

GRRosso guaio a Chinatown

Pasquale Stirparo



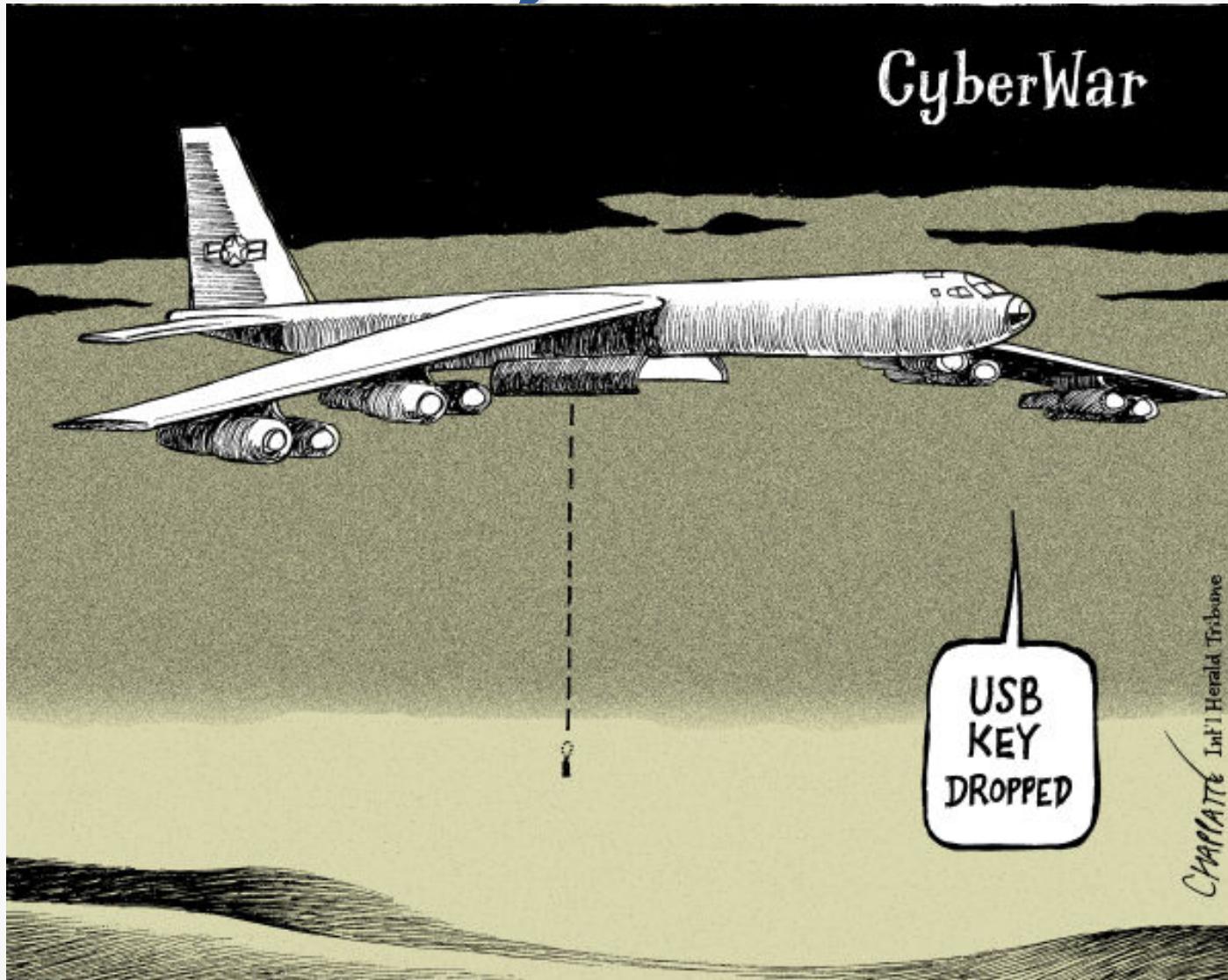
\$whoami

- Pasquale Stirparo
 - Ing. Informatico, Dottorando presso KTH – Royal Institute of Technology
- GCFA, GREM, OPST, OWSE, ECCE
- Mobile Security e Digital Forensics Engineer,
Fondatore @ SefirTech
- Socio Fondatore e Consigliere @ DFA
- Fellow @ Tech and Law Center

Di cosa non parliamo oggi



Cyber*



APT - Advanced Persistent Threat

- **Advanced**, fa riferimento all'elevato livello di sofisticazione nelle tecniche utilizzate per fare breccia nei sistemi
- **Persistent**, l'attaccante rimane presente all'interno del sistema per un periodo prolungato nel tempo, effettuando un continuo monitoraggio ed esfiltrazione di dati tramite C&C
- **Threat**, perché non si tratta di mero codice, ma l'avversario è un umano organizzato, motivato e con ingenti risorse
- APT ha come obiettivo organizzazioni e governi, per spionaggio industriale, per motivi politici e militari.

