

Incident Response for Targeted attacks

Jose Ramon Palanco

about:

Jose Ramon Palanco

From Spain

Security Researcher

+10 years experience

SOC: What does SOC stand for?

A security operations center (SOC) is a centralized unit that deals with security issues on an organizational and technical level. A SOC within a building or facility is a central location from where staff supervises the site, using data processing technology.

SOC



SOC Organization

- SOC Manager
- Intelligence Team Leader
- Operations Team Leader
- Tier 3 / Security Engineer
- Tier 2
- Tier 1

SOC Incident types

- Denial of Service
- Unauthorized access
- Vulnerability identification
- Hacker activity
- Data loss
- Malicious software activity

SOC Tools

- Endpoint Security (Antivirus/DLP/..)
- Network Security (IDS/IPS/Firewalls/..)
- Malware Sandbox
- SIEM
- Ticketing system

SOC Methodology

DataFlow: logs > events > alerts > incidents

WorkFlow: incident > ticket > analysis/scale

SIEM

- Security Information and Event Manager
- Sometimes SIM or SEM
- SIEM is not just Log Management

SIEM

- Relevant log collection
- Aggregation
- Normalization
- Retention Analysis (correlation & prioritization)
- Presentation (Reporting & Visualization)
- Workflow

SIEM: logs

```
Aug 18 20:22:31 server sshd[1891]: error:  
PAM: authentication error for root from  
localhost via 127.0.0.1
```

SIEM: logs

Date: Aug 18 20:22:31

Server: server

Service/Process: sshd[1891]:

