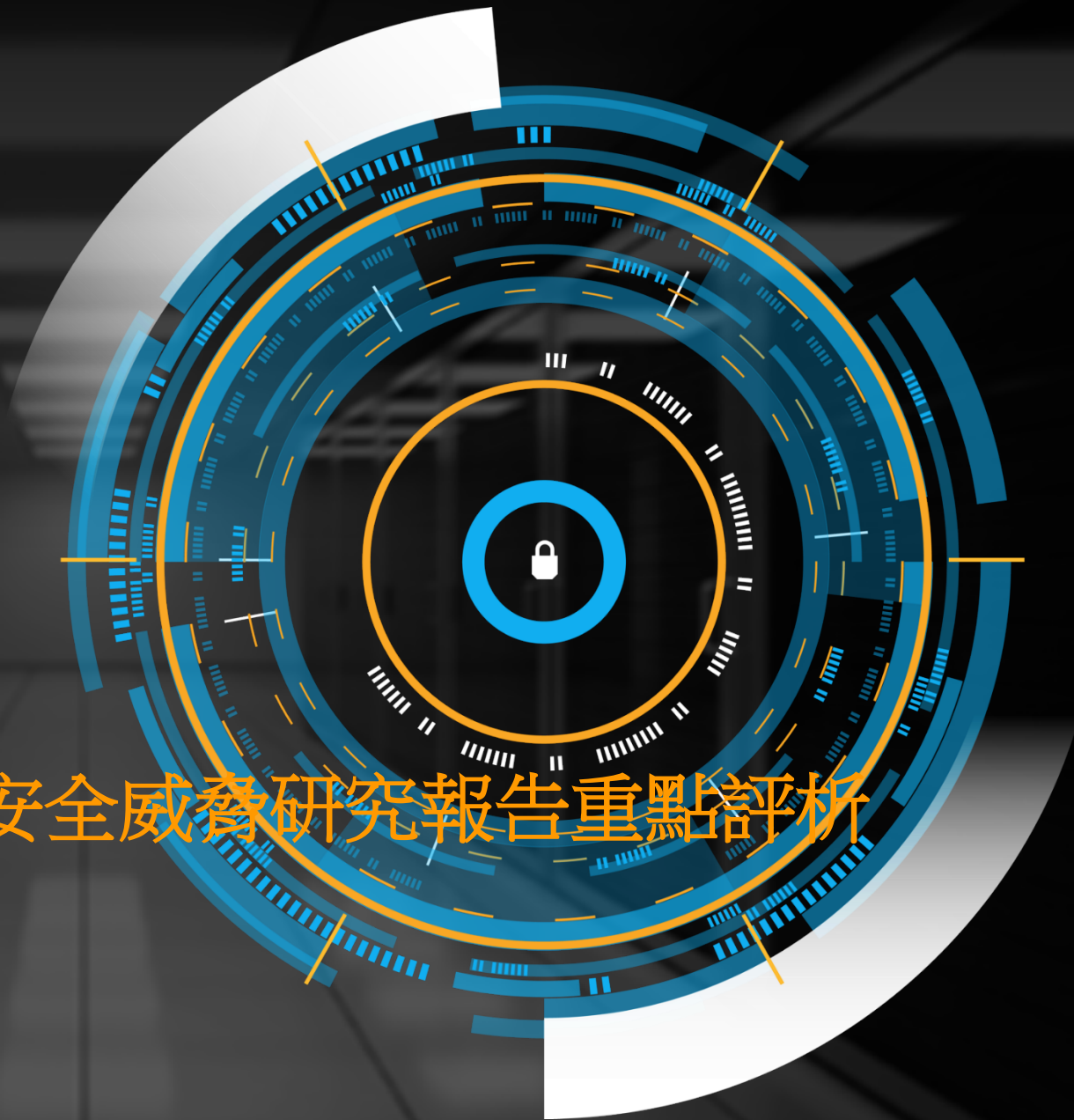




ISTR

Internet Security Threat Report



最新-第 21 期賽門鐵克網路安全威脅研究報告重點評析

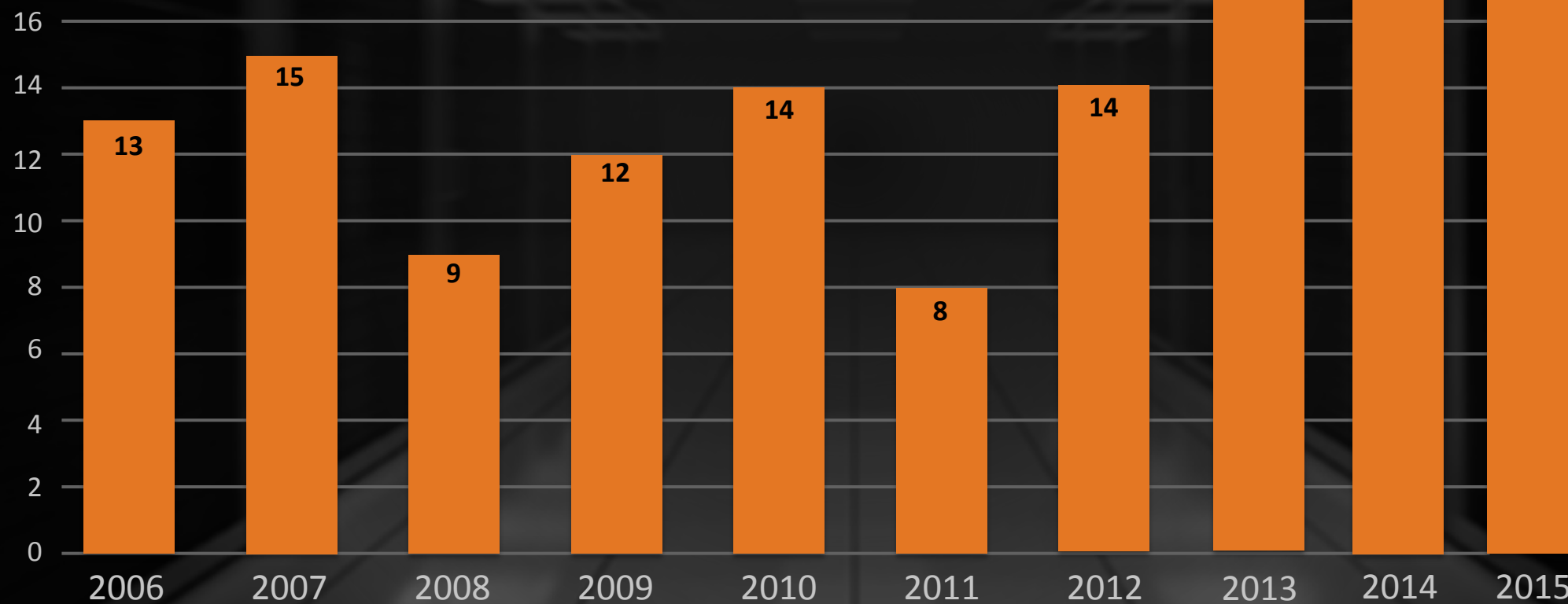
2009年有
2,361,414個
新變種惡意軟體 (每天約:6400)

到了2015 年有
430,555,582個

每天有
1,179,000個
新變種惡意軟體

零時差漏洞

零時差漏洞



54

前五大被駭客利用的零時差漏洞

排名	軟體	2014	排名	軟體	2015
1	Microsoft ActiveX Control CVE-2013-7331	81%	1	Adobe Flash Player CVE-2015-0313	81%
2	Microsoft Internet Explorer CVE-2014-0322	10%	2	Adobe Flash Player CVE-2015-5119	14%
3	Adobe Flash Player CVE-2014-0515	7%	3	Adobe Flash Player CVE-2015-5122	5%
4	Adobe Flash Player CVE-2014-0497	2%	4	Heap-Based Buffer Overflow aka 'Ghost' CVE-2015-0235	<1%
5	Microsoft Windows CVE-2014-4114 OLE	<1%	5	Adobe Flash Player CVE-2015-3113	<1%

Hacking Team也被駭

- Hacking Team (HT) 在Adobe Flash, Internet Explorer and Microsoft Windows都存在零時差漏洞