APT – Qualche numero*

- Attacchi di tipo APT “quasi sempre” riconducibili alla Cina, diversi dei quali direttamente al People's Liberation Army (PLA's) Unit 61398
- Oltre 20 diversi gruppi APT provengono dalla Cina
- Il solo gruppo APT1 è ritenuto responsabile di aver violato oltre 141 aziende dal 2006 ad oggi
- Il “furto” più imponente di proprietà intellettuale è pari a 6.5TB di dati compressi, rubati ad una sola azienda nell'arco di 10 mesi
- ... non solo Cina, Stuxnet è un classico esempio

* *“APT1: Exposing One of China's Cyber Espionage Units”*; Mandiant Intelligence Center Report, 2013.

APT – Anatomia di un attacco

- Compromissione iniziale
 - Spear-phishing email
- Stabilire l'accesso
 - backdoor
- Privilege Escalation
 - Mimikatz, lsass, fgdump, etc.
- Internal Reconnaissance
 - Raccolta di informazioni relative al sistema compromesso ed alla rete
- Lateral Movement
 - pass-the-hash, etc.
- Mantenimento dell'accesso
 - Aggiornamento delle backdoor
- Esfiltrazione delle informazioni

Non solo l'attacco

- Anche alle conferenze, si parla più spesso della fase di “hacking”
- Le aziende non sono da meno... “Prima dimostrami che posso essere bucato, poi parliamo di forensics”
- E’ giusto e necessario fare verifiche di sicurezza, aiutano a scovare (e chiudere) quantomeno le falle evidenti...

... tipo password di accesso deboli



Incidenti Informatici e Forensics Readiness

- Se qualcuno attacca... dall'altra parte c'è chi è attaccato e/o difende
- Incidente Informatico
 - Nel campo della sicurezza, un incidente informatico è definito come qualsiasi azione *illegal*, non autorizzata, o *inaccettabile* che coinvolge un computer o una rete di computer.
- Forensics Readiness
 - Le procedure che un'organizzazione può prendere in anticipo di un'intrusione, al fine di accelerare il processo di risposta agli incidenti.



Attacco → **Incident Response** → Digital Forensics

Essere pronti

Non si tratta più di “se sarò attaccato o meno”, ma di quando.



Quindi che fare?

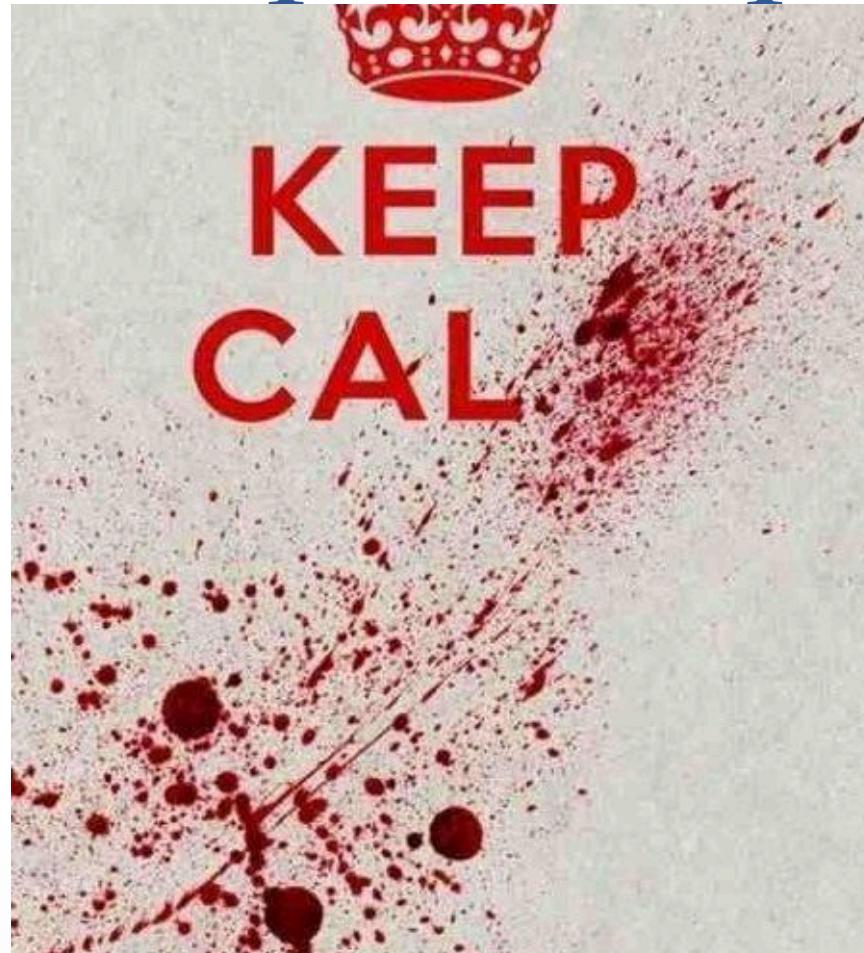
Diventa fondamentale essere attrezzati per effettuare la fase di triage

- Forensics vs Triaging
 - **L'analisi forense** mira a stabilire conclusioni inconfutabili, a provare con metodo scientifico che un evento si è verificato o meno
 - **La fase di triaging** cerca semplicemente di stabilire se il sistema rischia di essere coinvolto con il caso o meno.
- Importante perché le mole di dati da acquisire/analizzare aumentano esponenzialmente
 - Dimensioni dei dischi
 - Numero di client in ambiente enterprise

Decidere dove intervenire

- Analogia con il campo medico, per definire un sistema di priorità d'intervento al pronto soccorso
- In campo forense possiamo avere 3 categorie
 1. Il sistema con molta probabilità contiene evidenze importanti, ma è improbabile che queste vadano distrutte/perse nel breve periodo
 2. Il sistema con molta probabilità contiene evidenze importanti, con un rischio elevato che queste vadano perse/distrutte nel breve periodo
 3. Il sistema con molta probabilità non contiene evidenze rilevanti
- Tenere in considerazione l'ordine di volatilità (OOV)
 - RAM image, connessioni di rete, utenti loggati, processi attivi, etc.

GRR Rapid Response



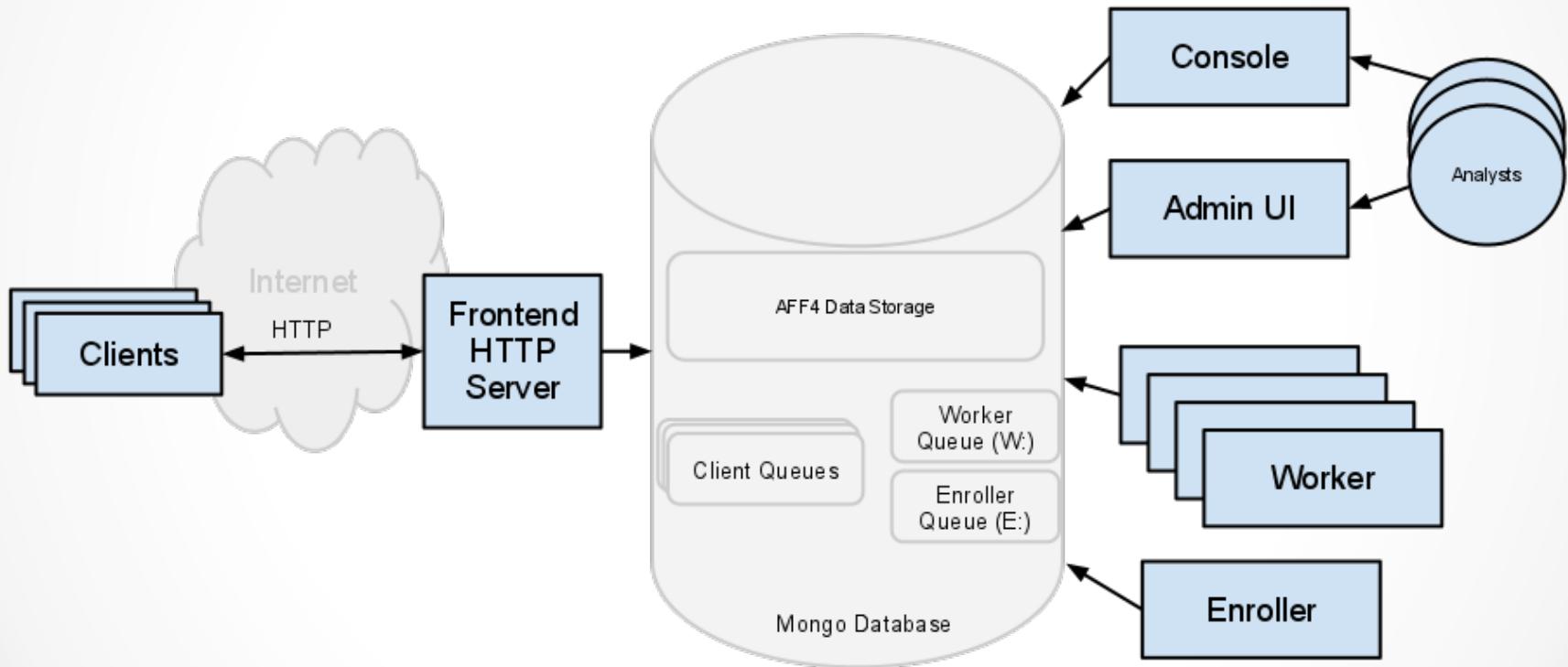
Perché GRR?

- Dimmi se questa macchina è compromessa
 - mentre ci sei, controlla anche le altre 1000
- Mattia ha notato qualcosa di strano, controllare la sua macchina
 - NB: Mattia è in vacanza in Costa Rica e ha una connessione 3G
- Come mai c'è del traffico IRC nella nostra rete?

GRR - Caratteristiche

- Scritto in **Python**, compilato exe/elf/mach-o
- Sistema **agent-based**
- Comunicazioni attraverso rete Internet via HTTP
- Comunicazioni client-server sono cifrate
- MongoDB NoSQL backend
- Ajax UI
- Elevata **scalabilità**
- **Open Source** (Apache/GPL Dual Licensed)
- Integrato con **Volatility**
- ... **Plaso** coming soon

GRR - Architettura



GRR - Attività

- Flow
 - Flows sono entità server-side che invocano azioni da parte dei client.
 - Queste “chiamate” sono effettuate in maniera asincrona.
- Hunt
 - Gestione e monitoraggio do flow su larga scala.
 - Il principio è che tutto ciò che può essere fatto su un singolo client, deve poter essere fatto su centinaia di client con la stessa facilità e tempistica.