Error: PAM

Authentication error for root from localhost

Details: via 127.0.0.1

SIEM: Event Correlation Rules

- Repetition Rules
- Combination Rules
- Missing Recurrence Rules

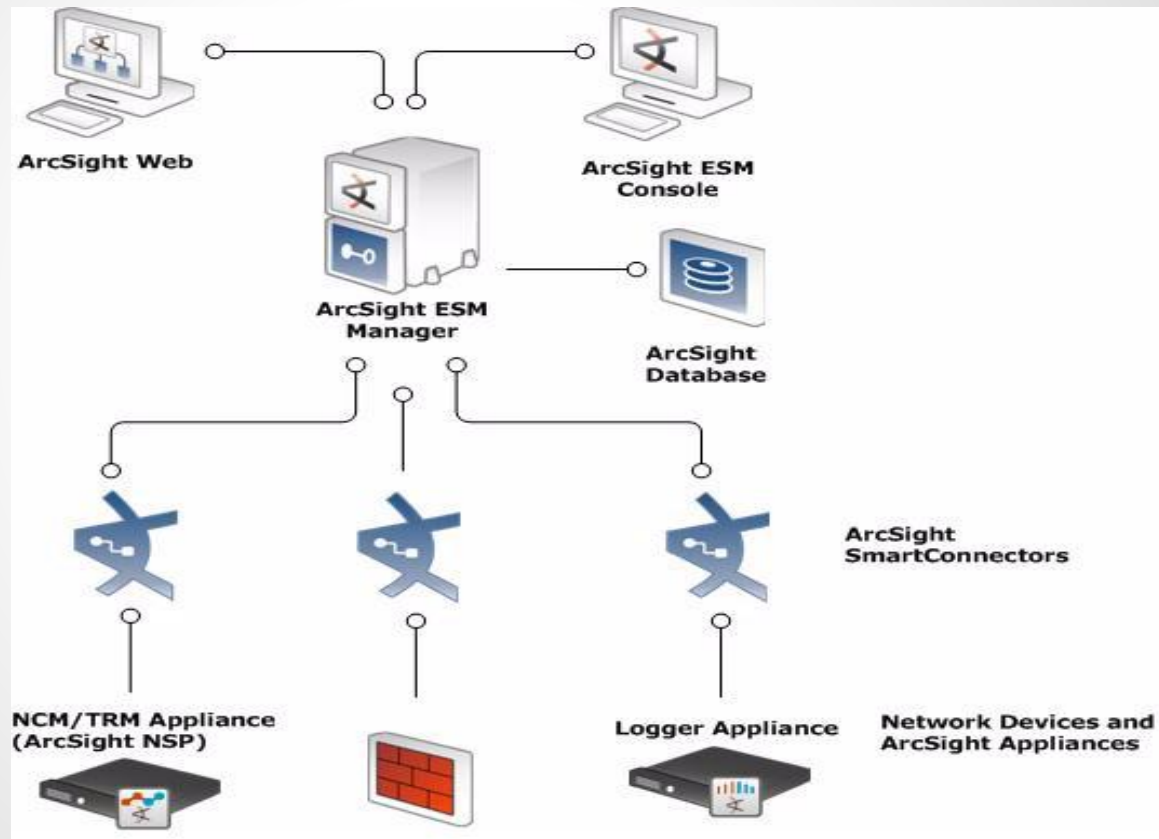
Arcsight

ArcSight Enterprise Security Manager (ESM)

ArcSight Express

ArcSight Logger

Arcsight



Arcsight: CEF

The Common Event Format (CEF) is an open log management standard.

It supports over 275 products across more than 35 solution categories.

Arcsight: CEF

```
CEF:0|Trend Micro Inc.|OSSEC HIDS|v2.5.1  
|5302|\ User missed the password to change  
UID to root.|9|dvc=ubuntusvr \ cs2=ubuntusvr-  
>/var/log/auth.log cs2Label=Location src=  
suser=root \ msg=May 11 21:16:05 ubuntusvr  
su[24120]: - /dev/pts/1 xavier:root
```

Arcsight: Smart Connectors

SmartConnectors provides source-optimized collection for leading security commercial products:

- Operating Systems, Apps, ..
- Antivirus, DLP, ..
- Firewalls, IPS, IDS, ..
- ...

Arcsight: Logger

- Collect logs
- Unify the data into CEF
- Search through millions of events
- Store years' worth of logs and events
- Automate analysis, alerting, reporting, intelligence of logs and events for IT security, IT operations, IT GRC and log analytics

Arcsight: Manager (ESM)

- A cost-effective solution for all your regulatory compliance needs
- Automated log collection and archiving
- Fraud detection
- Real-time threat detection
- Forensic analysis capabilities for cybersecurity

