SOC e Sicurezza gestita: rilevamento e risposta al Malware Evasivo

Security Summit Milano 2015

I relatori

Marco Ceccon
Principal Security Advisor
at Sinergy SpA

- Esperienza pluriennale (15+) nei settori ICT ed Information Security.
- Ha acquisito esperienze rilevanti e di successo in diversi ambiti, tra cui quello ICT e di Governo della sicurezza (COBIT, ISO 27001), Risk Management, Business Continuity e Disaster Recovery, Compliance normativa (SOX, Privacy, ITIL) e in innumerevoli progetti InfoSec.
- Marco Ceccon è membro di Information System Audits and Control Association (ISACA) e di International Information Systems Security Certification Consortium (ISC2), ha inoltre acquisito e detiene le seguenti certificazioni professionali: **CISSP, CISA, CISM, CRISC, ISO27001:13 LA, Cobit 5.0, ITILv3**

Marco Cova
Founding Team Member
at Lastline,Inc.

- Marco Cova è membro del founding team di Lastline, Inc, di cui guida il centro di R&D a Londra
- E` stato professore di Computer Security presso l'University of Birmingham, UK
- Ha ricevuto il PhD in Computer Science presso l'University of California, Santa Barbara
- Ha pubblicato oltre 25 articoli in conferenze e riviste internazionali su temi di systems security
- Ha progettato e implementato strumenti di sicurezza disponibili pubblicamente (e.g., Wepawet)

Il problema APT
Definizione 1/2

- Originariamente definiti come Advanced Persistent Threat (**APT**) hanno acquisito nel tempo altre nomenclature come Advanced Targeted Attack (**ATA**), Stealthy Threat ed oggi anche Advanced Evasion Technique (**AET**).

L'APT è una minaccia molto sofisticata con elevate risorse che gli consentono, attraverso l'utilizzo di vettori multipli di attacco (informatici, fisici e/o con l'utilizzo di azioni ingannevoli), di generare opportunità ed alte probabilità di raggiungere i propri obiettivi. Questi consistono tipicamente nello stabilire e ampliare il più possibile i propri presidi all'interno dell'infrastruttura informatica dei propri target allo scopo di ottenere informazioni e dati in modo continuativo e, quindi, di compromettere od ostacolare la mission e gli obiettivi dell'azienda.

Inoltre, l'APT tenta di perseguire i propri obiettivi ripetutamente per periodi di tempo prolungati, adattandosi e resistendo agli sforzi di eventuali contromisure con lo scopo di mantenere il livello di interazione necessario per raggiungere i propri obiettivi **[NIST SP 800-53 R4]**

Il problema APT
Definizione 2/2

In sintesi:

APT non è (solo) malware oppure una singola attività ostile ma definisce una serie di azioni offensive dalle seguenti caratteristiche:

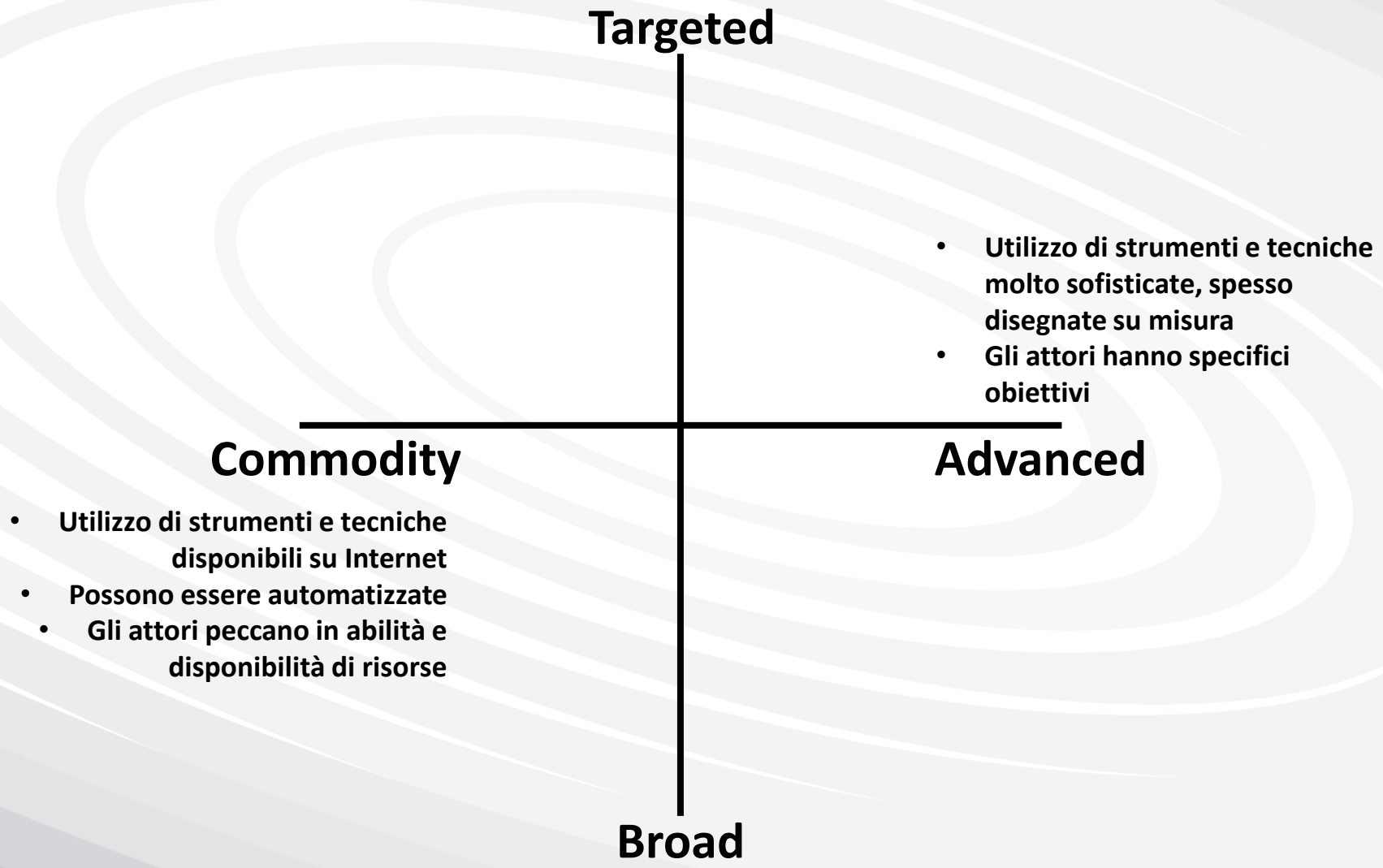
- **Target**: mirati su obiettivi specifici, con una strategia d'attacco complessa
- **Attori**: criminali organizzati, entità governative, spie industriali, mercenari o gruppi con capacità equivalenti
- **Strumenti**: sistemi di intrusione allo stato dell'arte: Malware avanzato, in combinazione con Social Engineering ed elevata capacità di infiltrazione
- **Timing**: Su intervalli di tempo anche molto lunghi (mesi o anni)

