



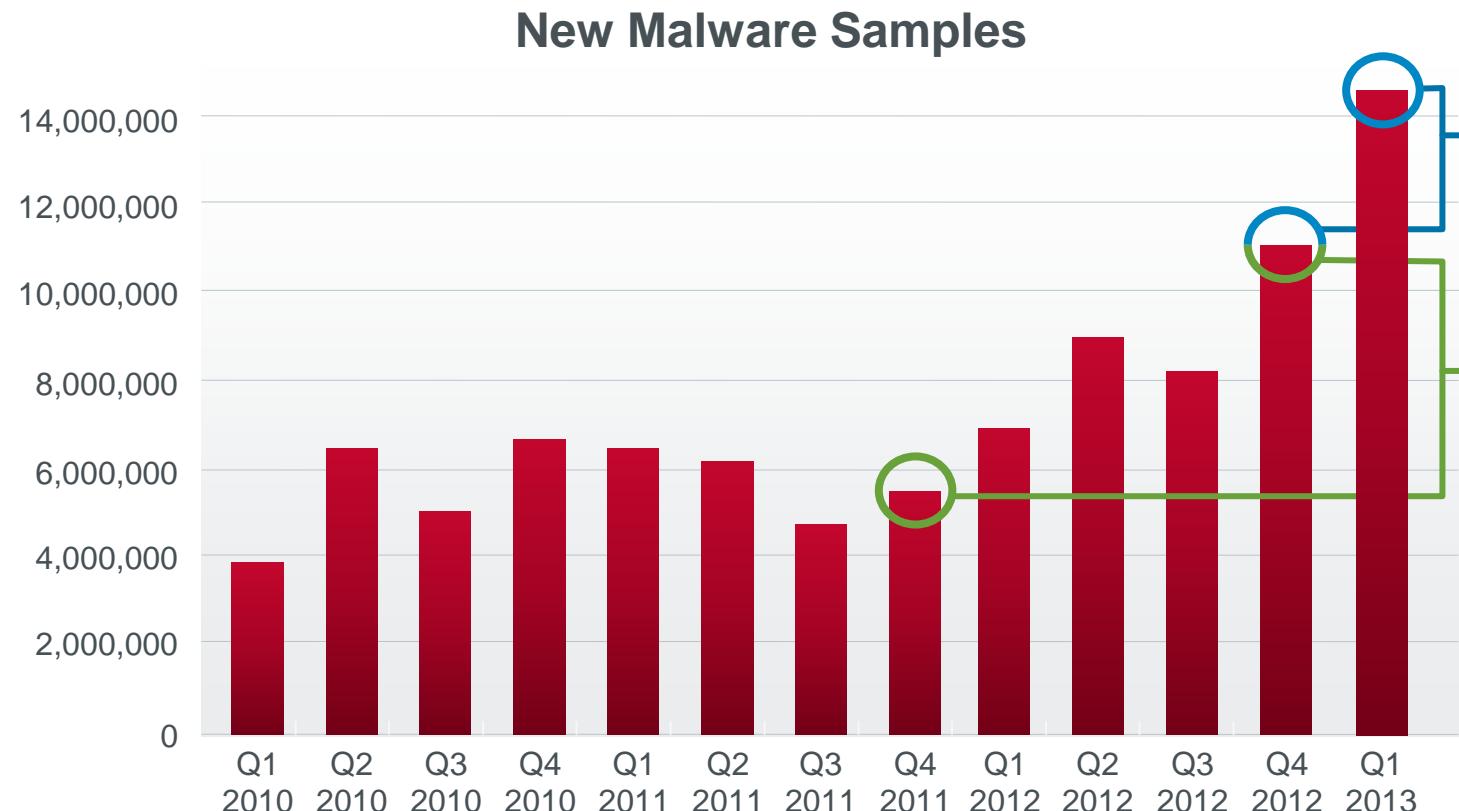
# Conectando las piezas para mitigar el riesgo

Jorge Herrerías, CISSP  
Sales System Engineer

SAFE NEVER SLEEPS™

# Malware Continues to Grow...

128M Total Malware Samples in the McAfee Labs Database



New malware samples grew 22% from Q4'12 to Q1'13

2012 new malware sample discoveries increased 50% over 2011.

Malware continues to grow, and getting more sophisticated...

The number of new, unique samples this quarter is greater than 320,000, more than twice as many as in the first quarter of 2013. During the past two quarters, McAfee Labs has catalogued more ransomware samples than in all previous periods combined.

## New Ransomware Samples



# Total Malware Samples



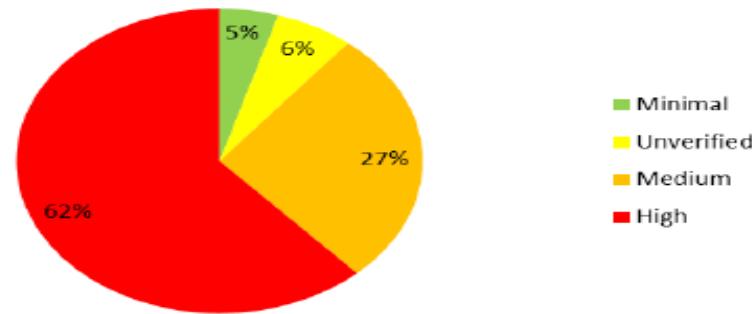
The McAfee “zoo” now contains more than 140 million unique malware samples.

## Total Malware Samples

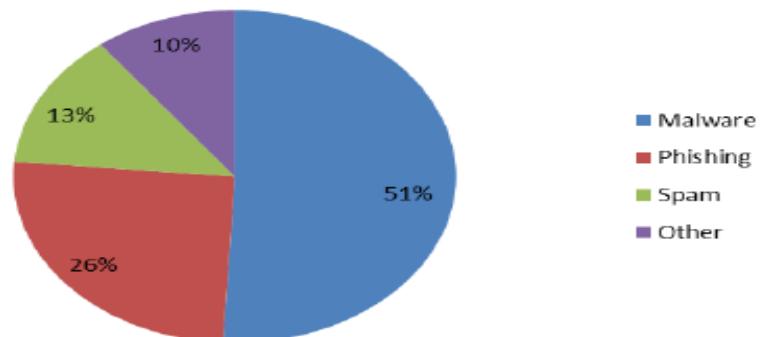


# Suspicious Internet (MX)

**Risk scale for suspect URLs**  
 (URLs hosted in Mexico)



**URLs and risks combination**  
 (URLs hosted in Mexico)



As of December 31, 2012, nearly 1,100 suspicious Internet addresses hosted in Mexico were analyzed by McAfee. There were only 800 in late 2011. 62 percent of the current ones are assigned with a maximum risk.

Nearly 51 percent of these URLs hide malware. About 26 percent of them are used in phishing campaigns and 13 percent in spam campaigns.