GRR – Flow view

GRR Admin Console - Mozilla Firefox

GRR Admin Console

localhost:8000/#aff4_path=aff4%3A%2FC.f65c9e9b5f60276c%2Fanalysis%2FArtifactCollectorFlow%2Fpaco-1398875760.82&c=C.f65c9e9b5f60276c

User: paco

Search

0

GRR Response Rig

User: paco

paco-62cf251042
Status: 18 seconds ago.
Internal IP address.

Host Information
Start new flows
Browse Virtual Filesystem
Manage launched flows
Advanced ▾
MANAGEMENT
Cron Job Viewer
Hunt Manager
Show Statistics
Start Global Flows
Advanced ▾
CONFIGURATION
Manage Binaries
Settings

State Path Flow Name Creation Time Last Active Creator

State	Path	Flow Name	Creation Time	Last Active	Creator
✓	W:E540307C	ListDirectory	2014-04-30 16:41:17	2014-04-30 16:41:32	paco
✓	W:30D5F9DD	UpdateVFSFile	2014-04-30 16:41:17	2014-04-30 16:41:17	paco
✓	W:1D097FF3	ArtifactCollectorFlow	2014-04-30 16:36:00	2014-04-30 16:39:31	paco
✓	W:A8D79B2F	ArtifactCollectorFlow	2014-04-30 14:44:08	2014-04-30 14:44:32	paco
✓	W:8593B1E1	ArtifactCollectorFlow	2014-04-30 14:39:18	2014-04-30 16:32:53	paco
✓	W:33B89F79	AnalyzeClientMemory	2014-04-30 08:10:51	2014-04-30 08:36:05	paco
✓	W:EEDB221A	Interrogate	2014-04-30 08:03:55	2014-04-30 08:03:59	GRRWorker
✓	CA:4D3164CE	CAEnroler	2014-04-30 08:03:54	2014-04-30 08:03:55	GRREnroler

Flow Information Requests

aff4:/C.f65c9e9b5f60276c/flows/W:8593B1E1 @

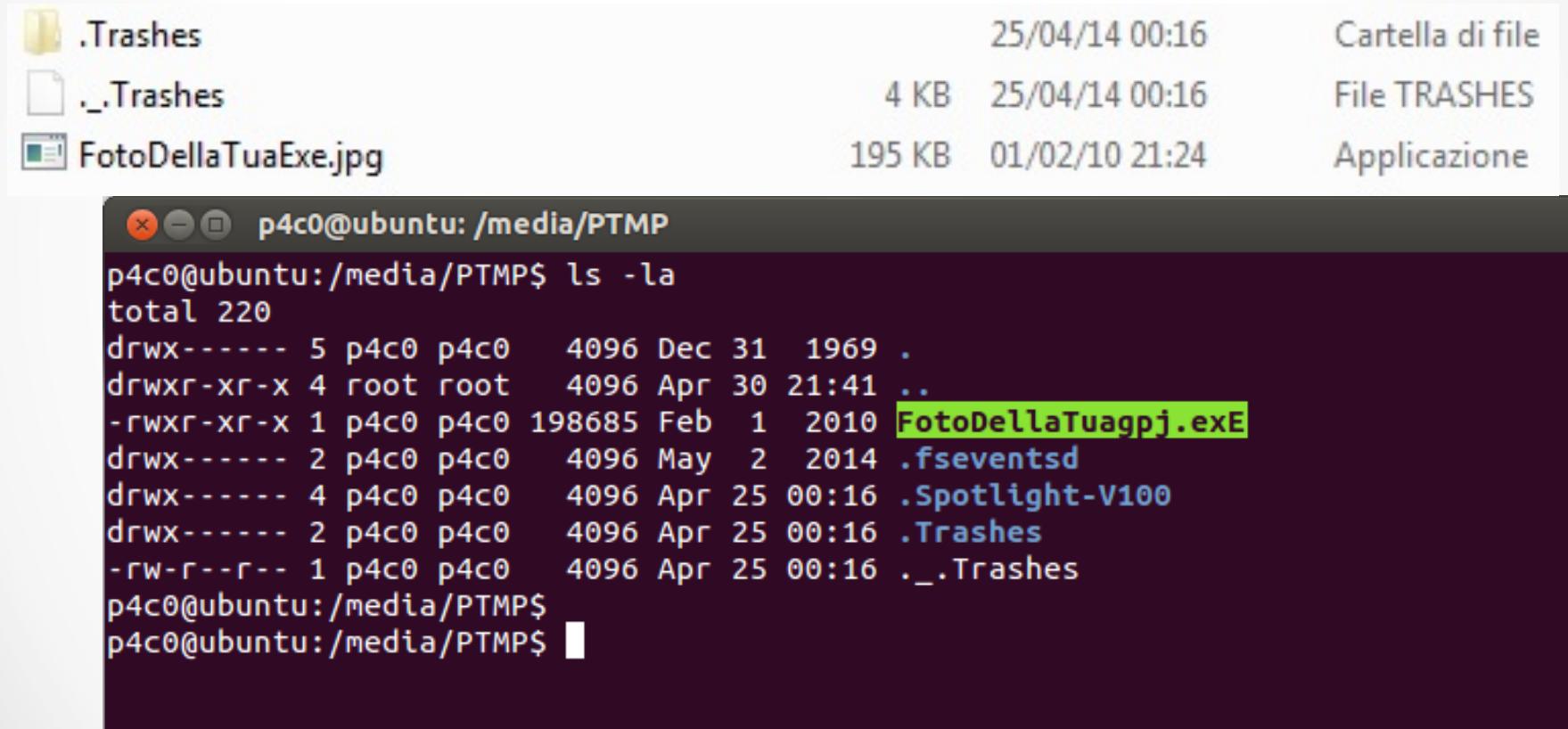
Attribute	Value	Age
ArtifactCollectorFlow	WinDirEnvironmentVariable WindowsPersistenceMechanisms WindowsRegistryProfiles WinCodePage WinPathEnvironmentVariable	