SINERGY

Targeted Attack
Alcuni esempi

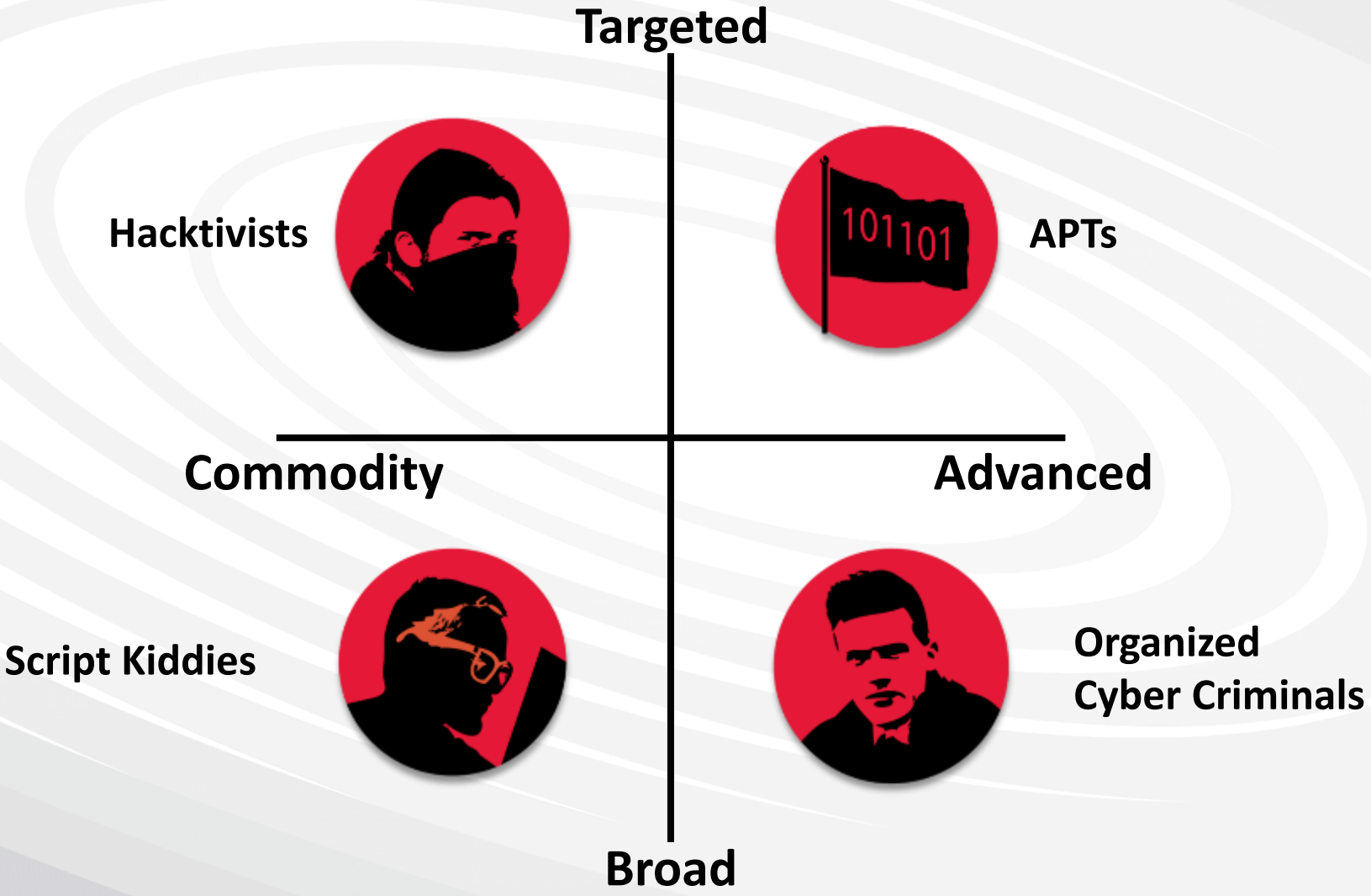
Il problema APT

Caratterizzazione della minaccia



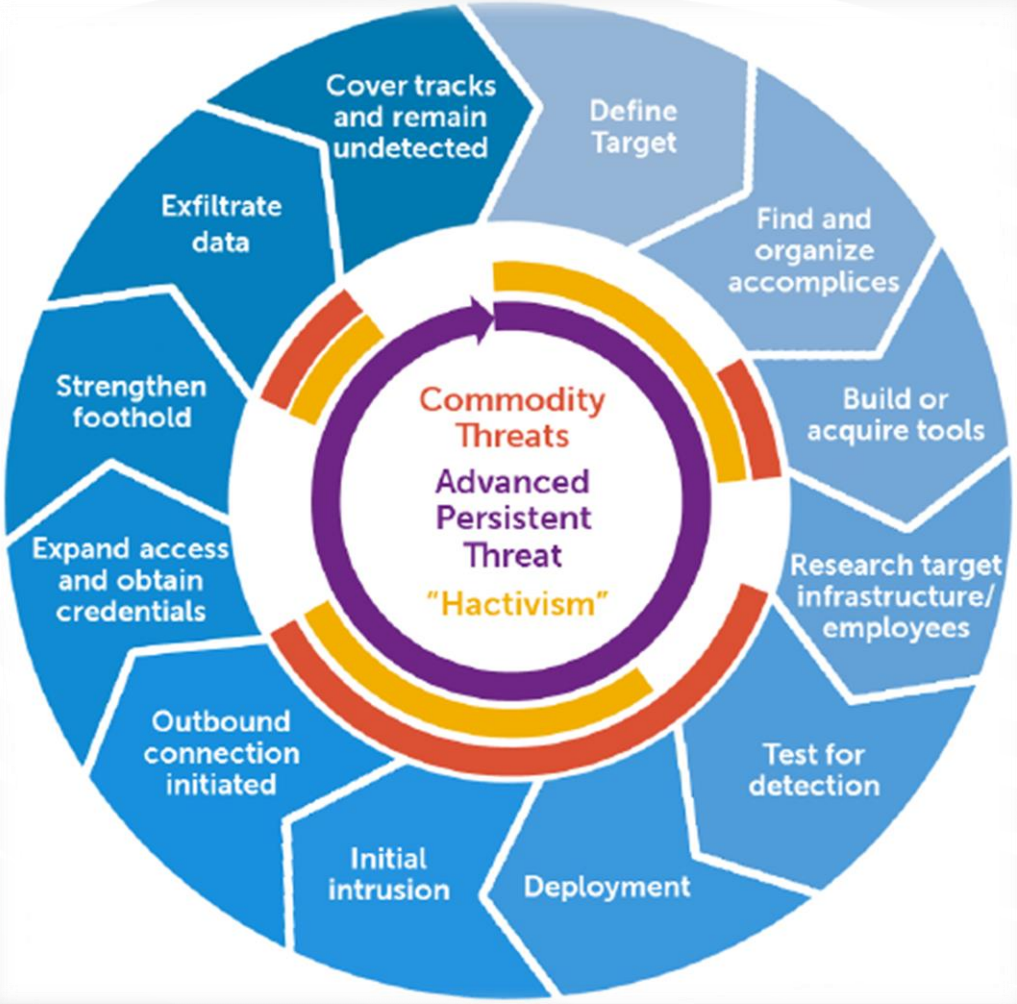
Il problema APT

Caratterizzazione della minaccia



Il problema APT

Comparazione sui modelli di attacco



Kill Chain

Gli APT possono utilizzare dapprima percorsi a minor resistenza usando strumenti e exploit semplici, graduando poi i livelli di sofisticazione in relazione ai risultati ottenuti.

Alcuni APT possono adattare e personalizzare le proprie Tattiche, Tecniche e Procedure (TTP) per prevedere ed **evadere** i controlli di sicurezza e le pratiche di risposta agli incidenti di sicurezza

La strategia di contrasto
«Breaking the Kill Chain»

La strategia di difesa, resistenza e risposta agli APT deve necessariamente basarsi su quattro elementi fondamentali di contrasto e cioè:

1. **Intelligence**: le Organizzazioni dovrebbero adottare soluzioni in grado di fornire informazioni utili al continuo miglioramento della «Security Posture» aziendale e alla prevenzione agli attacchi
2. **Operations**: è necessario valutare i livelli di efficacia ed efficienza dello staff di Security e perfezionare le competenze interne mediante esperti esterni in grado di monitorare e indirizzare le nuove minacce
3. **Visibility**: gli staff di Security dovrebbero avere piena visibilità della sicurezza dei propri sistemi per calibrare opportunamente le proprie policy in relazione a quello che sta succedendo dentro e fuori dei propri firewall
4. **Response**: risulta fondamentale che l'azienda disponga di un piano di Incident Response con i dettagli su ruoli e responsabilità. Il piano deve essere solido e collaudato per gestire l'incidente quando (**e non se**) capiterà

La soluzione integrata di contrasto

People – Processes – Technology

La soluzione è basata su:

- La predisposizione di opportuni **processi di gestione degli incidenti di Security**, eventualmente ingegnerizzati all'interno di un SOC aziendale
- L'utilizzo di servizi avanzati di **Managed Security**
- L'impiego di **tecnologie all'avanguardia** per capacità di rilevazione degli attacchi

La soluzione integrata di contrasto
Predisposizione processi di Incident Handling

Analisi e definizione dei processi di Security aziendali – **anche ingegnerizzati all'interno di un SOC** – utili alla gestione degli incidenti di sicurezza. Ciò concretizza in:

