

Catching the “Inception Framework” Phishing Attack

 logrhythm.com/blog/catching-the-inception-framework-phishing-attack

January 14, 2015

A new sophisticated, layered and targeted malware has been hitting Russia and Russian interests lately, and is starting to spread out.

This has been named “Inception Framework” because of its massively layered design, in reference to the 2010 “Inception” movie.

The malware is very ingenious:

- exploits at least [CVE-2010-3333](#), [CVE-2012-0158](#) and [CVE-2014-1761](#)
- exists only in RAM
- polymorph
- targeted
- multilayered
- C&C hidden in normal traffic and to legitimate servers
- attacks both computers and mobile phones
- etc...

But all is not lost, as there are a very few things that can still be caught when a person is infected.

As per BlueCoat’s very informative [blog post](#):

Signs of compromise:

- *Unauthorized WebDAV traffic*
- *exe continuously running in the process list*

Ways to prevent infection:

- Keep software updated
- Don’t jailbreak mobile phones
- Don’t Install apps from unofficial sources

Signs of being targeted:

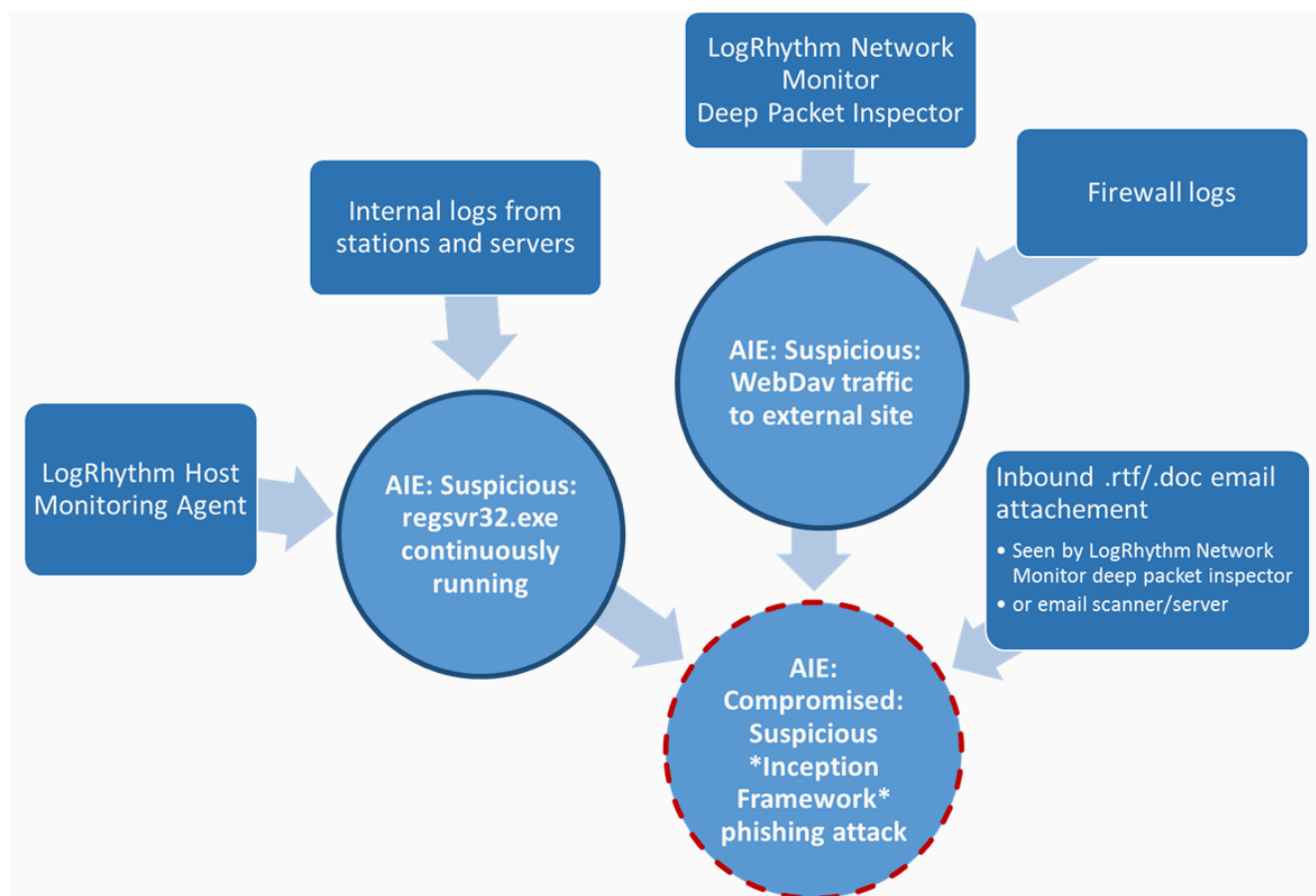
- *Unsolicited emails containing rtf documents*
- Unsolicited emails or MMS messages suggesting smart phone applications need updating