Help Report a problem

GRR – Demo time

- Riceviamo una email, con allegata un'immagine, dall'indirizzo ilTuoMiglioreAmico@gmail.com, non abbiamo motivo di non fidarci
- Doppio click, ma non si apre nessuna immagine e dopo qualche secondo il file sparisce
- Iniziamo a sospettare qualcosa, avvisiamo il sistemista in azienda che nota del traffico IRC anomalo verso irc.mcs.net
- Veniamo contattati dal sistemista per controllare la macchina

Punti di vista... RTLO



The screenshot shows a Linux desktop environment with a terminal window and a file browser window.

File Browser (Nautilus) Content:

	.Trashes			25/04/14 00:16	Cartella di file
	._Trashes	4 KB	25/04/14 00:16		File TRASHES
	FotoDellaTuaExe.jpg	195 KB	01/02/10 21:24		Applicazione

Terminal Window (p4c0@ubuntu:/media/PTMP\$)

```
p4c0@ubuntu:/media/PTMP$ ls -la
total 220
drwx----- 5 p4c0 p4c0 4096 Dec 31 1969 .
drwxr-xr-x 4 root root 4096 Apr 30 21:41 ..
-rwxr-xr-x 1 p4c0 p4c0 198685 Feb 1 2010 FotoDellaTuagpj.exe
drwx----- 2 p4c0 p4c0 4096 May 2 2014 .fsevents.d
drwx----- 4 p4c0 p4c0 4096 Apr 25 00:16 .Spotlight-V100
drwx----- 2 p4c0 p4c0 4096 Apr 25 00:16 .Trashes
-rw-r--r-- 1 p4c0 p4c0 4096 Apr 25 00:16 ._Trashes
p4c0@ubuntu:/media/PTMP$
```

GRR – Filesystem view

GRR Admin Console - Mozilla Firefox

GRR Admin Console

localhost:8000/#aff4_path=aff4%3A%2FC.f65c9e9b5f60276c%2Fanalysis%2FAnalyzeClientMemory%2Fpaco-1398921303.66&c=C.f65c9e9b5f60276c

User: paco

GRR Response Rig

User: paco

Icon Name type size stat.st_size stat.st_mtime stat.st_ctime Age

Icon	Name	type	size	stat.st_size	stat.st_mtime	stat.st_ctime	Age
📁	CaptureBAT	VFSDirectory	0	0	2013-10-08 10:08:51	2013-10-08 10:08:49	2014-05-01 04:59:47
📄	IDA Pro Free.lnk	VFSFile	0	606	2013-10-08 10:14:30	2013-10-08 10:14:30	2014-05-01 04:59:47
📁	PeStudio824	VFSDirectory	0	0	2014-04-26 18:17:13	2014-04-26 18:14:15	2014-05-01 04:59:47
📄	Process Hacker 2.lnk	VFSFile	0	1711	2013-10-08 10:06:48	2013-10-08 10:06:48	2014-05-01 04:59:47
📄	Shortcut to CHimpREC.lnk	VFSFile	0	682	2013-10-08 10:21:56	2013-10-08 10:21:56	2014-05-01 04:59:47
📄	Shortcut to LordPE.lnk	VFSFile	0	654	2013-10-08 10:16:54	2013-10-08 10:16:54	2014-05-01 04:59:47
📄	Shortcut to OLLYDBG.lnk	VFSFile	0	666	2013-10-08 10:15:36	2013-10-08 10:15:36	2014-05-01 04:59:47
📄	Shortcut to PEID.lnk	VFSFile	0	626	2013-10-08 10:18:34	2013-10-08 10:18:34	2014-05-01 04:59:47

Browse Virtual Filesystem

Manage launched flows

Advanced ▾

MANAGEMENT

Cron Job Viewer

Hunt Manager

Show Statistics

Start Global Flows

Advanced ▾

CONFIGURATION

Manage Binaries

Settings

Icon Name type size stat.st_size stat.st_mtime stat.st_ctime Age

Stats Download TextView HexView

aff4:/C.f65c9e9b5f60276c/analysis/AnalyzeClientMemory/paco-1398921303.66 @ 2014-05-01 05:17:31

Help Report a problem

join

Highlight All Match Case

Join

Highlight All Match Case

WinXP infetto



Analisi del Registro

The screenshot shows the GRR Admin Console interface in Mozilla Firefox. The left sidebar contains various monitoring and management tools like Host Information, Start new flows, and Management. The main area displays a tree view of collectors and artifacts. A search bar at the top right filters results by the user 'paco'. On the right, a detailed configuration panel for the 'WindowsRunKeys' collector is shown, along with artifact collectors and processors.

WindowsRunKeys
Collect windows run keys.

