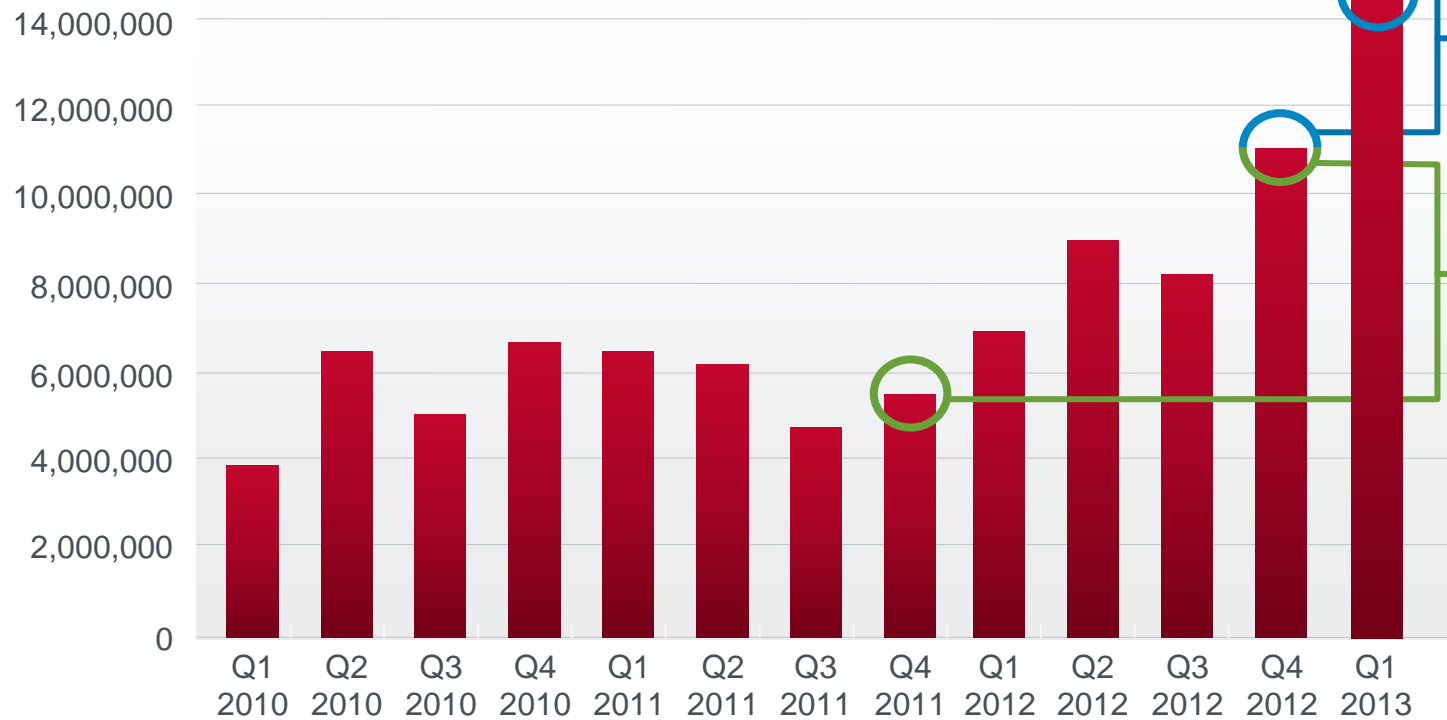


Conectando las piezas para mitigar el riesgo

Jorge Herrerías, CISSP
Sales System Engineer

128M Total Malware Samples in the McAfee Labs Database

New Malware Samples



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.

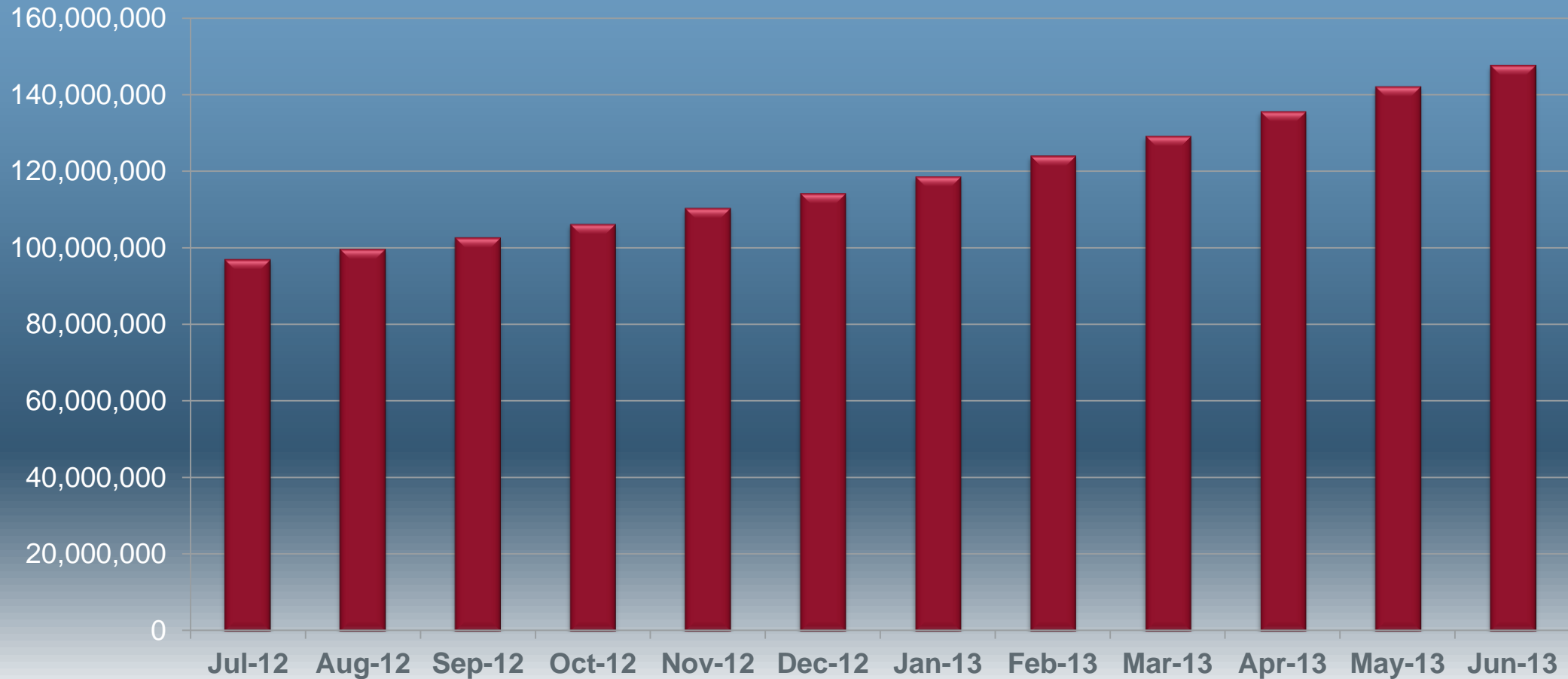
New Ransomware Samples

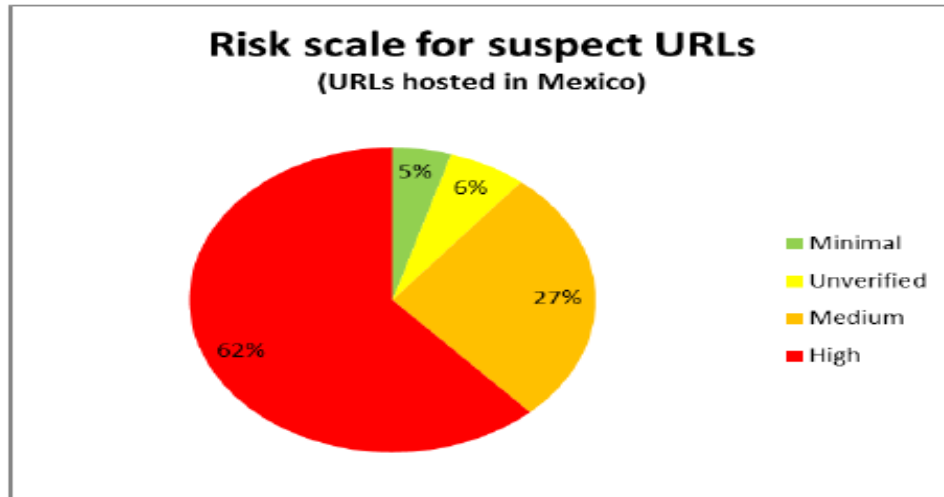


Total Malware Samples

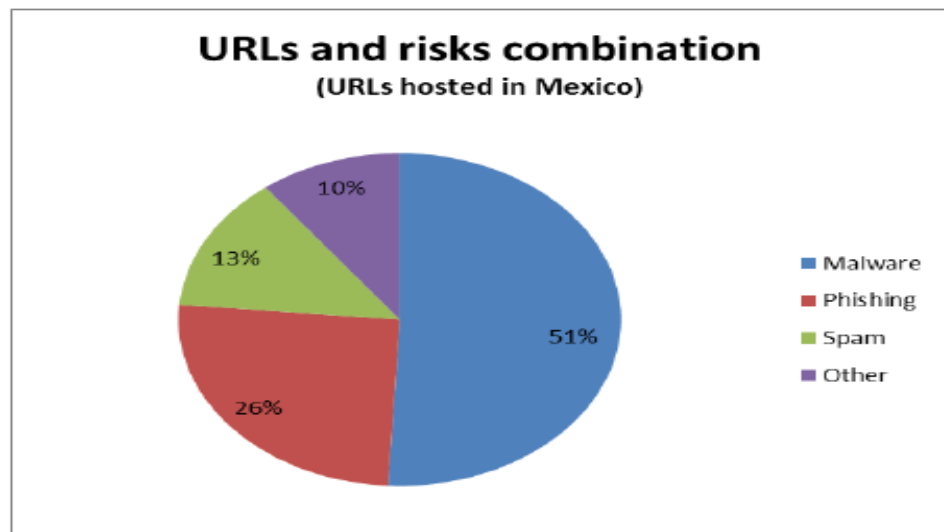
The McAfee “zoo” now contains more than 140 million unique malware samples.

Total Malware Samples





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

GLOBAL THREAT INTELLIGENCE

- Web Activity
- DNS Server
- Protocol/Port
- Web Reputation
- File Reputation
- URL
- IP Address
- Affiliations
- Sender Reputation
- Application
- Domain(s)
- Data Activity
- Mail Activity
- Network Activity
- Email Address



Comprehensive Malware Protection

Second Layer of Defense: McAfee Advanced Threat Defense

GLOBAL THREAT INTELLIGENCE

- Web Activity
- DNS Server
- Protocol/Port
- File Reputation
- URL
- IP Address
- Affiliations
- Sender Reputation
- Application
- Domain(s)
- Data Activity
- Network Activity
- Mail Activity
- Email Address



Network
Anti Malware

Comprehensive Malware Protection

Third Layer of Defense:
Network Threat Protection

GLOBAL THREAT INTELLIGENCE

- Web Activity
- DNS Server
- Protocol/Port
- Web Reputation
- File Reputation
- URL
- IP Address
- Affiliations
- Sender Reputation
- Application
- Domain(s)
- Data Activity
- Network Activity
- Mail Activity
- Email Address



Comprehensive Malware Protection

Fourth Layer of Defense:
Comprehensive Endpoint
Threat Defense



Comprehensive Malware Protection

Fifth layer of defense:
Real Time Endpoint Awareness



GLOBAL THREAT INTELLIGENCE

- Web Activity
- Web Reputation
- File Reputation
- Protocol/Port
- Affiliations
- Sender Reputation
- Data Activity
- Application
- URL
- IP Address
- Domain(s)
- Mail Activity
- Network Activity
- Email Address



Comprehensive Malware Protection

Sixth Layer of Defense:
Heal Endpoints

GLOBAL THREAT INTELLIGENCE

- Web Activity
- DNS Server
- Protocol/Port
- Web Reputation
- File Reputation
- URL
- IP Address
- Affiliations
- Sender Reputation
- Application
- Domain(s)
- Data Activity
- Mail Activity
- Network Activity
- Email Address