Arcsight ESM Console

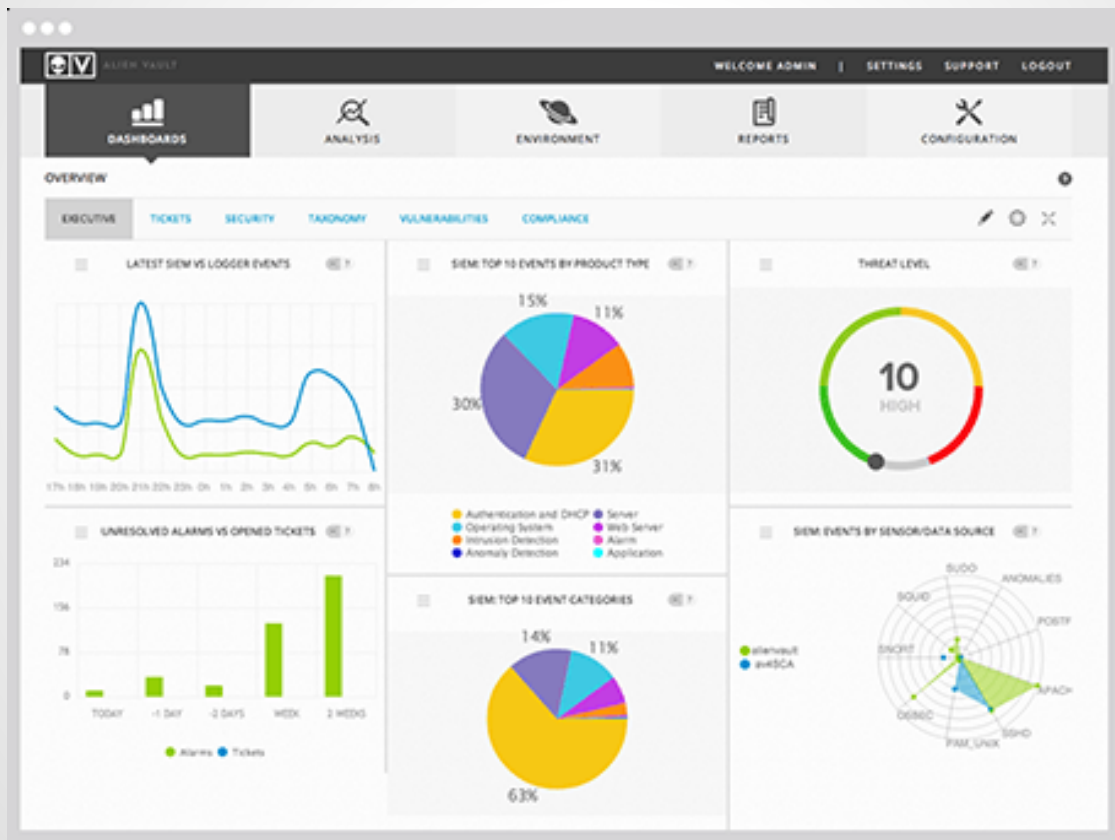
The screenshot displays the Arcsight ESM Console interface. The top menu bar includes File, Edit, View, Window, Tools, System, and Help. The main window is divided into several sections:

- Viewer:** Shows the active channel as 'Live'. It includes a timeline with 'Start Time: 15 Nov 2011 06:57:00' and 'End Time: 15 Nov 2011 08:57:59'. A filter is applied: '(MatchesFilter ("Not Correlated and Not Closed and Not Hidden") And MatchesFilter ("Non-ArcSight Internal Even...))'. The 'Total Events: 258' are displayed. A 'Radars' section shows a bar chart with green and orange bars.
- Table:** A table listing events with columns: Manager Receipt Time, Name, Attacker Address, Source User Name, Target Address, Target Port, Priority, and Device. The table shows multiple entries for 'Unauthorized Launch of a Monitored File' with various IP addresses and user names.
- Inspect/Edit:** A panel on the right showing event details. It includes a 'Description' section with 'Unauthorized Launch of a Monitored File'. Below this, there are tabs for 'Event', 'Details', 'Annotations', and 'Payload'. The 'Event' tab is selected, showing a table with 'Name' and 'Value' columns. The table lists various device information such as 'Final Device Time Zone', 'Final Device Time Zone...', 'Final Device Vendor', 'Final Device Product', 'Event Annotation', 'Event Annotation St...', 'Event Annotation St...', 'Event Annotation St...', 'Event Annotation M...', 'Event Annotation Au...', 'Event Annotation Ve...', 'Device Custom', 'Device Custom Num...', 'Device Custom Num...', and 'Device Custom Num...'. The values are displayed in the 'Value' column.

Alienvault OSSIM

- Open Source SIEM (GPL)
- Version 5.0 released on April 20, 2015
- Based on third party Open Source projects

Alienvault OSSIM



Alienvault OSSIM Components

- PRADS: passive identification of hosts
- OpenVAS: vulnerability scanner
- Snort/Suricata: IDS/IPS
- Tcptrack: session data information
- Nagios: monitoring
- OSSEC: HIDS
- FProbe, NFSen/NFDump: NetFlow Analysis

Reversing

Is the study of a malware by dissecting its different components and studying its behavior on the host computer's operating system.