# Comprehensive Malware Protection



First Layer of Defense:  
Global Visibility and  
Situational Awareness



# Comprehensive Malware Protection



Second Layer of Defense:  
McAfee Advanced Threat Defense



# Comprehensive Malware Protection



Third Layer of Defense:  
Network Threat Protection



# Comprehensive Malware Protection



Fourth Layer of Defense:  
Comprehensive Endpoint  
Threat Defense



# Comprehensive Malware Protection



Fifth layer of defense:  
Real Time Endpoint Awareness



# Comprehensive Malware Protection



Sixth Layer of Defense:  
Heal Endpoints

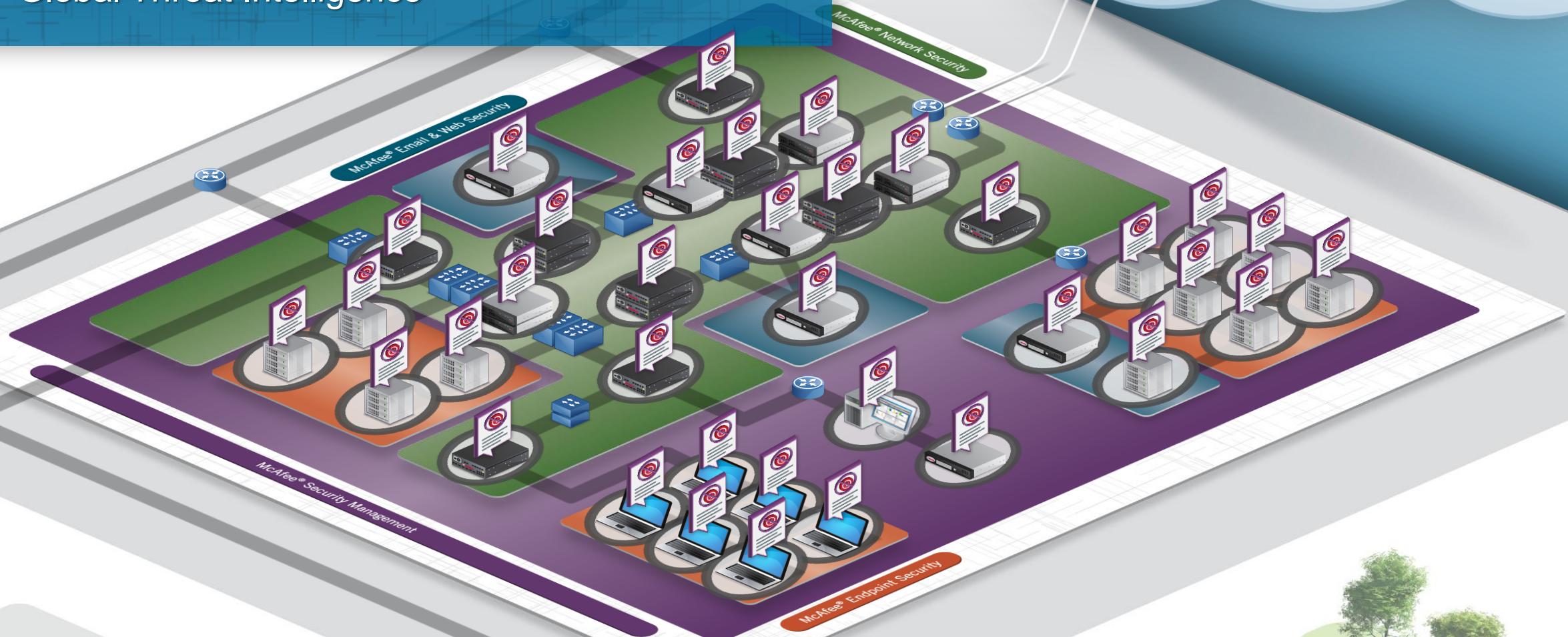


# Comprehensive Malware Protection

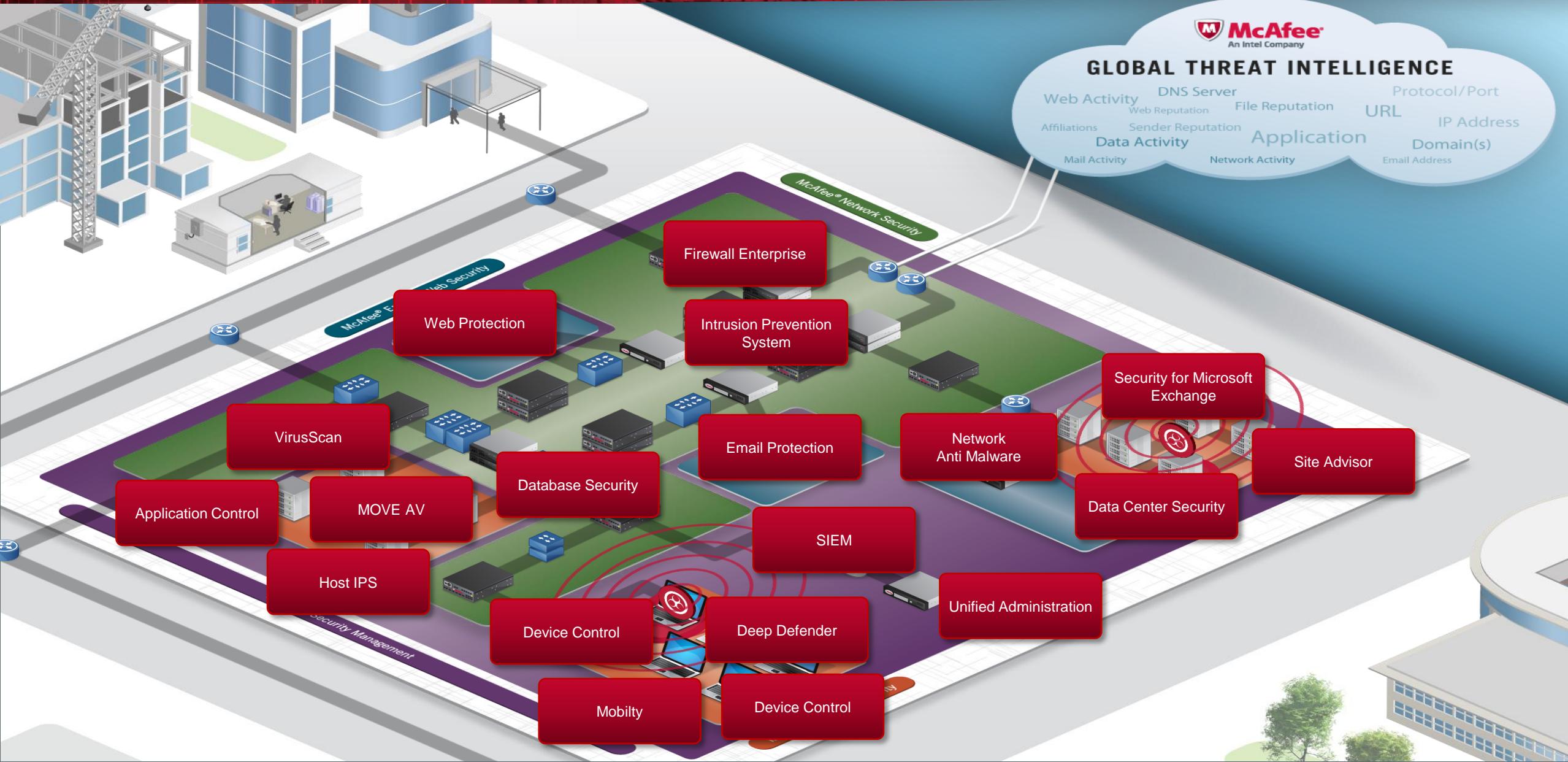


Seventh Layer of Defense:  
Global Threat Intelligence

GTI



# Multi-Layering Defense | Interconnected



# Escena 1

➊ Click here to download pictures. To help protect your privacy, Outlook prevented automatic download of some pictures in this message.

From:  eFax.com <message@inbound.efax.com>

To:  Vazquez, Juan Carlos

Cc:

Subject: eFax message from 15125280184 - 1 page(s), Caller-ID: 512-528-0184



## Fax Message [Caller-ID: 512-528-0184]

You have received a 1 page fax at 2013-09-12 06:56:56 CDT.

\* The reference number for this fax is min1\_did13-1368734175-5125280184-49.

View this fax online, on our website : [http://www.efax.com/faxes/view\\_fax.aspx?fax\\_id=5125280184](http://www.efax.com/faxes/view_fax.aspx?fax_id=5125280184)

Please visit [www.efax.com/en/efax/twa/page/help](http://www.efax.com/en/efax/twa/page/help) if you have any questions regarding this message or your service.

Thank you for using the eFax service!

# Escena 2

McAfee SiteAdvisor Software – Website Safety Ratings and Secure Search - Mozilla Firefox

File Edit View History Bookmarks Tools Help

McAfee SiteAdvisor Software – Website ... +

www.siteadvisor.com/restricted.html?domain=http%3F%2Fnavegandigital.com.ar%2Ftmp%2Fpdf\_efax\_5125280184.zip&originalURL=-2007387797&pip=false&premium=false&client\_uid=3427708180 ★ C Secure Search

Most Visited Getting Started InfraEnterprise Cust... Web Slice Gallery Connect

 SiteAdvisor® An Intel Company

Contact us

**Warning: Dangerous Site**

**Whoa!**  
Are you sure you want to go there?

http://navegandigital.com.ar/tmp/pdf\_efax\_512528... may be risky to visit.

**Why were you redirected to this page?**

✖ When we visited this site, we found it exhibited one or more risky behaviors.

Opening pdf\_efax\_5125280184.zip

You have chosen to open:  
**pdf\_efax\_5125280184.zip**  
which is: WinZip File (323 KB)  
from: http://navegandigital.com.ar

What should Firefox do with this file?

Open with WinZip (default)  
 Save File  
 Do this automatically for files like this from now on.

OK Cancel

© 2003-2013 McAfee, Inc. [Legal Notices](#)

Secure Search

Back Visit anyway

12:48 PM 9/13/2013

Windows Taskbar icons: Internet Explorer, File Explorer, Media Player, Firefox, Task View, Task Manager, Paint, File, Print, Mail, Chat, PDF, Word, Excel, Powerpoint, Paint.

# Escena 3

**Warning: Dangerous Site**



**Whoa!**  
Are you sure you want to go there?

[http://navegandodigital.com.ar/tmp/pdf\\_efax\\_512528...](http://navegandodigital.com.ar/tmp/pdf_efax_512528...) may be risky to visit.

**Why were you redirected to this page?**

- ✖ When we visited this site, we found it exhibited one or more risky behaviors.

**McAfee SiteAdvisor** | SiteAdvisor®

**Potentially Dangerous Download Detected!**

You are downloading: **pdf\_efax\_5125280184.zip**  
From: <http://navegandodigital.com.ar/tmp/>

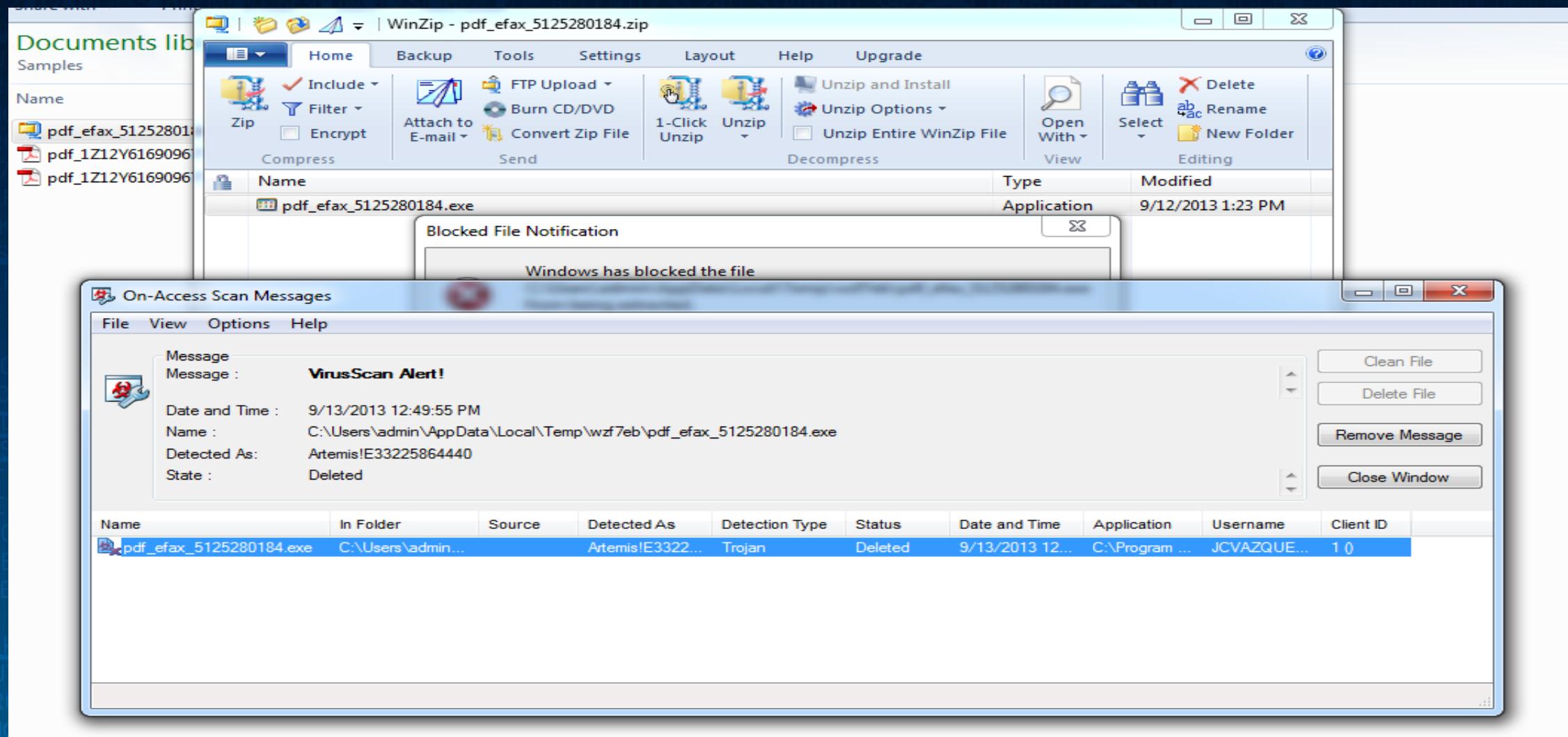
McAfee has detected that your download contains viruses, spyware, and other potentially unwanted programs. These programs can damage your hard drive or steal your personal information.

[Download Anyway](#) [Block Download](#)

[Back](#) [Visit anyway](#)

© 2003-2013 McAfee, Inc. [Legal Notices](#)

# Escena 4



The screenshot shows a Windows desktop environment with two open windows. The top window is 'WinZip - pdf\_efax\_5125280184.zip' which displays a list of files. A 'Blocked File Notification' dialog box is overlaid on the WinZip interface, stating 'Windows has blocked the file'. The bottom window is 'On-Access Scan Messages', which contains a message log. The log entry details a 'VirusScan Alert!' for a file named 'pdf\_efax\_5125280184.exe' at 9/13/2013 12:49:55 PM. The file was detected as 'Artemis!E33225864440' and was deleted. The McAfee interface includes buttons for 'Clean File', 'Delete File', 'Remove Message', and 'Close Window'.