Comprehensive Malware Protection

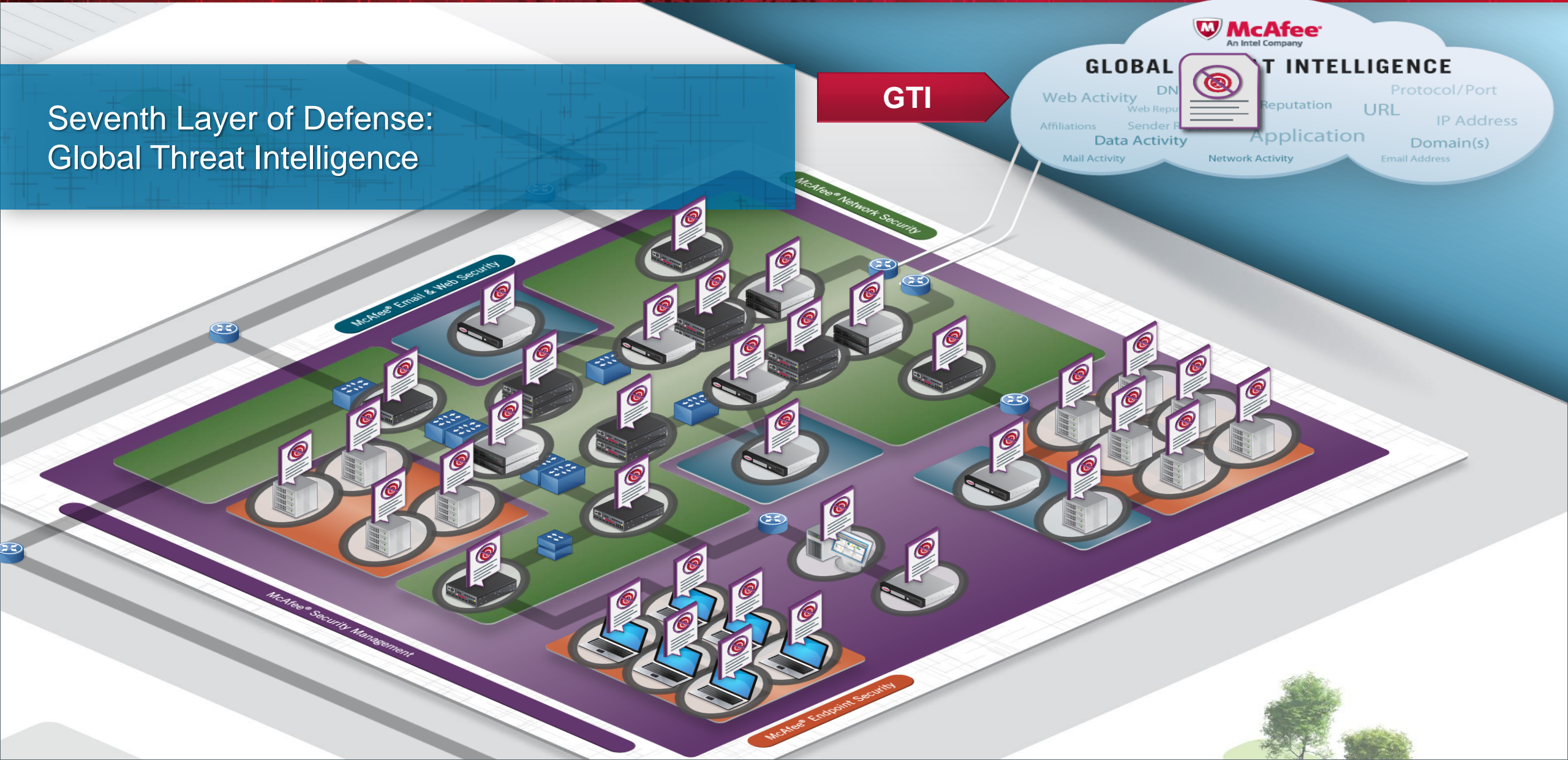
Seventh Layer of Defense: Global Threat Intelligence

GTI

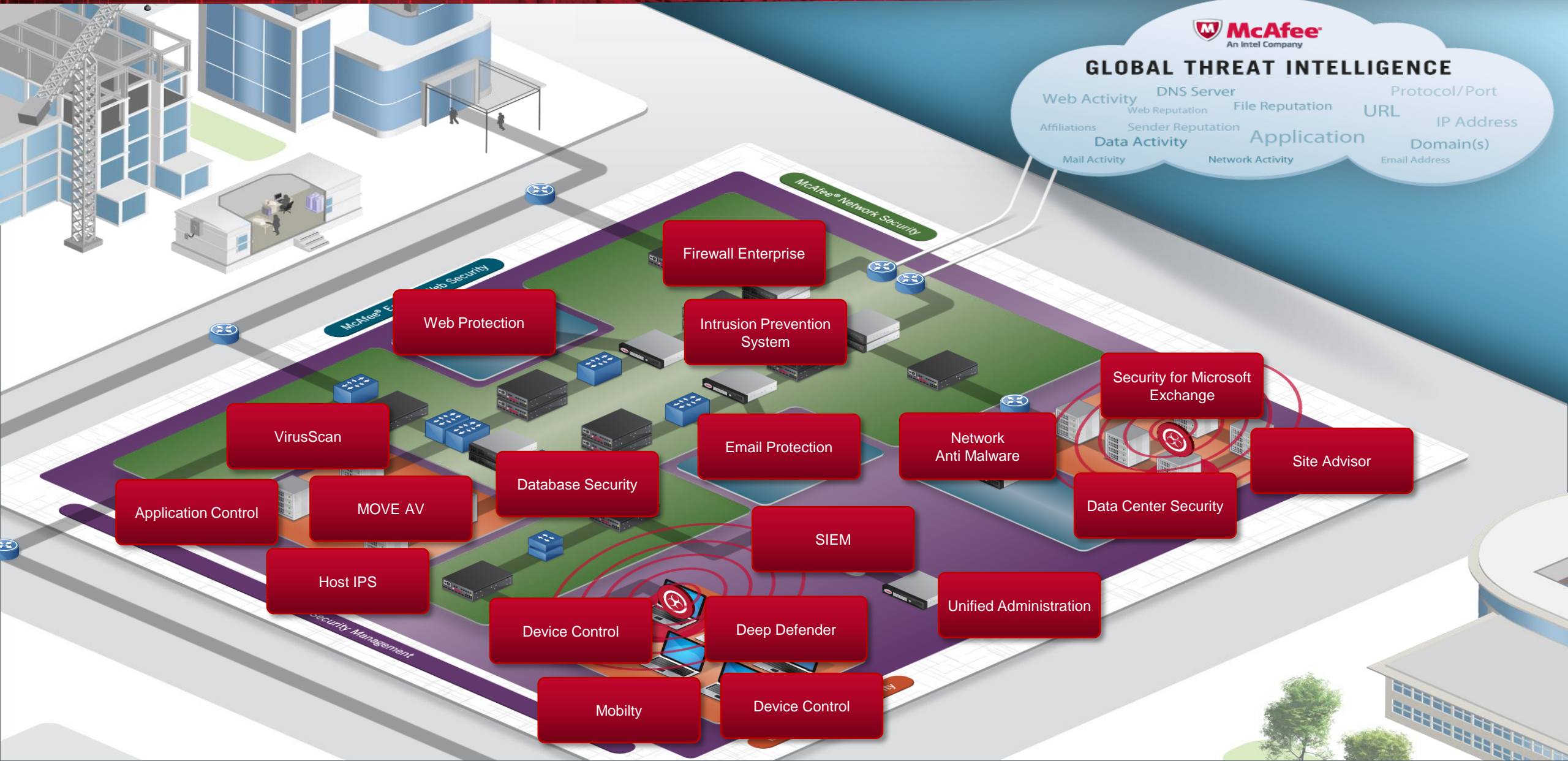
GLOBAL THREAT INTELLIGENCE



Web Activity, DN, Web Reput, Reputation, Protocol/Port, URL, IP Address, Affiliations, Sender P, Application, Domain(s), Data Activity, Mail Activity, Network Activity, Email Address



Multi-Layering Defense | Interconnected



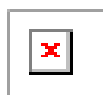
 Click here to download pictures. To help protect your privacy, Outlook prevented automatic download of some pictures in this message.

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]

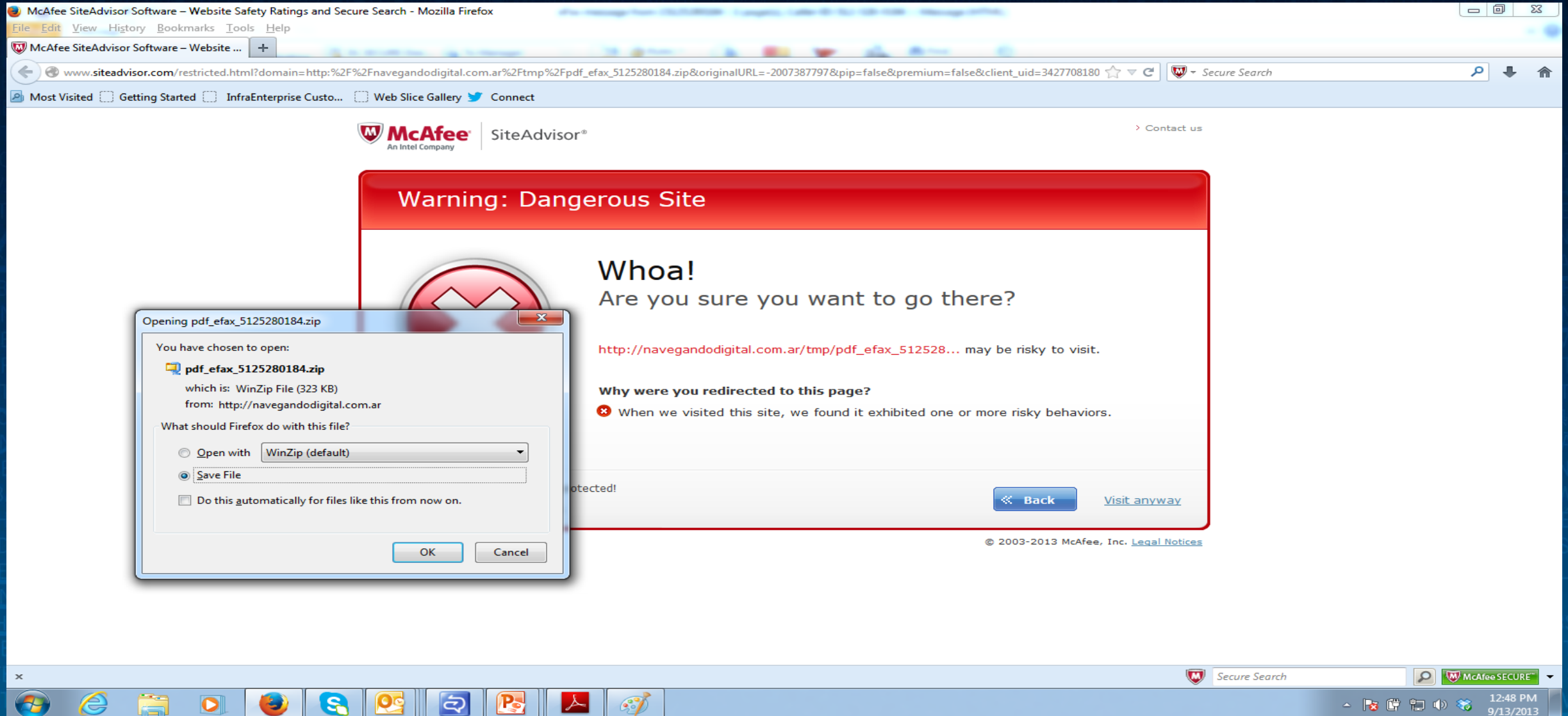
You have received a 1 page fax at 2013-09-12 06:56:56 CDT.

* 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

Please visit 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!



The screenshot shows a Mozilla Firefox browser window with the McAfee SiteAdvisor Software interface. The address bar displays the URL: www.siteadvisor.com/restricted.html?domain=http:%2F%2Fnavegandodigital.com.ar%2Ftmp%2Fpdf_efax_5125280184.zip&originalURL=-2007387797&pip=false&premium=false&client_uid=3427708180. The page features a prominent red warning box with the text: "Warning: Dangerous Site", "Whoa! Are you sure you want to go there?", and "http://navegandodigital.com.ar/tmp/pdf_efax_512528... may be risky to visit." Below this, it explains the reason: "Why were you redirected to this page? When we visited this site, we found it exhibited one or more risky behaviors." The warning box includes "Back" and "Visit anyway" buttons. In the foreground, a file dialog box titled "Opening pdf_efax_5125280184.zip" is open, showing the file name, size (323 KB), and source. It offers options to "Open with WinZip (default)", "Save File", or "Do this automatically for files like this from now on." The Windows taskbar at the bottom shows the system tray with the time 12:48 PM and date 9/13/2013, along with McAfee SECURE and Secure Search icons.

Warning: Dangerous Site



Whoa!
Are you sure you want to go there?

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 ke

Like 74,424 pe



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.