All the above vectors that are italic are covered by the correlation set below.

Layered approach to detection

For such a layered malware, it only sounds appropriate to engage in a layered detection method:

1. So, first we will track any “regsvr32.exe” process that starts but never stops, on servers and workstations, using one real-time AIE correlation rule, that will spit out an Event flagged as Security: Suspicious and an Alarm.
2. In parallel we’ll keep an eye on any outbound WebDav traffic, using a second real-time AIE correlation rule and generate a Security: Suspicious Event and an Alarm here too.
3. Finally, we will corroborate all these correlations together and if they both occur on the machine of someone who just received an inbound email with an RTF or Word documents attached, then raise a Security:Compromised Event as well as an Alarm.



! Please note




These correlations work together, even though they can each emit their own Alarm.

The use of LogRhythm Network Monitor is a great plus, as it allows more vectors to be caught, but is not required by all the correlations below and thus we could still detect the malware without it.

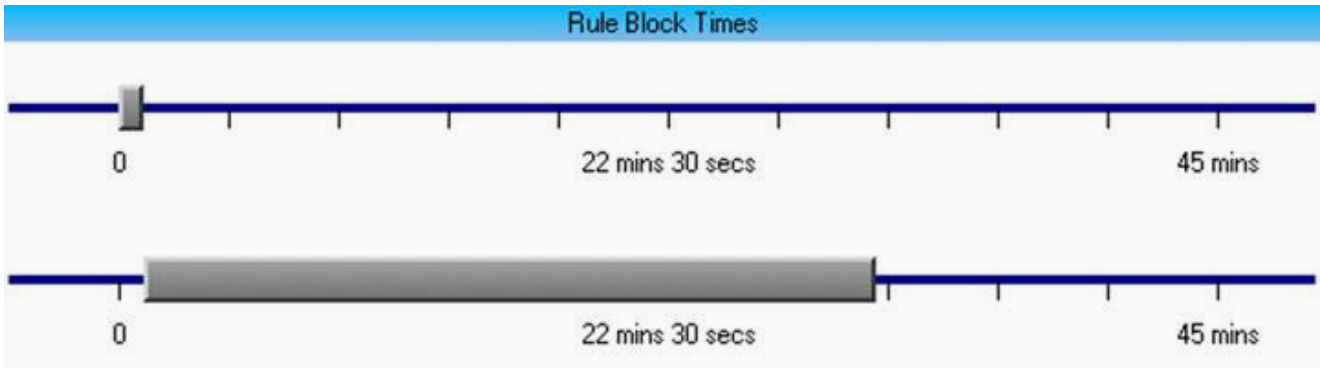
Rule 1, detecting the (too) long running regsvr32.exe:

Suspicious: regsvr32.exe continuously running

One of the most common tale tail of the presence of the "Inception Framework", a very sophisticated, layered malware.

Relationships	Rule Blocks	Rule Block Summaries
		<p>Log Observed</p> <p>Data Source: Log Manager Logs</p> <p>Primary Criteria:</p> <p>Common Event Is: Process/Service Started and Process Is: regsvr32.exe</p> <p>Group By:</p> <p>Process Process ID Origin Host</p>
<p>Related Fields:</p> <p>Process = Process Process ID = Process ID Origin Host = Origin Host</p> <p>Time Limit:</p> <p>This Rule Block must be satisfied within: 30 minutes</p> <p>Begin evaluating this Rule Block: 0 seconds after the prior Rule Block is satisfied</p>		
		<p>Log Not Observed Compound</p> <p>Data Source: Log Manager Logs</p> <p>Primary Criteria:</p> <p>Common Event Is:</p> <ul style="list-style-type: none"> Process/Service Stopped Process/Service Stopping <p>Group By:</p> <p>Process Process ID Origin Host</p>

Time line:



Settings:

AI Engine Rule Wizard

New Event Settings

Common Event Name

 Sync with rule name

Classification:

Risk Rating:

Event Suppression

Enable suppression

Suppression Multiple:

x Suppression Interval: 00:30:00
 = Suppression Period: 00:30:00

AIE Event Forwarding

Forward AIE Event to Event Manager

New Alarm Settings

Alarm on event occurrence.