**WinZip - pdf\_efax\_5125280184.zip**

**Blocked File Notification**  
Windows has blocked the file

**On-Access Scan Messages**

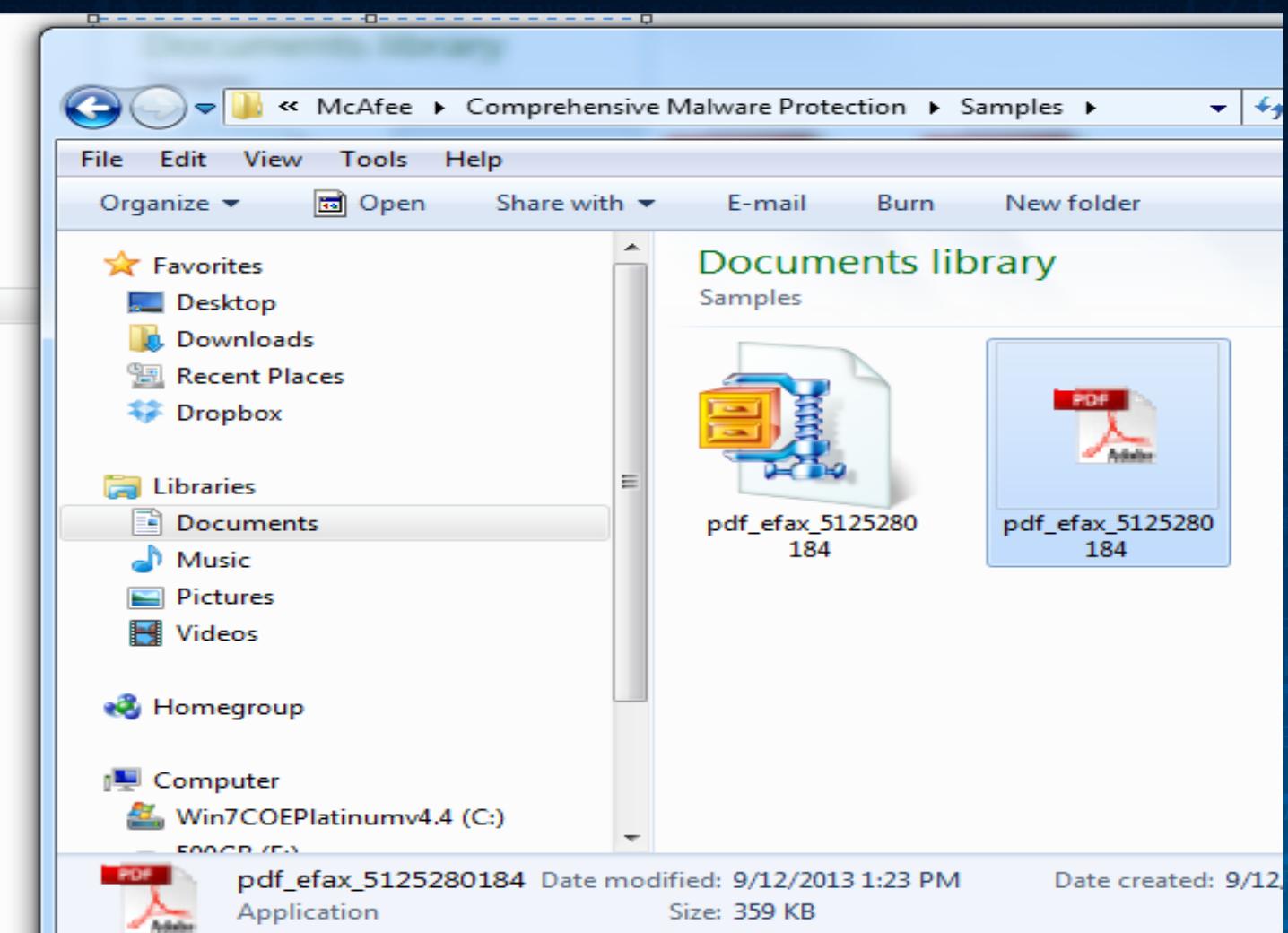
**Message**  
**Message :** VirusScan Alert!

**Date and Time :** 9/13/2013 12:49:55 PM  
**Name :** C:\Users\admin\AppData\Local\Temp\wzf7eb\pdf\_efax\_5125280184.exe  
**Detected As:** Artemis!E33225864440  
**State :** Deleted

**Clean File**  
**Delete File**  
**Remove Message**  
**Close Window**

Name	In Folder	Source	Detected As	Detection Type	Status	Date and Time	Application	Username	Client ID
pdf_efax_5125280184.exe	C:\Users\admin...		Artemis!E3322...	Trojan	Deleted	9/13/2013 12...	C:\Program ...	JCVAZQUE...	10

# Escena 5





# virustotal

VirusTotal is a free service that **analyzes suspicious files and URLs** and facilitates the quick detection of viruses, worms, trojans, and all kinds of malware.

[Choose File](#)

Maximum file size: 64MB

By clicking 'Scan it!', you consent to our [Terms of Service](#) and allow VirusTotal to share this file with the security community. See our [Privacy Policy](#) for details.

[Scan it!](#)

You may prefer to [scan a URL](#) or search through the VirusTotal dataset

# Escena 7

Community Statistics Documentation FAQ About English Join our community Sign in

**File already analysed**

This file was already analysed by VirusTotal on **2013-09-13 09:30:38**.

Detection ratio: **28/47**

You can take a look at the [last analysis](#) or analyse it again now.

[Reanalyse](#) [View last analysis](#)

pdf\_efax\_5125280184.exe [Choose File](#)

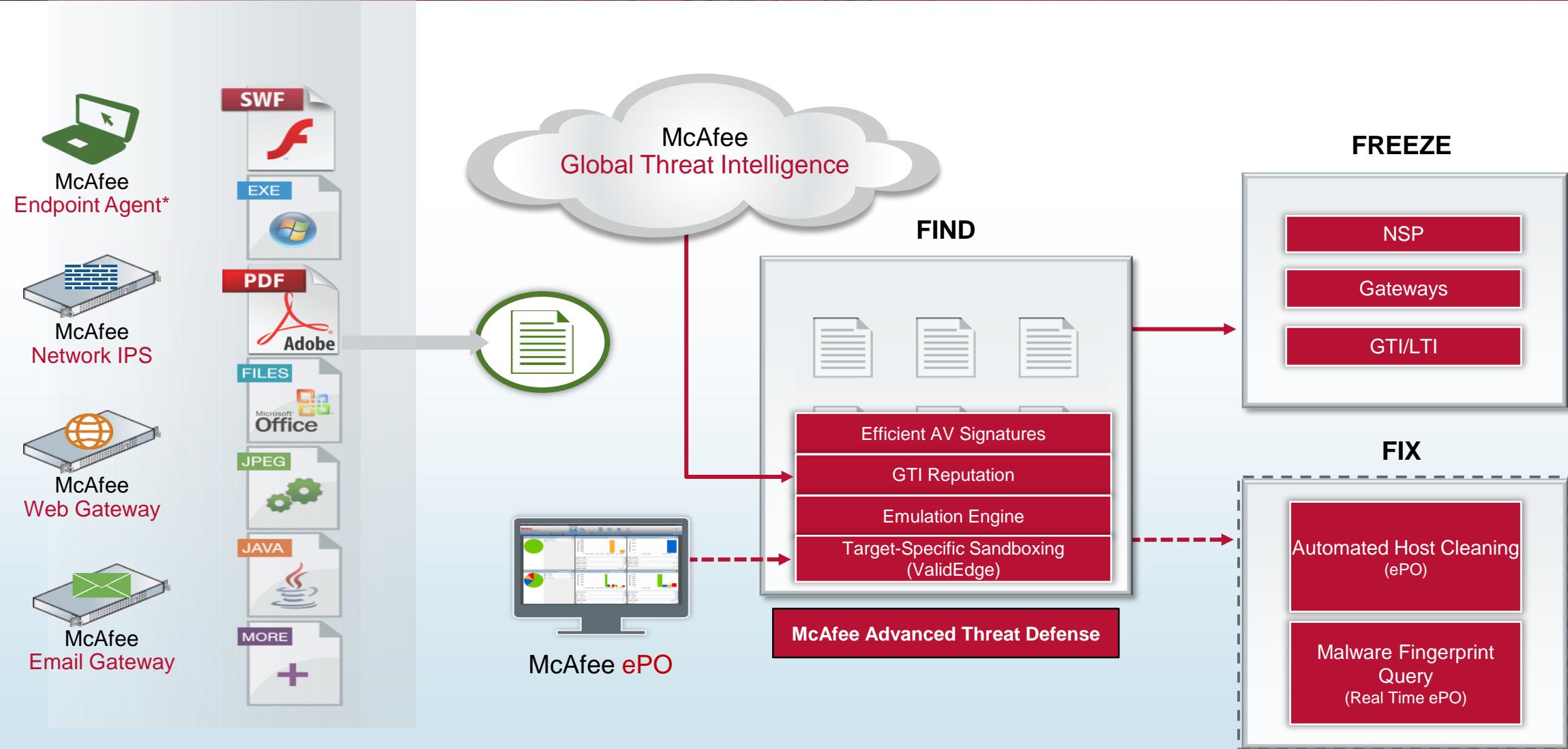
Maximum file size: 64MB

By clicking 'Scan it!', you consent to our [Terms of Service](#) and allow VirusTotal to share this file with the security community. See our [Privacy Policy](#) for details.

**Scan it!**

You may prefer to scan a URL or search through the VirusTotal dataset

# McAfee Comprehensive Malware Protection Solution Overview

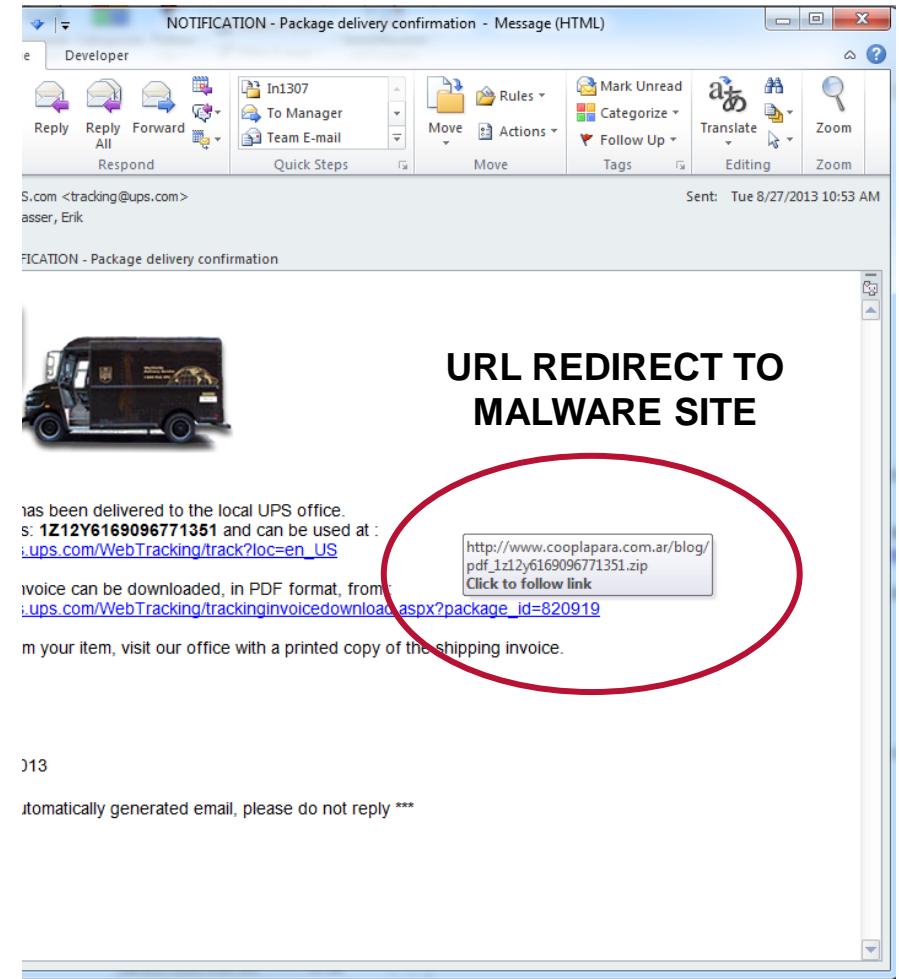


# Discovering ZeroDay and Targeted Attacks

Live Walkthrough



LIVE E-MAIL RECEIVED 08-27-2013



# Discovering ZeroDay and Targeted Attacks

Live Walkthrough



MFE FINDS VIA CLOUD

REPUTATION CHECK OF THE URL PASSES

Check URL

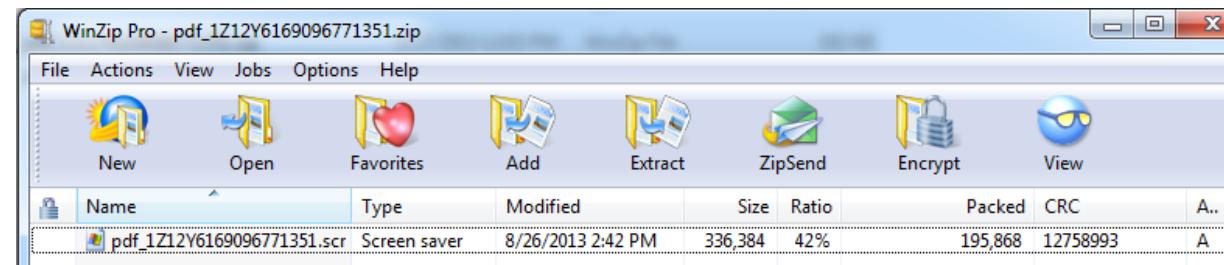
Enter the URL to check:  
[http://www.cooplapara.com.ar/blog/pdf\\_1Z12Y6169096771351.zip](http://www.cooplapara.com.ar/blog/pdf_1Z12Y6169096771351.zip)