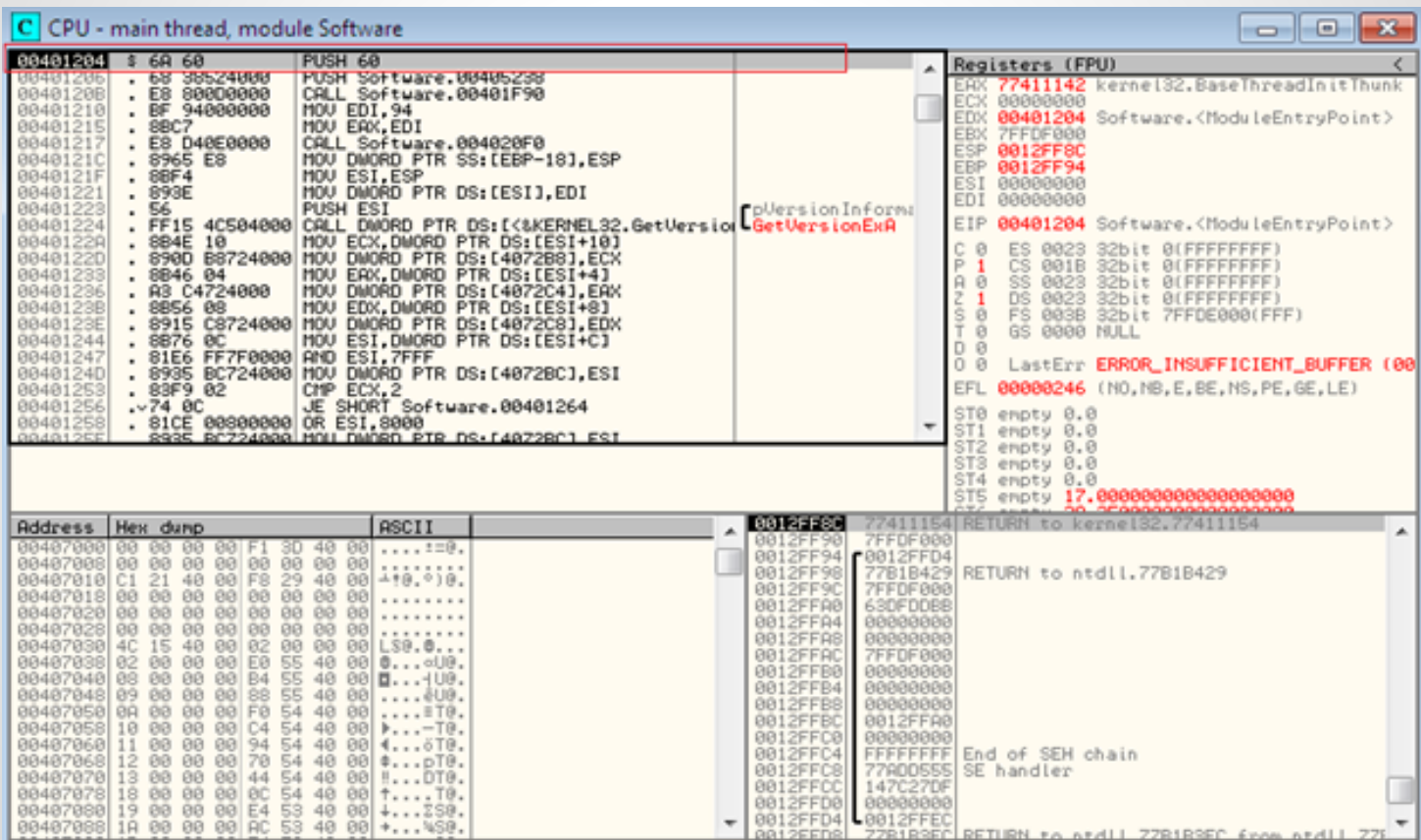
Reversing: Static Analysis

- Strings
- Yara rules
- IAT/imphash
- IDA Pro
- UPX, Bytehist, Density Scout, PackerID
- Signsrch, pescanner, ExeScan, pev, Peframe, pedump

Reversing: Dynamic Analysis

- OllyDBG
- WinDBG
- Cuckoo Sandbox

Reversing: OllyDBG



IoC

Indicator of compromise (IOC) are artifacts observed on a network or in an operating system that with high confidence indicates a computer intrusion (ip, hash, ip, host, ..)

Standards: openioc, stix, snort, yara

OpenIOC

Name:	SVCHOST.EXE	T..	R..	
Author:				
GUID:	658a4993-d53b-4a95-aeaa-93f0e020f			
Description:	Initial indicator of compromise for "svchost.exe" downloader			
Add:	Definition:			
Item	<div><div>OR</div><div>AND</div><div>Process Name contains svchost.exe</div><div>Process arguments contains not -k</div><div>AND</div><div>File Name contains svchost.exe</div><div>OR</div><div>File Full Path contains not system32</div><div>File Digital Signature Verified contains False</div></div>			
AND				
OR				

OpenIOC

Investigate:

<https://www.mandiant.com/resources/download/redline>

Client/Server:

<https://github.com/jeffbryner/pyioc>

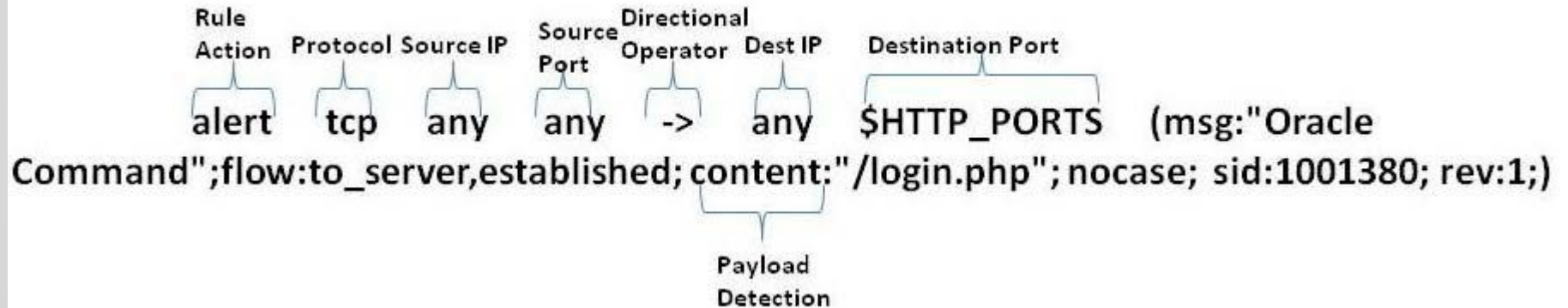
Web Editor:

<http://bluecloudws.github.io/ioceditor/>

Snort

- Snort is a free and open source IDS
- Considered the de facto standard
- Modes:
 - Sniffer
 - Packet logger
 - Network intrusion detection

Snort rule



The diagram illustrates a Snort rule with various components and their functions. Brackets are used to group parts of the rule and label them with their respective roles.

Rule	Action	Protocol	Source IP	Source Port	Directional Operator	Dest IP	Destination Port	Additional Options
	alert	tcp	any	any	->	any	\$HTTP_PORTS	(msg:"Oracle Command";flow:to_server,established;content:"/login.php";nocase; sid:1001380; rev:1;)

Annotations in the diagram:

- Payload Detection:** A bracket groups the `content:"/login.php"` and `nocase` options, with a label pointing to them.
- Destination Port:** A bracket groups the `$HTTP_PORTS` option, with a label pointing to it.

Suricata

Suricata is a snort compatible IDS.

Main features:

- Multi-threading
- Lua scripting
- GPU (Graphics card) acceleration
- HTTP log module
- Fast IP matching

Yara

“YARA is to files what Snort is to network traffic.”
-- Victor Manuel Alvarez, Yara Developer

Yara

With YARA you can create rules of malware families based on textual or binary patterns.