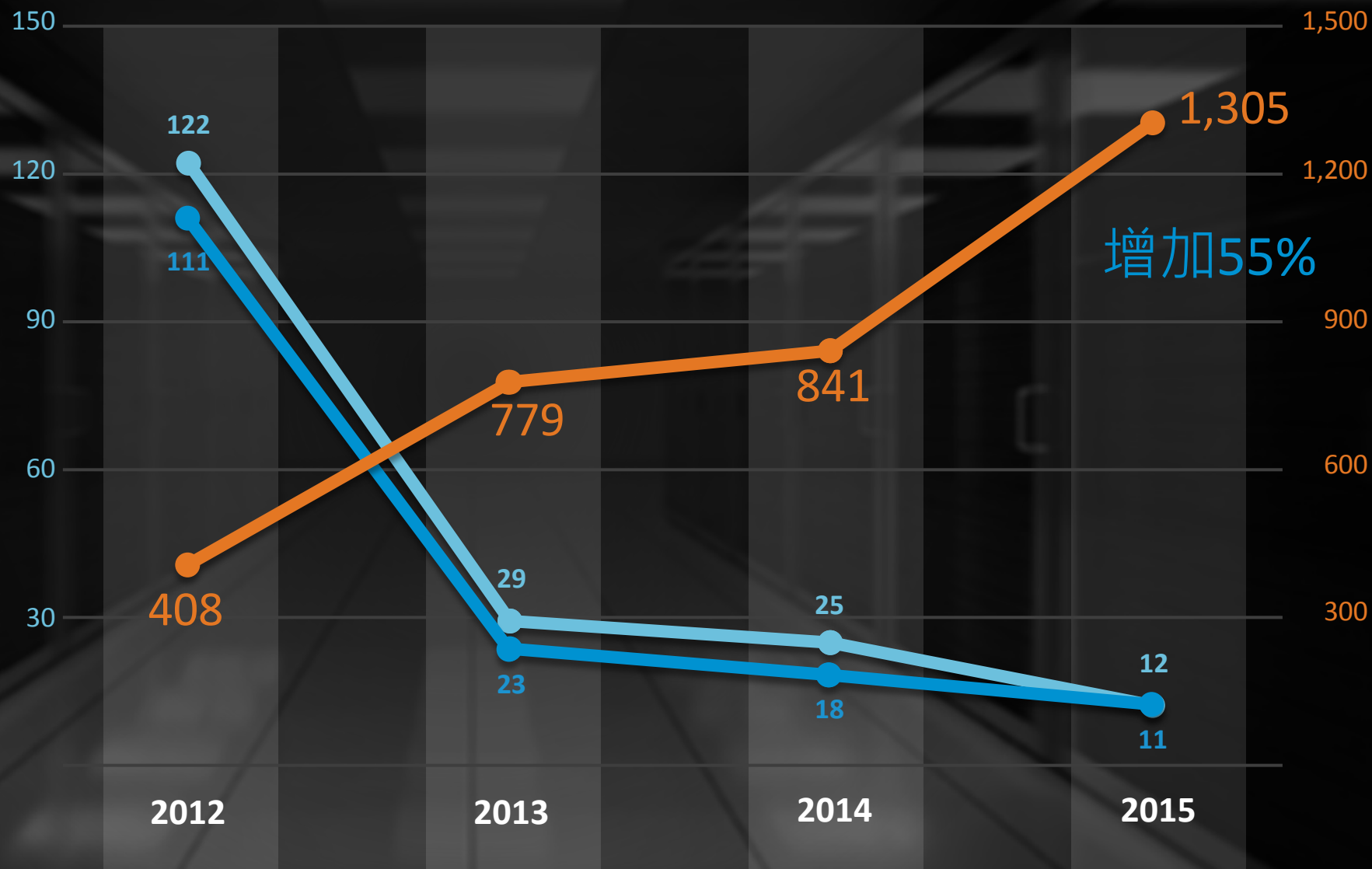
CVE	受影響的產品	第一次通報	修補日期
CVE-2015-5119	Adobe Flash	July 7	July 8
CVE-2015-5122	Adobe Flash	July 10	July 14
CVE-2015-5123	Adobe Flash	July 10	July 14
CVE-2015-2425	Internet Explorer	July 14	July 14
CVE-2015-2426	Microsoft Windows	July 20	July 20
CVE-2015-2387	Microsoft Windows	July 8	July 14



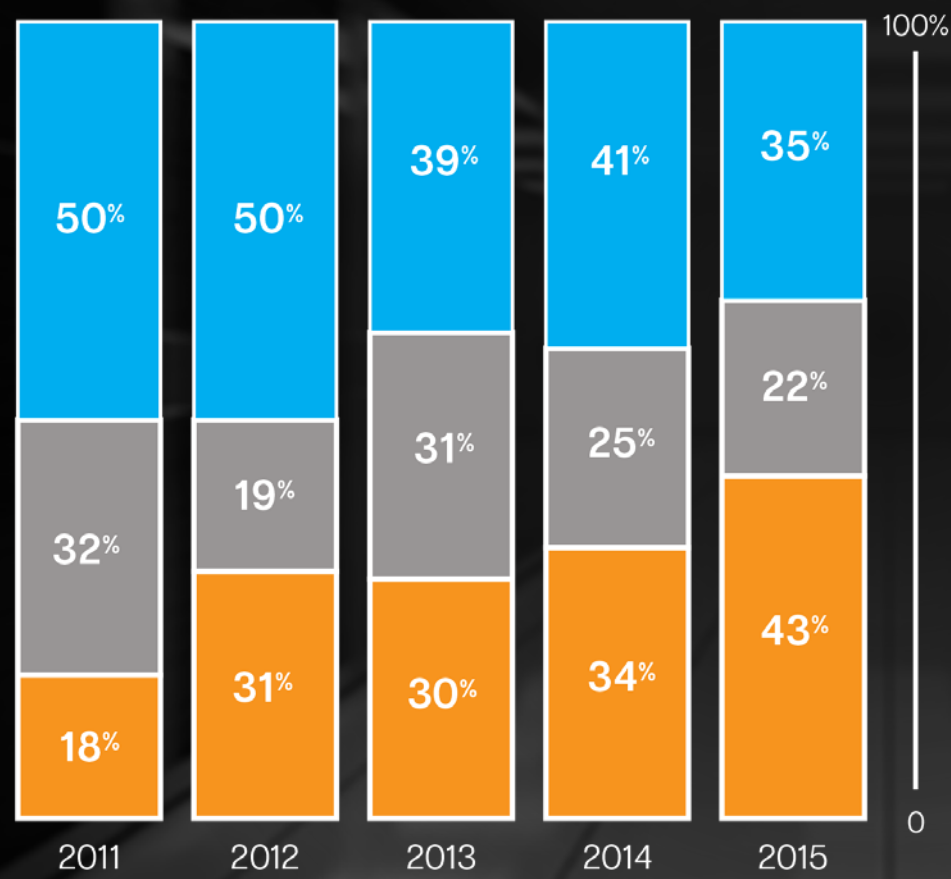
針對式攻擊

針對式攻擊行動

- 平均電子郵件病毒攻擊數目
- 收件者人數
- 針對式攻擊數目



魚叉式網路釣魚攻擊依企業規模而不同



企業規模	2015 風險機率	2015 以百分比 顯示風險 機率
超過 2500以上員工 的大企業	1 in 2.7	38%
251-2500 名員工的 中型企業	1 in 6.8	15%
1-250名 員工的 小企業 (SMB)	1 in 40.5	3%

魚叉式網路釣魚攻擊使用檔案型態

Rank	Attachment Type	2015 Overall Percentage	Attachment Type	2014 Overall Percentage
1	.doc	40.4%	.doc	38.7%
2	.exe	16.9%	.exe	22.6%
3	.scr	13.7%	.scr	9.2%
4	.xls	6.2%	.au3	8.2%
5	.bin	5.4%	.jpg	4.6%
6	.js	4.2%	.class	3.4%
7	.class	2.6%	.pdf	3.1%
8	.ace	1.7%	.bin	1.9%
9	.xml	1.6%	.txt	1.4%
10	.rtf	1.4%	.dmp	1.0%

