惡意程式與防毒軟體之爭

伙計

NISRA

教學目的

- 提供同學們資安相關入門知識，並開啟同學們資安研究的興趣

NISRA

要感謝的人太多

那就謝天吧！

NISRA

大綱

- 前言
- 我的電腦中毒了！？
- 什麼是惡意程式？
- 惡意程式的三種躲避偵測原理
- 防毒軟體的三道防禦機制
- 資安相關名詞與工具介紹
- 資安防護的迷思
- 補充：JS木馬簡單分析心得

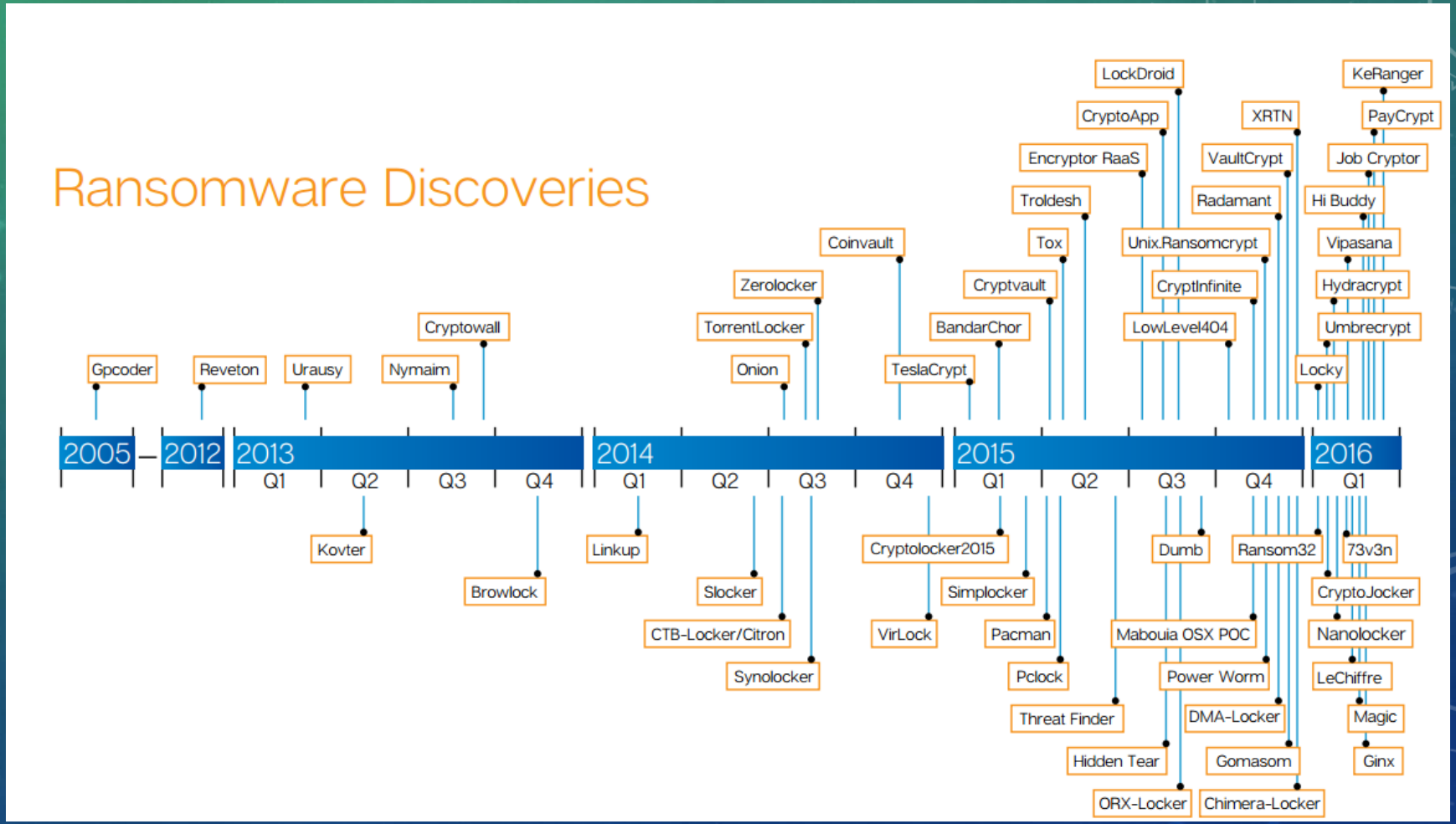
NISRA

前言


CryptoLocker
Your personal files are encrypted!
Private key will be destroyed on
13/10/2013
23:07
Time left
71 : 58 : 09
小心！
史上最狠的勒索軟體
電腦檔案被加密鎖死，
限期3天付9000元，否
則銷毀解鎖密碼！

NISRA

前言


Ransomware Discoveries
2005
2012
2013
2014
2015
2016
Q1
Q2
Q3
Q4
Gpcoder
Reveton
Urausy
Nymaim
Cryptowall
Kovter
Browlock
Zerolocker
TorrentLocker
Onion
Coinvault
TeslaCrypt
Linkup
Slocker
CTB-Locker/Citron
Synolocker
BandarChor
Cryptvault
Tox
Troldesh
Encryptor RaaS
CryptoApp
LockDroid
Cryptolocker2015
VirLock
Simplocker
Pacman
Pclock
Threat Finder
Hidden Tear
ORX-Locker
Unix.Ransomcrypt
CryptInfinite
LowLevel404
Dumb
Mabouia OSX POC
Power Worm
DMA-Locker
Gomasom
Chimera-Locker
VaultCrypt
XRTN
Radamant
Ransom32
KeRanger
PayCrypt
Job Cryptor
Hi Buddy
Vipasana
Hydracrypt
Umbrecrypt
Locky
73v3n
CryptoJocker
Nanolocker
LeChiffre
Magic
Ginx