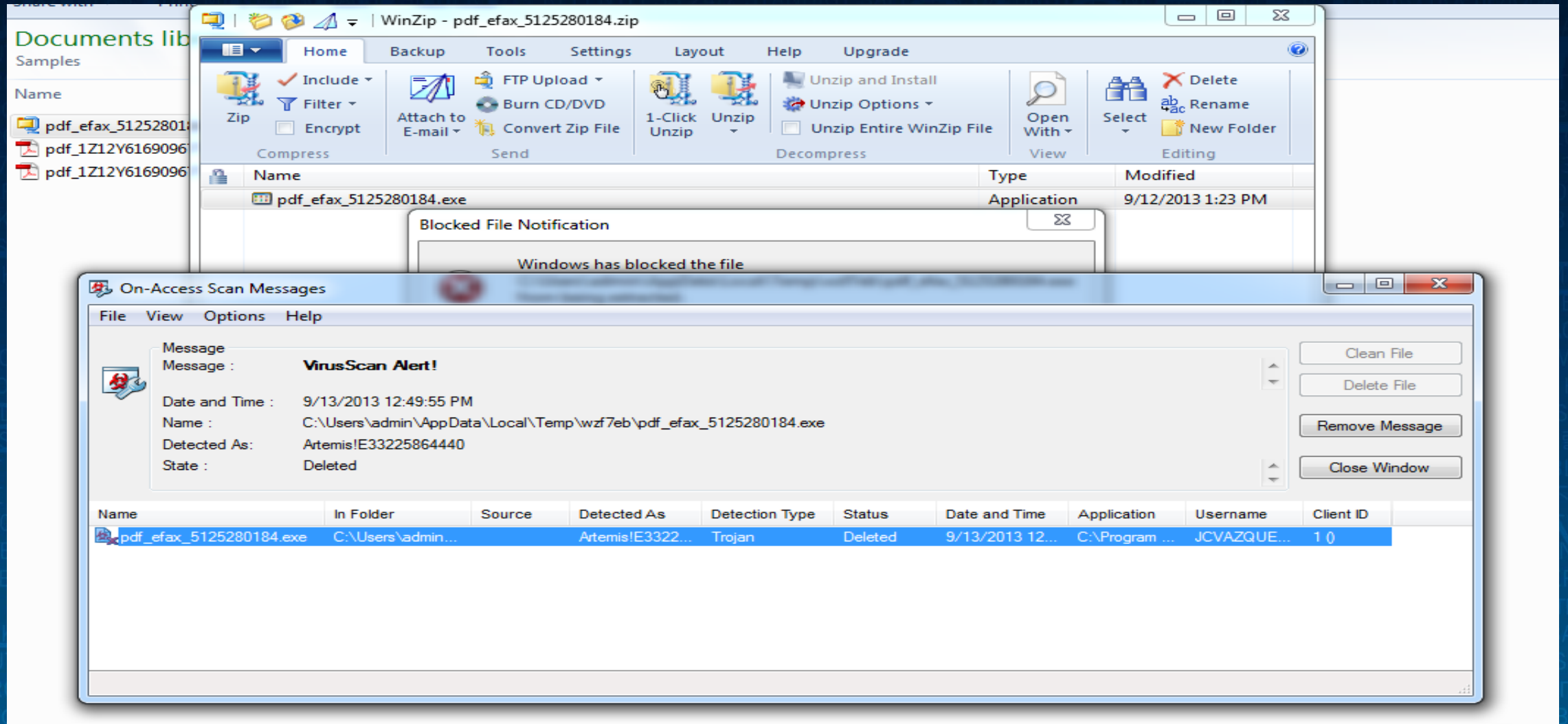
Download Anyway

Block Download

Back

Visit anyway

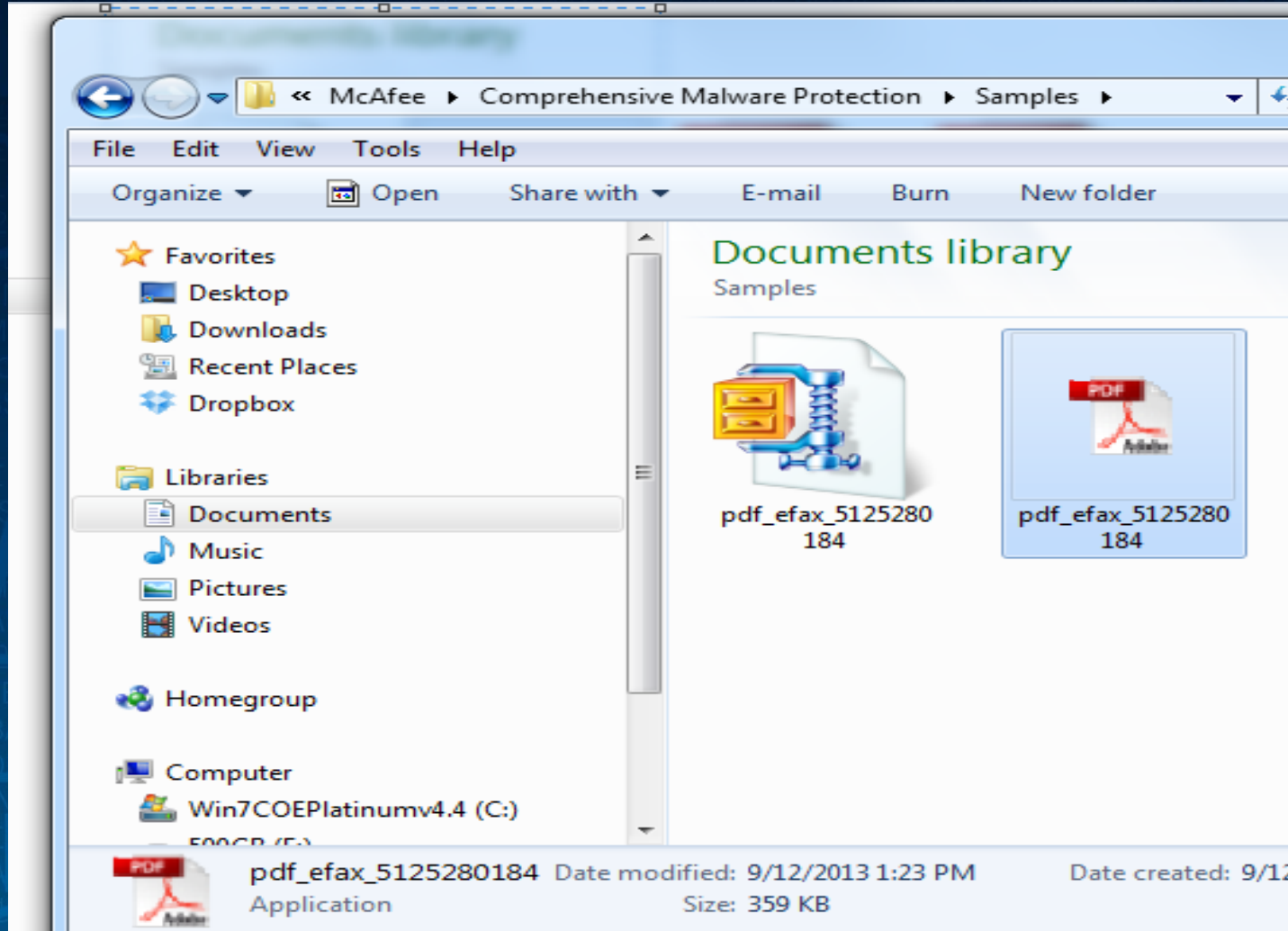
© 2003-2013 McAfee, Inc. [Legal Notices](#)



The screenshot displays a Windows desktop environment with three overlapping windows:

- WinZip - pdf_efax_5125280184.zip**: A file management window showing a file named `pdf_efax_5125280184.exe` of type `Application` modified on `9/12/2013 1:23 PM`. The interface includes various toolbars for file operations like 'Include', 'Filter', 'Zip', 'Unzip', and 'Unzip and Install'.
- Blocked File Notification**: A small dialog box stating "Windows has blocked the file".
- On-Access Scan Messages**: A window displaying a **VirusScan Alert!** message. The message details are:
 - 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**: DeletedA table below the message provides a detailed scan log entry:

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...	1 0





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.

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

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

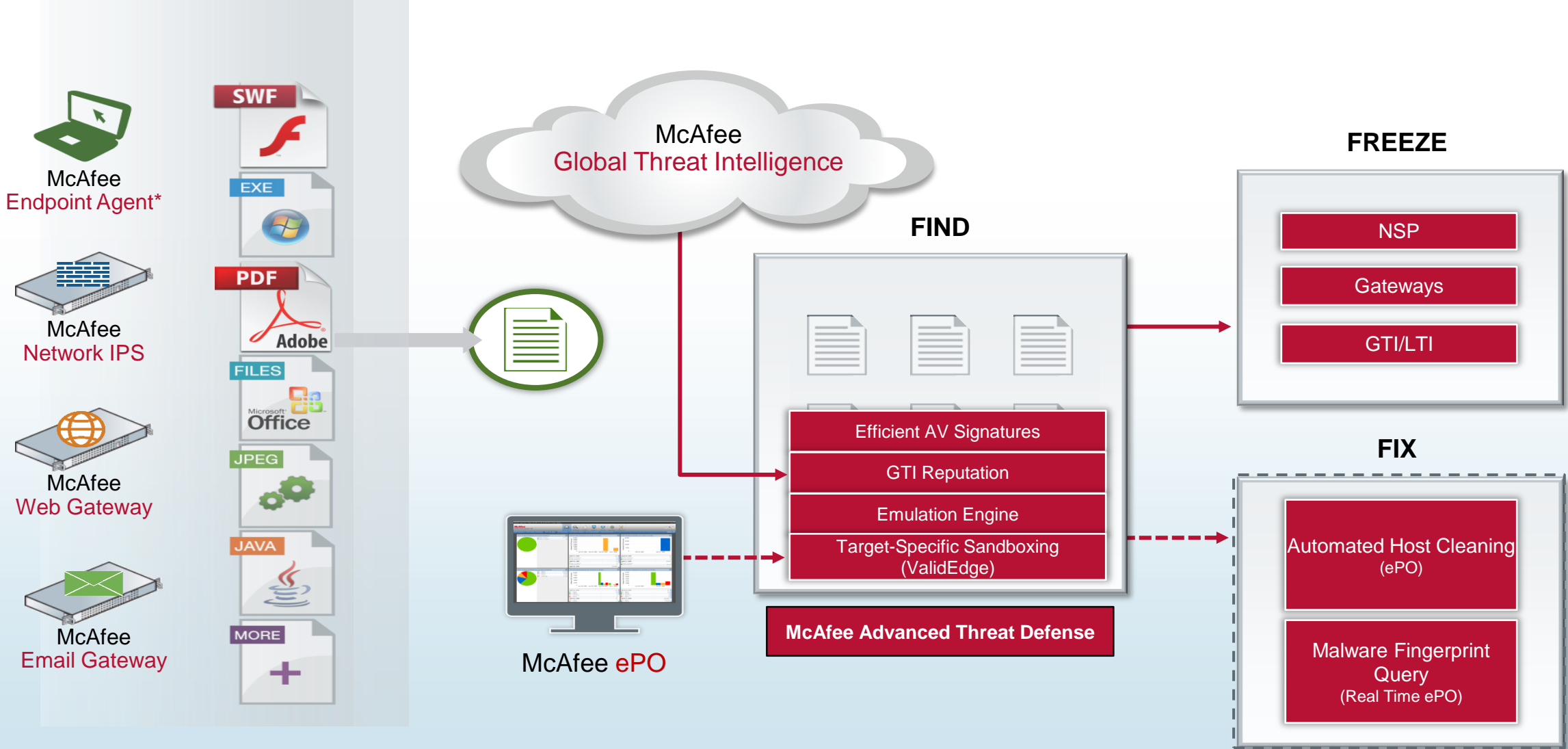
Maximum file size: 64MB

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!

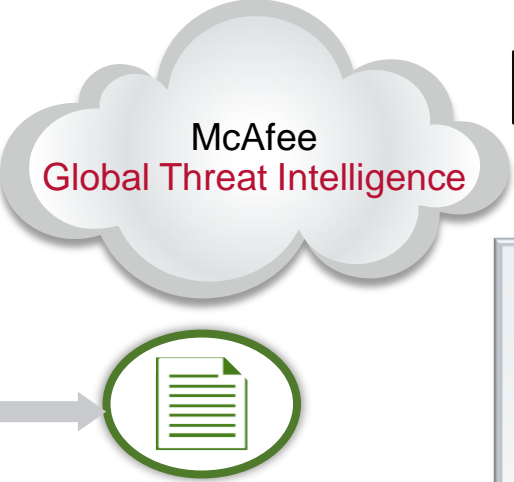
You may prefer to [scan a URL](#) or [search through the VirusTotal dataset](#)

McAfee Comprehensive Malware Protection Solution Overview

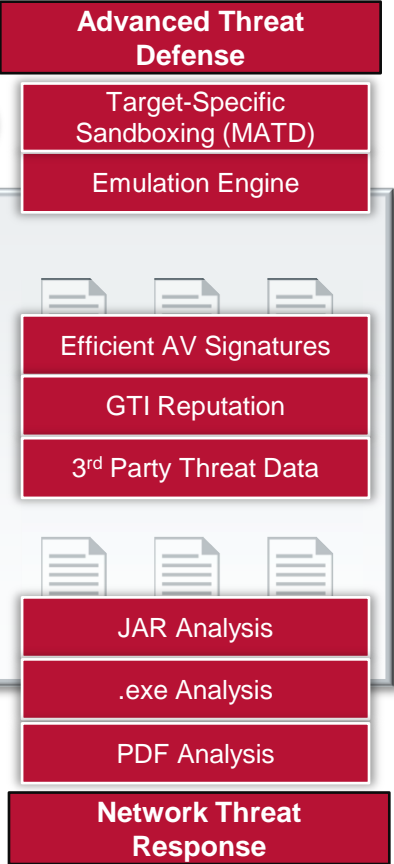


Discovering ZeroDay and Targeted Attacks

Live Walkthrough

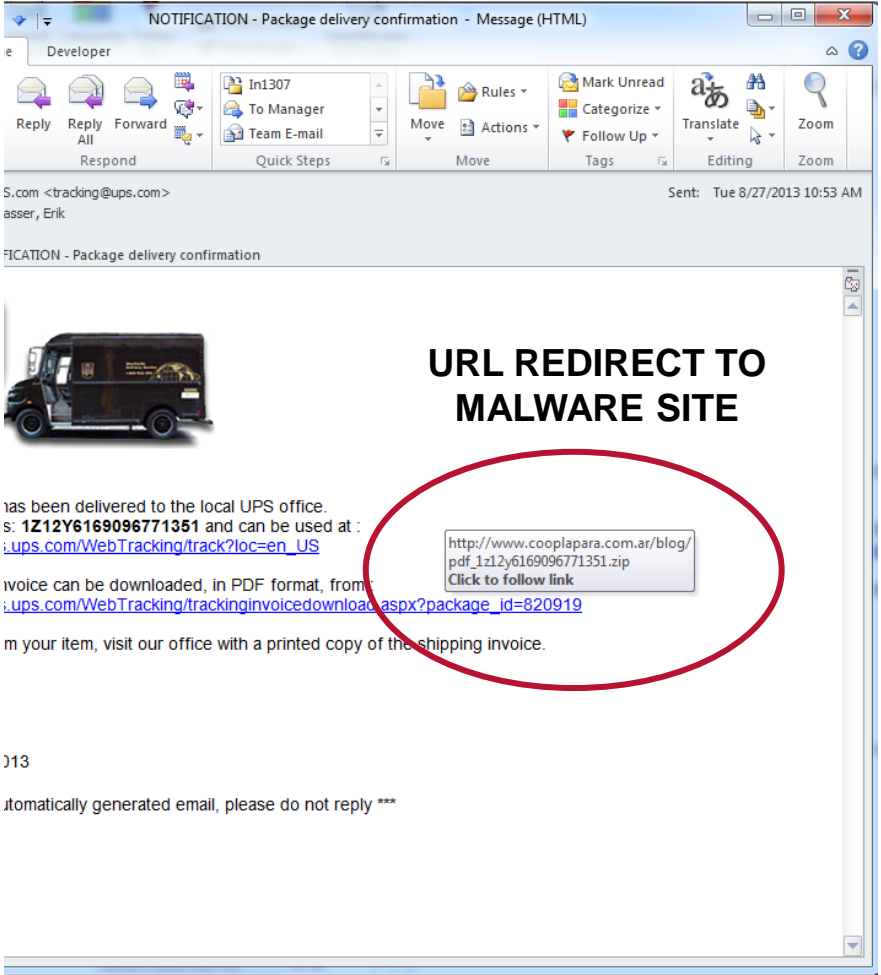


YOU FIND ON-PREM



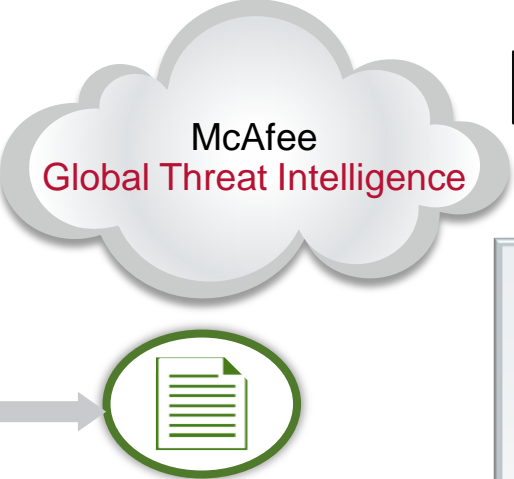
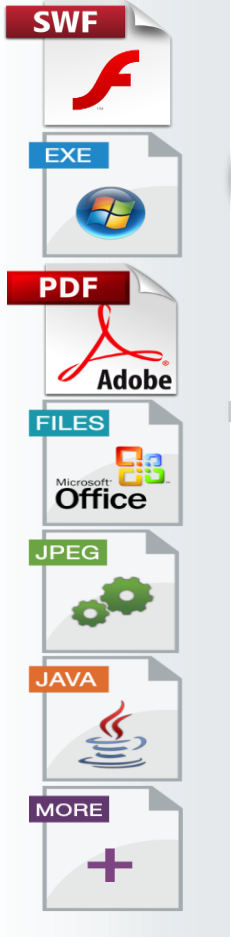
MFE FINDS VIA CLOUD