Local  Cloud

**URL:** http://www.cooplapara.com.ar/blog/pdf\_1Z12Y6169096771351.zip (181.16.152.254)  
**Geolocation:** AR:Argentina

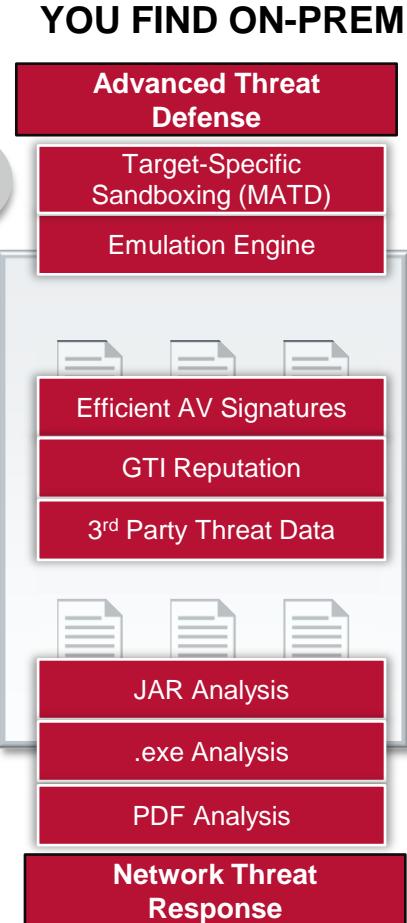
Local	Cloud
Minimal Risk (0) McAfee®	Unverified (15) McAfee®

PAYOUT APPEARS TO BE A .SCR INSIDE A .ZIP



# Discovering ZeroDay and Targeted Attacks

Live Walkthrough



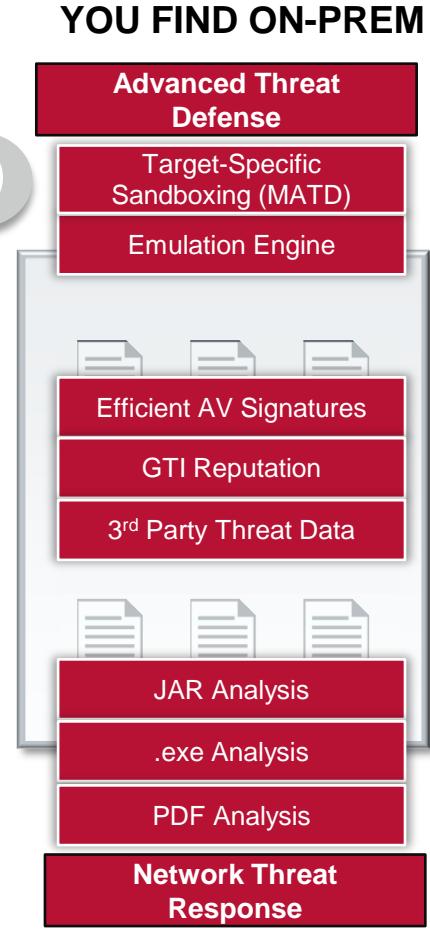
DUE TO ZERO DAY, FEW A/V SIGNATURE CATCHES



SHA256:	5e59097b1ab24f508aa8e9fac859507c406689d599bbe4ba3b8880b78a7371eb
File name:	pdf_1Z12Y6169096771351.scr
Detection ratio:	2 / 45
Analysis date:	2013-08-27 15:27:00 UTC ( 37 minutes ago )
TotalDefense	✓ 20130827
TrendMicro	✓ 20130827
TrendMicro-HouseCall	✓ 20130826
VBA32	✓ 20130827
VIPRE	✓ 20130827
ViRobot	✓ 20130827

# Discovering ZeroDay and Targeted Attacks

## Live Walkthrough



**MFE FINDS VIA CLOUD**

### MATD OR NTR EXECUTION DEMONSTRATES:

#### Malware Detected

The transferred file contained a virus and was therefore blocked.

**URL:** [http://www.cooplapara.com.ar/blog/pdf\\_1Z12Y6169096771351.zip](http://www.cooplapara.com.ar/blog/pdf_1Z12Y6169096771351.zip)  
**Media Type:** application/executable

#### Advanced Threat Defense Results:

**MATD Hash:** 066bec76edda836ba0976485b2eb036f  
**MATD Severity:** 5  
**File Name:** pdf\_1Z12Y6169096771351\_scr.exe  
**Verdict:** Subject is malicious

#### Statistics

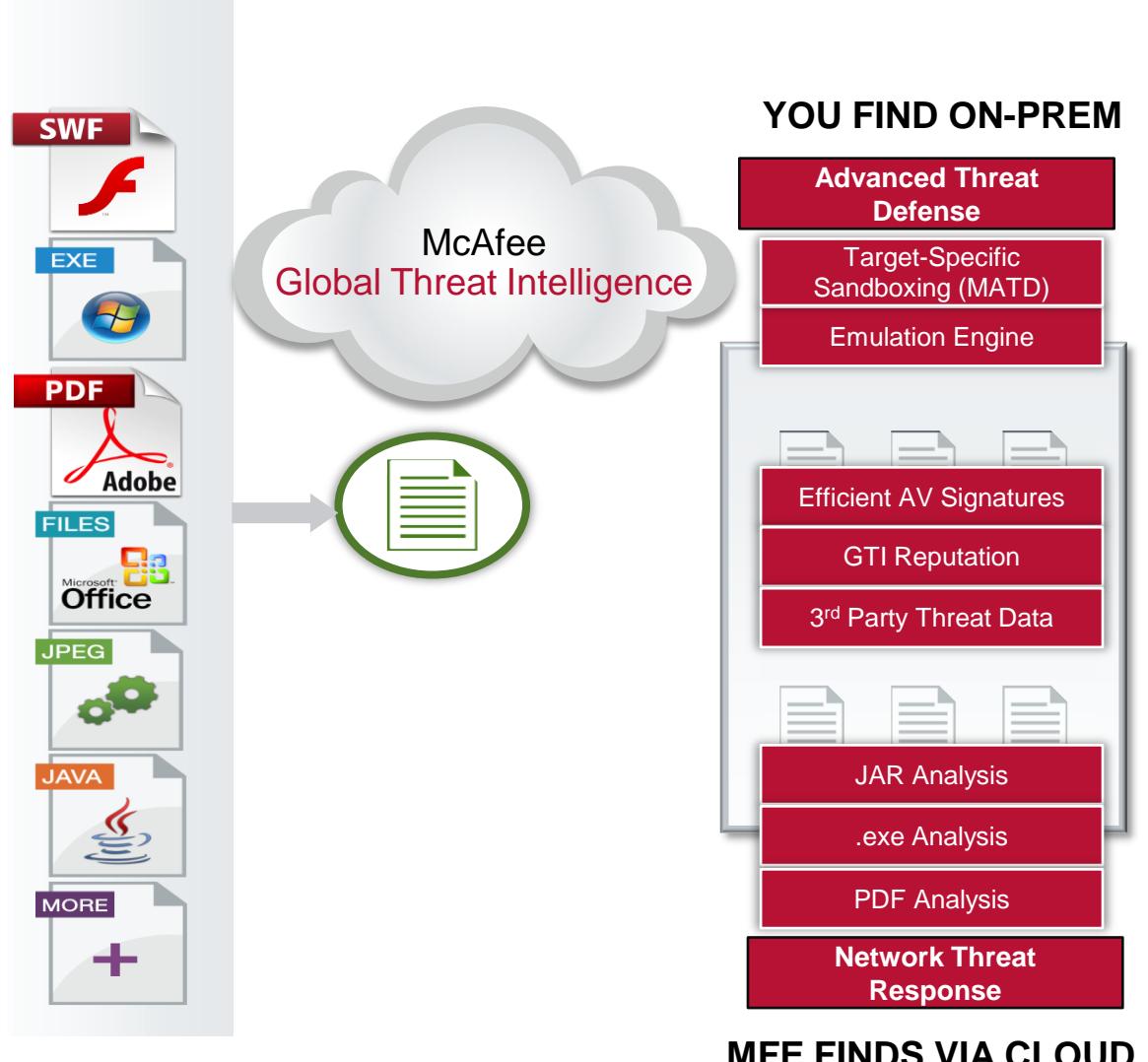
	Severity
Persistence, Installation Boot Survival	5
Hiding, Camouflage, Stealthness, Detection and Removal Protection	5
Security Solution / Mechanism bypass, termination and removal, Anti Debugging, VM Detection	3
Spreading	5
Exploiting, Shellcode	4
Networking	0
Data spying, Sniffing, Keylogging, Ebanking Fraud	5

#### Behavior

Installs itself into Appdata and behaves like Zbot  
Created active content under RECYCLER folder  
Infected Analyzer 'bait' application  
Detected active embedded content in the sample  
Obtained and used icon of legit system application  
Examined content under Analyzer temporary directory  
Deleted file(s) from the Analyzer folder  
Injects into a different process memory and changes the access protection of the committed pages  
Wrote (injected) data to an area of a foreign process memory  
Set callback function to control system and computer's hardware events  
Enumerated all running system's processes in the snapshot  
Contained long sleep  
Created named mutex object  
Created and set up new security descriptor for the running process  
Created itself in suspended state and waited for the resuming thread call  
Updated information in a system access control list (SACL)  
Changed the protection attribute of the process

# Discovering ZeroDay and Targeted Attacks

## Live Walkthrough



### WHAT'S LEARNED THROUGH EXECUTION:

Behaviors
Uses obfuscation techniques
Utilizes VM detection
Will utilize host to spread to others
Will spy on and/or record data
Indicators
Creates active content in Recycler
Embedded executable content
Grabbed approved system icon to re-use
Changes memory access protection
Set function to control system/hardware events
Changed process protection attributes
Captured all running processes for examination

# Escena 8 (Malware)

Sample Name: pdf\_efax\_5125280184.exe  
MD5 Hash Identifier: E33225864440ABE7F1CC714ABE94C5D9  
SHA-1 Hash Identifier: 009E653E28C0A2D5B2A39EE05AD7553E7BABE3DD  
File Size: 368341

Down Selector's Analysis:

Engine	GTI	File Reputation	Gateway	Anti-Malware	Anti-Malware	PDF Emulation	Sandbox	Final
Threat Name	---	---	---	---	---	---	---	---
Severity	None	None	None	None	5	5	5	5