NISRA

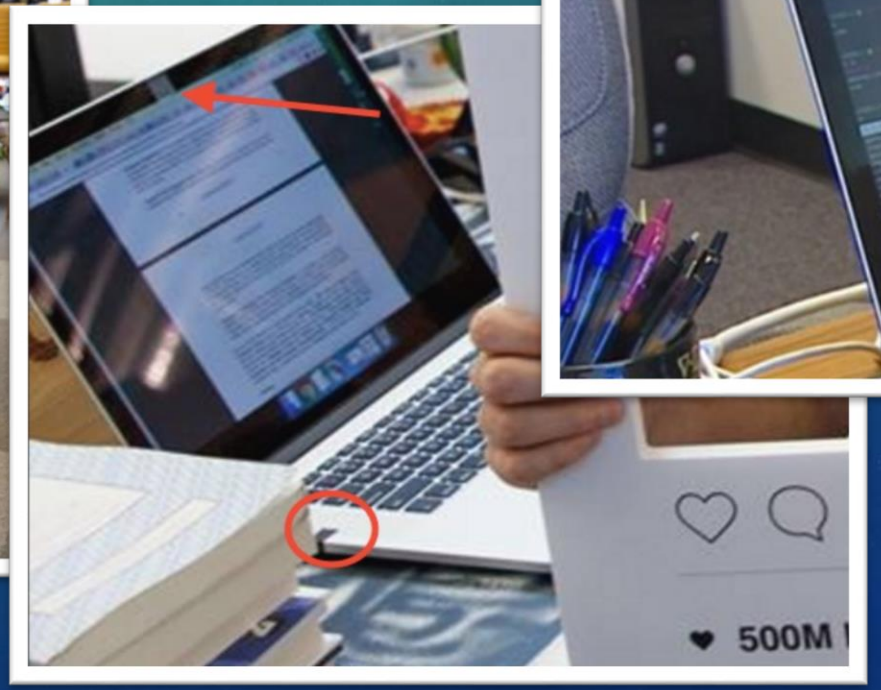
每一個人心中或多或少，都有中毒恐懼症

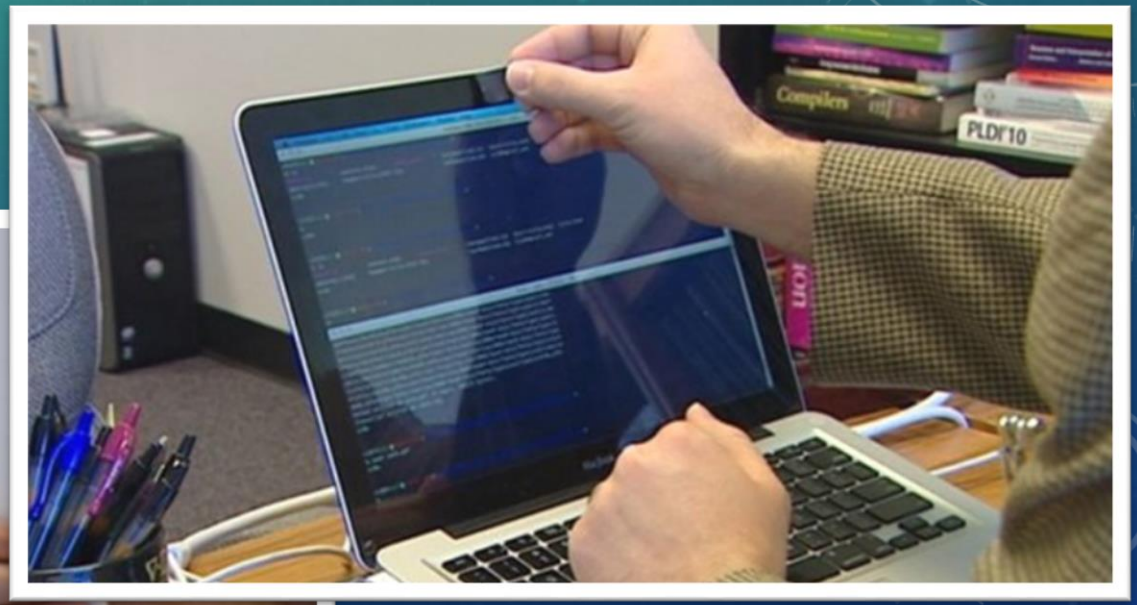
NISRA


avast! be free
AVG
AVIRA
Bitdefender
BullGuard
eset
F-Secure
G DATA
金山网络
KASPERSKY lab
McAfee
An Intel Company
PANDA SECURITY
Norton by Symantec
TREND MICRO
360 www.360.cn

NISRA

不只祖克伯，FBI 局長也在筆電視訊鏡頭貼膠帶防偷窺 [科技新報]





NISRA

敵暗我明，草木皆兵

NISRA

我的電腦中毒了！？

- 電腦速度變慢
- 系統不穩定、常當機
- 出現不明視窗、廣告
- 首頁被綁架
- 防毒軟體跳出警告、或「被」消失
- 出現要求付贖金畫面
- 用起來很正常

NISRA

什麼是惡意程式？

- 影響使用者的電腦
- 影響使用者的資料或財產
- 影響使用者的隱私

安全

NISRA

病毒、特洛伊木馬、蠕蟲

專業術語	基本介紹	感染	散播	影響
木馬	會偷偷傳送使用者資料			
病毒	會感染或破壞使用者檔案			
蠕蟲	會運用漏洞或網路主動散播自己			

NISRA

統稱為「惡意程式」

- 病毒、特洛伊木馬、蠕蟲
- 病毒產生器
- 病毒下載器
- 瀏覽器綁架
- 廣告程式
- 鍵盤側錄器
- 間諜程式等等

NISRA

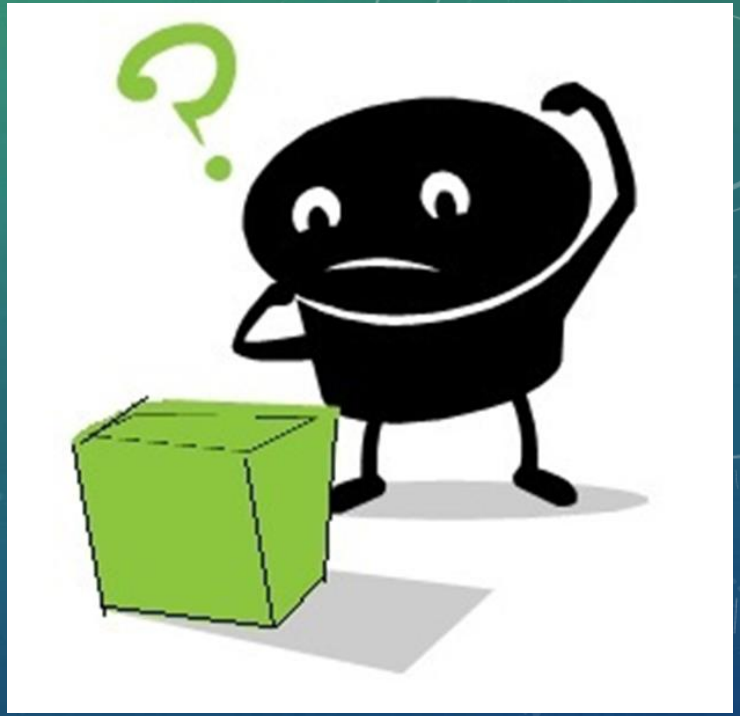
惡意程式常見的三種躲避偵測方法

- 加殼
- 加花
- 去除特徵

NISRA

加殼

- 保護檔案，不被破解
- 加密殼、壓縮殼
- 外殼程式包裹著被保護的程式
- 防毒軟體無法辨識內容物
- 常見加殼軟體—UPX、ASPACK



NISRA

加花

- 程式碼中塞入無意義的指令
- 影響防毒軟體的偵測與工程師的分析

```
mov ebp,esp
push ebp      ;把基址指针寄存器压入堆栈
pop ebp           ;把基址指针寄存器弹出堆栈
push eax          ;把数据寄存器压入堆栈
pop eax           ;把数据寄存器弹出堆栈
nop               ;不执行
add esp,1         ;指针寄存器加1
sub esp,1         ;指针寄存器减1
inc ecx           ;计数器加1
dec ecx           ;计数器减1
sub esp,1         ;指针寄存器加1
sub esp,-1        ;指针寄存器加-1
push 321BA        ;跳到内存入口地址321BA
retn              ;反回到入口地址
jb 456CD          ;跳到内存入口地址456CD
jnb 321BA         ;跳到内存入口地址321BA
```

