



Confidence in a connected world.



以加密勒索軟體為例，拆解網路攻擊鏈—— 最佳化端點、電郵與網頁防護實務

保安資訊有限公司 陳炳銘 顧問

www.SaveTime.com.tw 好記:幫您節省時間.的公司.在台灣

We **Keep** IT **Safe** , Secure & **Save** you **Time** , Cost

“知己知彼，百戰百勝”-拆解網路攻擊模式:以洛克希德馬丁公司的網路攻擊鏈(Cyber Kill Chain)框架

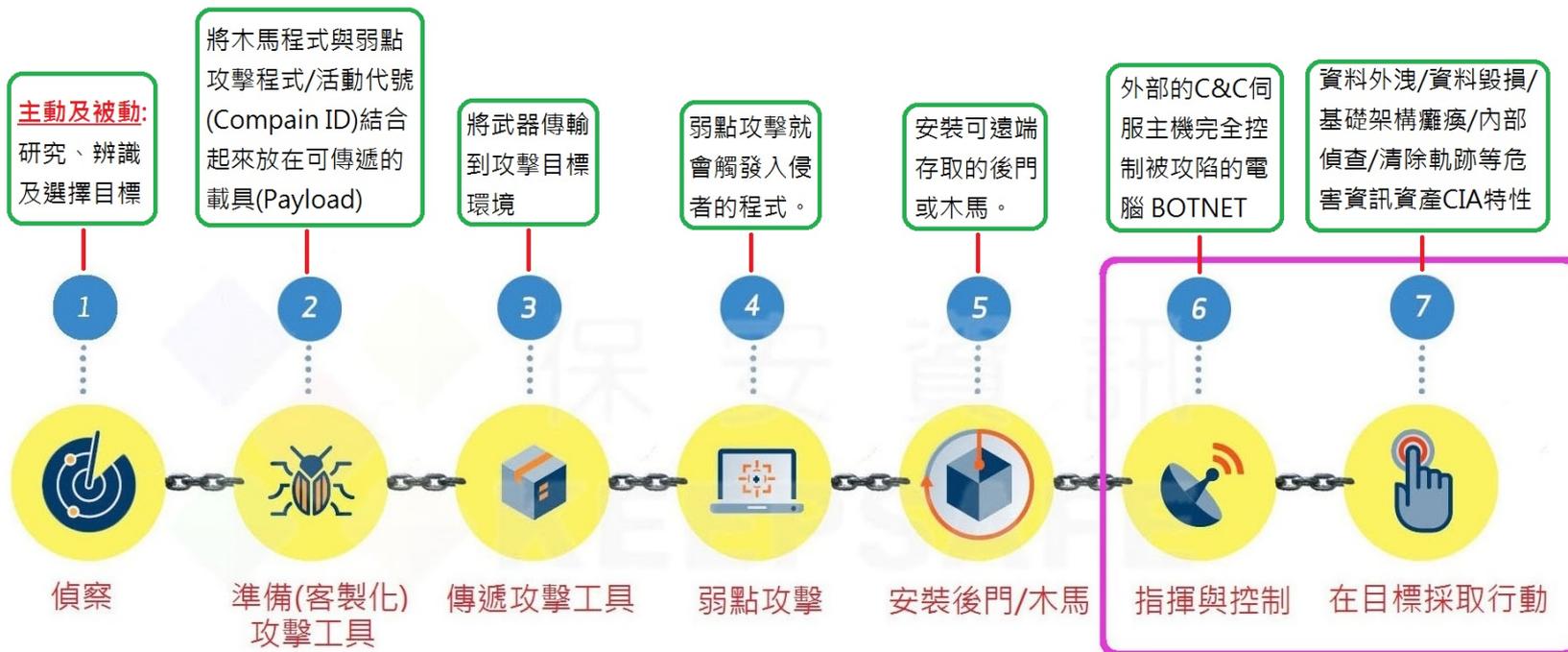


時間軸

數小時/數個月

數秒鐘

數個月至數年

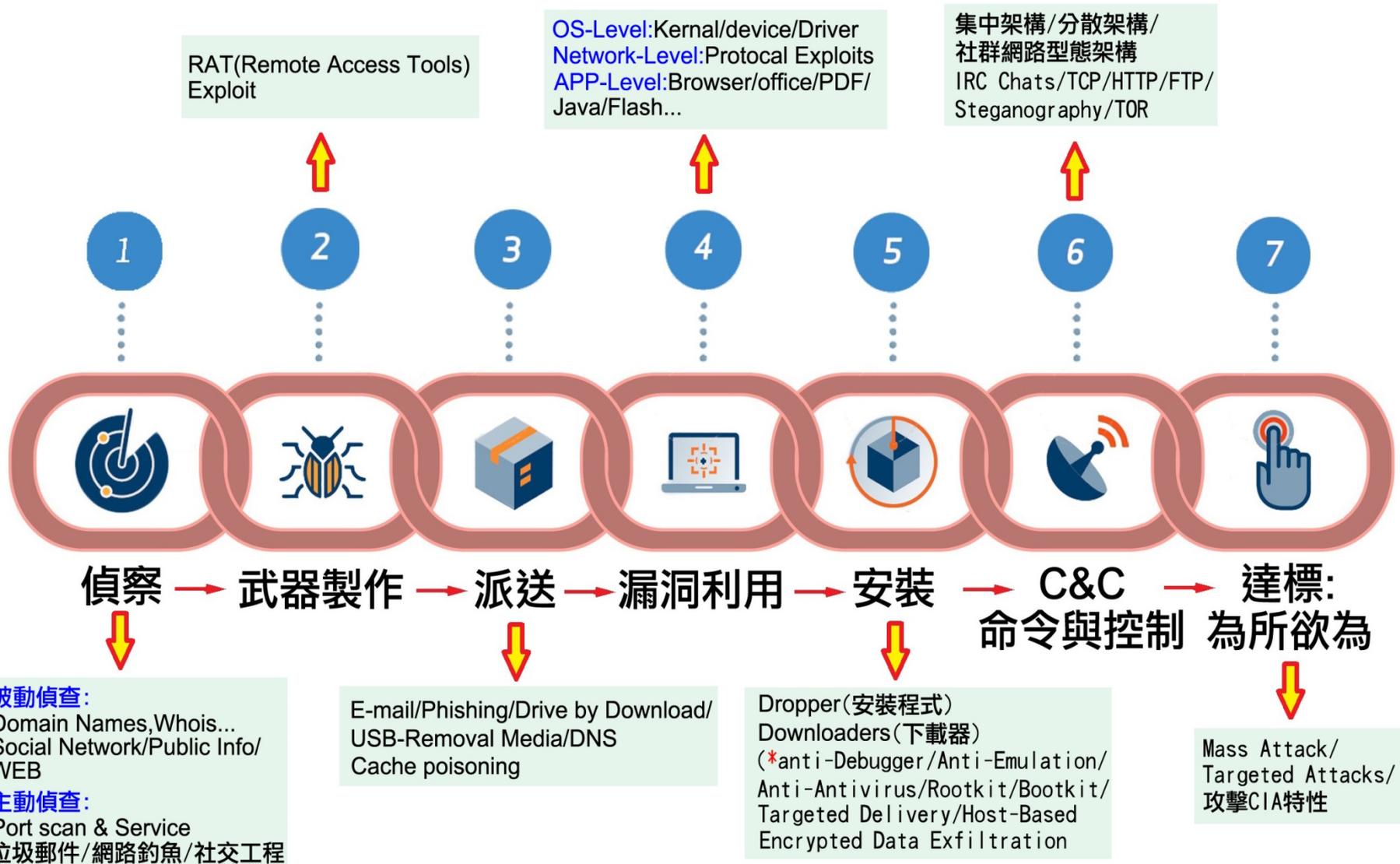


準備階段

入侵階段

控制及採取行動階段

對應網路攻擊鏈(Cyber Kill Chain)框架-攻擊者常用的攻擊技術(Technical Aspects)