Each rule, consists of a set of strings and a boolean expression which determine its logic.

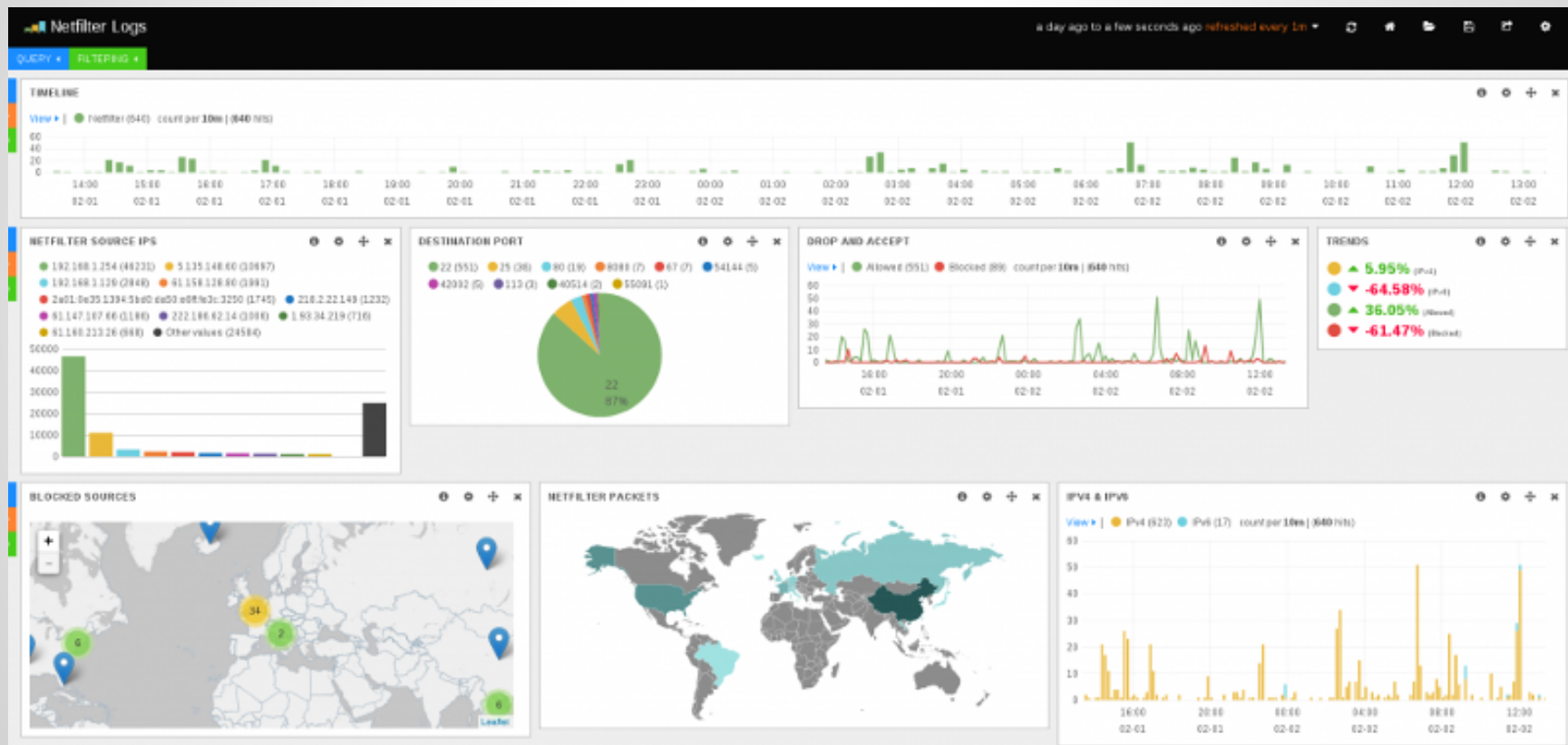
Yara rule

```
1 rule DarkRAT
2 {
3     meta:
4         date = "11/02/2015"
5         tags = "rat"
6     strings:
7         $a = "@1906dark1996coder@"
8         $b = "SHEmptyRecycleBinA"
9         $c = "mciSendStringA"
10        $d = "add_Shutdown"
11        $e = "get_SaveMySettingsOnExit"
12        $f = "get_SpecialDirectories"
13    condition:
14        all of them
15 }
```