LIVE E-MAIL RECEIVED 08-27-2013



Discovering ZeroDay and Targeted Attacks

Live Walkthrough



YOU FIND ON-PREM



MFE FINDS VIA CLOUD

REPUTATION CHECK OF THE URL PASSES

Check URL

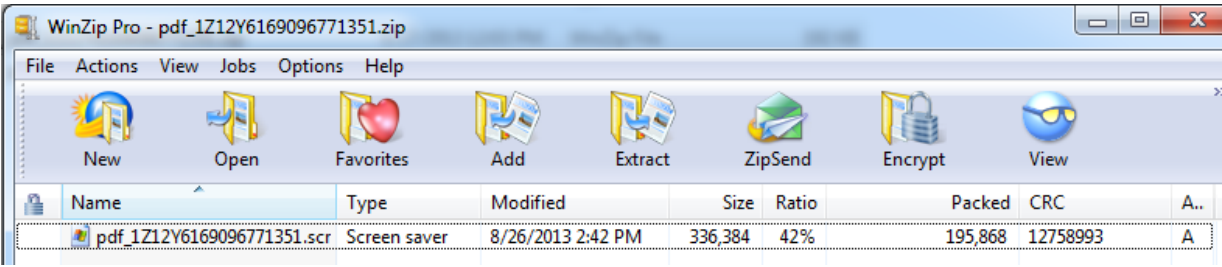
Enter the URL to check:

Local Cloud

URL: http://www.cooplapara.com.ar/blog/pdf_1Z12Y6169096771351.zip (181.16.152.254)
Geolocation: AR:Argentina

Local	Cloud
Minimal Risk (0) 	Unverified (15)

PAYLOAD APPEARS TO BE A .SCR INSIDE A .ZIP

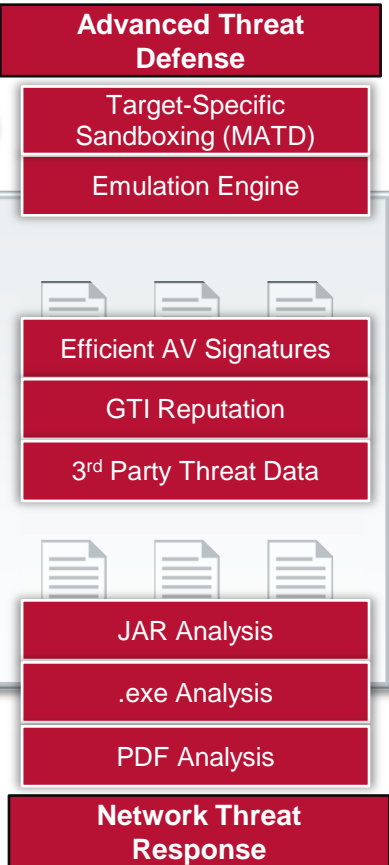


Discovering ZeroDay and Targeted Attacks

Live Walkthrough



YOU FIND ON-PREM



MFE FINDS VIA CLOUD

DUE TO ZERO DAY, FEW A/V SIGNATURE CATCHES



SHA256: 5e59097b1ab24f508aa8e9fac859507c406689d599bbe4ba3b8880b78a7371eb

File name: pdf_1Z12Y6169096771351.scr

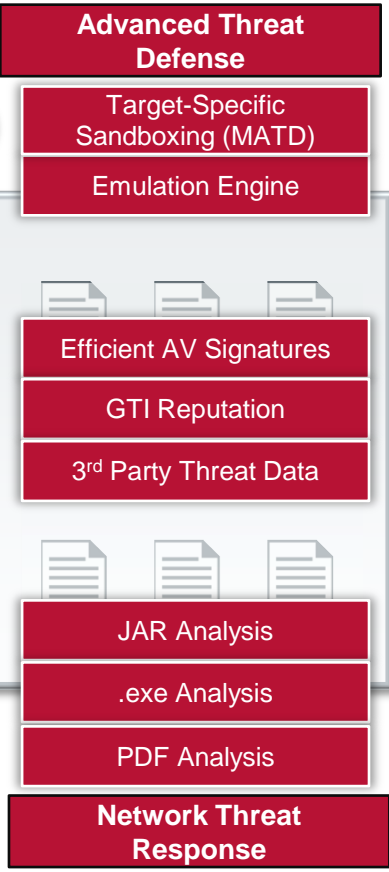
Detection ratio: 2 / 45

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



YOU FIND ON-PREM



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
Media Type: application/executable

Advanced Threat Defense Results:
MATD Hash: 066bec76edda836ba0976485b2eb036f
MATD Severity: 5
File Name: pdf_1Z12Y6169096771351_scr.exe
Verdict: Subject is malicious

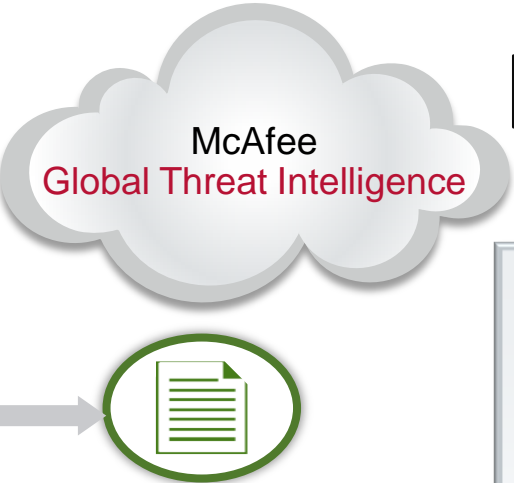
Statistics	Severity
Persistence, Installation Boot Survival	5
Hiding, Camouflage, Stealthness, Detection and Removal Protection	5
Security Solution / Mechanism bypass, termination and removal, Anti Debugging, VM Detection	3
Spreading	5
Exploiting, Shellcode	4
Networking	0
Data spying, Sniffing, Keylogging,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

Behavior

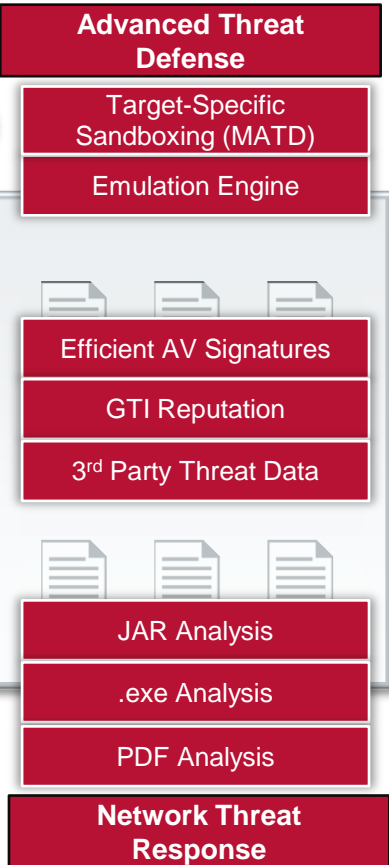
- Installs itself into Appdata and behaves like Zbot
- Created active content under RECYCLER folder
- Infected Analyzer 'bait' application
- Detected active embedded content in the sample
- Obtained and used icon of legit system application
- Examined content under Analyzer temporary directory
- Deleted 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



YOU FIND ON-PREM

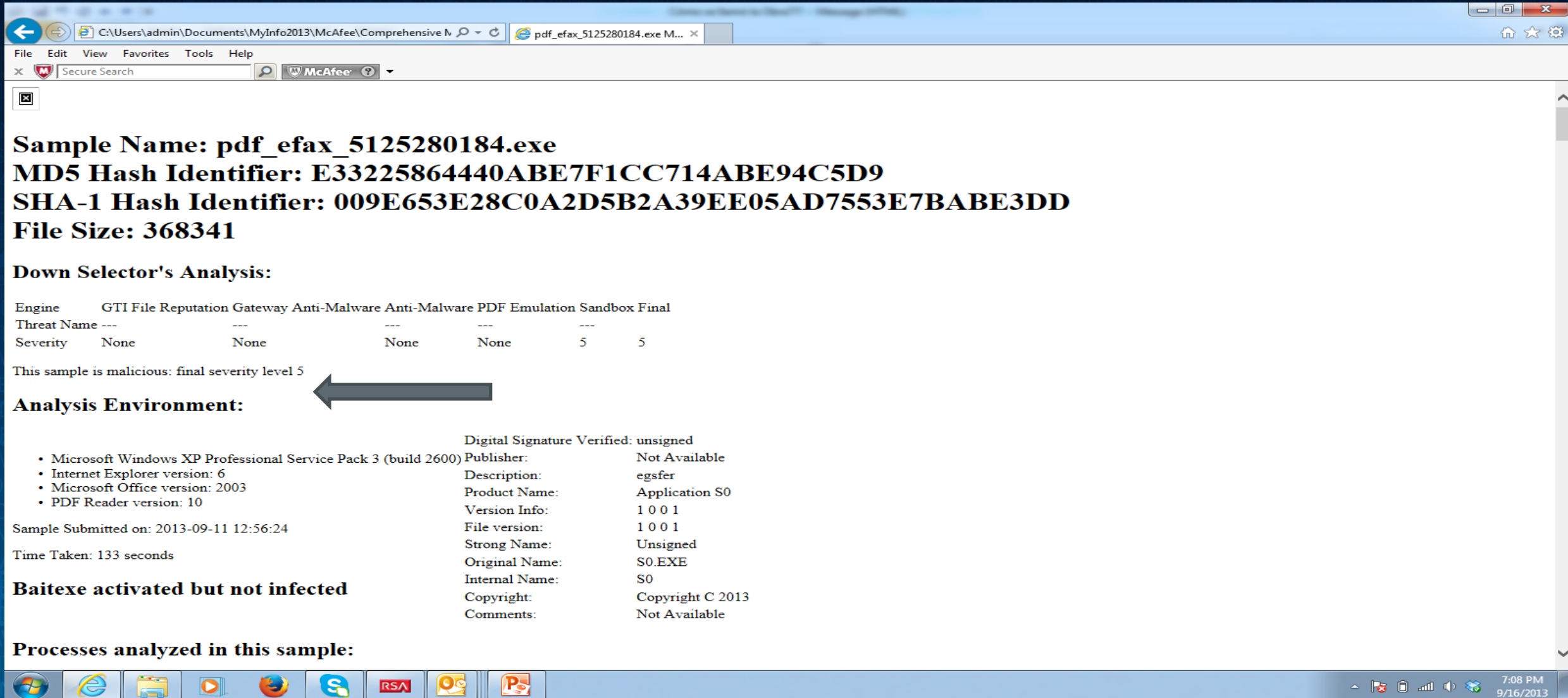


MFE FINDS VIA CLOUD

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)



The screenshot shows a McAfee Secure Search window displaying analysis results for a file named 'pdf_efax_5125280184.exe'. The file is identified as malicious with a final severity level of 5. The analysis environment includes details about the operating system (Windows XP), browser (Internet Explorer), and application (PDF Reader). The file's digital signature is unsigned, and its publisher is not available. The sample was submitted on 2013-09-11 and the analysis took 133 seconds. The results indicate that the baitexe was activated but not infected.