Labels	Software
Platforms	Windows
Conditions	None
Dependencies	users.sid
Links	
Output Type	StatEntry

Artifact Collectors

Action	GetRegistryKeys HKEY_USERS\%users.sid%\Software \Microsoft\Windows\CurrentVersion \Run*, HKEY_USERS\%users.sid%\Software \Microsoft\Windows\CurrentVersion\RunOnce \Run*, HKEY_LOCAL_MACHINE\Software\Microsoft \Windows\CurrentVersion \Run*, HKEY_LOCAL_MACHINE\Software \Microsoft\Windows\CurrentVersion\RunOnce*
arg:path_list	

Artifact Processors

Persistenza del trojan

GRR Admin Console - Mozilla Firefox

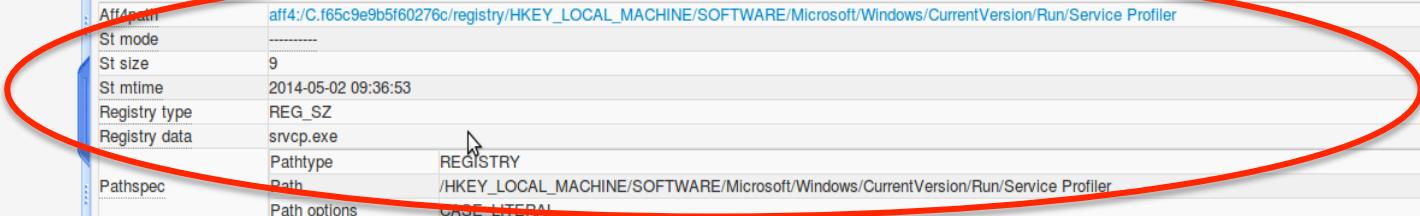
localhost:8000/#aff4_path=aff4%3A%2FC.f65c9e9b5f60276c%2Fanalysis%2FArtifactCollectorFlow%2Fpaco-1398917147.89&c=C.f65c9e9b5f60276c

User: paco

Path options CASE_LITERAL

Aff4path	aff4:/C.f65c9e9b5f60276c/registry/HKEY_LOCAL_MACHINE/SOFTWARE/Microsoft/Windows/CurrentVersion/Run/BluetoothAuthenticationAgent
St mode	-----
St size	55
St mtime	2014-05-02 09:36:53
Registry type	REG_SZ
Registry data	rundll32.exe bthprops.cpl,,BluetoothAuthenticationAgent
Pathspec	Pathtype REGISTRY Path /HKEY_LOCAL_MACHINE/SOFTWARE/Microsoft/Windows/CurrentVersion/Run/BluetoothAuthenticationAgent Path options CASE_LITERAL
Aff4path	aff4:/C.f65c9e9b5f60276c/registry/HKEY_LOCAL_MACHINE/SOFTWARE/Microsoft/Windows/CurrentVersion/Run/Service Profiler
St mode	-----
St size	9
St mtime	2014-05-02 09:36:53
Registry type	REG_SZ
Registry data	srvcpc.exe
Pathspec	Pathtype REGISTRY Path /HKEY_LOCAL_MACHINE/SOFTWARE/Microsoft/Windows/CurrentVersion/Run/Service Profiler Path options CASE_LITERAL
Aff4path	aff4:/C.f65c9e9b5f60276c/registry/HKEY_USERS/S-1-5-21-57989841-1085031214-1606980848-1003/Software/Microsoft/Windows/CurrentVersion/Run/ctfmon.exe
St mode	-----
St size	30
St mtime	2013-10-04 14:37:09
Registry type	REG_SZ
Registry data	C:\WINDOWS\system32\ctfmon.exe
Pathspec	Pathtype REGISTRY Path /HKEY_USERS/S-1-5-21-57989841-1085031214-1606980848-1003/Software/Microsoft/Windows/CurrentVersion/Run/ctfmon.exe Path options CASE_LITERAL

Help Report a problem



Alla ricerca della stringa perduta

The screenshot shows the GRR Admin Console interface in Mozilla Firefox. The title bar reads "GRR Admin Console - Mozilla Firefox". The address bar shows the URL "localhost:8000/#aff4_path=aff4%3A%2FC.f65c9e9b5f60276c%2Fanalysis%2FArtifactCollectorFlow%2Fpaco-1398917147.89&c=C.f65c9e9b5f60276c". The user is "paco".

The left sidebar contains various icons and links:

- Host Information: "paco-62cf251042" (Status: 22 seconds ago), Internal IP address.
- Start new flows: "Browse Virtual Filesystem", "Manage launched flows", "Advanced".
- MANAGEMENT: "Cron Job Viewer", "Hunt Manager", "Show Statistics", "Start Global Flows", "Advanced".
- CONFIGURATION: "Manage Binaries", "Settings".

The main panel shows a tree view of flow types under "Memory":

- Administrative
- Browser
- Collectors
- FileTypes
- Filesystem
- Memory
 - AnalyzeClientMemory
 - DownloadMemoryImage
 - ImageMemoryToSocket
 - LoadMemoryDriver
 - ScanMemory** (selected)
 - UnloadMemoryDriver
- Misc
- Network
- Processes
- Registry
- Services
- Timeline

On the right, there are search fields and filters:

- Grep: "paco"
- Start offset: "10737418240"
- Length: "10737418240"
- Regex: "JOIN|NICK|PASS" (highlighted)
- Literal: ""
- Mode: "ALL_HITS (default)"

Below the search fields, there is an "Advanced" button and a checkbox for "Also download".

The bottom section displays the details for the selected "ScanMemory" flow:

ScanMemory

Grep client memory for a signature.

This flow grops memory on the client for a pattern or a regex.

Returns to parent flow:
RDFValueArray of BufferReference objects.

Call Spec:
flow.GRRFlow.StartFlow(client_id=client_id, flow_name="ScanMemory", grep=grep, also_download=also_download)

Args:
grep

At the bottom right, there are "Help" and "Report a problem" links.

Comandi IRC in memoria

GRR Admin Console - Mozilla Firefox

GRR Admin Console

localhost:8000/#aff4_path=aff4%3A%2FC.f65c9e9b5f60276c%2Fanalysis%2FScanMemory%2Fpaco-1398917627.3

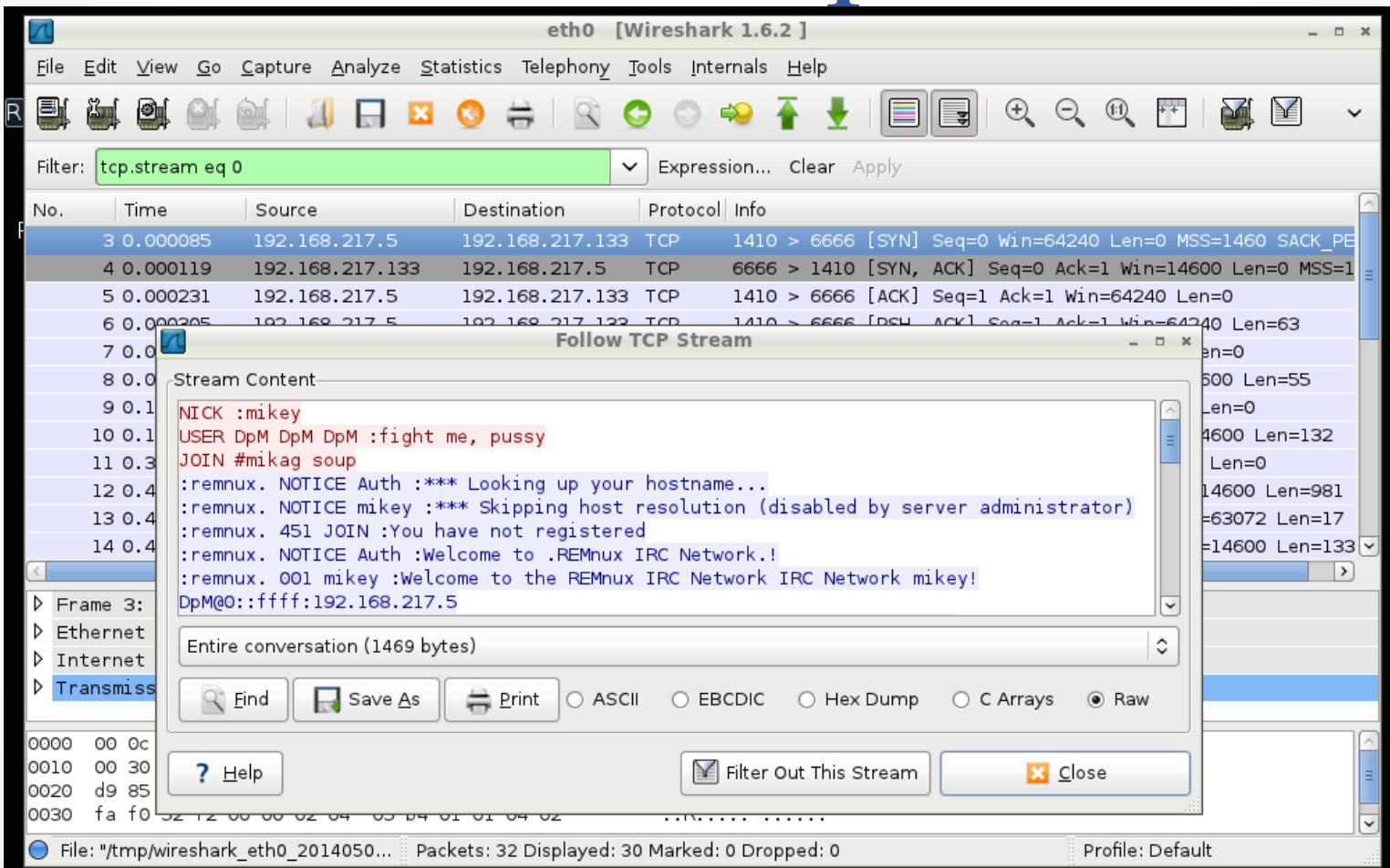
GRR Response Rig User: paco

paco-62cf251042 Status: 1 seconds ago. Internal IP address.

