## 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 Methodolody**

#### 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

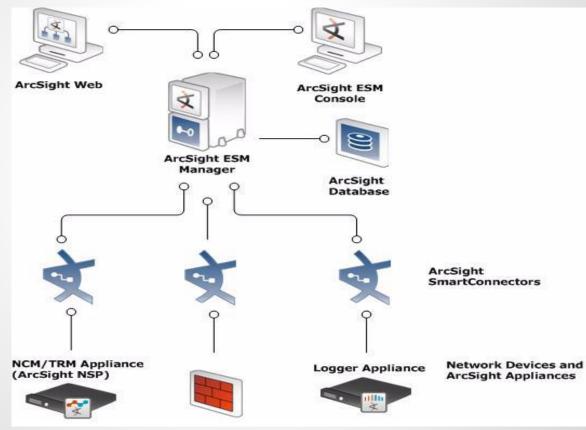
#### **SIEM: Event Correlation Rules**

- 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**

5	X A	ArcSight Console 4.5.1.58	91.0 [arcmgr:adm <mark>in.ast</mark> ] Trial license, iss	ued to ArcSight Der	no Key, expires De	c 31, 2011.						x
	File	e Edit View Window	Tools System Help									
xxxx   □ - ▷ 】   X = = × <     141 44 Ⅲ [ ] □ >> >>         □ □ >> >>     2 = ▷ =     2 = □												
e :	4	a - 🗁 🎽 🐰 🖻 🛙				ا المرا المرا المرا						9 🖬
	¥ie	ewer		45					e" ? ×	Inspect/Edit		d'? ×
Ī	N	Live								Event Inspector		
							311 Description					
						Events						
	Ene	d Time: 15 Nov 2011 08					High: 1	158		Grauthorized Launch of a Monitored File		
.	Filt	iter: (MatchesFilter)	("Not Correlated and Not Closed and Not Hid	Iden") And MatchesFill	ter ("Non-ArcSight Ir	iternal Even N	1edium:					
	Ini	line Filter: No Filter				Ve	Low: ry Low: 1		1			
						0.0	an Grandelle			<b>AV</b>		
	Ra	adar							_	Event Details Annotations Payload		
										E s	elect a Field Set	•
											Value	
F		(					1			Name	value	
	۶	Manager Receipt Time 1		Attacker Address 🖨		Target Address 🗢	Target P	A second second second	Devic 🥒	Final Device Time Zone	America/Chicago	-
			Unauthorized Launch of a Monitored File	192.168.1.2	gabe		00	8	and the second se	Final Device Time Zo	-21600000	
			Unauthorized Launch of a Monitored File Unauthorized Launch of a Monitored File	192.168.195.1	Grade December -		80		Invinc	Final Device Vendor	Invincea	
			Unauthorized Launch of a Monitored File		- CFL 247 3	127.0.0.1 127.0.0.1	1092 1096		Invinc		Invincea Browser Protection	
			Unauthorized Launch of a Monitored File	192.168.195.1	eric.hay	127.0.0.1	1098		Invinc	Event Annotation	anniecu bronsei frotection	_
			Unauthorized Launch of a Monitored File	10.9.8.140	eric.hay	127.0.0.1	1057				<resource id<="" p="" uri="/All Stages/Queued"></resource>	-100
	-		Unauthorized Launch of a Monitored File	10.9.8.140		81.203.210.140	80		Invinc			= K9P
			Unauthorized Launch of a Monitored File	Contraction of the second s	Colorado de Col	A second s	80	2			R9MHiNfoAABCASsxbPIxG0g==	
			Unauthorized Launch of a Monitored File	10.9.8.140	eric.hay	127.0.0.1	1129		Invinc	Event Annotation St	/All Stages/Queued	
			Unauthorized Launch of a Monitored File	10.9.8.140		127.0.0.1	1128		Invinc	Event Annotation St	Queued	
			Unauthorized Launch of a Monitored File			127.0.0.1	1132	2	and the second se	Event Annotation St	Queued	
			Unauthorized Launch of a Monitored File	10.9.8.140	eric.hay	127.0.0.1	1131	2		Event Annotation M	15 Nov 2011 08:47:12	
		15 Nov 2011 08:29:37	Unauthorized Launch of a Monitored File	10.9.8.140	eric.hav			8		Event Annotation Au	Constraint and a constraints	_
			Unauthorized Launch of a Monitored File	10.9.8.140	0.00000000000	95.76.139.33	80	and the second design of the s	Invinc			
			Unauthorized Launch of a Monitored File	10.9.8.140	Contraction of the second s	127.0.0.1	4296		Invinc	Event Annotation Ve	1	
		15 Nov 2011 08:29:37	Unauthorized Launch of a Monitored File	10.9.8.140	eric.hay	127.0.0.1	4297		Invinc _	Device Custom		
	4		······································		La C		122			Device Custom Num		===
	-	in the second se								Device Custom Num		2
		Grid								Device Custom Num	0	
									0	•		*
												-

#### **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: IDA Pro**

-A .text:373768E3				
.text:373768E3		Names window		1 Structures
	*	Name Addam P Strings window	es38gp" ox11 ds:GetLastError	0000 ; Ins/Del : create/delete structure
.text:373768E3 loc_373768E3:	; CODE XREF: sub_3737681C+B31j	C Start&ddress 37372DAB	all dsterLastError	0000 ; D/A/* : create structure member (
.text:373768E3 lea		F DIMain(v.v.) 97376324 - data:37 0000000C C Working Set	ар езж, 067h jnz short loc_37376887	0000 ; N : rename structure or struc
.text:373768E7 pusi		27277429 *** .data:37 0000000C C % User Time		8888 ; U : delete structure nember
.text:373768E8 pust				0000 ; [00000010 BYTES. COLLAPSED STRUCT
.text:373768E9 pust				0000 ; [00000094 BYTES. COLLAPSED STRUCT
.text:373768EE call	ll strlen	F stlen 37377444 - data 37 0000001 C Process		8888 ;
.text:373768F3 pop	ecx ecx	E memcpy 3737744A	true false	0000
.text:373768F4 pust		F streat 3/3/7450 = date 27_00000029_Ccobusted/usingereat/using	1100	8888 _PROCESS_INFORMATION struc ; (sizeof-
.text:373768F5 pust	sh offset aMineVersion1 0 ; 1pBuffer	0/074%		8888
.text:373768FA pus	th [esp+438b+b0bject] : bFile Recent scripts	L_CRT_INT(x,x,x) & WinGraph32 - Xrefs to CloseHandle	push ebx	8888 hProcess dd ?
.text:373768FE call		L start File View Zoom Move Help	push edi ; h0bject call ds:CloseHandle	0084 hThread dd ?
.text:37376984 pust		Finitem of a last scientist for a last scientist	nov ebx. do:GetHoduleFileNameA	0008 duProcessId dd ?
.text:37376908 call		F_inflerm RegDeleteKeyA		888C duThreadId dd ?
.text:3737690E lea			73,17% (-210,-304) 10 nodes, 33 edge segments, 0 crossings	8818 PROCESS INFORMATION ends
.text:37376912 pus		BegQueryWalueA ub.37875570	Hex View	
.text:37376913 pus				44 24 14 53-50 68 0C 91 37 37 E8 51 "rw HD\$¶SP!
.text:37376914 call		I RegEnumVakusA		50 68 8C 91-37 37 FF 74 24 28 FF 15 "5. YPh5C77
		I RegCloseKey		FF 74 24 10-FF 15 60 80 37 37 8D 44 "dA77 t\$b 8
.text:37376919 pop .text:37376910 lea				
		RegEnumKeyExA aub_37373623 aub_37377163 aub_373736893 aub_373774992 4 a		E8 63 E9 <mark>FF-</mark> FF 59 8D 44 24 24 59 50 "\$ VPucu
	ecx			37 37 53 55-6A 84 53 53 68 88 88 88 "§6677SUjT
.text:3737691F pusi		Line 17 of 352		88 F8 83 <mark>FF</mark> - <mark>FF</mark> 75 08 <u>56</u> <mark>FF</mark> 15 10 81 "@U +Л°Г с
.text:37376928 call		Fin Callers and Callees: sub. 37		EB 34 6A 02-53 53 57 <mark>FF</mark> 15 68 80 37 "773Lw4j%S
.text:37376926 push				14 53 BE E0-93 37 <mark>37</mark> 50 56 89 5C 24 "7HD\$¶S-p97
.text:37376927 pusi		Address Caler Disperiordia - 300 305/4/0F		88 88 59 58-56 57 FF 15 64 88 37 37 " ut
.text:37376928 pusi		text:373764F1 DIMain(xxx)		88 37 37 6A-81 58 5F 5E 5D 5B 81 C4 "W §`A77jħ>
.text:3737692A pusi				C3 81 EC 44-01 00 00 53 55 56 57 BF "TE+66DE.
.text:37376928 pusi				57 6А 08 <mark>FF</mark> -35 14 AD 37 37 <mark>FF</mark> 15 D4 ".ЂWjЂ 54
.text:37376920 pust			AC 37 37 88 F	F0 85 F6 0F-84 BD 00 00 00 BD 18 B5 "H77ЛЁЕЎ¤Д-
.text:37376931 pusl		83.33% (-267,-400) 35 nodes, 104 edge segments, 11 crossings		56 <mark>FF</mark> 15 30-81 37 37 56 E8 AD AE <mark>FF</mark> "77WUV §06
.text:37376932 call		Address and a second contract of the second se		8A 88 88 8B-1D 54 81 37 37 8B CF 2B " Uu)T
.text:37376934 nov		"".data:37 0000002F C net%20use%20\\\\%s\\ipc\$%20\'	Name Start End . C8 51 68 BC A	A3 37 37 56-FF D3 83 C4 20 8D 44 24 "LQh-r77V L
.text:37376936 cmp	edi, OFFFFFFFh			15 84 80 37-37 83 F8 FF 89 44 24 10 " PU \$00771
.text:37376939 inz	short loc 37376946	Line 196 of 318		88 FE 35 14-AD 37 37 FE 15 D8 AC 37 "ubVi. 54H7
.text:3737693B pusi		Address Lalied function		55 56 FF 15-30 81 37 37 56 E8 32 0A "7wdWUU 806
.text:3737693C call		.text:37376838 call d::GetTempFileNameA	Pilodia 31370104 37373000 00 00 00 00	2B C8 51 68-84 94 37 37 56 FF D3 56 "
.text:37376942		text37375849 call dcCopyFieA		80 88 CF 28-C8 80 44 24 60 51 50 56 "ubb
.text:37376942 loc 37376942:	: CODE XREF: sub 3737681C+C5†i			2C 56 FF 15-10 81 37 37 8D 44 24 14 " LF-,U STA
+ .text:37376942 xor			Fa FF 7h 2h 1	14 FF 15 88-80 37 37 85 C0 75 B4 56 "P t\$4 8447
.text:37376944 imp				AD 37 37 FE-15 D8 AC 37 37 FE 74 24 "P 54H77 8
.text:37376946 ;	, ,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,	Line 2222004F and do C of and the C of and the C of and the C of the Control of t		80 37 37 6A-01 58 5F 5E 5D 5B 81 C4 "T § A77jT
		text 37376806 call edi citeter en entere entranse.	18 11 15 70 8	30 ar ar on-or 30 ar 30 50 50 50 81 64 6 8 81 7 167
<b>T</b>		text 37375808 cal eti : DeleterFieA	•	
			37376930: sub 3737	2010-114