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	None	5	5	5

This sample is malicious: final severity level 5

Analysis Environment:

- Microsoft Windows XP Professional Service Pack 3 (build 2600)
- Internet Explorer version: 6
- Microsoft Office version: 2003
- PDF Reader version: 10

Sample Submitted on: 2013-09-11 12:56:24
Time Taken: 133 seconds

Baitexe activated but not infected

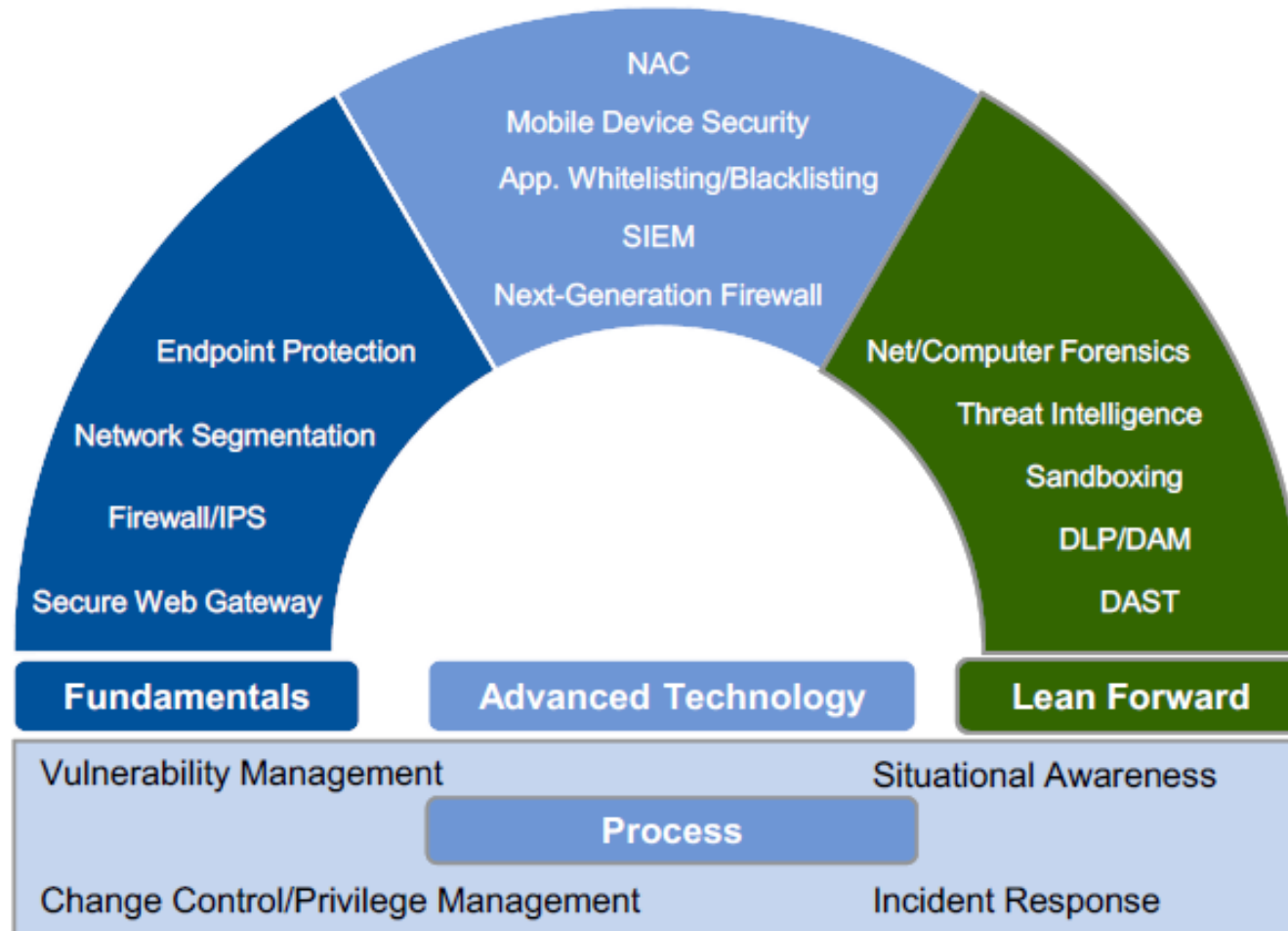
Processes analyzed in this sample:

Digital Signature Verified: unsigned
Publisher: Not Available
Description: egsfer
Product Name: Application S0
Version Info: 1 0 0 1
File version: 1 0 0 1
Strong Name: Unsigned
Original Name: S0.EXE
Internal Name: S0
Copyright: Copyright C 2013
Comments: Not Available

Usar los controles adecuados...

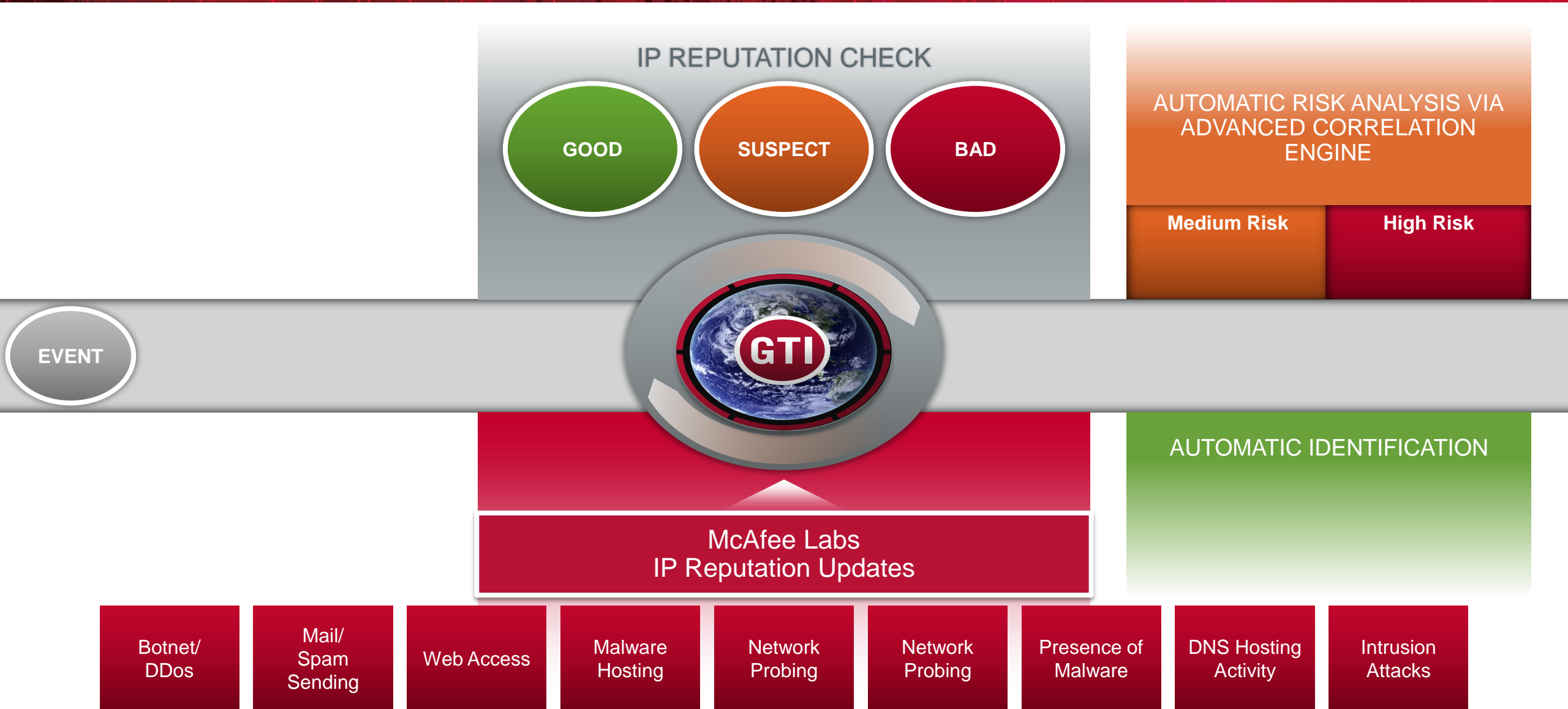


Defending Against Targeted Attacks Requires Lean-Forward Technologies and Processes



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

Global Threat Intelligence and SIEM



Manejo de Eventos...



Total Correlated Events

91,488

Average Severity - Correlated Events

Rogue DNS Communication with ...	95
Anomalous activity after exploit	93
High Severity Events to a Suspici...	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... 91,488 (100%)

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

Total Events

3,153,053

Destination IPs

Bound to: Average Severity - C... 91,488 (100%)

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 19:00:00	06/25/2013 19:34:27
71	1	192.175.48.42	dns:53	172.25.109.6	58774	06/25/2013 19:00:00	06/25/2013 19:34:27
83	1	172.25.109.6	58774	192.175.48.42	dns	06/25/2013 19:00:00	06/25/2013 19:34:27
83	1	172.25.109.6	58774	192.175.48.42	dns	06/25/2013 19:00:00	06/25/2013 19:34:27
73	1	192.175.48.42	dns:53	172.25.109.6	58774	06/25/2013 19:00:00	06/25/2013 19:34:27
1400	28	172.25.161.9	2739	88.85.72.75	http:80	06/25/2013 19:00:00	06/25/2013 19:33:32
82	1	172.25.162.181	port/type:0	...	port/code:0	06/25/2013 19:00:00	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** Auto get packet

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=dnsp,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:

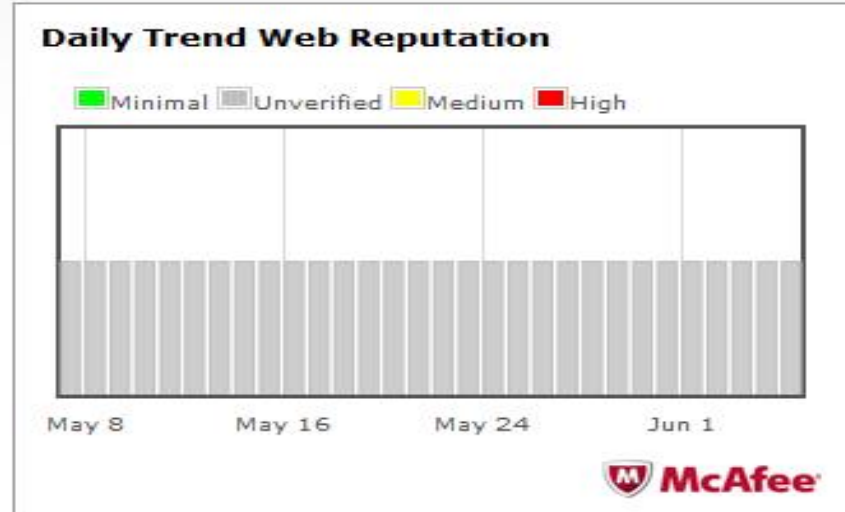
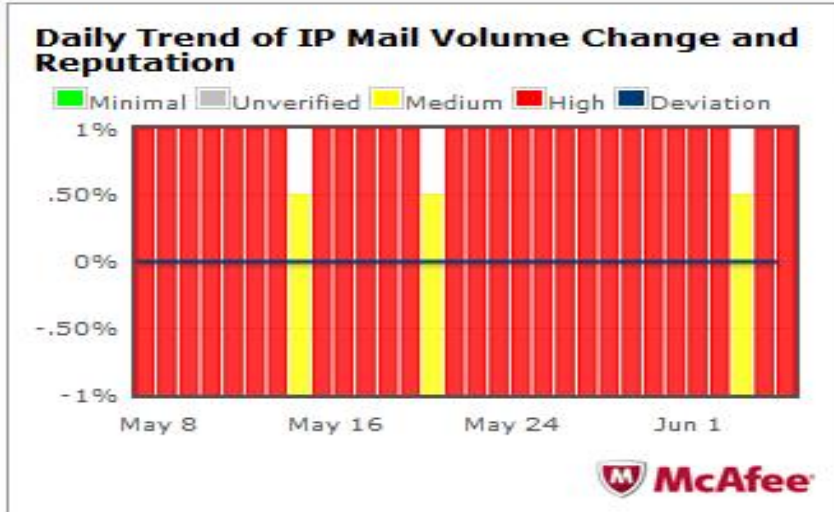
Hostname:

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.





Recycle Bin



temp



WindowsXP-KB
835935-SP2-E
NU



WindowsXP-...

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



Windows Task Manager

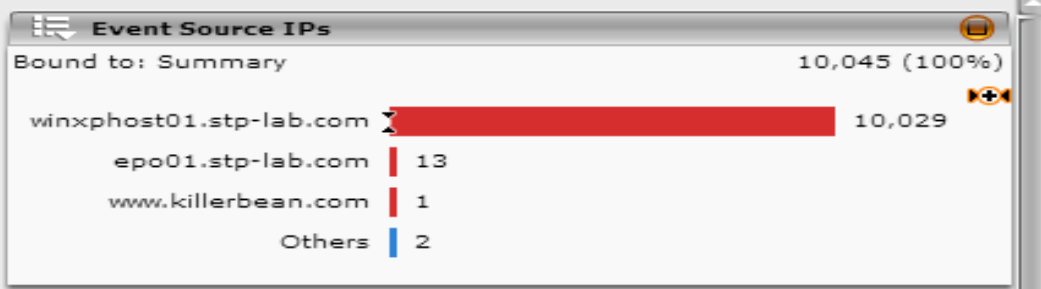
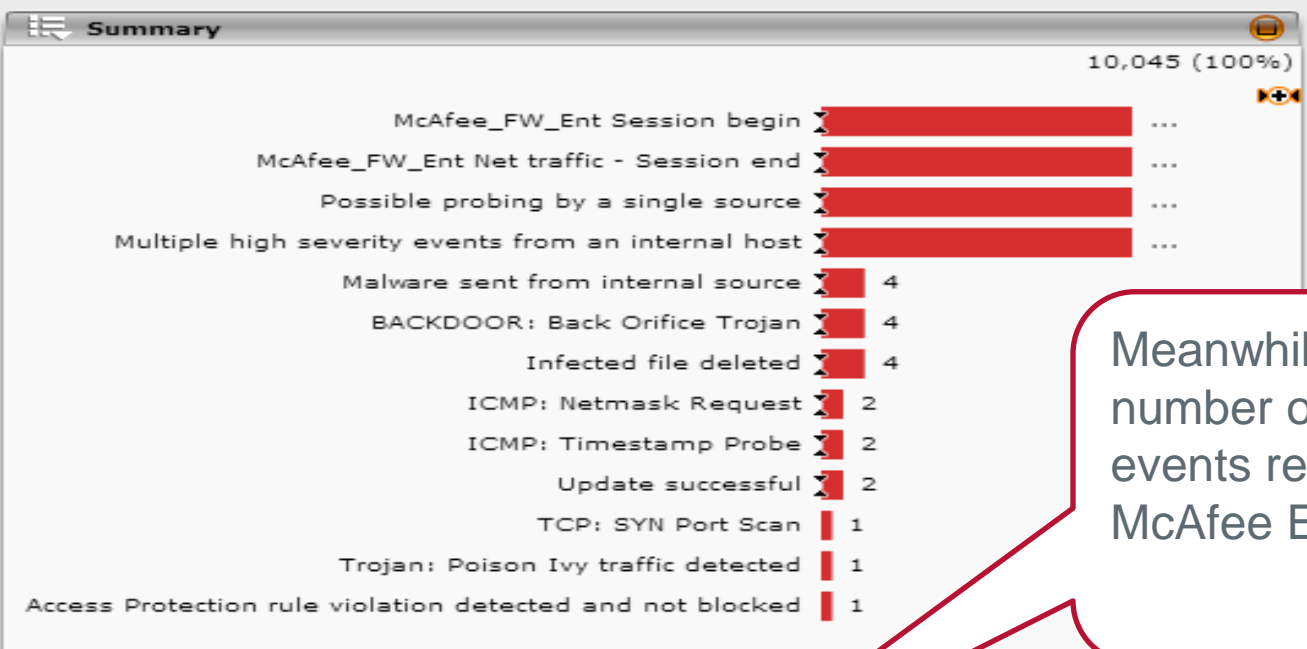
Inbox - Outlook Express

temp



Physical Display

Events and Hosts Summary Current Day



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

Events

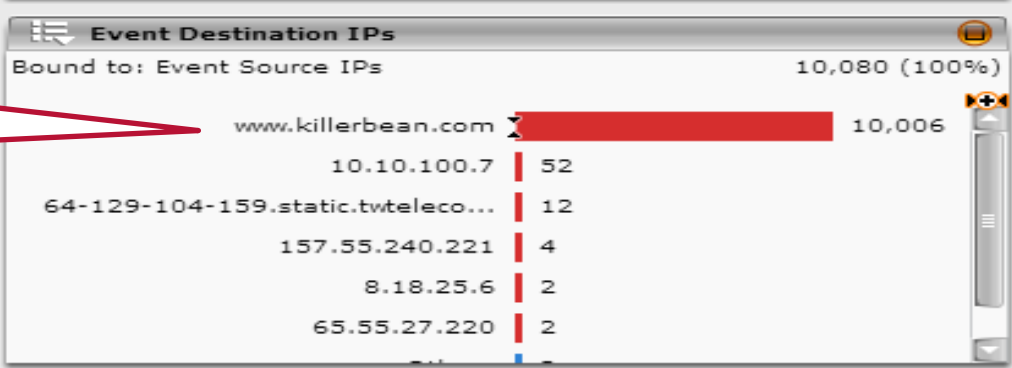
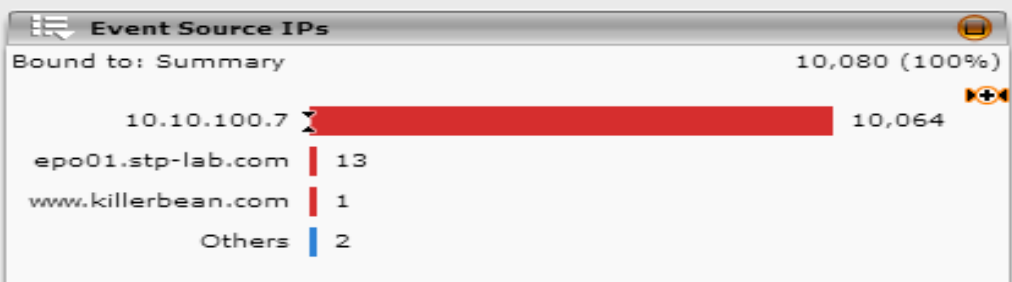
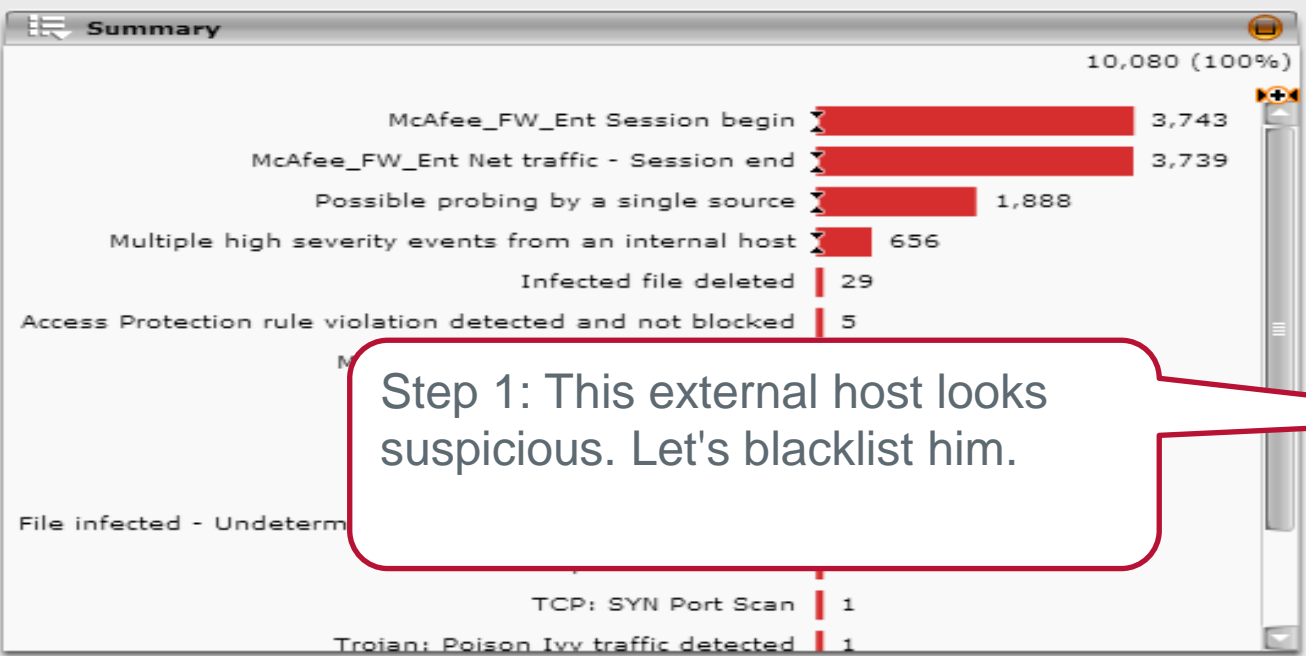
Bound to: Event Destination IPs

Severity	Rule Message	Event Count	Source IP	Destination IP	Protocol	Last Time	Event Status
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

02/03/2013 00:00:00-02/04/2013 00:00:00



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

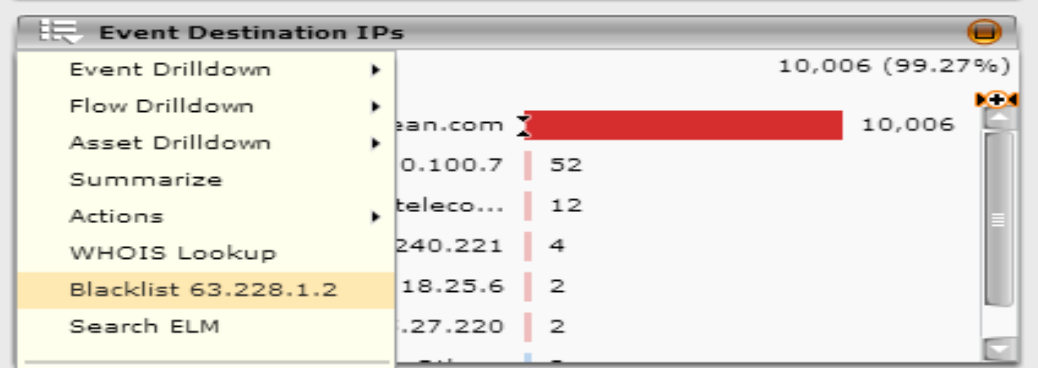
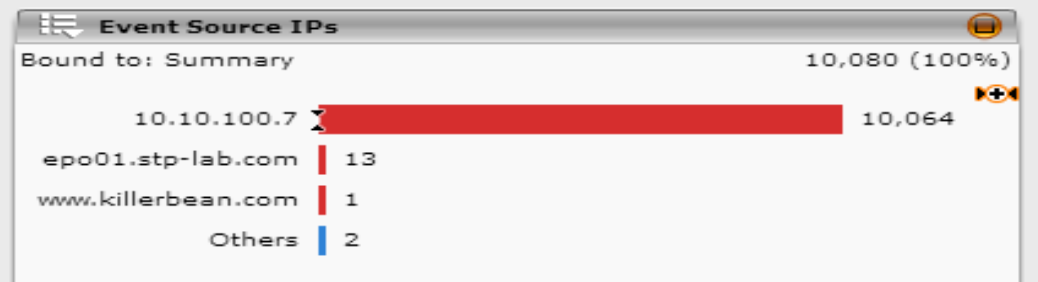
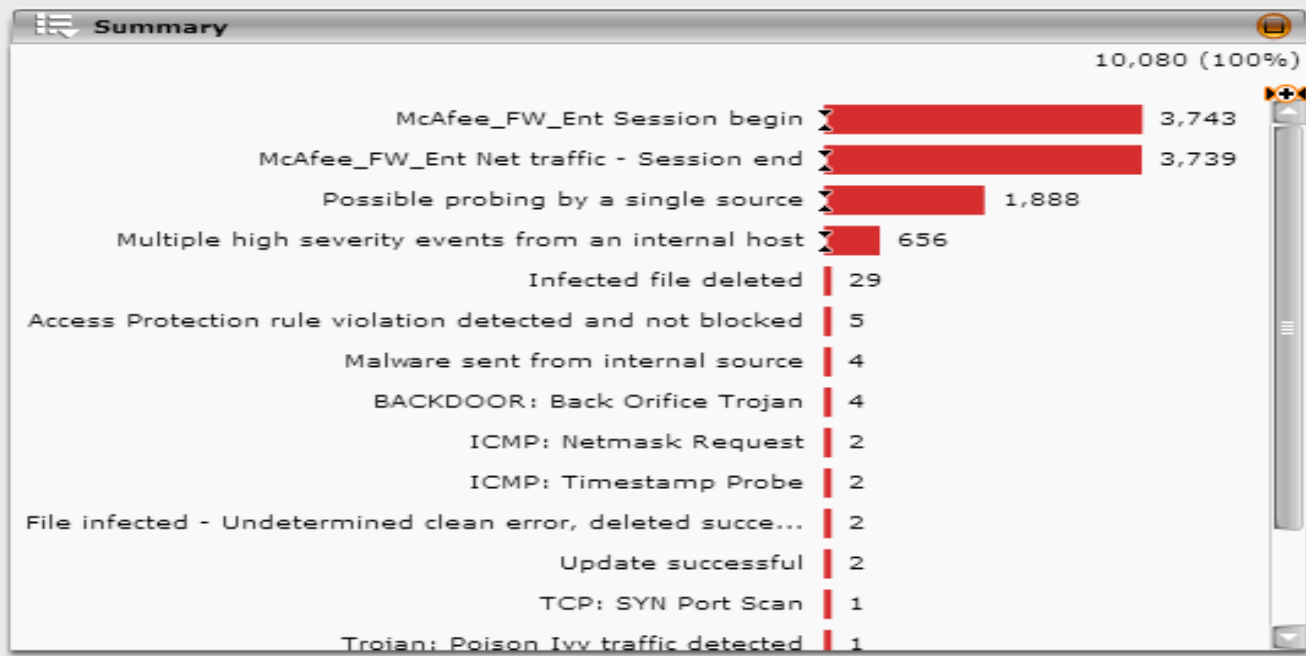
Events

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	tco	02/03/2013 20:47:27	reiect

Physical Display

Events and Hosts Summary 02/03/2013 00:00:00-02/04/2013 00:00:00

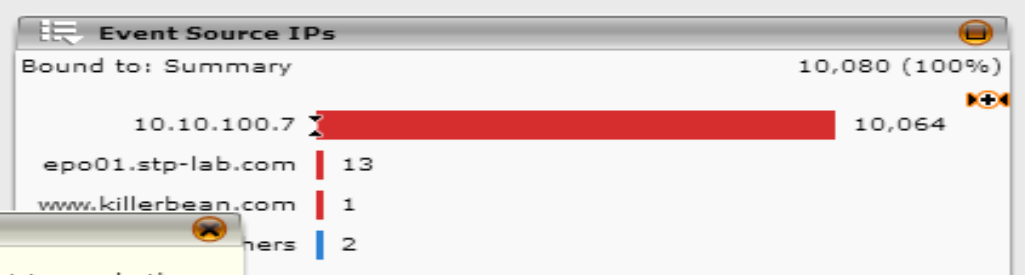
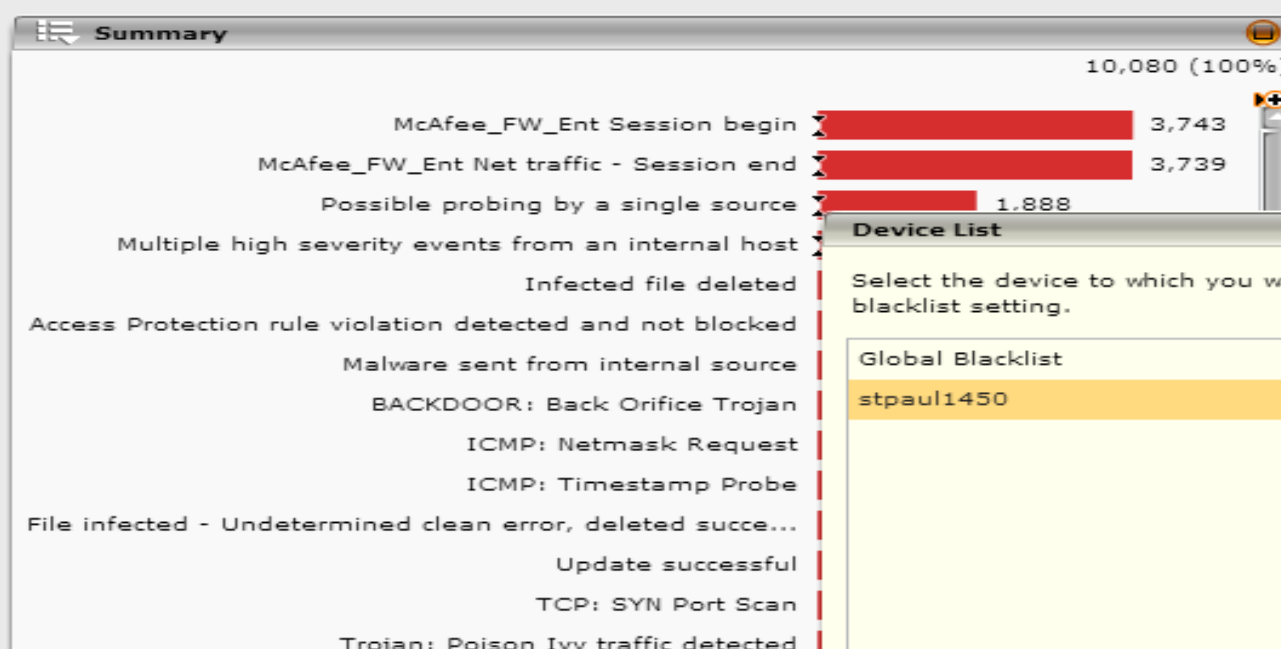