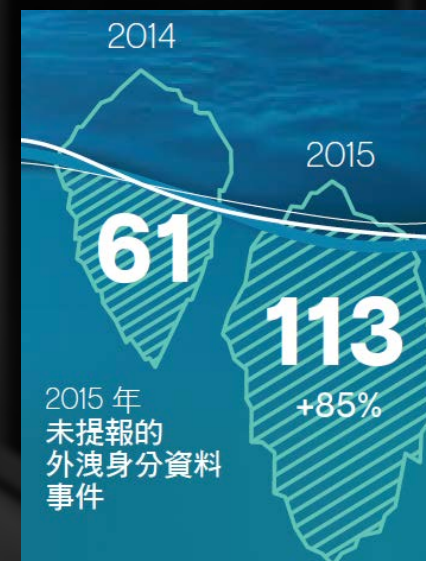
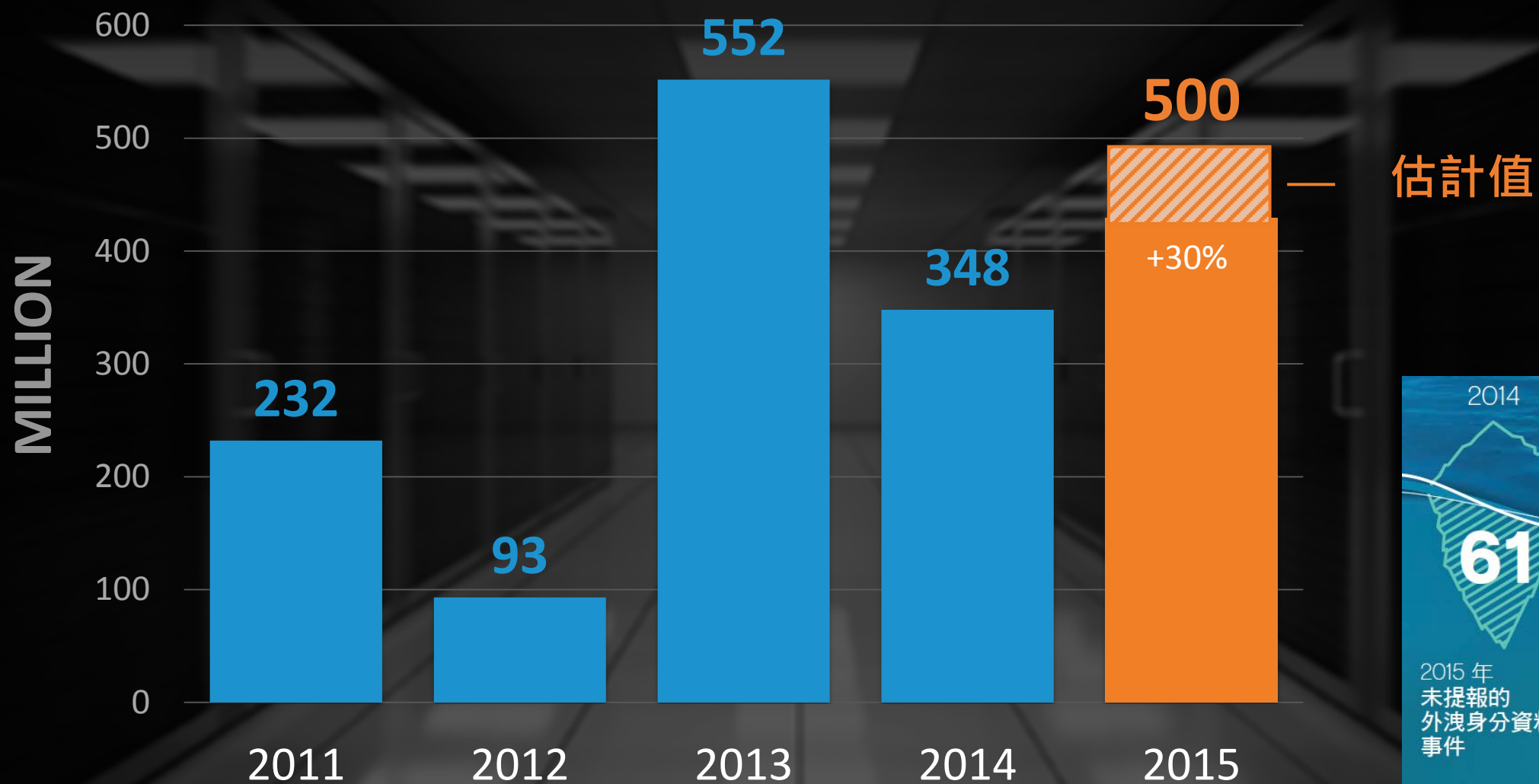
40.4% .DOC
16.9% .EXE

- 反轉字元 (RTLO)：重要報告RCS.TXT →重要報告\0x202ETXT.SCR



資料外洩

個資外洩總數



2015年超級資料外洩



網站漏洞

含有漏洞詐騙網站

Scanned Websites with Vulnerabilities ...