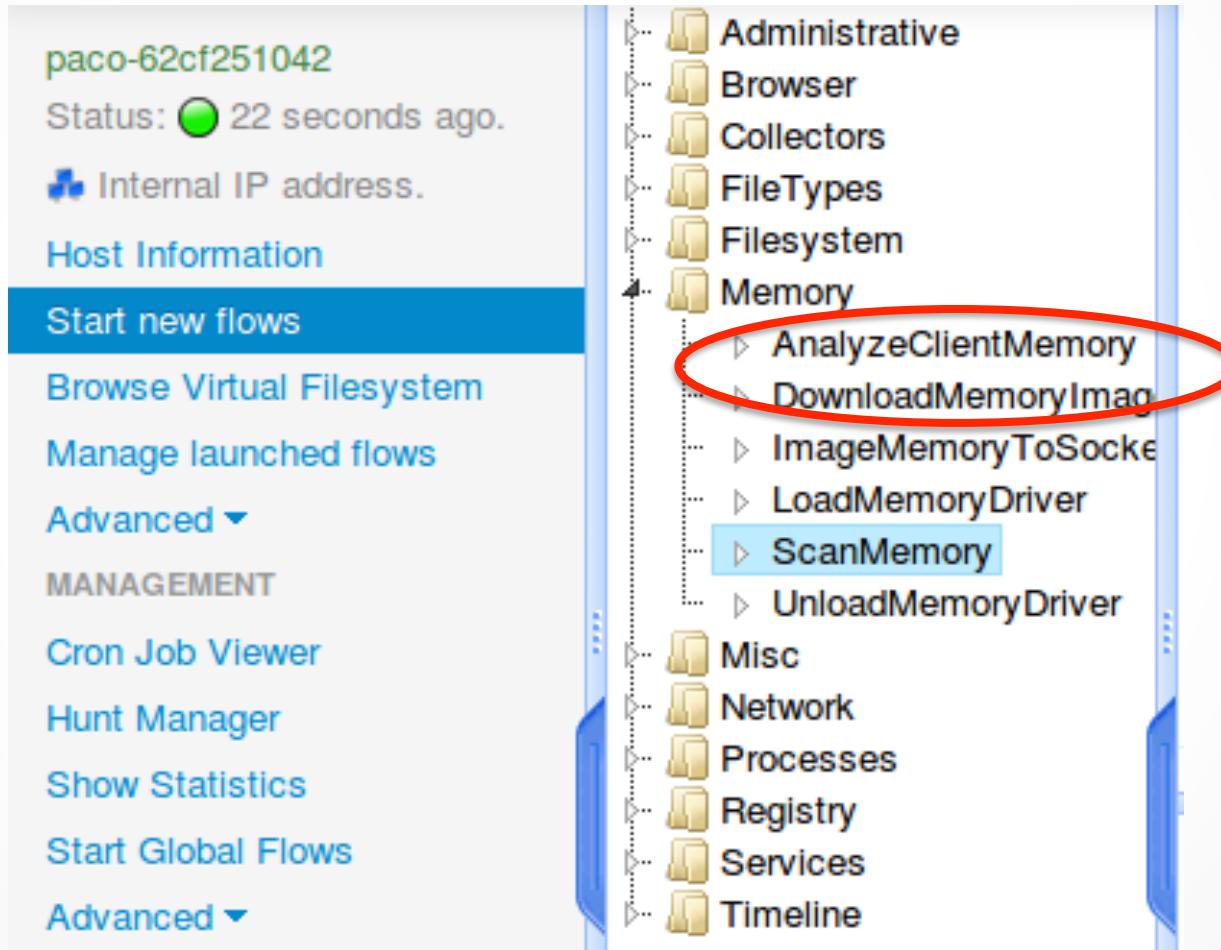
Host Information Start new flows Browse Virtual Filesystem Manage launched flows Advanced ▾ MANAGEMENT Cron Job Viewer Hunt Manager Show Statistics Start Global Flows Advanced ▾ CONFIGURATION Manage Binaries Settings

Offset	Data
162465947	6D 6E 75 78 2E 20 34 35 31 20 4A 4F 49 4E 20 3A mnux..451.JOIN.: 59 6F 75 20 68 61 76 65 You have
162504791	31 36 38 2E 32 31 37 2E 35 20 4A 4F 49 4E 20 3A 168.217.5.JOIN.: 23 6D 69 6B 61 67 0D 0A #mikag..
162777142	69 9B 50 10 FA F0 3D 46 00 00 4E 49 43 4B 20 3A i.P...=F..NICK.: 6D 69 6B 65 79 0A 55 53 mikey.US
162777188	6D 65 2C 20 70 75 73 73 79 0A 4A 4F 49 4E 20 23 me,.pussy.JOIN.# 6D 69 6B 61 67 20 73 6F mikag.so
162787382	15 DF 50 10 FA F0 BB 64 00 00 4E 49 43 4B 20 6D ..P....d..NICK.m 69 6B 65 79 0A 43 4E 44 ikey.CND

Dietro le quinte



Memory kung-fu e molto altro



GRR - Riferimenti

- URL: <https://code.google.com/p/grr/>
- Developer Documentation
<https://github.com/google/grr-doc/blob/master/implementation.adoc>
- Mailinglist:
grr-users@googlegroups.com
grr-dev@googlegroups.com

“Built by engineers for engineers”

Domande?

I has a question...



Grazie per l'attenzione

- Pasquale Stirparo
 - <http://it.linkedin.com/in/pasqualestirparo>
- Twitter:
 - @pstirparo, @sefirtech
- E-mail:
 - pasquale.stirparo@sefirtech.com
 - pstirparo@gmail.com



sefirtech