Notification Settings

Number of decimal places to print for quantitative values:

Rule 2, detecting outbound traffic using WebDav protocol:

Suspicious: <u>WebDav</u> traffic to external site		
<p><i>One of the most common vector of C&C communication and data exfiltration from the "Inception Framework", a very sophisticated, layered malware.</i></p>		
Relationships	Rule Blocks	Rule Block Summaries
		<p>Log Observed</p> <p>Data Source: Log Manager Logs</p> <p>Primary Criteria:</p> <p>Application Is: <u>WebDav</u> and Direction Is: External or Outbound</p> <p>Group By:</p> <p>Origin Host</p>

Settings:

AI Engine Rule Wizard

New Event Settings

Common Event Name
AIE: Suspicious: WebDav traffic to external site

Sync with rule name

Classification: Security : Suspicious

Risk Rating: 7 - High-Low

Event Suppression

Enable suppression

Suppression Multiple: 3600

x Suppression Interval: 00:00:01

= Suppression Period: 01:00:00

AIE Event Forwarding

Forward AIE Event to Event Manager

New Alarm Settings

Alarm on event occurrence.



Notification Settings


Number of decimal places to print for quantitative values: 2

Rule 3, corroborate all the above and check precedence of inbound RTF or DOC email attachments:

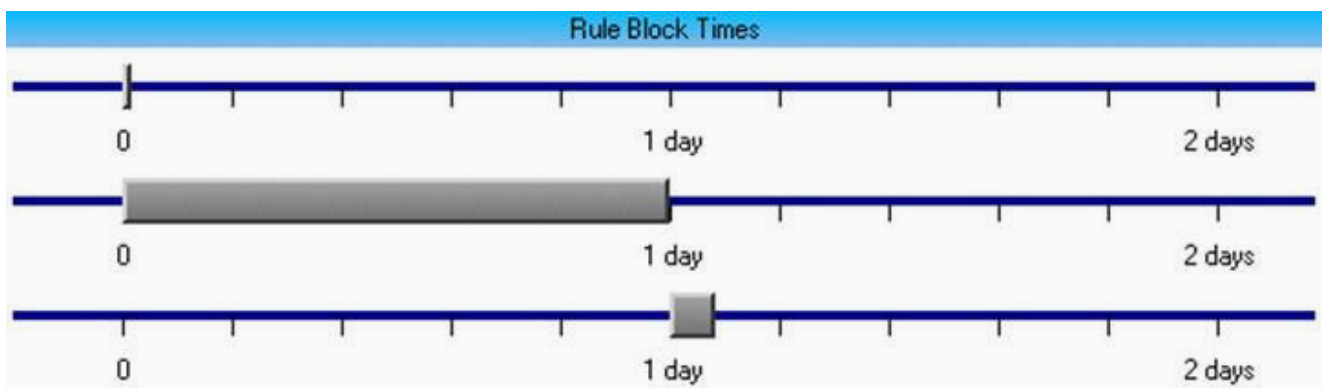
Compromised: Suspicious *Inception Framework* phishing attack

One member of staff has been victim of the "Inception Framework", a very sophisticated, layered malware.