- Event Drilldown
- Flow Drilldown
- Asset Drilldown
- Summarize
- Actions
- WHOIS Lookup
- Blacklist 63.228.1.2
- Search ELM
- Export
- Delete
- Mark as reviewed

Events

Bound to: Event Destination IPs

Severity	Rule Message	Eve...	Source IP	Des...	Protocol	Last Time	Event Su
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

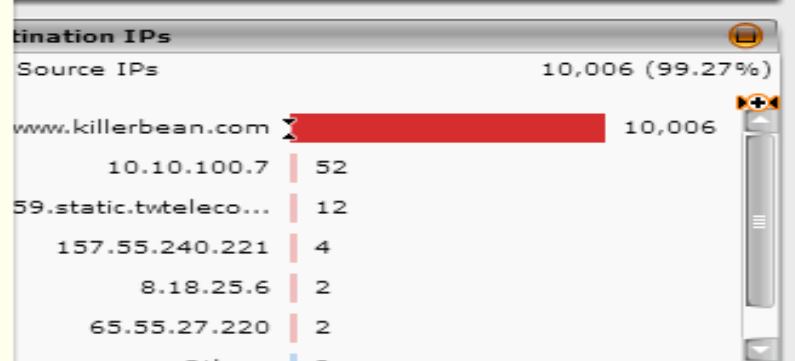


Device List

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

- Global Blacklist
- stpaul1450

OK Cancel



Events

Bound to: Event Destination IPs

Severity	Rule Message	Event Count	Source IP	Destination IP	Protocol	Last Time	Event Su
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



Physical Display

NSM Sensor Properties

Sensor: stpaul1450

Include Global Blacklist

IP Address	Duration	Description

Add
Edit
Delete

Add NSM Blacklist Entry

IP Address:

Duration:

Description:

OK Cancel

Ever

Bound to:

Severity

- 75
- 1530
- 2250
- 2250
- 2241
- 2025
- 2025
- 1581

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

- Summary
- Mu
- Access Pr
- File infect

Event

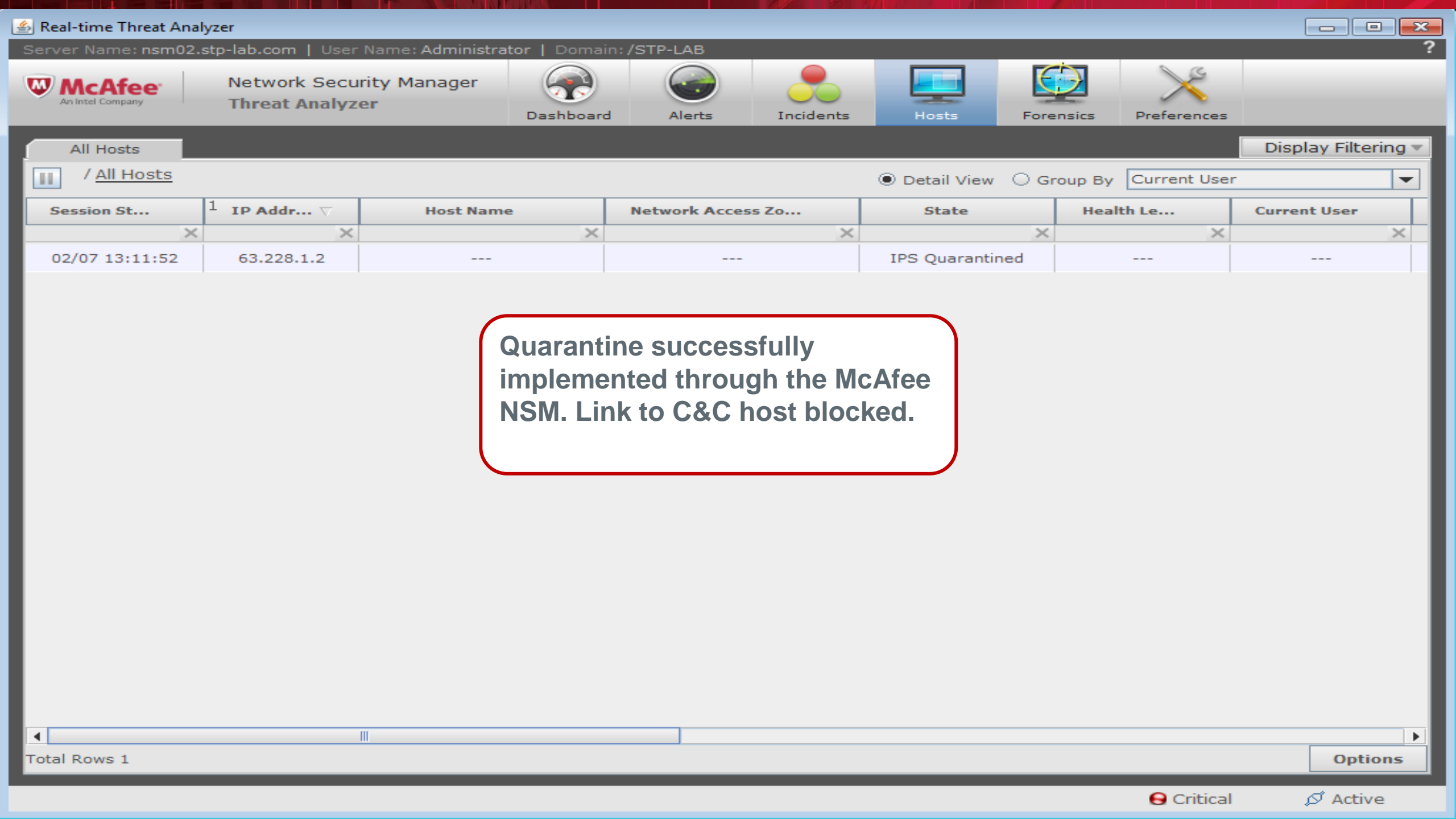
Bound to:

Severity

- 75
- 1530
- 2250
- 2250
- 2241
- 2025
- 2025
- 1581

Close

Possible probing by a single source	31	10.10.100.7	www.killerbean.com	tcp	02/03/2013 20:47:27	reject
-------------------------------------	----	-------------	--------------------	-----	---------------------	--------



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

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

Total Rows 1

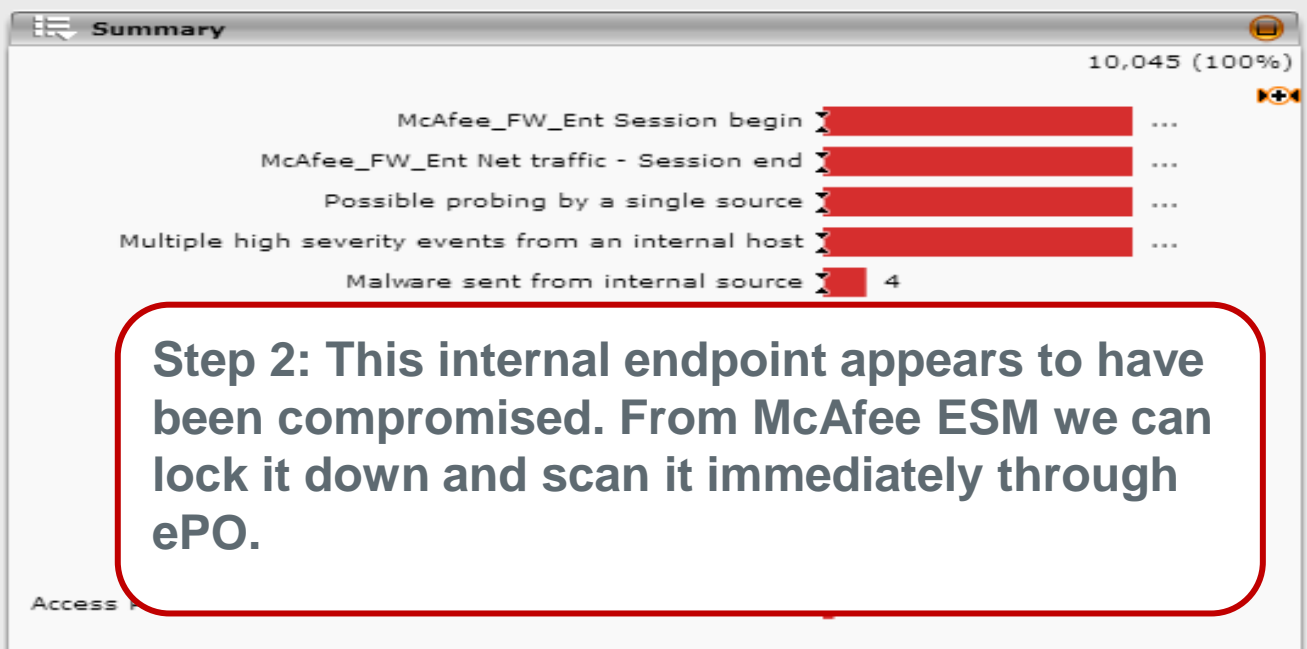
Options

Critical Active

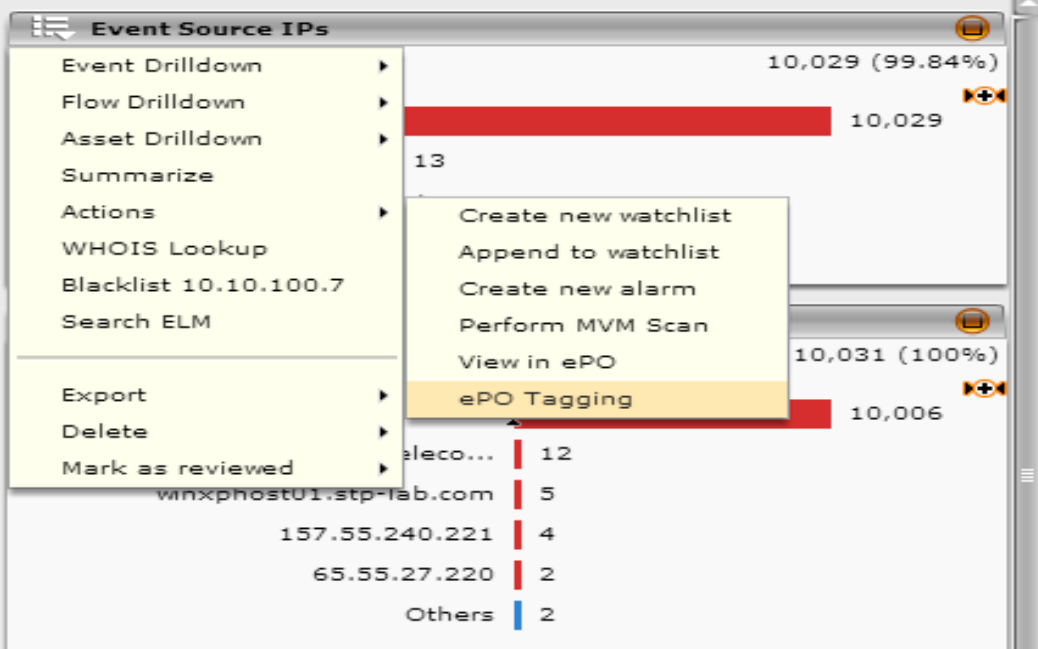


Physical Display

Events and Hosts Summary Current Day



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



- Event Drilldown
- Flow Drilldown
- Asset Drilldown
- Summarize
- Actions
- WHOIS Lookup
- Blacklist 10.10.100.7
- Search ELM
- Export
- Delete
- Mark as reviewed

- Create new watchlist
- Append to watchlist
- Create new alarm
- Perform MVM Scan
- View in ePO
- ePO Tagging**

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 Current Day

Summary

Multiple high severity events from an internal IP address

Access Protection

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.

10,029 (99.84%)

10,031 (100%)

10,006

Events

Bound to: Event D

Severity	Rule Name
70	Trojan
75	McAfee
1530	Possible
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: Wake up client

Assign the selected tags

Severity	Rule Name	Count	IP Address	Host Name	Protocol	Time	Action
35	alert	35					reject
30	alert	30					reject
56	alert	56					reject
14	start	14					reject
30	winxphost01.stp-lab.com	30	winxphost01.stp-lab.com	www.killerbean.com	tcp	02/03/2013 21:07:14	reject
30	winxphost01.stp-lab.com	30	winxphost01.stp-lab.com	www.killerbean.com	tcp	02/03/2013 21:07:14	reject
30	winxphost01.stp-lab.com	30	winxphost01.stp-lab.com	www.killerbean.com	tcp	02/03/2013 21:07:13	start
27	winxphost01.stp-lab.com	27	winxphost01.stp-lab.com	www.killerbean.com	tcp	02/03/2013 20:56:52	reject
27	winxphost01.stp-lab.com	27	winxphost01.stp-lab.com	www.killerbean.com	tcp	02/03/2013 20:56:52	reject



Recycle Bin



temp



WindowsXP-...



WindowsXP-...

McAfee Host Intrusion Prevention

Task Edit View Help

IPS Policy **Firewall Policy** Blocker

Use this tab to enable

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...