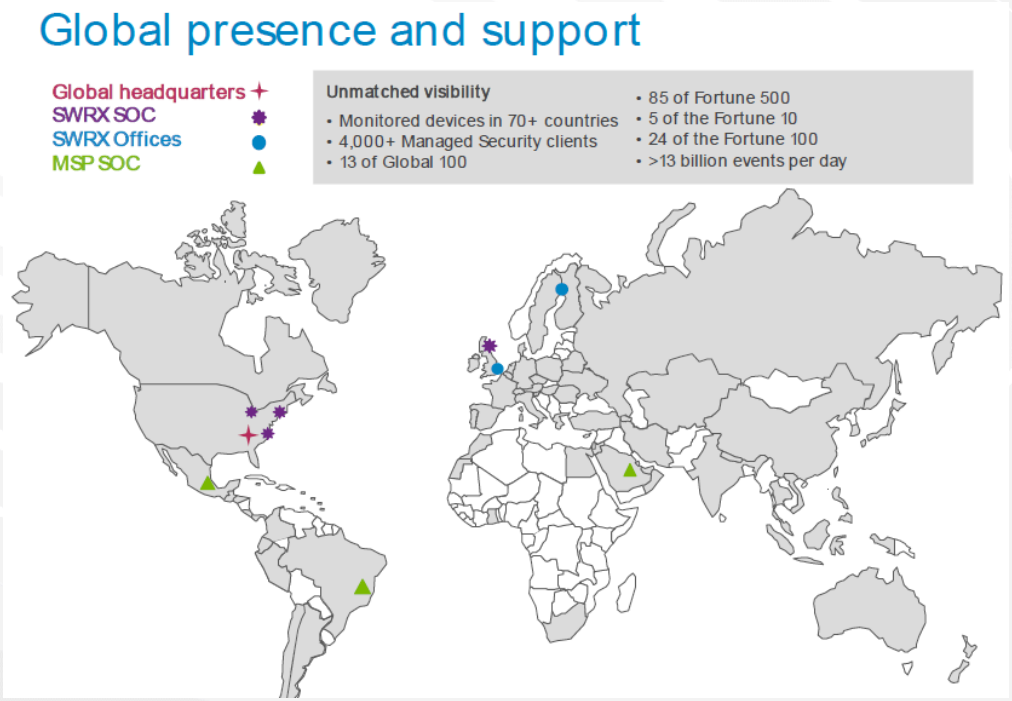
- Attribuzione di ruoli e responsabilità;
- Formalizzazione dei workflow di processo;
- Interazioni con Managed Security Services esterni

Processi di Incident Handling	Obiettivo
Incident Identification	Individuazione di potenziali infezioni o attività maliziose in corso
Incident Classification	Classificazione dell'incidente in corso al fine di individuarne la criticità del target coinvolto, la tipologia di attacco e la gravità dell'allarme
Incident Notification	Comunicazione dell'incidente in corso ai riferimenti prestabiliti
Incident Response & Containment	Individuazione delle appropriate strategie di contenimento e reazione all'incidente in corso, al fine di limitarne l'impatto sui sistemi e servizi

La soluzione integrata di contrasto

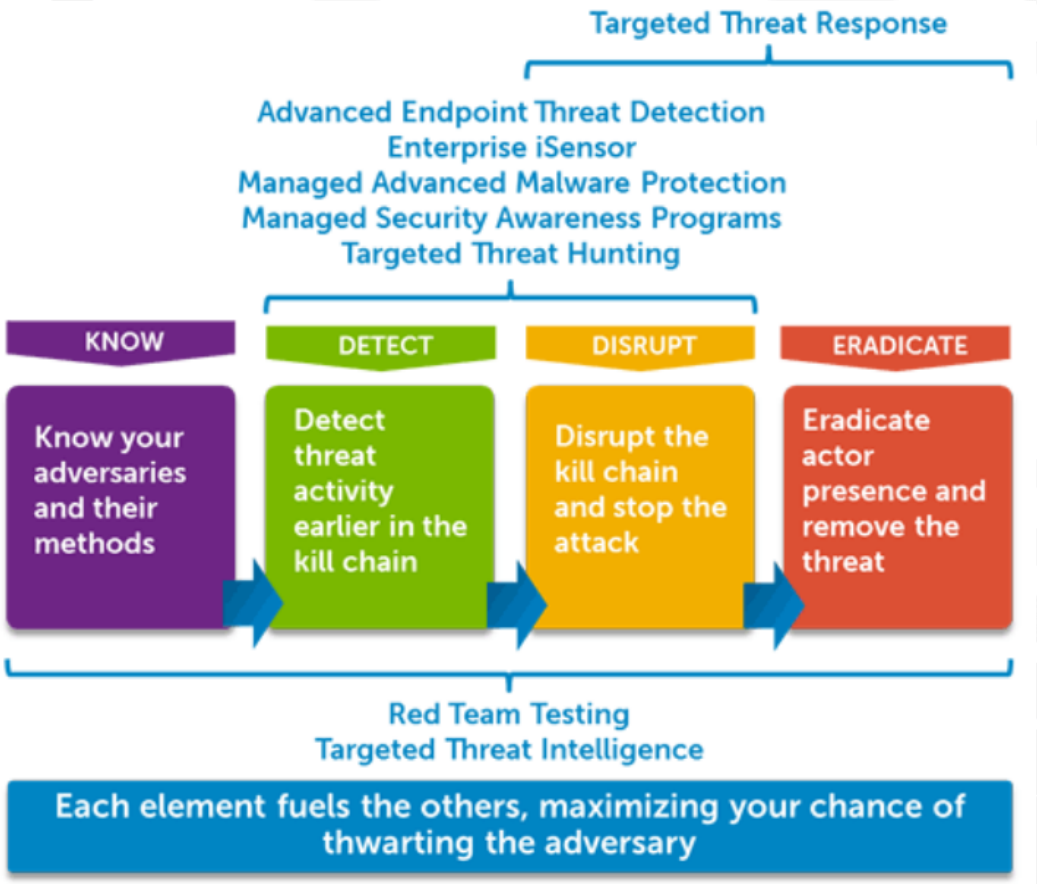
Utilizzo di servizi avanzati di Managed Security

- Gamma completa di servizi di Managed Security, Consulting ed Intelligence
- 15+ anni di esperienza su servizi di sicurezza
- 7 Security Operations Center
- 3,600+ client in tutto il mondo in 70+ paesi
- Gestione/Monitoraggio di 150K+ device
- 70 miliardi di eventi al giorno
- Visibilità globale
- Analisti certificati
- Team di ricerca avanzato: Counter Threat Unit (CTU)
- Supporto Vendor-neutral



Dell SecureWorks
Advanced Threat Services

Costituisce una serie completa di servizi avanzati disegnati specificatamente per combattere gli APT e contrastare la Kill Chain:



AETD: avverte sulla possibilità che gli endpoint possano ospitare un malware avanzato