AU: idle Down Disk: 54GB 0000693C 3737693C: sub\_3737681C+120

#### **Reversing: Dynamic Analysis**

- OllyDBG
- WinDBG
- Cuckoo Sandbox

#### **Reversing: OllyDBG**

00401204	\$ 6A 60 PU	SH 60		Registers (FPU) <
00401206 00401208 00401215 00401215 00401217 00401217 00401217 00401217 00401221 00401223	. E8 9000000 CAL BF 94000000 M0 . 8BC7 M0 E8 D40E0000 CAL 8965 E8 M0 . 8BF4 M0 . 893E M0 . 56 PU	SH Software.00405238 L Software.00401590 J EDI,94 J ERX,EDI L Software.004020F0 J DMORD PTR SS:[EBP-18],ESP J ESI,ESP J ESI,ESP J DMORD PTR DS:[ESI],EDI SH ESI	Puersion Informa	EAX 77411142 kernel32.BaseThreadInitThunk ECX 00000000 EDX 00401204 Software. <moduleentrypoint> EBX 7FFDF000 ESP 0012FF9C EBP 0012FF94 ESI 00000000 EDI 00000000</moduleentrypoint>
00401224 00401220 00401220 00401233 00401238 00401238 00401238 00401234 00401244	. SB4E 10 MO	CALL DWORD PTR DS:[{&KERNEL32.GetUersic HOU ECX,DWORD PTR DS:[ESI+10] HOU DWORD PTR DS:[ESI+10] HOU DWORD PTR DS:[ESI+4] HOU EAX,DWORD PTR DS:[ESI+4] HOU DWORD PTR DS:[ESI+4] HOU DWORD PTR DS:[ESI+8] HOU DWORD PTR DS:[ESI+8] HOU DWORD PTR DS:[ESI+6] HOU ESI,DWORD PTR DS:[ESI+C] HOU ESI,DWORD PTR DS:[ESI+C]	rs Lot E Get Vers Lon ExA	EIP 00401204 Software. C 0 ES 0023 32bit 0(FFFFFFF) P 1 CS 001B 32bit 0(FFFFFFFF) A 0 SS 0023 32bit 0(FFFFFFFF) Z 1 DS 0023 32bit 0(FFFFFFFF) S 0 FS 0038 32bit 0(FFFFFFFF) T 0 GS 0000 NULL D 0
0040124D 00401253	000E 00724000 MOI	I DUDDD DTD DC. L4079DC1 ECT		0 0 LastErr ERROR_INSUFFICIENT_BUFFER (0 EFL 00000246 (NO,NB,E,BE,NS,PE,GE,LE)
00401256 00401258 00401258	.~74 8C JE . 81CE 00800000 0R 8935 8C724000 M0	ECX,2 ECX,2 SHORT Software.00401264 ESI,8000 DMNRD PTR DS-140728C1 ESI	-	ST0 empty 0.0 ST1 empty 0.0
				ST2 enpty 0.0 ST3 enpty 0.0 ST4 enpty 0.0 ST5 enpty 17.000000000000000000000000000000000000
Address	Нек dump 00 00 00 00 F1 3D 44	ASCII	0012FF90 7FFDF00	
00407008 00407018 00407018 00407028 00407028 00407038 00407038 00407038 00407038 00407058 00407058 00407058	00     00     00     00     00     00       C1     21     40     00     F8     29     40       00     00     00     00     00     00     00     00       00     00     00     00     00     00     00     00       00     00     00     00     00     00     00     00       00     00     00     00     00     00     00     00       00     00     00     00     00     00     00     00       00     00     00     00     00     00     00     00       02     00     00     00     00     00     00     00       02     00     00     00     00     00     00     00       02     00     00     00     00     00     00     00       02     00     00     00     00     00	3 00 3 00 4 0. 0 10 3 00 3 00 5 00 5 00 LS0.0 3 00 0 00 LS0.0 3 00 0 00 	0012FF9C 7FF0F00 0012FFA0 630FDDB 0012FFA0 000000 0012FFAC 7FF0F00 0012FFB0 000000 0012FFB0 000000 0012FFB0 000000 0012FFB0 000000 0012FFB0 0012FFB	9 RETURN to ntdll.77818429 10 10 10 10 10 10 10 10
00407060 00407068 00407070 00407078 00407078	11 00 00 00 94 54 40 12 00 00 00 00 70 54 40	3 00 4570. 3 00 4pT0. 3 00 4pT0. 3 00 4T0. 3 00 4T0.	0012FFC8 77ADD55 0012FFCC 147C27D 0012FFD0 0000000 0012FFD4 0012FFE	F End of SEH chain SS SE handler F 90

#### loC

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	Т	R						
Author:									
GUID:	658a4993-d53b-4a95-aeaa-93f0e0208								
Description:									
Initial indicator of compromise for "svchost.exe" downloader									
					÷				
Add:	Definition:								
ltem									
AND Process Name contains sychost.exe									
	AND Process Name contains sychost.exe OR Process arguments contains not -k OR - AND								
OR									
	File Name contains sychost.exe								
	File Full Path contain			-					
	File Digital Signature	e Ve	rifi	ed contains False.					