NISRA

加花

- 程式碼中塞入無意義的指令
- 影響防毒軟體的偵測與工程師的分析

題目：我的夢想

第一行：請從第四行開始閱讀

第二行：請到第412行開始閱讀

第三行：請從第五行開始閱讀

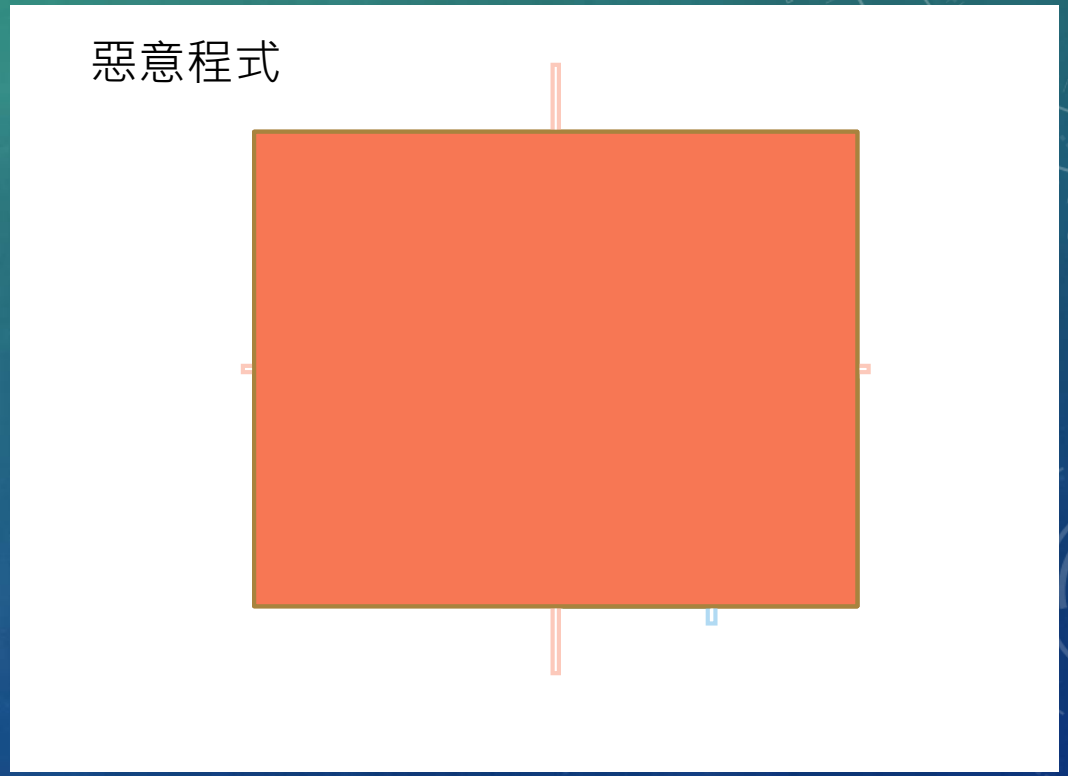
第四行：請到$1+1+\sin 90°$行開始閱讀

第五行：我夢想每天睡到自然...

NISRA

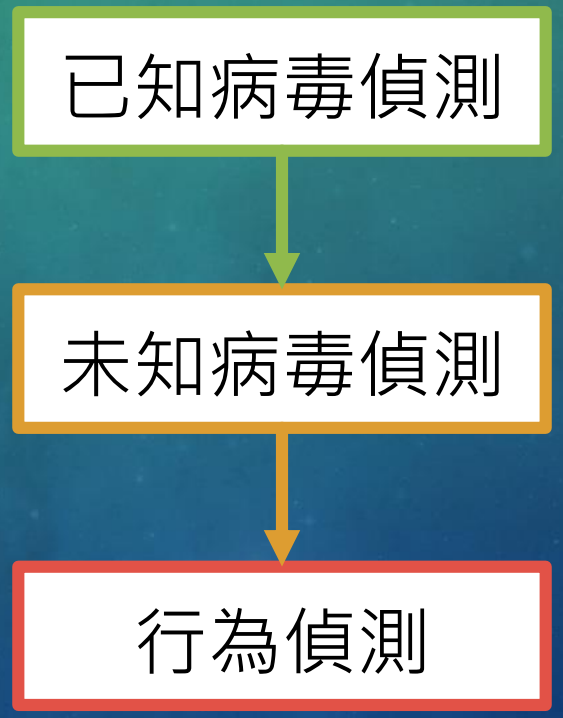
去除特徵

- 修改被防毒廠商定義為特徵的程式碼
- 針對特定防毒軟體來達成免殺
- 免殺能力強



NISRA

防毒軟體的三道防禦機制



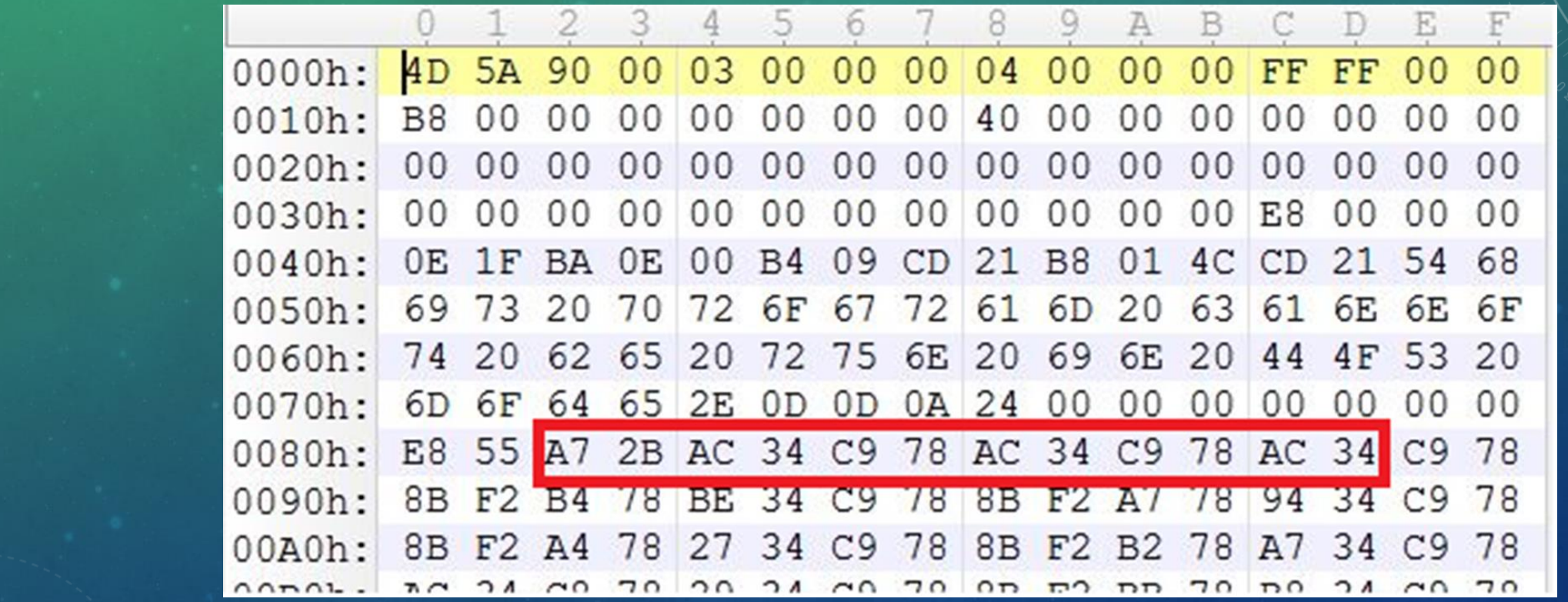
NISRA

已知病毒偵測→病毒碼

- 防毒軟體辨識病毒的基本方法
- 防毒公司會依每個病毒的特徵給予獨一無二的病毒特徵碼
- 不同防毒軟體無法通用

NISRA

已知病毒偵測→病毒碼



	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0000h:	4D	5A	90	00	03	00	00	00	04	00	00	00	FF	FF	00	00
0010h:	B8	00	00	00	00	00	00	00	40	00	00	00	00	00	00	00
0020h:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
0030h:	00	00	00	00	00	00	00	00	00	00	00	00	E8	00	00	00
0040h:	0E	1F	BA	0E	00	B4	09	CD	21	B8	01	4C	CD	21	54	68
0050h:	69	73	20	70	72	6F	67	72	61	6D	20	63	61	6E	6E	6F
0060h:	74	20	62	65	20	72	75	6E	20	69	6E	20	44	4F	53	20
0070h:	6D	6F	64	65	2E	0D	0D	0A	24	00	00	00	00	00	00	00
0080h:	E8	55	A7	2B	AC	34	C9	78	AC	34	C9	78	AC	34	C9	78
0090h:	8B	F2	B4	78	BE	34	C9	78	8B	F2	A7	78	94	34	C9	78
00A0h:	8B	F2	A4	78	27	34	C9	78	8B	F2	B2	78	A7	34	C9	78

NISRA

未知病毒偵測→基因偵測、啟發式偵測

基因偵測

- 現有已知病毒中，尋找共同的特徵，作為基因偵測病毒碼

啟發式掃描

- 啟發式(Heuristic)是指探索和發現的行為過程
- 依靠經驗，並在失敗中不斷學習的過程
- 不倚靠病毒碼來檢測
- 啟發式引擎用本身的規則庫，以靜態分析樣本代碼的方式，來偵測惡意程式

NISRA

基因偵測

- 假設 3A 20 B2 9C 55 FF 08 13 7B 58 1D -> Trojan
- 假設 3A 20 B2 9C 55 FF 08 ->GEN

- BC 15 0C 3A 20 B2 9C 55 FF 08 13 7B 58 1D
- CA 03 14 AA 3A 20 B2 9C 55 FF 08 43 2D FC

NISRA

啟發式掃描

- 修改註冊表
- 對外連線
- 更改系統檔案
- 安裝驅動程式
- 生成新執行檔並執行
- 刪除自己

總分：_____

NISRA

行為偵測→HIPS主動式入侵防禦系統

- hostbased intrusion prevension system
- 現今防毒軟體最終且最重要的防禦技術

- 監控系統程序，阻止異常行為

NISRA


COMODO HIPS
WerFault.exe 正試著存取 iexplore.exe 的記憶體
WerFault.exe
iexplore.exe
WerFault.exe 為安全的應用程式。您可以放心允許本次請求。
允許
允許應用程式執行上述動作
封鎖
封鎖應用程式執行上述動作
視為
讓您選擇規則集來套用
記住我的回答


使用者帳戶控制
您是否要允許下列程式變更這部電腦?
程式名稱: Norton 360
已驗證的發行者: Symantec Corporation
檔案來源: 從網際網路下載
顯示詳細資料(D)
是(Y)
否(N)
變更這些通知顯示的時機

NISRA

防毒軟體的三道防禦機制

NISRA

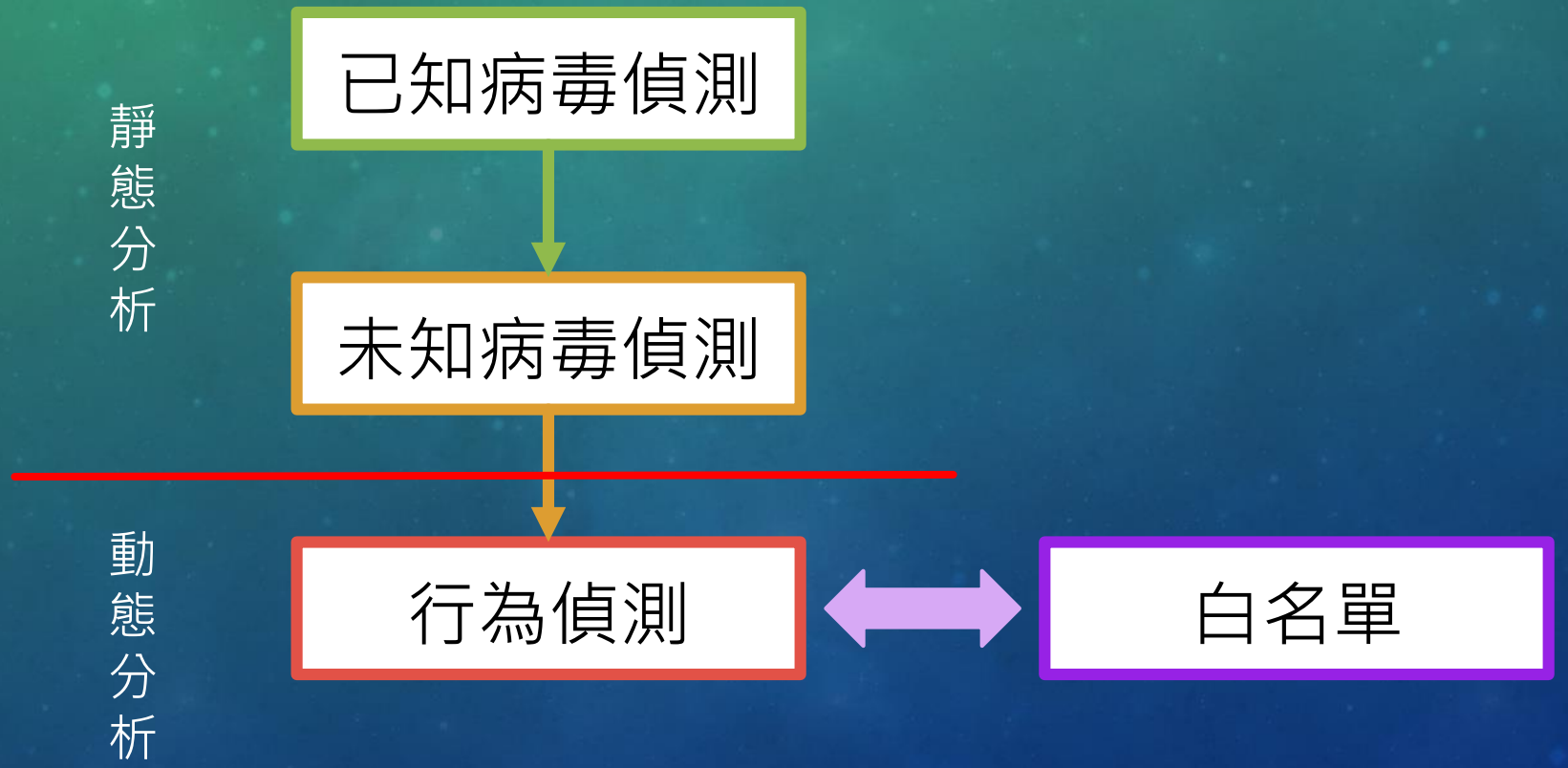
雲端白名單


卡巴斯基網路安全軟體
雲端防護
KASPERSKY
體驗卡巴斯基安全網路進階雲端防護
連線全球使用者的一個安全網路
即時回應最新威脅
即時網站信譽資訊
了解更多
KSN
已連線
目前 KSN 狀態
同步： 2014/2/14 下午 05:15:23
安全項目：
928049866
危險項目：
415402136
正在處理：
139923820
在最近的 24 小時中：
受防護的 KSN 參與者： 2263762
已解毒的威脅： 15314738
KASPERSKY
TRUSTED
我的簡介
設定

NISRA


資源監視器
檔案(F) 監視器(M) 說明(H)
概觀 CPU 記憶體 磁碟 網路
具有網路活動的處理程序
影像 PID 傳送 (B/秒) 接收 (B/秒) 總計 (B/秒)
avp.exe 2748 774,552 1,502,632 2,277,183
Google Photos Backup.exe 11820 774,179 607 774,786
System 4 241 224 465
svchost.exe (NetworkService) 1584 177 20 197

防毒軟體的三道防禦機制



NISRA

資安相關名詞與工具介紹

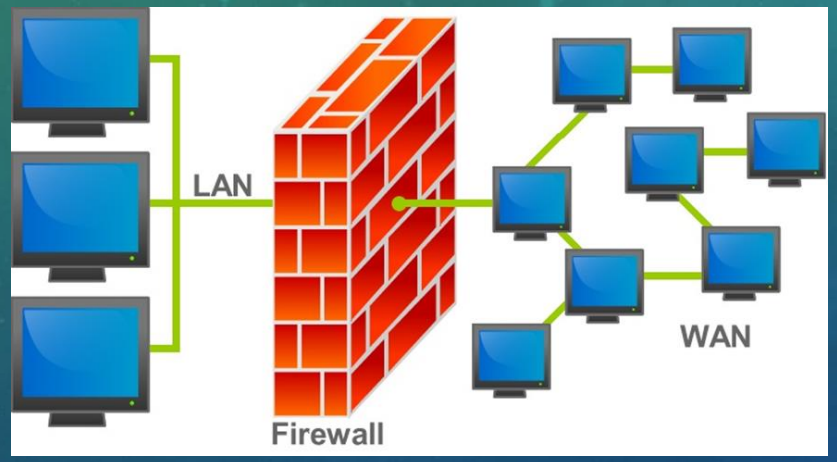
- 防火牆
- 社交工程與網路釣魚
- 假防毒軟體
- Zero Day 漏洞
- 蜜罐

- 沙盤與虛擬機
- AV-TEST
- VirusTotal
- Payload security

NISRA

防火牆

- 隔離網路，過濾網路中傳送的封包



老闆：不是有防火牆嗎？

NISRA

社交工程與網路釣魚

- 獲取使用者信任的欺騙行為
- 假冒客服電話
- 假的好友訊息
- 假的官方郵件
- 假的正常網頁
- www.staysecureonline.com/staying-safe-online