This sample is malicious: final severity level 5

Analysis Environment: ←

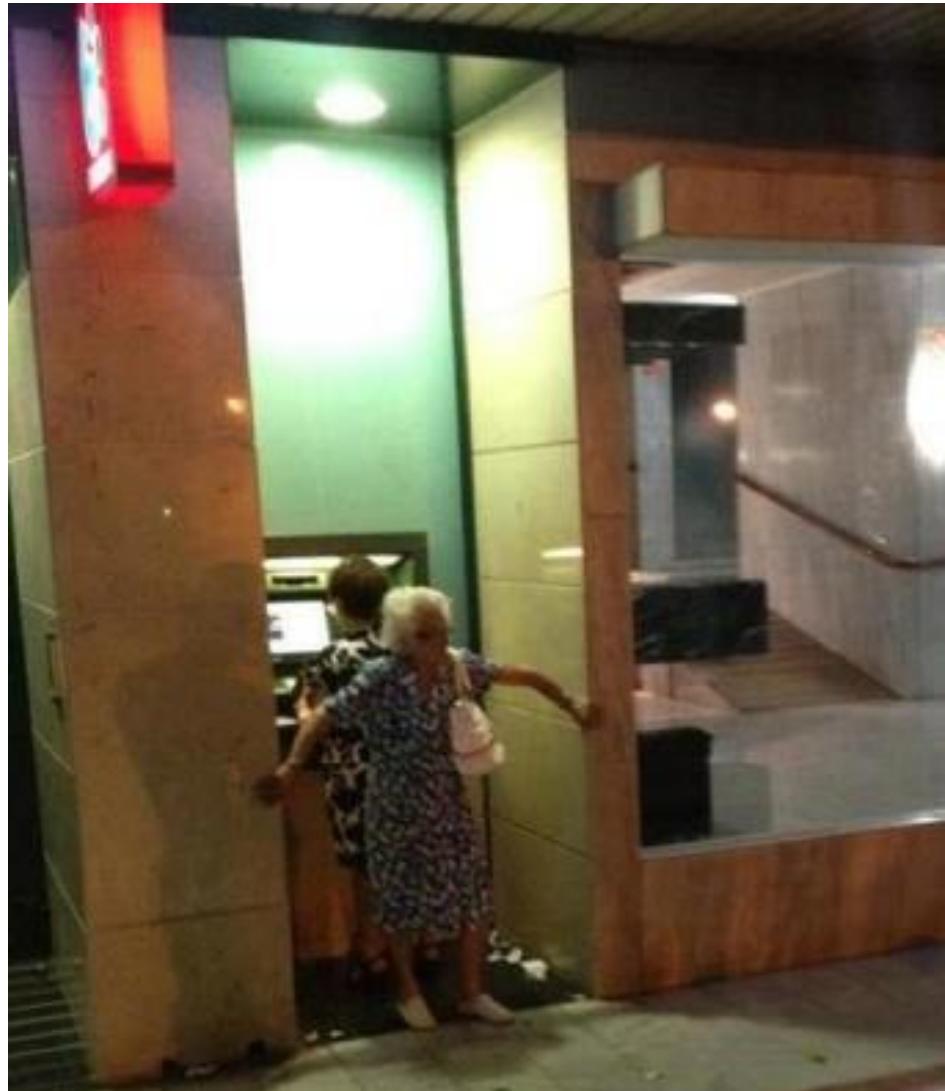
Digital Signature Verified:	unsigned
• Microsoft Windows XP Professional Service Pack 3 (build 2600)	Publisher: Not Available
• Internet Explorer version: 6	Description: egsfer
• Microsoft Office version: 2003	Product Name: Application S0
• PDF Reader version: 10	Version Info: 1 0 0 1
Sample Submitted on: 2013-09-11 12:56:24	File version: 1 0 0 1
Time Taken: 133 seconds	Strong Name: Unsigned
<b>Baitexe activated but not infected</b>	Original Name: S0.EXE
	Internal Name: S0
	Copyright: Copyright C 2013
	Comments: Not Available

Processes analyzed in this sample:

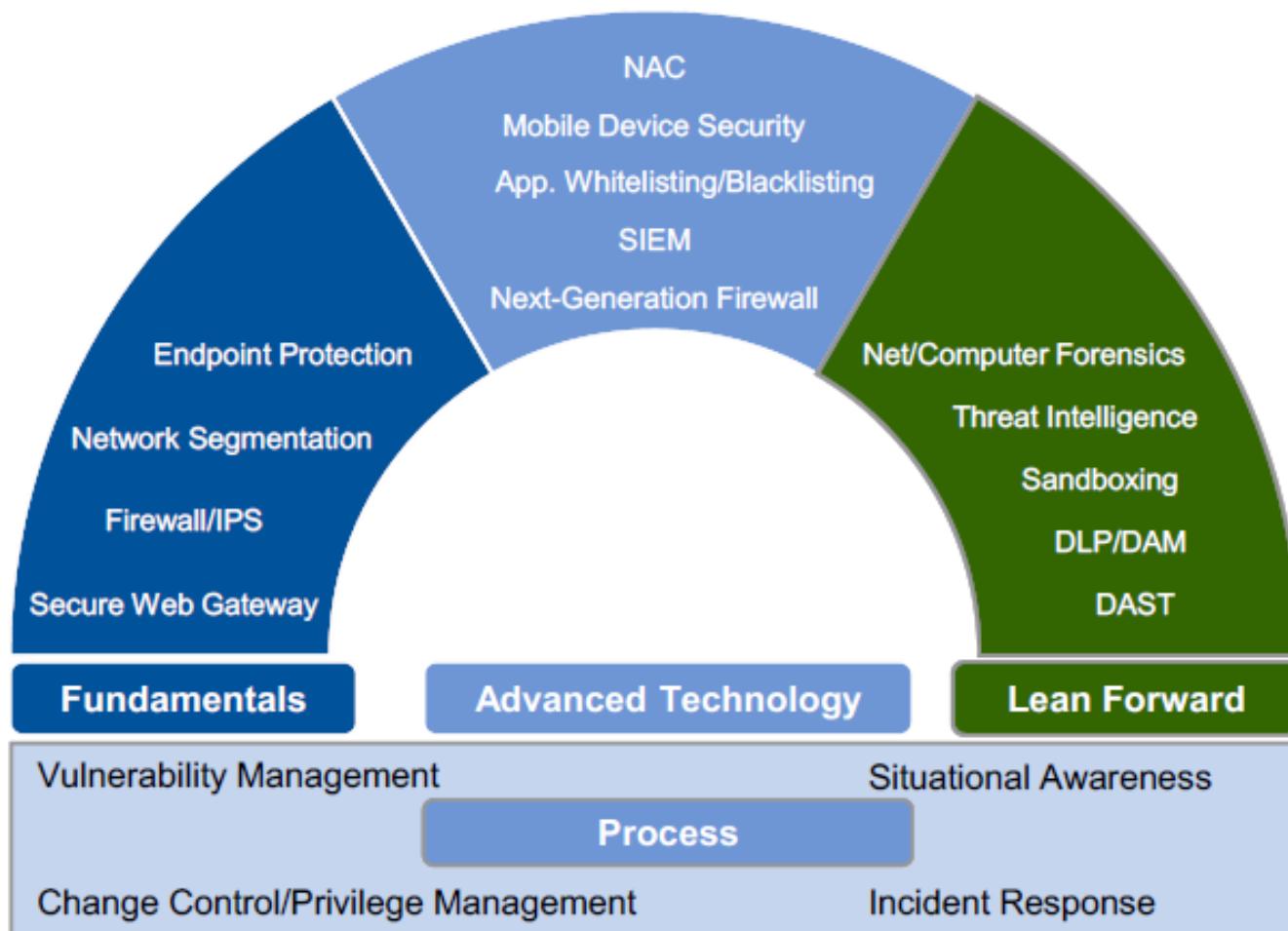


7:08 PM  
9/16/2013

# Usar los controles adecuados...



# Defending Against Targeted Attacks Requires Lean-Forward Technologies and Processes



DAM = digital asset management; DAST = dynamic application security testing; DLP = data loss prevention; IPS = intrusion prevention system; NAC = network access control; SIEM = security information and event management

Source: Gartner (June 2013)

# Global Threat Intelligence and SIEM



# Manejo de Eventos...

**Total Correlated Events**



91,488

**Total Events**



3,153,053

**Average Severity - Correlated Events**

Event Type	Average Severity
Rogue DNS Communication with ...	95
Anomalous activity after exploit	93
High Severity Events to a Suspicio...	91
Multiple scans from a local host	91
Unauthorized database access	90
Scans - Targeted	89
Off-hours Events from a Local Host	83
Multiple high severity events fro...	83
Off-hours Events to a Local Host	83
Off-hours Events from a Non-Co...	83
Off-hours Events from a Suspicio...	83
Off-hours Events from a Suspicio...	83
Off-hours Events from a Suspicio...	83
Malware sent from internal source	79

**Source IPs**

Bound to: Average Severity - C...

IP Address	Event Count
172.25.161.9	25,159
172.25.109.80	6,057
69.20.46.147	3,641
172.25.109.6	3,273
69.20.46.145	3,261

**Destination IPs**

Bound to: Average Severity - C...

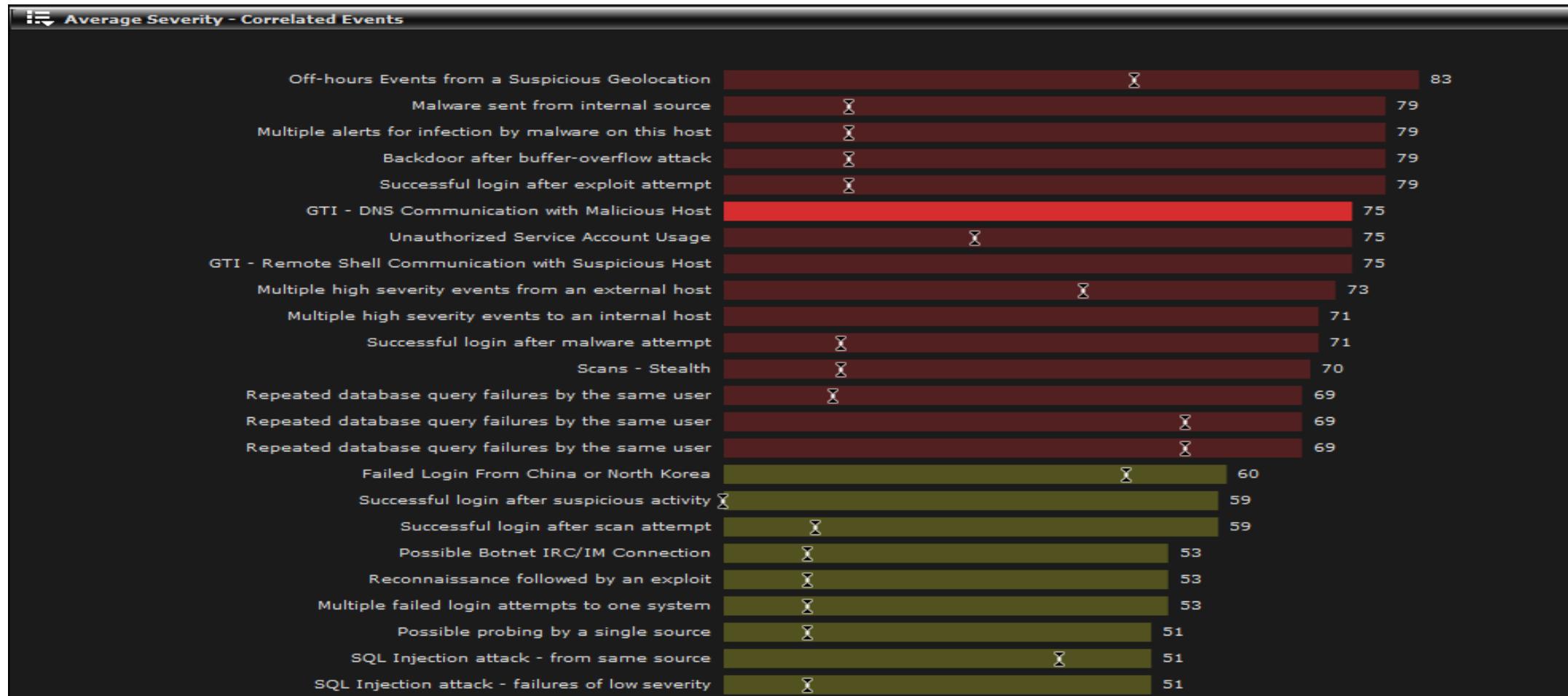
IP Address	Event Count
88.85.72.59	9,718
88.85.72.76	7,930
88.85.72.75	7,509
172.25.109.80	5,235
69.20.9.100	4,051