#### **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

#### **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.

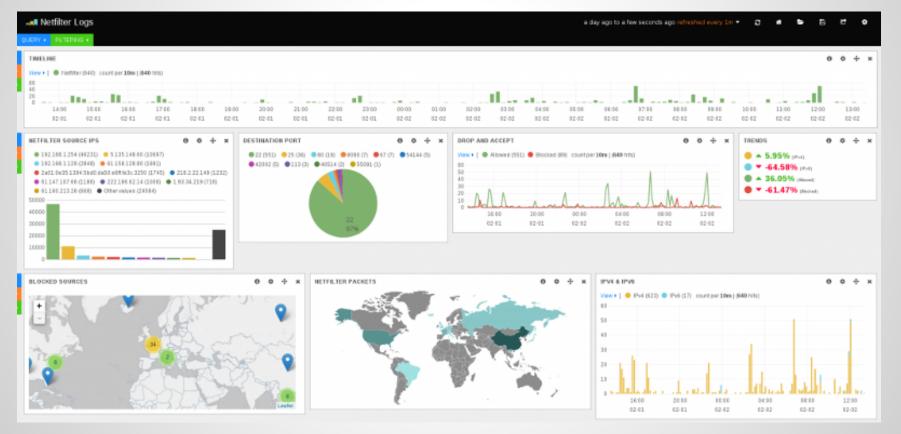
### Yara rule

1	rule DarkRAT
2	{
3	meta:
4	date = "11/02/2015"
5	tags = "rat"
6	strings:
7	\$a = "@1906dark1996coder@"
8	<pre>\$b = "SHEmptyRecycleBinA"</pre>
9	<pre>\$c = "mciSendStringA"</pre>
10	\$d = "add_Shutdown"
11	<pre>\$e = "get_SaveMySettingsOnExit"</pre>
12	<pre>\$f = "get_SpecialDirectories"</pre>
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.						
Web interface — Cuc × Cucko @ 127.0.0.1:0000/analysis/	o Sandbox x 🔥 Ma	Collects information to fingerprint the system (MachineGuid, DigitalProductId, SystemBiosDate)						
Dashboard 🖀 Recent 🛇 Penc	ding Q Search @ Submit	Executed a process and injected code into it, probably while unpacking						
cuckoo		Installs itself for autorun at Windows startup						
Files URLs		Creates known Fynloski/DarkComet mutexes						
Recent Files								
Timestamp	Filename		MDS	Status				
2015-05-17 01:19:44	crackme.pdf		9a8e90fb547d8fd3c865ed74782af600	reported	-			
2015-05-17 01:15:08	0db9979ed1b807712 052aa9972f5afc5c19	27e5530202d392797cb016 17coe732b.bin	e4c8813564858969aa37c5fb7a6ce363	reported				
2015-05-17 01:02:37	ad2caa30a9185a812 7538eae9aee391b11	0d3b945d812011b87ecf7 61aac7a6.bin	85e9061626704239ae5de766b953229f	reported				
2015-05-17 00:53:06	8.610		7c60feaa6ac08243e4c468a752753d74	reported				
2015-05-17 00:35:03	b622e73b8b4be93a	3c31e57ca9a357d8bae695	e85d64dd896a967de0771321d6222d19	reported	w			

### **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**

### ELJEFE

Stations -	Binaries - 📋 Events - 👖 Intrusion - 🌍 D	ta - 🗼 Experimental - 💥 Sandbox -	- Docs	Welcome, <b>nico</b>	Log ou
------------	---	-----------------------------------	--------	----------------------	--------

#### Browse Events

Username
Binary Name
Parent Name
Query

#### **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\slui.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\slui.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 Conso	ole	×										
← → C 🗋 ec2-23-22-11	1-202.co	ompute-1.amazon	aws.com:80	00/#c=C.4dbfb75	6101а0910&геа	son=&mai	in=Man	ageHunts&tab=Hu	ntOverviewRenderer&ft=FlowInforma	ation&ftv=ShowF	lowInforma	I\$ <b>Ξ</b>
GRR Response Rig	User: a	dmin								Search	7	۲
WIN-JTWK71ONUX4 Status:	+		٢									0
Ip-10-204-62- 88.ec2.internal	Status	Hunt ID	Name	Start Time	Expires	Client Limit	Creator	Description				
Host Information	۲	hunts/W:602FA2FD	GenericHunt	2013-11-18 07:39:08	2013-12-19 07:39:	12 0	admin	Scan memory for bac	d string 1			
Start new flows		hunts/W:E2890D	GenericHunt	2013-11-18 07:38:09	2013-11-18 07:38:	09 0	admin	This is a hunt to start	t any flow on multiple clients.			
Browse Virtual Filesystem Manage launched flows												
Advanced -												
Client Performance Stats												
Crashes												
Debug Client Requests												
MANAGEMENT	Viev	w hunt details										
Automated flows			_									
Cron Job Viewer		Name Hunt ID										
Hunt Manager Show Statistics		Hunt URN	aff4:/hunts	/W:602FA2FD								
Start Global Flows		Creator Client Limit			N							
Advanced -		Client Count			3							
CONFIGURATION		Outstanding Completed										
Manage Binaries		I CPU seconds used	0.00									
Settings		Total network traffic Arguments		<b>5</b> 1	-	-		1.161				- 1
		rugumente	args	Flow arg Flow run		v name		Literal ScanMemory	testtesttest			_
						it name		GenericHunt				
					Des	cription		Scan memory for bad	string 1 Windows			
					Reg	ex rules		Attribute regex Attribute name	System			
				args				Username	admin			
					Tok	en		Reason Expiry	294247-01-10 04:00:54			
								Source ips	::ffff:74.125.56.17			
				backtrac	e Non	<u>_</u>		Process	GRRAdminUI			
				client_re		e						
				create_ti creator	ime 201 adm	3-11-18 07:3	39:08					
				current_								
				descripti		nMemory 3-12-19 07:3	20.12					
				expires network	_bytes_sent 0	0-12-19 07.3	00.12					
				next out	bound 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