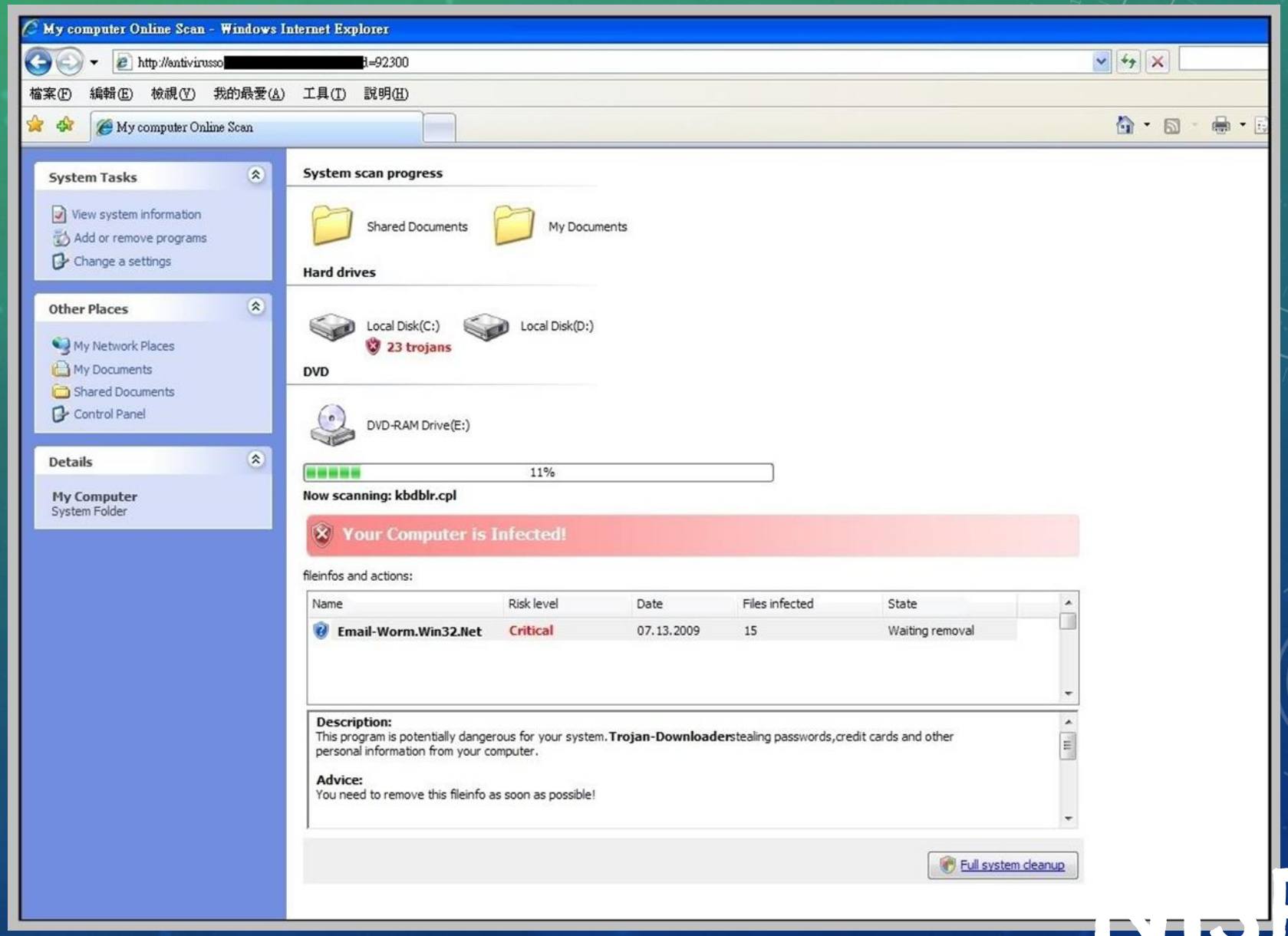
NISRA

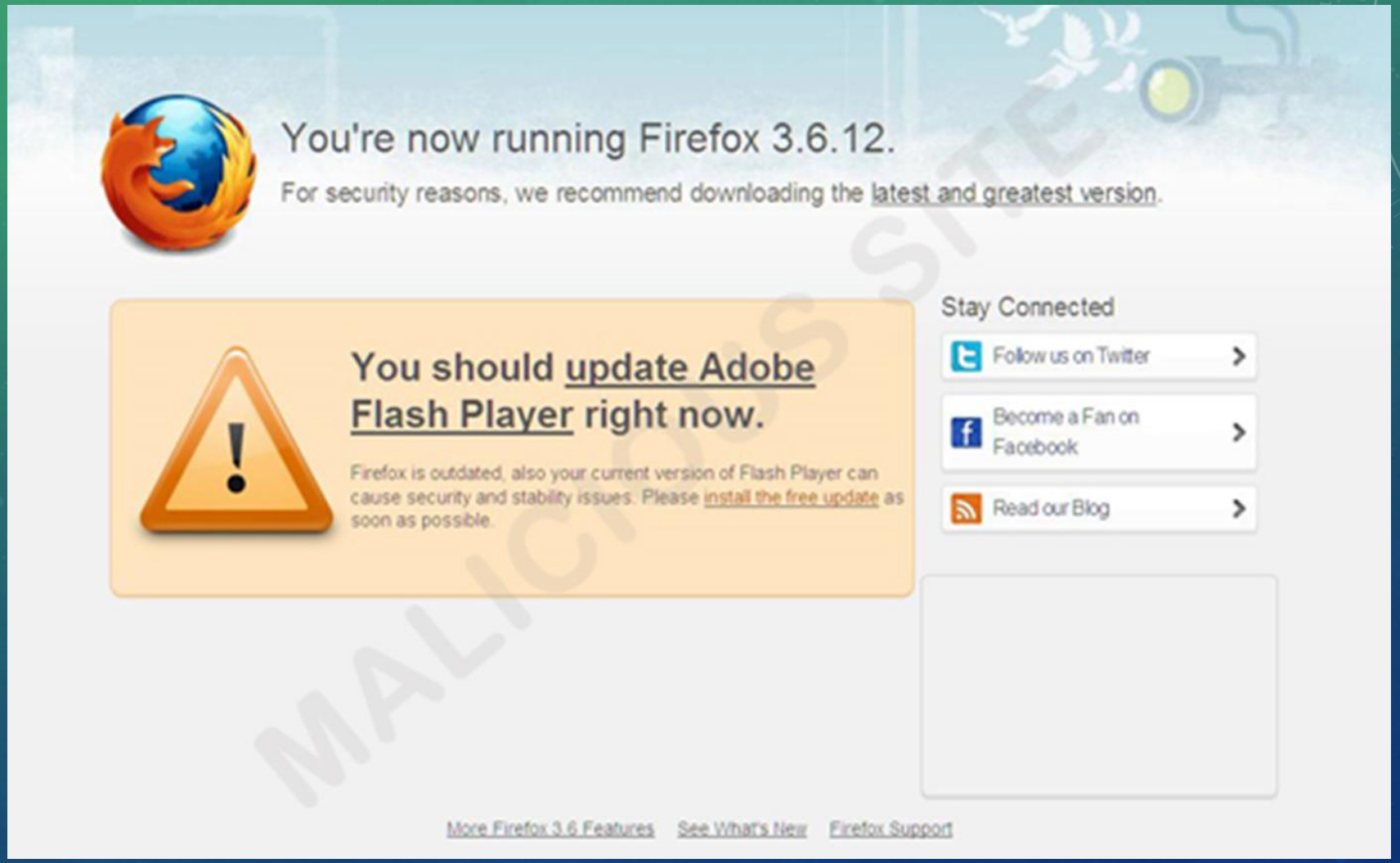
假防毒軟體


Windows Internet Explorer
Warning!!! Your computer contains various signs of viruses and malware programs presence. Your system requires immediate anti viruses check! System Security will perform a quick and free scanning of your PC for viruses and malicious programs.
確定
取消