**Events**

Bound to: Average Severity - Correlated Events

Severity	Event Count	Source IP	Source Port	Destination IP	Destination Port	First Time	Last Time
83	1	172.25.109.6	58774	192.175.48.42	dns	06/25/2013 19:	06/25/2013 19:34:27
71	1	192.175.48.42	dns:53	172.25.109.6	58774	06/25/2013 19:	06/25/2013 19:34:27
83	1	172.25.109.6	58774	192.175.48.42	dns	06/25/2013 19:	06/25/2013 19:34:27
83	1	172.25.109.6	58774	192.175.48.42	dns	06/25/2013 19:	06/25/2013 19:34:27
73	1	192.175.48.42	dns:53	172.25.109.6	58774	06/25/2013 19:	06/25/2013 19:34:27
1400	28	172.25.161.9	2739	88.85.72.75	http:80	06/25/2013 19:	06/25/2013 19:33:32
92	1	172.25.161.181	port/type:0	..	port/code:0	06/25/2013 19:	06/25/2013 19:33:32

# Priorizar los eventos de seguridad



# De arriba hacia abajo...

Events

Bound to: Average Severity - Correlated Events

Severity	Rule Message	Event Count	Source IP	Destination IP	Protocol	Last Time	Event Subtype
75	GTI - DNS Communication with Ma	1	172.25.109.80	204.11.108.12	udp	06/25/2013 17:39:07	stop
75	GTI - DNS Communication with Ma	1	10.10.6.15	61.74.75.1	udp	06/25/2013 17:37:35	start
75	GTI - DNS Communication with Ma	1	10.10.6.15	61.74.75.1	udp	06/25/2013 17:37:35	stop
75	GTI - DNS Communication with Ma	1	172.25.109.80	194.85.61.20	udp	06/25/2013 17:34:17	stop
75	GTI - DNS Communication with Ma	1	172.25.109.80	194.85.61.20	udp	06/25/2013 17:34:17	start
75	GTI - DNS Communication with Ma	1	172.25.109.80	194.85.61.20	udp	06/25/2013 17:34:17	stop
75	GTI - DNS Communication with Ma	1	172.25.109.80	194.85.61.20	udp	06/25/2013 17:34:17	alert
75	GTI - DNS Communication with Ma	1	172.25.109.80	194.85.61.20	udp	06/25/2013 17:34:17	alert

Details Advanced Details Geolocation Description Notes Custom Types Source Events Source Flows

Events

Severity	Rule Message	Event Count	Source IP	Destination IP	Protocol	Last Time	Event Subtype
3300	McAfee_FW_Ent Session begin	44	10.10.6.15	61.74.75.1	udp	06/25/2013 17:37:35	start

Details Advanced Details Geolocation Description Notes Custom Types Packet

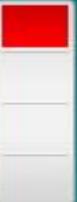
Packet Format: Auto

Find text:

```
<141>Jun 4 07:35:14 fw auditd: date="2013-06-25 22:27:51
+0000",fac=f_dns_proxy,area=a_proxy,type=t_nettraffic,pri=p_major,pid=2008,logid=0,cmd=dnspr,hostname=fw.stp-
lab.com,event="session
begin",netsessid=a2dc951add0f2,srcip=10.10.6.15,srcport=54108,srczone=internal,protocol=17,dst_geo=US,dstip=61.74.75.1,dstp-
ort=53,dstzone=external,rule_name="Port 53 wide open",cache_hit=1,start_time="2013-06-25 22:27:51 +0000",application=DNS
```

# Si bueno, con quién hablo?

Email Reputation Web Reputation

High Risk 

Medium Risk 

Unverified 

Minimal Risk 

**61.74.75.1**

This page shows details and results of our analysis on the IP address 61.74.75.1

**Threat Detail**

Location:  Hostname: Domain:

**Next Steps:** [Search Again](#) [View All Threats](#) [Sign Up for McAfee Labs Security Advisories](#) [Threat Feedback](#)

► Overview

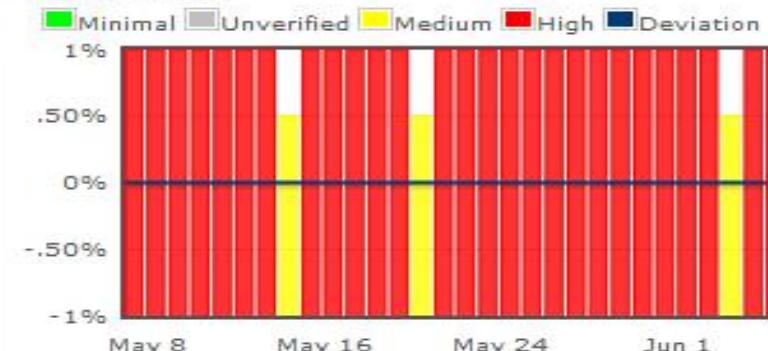
[Intrusion Attacks](#)

[Associated Domains](#)

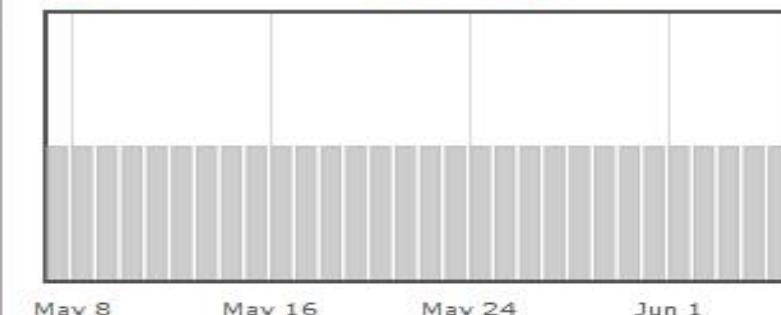
[Neighboring IP Addresses](#)

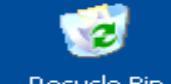
This page shows information on the IP address's email and web reputations, location, registration, associations, activities, and threats.

**Daily Trend of IP Mail Volume Change and Reputation**



**Daily Trend Web Reputation**





Recycle Bin



temp



WindowsXP-KB  
835935-SP2-E  
NU



WindowsXP-...

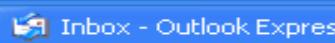
User on WinXPHost01  
downloads “Windows update”  
from fake site. Executes it,  
nothing sinister appears.



start



Windows Task Manager



Inbox - Outlook Express



temp





**Physical Display**

**Events and Hosts Summary**

**Summary**

10,045 (100%)

- McAfee\_FW\_Ent Session begin ...
- McAfee\_FW\_Ent Net traffic - Session end ...
- Possible probing by a single source ...
- Multiple high severity events from an internal host ...
- Malware sent from internal source 4
- BACKDOOR: Back Orifice Trojan 4
- Infected file deleted 4
- ICMP: Netmask Request 2
- ICMP: Timestamp Probe 2
- Update successful 2
- TCP: SYN Port Scan 1
- Trojan: Poison Ivy traffic detected 1
- Access Protection rule violation detected and not blocked 1

**Event Source IPs**

Bound to: Summary 10,045 (100%)

- winxphost01.stp-lab.com 10,029
- epo01.stp-lab.com 13
- www.killerbean.com 1
- Others 2

Meanwhile, we start to see a number of potentially malicious events related to this host on McAfee ESM.

**Events**

Bound to: Event Destination IPs

Severity	Rule Message	Eve...	Source IP	Destination IP	Protocol	Last Time	Event Su
70	Trojan: Poison Ivy traffic detected	1	winxphost01.stp-lab.com	winxphost01.stp-lab.com	n/a	02/03/2013 21:33:35	alert
75	McAfee_FW_Ent Session begin	1	winxphost01.stp-lab.com	winxphost01.stp-lab.com	n/a	02/03/2013 21:27:00	alert
1530	Possible probing by a single source	3	winxphost01.stp-lab.com	winxphost01.stp-lab.com	n/a	02/03/2013 21:24:56	alert
70	Trojan: Poison Ivy traffic detected	1	www.killerbean.com	winxphost01.stp-lab.com	n/a	02/03/2013 21:22:09	alert
75	McAfee_FW_Ent Session begin	1	winxphost01.stp-lab.com	www.killerbean.com	tcp	02/03/2013 21:08:14	start
1530	Possible probing by a single source	30	winxphost01.stp-lab.com	www.killerbean.com	tcp	02/03/2013 21:07:14	reject
2250	McAfee_FW_Ent Net traffic - Session end	30	winxphost01.stp-lab.com	www.killerbean.com	tcp	02/03/2013 21:07:14	reject
2250	McAfee_FW_Ent Session begin	30	winxphost01.stp-lab.com	www.killerbean.com	tcp	02/03/2013 21:07:13	start
2025	McAfee_FW_Ent Net traffic - Session end	27	winxphost01.stp-lab.com	www.killerbean.com	tcp	02/03/2013 20:56:52	reject





**Physical Display**

**Events and Hosts Summary**

**Summary**

- McAfee\_FW\_Ent Session begin 10,080 (100%)
- McAfee\_FW\_Ent Net traffic - Session end 3,743
- Possible probing by a single source 3,739
- Multiple high severity events from an internal host 1,888
- Infected file deleted 656
- Access Protection rule violation detected and not blocked 29
- File infected - Undetermined 5
- TCP: SYN Port Scan 1
- Trojan: Poison Ivy traffic detected 1

**Event Source IPs**

IP Address	Count
10.10.100.7	10,064
epo01.stp-lab.com	13
www.killerbean.com	1
Others	2

**Event Destination IPs**

IP Address	Count
www.killerbean.com	10,006
10.10.100.7	52
64-129-104-159.static.twteleco...	12
157.55.240.221	4
8.18.25.6	2
65.55.27.220	2

**Events**

Bound to: Event Destination IPs

Severity	Rule Message	Eve...	Source IP	Destination IP	Protocol	Last Time	Event Su...
70	Trojan: Poison Ivy traffic detected	1	www.killerbean.com	10.10.100.7	n/a	02/03/2013 21:22:09	alert
75	McAfee_FW_Ent Session begin	1	10.10.100.7	www.killerbean.com	tcp	02/03/2013 21:08:14	start
2250	McAfee_FW_Ent Net traffic - Session end	30	10.10.100.7	www.killerbean.com	tcp	02/03/2013 21:07:14	reject
1530	Possible probing by a single source	30	10.10.100.7	www.killerbean.com	tcp	02/03/2013 21:07:14	reject
2250	McAfee_FW_Ent Session begin	30	10.10.100.7	www.killerbean.com	tcp	02/03/2013 21:07:13	start
2241	Multiple high severity events from an inter...	27	10.10.100.7	www.killerbean.com	tcp	02/03/2013 20:56:52	reject
2025	McAfee_FW_Ent Net traffic - Session end	27	10.10.100.7	www.killerbean.com	tcp	02/03/2013 20:56:52	reject
2025	McAfee_FW_Ent Session begin	27	10.10.100.7	www.killerbean.com	tcp	02/03/2013 20:56:51	start
2325	McAfee_FW_Ent Net traffic - Session end	31	10.10.100.7	www.killerbean.com	tcp	02/03/2013 20:47:27	reject