Relationships	Rule Blocks	Rule Block Summaries
		<p>Log Observed</p> <p>Data Source: Log Manager Logs</p> <p>Primary Criteria:</p> <p>Log Source Type Is: Syslog - LogRhythm Network Monitor</p> <p>and Application Is: smtp</p> <p>and Direction Is: External</p> <p>and Object Name Is:</p> <ul style="list-style-type: none"> • \.doc\$ • \.rtf\$ <p>Group By:</p> <p>Object Name</p> <p>TCP/UDP Port (Origin)</p> <p>TCP/UDP Port (Impacted)</p> <p>IP Address (Origin)</p> <p>IP Address (Impacted)</p> <p>Session</p> <p>Recipient</p> <p>Sender</p>
<p>Related Fields:</p> <p>Sender = Sender</p> <p>Recipient = Recipient</p> <p>Time Limit:</p> <p>This Rule Block must be satisfied within:</p> <p>1 day</p> <p>Begin evaluating this Rule Block:</p> <p>0 seconds</p> <p>after the prior Rule Block is satisfied</p>	<p> </p>	
		<p>Log Observed</p> <p>Data Source: Log Manager Logs</p> <p>Primary Criteria:</p> <p>Common Event Is: Email Message Received</p> <p>and Origin Login Is Not: Nothing</p> <p>and Recipient Is Not: Nothing</p> <p>and Sender Is Not: Nothing</p> <p>Group By:</p>

		Sender Recipient Origin Login Origin Host
Related Fields: Origin Host = Origin Host Time Limit: This Rule Block must be satisfied within: 2 hours Begin evaluating this Rule Block: 0 seconds after the prior Rule Block is satisfied		
		Log Observed Data Source: Advanced Intelligence Engine Events Primary Criteria: Common Event Is: <ul style="list-style-type: none"> • AIE: Suspicious: regsvr32.exe continuously running • AIE: Suspicious: <u>WebDay</u> traffic to external site Group By: Origin Host

Time line:



Settings:

AI Engine Rule Wizard

New Event Settings

Common Event Name
AIE:

Sync with rule name

Classification:

Risk Rating:

Event Suppression

Enable suppression

Suppression Multiple:

x Suppression Interval: 02:00:00

= Suppression Period: 02:00:00

AIE Event Forwarding

Forward AIE Event to Event Manager

New Alarm Settings

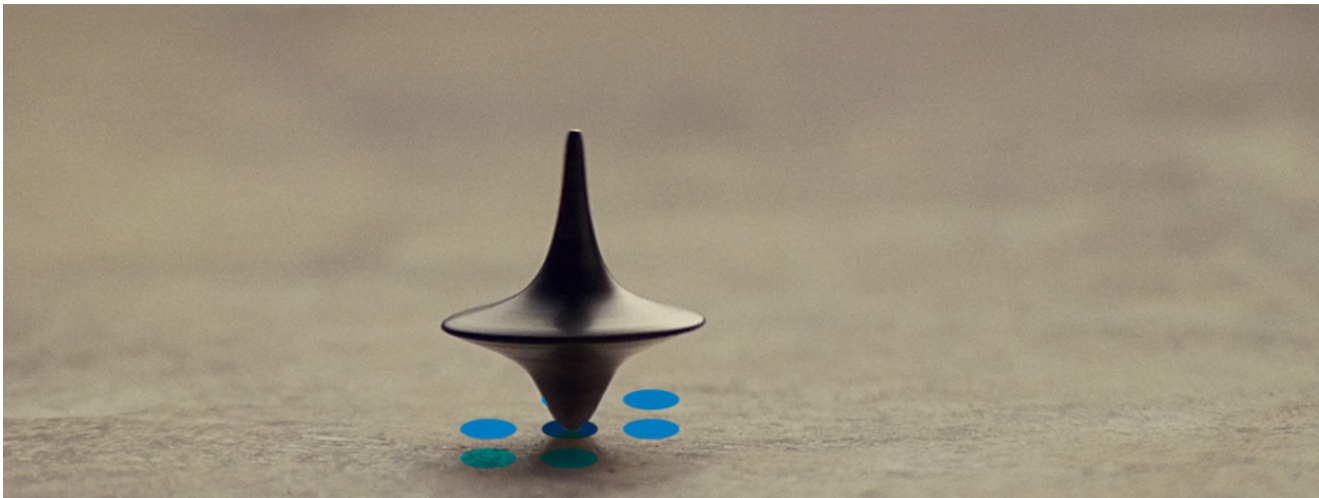
Alarm on event occurrence.

Notification Settings

Number of decimal places to print for quantitative values:

Equipped with these little helpers, you should now be able to relax for this festive season with the knowledge that any Inception style incursion into your workstations will be flagged.

Moreover, you'll be made aware of who in your organization is being targeted by the attack early enough before any critical data is siphoned out.



Sources: