

# NSP 9.1 PORTABLE DEMO SCRIPT

V20170620

## CONTENTS

Overview.....	3
New in the 9.1 Demo.....	3
Demo Preparation .....	4
Solutions Center .....	4
Local Installation .....	5
One-Time Setup.....	5
Repeat for Each Demo Session .....	6
Demo Checklist.....	6
Fictional Company Profile for the Demo .....	7
About H.E. Ltd .....	7
Characters .....	7
Demo Story Overview .....	7
The Demo Script .....	8
1. Review the Dashboard and find the Top Callback Activity monitor .....	8
2. click Zeus On Top Callback Activity monitor .....	9
3. Click the Info icon for Zeus. ....	10
4. Scroll through the list of zombies and select JScott. ....	11
5. Double-click JSCOTT to open the Attack Log and view Zeus attacks matching his endpoint. ....	12
6. Remove the Zeus filter to view all attacks matching jscott’s endpoint. ....	13
7. Select an attack and review the “Other Actions” button. ....	14
8. Close the Attack Log to investigate endpoint-specific details. ....	15
9. Click the Endpoint Security Events tab. ....	16
10. Click the Vulnerability Assessment tab .....	17
11. Click the Endpoint Information tab .....	18
12. Hover over the Quarantine button. (No need to press it) .....	19
13. Click the Network Forensics button. ....	20
14. Review Network Forensics data. ....	21
15. Investigate gkcalt.exe on the Endpoint Executables page. ....	22
16. Click the Endpoints tab. ....	23
17. Blacklist gkcalt.exe. ....	24
18. Investigate collectmail.pdf on the Malware Files page.....	25
19. Blacklist collectmail.pdf.....	26
Recap .....	27

## OVERVIEW

The purpose of this document is to provide guidance to those demoing the NSP GUI and, in particular, its event management workflows.

To that end, this document presents a simple user story that covers essential functionality, with click-by-click guidance and key talking points.

## NEW IN THE 9.1 DEMO

1. The demo installer is no longer a standalone executable – the demo data has been merged into the production NSM installer. Also, the one-time database setup task that has traditionally been required to initialize the demo has been incorporated into the installer. (Installing the demo is now a hidden option in the production installer: [Instructions Here](#))
2. The version of NS sensor used in the demo has been upgraded to make the SSL decryption configuration pages available at the device level.
3. Sample CTD alerts and file analysis results have been added.
4. The active signature set has been updated to include improved attack descriptions for advanced malware attacks.

## DEMO PREPARATION

You can schedule an NSP demo in Solutions Center (formerly CloudRunner), which is recommended for most situations, or download and install the portable demo build and running it locally.

In either case, you can find demo reference documentation here:

<https://planet.mcafee.com/docs/DOC-25463>

## SOLUTIONS CENTER

You can schedule/start an NSP demo here:

<http://solutionscenter.intelsecurity.com>

As shown below:

1. Once logged in, select the *Catalog* menu.
2. Select the 9.1 demo package.
3. Press the *Schedule* or *Quick Launch* button to start the demo in the future or now, respectively.

The screenshot displays the McAfee Solutions Center interface. The top navigation bar includes 'Welcome Chuck Slate', 'Defect', 'PER', 'Community', and 'Support'. The main header shows the McAfee logo and 'Security Solutions On-Demand' alongside the Intel Security logo. A left sidebar contains navigation options: Home, Catalog (circled in green), Reports, and Profile. The main content area features a 'Keyword Search' box, 'Package Details' (with checkboxes for Quick Launch, Demo, POC, Training, Beta Test, Partner), 'Languages' (English, Spanish, French, German), and 'Regions' (APAC, EMEA, JAPAN, LTAM, NA). A list of 20 packages is shown, with 'McAfee Network Security Platform (NSP) Version 8.3' highlighted in blue and circled in green. The right pane displays the details for this package, including 'Package Information' (Demo, 20 minutes spinup, English language, APAC/EMEA/JAPAN/LTAM/NA regions) and 'Schedule' and 'Quick Launch' buttons (both circled in green).

4. In both cases, you will be prompted for details about the customer and opportunity, and to confirm the schedule/launch.
5. Once the demo is ready, an email will be sent to you with demo details, including the server name and credentials needed to access the demo via Remote Desktop (RDP).
6. Connect via RDP and log into the NSM GUI using the provided credentials.

Notes:

1. RDP is required to access the demo.
2. It may take up to 20 minutes to spin up the demo.

3. In addition to the email notification, you can always access the demo details from within the Solution Center GUI itself:
  - a. Go to the *Home* menu.
  - b. On the *My Activity Scheduled* tab, click the running demo in question.
  - c. Click the *Run Time Information* tab.

## LOCAL INSTALLATION

For an offline version of the portable demo, download the production 9.1 NSM installer from the McAfee Download site and follow the steps below.

---

### ONE-TIME SETUP

1. In previous NSM versions, the demo installer was a separate binary from the production installer, and there was an explicit/manual step required to run the one-time demo setup.
2. As of NSM 9.1, there is a single binary that can be used to install both the demo and production NSM, and the one-time demo setup is performed automatically.
3. If you execute the NSM installer as you have in the past, e.g., by double-clicking setup.exe, the production version will be installed.
4. To install the demo version, there is a special parameter that must be passed to the installer, as follows:
  - a. Open a command prompt (“Run as administrator” to avoid access issues.)
  - b. Change to the directory where you have stored setup.exe.
  - c. Execute the following command: **setup.exe -D\$DEMO\$=YES**
  - d. Follow the GUI prompts for a standard NSM installation. (Do not install NSCM.)

Note that the exact syntax and case above are required to install the demo version.

---

### TROUBLESHOOTING THE INSTALLATION

If you pass the installer an invalid parameter, e.g., “-d” instead of “-D”, the installer will come into memory for a moment, but quickly drop out.

If you instead pass the installer the correct parameter, but an unknown/wrong value, e.g., “-D\$demo\$=yes” (incorrect casing of “demo” and “YES”), the production NSM will be installed.

So, if the installer does not launch and complete as expected, you likely passed it an invalid parameter. If it does indeed complete successfully, there are two ways to confirm that you passed it the correct value:

- You can view the parameter value passed to the installer in the following file:  
**<INSTALL\_DIR>/App/UninstallerData/Logs/installer\_debug.txt**
- Log into the GUI. If the demo was installed, you should see a single IPS sensor (called “NS9200”) and a single NTBA appliance (called “NTBA-GARUDA”) managed. If the production version was installed, there will be no devices managed.

---

## REPEAT FOR EACH DEMO SESSION

1. Confirm that the NSM is up and running. E.g., log into the NSM GUI.
2. Open a command prompt (“Run as administrator” to avoid access issues) and start the demo using the following command:

```
<INSTALL_DIR>\App\diag\Demo\demo-run.bat
```

### Notes:

1. Alert generation stops automatically after a few hours. To restart alert generation, simply close out the existing command prompts created by demo-run.bat and execute demo-run.bat again.

## DEMO CHECKLIST

1. Log into the NSM GUI.
2. On the Dashboard, make sure you have selected a time period so that **Zeus** shows up on the *Top Callback Activity* monitor.
3. Click Zeus and confirm that the IP address **172.16.232.9** (jscott) is present on the *Callback Activity* page.
4. Go to the *Malware Files* page on the *Analysis* menu and confirm that the following hash has the “info” icon in the *NSP Analysis* and *Advanced Threat Defense* columns: **a4bf70bdfa21192c1b33f44fb087220c** ⓘ
5. Ensure that you can click those info icons and view the engine-specific details.

### Troubleshooting Tips:

1. If you don’t see the above after recently starting the demo, wait up to 15 minutes and try again. Alerts are generated semi-randomly, so it may take a few alert generation cycles for the above combinations to be created.
2. If you see an error when trying to access the ATD-specific details for the above hash, restart the *McAfee Network Security Manager* service and try again.

## FICTIONAL COMPANY PROFILE FOR THE DEMO

<b>Company Name:</b>	H.E. Ltd.
<b>Founded:</b>	May, 1995
<b>Global Operations:</b>	United States - 751 employees Europe – 562 Japan – 437
<b>Annual Revenue:</b>	One of their best kept secrets.

### ABOUT H.E. LTD

H.E. Ltd is a leading company in hybrid engine development and tuning trends. Despite having a small number of employees, they are delivering added value to almost all car manufacturers that play in the fuel-efficiency and hybrid car space.

Their best kept secrets are their intellectual property (specifically when it comes to engineering principles) and their financial results.

### CHARACTERS

<b>Ken Lance:</b>	Security Operations: Network Security Lead
<b>Pete Johnson:</b>	IT Director: 7 direct reports, 5 dotted-line reports
<b>Jonathan Scott:</b>	VP of Development

### DEMO STORY OVERVIEW

In this demo, Ken sees callback activity in the organization. He drills in to find that the endpoint belonging to the VP of Development (Jonathan Scott) appears infected. With just a few clicks, Ken confirms the infection and neutralizes the immediate risk with a simple quarantine action.

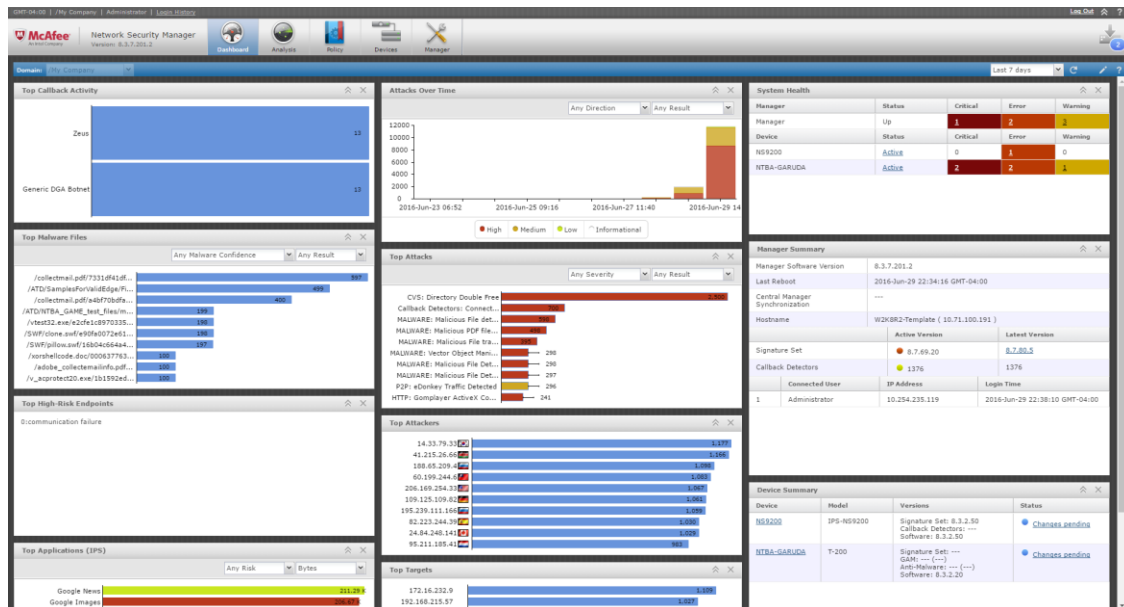
With a few more clicks, Ken takes advantage of NSP integration points to easily gather supporting details (without having to contact other departments), identify the root cause of the infection and take proactive steps to keep his environment protected moving forward.

## THE DEMO SCRIPT

Follow the steps below to walk through the demo.

### 1. REVIEW THE DASHBOARD AND FIND THE TOP CALLBACK ACTIVITY MONITOR

Ken starts his morning routine by logging into the NSP GUI and reviewing its *Dashboard*, and he immediately notices callback activity. He is particularly interested in Zeus activity because he recognizes the name and has heard that it is dangerous, but he doesn't actually know how Zeus works.



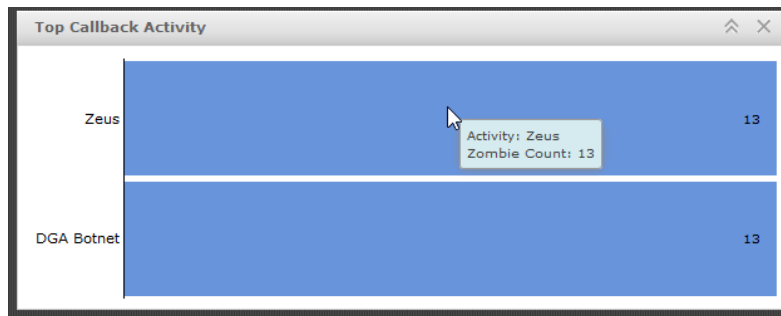
#### Sidebar

McAfee has changed the way threat management is performed by replacing a traditional, bottom-up approach with “progressive disclosure.” The traditional approach, which is still used by our competitors, tries to build workflows around individual events. That puts the burden on the analyst to research and correlate potentially thousands of events, whereas NSP has built the intelligence directly into the workflow. So the *Dashboard* immediately draws your attention to the problem areas, from which you can peel back the layers until you have the appropriate level of detail for the situation at hand.




## 2. CLICK ZEUS ON TOP CALLBACK ACTIVITY MONITOR

So, Ken's first investigative step is to click *Zeus* to get context around this particular activity, such as a description of the activity and an understanding for the internal endpoints involved.

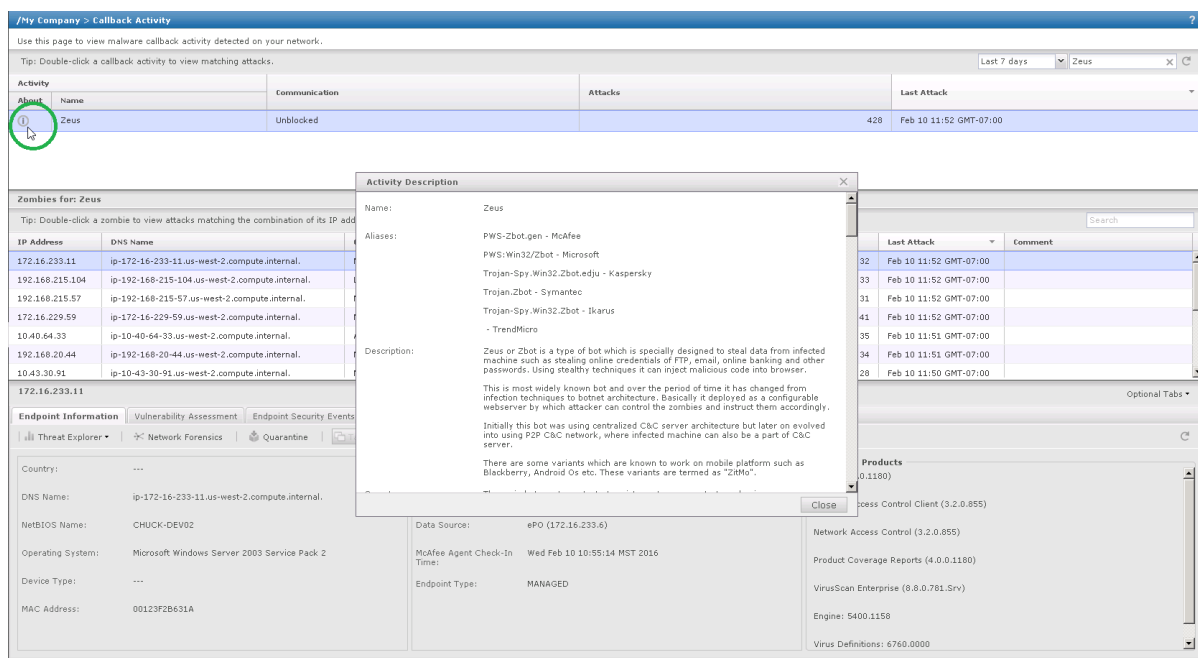


### 3. CLICK THE INFO ICON FOR ZEUS.

Drilling into Zeus brings Ken to the *Callback Activity* page on the *Analysis* menu, which has been filtered for Zeus automatically.

To educate himself, Ken clicks the  “info” icon next to Zeus in the top panel, which displays a significant amount of detail, including a description of Zeus, changes it makes to an endpoint, how it behaves on the network, and even tips for preventing and removing it.

**Note:** Internet access is required to see the activity descriptions.



#### Sidebar

The *Callback Activity* page is organized into 3 panels to provide optimal context:

- \* The top panel provides the overall posture of Zeus on Ken’s network, including its description, whether communication is being blocked or not overall, the total number of attacks during the selected time period and the time of the last one.
- \* The middle panel lists the endpoints that are currently under the control of Zeus, and it exposes the same summary information as the top panel, but for each of the zombied endpoints.
- \* The bottom panel displays all available details about the selected endpoint, including hostname, user, OS, installed products, vulnerability assessment results, and anti-virus and HIP events.

#### 4. SCROLL THROUGH THE LIST OF ZOMBIES AND SELECT JSCOTT.

As Ken scrolls through the list of zombies, he notices the user **jscott** (172.16.232.9), who he recognizes as Jonathan Scott (the VP of Development at H.E. Ltd). He double-clicks that endpoint to view the Zeus-specific events affecting the jscott endpoint.

The screenshot shows a security dashboard with the following sections:

- Activity:** A table showing a single activity named 'Zeus' with status 'Unblocked' and 220 attacks.
- Zombies for: Zeus:** A table listing endpoints affected by Zeus. The row for IP 172.16.232.9 and user 'jscott' is highlighted.
- Endpoint Information:** A detailed view for the selected endpoint (172.16.232.9) showing system details and installed products.

IP Address	DNS Name	OS	User	Communication	Attacks	Last Attack	Comment
10.40.64.33	ip-10-40-64-33.us-west-2.compute.internal.	Apple based OS	schandolu	Unblocked	13	Feb 10 11:16 GMT-07:00	
10.10.20.11	ip-10-10-20-11.us-west-2.compute.internal.	Microsoft Windows Server 2003 Servic...	nprabhu	Unblocked	13	Feb 10 11:16 GMT-07:00	
172.16.232.9	ip-172-16-232-9.us-west-2.compute.internal.	Microsoft Windows XP Base Version	jscott	Unblocked	17	Feb 10 11:16 GMT-07:00	
10.43.46.32	ip-10-43-46-32.us-west-2.compute.internal.	Microsoft Windows Server 2008 R2 64b...	maggy	Unblocked	22	Feb 10 11:15 GMT-07:00	
192.168.215.57	ip-192-168-215-57.us-west-2.compute.internal.	Microsoft Windows Server 2003 Servic...	srajanna	Unblocked	18	Feb 10 11:15 GMT-07:00	
172.16.229.59	ip-172-16-229-59.us-west-2.compute.internal.	Microsoft Windows Server 2003 Servic...	mchitti	Unblocked	14	Feb 10 11:14 GMT-07:00	
172.16.230.81	ip-172-16-230-81.us-west-2.compute.internal.	Microsoft Windows XP Base Version	amohan	Unblocked	19	Feb 10 11:14 GMT-07:00	

Country:	---	Domain/Workgroup:	NSM <th>Installed Products</th> <td>Agent (4.0.0.1180) Endpoint Intelligence Agent (2.0.0.214) Product Coverage Reports (4.0.0.1180) VirusScan Enterprise (6.8.0.781.Wrk) Engine: N/A Virus Definitions: N/A</td>	Installed Products	Agent (4.0.0.1180) Endpoint Intelligence Agent (2.0.0.214) Product Coverage Reports (4.0.0.1180) VirusScan Enterprise (6.8.0.781.Wrk) Engine: N/A Virus Definitions: N/A
DNS Name:	ip-172-16-232-9.us-west-2.compute.internal.	User:	jscott		
NetBIOS Name:	VP-DEV	Data Source:	ePO (172.16.233.6)		
Operating System:	Microsoft Windows XP Base Version	McAfee Agent Check-In Time:	Wed Feb 10 10:55:14 MST 2016		
Device Type:	General Purpose Computing Device	Endpoint Type:	MANAGED		
MAC Address:	000D56CFA04D				

#### Sidebar

At this point, we have narrowed the scope of our investigation to a single activity, Zeus, and the endpoints it is affecting. The advantage here is that we don't need to build manual filters to get a better understanding of the activity's impact. On the contrary, NSP has implicitly created those filters for us as part of its workflow, which provides a natural disclosure of details as you click through it.

5. DOUBLE-CLICK JSCOTT TO OPEN THE ATTACK LOG AND VIEW ZEUS ATTACKS MATCHING HIS ENDPOINT.

Further drilling into jscott’s endpoint brings up the *Attack Log* so Ken can see all Zeus activity specific to jscott’s IP address. The individual attacks and their severities enable Ken to conclude that jscott’s endpoint has likely been compromised. But before he takes action, he’d like to understand the extent of jscott’s suspicious activity on the network.

	Name	Event			Attack Count	Attacker			Target			Callback Activity
		Time	Direction	Result		IP Address	Port	Risk	IP Address	Port	Risk	
1	Callback Detectors: High Confidence C&C Server Name Match	Jan 04, 2016 12:17:51	Outbound	Inconclusive	1	172.16.232.9	53	●	10.43.30.91	6015	●	Zeus
2	Callback Detectors: High Confidence C&C Server Name Match	Jan 04, 2016 12:16:21	Outbound	Inconclusive	1	172.16.232.9	53	●	10.40.64.33	6015	●	Zeus
3	Callback Detectors: High Confidence C&C Server Name Match	Jan 04, 2016 12:13:35	Outbound	Inconclusive	1	172.16.232.9	53	●	172.16.230.151	6015	●	Zeus
4	Callback Detectors: High Confidence C&C Server Name Match	Jan 04, 2016 12:13:15	Outbound	Inconclusive	1	195.239.111.166	53	●	172.16.232.9	6015	●	Zeus
5	Callback Detectors: High Confidence C&C Server Name Match	Jan 04, 2016 12:13:00	Outbound	Inconclusive	1	172.16.232.9	53	●	10.10.20.11	6015	●	Zeus
6	Callback Detectors: High Confidence C&C Server Name Match	Jan 04, 2016 12:12:55	Outbound	Inconclusive	1	24.84.248.141	53	●	172.16.232.9	6015	●	Zeus

**Sidebar**

With a simple double-click on the jscott endpoint, we are presented with the individual Zeus activities that, collectively, caused this endpoint to be considered a Zeus zombie and therefore brought to our attention. At this point, we already have a narrowed list of pertinent attacks, and the ability to view alert details, export packet captures and update policy are each just a click away. Contrast this against the traditional method of sifting through 1000s of individual events to determine if there is any connection between them.

## 6. REMOVE THE ZEUS FILTER TO VIEW ALL ATTACKS MATCHING JSCOTT'S ENDPOINT.

To see all attacks involving jscott's endpoint, Ken simply clicks the *Callback Activity* column and clears the *Filters* checkbox (see below screenshot) to remove the Zeus filter from the *Attack Log* window, and he quickly understands from the additional attacks that jscott's endpoint has been involved in many other attacks as well.

	Name	Event			Attack Count	Attacker			Target			Callback Activity
		Time	Direction	Result		IP Address	Port	Risk	IP Address	Port	Risk	
1	HTTP: Allaire JRun JSP Execute	Jan 04, 2016 12:18:40	Outbound	Inconclusive	1	172.16.232.9	1063	●	172.16.230.81	80	●	Sort Ascending
2	Botnet: DGA Heuristic Detection of C&C Server in DNS Response	Jan 04, 2016 12:18:36	Outbound	Inconclusive	1	41.215.26.66	53	●	172.16.232.9	4670	●	Sort Descending
3	DTSPDCD: CDE dtspcd Remote Buffer Overflow	Jan 04, 2016 12:18:35	Outbound	Smart Blocked	1	172.16.232.9	4185	●	10.40.39.22	6112	●	Columns
4	IRC: mIRC Userhost Buffer Overflow	Jan 04, 2016 12:17:55	Outbound	n/a	1	195.239.111.166	9908	●	172.16.232.9		Zeus	Filters
5	Callback Detectors: High Confidence C&C Server Name Match	Jan 04, 2016 12:17:51	Outbound	Inconclusive	1	172.16.232.9	53	●	10.43.30.91	6015	●	Zeus
6	BACKDOOR: Mneah	Jan 04, 2016 12:17:00	Inbound	Attack Success...	1	41.215.26.66	1055	●	172.16.232.9	4666	●	---
7	Callback Detectors: High Confidence C&C Server Name Match	Jan 04, 2016 12:16:56	Outbound	Inconclusive	1	41.215.26.66	53	●	172.16.232.9	6016	●	---
8	BACKDOOR: NetTrash/WinRAT/Oxon	Jan 04, 2016 12:16:50	Outbound	Smart Blocked	1	188.65.209.4	1243	●	172.16.232.9	23005	●	---
9	Callback Detectors: High Confidence C&C Server Name Match	Jan 04, 2016 12:16:26	Outbound	Inconclusive	1	172.16.232.9	53	●	172.16.229.59	6016	●	---
10	Callback Detectors: High Confidence C&C Server Name Match	Jan 04, 2016 12:16:21	Outbound	Inconclusive	1	172.16.232.9	53	●	10.40.64.33	6015	●	Zeus
11	Botnet: Heuristic Detection of Fast Flux DNS	Jan 04, 2016 12:16:11	Unknown	Inconclusive	1	195.239.111.166	53	●	172.16.232.9	---	●	---
12	Botnet: Heuristic Detection of Fast Flux DNS	Jan 04, 2016 12:16:06	Unknown	Inconclusive	1	172.16.232.9	53	●	192.168.215.57	---	●	---
13	DCERPC: Suspicious DCERPC Call	Jan 04, 2016 12:15:39	Outbound	Inconclusive	1	172.16.232.9	42308	●	10.40.39.22	445	●	---

### Sidebar

The Attack Log makes it very easy to increase or, in this case, decrease the scope of information displayed to provide the appropriate level of focus.

## 7. SELECT AN ATTACK AND REVIEW THE "OTHER ACTIONS" BUTTON.

Feeling comfortable that jscott has indeed been compromised, but not ready to take action just yet, Ken considers his options...

He selects an attack and presses the *Other Actions* button to review the possibilities.

(There is no need for policy change or exception creation at this point, and it is a bit premature to take quarantine or tagging action on the endpoint.)

The screenshot shows the 'Attack Log' window with a table of attack events. The table has columns for Name, Event (Time, Direction, Result, Attack Count), Packet Capture, Attacker (IP Address, Port, Risk), Target (IP Address, Port, Risk), Callback Activity, and Layer 7. A green circle highlights the 'Other Actions' button in the bottom row of the table.

Name	Event				Packet Capture	Attacker			Target			Callback Activity	Layer 7
	Time	Direction	Result	Attack Count		IP Address	Port	Risk	IP Address	Port	Risk		
1	Feb 04, 2016 09:08:28	Outbound	Inconclusive	1	Export	195.239.111.166	53	Zeus	172.16.232.9	6015	Zeus	---	
2	Feb 04, 2016 09:06:18	Outbound	Inconclusive	1	Export	172.16.232.9	53	Zeus	192.168.20.44	6015	Zeus	---	
3	Feb 04, 2016 09:06:13	Outbound	Inconclusive	1	Export	172.16.232.9	53	Zeus	172.16.233.11	6015	Zeus	---	
4	Feb 04, 2016 09:04:23	Outbound	Inconclusive	1	Export	172.16.232.9	53	Zeus	10.40.39.22	6015	Zeus	---	
5	Feb 04, 2016 09:03:18	Outbound	Inconclusive	1	Export	206.169.254.33	53	Zeus	172.16.232.9	6015	Zeus	---	
6	Feb 04, 2016 09:01:48	Outbound	Inconclusive	1	Export	172.16.232.9	53	Zeus	172.16.230.151	6015	Zeus	---	
7	Feb 04, 2016 08:59:53	Outbound	Inconclusive	1	Export	172.16.232.9	53	Zeus	192.168.215.104	6015	Zeus	---	
8	Feb 04, 2016 08:59:00	Outbound	Inconclusive	1	Export	172.16.232.9	53	Zeus	192.168.215.57	6015	Zeus	---	
9	Feb 04, 2016 08:59:03	Outbound	Inconclusive	1	Export	109.125.109.82	53	Zeus	172.16.232.9	6015	Zeus	---	
10	Feb 04, 2016 08:58:48	Outbound	Inconclusive	1	Export	188.65.209.4	53	Zeus	172.16.232.9	6015	Zeus	---	
11	Feb 04, 2016 08:57:18	Outbound	Inconclusive	1	Export	172.16.232.9	53	Zeus	172.16.229.59	6015	Zeus	---	
12	Feb 04, 2016 08:55:47	Outbound	Inconclusive	1	Export	14.33.79.33	53	Zeus	172.16.232.9	6015	Zeus	---	
13	Feb 04, 2016 08:54:12	Outbound	Inconclusive	1	Export	172.16.232.9	53	Zeus	172.16.232.9	6015	Zeus	---	
14	Feb 04, 2016 08:53:27	Outbound	Inconclusive	1	Export	172.16.232.9	53	Zeus	10.43.30.91	6015	Zeus	---	
15	Feb 04, 2016 08:50:57	Outbound	Inconclusive	1	Export	60.199.244.6	53	Zeus	172.16.232.9	6015	Zeus	---	
16	Feb 04, 2016 08:50:02	Outbound	Inconclusive	1	Export	172.16.232.9	53	Zeus	172.16.230.151	6015	Zeus	---	
17	Feb 04, 2016 08:47:27	Outbound	Inconclusive	1	Export	172.16.232.9	53	Zeus	10.40.64.33	6015	Zeus	---	
18	Feb 04, 2016 08:47:07	Outbound	Inconclusive	1	Export	188.65.209.4	53	Zeus	172.16.232.9	6015	Zeus	---	
19	Feb 04, 2016 08:45:17	Outbound	Inconclusive	1	Export	172.16.232.9	53	Zeus	172.16.230.151	6015	Zeus	---	
20	Feb 04, 2016 08:44:52	Outbound	Inconclusive	1	Export	172.16.232.9	53	Zeus	172.16.230.81	6015	Zeus	---	
21	Feb 04, 2016 08:44:07	Outbound	Inconclusive	1	Export	195.239.111.166	53	Zeus	172.16.232.9	6015	Zeus	---	
22	Feb 04, 2016 08:43:47	Outbound	Inconclusive	1	Export	172.16.232.9	53	Zeus	10.43.46.32	6015	Zeus	---	
23	Feb 04, 2016 08:41:53	Outbound	Inconclusive	1	Export	172.16.232.9	53	Zeus	172.16.230.81	6015	Zeus	---	

## 8. CLOSE THE ATTACK LOG TO INVESTIGATE ENDPOINT-SPECIFIC DETAILS.

Instead, Ken decides to take a step back and look more closely at jscott's endpoint...

Ken wants to understand if the security software on jscott's endpoint is reporting anything out of the ordinary. So he backs out of the Attack Log (by clicking the *X* in the top-right corner or the *<Back* button in the bottom-right corner) and reviews the tabs on the bottom panel of the previous (*Callback Activity*) page.

The screenshot shows a security console interface for IP 172.16.232.9. It features a navigation bar with tabs for 'Endpoint Information', 'Vulnerability Assessment', and 'Endpoint Security Events'. Below the navigation bar, there are two main sections: 'Latest Anti Virus Events' and 'Latest Host Intrusion Prevention Events'. The 'Latest Anti Virus Events' section contains one event: 'Anti-virus Standard Protection:Prevent IRC communication' with a severity of 'access protection' and an action of 'blocked'. The 'Latest Host Intrusion Prevention Events' section contains three events, all of which are 'TCP Port Scan' with a severity of 'High' and a reaction of 'BLOCK'. The source IP for all three events is 172.16.226.86.

Event Time	Threat Name	Threat Type	Action Taken	File Path	Detection Mode
Jan 01, 2015 18:10:12	Anti-virus Standard Protection:Prevent IRC communication	access protection	blocked		OAS

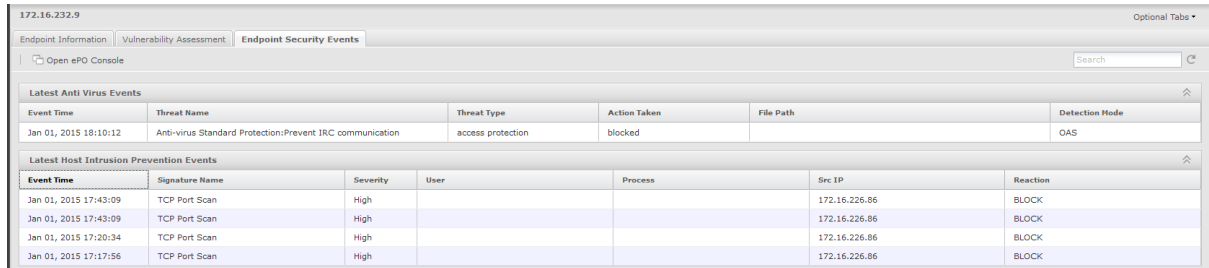
Event Time	Signature Name	Severity	User	Process	Src IP	Reaction
Jan 01, 2015 17:43:09	TCP Port Scan	High			172.16.226.86	BLOCK
Jan 01, 2015 17:43:09	TCP Port Scan	High			172.16.226.86	BLOCK
Jan 01, 2015 17:29:34	TCP Port Scan	High			172.16.226.86	BLOCK
Jan 01, 2015 17:17:56	TCP Port Scan	High			172.16.226.86	BLOCK

### Sidebar

Of note is the fact that the customer did not lose his context when he went to view the corresponding attacks – the *Attack Log* was opened on top of the *Callback Activity* page – so he was brought back to the details of Zeus and jscott's endpoint, and can pick up right where he left off.

## 9. CLICK THE ENDPOINT SECURITY EVENTS TAB.

On the bottom panel of the page, Ken can see on the *Endpoint Security Events* tab that the anti-virus software running on jscott's machine has blocked IRC communication. He further notices that HIPS has blocked port scans by an internal IP address, which could very well be the source of the infection. So Ken now wants to confirm that Jonathan is running the latest virus definitions.



172.16.232.9						Optional Tabs ▾
Endpoint Information		Vulnerability Assessment		Endpoint Security Events		
Open ePO Console						Search
<b>Latest Anti Virus Events</b>						⌵
Event Time	Threat Name	Threat Type	Action Taken	File Path	Detection Mode	
Jan 01, 2015 18:10:12	Anti-virus Standard Protection:Prevent IRC communication	access protection	blocked		OAS	
<b>Latest Host Intrusion Prevention Events</b>						⌵
Event Time	Signature Name	Severity	User	Process	Src IP	Reaction
Jan 01, 2015 17:43:09	TCP Port Scan	High			172.16.226.86	BLOCK
Jan 01, 2015 17:43:09	TCP Port Scan	High			172.16.226.86	BLOCK
Jan 01, 2015 17:20:34	TCP Port Scan	High			172.16.226.86	BLOCK
Jan 01, 2015 17:17:56	TCP Port Scan	High			172.16.226.86	BLOCK

### Sidebar

By clicking the *Endpoint Security Events* tab, we can view the last 10 anti-virus alerts and the last 10 HIPS events. If customers use McAfee for Desktop protection, there is nothing more powerful than showing the integration between ePO and NSM. If customers don't currently use McAfee on the Desktop, this can instead give them a sense for what they are currently missing!



## 10. CLICK THE VULNERABILITY ASSESSMENT TAB

On his way to check out the endpoint's DAT version, Ken takes advantage of the *Vulnerability Assessment* tab to see if it exposes anything interesting, such as a high-risk vulnerability or suspicious open ports. In this case, there's no vulnerability information that helps Ken isolate this particular issue.

172.16.232.9 Optional Tabs ▾

Endpoint Information | **Vulnerability Assessment** | Endpoint Security Events

Scan for Vulnerabilities Search

**General Activity** ⤴

Overall Criticality: Significant

Last Scan Time: 2015-01-01 16:11:01.0

By Scan Engine: suresh-dev3

**Open Ports** ⤴

ProtoPort	Service	Description
udp/123	ntp	Network Time Protocol

**Vulnerabilities** ⤴

Risk	Name	CVE
● Medium	Windows Firewall Standard Profile Log File Path Policy	<a href="#">CVE-1999-0585</a> ...

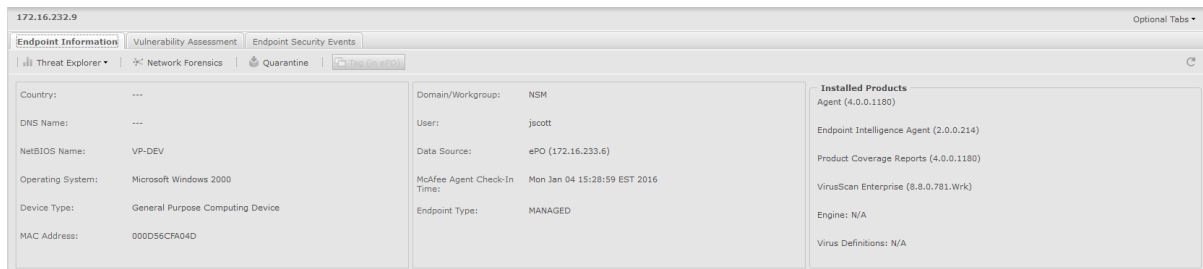
### Sidebar

This content is made available by McAfee Vulnerability Manager (MVM). The value of showing this tab is once again the integration with other McAfee products and how they help build a solution that is greater than the sum of its individual parts. Of note here is the *Scan for Vulnerabilities* button, which was added in 8.3. It enables the customer to kick off a new scan against an endpoint, as needed, to get updated information.

## 11. CLICK THE ENDPOINT INFORMATION TAB

Ken continues to the *Endpoint Information* tab to see the countermeasures installed on the endpoint, such as the McAfee Agent, VirusScan software and EIA. He sees that anti-virus software is installed, but the engine version and virus definitions have values of “N/A”, which is of course inconsistent with his expectations.

It looks like something or someone is interfering with the anti-virus software installed on jscott’s endpoint. Ken will continue to explore the details of this issue, but he already has enough insight and evidence to know it’s time to take action.



### Sidebar

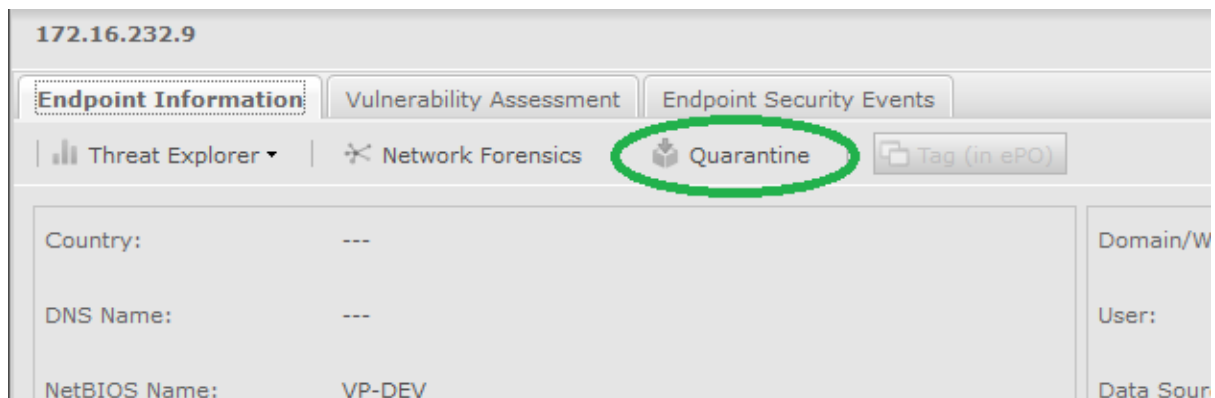
The information shown on this tab is gathered automatically from a combination of ePO, MVM and the NSP sensor itself, and can be extremely useful when isolating the root cause of a compromise.

From this tab, the indication is that malware was able to circumvent the Desktop protection. (Be careful here because we don’t want to make our Desktop products look bad. On the contrary, we should convey that it’s extremely difficult to shut down McAfee Desktop protection, so perhaps the company has a policy that permits users to disable on-access scanning on their own, for example.)

## 12. HOVER OVER THE QUARANTINE BUTTON. (NO NEED TO PRESS IT)

Ken walks over to his manager, Pete, and explains the situation. Pete sanctions Ken to quarantine Jonathan's endpoint until further notice. Once quarantined, no traffic originating from Jonathan's machine will be able to traverse the segments that are protected by the NSP sensor.

With jscott's endpoint safely quarantined, Ken can further research how it actually came to be infected and any exposure that may have come from that infection.



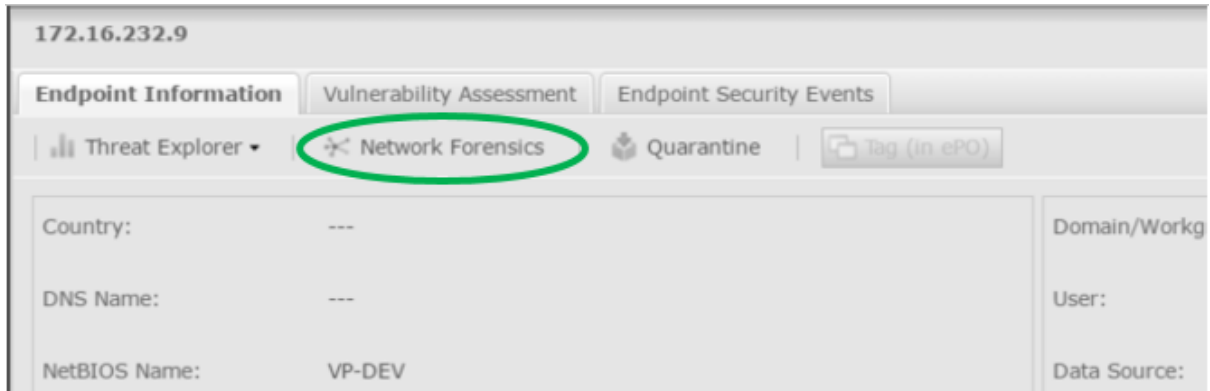
### Sidebar

That which started as an anomalous activity (Zeus) quickly allowed Ken to isolate, identify and take action on a compromised endpoint. The *Callback Activity* page is just one example of the overall logic applied across all the *Analysis* pages, which is to correlate data in a way that gives the customer a list of items that need attention – be it callback activity, malware files, high-risk endpoints, etc. – and makes it easy for him to get the context he needs to make an informed decision quickly. Note the small number of clicks it took to get us to this point!

jscott's endpoint is now quarantined. With one click, we've stopped all communication from his machine through the NSP sensor. It doesn't get any easier than that!

13. CLICK THE NETWORK FORENSICS BUTTON.

Ken wants to raise his situational awareness around the recent events and understand if there has been exposure, so he opens the *Network Forensics* window from the *Endpoint Information* tab, which displays network activity to and from jscott's endpoint. The content shown in this window comes from our NTBA solution, which collects NetFlow data from routers and/or IPS sensors.



## 14. REVIEW NETWORK FORENSICS DATA.

Ken looks at the 60 minutes before (and after) he quarantined the endpoint. The *Summary* window summarizes the traffic to and from the endpoint during that time.

The *Suspicious Flows* grid shows all the flows that took place just before or after an attack, which can help determine whether jscott's endpoint has been spreading Zeus on the internal network. (In this case, it is a good sign that no flows with other internal endpoints have been seen!)

The *Suspicious Flows* grid also takes advantage of our GTI capabilities to highlight activities to and from this endpoint that may put the endpoint or the rest of the internal network at risk. In particular, if a flow includes a URL, file or endpoint whose risk is known to be bad or cannot be verified, it is also shown here.

In this case, the endpoint appears to be the victim of a drive-by download – it browsed to a compromised Website where it was exploited and infected, and it may well now be controlling external zombies of its own.

Ken doesn't recognize the name of the executable running on jscott's machine, nor does he recognize the PDF file it downloaded, but he sees that both have a *Very High* malware confidence, so he notes the information for both files to be able to investigate them across his enterprise:

- **gkcalt.exe** (9c7aa16e59d7a54a1bb10a34ce1fc763)
- **collectmail.pdf** (a4bf70bdfa21192c1b33f44fb087220c)

The screenshot displays the Network Forensics interface for endpoint 172.16.232.9. The **Summary** window shows analysis details for Jan 04, 2016, 03:33 PM. It lists connections from and to the endpoint, including applications like BitTorrent and GoToMyPc, and services like SMTP and ntp. The endpoint's risk level is marked as **Very High**.

The **Suspicious Flows** window shows a table of network activity. Two entries are circled in red:

Time	Suspicious Activity	Source	Destination	Applications	Attack	File / URL Accessed
		Endpoint	Endpoint		Name	
1 Jul 07 04:39:42	Suspicious connecti... New service detected	164.39.1.52	172.16.232.9	TCP	---	---
2 Jul 07 04:39:42	Suspicious connecti...	174.2.3.44	172.16.232.9	TCP	---	---
3 Jul 07 04:39:42	Unverified connectio... Source matches att...	145.65.9.7	172.16.232.9	TCP	---	---
4 Jul 07 04:29:43	Unverified connectio... Attack detected Suspicious file malw...	172.16.232.9	145.65.9.7	SMTP	MALWARE: M...	collectmail.pdf (a4bf70bdfa21192...)
5 Jul 07 04:29:42	Suspicious connecti... Attack detected Unverified URL risk	172.16.232.9	92.65.32.31	HTTP	HTTP: SQL In...	http://www.bigtorrent.com
6 Jul 07 04:29:42	Unverified connectio... Attack detected Suspicious URL risk	172.16.232.9	51.12.92.92	HTTP	HTTP: Malfor...	http://www.musiccocoz.com

### Sidebar

NTBA can certainly fill the visibility gap when it doesn't make fiscal sense to place an IPS sensor on a particular segment, but the *Network Forensics* window is a good example of how having an NTBA appliance as a standard part of your solution can provide unprecedented insight.

## 15. INVESTIGATE GKCALT.EXE ON THE ENDPOINT EXECUTABLES PAGE.

Ken jumps to the *Endpoint Executables* page to get a global view of **gkcalt.exe**'s posture and prevalence on his network.

Ken could normally type the executable name into the *Search* field to filter against it, but the *Endpoint Executables* page provides a default filter to only show the executables with *High or above* malware confidence, so gkcalt.exe is already visible by default. Ken simply selects it to see its details.

The *EIA Details* tab on the bottom of the page shows product name and version information for signed executables, and it summarizes the malware-specific findings.

In this case, the executable does not have a certificate, nor is it known to GTI, which is a good indication that it is homegrown and new. Ken reviews the *File Execution Summary* tab to get a sense of how active the file is, and he then reviews (and saves out) the *File Execution Details* tab, which confirm malicious behavior.

Actions	Hash	Name	Version	Malware Confidence	Classification	First Seen	Last Seen
<a href="#">Take action</a>	d421c3f3848d23ad47b3...	skype.exe	---	High	Blacklisted	Jul 08, 2013 04:50:00	Jul 08, 2013 04:50:00
<a href="#">Take action</a>	9c7aa16e59d7a54a1bb10...	gkcalt.exe	---	Very High	Unclassified	Jul 08, 2013 08:11:00	Jul 08, 2013 13:15:00
<a href="#">Take action</a>	aaf5faf226f15542d4f1c1d...	flame.exe	---	Very High	Unclassified	Jul 08, 2013 08:11:00	Jul 08, 2013 13:15:00

**Details for: gkcalt.exe**

**EIA Details** | Endpoints | Applications

Hash: 9c7aa16e59d7a54a1bb10a34ce1fc763

Binary Name: gkcalt.exe

Product Name: ---

Version: ---

**Malware Summary**

Malware Confidence: Very High

Malware Name: ---

**File Execution Summary** | File Execution Details

A summary of the tasks performed during the execution of this program

1. connects to internet
2. creates files with filenames similar to system files
3. creates new files
4. creates new processes

### Sidebar

This page helps us to understand a few things:

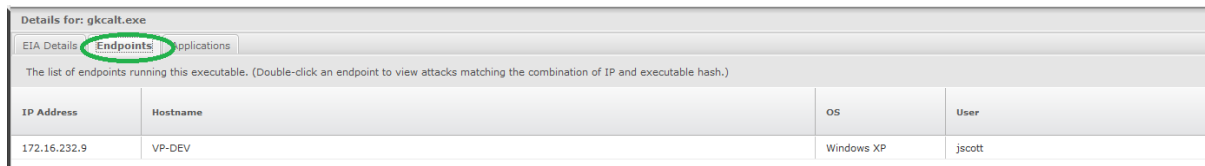
- \* The list of executables running on the network and their malware confidences.
- \* For a given executable, the reason for its malware confidence, including full execution details when *Raptor* is used by EIA to analyze the file.
- \* For a given executable, which endpoints are using it and over which applications.

Note: As is the case on all *Analysis* pages, the customer can double click a hash, endpoint or application to view attacks/PCAPs matching them.

## 16. CLICK THE ENDPOINTS TAB.

Ken goes to the *Endpoints* tab where he is very happy to confirm that only jscott's machine has been seen running gkcalt.exe.

Now he can be proactive...



Details for: gkcalt.exe

EIA Details **Endpoints** Applications

The list of endpoints running this executable. (Double-click an endpoint to view attacks matching the combination of IP and executable hash.)

IP Address	Hostname	OS	User
172.16.232.9	VP-DEV	Windows XP	jscott

## 17. BLACKLIST GKCALT.EXE.

Ken clicks the *Take action* hyperlink for gkcalt.exe and selects *Blacklist*.

Moving forward:

- If NTBA sees gkcalt.exe running on another endpoint, an alert will be generated.
- If an IPS sensor sees gkcalt.exe transferred on the wire, an alert will be generated and the transfer blocked.

**/My Company > Endpoint Executables**

Use this page to view the details of executables running on your endpoints.

Tip: Double-click an executable to view matching attacks.

Executable				Malware Confidence	Classification
Actions	Hash	Name	Version		
<a href="#">Take action</a>	d421c3f3848dd23ad47b3...	skype.exe	---	High	Blacklisted
Take action   ▾	9c7aa16e59d7a54a1bb10...	gkcalt.exe	---	Very High	Unclassified
Whitelist	aaf5faf226f15542d4f1c1d...	flame.exe	---	Very High	Unclassified

Blacklist  
Mark as  
Unclassified

### Sidebar

Note that the response actions taken by IPS sensors for blacklisted executables are ultimately controlled in the advanced malware policy.




## 18. INVESTIGATE COLLECTMAIL.PDF ON THE MALWARE FILES PAGE.

Ken now jumps to the *Malware Files* page to get a global view of collectmail.pdf's posture and prevalence on his network.

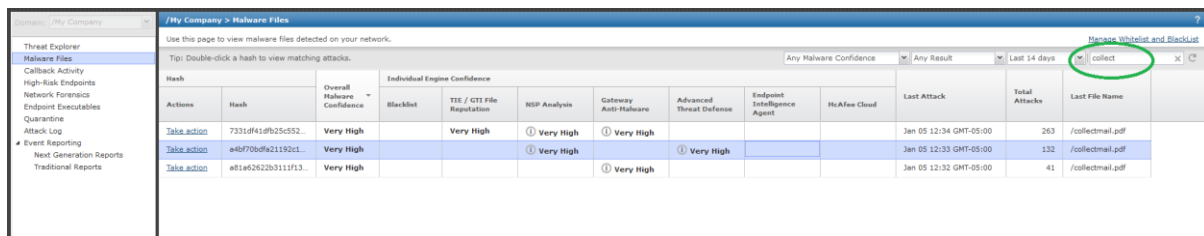
He starts to type the file name into the search field and quickly realizes that there are multiple malware files that use the same file name, so he consults the hash to clarify the file in question.

**(a4bf70bdfa21192c1b33f44fb087220c)**

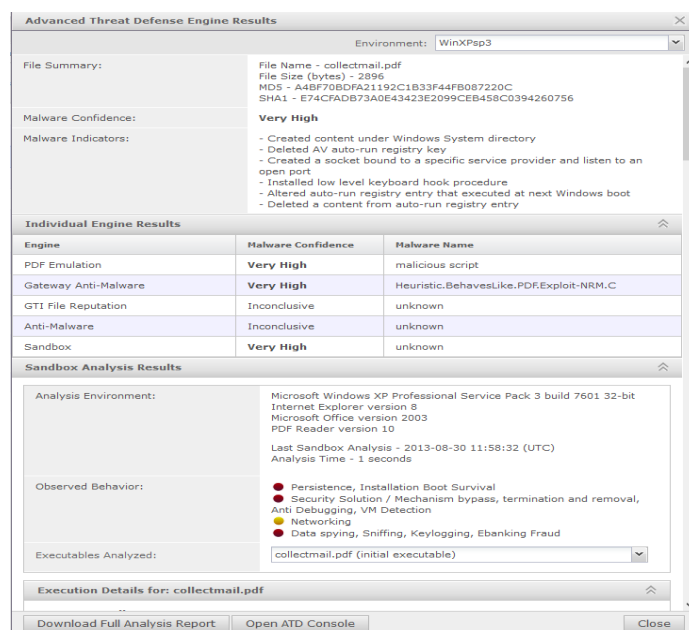
At a glance, Ken can see that multiple engines have caught the file. Ken clicks the  "info" icon to view engine-specific details for each engine:

- The *NSP Analysis* engine displays a summary of the highlights seen when the JavaScript code within the PDF file is analyzed, and it even includes the malicious JavaScript code itself.
- The *ATD* engine provides a comprehensive report of the analysis performed on the file, including down-select engines that were used and full sandbox execution results.

Ken could double-click the file in question to view all attacks containing it, but thanks to the engine-specific details, Ken is already convinced that the file is malicious, and he can now take action to block it in the future too.



Hash	Overall Malware Confidence	Blacklist	TIE / GTI File Reputation	NSP Analysis	Gateway Anti-Malware	Advanced Threat Defense	Endpoint Intelligence Agent	RuAfee Cloud	Last Attack	Total Attacks	Last File Name
<a href="#">Take action</a> 7331df41df923c552	Very High		Very High	Very High	Very High				Jan 05 12:34 GMT-05:00	263	/collectmail.pdf
<a href="#">Take action</a> a4bf70bdfa21192c1b33f44fb087220c	Very High			Very High		Very High			Jan 05 12:33 GMT-05:00	132	/collectmail.pdf
<a href="#">Take action</a> e81a6262b29311f13	Very High				Very High				Jan 05 12:32 GMT-05:00	41	/collectmail.pdf



**Advanced Threat Defense Engine Results**

Environment: WinXPsp3

**File Summary:**  
 File Name - collectmail.pdf  
 File Size (bytes) - 2896  
 MD5 - A4BF70BDF421192C1B33F44FB087220C  
 SHA1 - E74CFAD873A0E43423E2099CEB458C0394260756

**Malware Confidence:** **Very High**

**Malware Indicators:**  
 - Created content under Windows System directory  
 - Deleted AV auto-run registry key  
 - Created a socket bound to a specific service provider and listen to an open port  
 - Installed low level keyboard hook procedure  
 - Altered auto-run registry entry that executed at next Windows boot  
 - Deleted a content from auto-run registry entry

**Individual Engine Results**

Engine	Malware Confidence	Malware Name
PDF Emulation	Very High	malicious script
Gateway Anti-Malware	Very High	Heuristic.BehavesLike.PDF.Exploit-NRM.C
GTI File Reputation	Inconclusive	unknown
Anti-Malware	Inconclusive	unknown
Sandbox	Very High	unknown

**Sandbox Analysis Results**

**Analysis Environment:**  
 Microsoft Windows XP Professional Service Pack 3 build 7601 32-bit  
 Internet Explorer version 8  
 Microsoft Office version 2003  
 PDF Reader version 10  
 Last Sandbox Analysis - 2013-08-30 11:58:32 (UTC)  
 Analysis Time - 1 seconds

**Observed Behavior:**  
 ● Persistence, Installation Boot Survival  
 ● Security Solution / Mechanism bypass, termination and removal, Anti-Debugging, VM Detection  
 ● Networking  
 ● Data spying, Sniffing, Keylogging, Ebanking Fraud

**Executables Analyzed:** collectmail.pdf (initial executable)

**Execution Details for: collectmail.pdf**

Download Full Analysis Report | Open ATD Console | Close

### Sidebar

The integration with ATD is a good example of NSP's zero-day anti-malware feature set, which is above and beyond the capabilities of a traditional network IPS solution. Note that, since v8.2, NS-series sensors perform GAM analysis locally. So files are only sent to ATD for analysis if they are not first detected by the local blacklist, GTI/TIE, the NSP Analysis engine or GAM, which optimizes performance. The tight integration between NSP and ATD helps the customer enhance the security of his network with minimal extra effort.

## 19. BLACKLIST COLLECTMAIL.PDF.

Ken clicks the *Take action* hyperlink for his instance of the collectmail.pdf file and selects *Blacklist*.

Moving forward, if an IPS sensor sees that version of collectmail.pdf transferred on the wire, an alert will be generated and the transfer blocked.

**/My Company > Malware Files**

Use this page to view malware files detected on your network.

Tip: Double-click a hash to view matching attacks.

Actions	Hash	Overall Malware Confidence	Individual Engine Confidence				
			Blacklist	TIE / GTI File Reputation	NSP Analysis	Gateway Anti-Malware	Advanced Threat Defense
<a href="#">Take action</a>	7331df41dfb25c55271c1f111ef...	Very High		Very High	<i>i</i> Very High	<i>i</i> Very High	
Take Action ▾	a4bf70bdfa21192c1b33f44fb08...	Very High			<i>i</i> Very High		<i>i</i> Very High
Export	a81a62622b3111f139ec4600ed...	Very High				<i>i</i> Very High	
Submit							
White List							
Black List							

### Sidebar

Note that the response actions taken by IPS sensors on blacklisted files are ultimately controlled in the advanced malware policy.

## RECAP

Today's attacks are multilayered and typically targeting high-value assets in the organization.

In our user story, we initially detected callback activity and readily followed the trail back to an infected VP. With a few, easy steps, we confirmed the infection and quarantined the endpoint. And with just a few more, we learned the root cause of the infection and took action to neutralize the threat moving forward.

The same situation would have been challenging to diagnose and remediate with traditional network security tools because they simply don't provide the same level of intelligence built directly into the workflows.

NSP makes it easy for you to educate yourself, draw quick and accurate conclusions, and to take meaningful action.