**Step 1: This external host looks suspicious. Let's blacklist him.**





**Physical Display**

**Events and Hosts Summary**

**Summary**

10,080 (100%)

- McAfee\_FW\_Ent Session begin 3,743
- McAfee\_FW\_Ent Net traffic - Session end 3,739
- Possible probing by a single source 1,888
- Multiple high severity events from an internal host 656
- Infected file deleted 29
- Access Protection rule violation detected and not blocked 5
- Malware sent from internal source 4
- BACKDOOR: Back Orifice Trojan 4
- ICMP: Netmask Request 2
- ICMP: Timestamp Probe 2
- File infected - Undetermined clean error, deleted succe... 2
- Update successful 2
- TCP: SYN Port Scan 1
- Trojan: Poison Ivy traffic detected 1

**Event Source IPs**

Bound to: Summary 10,080 (100%)

- 10.10.100.7 10,064
- epo01.stp-lab.com 13
- www.killerbean.com 1
- Others 2

**Event Destination IPs**

10,006 (99.27%)

- Event Drilldown > 10,006
- Flow Drilldown > 10,006
- Asset Drilldown > 52
- Summarize > 12
- Actions > 240.221
- WHOIS Lookup > 4
- Blacklist 63.228.1.2 > 2
- Search ELM > 2

**Events**

Bound to: Event Destination IPs

Severity	Rule Message	Event ID	Source IP	Destination IP	Protocol	Last Time	Event Source IP
75	McAfee_FW_Ent Session begin	1	10.10.100.7	www.killerbean.com	tcp	02/03/2013 21:08:14	start
1530	Possible probing by a single source	30	10.10.100.7	www.killerbean.com	tcp	02/03/2013 21:07:14	reject
2250	McAfee_FW_Ent Net traffic - Session end	30	10.10.100.7	www.killerbean.com	tcp	02/03/2013 21:07:14	reject
2250	McAfee_FW_Ent Session begin	30	10.10.100.7	www.killerbean.com	tcp	02/03/2013 21:07:13	start
2241	Multiple high severity events from an inter...	27	10.10.100.7	www.killerbean.com	tcp	02/03/2013 20:56:52	reject
2025	McAfee_FW_Ent Net traffic - Session end	27	10.10.100.7	www.killerbean.com	tcp	02/03/2013 20:56:52	reject
2025	McAfee_FW_Ent Session begin	27	10.10.100.7	www.killerbean.com	tcp	02/03/2013 20:56:51	start
1581	Possible probing by a single source	31	10.10.100.7	www.killerbean.com	tcp	02/03/2013 20:47:27	reject
2325	McAfee_FW_Ent Net traffic - Session end	31	10.10.100.7	www.killerbean.com	tcp	02/03/2013 20:47:27	reject

**Contextual Menu (Right-clicked on Blacklist 63.228.1.2)**

- Event Drilldown
- Flow Drilldown
- Asset Drilldown
- Summarize
- Actions
- WHOIS Lookup
- Blacklist 63.228.1.2
- Search ELM
- Export
- Delete
- Mark as reviewed



**Physical Display**

**Events and Hosts Summary**

**Summary**

- McAfee\_FW\_Ent Session begin 10,080 (100%) 3,743
- McAfee\_FW\_Ent Net traffic - Session end 3,739
- Possible probing by a single source 1,888
- Multiple high severity events from an internal host
- Infected file deleted
- Access Protection rule violation detected and not blocked
- Malware sent from internal source
- BACKDOOR: Back Orifice Trojan
- ICMP: Netmask Request
- ICMP: Timestamp Probe
- File infected - Undetermined clean error, deleted successfully
- Update successful
- TCP: SYN Port Scan
- Trojan: Poison Ivy traffic detected

**Event Source IPs**

Bound to: Summary 10,080 (100%)

IP Address	Count
10.10.100.7	10,064
epo01.stp-lab.com	13
www.killerbean.com	1
Others	2

**Device List**

Select the device to which you want to apply the blacklist setting.

Global Blacklist

stpaul1450

**Destination IPs**

Source IPs 10,006 (99.27%)

IP Address	Count
www.killerbean.com	10,006
10.10.100.7	52
59.static.twteleco...	12
157.55.240.221	4
8.18.25.6	2
65.55.27.220	2

**Events**

Bound to: Event Destination IPs

Severity	Rule Message	Event ID	Source IP	Destination IP	Protocol	Last Time	Event Sub
75	McAfee_FW_Ent Session begin	1	10.10.100.7	www.killerbean.com	tcp	02/03/2013 21:08:14	start
1530	Possible probing by a single source	30	10.10.100.7	www.killerbean.com	tcp	02/03/2013 21:07:14	reject
2250	McAfee_FW_Ent Net traffic - Session end	30	10.10.100.7	www.killerbean.com	tcp	02/03/2013 21:07:14	reject
2250	McAfee_FW_Ent Session begin	30	10.10.100.7	www.killerbean.com	tcp	02/03/2013 21:07:13	start
2241	Multiple high severity events from an internal host	27	10.10.100.7	www.killerbean.com	tcp	02/03/2013 20:56:52	reject
2025	McAfee_FW_Ent Net traffic - Session end	27	10.10.100.7	www.killerbean.com	tcp	02/03/2013 20:56:52	reject
2025	McAfee_FW_Ent Session begin	27	10.10.100.7	www.killerbean.com	tcp	02/03/2013 20:56:51	start
1581	Possible probing by a single source	31	10.10.100.7	www.killerbean.com	tcp	02/03/2013 20:47:27	reject
2325	McAfee_FW_Ent Net traffic - Session end	31	10.10.100.7	www.killerbean.com	tcp	02/03/2013 20:47:27	reject

**McAfee® | Enterprise Security Manager**

admin | options | help

Physical Display NSM Sensor Properties

Sensor: stpaul1450

Include Global Blacklist

IP Address	Duration	Description

Add Edit Delete

Add NSM Blacklist Entry

IP Address: 63.228.1.2

Duration: 15 minutes

Description: Suspected PoisonIvy C&C Server

OK Cancel

Possible probing by a single source

10.10.100.7

www.kitterbean.com

tcp

02/03/2013 20:47:27

reject

Close



#### **Physical Display**

## **NSM Sensor Properties**

Sensor: stpaul1450

#### Include Global Blacklist

IP Address	Duration	Description
63.228.1.2	02/07/2013 13:15:38	Suspected PoisonIvy C&C Server

Add

Edit

## Delete

**Close**



All Hosts

Display Filtering ▾

/ All Hosts

 Detail View Group By

Current User

Session St...	1 IP Addr...	Host Name	Network Access Zo...	State	Health Le...	Current User
02/07 13:11:52	63.228.1.2	---	---	IPS Quarantined	---	---

Quarantine successfully  
implemented through the McAfee  
NSM. Link to C&C host blocked.



**Physical Display**

**Events and Hosts Summary**

**Summary**

- McAfee\_FW\_Ent Session begin 10,045 (100%)
- McAfee\_FW\_Ent Net traffic - Session end ...
- Possible probing by a single source ...
- Multiple high severity events from an internal host ...
- Malware sent from internal source 4

**Event Source IPs**

- Event Drilldown
- Flow Drilldown
- Asset Drilldown
- Summarize
- Actions
- WHOIS Lookup
- Blacklist 10.10.100.7
- Search ELM
- Export
- Delete
- Mark as reviewed
- 13 10,029 (99.84%)
- 13 10,029
- Create new watchlist
- Append to watchlist
- Create new alarm
- Perform MVM Scan
- View in ePO 10,031 (100%)
- ePO Tagging 10,006
- aleco... 12
- winxphost01.stp-lab.com 5
- 157.55.240.221 4
- 65.55.27.220 2
- Others 2

**Access P**

**Events**

Bound to: Event Destination IPs

Severity	Rule Message	Eve...	Source IP	Destination IP	Protocol	Last Time	Event Su
70	Trojan: Poison Ivy traffic detected	1	winxphost01.stp-lab.com	winxphost01.stp-lab.com	n/a	02/03/2013 21:33:35	alert
75	McAfee_FW_Ent Session begin	1	winxphost01.stp-lab.com	winxphost01.stp-lab.com	n/a	02/03/2013 21:27:00	alert
1530	Possible probing by a single source	3	winxphost01.stp-lab.com	winxphost01.stp-lab.com	n/a	02/03/2013 21:24:56	alert
75	McAfee_FW_Ent Session begin	1	winxphost01.stp-lab.com	www.killerbean.com	tcp	02/03/2013 21:08:14	start
1530	Possible probing by a single source	30	winxphost01.stp-lab.com	www.killerbean.com	tcp	02/03/2013 21:07:14	reject
2250	McAfee_FW_Ent Net traffic - Session end	30	winxphost01.stp-lab.com	www.killerbean.com	tcp	02/03/2013 21:07:14	reject
2250	McAfee_FW_Ent Session begin	30	winxphost01.stp-lab.com	www.killerbean.com	tcp	02/03/2013 21:07:13	start
2025	McAfee_FW_Ent Net traffic - Session end	27	winxphost01.stp-lab.com	www.killerbean.com	tcp	02/03/2013 20:56:52	reject
2241	Multiple high severity events from an inter	27	winxphost01.stp-lab.com	www.killerbean.com	tcp	02/03/2013 20:56:52	reject

**Step 2:** This internal endpoint appears to have been compromised. From McAfee ESM we can lock it down and scan it immediately through ePO.

**Events**

Bound to: Event Destination IPs

Severity	Rule Message	Eve...	Source IP	Destination IP	Protocol	Last Time	Event Su
70	Trojan: Poison Ivy traffic detected	1	winxphost01.stp-lab.com	winxphost01.stp-lab.com	n/a	02/03/2013 21:33:35	alert
75	McAfee_FW_Ent Session begin	1	winxphost01.stp-lab.com	winxphost01.stp-lab.com	n/a	02/03/2013 21:27:00	alert
1530	Possible probing by a single source	3	winxphost01.stp-lab.com	winxphost01.stp-lab.com	n/a	02/03/2013 21:24:56	alert
75	McAfee_FW_Ent Session begin	1	winxphost01.stp-lab.com	www.killerbean.com	tcp	02/03/2013 21:08:14	start
1530	Possible probing by a single source	30	winxphost01.stp-lab.com	www.killerbean.com	tcp	02/03/2013 21:07:14	reject
2250	McAfee_FW_Ent Net traffic - Session end	30	winxphost01.stp-lab.com	www.killerbean.com	tcp	02/03/2013 21:07:14	reject
2250	McAfee_FW_Ent Session begin	30	winxphost01.stp-lab.com	www.killerbean.com	tcp	02/03/2013 21:07:13	start
2025	McAfee_FW_Ent Net traffic - Session end	27	winxphost01.stp-lab.com	www.killerbean.com	tcp	02/03/2013 20:56:52	reject
2241	Multiple high severity events from an inter	27	winxphost01.stp-lab.com	www.killerbean.com	tcp	02/03/2013 20:56:52	reject





**Physical Display**

**Events and Hosts Summary**

**Summary**

Select tags and enter an IP address to apply the tags to that endpoint.

Name	Notes
Server	Default tag for systems identified as a Server
Workstation	Default tag for systems identified as a Workstation
Policy: Lockdown System	Deploys restrictive lockdown policies for HIPS
Task: Full AV Scan	Run deep anti-malware scan. No exclusions.
Test Tag	Tag for Testing
Task: Deploy Advanced C	Triggers deployment of Application Whitelisting (App Control) and anti-rootkit (Deep Defender) technology.