VirusScan Console

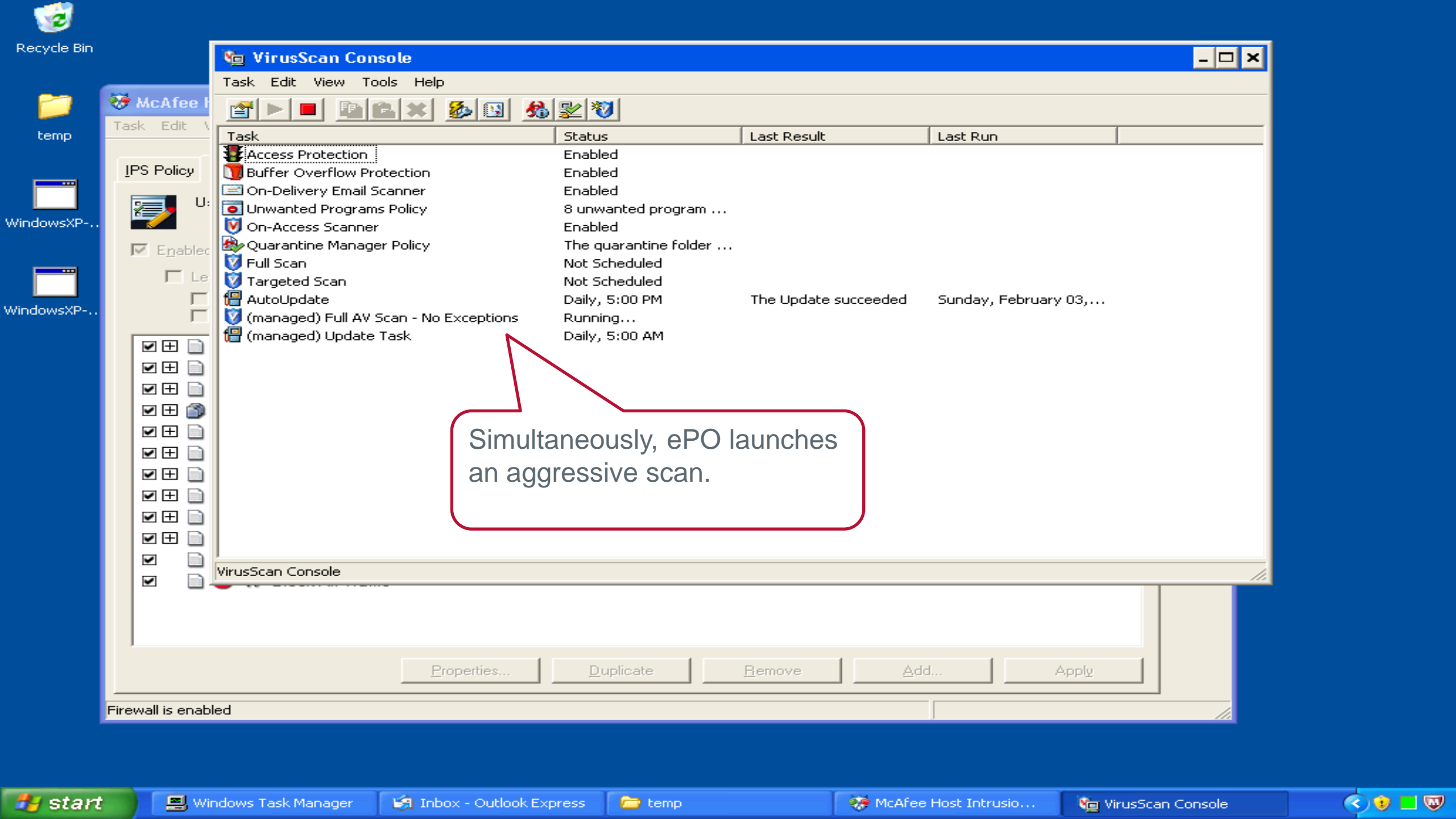
Task Edit View Tools Help

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		

Properties... Duplicate Remove Add... Apply

Firewall is enabled

Simultaneously, ePO launches an aggressive scan.



VirusScan Console

Task Edit View Tools Help

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 Scan Messages

File View Options Help

Message

Message :

Date and Time :

Name :

Detected As :

State :

Clean File

Delete File

Remove Message

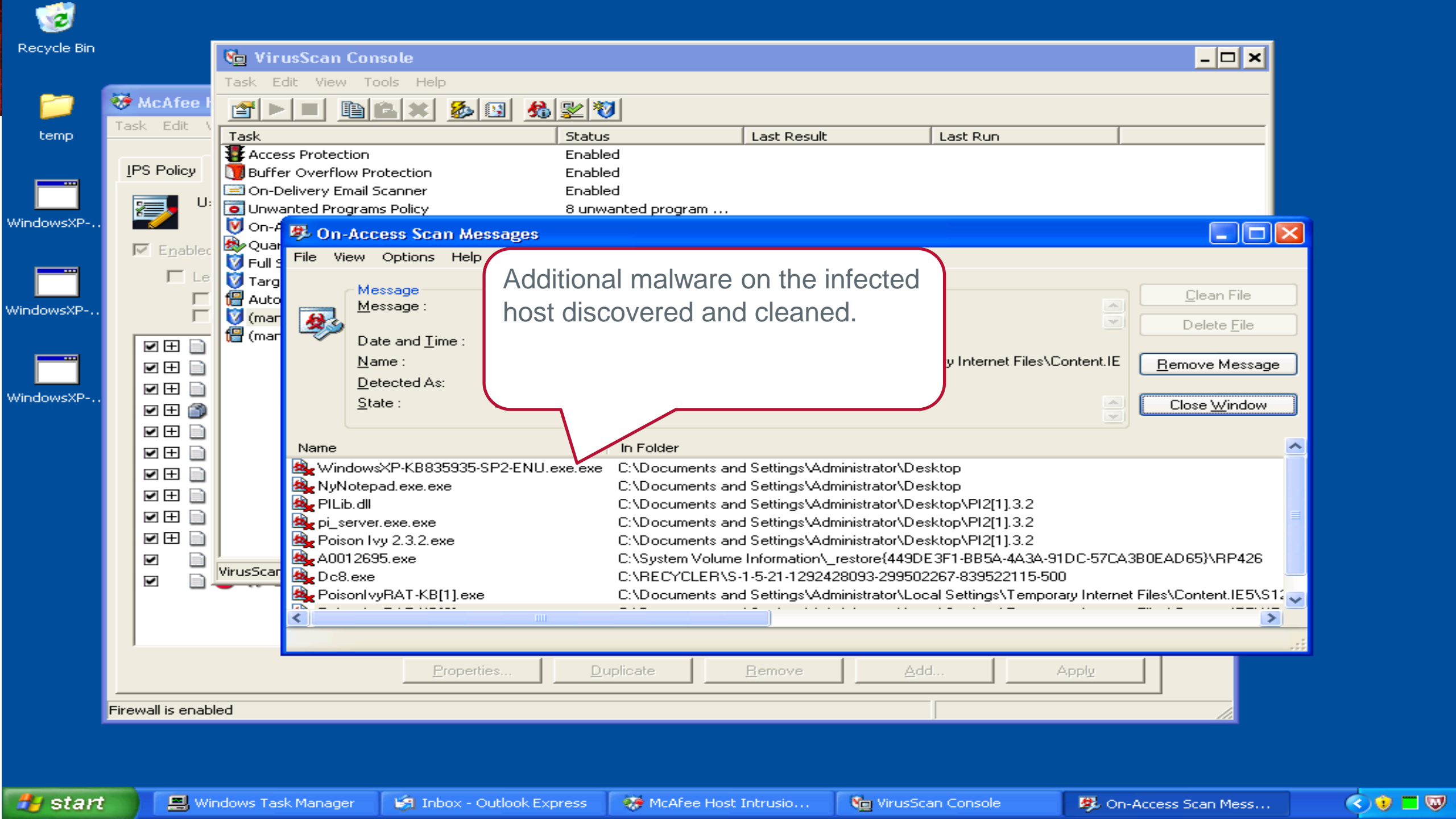
Close Window

Name	In Folder
WindowsXP-KB835935-SP2-ENU.exe.exe	C:\Documents and Settings\Administrator\Desktop
NyNotepad.exe.exe	C:\Documents and Settings\Administrator\Desktop
PILib.dll	C:\Documents and Settings\Administrator\Desktop\PI2[1].3.2
pi_server.exe.exe	C:\Documents and Settings\Administrator\Desktop\PI2[1].3.2
Poison Ivy 2.3.2.exe	C:\Documents and Settings\Administrator\Desktop\PI2[1].3.2
A0012695.exe	C:\System Volume Information_restore{449DE3F1-BB5A-4A3A-91DC-57CA3B0EAD65}\RP426
Dc8.exe	C:\RECYCLER\S-1-5-21-1292428093-299502267-839522115-500
PoisonIvyRAT-KB[1].exe	C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5\S1:

Properties... Duplicate Remove Add... Apply

Firewall is enabled

Additional malware on the infected host discovered and cleaned.

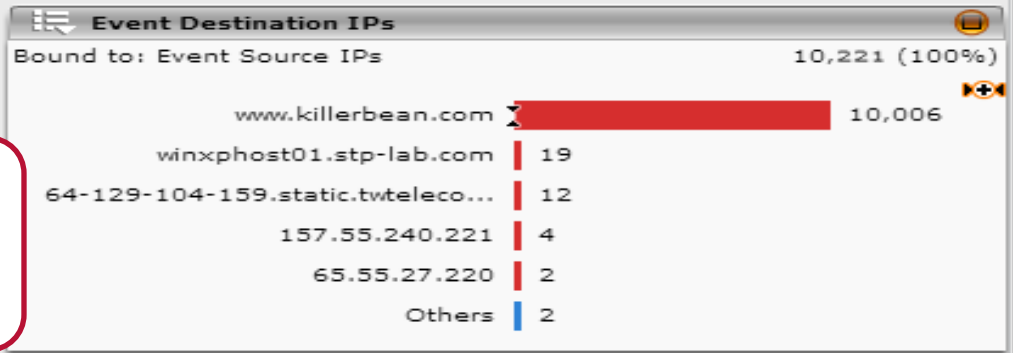
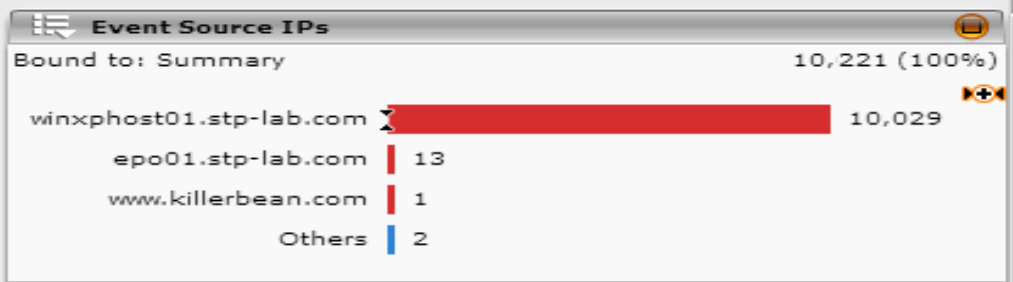
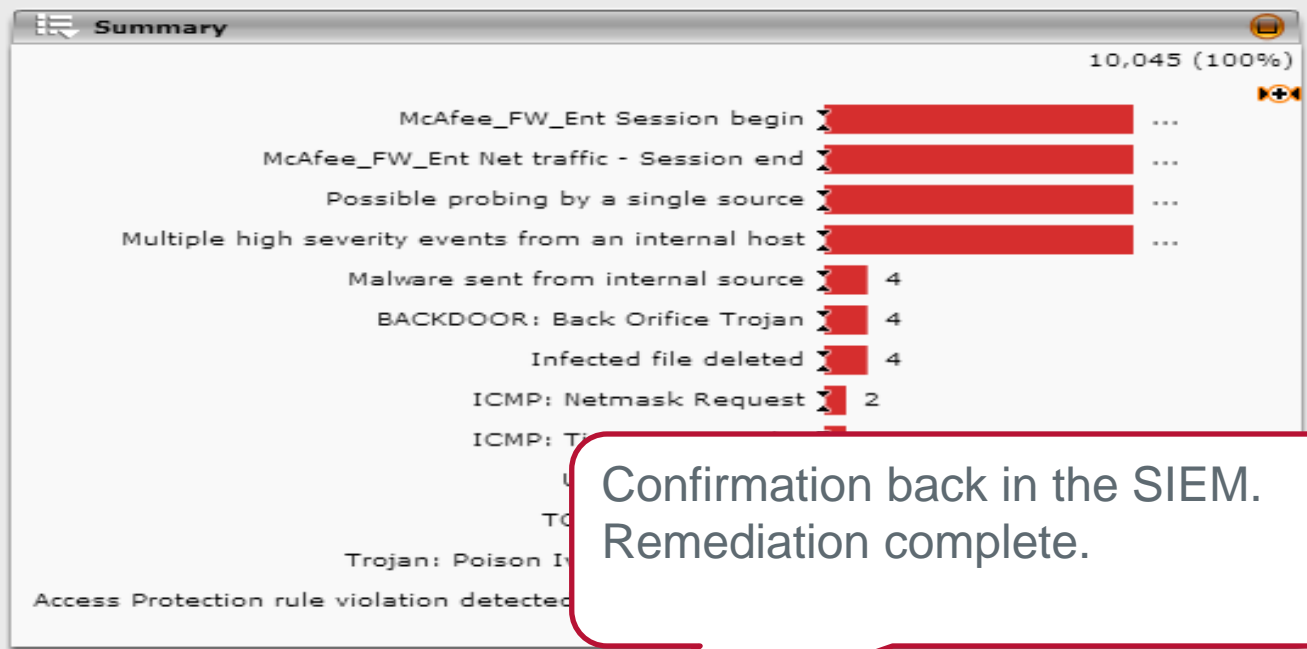




Physical Display

Events and Hosts Summary

Current Day



Confirmation back in the SIEM.
Remediation complete.

Events

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™