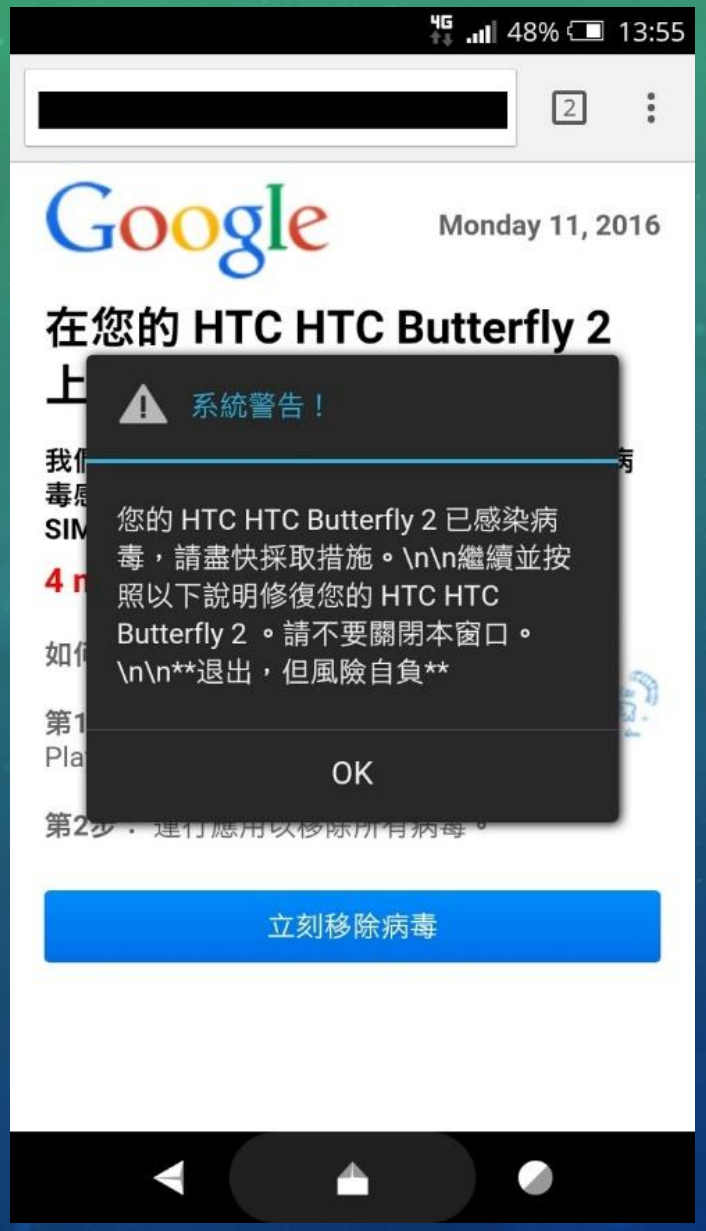
NISRA

假防毒軟體


My computer Online Scan - Windows Internet Explorer
http://antivirusso[redacted]=92300
檔案(F) 編輯(E) 檢視(V) 我的最愛(A) 工具(T) 說明(H)
My computer Online Scan
System Tasks
View system information
Add or remove programs
Change a settings
Other Places
My Network Places
My Documents
Shared Documents
Control Panel
Details
My Computer
System Folder
System scan progress
Shared Documents
My Documents
Hard drives
Local Disk(C:)
23 trojans
Local Disk(D:)
DVD
DVD-RAM Drive(E:)
11%
Now scanning: kbdblr.cpl
Your Computer is Infected!
fileinfos and actions:
Name
Risk level
Date
Files infected
State
Email-Worm.Win32.Net
Critical
07.13.2009
15
Waiting removal
Description:
This program is potentially dangerous for your system. Trojan-Downloaders tealing passwords,credit cards and other personal information from your computer.
Advice:
You need to remove this fileinfo as soon as possible!
Full system cleanup

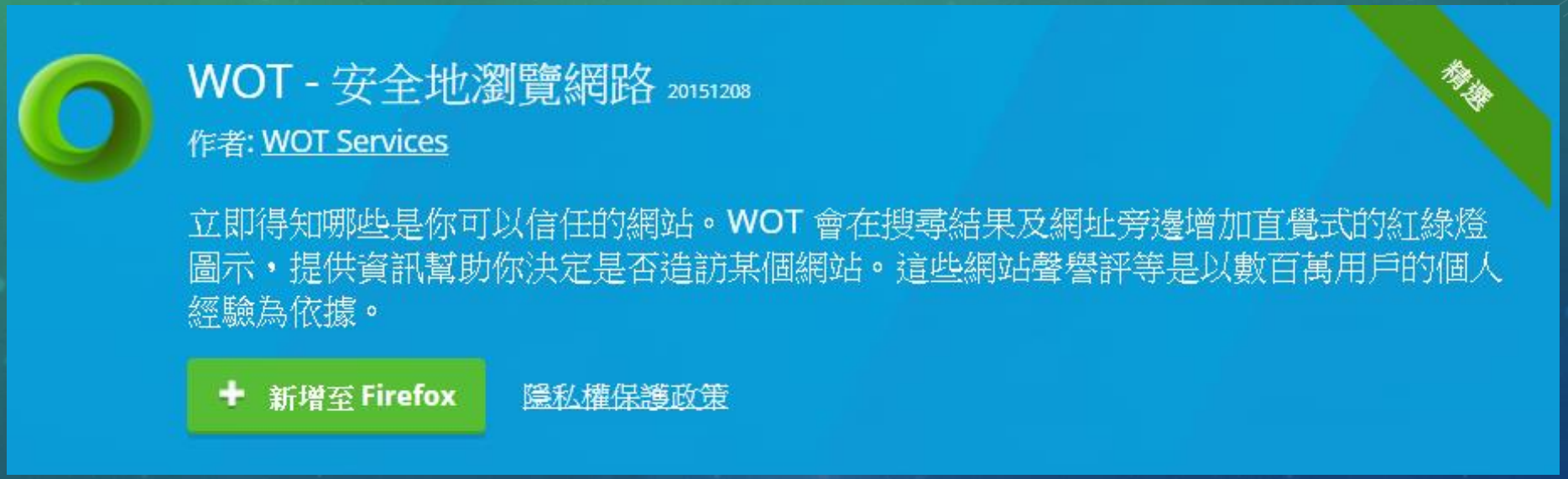

You're now running Firefox 3.6.12.
For security reasons, we recommend downloading the latest and greatest version.
You should update Adobe Flash Player right now.
Firefox is outdated, also your current version of Flash Player can cause security and stability issues. Please install the free update as soon as possible.
Stay Connected
Follow us on Twitter
Become a Fan on Facebook
Read our Blog
More Firefox 3.6 Features
See What's New
Firefox Support

NISRA


48% 13:55
[redacted]
Google
Monday 11, 2016
在您的 HTC HTC Butterfly 2
上
系統警告！
您的 HTC HTC Butterfly 2 已感染病毒，請盡快採取措施。\n\n繼續並按照以下說明修復您的 HTC HTC Butterfly 2 。請不要關閉本窗口。\n\n**退出，但風險自負**
OK
立刻移除病毒

NISRA

NISRA


WOT - 安全地瀏覽網路 20151208
作者: WOT Services
精選
立即得知哪些是你可以信任的網站。WOT 會在搜尋結果及網址旁邊增加直覺式的紅綠燈圖示，提供資訊幫助你決定是否造訪某個網站。這些網站聲譽評等是以數百萬用戶的個人經驗為依據。
新增至 Firefox
隱私權保護政策

NISRA


網站已由 PC-cillin 雲
www.[redacted].com
TREND MICRO 網站已由 PC-cillin 雲端版封鎖
危險網頁
位址： http://www.[redacted].com/
趨勢科技已確認此網站會傳送惡意軟體，或曾經從事過網路詐騙。
請關閉此網頁。
儘管存在危險，仍要開啟此網頁？
版權所有 © 2013 Trend Micro Incorporated/趨勢科技股份有限公司。保留所有權利。

NISRA

ZERO-DAY漏洞（零天漏洞)

- 先前未知、未發現的漏洞

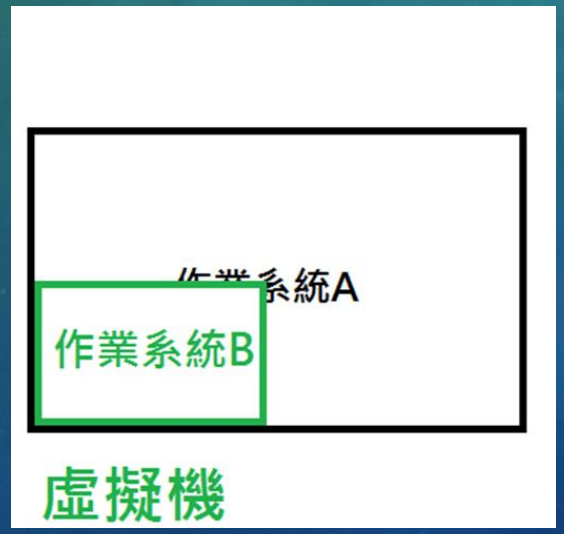
NISRA

蜜罐

- 具有漏洞的主機
- 吸引駭客的入侵
- 紀錄駭客的攻擊方式，並收集惡意程式

虛擬機

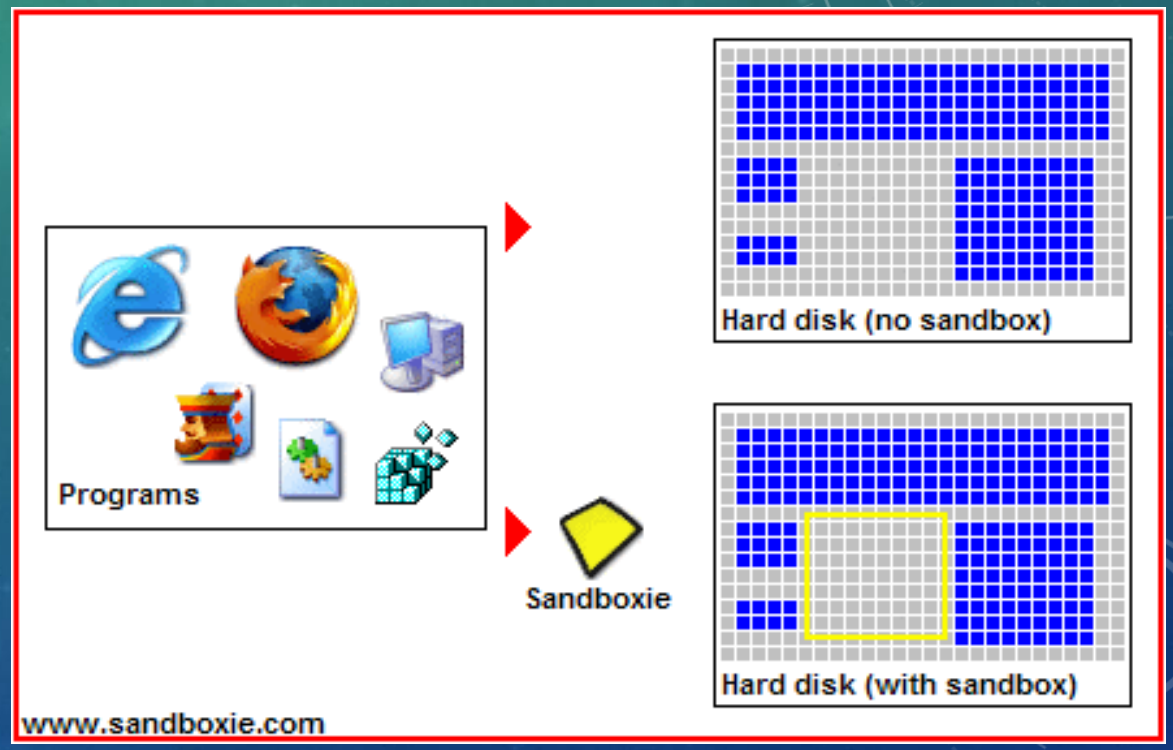
- 在作業系統上另外在模擬一台虛擬電腦，兩者互不影響



NISRA

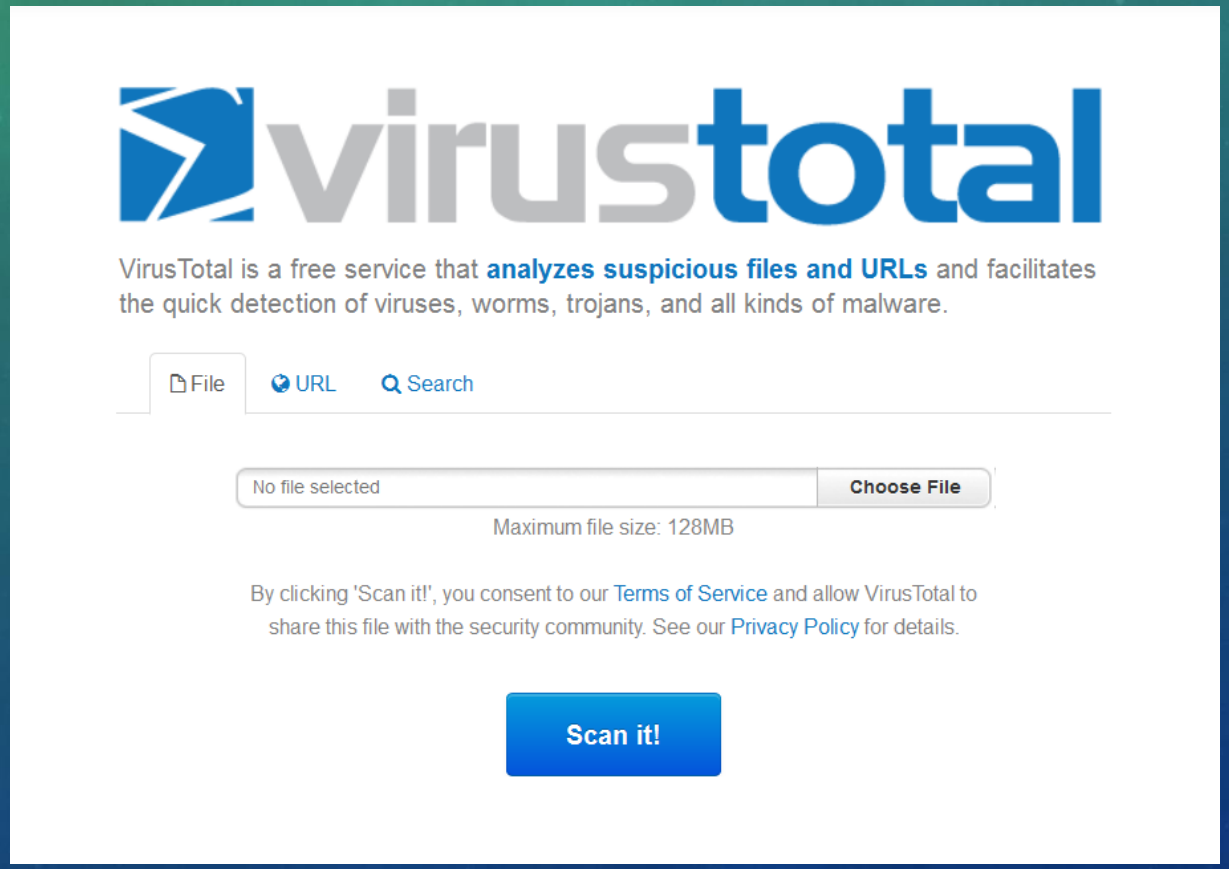
沙箱

- 在當前系統下創造一個虛擬環境(sandbox)
- 在沙盤內運行的程式，所做的修改都會隔離於沙盤內
- 強力推薦sandboxie



NISRA

單一檔案線上掃描工具-VirusTotal



NISRA

線上沙盤分析

NISRA

最後

- 1+1<2
- 養成良好習慣
- 不點奇怪連結、奇怪廣告、奇怪信件、奇怪檔案
- 隨手更新

NISRA