2013
77%
—

2014
76%
-1% pts

2015
78%
+2% pts



... Percentage of Which Were Critical

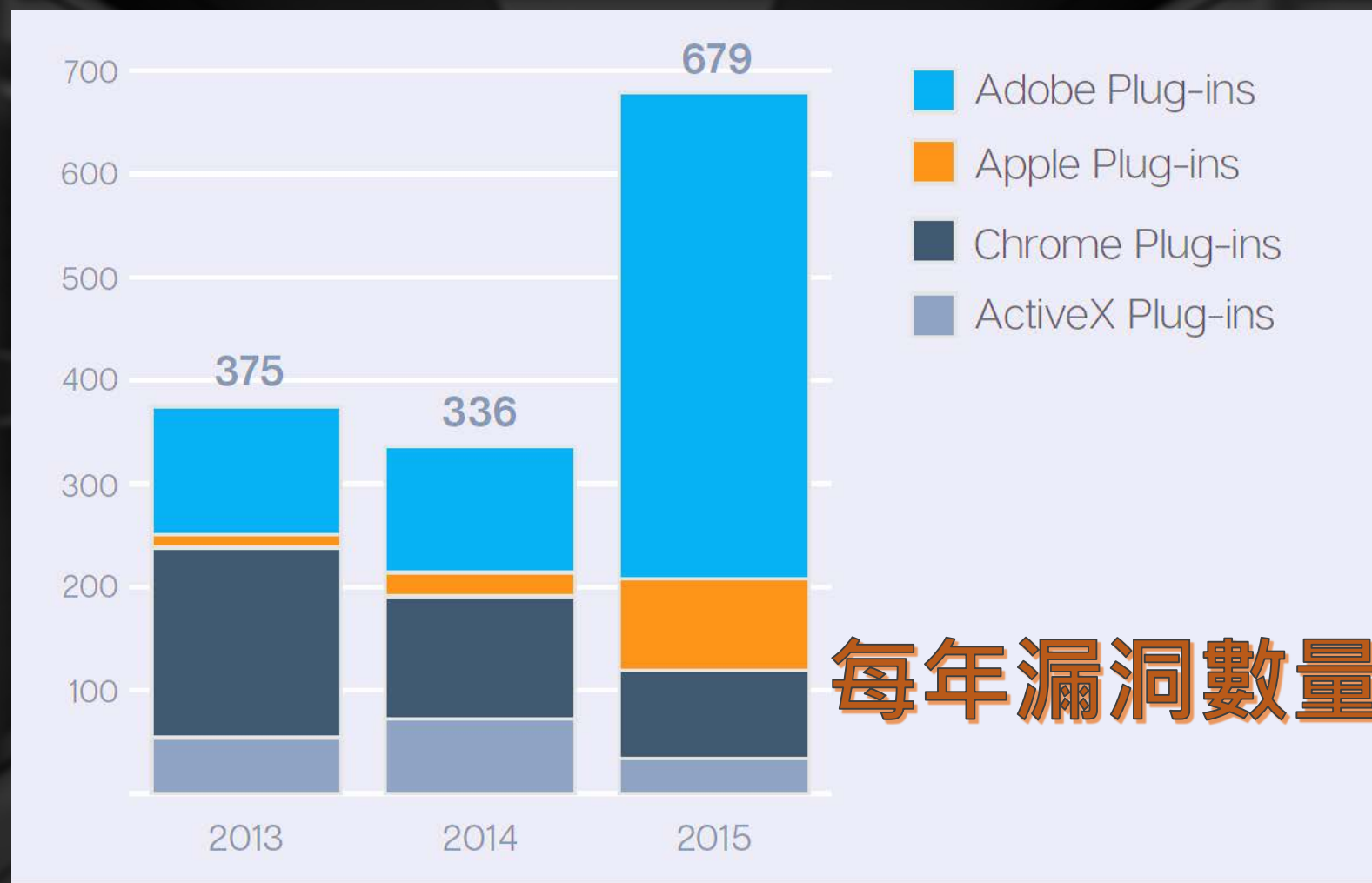
2013
16%
—

2014
20%
+4% pts

2015
15%
-5% pts



瀏覽器外掛程式



每年漏洞數量

誰在意網站漏洞？



美國司法部3/4日公布了一份起訴書，指控七名伊朗駭客攻擊美國在2011-2013年至少四十六間金融機構，以及紐約州的一座水壩，造成的財務損失高達數千萬美元

他們在意！

駭客宣稱使用DDoS惡意程式攻擊

駭客在網路上掃描未使用更新“網站管理系統”的伺服器並建立殭屍網路。這些漏洞讓駭客得以在受影響的伺服器上植入惡意程式。

Discovered: January 10, 2013
Updated: January 10, 2013 1:00:19 PM
Type: Trojan
Infection Length: 4,096 Bytes
Systems Affected: Linux



PHP.Brobot is a PHP Trojan horse that allows a remote attacker to use a compromised computer, hosting a Web server, to launch distributed denial-of-service (DDoS) attacks.

Antivirus Protection Dates

- **Initial Rapid Release version** January 10, 2013 revision 009
- **Latest Rapid Release version** January 10, 2013 revision 009
- **Initial Daily Certified version** January 10, 2013 revision 022
- **Latest Daily Certified version** January 10, 2013 revision 022
- **Initial Weekly Certified release date** January 16, 2013

Click [here](#) for a more detailed description of Rapid Release and Daily Certified virus definitions.

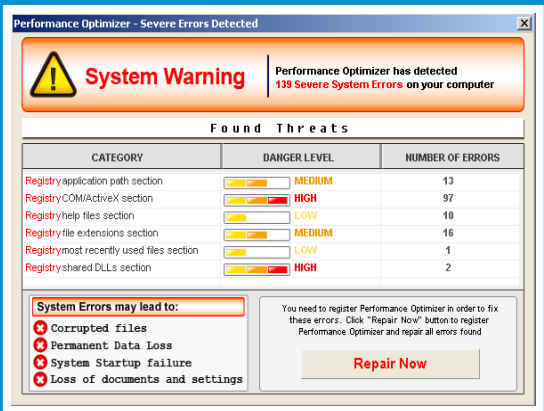
Writeup By: Andrea Lelli

[Summary](#) | [Technical Details](#) | [Removal](#)

勒索軟體

發展進程

MISLEADING APP



2005-2009

“修正”

FAKE AV



2010-2011

“清除”

LOCKER RANSOMWARE



2012-2013

“罰金”

CRYPTO RANSOMWARE



2014-2015

“贖金”

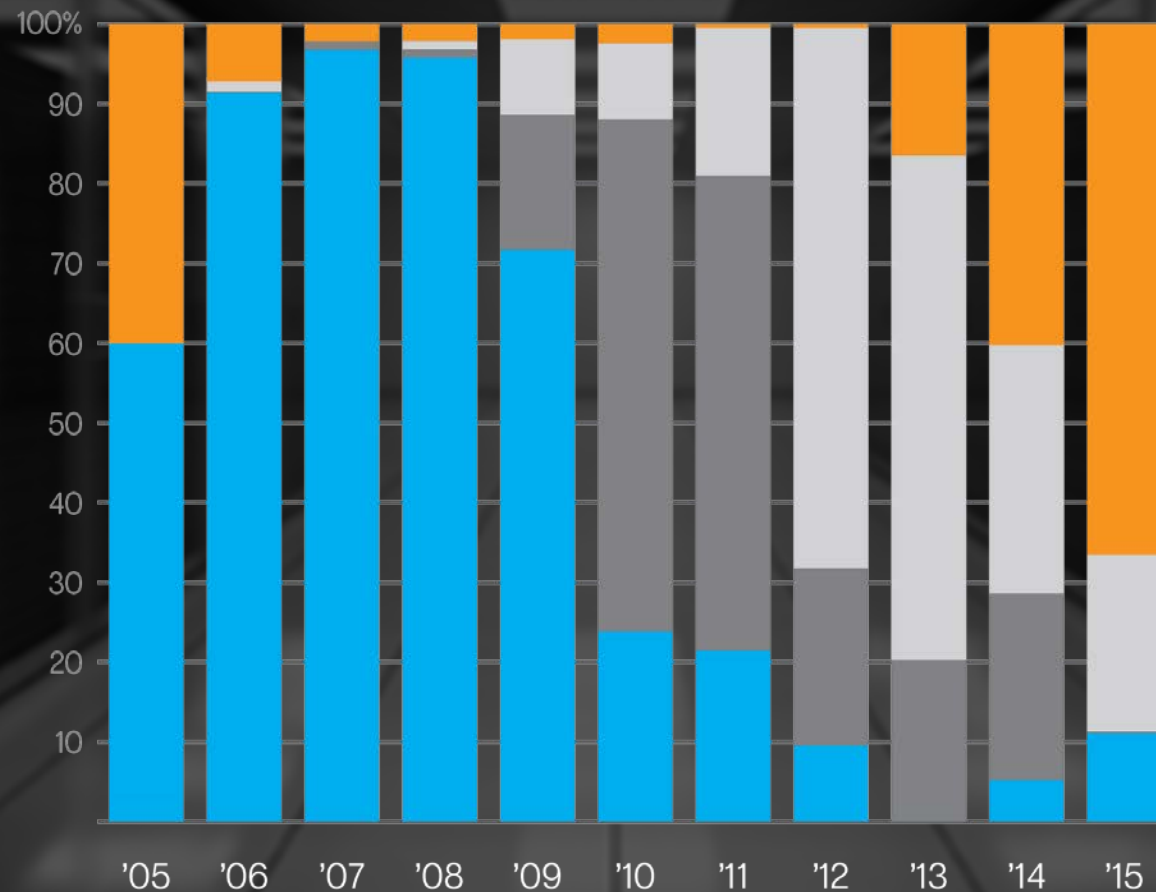
加密勒索軟體漸成主流

MISLEADING APP

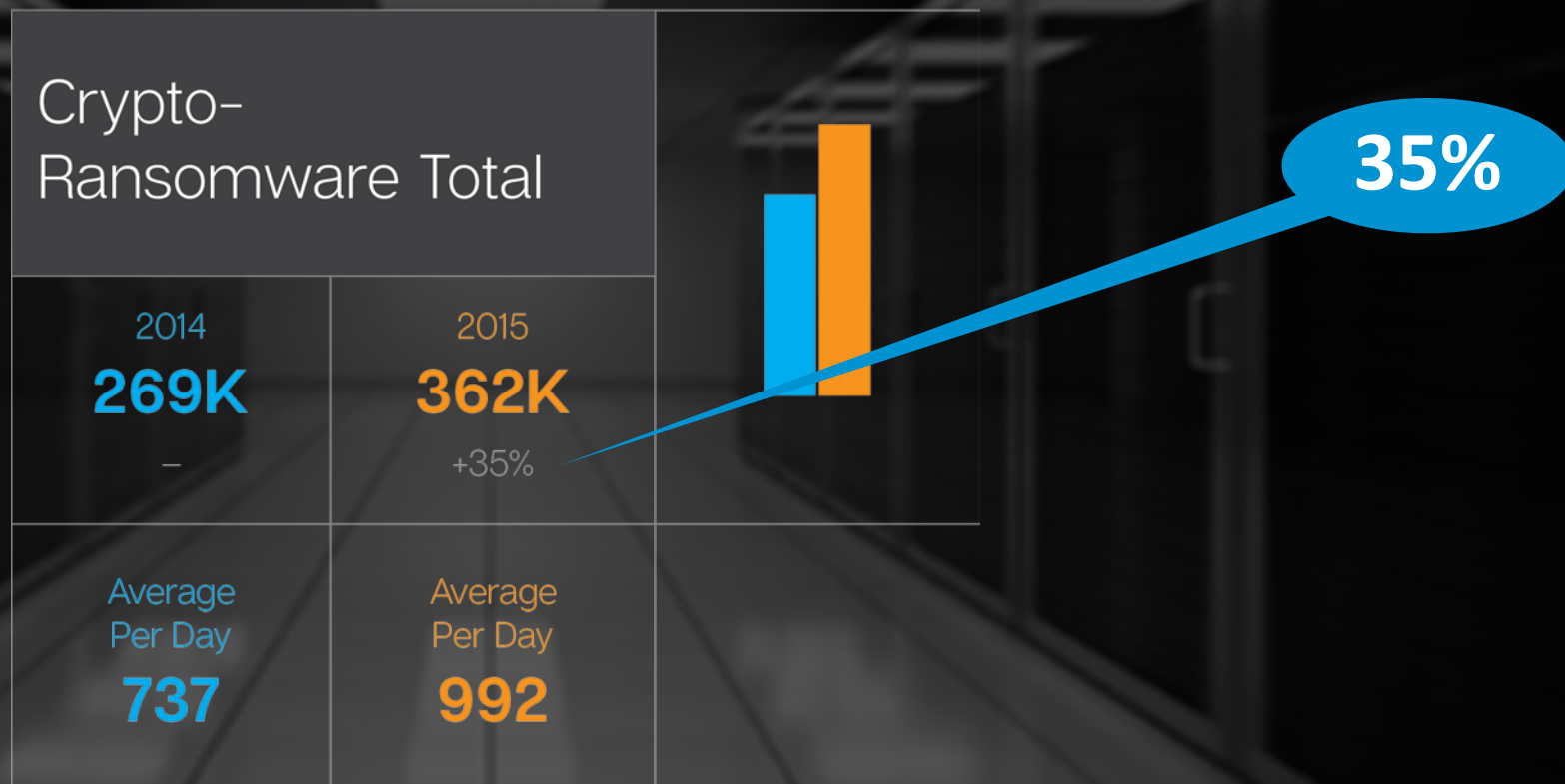
FAKE AV

LOCKER RANSOMWARE

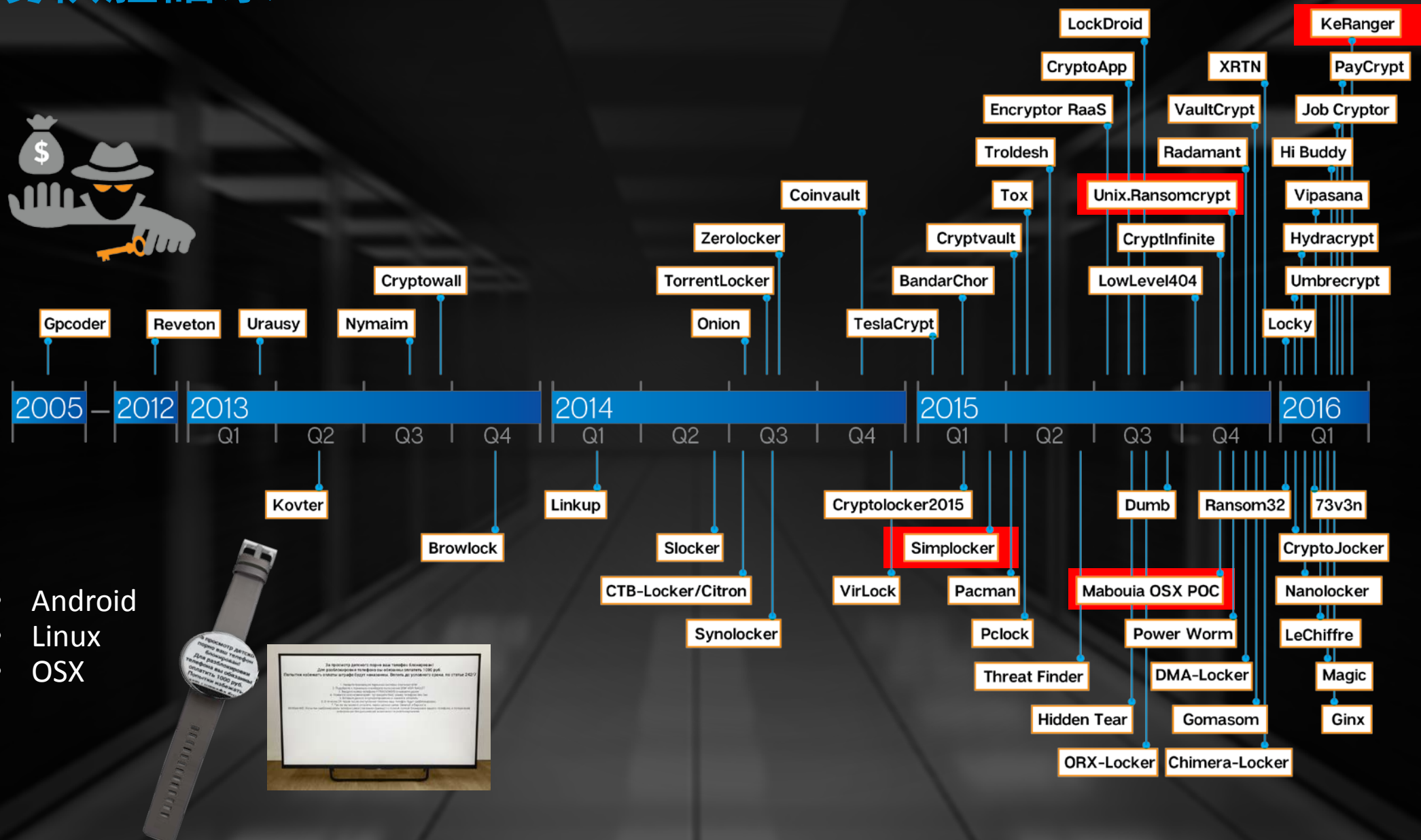
CRYPTO RANSOMWARE



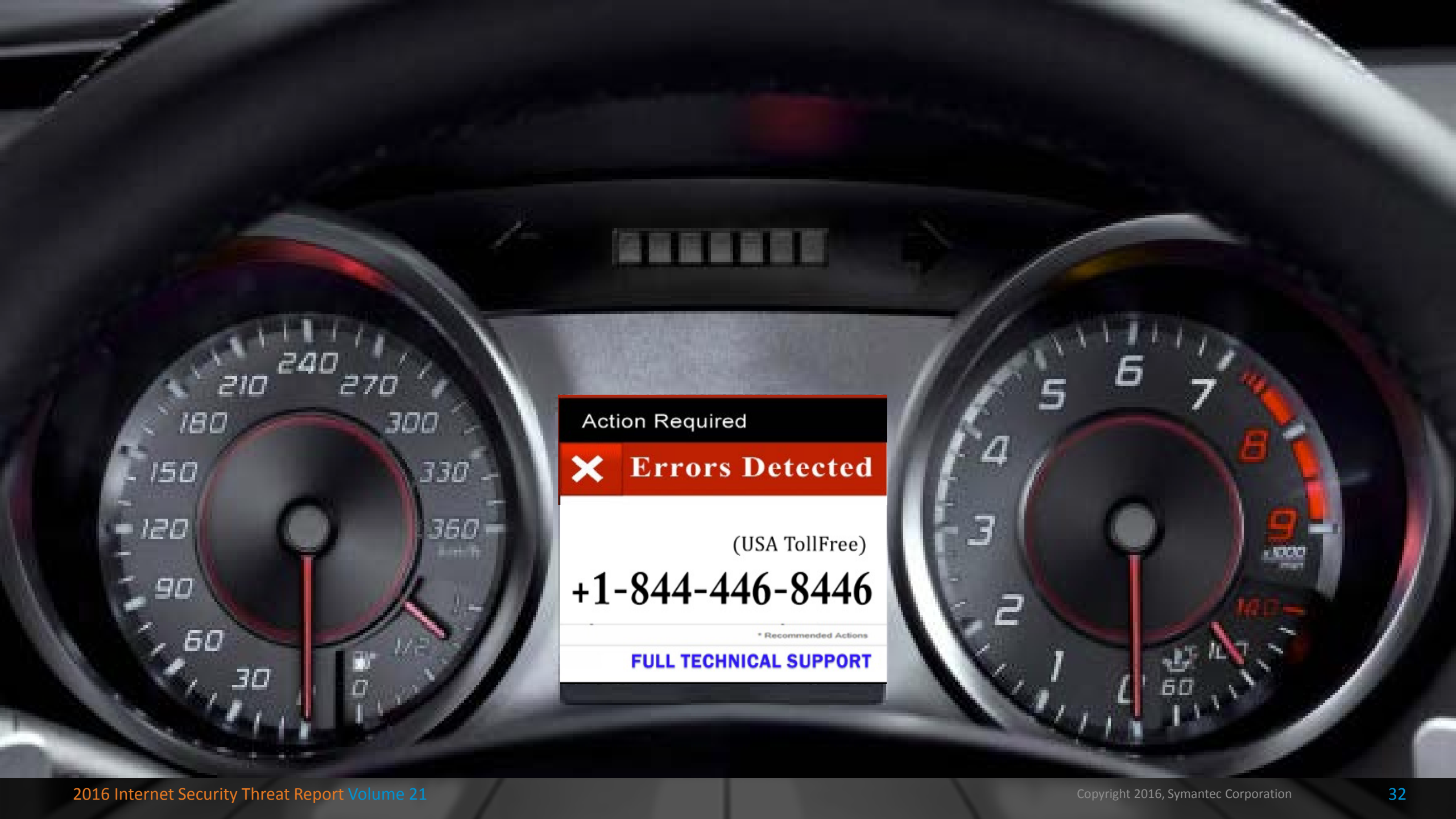
加密勒索軟體攻擊增加35%



勒索軟體譜系







Action Required

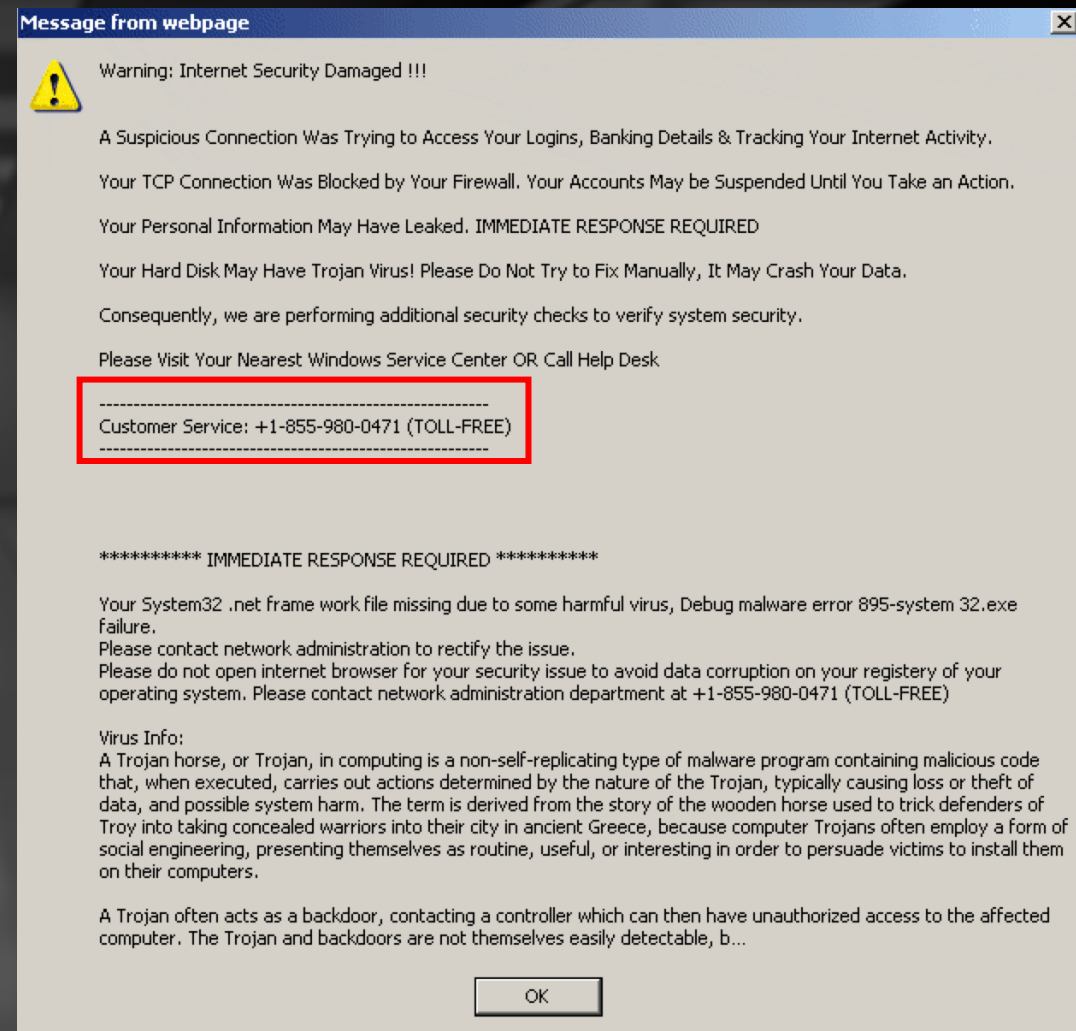
✖ Errors Detected

(USA TollFree)

+1-844-446-8446

* Recommended Actions

FULL TECHNICAL SUPPORT



賽門鐵克安全應變中心早有警告

Security Response Blog

 Symantec Official Blog

Technical Support Phone Scams

By: **Orla Cox**  SYMANTEC EMPLOYEE

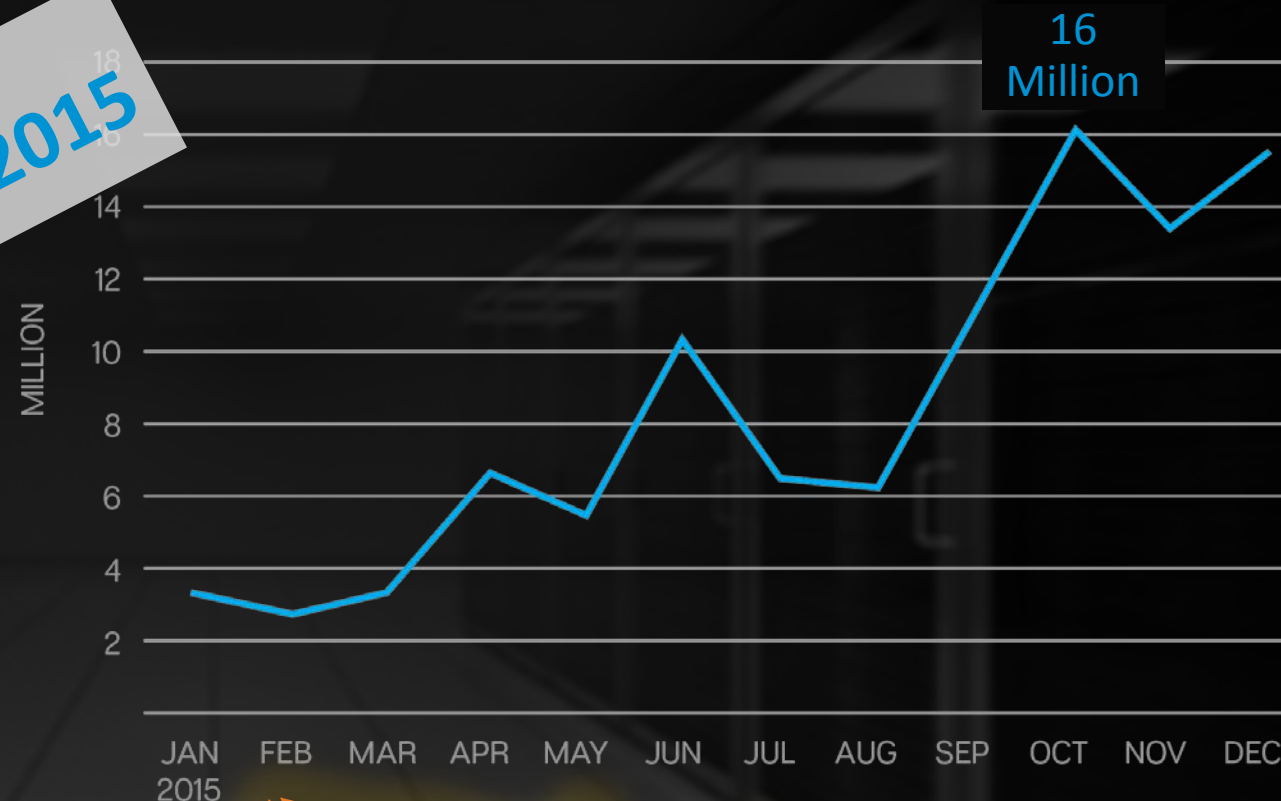
Created 22 Jun 2010

專業詐騙技術客服中心快速增加

100 MILLION BLOCKED in 2015



The screenshot shows a scam call interface. At the top, it says 'Action Required'. Below that, a red banner with a white 'X' icon and the text 'Errors Detected'. Underneath, it says '(USA TollFree)' and displays the phone number '+1-844-446-8446'. At the bottom, it says '* Recommended Actions' and 'FULL TECHNICAL SUPPORT'.



**3 COUNTRIES
MOST AFFECTED:**



USA



CANADA



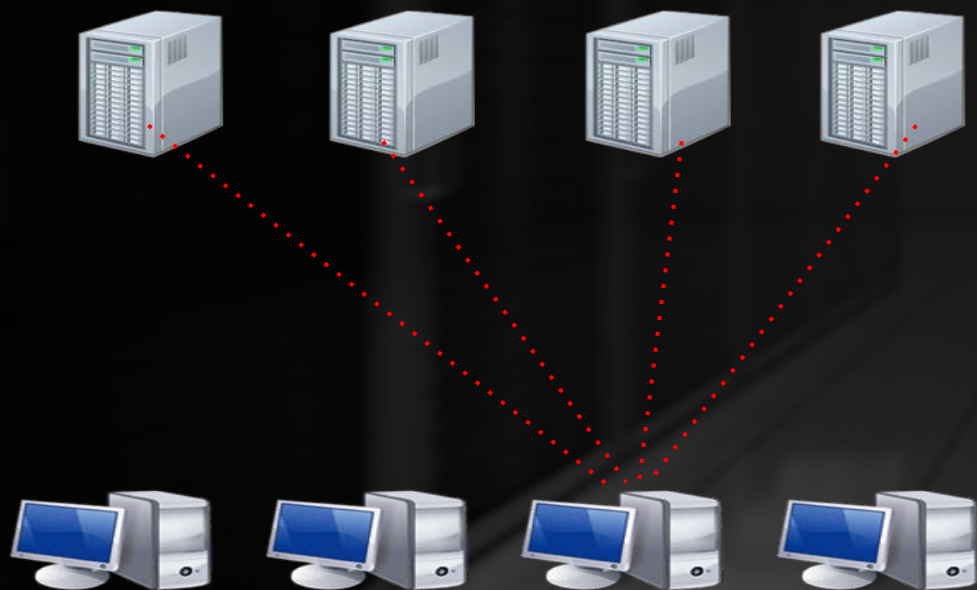
UK

網路犯罪專業化

專業化駭客組織

- Emissary Panda(使者熊貓):中國的駭客組織，專門針對外交官攻擊，收集政府，國防，和高科技數據。值得注意該組織經常透過零時差漏洞(CVE-2015-5119)
- Waterbug: 疑似為俄羅斯APT駭客組織，該組織因其不斷演進的惡意軟體工具包含：魚叉式網絡釣魚與水坑式攻擊。而攻擊對象主要以政府單位為主
- **Butterfly**:對數十億美元的公司攻擊在 IT，醫藥，日用品，包括 Facebook 和蘋果等財經內幕交易

Butterfly – 攻擊工具

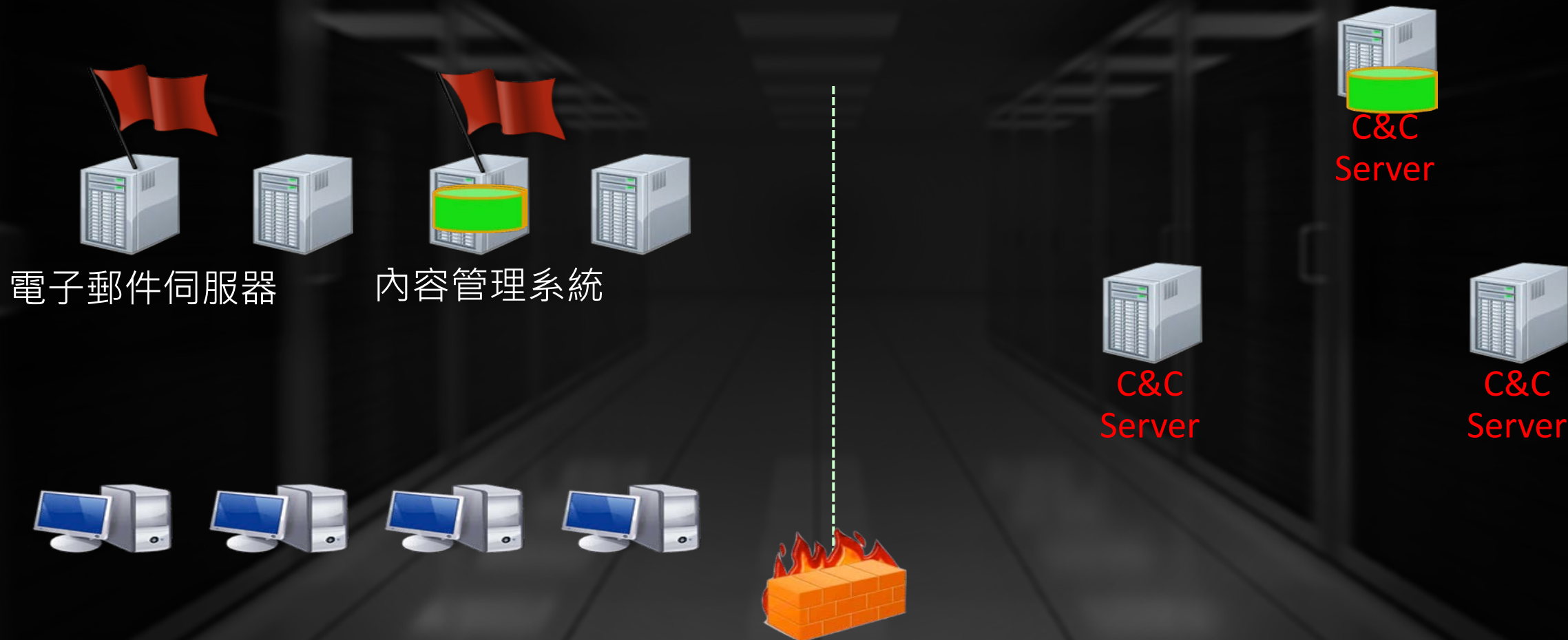


竊取未公開財經資訊超過150,000 筆

- **Hacktool.Bannerjack** – 用以偵測本地有漏洞的伺服器
- **Hacktool.Multipurpose** – 基本的網路列舉，透過編輯日誌、刪除檔案隱藏活動
- **Hacktool.Eventlog** – 編輯活動日誌、丟棄內容，刪除條目。



Butterfly – 指揮控制作法



Butterfly – 指揮控制作法

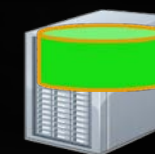


電子郵件伺服器

內容管理系統



- C&C 在虛擬OS運作
- 虛擬OS被加密
- 伺服器日誌已被清除



C&C
Server

Hacktool.MultiPurpose

General options

--install: install server on local host and load it
--host <host>: hostname or IP (local host if not set)
--password <password>: server password connection (mandatory)
--forceload: load server on local host without test

Server options

--cmd: server command:
 dump: dump stuffz
 --sam: fetch LM/NTLM hashes
 --machines: fetch machines hashes
 --history: fetch history for LM/NTLM hashes
 --sh: fetch logon sessions hashes
 --sp: fetch security packages cleartext passwords
 --accounts: <account list>: with --sam, specify accounts to dump
(comma separated)
 --lsa: fetch LSA secrets

Adobe釋出臨時性安全碼補強Flash安全漏洞

- Adobe 在6/23針對零日漏洞緊急釋出臨時性重大安全漏洞 **CVE-2015-3113**
- 一周內，五種知名的攻擊套件已利用此漏洞植入他們的平台

攻擊套件	第一次被發現
Magnitude	June 27, 2015
Angler	June 29, 2015
Nuclear	July 1, 2015
RIG	July 1, 2015
Neutrino	July 1, 2015

科技支援詐騙 – 外地客服中心 (Boiler Rooms) 支援詐騙



先生您好，您的電腦
已遭病毒感染，請購
買75元的維修計劃
Hello sir，讓我們幫
您解決問題。

TeslaCrypt 勒贖軟體 – 提供線上客戶技術支援



T E S L A C R Y P T

All your important files are encrypted.

At the moment, the cost of private key for decrypting your files is 1.5 BTC ≈ 415 USD.
Your Bitcoin address for payment: 1LvjW9wyaipsC3j9RitZDip6cDcZ7jjMG5

PURCHASE PRIVATE KEY
WITH BITCOIN

You can also make a payment with PaySafeCard or Ukash

In case of payment with PaySafeCard or Ukash your total payment is £ 400

PURCHASE PRIVATE KEY
WITH PAYSAFECARD OR UKASH

Payment verification may take up to 12 hours.

Support

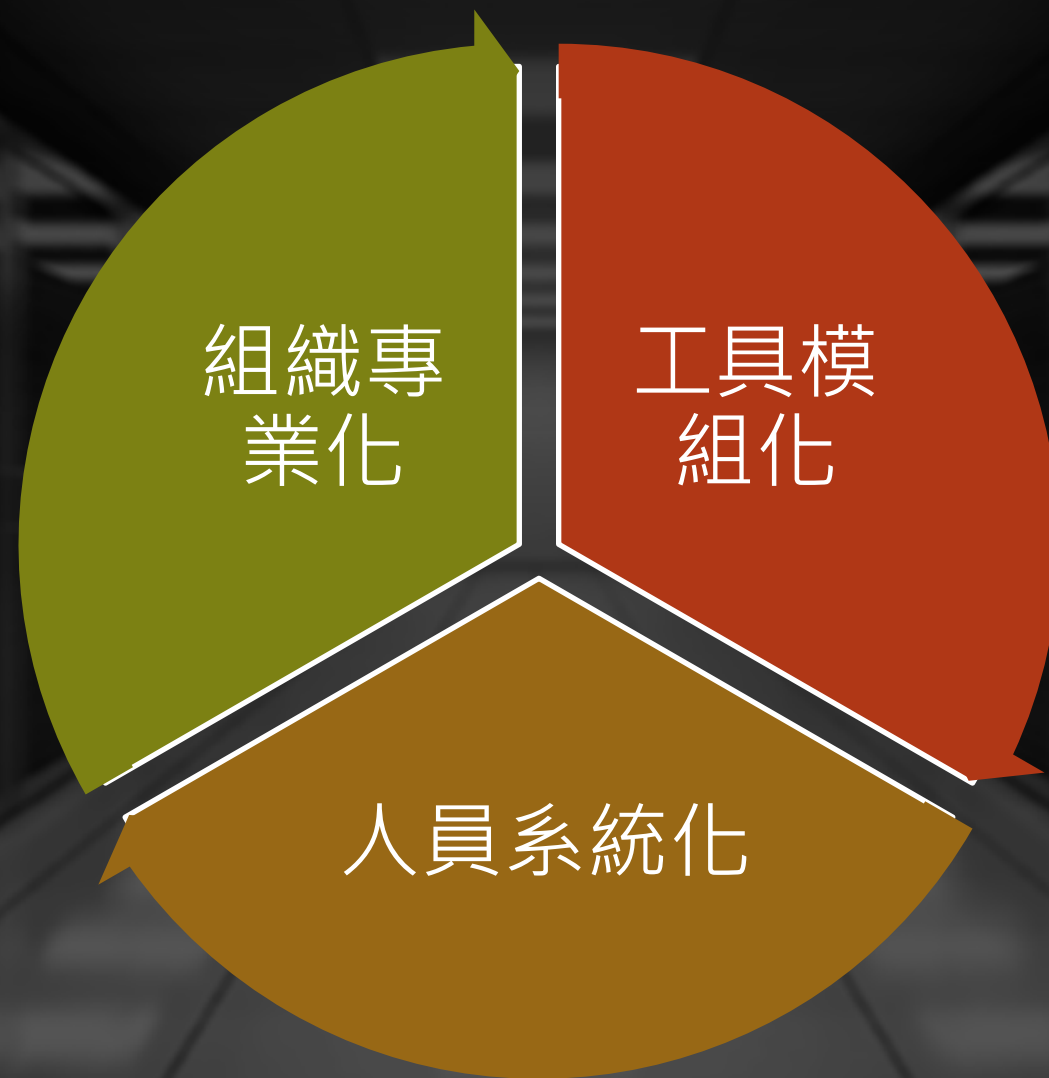
[Message Center](#)

Try to decrypt your file here

You can test the decryption service once for FREE.

Browse...

什麼是網路犯罪專業化



當網路犯罪者已經在客服中心工作

接電話，寫文件，周休二日，

這已經變成一個專業的行業



安全提示和訣竅 – 企業

專家提供的安全提示和訣竅

面對攻擊者的演變，企業和消費者可採取多項措施來保障自己。作為起步點，賽門鐵克建議以下最佳做法：

- **準備充足**：採用進階威脅智慧型解決方案，有助及時發現入侵跡象並快速回應。
- **保持強大的安全態勢**：部署多層端點安全防護、網路安全防護、加密、有效的身份驗證和採用具有聲譽的技術。與安全託管服務供應商合作，增強 IT 團隊的防範能力。
- **作最壞打算**：故障管理確保用戶的安全框架是可測量及可重複，得以優化，而且還可幫助用戶汲取教訓以改善安全部署。用戶亦可考慮與第三方專家合作，強化危機管理。
- **持續提供教育和培訓**：建立指導方針及企業的策略和程式，以保護個人和企業裝置上的敏感資料。定期評估內部調查團隊，進行演習，確保用戶能有效對抗網路威脅。

安全提示和訣竅 – 消費者

- **使用安全密碼**：為帳戶設定獨特及保護性強的密碼。每三個月更改密碼一次，以及切勿重用密碼。此外，考慮使用密碼管理工具進一步保護用戶資料。
- **點擊前想清楚**：開啟錯誤附件可令惡意軟體進入用戶系統。除非是預期會收到的電郵和來自信任的寄件人，否則切勿檢視、開啟或複製電郵附件。
- **保護自身安全**：預防勝於治療。使用防毒軟體、防火牆、瀏覽器保護工具和可靠的網上威脅防護工具等互聯網安全解決方案。
- **慎防恐嚇軟體**：聲稱免費、已破解或盜版的軟件版本可令用戶暴露於惡意的軟體攻擊。社交工程和勒索軟體攻擊使用戶認為其電腦受到感染，並誘騙購買無作用的軟體或直接付款將之移除。
- **保護個人資料**：用戶在網上分享資料會讓自己處於社交工程攻擊的風險。盡量避免在社交網路和網上分享個人資料，包括登入資料、出生日期和寵物名稱等。



Thank you!

保安資訊有限公司 – 賽門鐵克解決方案專家

www.SaveTime.com.tw 好記:幫您節省時間.的公司.在台灣

We Keep Info. Safe , Secure & Save you Time , Cost

Copyright © 2012 Symantec Corporation. All rights reserved. Symantec and the Symantec Logo are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

This document is provided for informational purposes only and is not intended as advertising. All warranties relating to the information in this document, either express or implied, are disclaimed to the maximum extent allowed by law. The information in this document is subject to change without notice.