ELK

- Elasticsearch for deep search and data analytics
- Logstash for centralized logging, log enrichment and parsing
- Kibana for powerful and beautiful data visualizations

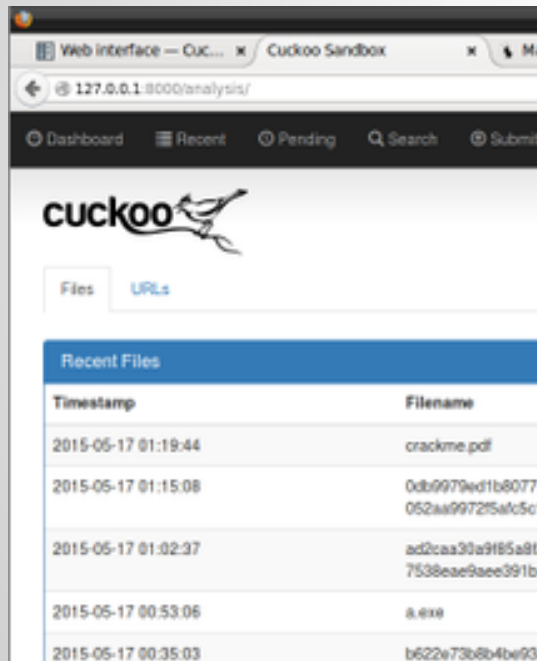
ELK



Cuckoo Sandbox

- Native functions and Windows API calls traces
- Copies/created/deleted files from the filesystem
- Dump of the memory of the selected process
- Full memory dump of the analysis machine
- Screenshots
- Network dump

Cuckoo sandbox



Signatures

The binary likely contains encrypted or compressed data.

Collects information to fingerprint the system (MachineGuid, DigitalProductId, SystemBiosDate)

Executed a process and injected code into it, probably while unpacking

Installs itself for autorun at Windows startup

Creates known Fynloski/DarkComet mutexes

El Jefe

EL JEFE is a Free situational awareness tool for securing organizations by making locating and responding to advanced threats by looking at what processes are started on your machine, and gathering that data for your entire Enterprise in a database.

El Jefe



Stations ▾ Binaries ▾ Events ▾ Intrusion ▾ Data ▾ Experimental ▾ Sandbox ▾ Docs

Welcome, **nico** [Log out](#)

Browse Events

« 1 2 3 4 5 6 7 8 9 10 »

Search Results :
226

Date	Parent Binary	Binary	Cmdline	Username	Station
April 10, 2014, 3:26 p.m.	C:\Windows\system32\svchost.exe	C:\Windows\System32\lsui.exe	C:\Windows\System32\	WIN-MEP0P1QJB13\X	WIN-MEP0P1QJB13
April 10, 2014, 3:03 p.m.	C:\Windows\system32\services.exe	C:\Windows\system32\taskhost.exe	taskhost.exe \$(Arg0)	NT AUTHORITY\LOCAL SERVICE	WIN-MEP0P1QJB13
April 10, 2014, 2:56 p.m.	C:\Windows\system32\svchost.exe	C:\Windows\System32\lsui.exe	C:\Windows\System32\	WIN-MEP0P1QJB13\X	WIN-MEP0P1QJB13
April 10, 2014, 2:55 p.m.	C:\Program Files\Citrix\SelfServicePlugin\SelfServicePlugin.exe	C:\Program Files\Citrix\SelfServicePlugin\SelfService.exe	"C:\Program Files\Ci	WIN-MEP0P1QJB13\X	WIN-MEP0P1QJB13
April 10, 2014, 2:48 p.m.	C:\Program Files\Google\Update\GoogleUpdate.exe	C:\Program Files\Google\Update\GoogleUpdate.exe	"C:\Program Files\Go	NT AUTHORITY\SYSTEM	WIN-MEP0P1QJB13
April 10, 2014, 2:48 p.m.	C:\Windows\system32\SearchIndexer.exe	C:\Windows\system32\SearchFilterHost.exe	"C:\Windows\system32	NT AUTHORITY\SYSTEM	WIN-MEP0P1QJB13