TTI: individua gli APT e gli attori dietro di essi, ottiene informazioni su exploit e prende le giuste precauzioni per evitarli

RTT: simula un attacco avanzato per determinare l'efficacia delle difese di Security

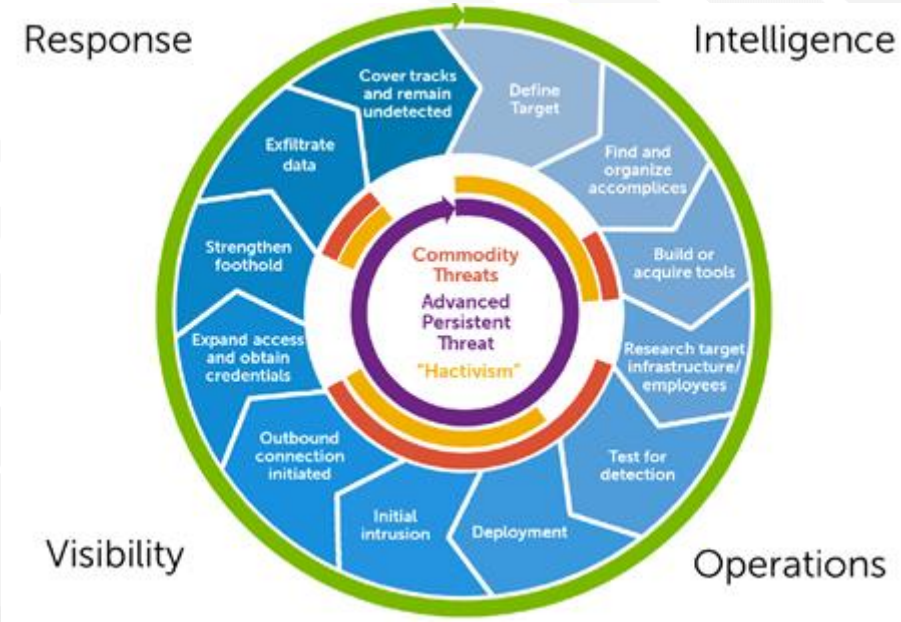
TTR: fornisce un rapido contenimento ed eradicazione di sofisticati APT, diminuendo la durata e l'impatto di una breccia di sicurezza

IRT: per il rapido contenimento ed l'eradicazione delle minacce

Dell SecureWorks
Advanced Malware Protection and Detection

Dell SecureWorks ha scelto la tecnologia ***Breach Detection Platform*** di ***Lastline*** per erogare i propri servizi di AMPD che comprendono:

- Rilevazione signature-less e blocco di malware avanzato o personalizzato ottenuto via email o contenuti web
- Rilevazione e blocco di traffico outbound di tipologia Command and Control (C2)
- Monitoraggio 24x7 ed analisi di eventi di sicurezza che includano malware in inbound ed alert C2
- Approvvigionamento, deployment e tuning di device anti-APT multivendor
- Amministrazione di aggiornamenti, patch e changes
- Supporto del Counter Threat Unit cyber intelligence team

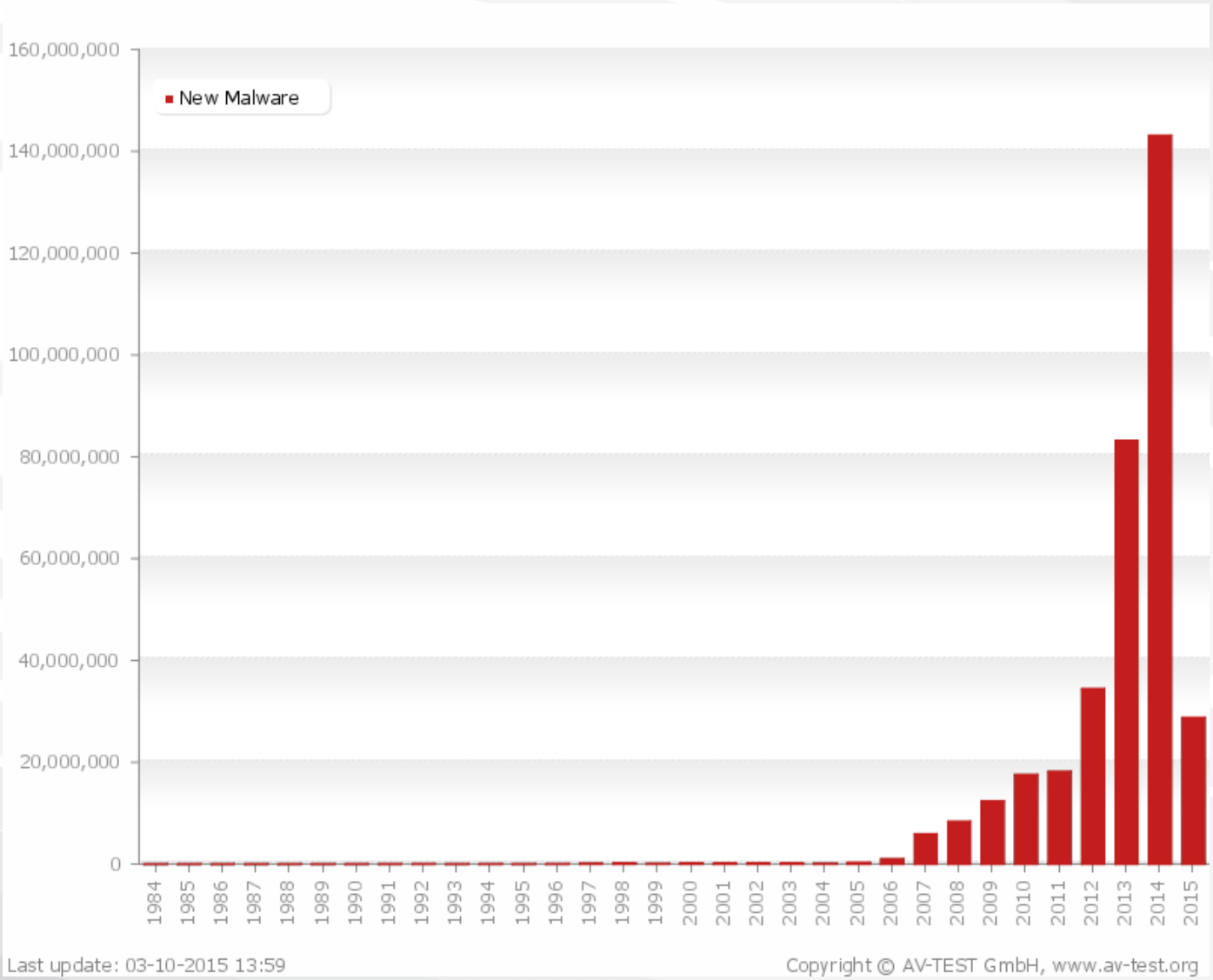


Analisi di malware, oggi

Quali sono le sfide principali?

- Scaling
- Precisione
- Robustezza contro tentativi di evasione

Scaling


New Malware
160,000,000
140,000,000
120,000,000
100,000,000
80,000,000
60,000,000
40,000,000
20,000,000
0
1984
1985
1986
1987
1988
1989
1990
1991
1992
1993
1994
1995
1996
1997
1998
1999
2000
2001
2002
2003
2004
2005
2006
2007
2008
2009
2010
2011
2012
2013
2014
2015
Last update: 03-10-2015 13:59
Copyright © AV-TEST GmbH, www.av-test.org

Precisione

NETWORK 1

- Command & Control traffic observed

STEAL 1

- Reading FTP client credentials
- Reading user's mail server credentials

SEARCH 4

- Enumerating keys related to FTP clients
- Searching for Firefox Key Database
- Searching for Firefox Security Certificates
- Searching for Firefox Security module database

FILE 1

- Searching for files iterating over directories

Analisi dinamica

- Implementata come esecuzione all'interno di un ambiente d'esecuzione instrumentato (*sandbox*)
  - Esegui il programma e osserva cio` che fa
  - Determina se il comportamento e` malevolo o meno
- Automazione!
  - Analisti non devono ispezionare ciascun sample manualmente
  - Chiave per ottenere scalability
  - Puo` rilevare zero-day

Analisi dinamica @ Lastline

- Abbiamo costruito e usiamo una nostra sandbox:
  - Basata su full system emulation
    - Puo` vedere ciascuna istruzione
  - Supporta analisi di *data flow* (*taint tracking*)
  - Monitora l'attivita` del sistema dall'esterno (meno rilevabile dal malware)
  - Piattaforma generica su cui implementare analisi
- Generazione successiva di Anubis: ANalyzing Unknown BInarieS
  - http://anubis.iseclab.org/

VM vs. Full system emulation


```
cmpl    $0x0c,%ebx
je      0x10000f21e
xorl    %esi,%esi
movq    %r15,%rdi
xorl    %eax,%eax
callq   0x100070478     ; symbol stub for: _open
movl    %eax,%r12d
testl   %eax,%eax
js      0x10000f21e
leaq    0xffffff70(%rbp),%rcx
movq    %rcx,0xfffffec0(%rbp)
movl    $0x00000050,%edx
movq    %rcx,%rsi
movl    %eax,%edi
callq   0x1000704b4     ; symbol stub for: _read
movq    %rax,%r13
movl    %eax,%r14d
movl    %r12d,%edi
callq   0x1000702b6     ; symbol stub for: _close
cmpl    $0x02,%r13d
jle     0x10000f21e
```