對應網路攻擊鏈(Cyber Kill Chain)框架-產業標準的建議防護

Phase	Detect (偵測)	Deny (避免)	Disrupt (阻止)	Degrade (降級)	Deceive (誘騙)	Contain (災情控管)
Reconnaissance (偵查)	Web Analytics	Firewall ACL				Firewall ACL
Weaponization (武器化)	NDIS	NIPS				
Delivery (傳遞)	Vigilant user(Security Awareness)	Proxy Filter	Inline AV	Queuing		APP-Aware Firewall
Exploitation (漏洞利用)	HIDS	Patch	DEP			Inter-Zone NIPS
Installation (安裝)	HIDS	'Chroot' Jail	AV			EPP
Command and Control (命令與控制)	NDIS	Firewall ACL	NIPS	Tarpit	DNS Redirect	Trust zones
Action on Targets(達標)	Audit Logs	Outbound ACL	DLP	Quality of service	Honeypot	Trust zones

對應網路攻擊鏈(Cyber Kill Chain)框架-Symantec 提供業界最完善的防護保護方案

Phase	Detect(偵測)	Deny(避免) or Contain(災情限制/控制)	Disrupt(阻止)·Eradicate(根除) or Deceive(誘騙)	Recover(恢復)
Reconnaissance (偵查)	DeepSight Threat Intelligence、MSS(Managed Security Services)、CSS(Control Compliance Suite)、SMG(*DHA Protect)	CSS, DCS(Data center Security)	N/A	N/A
Weaponization (武器化)	DeepSight™ Adversary Intelligence	CSS、Altiris ITMS (Symantec™ IT Management Suite)	SMG(Decoy Account)、Symantec.Security.cloud(email/web)	N/A
Delivery (傳遞)	MSS、DeepSight™ Intelligence、 \$Blackfin (user training, phishing tests)	ATP、Deepsight Threat Intelligence	SEP(*AV(Sonar/Insight)/*HIPS)	SEP(*Power Eraser)、Veritas
Exploitation (漏洞利用)	SEP(*HIPS/*HI)、DCS、MSS	SEP(*FW)、DCS、ATP、DeepSight™ Intelligence	SEP(AV)、ATP、DCS	Veritas
Installation (安裝)	SEP、ATP、DCS	SEP、Mobility Suite、Authentication Manager、VIP, Managed PKI	SEP(*AV/*HIPS/*HI)、ATP(Sandbox & Correlation)、DCS(Sandbox/完全白名單/帳戶權限限縮)	Incident Response Retainer Services
Command and Control (命令與控制)	SWG、ATP、MSS、DeepSight™ Intelligence、 \$BlueCoat	DeepSight™ Intelligence、DLP、ATP	DeepSight™ Intelligence	Incident Response Retainer Services
Action on Targets(達標)	MSS、DLP、DeepSight™ Intelligence	DLP (Symantec Data Loss Prevention)	DLP、ATP	Incident Response Retainer Services

對應網路攻擊鏈(CKC): Symantec產品的防護/Hardening Tips

防護產品: SMG (Symantec Message Gateways)

郵件及訊息閘道安全 **Symantec Messaging Gateway**

不只是反垃圾郵件全球第一品牌

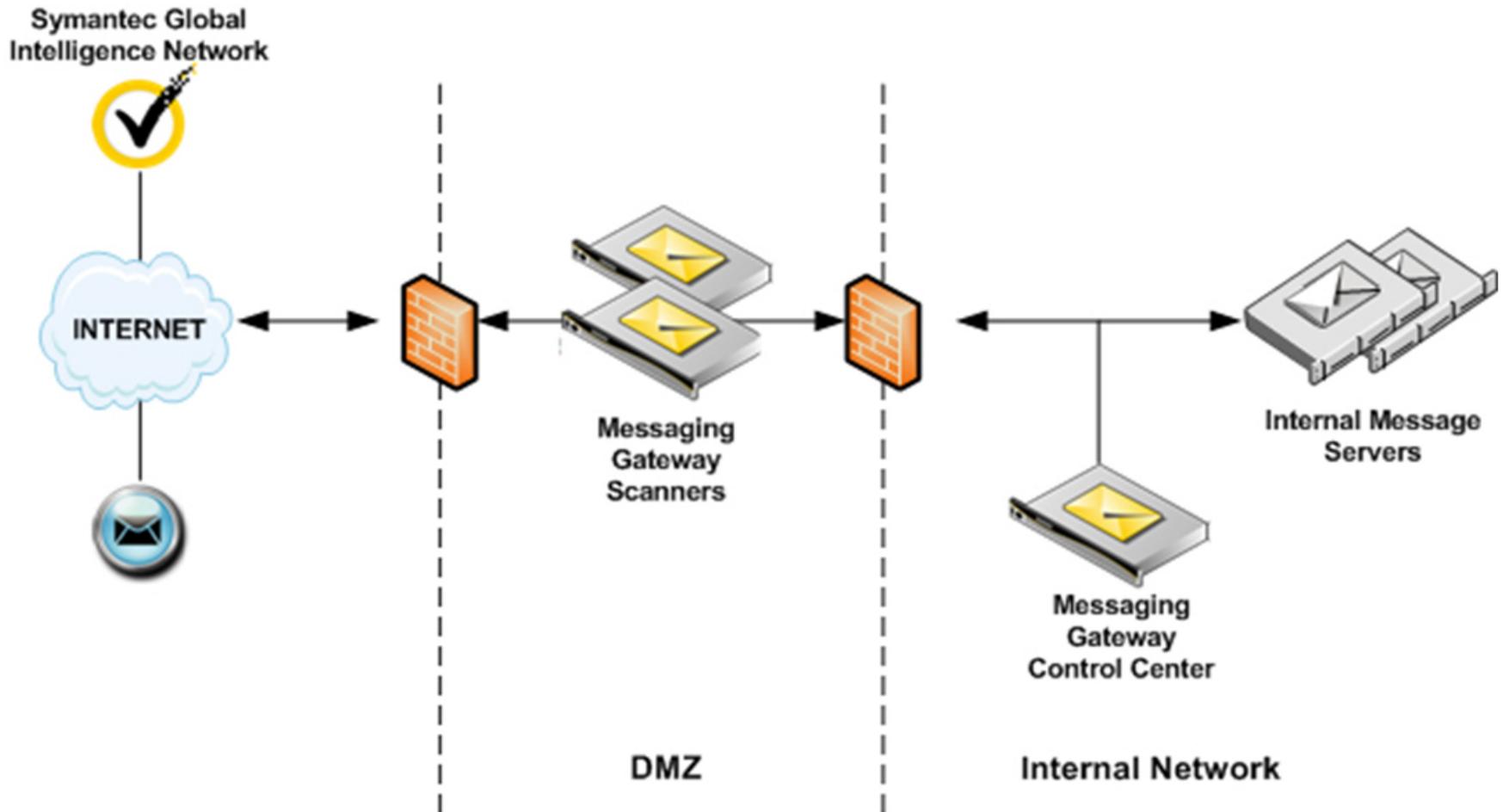
SMG集六大安全功能於一身:

- 1.防垃圾郵件
- 2.防惡意程式
- 3.內容過濾
- 4.資料遺失預防
- 5.即時通訊安全
- 6.郵件加密



實體專用硬體主機與VM/Hyper-V三平台版本同時推出

SMG:部署位於開道第一關



A closer look at Symantec Messaging Gateway

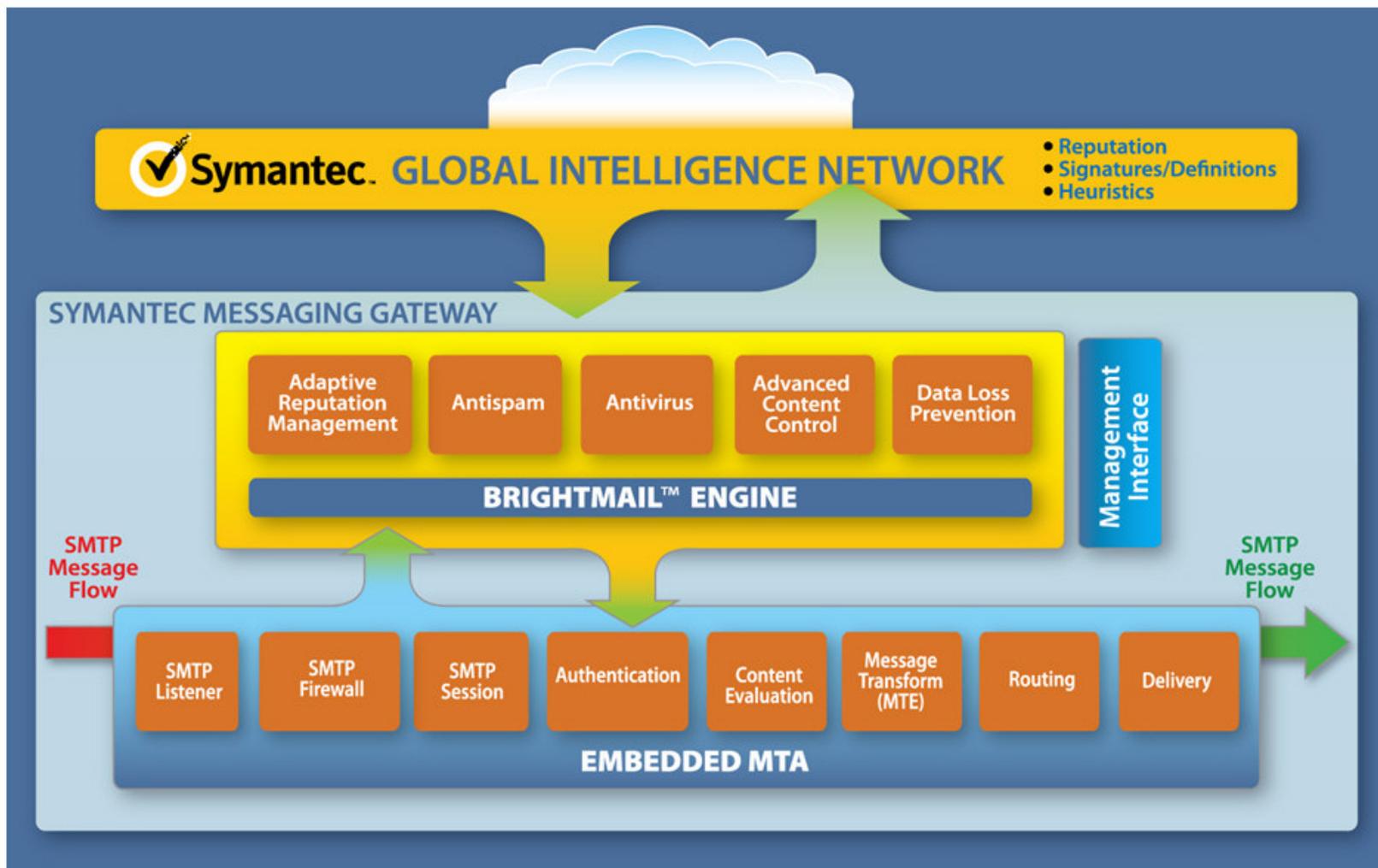
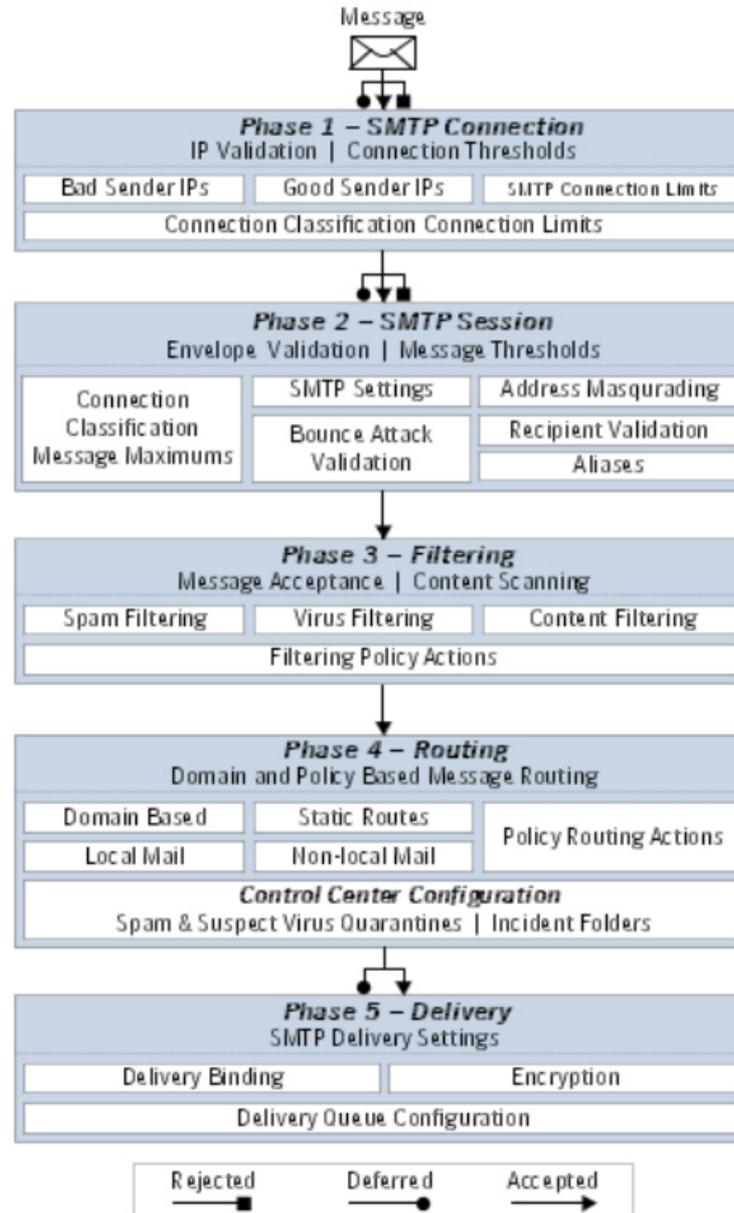


Figure: Inbound Message Flow





SMG:網路層防火牆->阻止電子郵件搜尋攻擊

狀態 報告 通訊協定 信譽 垃圾郵件 惡意軟體 內容

政策
 覆載的寄件者
 連線類別
 允許的寄件者
信譽工具
 尋找寄件者
 IP 信譽查閱

電子郵件地址搜尋攻擊

架構電子郵件地址搜尋攻擊識別，並指定發生電子郵件地址搜尋攻擊時要採取的動作。

電子郵件地址搜尋攻擊

啟用 DHA 偵測

電子郵件地址搜尋攻擊組態

錯誤收件者百分比下限:	<input type="text" value="30"/>
錯誤收件者數目下限:	<input type="text" value="2"/>
條件限定時間視窗:	<input type="text" value="5"/> 分鐘
處罰 原時間:	<input type="text" value="90"/> 分鐘

動作

如果發生「電子郵件地址搜尋攻擊」：
指定要對觸發此政策之郵件採取的動作。

新增 編輯 刪除

動作

延遲 SMTP 連線

儲存 取消



SMG:系統預設的可執行檔類型, 可自行再增減

- | | | |
|---|--------------------------------------|------------------------------------|
| <input type="checkbox"/> 附件類型 | | |
| <input type="checkbox"/> 真實檔案類型 是 ELF Executable | <input type="checkbox"/> 副檔名 是 ade | <input type="checkbox"/> 副檔名 是 com |
| <input type="checkbox"/> 真實檔案類型 是 MS-DOS Batch File | <input type="checkbox"/> 副檔名 是 adp | <input type="checkbox"/> 副檔名 是 cpl |
| <input type="checkbox"/> 真實檔案類型 是 MSDOS Device Driver | <input type="checkbox"/> 副檔名 是 app | <input type="checkbox"/> 副檔名 是 crt |
| <input type="checkbox"/> 真實檔案類型 是 MSDOS/Windows Program | <input type="checkbox"/> 副檔名 是 bas | <input type="checkbox"/> 副檔名 是 dll |
| <input type="checkbox"/> 真實檔案類型 是 PC (.COM) | <input type="checkbox"/> 副檔名 是 bat | <input type="checkbox"/> 副檔名 是 drv |
| <input type="checkbox"/> 真實檔案類型 是 Unix Executable (3B20) | <input type="checkbox"/> 副檔名 是 bin | <input type="checkbox"/> 副檔名 是 exe |
| <input type="checkbox"/> 真實檔案類型 是 Unix Executable (Basic-16) | <input type="checkbox"/> 副檔名 是 chm | <input type="checkbox"/> 副檔名 是 fpx |
| <input type="checkbox"/> 真實檔案類型 是 Unix Executable (Bell 5.0) | <input type="checkbox"/> 副檔名 是 class | <input type="checkbox"/> 副檔名 是 hlp |
| <input type="checkbox"/> 真實檔案類型 是 Unix Executable (iAPX 286) | <input type="checkbox"/> 副檔名 是 cmd | <input type="checkbox"/> 副檔名 是 hta |
| <input type="checkbox"/> MIME-類型 開頭是 application/bat | <input type="checkbox"/> 副檔名 是 ins | <input type="checkbox"/> 副檔名 是 inf |
| <input type="checkbox"/> MIME-類型 開頭是 application/com | <input type="checkbox"/> 副檔名 是 isp | <input type="checkbox"/> 副檔名 是 ink |
| <input type="checkbox"/> MIME-類型 開頭是 application/exe | <input type="checkbox"/> 副檔名 是 js | <input type="checkbox"/> 副檔名 是 scr |
| <input type="checkbox"/> MIME-類型 開頭是 application/hta | <input type="checkbox"/> 副檔名 是 jse | <input type="checkbox"/> 副檔名 是 sct |
| <input type="checkbox"/> MIME-類型 開頭是 application/javascript | <input type="checkbox"/> 副檔名 是 Ink | <input type="checkbox"/> 副檔名 是 shb |
| <input type="checkbox"/> MIME-類型 開頭是 application/x-bat | <input type="checkbox"/> 副檔名 是 mda | <input type="checkbox"/> 副檔名 是 shs |
| <input type="checkbox"/> MIME-類型 開頭是 application/x-com | <input type="checkbox"/> 副檔名 是 mdb | <input type="checkbox"/> 副檔名 是 sys |
| <input type="checkbox"/> MIME-類型 開頭是 application/x-download | <input type="checkbox"/> 副檔名 是 mde | <input type="checkbox"/> 副檔名 是 url |
| <input type="checkbox"/> MIME-類型 開頭是 application/x-exe | <input type="checkbox"/> 副檔名 是 mdt | <input type="checkbox"/> 副檔名 是 vb |
| <input type="checkbox"/> MIME-類型 開頭是 application/x-helpfile | <input type="checkbox"/> 副檔名 是 mdw | <input type="checkbox"/> 副檔名 是 vbe |
| <input type="checkbox"/> MIME-類型 開頭是 application/x-javascript | <input type="checkbox"/> 副檔名 是 mdz | <input type="checkbox"/> 副檔名 是 vbs |
| | | <input type="checkbox"/> 副檔名 是 vxd |
| | | <input type="checkbox"/> 副檔名 是 wsc |
| | | <input type="checkbox"/> 副檔名 是 msc |
| | | <input type="checkbox"/> 副檔名 是 msi |
| | | <input type="checkbox"/> 副檔名 是 msp |
| | | <input type="checkbox"/> 副檔名 是 mst |
| | | <input type="checkbox"/> 副檔名 是 nlm |
| | | <input type="checkbox"/> 副檔名 是 ops |
| | | <input type="checkbox"/> 副檔名 是 ovl |
| | | <input type="checkbox"/> 副檔名 是 pcd |
| | | <input type="checkbox"/> 副檔名 是 pif |
| | | <input type="checkbox"/> 副檔名 是 prf |
| | | <input type="checkbox"/> 副檔名 是 prg |



SMG: Disarm

(解除Office/PDF 檔案的物件)

New: Gateway: *Disarm for Symantec Messaging Gateway*



- Disarm removes all active content and reconstructs a clean version
- Clean attachment is delivered in real-time
- User is **never exposed** to the attack

Blocked
98%

of Zero Day Exploits in 2013

Works with



Attachments



SMG:Disarm, 支援的檔案類型&物件

電子郵件掃描設定

架構惡意軟體設定。

電子郵件掃描設定

一般 排除掃描 **解除**

解除內容類型

選取可以解除的內容類型。

- Office 2003
 - 內嵌檔案和附件
 - Flash
 - 巨集
- Office 2007 和以上版本
 - 內嵌檔案和附件
 - Flash
 - 巨集
- PDF
 - 3D 元件
 - 內嵌檔案和附件
 - Flash
 - 字型 !
 - 結尾資訊
 - Javascript
 - 啟動
 - XFA (及其 Javascript)
 - 全螢幕

解除選項

- 前置處理不合格的 PDF

儲存

取消



SMG: Disarm政策, 先保留一份稽核再解除物件

通訊協定 | 信譽 | 垃圾郵件 | **惡意軟體** | 內容

編輯電子郵件惡意軟體政策

架構電子郵件惡意軟體政策，並將其套用至選取的政策群組。指定過濾條件以及針對受感染電子郵件採取的對應動作。

電子郵件惡意軟體政策

政策名稱:

條件

套用至:

如果郵件:

動作

指定要對觸發此政策之郵件採取的動作

動作

封存郵件

解除附件

套用至下列政策群組

政策群組

架構動作

封存電子郵件地址:

選擇性封存標籤:

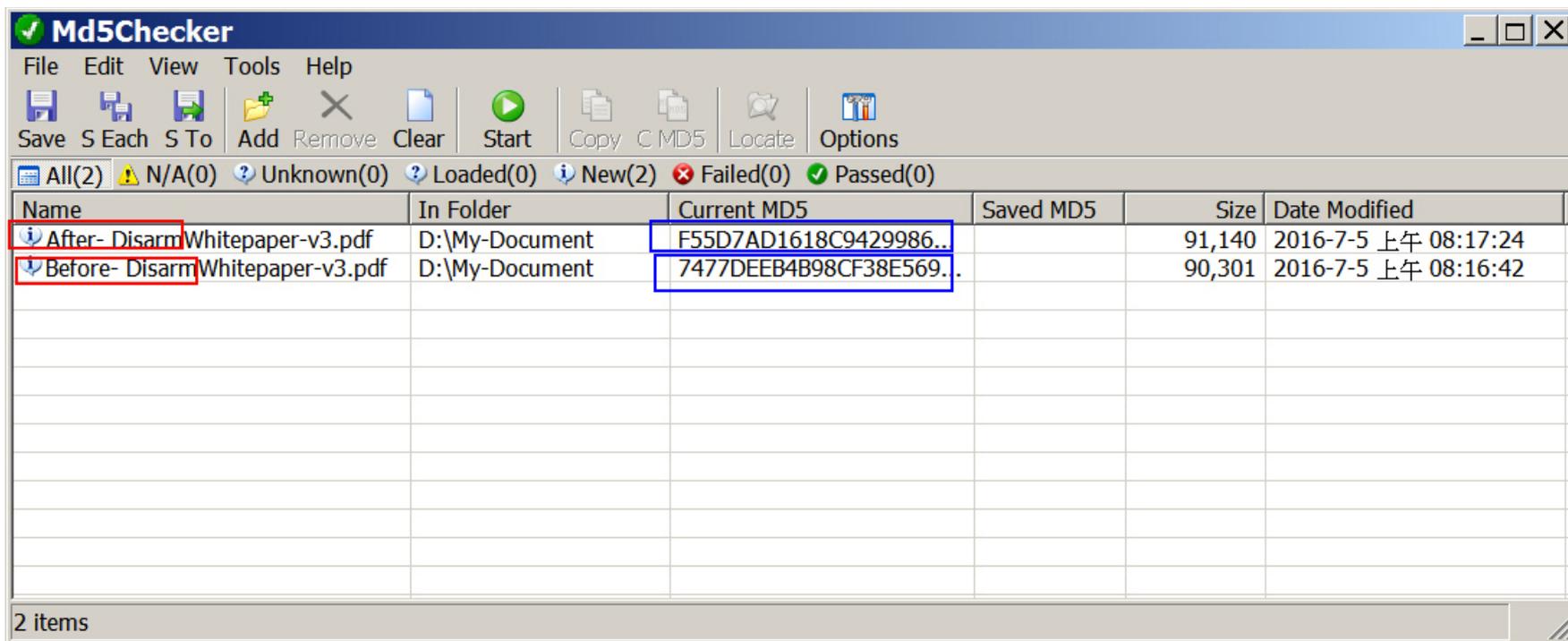
編碼:

封存伺服器主機:

封存伺服器通訊埠:

啟用 MX 查詢

SMG:檔案經 Disarm 後,檔案已 被修改

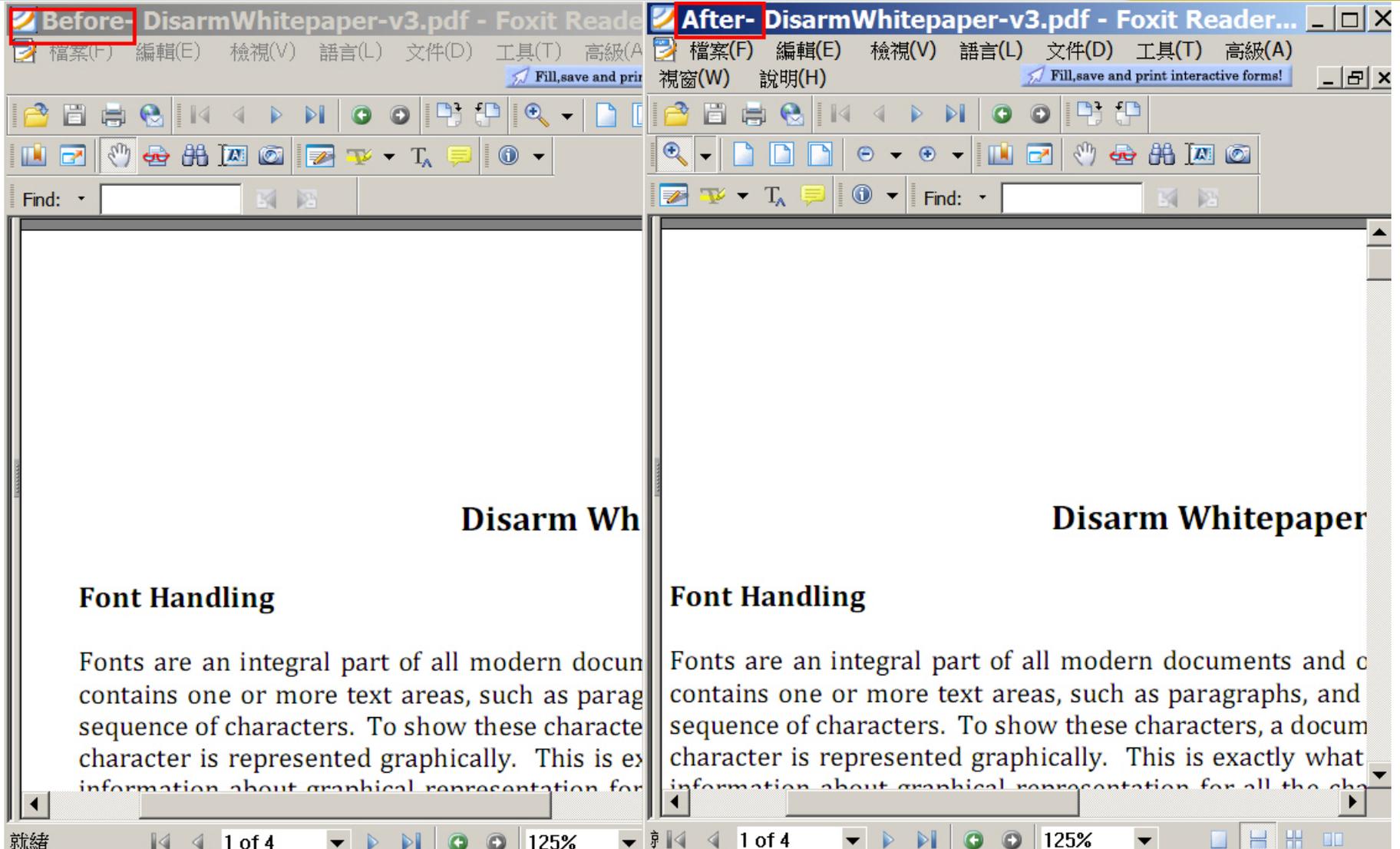


The screenshot shows the Md5Checker application window. The title bar reads "Md5Checker". The menu bar includes "File", "Edit", "View", "Tools", and "Help". The toolbar contains icons for "Save", "S Each", "S To", "Add", "Remove", "Clear", "Start", "Copy", "C MD5", "Locate", and "Options". The status bar shows "All(2)", "N/A(0)", "Unknown(0)", "Loaded(0)", "New(2)", "Failed(0)", and "Passed(0)". The main area is a table with the following data:

Name	In Folder	Current MD5	Saved MD5	Size	Date Modified
After- Disarm Whitepaper-v3.pdf	D:\My-Documnt	F55D7AD1618C9429986..		91,140	2016-7-5 上午 08:17:24
Before- Disarm Whitepaper-v3.pdf	D:\My-Documnt	7477DEEB4B98CF38E569..		90,301	2016-7-5 上午 08:16:42

2 items

SMG:檔案經Disarm後, 不影響"可讀性"





SMG:連線類別,網路層流量管控

狀態 報告 通訊協定 **信譽** 垃圾郵件 惡意軟體 內容 管理

- 政策
 - 攔截的寄件者
 - 連線類別**
 - 允許的寄件者
- 信譽工具
 - 尋找寄件者
 - IP 信譽查閱

連線類別

檢視每個連線類別的連線參數。連線類別初始會將新的 IP 位址新增至預設的類別。基於本機信譽 - 每個掃描器從該 IP 位址接收到的垃圾郵件數量與合法電子郵件數量，發送者可隨時在兩個類別之間移動。每個類別的預設設定可確保在大多數環境下具有最佳效能。

啟用連線類別

編輯	預設	← 極差			中等				→ 極佳	
		9	8	7	6	5	4	3	2	1
連線類別										
連線數目上限 (總和必須是 100%)	10.0%	0.2%	0.4%	1.0%	5.0%	10.0%	10.0%	10.0%	19.0%	34.4%
每個 IP 的連線數目上限	2	1	1	1	1	1	25	50	100	200
每個連線的郵件	20	1	1	1	1	5	10	20	40	0
重新連線逾時	10 秒	60 秒	30 秒	30 秒	15 秒	5 秒	2 秒	1 秒	1 秒	0 秒
延遲的郵件	10%	95%	80%	60%	30%	10%	5%	0%	0%	0%

儲存 取消

SMG:網路層流量管控,基於IP連 線歷史資料智慧分析

Symantec Messaging Gateway does not take any action based on Connection Classification until the appliance has recorded enough data to make accurate predictions. Immediately after the initial installation of a Scanner, Connection Classification is in learning mode. **Learning mode ends when 50,000 messages** are received and the statistics gathered from them have been added to the database.



SMG:防禦電子郵件退回攻擊

Symantec Messaging Gateway 登入為: admin [mx776.savetime.com.tw] | ⚙

狀態 報告 通訊協定 信譽 垃圾郵件 惡意軟體 內容 管理

政策
電子郵件
設定
 探查帳戶
 隔離所設定
 掃描設定
 寄件者驗證
 提交設定
提交
 提交郵件
隔離所
 垃圾郵件

編輯垃圾郵件政策

架構垃圾郵件政策，並將它套用於選取的政策群組。指定過濾條件和針對垃圾郵件或不想要的郵件採取的對應動作。

垃圾郵件政策

政策名稱:
Failed Bounce Attack Validation: Reject message (default)

條件

套用至:
入埠郵件

如果符合下列條件:
如果郵件無法通過退回攻擊驗證

動作

指定要對觸發此政策之郵件採取的動作。

新增 編輯 刪除

動作

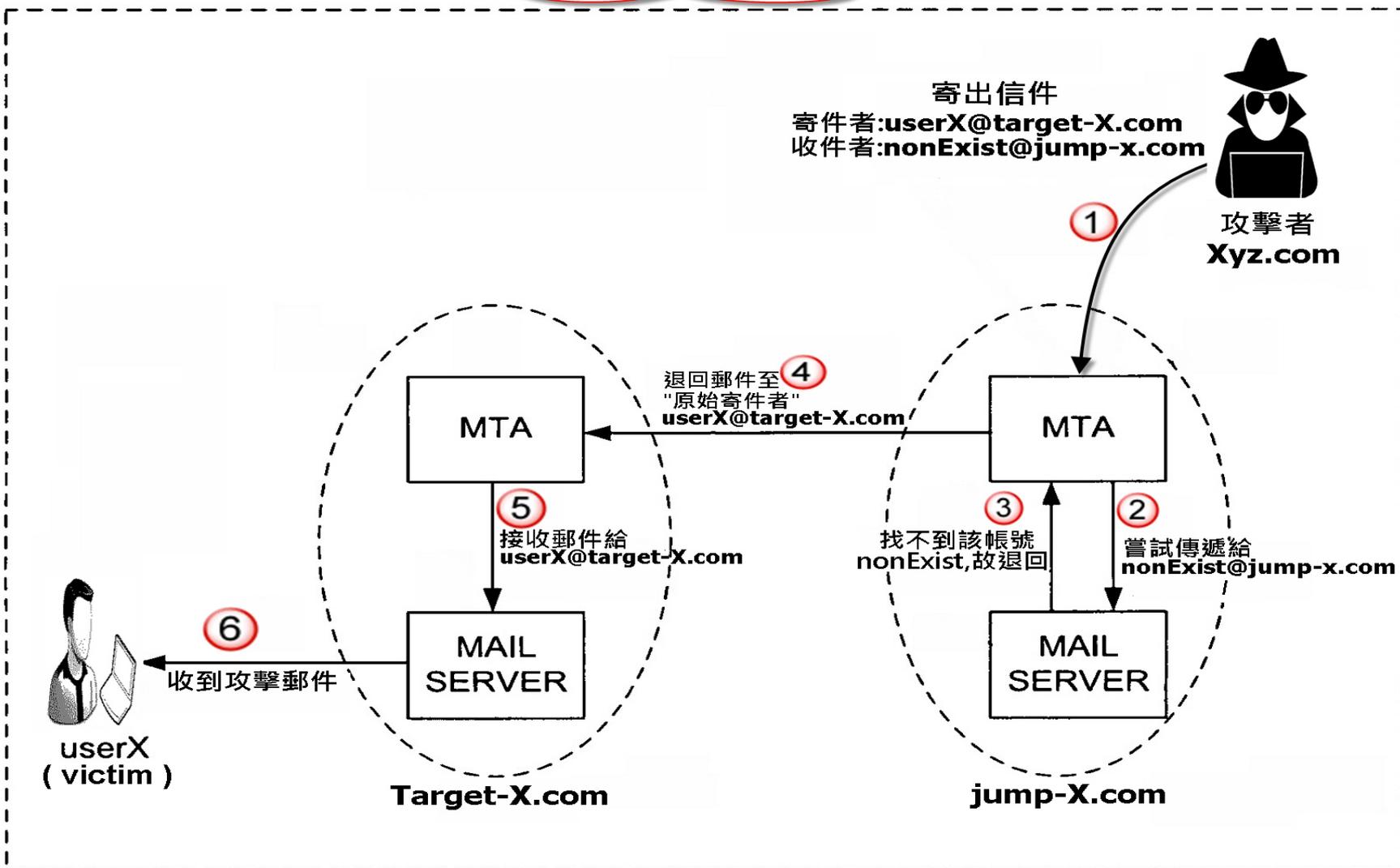
拒絕未通過退回攻擊驗證的郵件

套用至下列政策群組

- 政策群組
- sales
- Jerry-only
- Default

電子郵件退回攻擊的原理

How E-mail Bounce Attack Work





產品: SEP (Symantec Endpoint Protection)
 應用程式控制, 預設的 Policy 可阻擋常見的惡意程式非經授權存取

0-Harden-Default-應用程式及裝置控制政策

應用程式和裝置控制
 政策

概述

應用程式控制

裝置控制

應用程式控制

應用程式控制規則集

「應用程式控制」會限制應用程式可執行的動作以及可使用的系統資源。「應用程式控制」具有多項功用, 包括防止惡意軟體劫取應用程式、防範不慎移除公司的機密資料, 以及限制可執行的應用程式。

只有進階管理員可建立「應用程式控制」規則集。

已啟用	規則集	測試/正式
<input checked="" type="checkbox"/>	防止用戶端改IP-Win7-2008-Vista 的副本	正式
<input type="checkbox"/>	擱阻應用程式執行 [AC1]	正式
<input type="checkbox"/>	擱阻從卸除式磁碟機執行程式 [AC2]	正式
<input type="checkbox"/>	將全部卸除式磁碟機設定為唯讀 [AC3]	正式
<input type="checkbox"/>	[AC4-1.1] 擱阻向 USB 磁碟機寫入內容	正式
<input type="checkbox"/>	[AC5-1.1] 記錄向 USB 磁碟機寫入的內容	正式
<input type="checkbox"/>	擱阻對主機檔案的修改	正式
<input checked="" type="checkbox"/>	擱阻存取程序檔	測試 (只記錄)
<input type="checkbox"/>	停止軟體安裝程式 [AC8]	正式
<input checked="" type="checkbox"/>	擱阻存取 Autorun.inf [AC9]	正式
<input type="checkbox"/>	擱阻密碼重設工具 [AC10]	正式
<input type="checkbox"/>	擱阻檔案共用 [AC11]	正式
<input type="checkbox"/>	防止變更 Windows shell 載入點 (HIPS) [AC12]	正式
<input checked="" type="checkbox"/>	防止使用瀏覽器和 Office 產品變更系統 (HIPS) [AC13]	測試 (只記錄)
<input type="checkbox"/>	防止修改系統檔案 (HIPS) [AC14]	測試 (只記錄)
<input checked="" type="checkbox"/>	防止註冊新的瀏覽器協助程式物件 (HIPS) [AC15]	正式
<input checked="" type="checkbox"/>	防止註冊新的工具列 (HIPS) [AC16]	正式
<input type="checkbox"/>	防止容易遭到攻擊的 Windows 程序撰寫程式碼 [AC17]	正式
<input type="checkbox"/>	防止 Windows 服務使用 UNC 路徑 [AC-23]	正式
<input type="checkbox"/>	擱阻對 Ink 和 pif 檔案的存取 [AC-24]	正式
<input type="checkbox"/>	擱阻應用程式用盡資源回收筒 [AC-25]	正式

新增... 編輯... 刪除 上移 下移

確定 取消 說明



Browser address bar: <http://www.rarlab.com/download.htm>

WinRAR archiver, a powerful tool to ...

File Name	Type	Size
RAR 5.40 beta 3 for Linux	Command line only	Trial 1095 KB
RAR 5.40 beta 3 for Linux x64	Command line only	Trial 1129 KB
RAR 5.40 beta 3 for FreeBSD	Command line only	Trial 1565 KB
RAR 5.40 beta 3 for Mac OS X	Command line only	Trial 496 KB
RAR 5.40 beta 3 for Windows	Command line only	Trial 2016 KB
RAR 5.40 beta 3 for Windows x64	Command line only	Trial 2238 KB
RAR 5.40 beta 3 for Windows x86	Command line only	Trial 1966 KB
RAR 5.40 beta 3 for Windows x86-64	Command line only	Trial 2191 KB
RAR 5.40 beta 3 for Windows x86-64	Command line only	Trial 1966 KB
RAR 5.40 beta 3 for Windows x86-64	Command line only	Trial 2191 KB
RAR 5.40 beta 3 for Windows x86-64	Command line only	Trial 1978 KB
RAR 5.40 beta 3 for Windows x86-64	Command line only	Trial 2270 KB
RAR 5.40 beta 3 for Windows x86-64	Command line only	Trial 2166 KB
RAR 5.40 beta 3 for Windows x86-64	Command line only	Trial 2382 KB
RAR 5.40 beta 3 for Windows x86-64	Command line only	Trial 1969 KB
RAR 5.40 beta 3 for Windows x86-64	Command line only	Trial 2194 KB
RAR 5.40 beta 3 for Windows x86-64	Command line only	Trial 2240 KB
RAR 5.40 beta 3 for Windows x86-64	Command line only	Trial 2456 KB

0% / wrar54b3tc.exe 從 www.rarlab.com 已完成

正在取得檔案資訊:
wrar54b3tc.exe 從 www.rarlab.com

檔案下載 - 安全性警告

是否要執行或儲存這個檔案?

名稱: wrar54b3tc.exe
類型: 應用程式, 2.11MB
從: www.rarlab.com

執行(R) 儲存(S) 取消

雖然來自網際網路的檔案可能是有用的, 但是這個檔案類型有可能會傷害您的電腦。如果您不信任其來源, 請不要執行或儲存這個軟體。有什麼樣的風險?

Risk !! 使用者直接從瀏覽器執行可執行檔 !!



- Dealers
- Feedback
- Partnership
- Imprint
- Other

正在確認 wrar54b3.exe 從 www.rarlab.com

Windows 無法存取指定的裝置、路徑或檔案。您可能沒有適當的權限，所以無法存取項目。

確定

Language	Size
Albanian (32 bit)	2016
Albanian (64 bit)	2238
Arabic (32 bit)	1966
Arabic (64 bit)	2191
Armenian (32 bit)	1966
Armenian (64 bit)	2191
Bulgarian (32 bit)	1978
Bulgarian (64 bit)	2270
Chinese Traditional (32 bit)	2166
Chinese Traditional (64 bit)	2382
Croatian (32 bit)	1969
Croatian (64 bit)	2194
Dutch (32 bit)	2240
Dutch (64 bit)	2456
English (32 bit)	1916
English (64 bit)	2131
Finnish (32 bit)	1968
Finnish (64 bit)	2192

Symantec Endpoint Protection

已攔截 iexplore.exe 存取 wrar54b3[1].exe
本組織不允許 Browser/Office 直接存取外部程式 !!





SEP:防火牆可封鎖老舊應用程式連外,此處IE為例,其他Chrome,Firefox,flash,java等亦同!

防火牆政策

防火牆 政策

- 概述
- 規則
- 內建規則
- 防護與隱蔽
- Windows 整合
- 點對點驗證設定

規則

規則 通報

防火牆規則會允許、攔截和記錄網路流量。您可以在下面表格中新增較高優先順序的規則。

從父群組繼承防火牆規則

否已...	名稱	動作	應用程式	
19	<input type="checkbox"/> 封鎖Facebook遊戲部份	攔截	*	任何
20	<input type="checkbox"/> 封鎖LINE	攔截	*	任何
21	<input type="checkbox"/> 封鎖舊Browser	攔截	c:\program files\internet explorer\iexplore.exe c:\program files (x86)\internet explorer\iexplore.exe c:\program files (x86)\internet explorer\iexplore.exe	目的: Domain-... 目的: LINE-we... 目的: LINE-we...

應用程式清單

指定觸發此規則的應用程式。

名稱	敘述	大小	上次修改日期	檔案指紋
c:\program files\internet explorer\iexplore.exe	Internet Explorer	638816	2009年3月8日	B60DDDD2D63CE41CB8C487FCFBB6...
c:\program files (x86)\internet explorer\iexplore.exe	Internet Explorer	770736	2015年7月31日	CD14FCA6675745F01C79CCCB86D2...
c:\program files (x86)\internet explorer\iexplore.exe	Internet Explorer	770736	2015年7月25日	27515D5193F89B9FA98E4C70E8AD...
c:\program files (x86)\internet explorer\iexplore.exe	Internet Explorer	772256	2015年9月17日	73F2285810A10AE505158D9AE4B04...
c:\program files\internet explorer\iexplore.exe	Internet Explorer	638120	2015年6月16日	D2A75993C096442227D8606E5E309...
c:\program files\internet explorer\iexplore.exe	Internet Explorer	775856	2015年12月16日	FE85E00B69D81981E182296AA899A...
c:\program files (x86)\internet explorer\iexplore.exe	Internet Explorer	770736	2015年12月16日	21CDC1BC5A23B230C2337F5686759...
c:\program files (x86)\internet explorer\iexplore.exe	Internet Explorer	673040	2010年11月21日	C613E69C3B191BB02C7A191741A1D...
c:\program files\internet explorer\iexplore.exe	Internet Explorer	775344	2015年7月31日	3F0928A025FCF901BB3397F7588C2...

新增... 新增自... 編輯... 刪除

確定 取消 說明

新增規則... 新增空白規則 刪除規則 上移 下移

確定 取消 說明

SEP:應用程式資料收集,方便管理者制定政策

🔍 搜尋應用程式
✕

查詢

您可以搜尋特定群組用戶端執行的應用程式相關資訊。您可以依據特定電腦或特定應用程式搜尋應用程式。

搜尋應用程式於: 瀏覽...

搜尋子群組

搜尋條件: 依據用戶端/電腦資訊
 依據應用程式

搜尋欄位	比較運算子	值
應用程式名稱	=	ieexplore.exe

查詢結果

匯出... 1/2

名稱	路徑	敘述	版本	
ieexplore.exe	c:\program files\internet explorer\	Internet Explorer	11.00.9600.16428 (winblue_gdr.13101...	813744
ieexplore.exe	c:\program files\internet explorer\	Internet Explorer	10.00.9200.16521 (win8_gdr_soc_ie.1...	776776
ieexplore.exe	c:\program files\internet explorer\	Internet Explorer	11.00.9600.16428 (winblue_gdr.13101...	814280
ieexplore.exe	c:\program files (x86)\internet explorer\	Internet Explorer	10.00.9200.16521 (win8_gdr_soc_ie.1...	770736
ieexplore.exe	c:\program files (x86)\internet explorer\	Internet Explorer	10.00.9200.16521 (win8_gdr_soc_ie.1...	770736
ieexplore.exe	c:\program files (x86)\internet explorer\	Internet Explorer	10.00.9200.16521 (win8_gdr_soc_ie.1...	772256
ieexplore.exe	c:\program files\internet explorer\	Internet Explorer	8.00.6001.23707 (longhorn_ie8_idr.15...	638120
ieexplore.exe	c:\program files\internet explorer\	Internet Explorer	7.00.6000.17080 (vista_qdr.100616-04...	634656
ieexplore.exe	c:\program files\internet explorer\	Internet Explorer	11.00.9600.16428 (winblue_gdr.13101...	814280
ieexplore.exe	c:\program files (x86)\internet explorer\	Internet Explorer	11.00.9600.16428 (winblue_gdr.13101...	815304
ieexplore.exe	c:\program files\internet explorer\	Internet Explorer	10.00.9200.16521 (win8_gdr_soc_ie.1...	775856
ieexplore.exe	c:\program files (x86)\internet explorer\	Internet Explorer	10.00.9200.16521 (win8_gdr_soc_ie.1...	770736



SEP:主機完整性檢查->事後補救 &災情控制

主機完整性政策

自訂需求

名稱: Trojan.Cryptolocker.AF
用戶端類型: Windows

自訂的需求指令碼

- /Minsert statements below:
 - IF
 - Registry: Registry value exists
 - OR Registry: Registry value exists
 - OR Registry: Registry key exists
 - THEN
 - 失敗
 - /Minsert statements here:
 - Utility: Show message dialog
 - /Der Nachrichtendialog muss durch den Nutzer aktiv bestätigt wer
 - Utility: Log message
 - Utility: Run a program
 - Utility: Set Timestamp
 - ELSE
 - /Minsert statements here:
 - 通過
 - END IF
 - 通過

選取函數:
公用程式: 顯示訊息對話方塊

顯示訊息並等待使用者回應。只有在使用者按下「確定」或「是」時才會傳回 True，否則會傳回 False。

訊息方塊的標題:
Trojan.Cryptolocker.AF/AG Infektion gefunden警告可能受感染病毒

訊息方塊的文字:
Es wurde eine Mögliche Infektion durch denTrojan.Cryptolocker.AF / AG gefunden.
Bitte informieren Sie Ihre IT-Sicherheit und trennen Sie den Rechner vom Netzwerk.
It was found a possible infection by denTrojan.Cryptolocker.AF / AG.
Please inform your IT security and disconnect the machine from the network.

指定要顯示的圖示: 錯誤

指定要顯示的按鈕: 確定

預設按鈕: 確定

經過以下等待時間上限之後，採取關閉訊息方塊的動作: 確定

等待秒數上限: 120

即使這項要求失敗，也允許主機完整性檢查通過

新增 刪除

確定 取消 說明



產品: ATP (Advanced Threat Protection, Network+Endpoint)

Advanced Threat Protection

ATP is Healthy SavetimeADM

Events

Show Filters

IP,File Name,Hash,Domain,Host ..

31 of 31 Results

Type	First Seen	Description	Internal	External
	2016-07-13 03:54:42 ...	Blacklist URL blocked: http://www.keepsafe.com.tw/repor...	WIN2K3-ENT	www.keepsafe.com.tw
	2016-07-13 03:54:03 ...	Malicious download detected: 0713.zip	WIN2K3-ENT	www.keepsafe.com.tw
	2016-07-07 09:25:40 ...	Malicious traffic blocked: Web Attack: Suspicious Execut...	PEACE	www.atpendpoint.com
	2016-07-07 09:25:40 ...	Malicious traffic blocked: Web Attack: Suspicious Execut...	PEACE	www.atpendpoint.com
	2016-07-07 09:25:22 ...	Malicious download blocked: DA_MaxBad.exe Insight convicted file from network	PEACE	www.atpendpoint.com
	2016-07-07 09:17:12 ...	Blacklisted external computer blocked: testblacklistatp.com	PEACE	testblacklistatp.com
	2016-07-07 09:17:12 ...	Blacklisted external computer blocked: testblacklistatp.com	PEACE	testblacklistatp.com



ATP(已整合Endpoint),可直接於ATP 介面隔離有風險的用戶端電腦

Endpoint: 192.168.188.5



At Risk
DISPOSITION

192.168.188.5
HOST NAME

192.168.188.5
LAST IP ADDRESS

2016-07-19 03:30:54 UTC
ATP LAST SEEN TIME

Not Available
HOST DOMAIN / WORKGROUP INFO

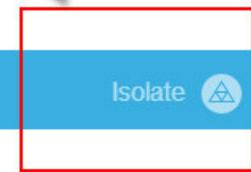
Not Available
MAC ADDRESS

Not Available
SEPM GROUP

Not Available
USER NAME

Not Available
OPERATING SYSTEM

Not Available
64-BIT



Isolate

Related Incidents

Description	Date Created	Current State	Priority
Multiple attacks have been detected targeting 192...	2016-07-19 03:30:54 UTC	Open	Low

1 Total



ATP(已整合Endpoint),可直接於ATP介面刪除(或黑名單化)用戶端電腦內有害檔案

Advanced Threat Protection

ATP is Healthy

SavetimeADM

File: 0713.zip



Bad

DISPOSITION

JS.Downloader

AV SIGNATURE NAME

No

TARGETED ATTACK

a916afa6524d2090dd02865d375f20251a919bbff51092196d52af...
SHA256

a06ad3f0f3caf82a6cfafa3f81ca44e9
MD5

Not Signed
CERTIFICATE

application/zip
FILE TYPE

File Overview

3
RELATED EVENTS

1
RELATED INCIDENTS

0
EMAIL DETECTIONS

0
CYNIC MODIFICATIONS

1
EXTERNAL DOMAINS
ACCESSED

Global Reputation

Not Available
FIRST SEEN

Fewer than 5 users
PREVALENCE

Local Reputation

Add to Whitelist

Submit to Cynic

Submit to VirusTotal

Download from file store

Delete File



產品:SWG(Symantec Web Gateway) URL Filter阻擋

Extreme	<input type="button" value="Block All"/> <input type="button" value="Allow All"/>
	<input type="button" value="Monitor All"/>
Child Abuse Images and Content	<input type="button" value="Monitor"/> ▾
Gore	<input type="button" value="Monitor"/> ▾
Self Harm	<input type="button" value="Monitor"/> ▾
Suicide	<input type="button" value="Monitor"/> ▾
Violence	<input type="button" value="Monitor"/> ▾
Illegal Activities	
	<input type="button" value="Block All"/> <input type="button" value="Allow All"/>
	<input type="button" value="Monitor All"/>
Pornography	
Plagiarism	<input type="button" value="Monitor"/> ▾
Nudism	<input type="button" value="Block"/> ▾
Pornography	<input type="button" value="Block"/> ▾
Games	
	<input type="button" value="Block All"/> <input type="button" value="Allow All"/>
	<input type="button" value="Monitor All"/>
Cash Gambling	<input type="button" value="Block"/> ▾
Gambling	<input type="button" value="Block"/> ▾
	<input type="button" value="Block"/> ▾
Malware	
	<input type="button" value="Block All"/> <input type="button" value="Allow All"/>
	<input type="button" value="Monitor All"/>
Adware/Spyware	<input type="button" value="Block"/> ▾
Malware Domain	<input type="button" value="Block"/> ▾
Criminal Activities	
	<input type="button" value="Block All"/> <input type="button" value="Allow All"/>
	<input type="button" value="Monitor All"/>
Criminal Skills	<input type="button" value="Block"/> ▾
Hacking	<input type="button" value="Block"/> ▾
Hate	<input type="button" value="Block"/> ▾



產品:SWG(Symantec Web Gateway) Inline AV 阻擋



Webgate
admin: log off

Reports

- Executive Summary
- Enterprise Summary
- Custom Reports
- Infected Clients
- Infections by Spyware Name
- Potential Attacks
- Infection Sources
- Client Applications
- Web Destinations
- Botnets
- File Uploads
- Saved Reports
- Alerts
- Search...

Policies

Configuration

Policies: Edit Policy

Insight Security	Action
	Block Unsafe Content
↑ ↓ Spyware Category	Action
Select Category	Use Default
↑ ↓ Spyware Severity	Action
Critical	Block
Major	Block
Minor	Monitor
↑ ↓ Detection Type	Action
Infection	Block
Malware URL	Block
Attack	Block
Spyware Default	Action
	Block

inline Antivirus



產品:SWG(Symantec Web Gateway) SSL Inspection



Webgate
admin: [log off](#)

Reports

- Executive Summary
- Enterprise Summary
- Custom Reports
- Infected Clients
- Infections by Spyware Name
- Potential Attacks
- Infection Sources
- Client Applications
- Web Destinations
- Botnets
- File Uploads
- Saved Reports
- Alerts
- Search...

Policies

- Configuration
- Blacklist
- Whitelist
- Blocking Feedback

Policies: Edit Policy

Save as Template [Cancel](#) [Save](#)

Base Policy On: (optional)

Policy Name:

Policy Description:

Block Page Message Group:

Applies to: All Computers Specific Work Groups

SSL Inspection

SSL inspection policy.

Content Filter Categories

All Categories

Criminal Activities

Criminal Skills

Hacking

Hate

Drugs



產品:SWG(Symantec Web Gateway) 阻擋 malware calling home 流量

Bot IP/Hostname	Status ▲	Latest Detection	Bot Activities	Hits	C&C (Command & Control)
- 129.210.219.75	Active	01/01/2015 09:39	3 Types	9,434	13 controllers
		01/01/2015 11:52	Botnet Control (C&C)	5,516	67.29.139.153 68.142.205.137 72.20.40.25 72.233.2.58 74.200.243.251 76.74.254.123 76.74.255.123 98.136.92.79 208.52.165.163 216.39.57.104 216.240.187.102 216.240.187.103 216.252.126.190
		01/01/2015 09:39	IP Scanning	3,914	
- 129.210.236.83	Active	01/01/2015 09:26	Spyware Phone Home and Downloads	4	
		01/01/2015 09:53	2 Types	3,683	6 controllers
		01/01/2015 09:53	Botnet Control (C&C)	2,953	66.220.146.11 72.233.2.58 72.233.2.59 74.200.243.251 76.74.254.123 208.73.210.27
- 129.210.239.66	Active	01/01/2015 09:39	IP Scanning	730	
		01/01/2015 09:20	2 Types	44,225	4 controllers
		01/01/2015 09:20	Botnet Control (C&C)	15,446	66.220.146.11 69.63.181.15 83.149.112.40 208.73.210.27
- 129.210.129.46	Active	01/01/2015 11:15	IP Scanning	28,779	
		01/01/2015 09:59	2 Types	4,028	11 controllers
		01/01/2015 11:59	Botnet Control (C&C)	3,364	64.106.198.79 66.220.146.11 67.29.139.153 69.63.181.15 72.32.147.161 74.125.53.100 89.202.108.100 174.143.45.97 208.73.210.27

最後一道防線 I.

Veritas BackupExec 15: 一次備份 - 多種復原選項讓作業保持簡單可靠



虛擬機器或
實體伺服器的
單程備份

儲存：
磁碟、磁帶、雲端



NDMP



磁碟



磁帶



NAS



雲端



Jbod

將整個伺服器備份至相同或不同的硬體



VM



應用程式與資料庫



檔案/資料夾



精細應用程式物件



最後一道防線II. Veritas System Recovery 2013 數分鐘內快速復原系統