GRR

- GRR is an Incident Response Framework focused on Remote Live Forensics.
- The disk and file system analysis capabilities are provided by the sleuthkit and pytsk projects.
- The memory analysis and acquisition capabilities are provided by the rekall project.

GRR

GRR Admin Console

ec2-23-22-11-202.compute-1.amazonaws.com:8000/#c=C.4dbfb756101a0910&reason=&main=ManageHunts&tab=HuntOverviewRenderer&ft=FlowInformation&ftv=ShowFlowInformal

User: admin

Search

7

WIN-JTWK71ONUX4
Status: 1 minutes ago.
ip-10-204-62-88.ec2.internal
Host information
Start new flows
Browse Virtual Filesystem
Manage launched flows
Advanced
Client Performance
Stats
Crashes
Debug Client Requests
MANAGEMENT
Automated flows
Cron Job Viewer
Hunt Manager
Show Statistics
Start Global Flows
Advanced
CONFIGURATION
Manage Binaries
Settings

+

▶

⏏

⚙

Status	Hunt ID	Name	Start Time	Expires	Client Limit	Creator	Description
🕒	hunts/W:602FA2FD	GenericHunt	2013-11-18 07:39:08	2013-12-19 07:39:12	0	admin	Scan memory for bad string 1
⏏	hunts/W:E2890D	GenericHunt	2013-11-18 07:38:09	2013-11-18 07:38:09	0	admin	This is a hunt to start any flow on multiple clients.

View hunt details

NameGenericHunt
Hunt IDW:602FA2FD
Hunt URNaff4:/hunts/W:602FA2FD
Creatoradmin
Client Limit0
Client Count0
Outstanding0
Completed0
Total CPU seconds used0.00
Total network traffic0 bytes

Arguments

args	Flow args	Grep	Literal	testtesttest
	Flow runner args	Flow name	ScanMemory	
		Hunt name	GenericHunt	
		Description	Scan memory for bad string 1	
		Attribute regex	Windows	
		Attribute name	System	
	args	Username	admin	
		Reason		
		Token	Expiry	294247-01-10 04:00:54
		Source ips	::ffff:74.125.56.17	
		Process	GRRadminUI	
	backtrace	None		
	client_resources			
	create_time	2013-11-18 07:39:08		
	creator	admin		
	current_state	None		
	description	ScanMemory		
	expires	2013-12-19 07:39:12		
	network_bytes_sent	0		
	next_outbound_id	1		

Help

Report a problem

Virustotal

VirusTotal is a website, originally developed by Hispasec, that provides free checking of files for viruses. It uses up to 54 different antivirus products and scan engines to check for viruses that the user's own antivirus solution may have missed, or to verify against any false positives.

Dinoflux

- IoC in different formats
 - snort
 - suricata
 - arcsight
- Cyber Intelligence Database
 - hash
 - ip/host
 - history

APT

An advanced persistent threat (APT) is a set of stealthy and continuous computer hacking processes, often orchestrated by human(s) targeting a specific entity. APT usually targets organizations and/or nations for business or political motives.

HAVEX: A targeted attack

1. Received suspicious file
2. Executed inside cuckoo with SCADA tools
3. Report reveals OPC communications
4. Perform Dynamic/Static analysis
5. Report