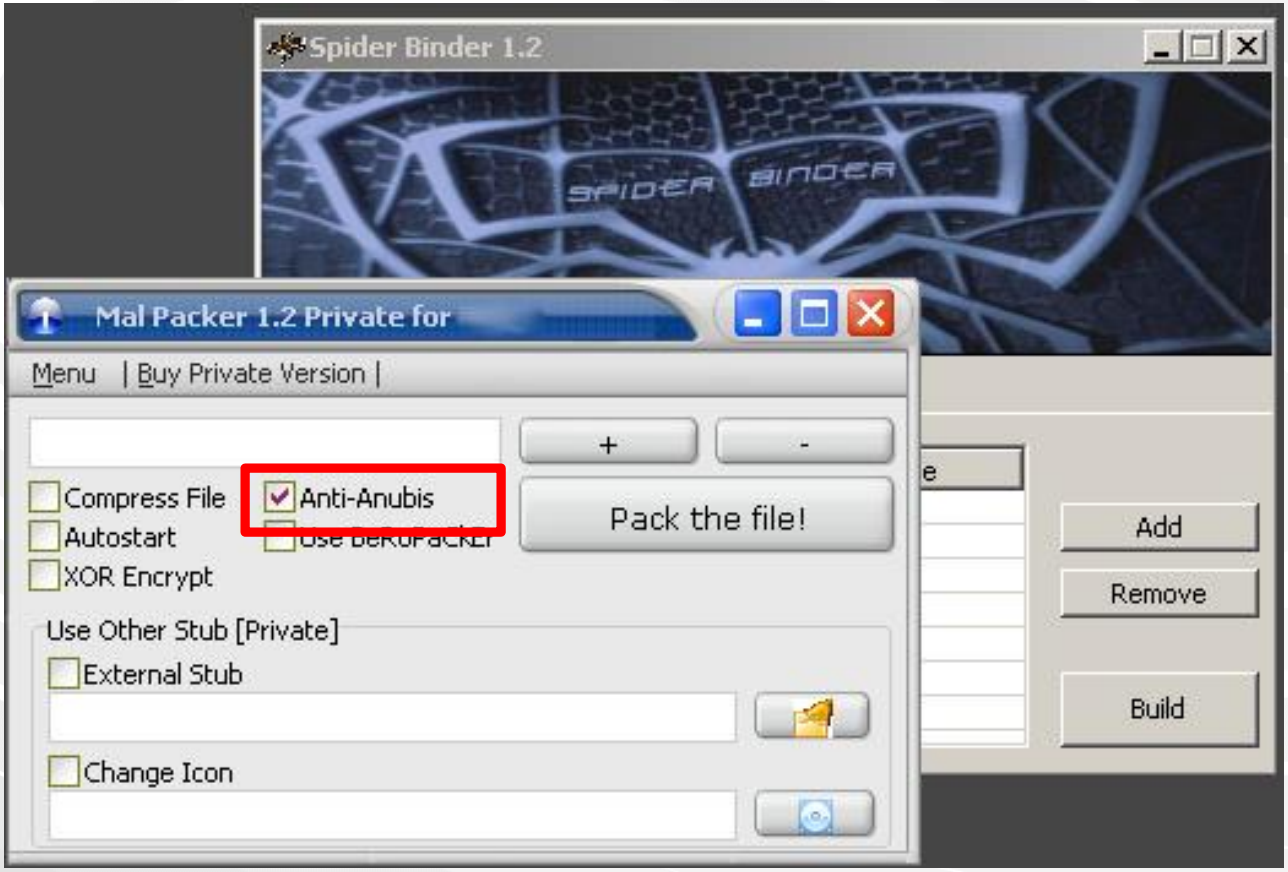
Codice evasivo

- Autori di malware vogliono evitare che i loro programmi siano rilevati
  - Sandbox esegue il codice → tante opzioni
- Codice evasivo:
  - Nessun comportamento malevolo all'interno di una sandbox, ma
  - infetta il vero bersaglio dell'attacco
- Miriade di tecniche…

Codice evasivo

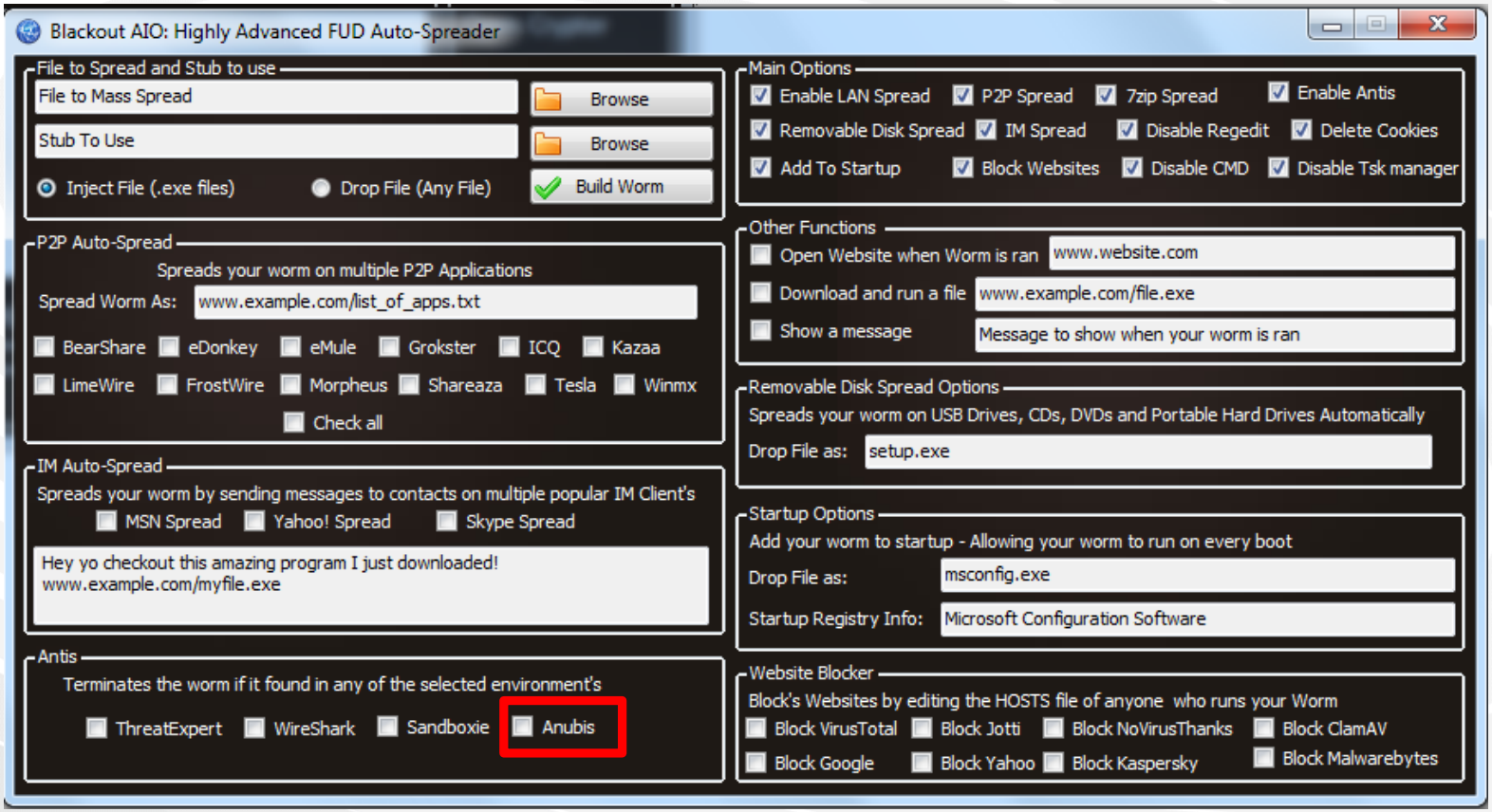
- Ambiente di esecuzione virtualizzato?
  - Differenze tra un ambiente virtuale e uno fisico (*bare metal*)
  - Controlli basati su caratteristiche della CPU
  - Artefatti del sistema operativo
- Malware puo` rilevare segni di un particolare ambiente di analisi:
  - File, processi, driver, etc.
- Malware puo` provare ad impedire l'analisi automatizzata
  - Esegue codice senza che il sistema di analisi lo "veda"
  - Verifica che ci sia una persona dietro la tastiera
  - Aspetta che l'analisi termini prima di fare azioni interessanti