**Event Source IPs**

0,029 (99.84%)  
10,029

10,031 (100%)  
10,006

**Access Protection**

**Events**

Bound to: Event D

Severity	Rule Name
70	Trojan
75	McAfee
1530	Poss
75	McAfee
1530	Possible probing by a single source
2250	McAfee_FW_Ent Net traffic - Session end
2250	McAfee_FW_Ent Session begin
2025	McAfee_FW_Ent Net traffic - Session end
2241	Multiple high severity events from an inter

IP address to assign the selected tags: 10.10.100.7  Wake up client

Assign the selected tags

**Event Summary**

Event ID	Event Type
35	alert
30	alert
56	alert
14	start
	reject
	reject
	start
	reject
	reject

**Close**



Recycle Bin



temp



WindowsXP...



WindowsXP...

**McAfee Host Intrusion Prevention**

Task Edit View Help

IIPS Policy Firewall Policy Blocked Hosts Application Protection List Activity Log

Use this tab to enable

Enabled

Learn Mode

Incoming

Outgoing

+ Allow ARP Rule

+ Allow EAPOL

+ Trusted Applications (Trusted for firewall)

+ McAfee Agent Communication

+ Allow McAfee signed applications

+ ePolicy Orchestrator Server

+ VPN

+ Allow Agent-to-Server Communication

+ Ping and ICMP

+ Allow 802.1X Authentication

+ Allow bootp

+ Allow DNS

+ Allow Net Time Protocol

+ NetBIOS Group

Allow All traffic

Properties... Duplicate Remove Add... Apply

Firewall is disabled - all traffic is allowed

A red callout box points from the text "Looking at the endpoint, we see that the firewall started off disabled." to the "Enabled" checkbox in the Firewall Policy tab.



Windows Task Manager

Inbox - Outlook Express

temp

McAfee Host Intrusio...





Recycle Bin



temp



WindowsXP...



WindowsXP...

**McAfee Host Intrusion Prevention**

Task Edit View Help

IPS Policy Firewall Policy **Blocks**

Use this tab to enable or disable specific traffic types.

Enabled

Learn Mode

Incoming

Outgoing

+ Allow ARP

+ Allow EAPOL

+ Trusted Applications (Trusted for firewall)

+ McAfee Agent Communication

+ TrustedSource - Allow Host IPS Service

+ TrustedSource - Get Rating

+ IP Spoof

+ Allow DNS

+ Allow McAfee signed applications

+ Allow RDP

- Block All

- Block All Traffic

Properties... Duplicate Remove Add... Apply

Firewall is enabled

ePO enables the firewall with a restrictive policy.  
The Trojan is contained on the endpoint.



Windows Task Manager

Inbox - Outlook Express

temp

McAfee Host Intrusio...





Recycle Bin



temp



WindowsXP...



WindowsXP...

VirusScan Console

Task Edit View Tools Help

Task Status Last Result Last Run

Task	Status	Last Result	Last Run
Access Protection	Enabled		
Buffer Overflow Protection	Enabled		
On-Delivery Email Scanner	Enabled		
Unwanted Programs Policy	8 unwanted program ...		
On-Access Scanner	Enabled		
Quarantine Manager Policy	The quarantine folder ...		
Full Scan	Not Scheduled		
Targeted Scan	Not Scheduled		
AutoUpdate	Daily, 5:00 PM	The Update succeeded	Sunday, February 03,...
(managed) Full AV Scan - No Exceptions	Running...		
(managed) Update Task	Daily, 5:00 AM		

IPS Policy U: Enabled

Le

Properties... Duplicate Remove Add... Apply

Firewall is enabled

Simultaneously, ePO launches an aggressive scan.



Windows Task Manager

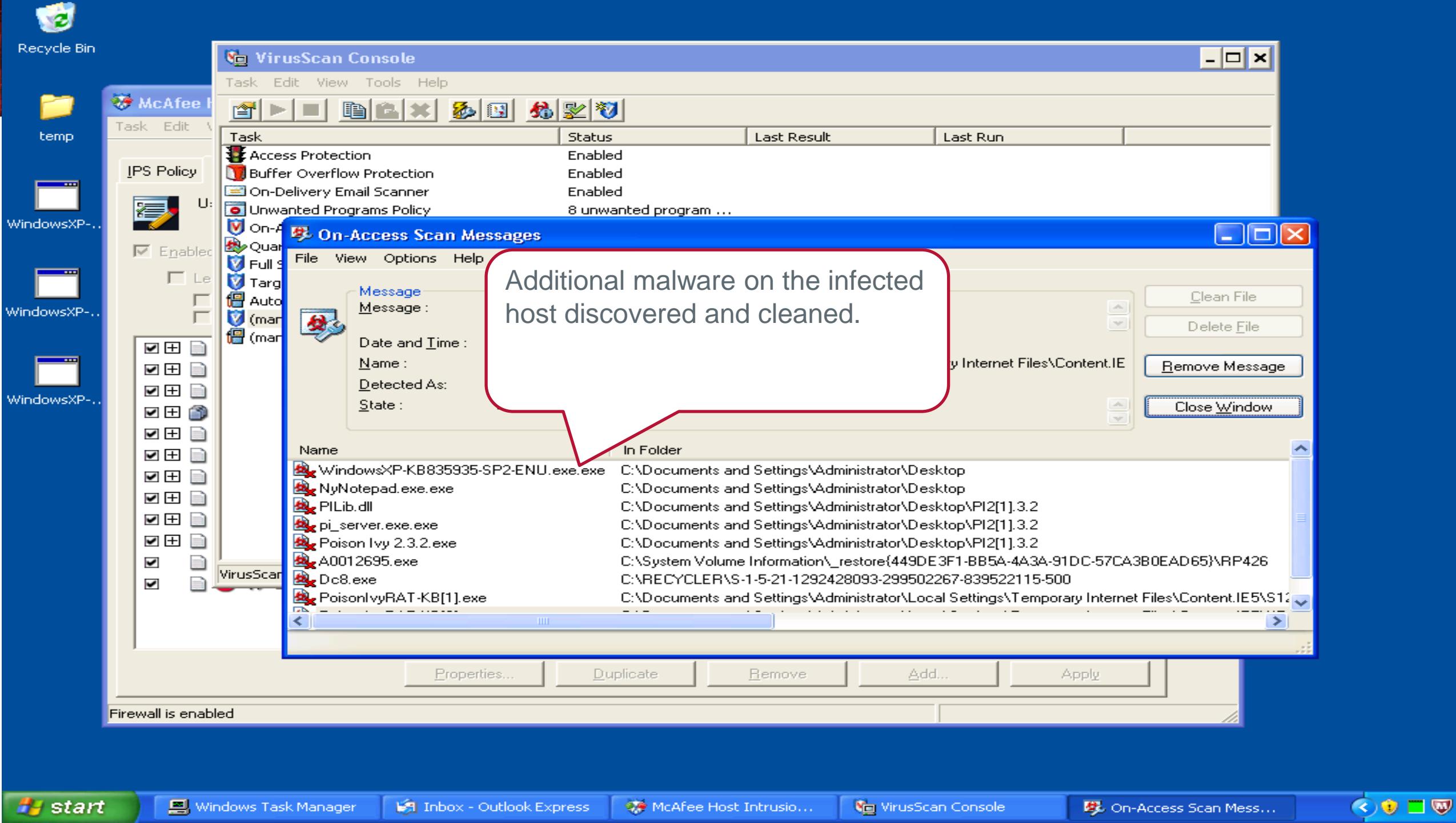
Inbox - Outlook Express

temp

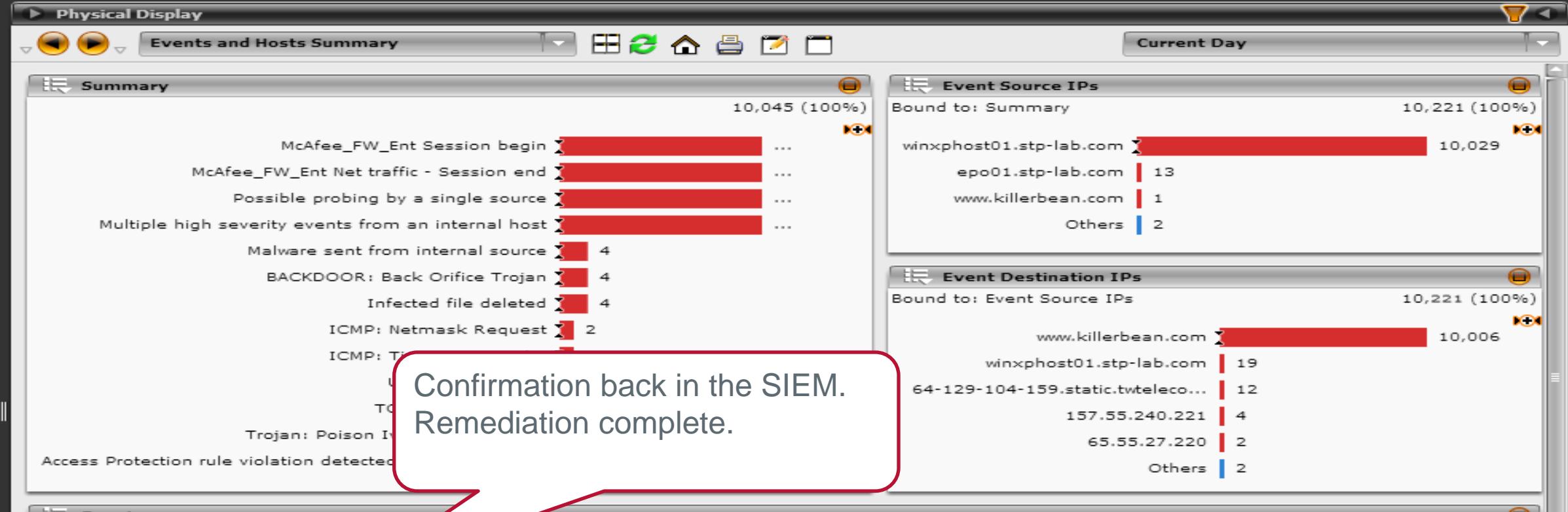
McAfee Host Intrusio...

VirusScan Console





Additional malware on the infected host discovered and cleaned.



**Events**

Bound to: Event Destination IPs

Severity	Rule Message	Eve...	Source IP	Destination IP	Protocol	Last Time	Event Su
10	Infected file deleted	1	winxphost01.stp-lab.com	winxphost01.stp-lab.com	n/a	02/03/2013 21:33:35	alert
50	Access Protection rule violation detected ar	1	winxphost01.stp-lab.com	winxphost01.stp-lab.com	n/a	02/03/2013 21:27:00	alert
30	Infected file deleted	3	winxphost01.stp-lab.com	winxphost01.stp-lab.com	n/a	02/03/2013 21:24:56	alert
50	Access Protection rule violation detected ar	1	winxphost01.stp-lab.com	winxphost01.stp-lab.com	n/a	02/03/2013 21:22:09	alert
30	Infected file deleted	3	winxphost01.stp-lab.com	winxphost01.stp-lab.com	tcp	02/03/2013 21:08:14	start
1530	Possible probing by a single source	30	winxphost01.stp-lab.com	www.killerbean.com	tcp	02/03/2013 21:07:14	reject
2250	McAfee_FW_Ent Net traffic - Session end	30	winxphost01.stp-lab.com	www.killerbean.com	tcp	02/03/2013 21:07:14	reject
2250	McAfee_FW_Ent Session begin	30	winxphost01.stp-lab.com	www.killerbean.com	tcp	02/03/2013 21:07:13	start
2025	McAfee_FW_Ent Net traffic - Session end	27	winxphost01.stp-lab.com	www.killerbean.com	tcp	02/03/2013 20:56:52	reject



Comprehensive  
malware protection,  
**only available from McAfee**,  
is an orchestrated approach  
to protect against malware.



SAFE NEVER SLEEPS™