Codice evasivo



Codice evasivo

Codice evasivo



Rilevare ambienti virtualizzati

- Lacune nel supporto hardware per la virtualizzazione:
  - J. Robin and C. Irvine: Analysis of the Intel Pentium's Ability to Support a Secure Virtual Machine Monitor; Usenix Security Symposium, 2000
  - RedPill

Rilevare ambienti virtualizzati

- Lacune nel supporto hardware per la virtualizzazione:
  - J. Robin and C. Irvine: Analysis of the Intel Pentium's Ability to Support a Secure Virtual Machine Monitor; Usenix Security Symposium, 2000
  - RedPill

Joanna Rutkowska

Swallowing the Red Pill is more or less equivalent to the following code (returns non zero when in Matrix):

```
int swallow_redpill () {
  unsigned char m[2+4], rpill[] = "\x0f\x01\x0d\x00\x00\x00\x00\xc3";
  *((unsigned*)&rpill[3]) = (unsigned)m;
  ((void(*)())&rpill)();
  return (m[5]>0xd0) ? 1 : 0;
}
```

Rilevare ambienti virtualizzati

- Lacune nel supporto hardware per la virtualizzazione:
  - J. Robin and C. Irvine: Analysis of the Intel Pentium's Ability to Support a Secure Virtual Machine Monitor; Usenix Security Symposium, 2000
  - RedPill

- Intel-VT and AMD-V aiutano
- Ma ci sono ancora differenze di timing

Rilevare ambienti virtualizzati

- Bug o imprecisioni nell'emulazione della CPU
  - Eccezioni per *opcode* invalidi, eccezioni incorrette, …
  - R. Paleari, L. Martignoni, G. Roglia, D. Bruschi: A fistful of red-pills: How to automatically generate procedures to detect CPU emulators; USENIX Workshop on Offensive Technologies (WOOT), 2009
  - Malware usa istruzioni matematiche tipicamente non usate…
- Ma e` vero che ambiente virtuale = sistema di analisi?

Rilevare sistema di analisi

- Controlli sul Product ID di Windows XP

```
HKLM\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\ProductID
```

- Controlli sullo user name, il nome dei processi, il nome del disco fisso

```
HKLM\SYSTEM\CURRENTCONTROLSET\SERVICES\DISK\ENUM
```

- Controlli su DLL non previste o mutex
- Controlli sul colore del background
- Controlli sul tipo di mouse, il layout della tastiera, ….

Rilevare sistema di analisi

```
.text:00401E39 loc_401E39:                             ; CODE XREF: .text:00401DCC↑j
.text:00401E39                                         ; .text:00401DC3↑j
.text:00401E39                 mov     eax, [ebp-270h]
.text:00401E3F
.text:00401E3F loc_401E3F:                             ; CODE XREF: .text:00401DD1↑j
.text:00401E3F                 mov     [ebp-170h], eax
.text:00401E45
.text:00401E45 loc_401E45:                             ; CODE XREF: .text:00401E2B↑j
.text:00401E45                 push    dword ptr [ebp-16Ch]
.text:00401E4B                 call    dword ptr [ebp-34h]
.text:00401E4E                 cmp     dword ptr [ebp-170h], 'awmv' ;
.text:00401E4E                                         ; search known sandboxes'
.text:00401E4E                                         ; substring in registry key value
.text:00401E4E                                         ; vbox
.text:00401E4E                                         ; qemu
.text:00401E4E                                         ; vmwa
.text:00401E58                 jz      short loc_401E95
.text:00401E5A                 cmp     dword ptr [ebp-170h], 'xobv'
.text:00401E64                 jz      short loc_401E95
.text:00401E66                 cmp     dword ptr [ebp-170h], 'umeq'
.text:00401E70                 jz      short loc_401E95
.text:00401E72
.text:00401E72 loc_401E72:                             ; CODE XREF: .text:00401D55↑j
.text:00401E72                                         ; .text:00401D6D↑j ...
.text:00401E72                 rdtsc
```

Rilevare sistema di analisi

Rilevare sistema di analisi


```
if( (snd = FindWindow("SandboxieControlWndClass", NULL)) ){
  return true; // Detected Sandboxie
} else if( (pch = strstr (str,"sample")) || (user == "andy") || (user == "Andy") ){
  return true; // Detected Anubis sandbox.
} else if( (exeName == "C:\file.exe") ){
  return true; // Detected Sunbelt sandbox.
} else if( (user == "currentuser") || (user == "Currentuser") ){
  return true; // Detected Norman Sandbox.
} else if( (user == "Schmidti") || (user == "schmidti") ){
  return true; // Detected CW Sandbox.
} else if( (snd = FindWindow("Afx:400000:0", NULL)) ){
  return true; // Detected WinJail Sandbox.
} else {
  return false;
}
```

Rilevare l'utente

- Apri una finistra e attendi che l'utente clicchi
  - Si aspetta che l'utente muova il mouse
  - Si aspetta che l'utente apra/chiuda finestre

```
var X=this.mouseX;
var Y=this.mouseY;
for (;;) {
 if ((this.mouseX!=X)||
     (this.mouseY!=Y)){
        break;
 }
}
do_evil_stuff();
```

Procrastinare

- Compie azioni malevole solo dopo che il sistema e` stato riavviato
  - Sistema di analisi puo` rilevare il fatto che il malware prova a rendersi persistente
- Gira solo prima/dopo date specifiche
- Dorme per un po’ (tutti i sistemi di analisi hanno timeout)
  - Tipicamente, qualche minuto
  - “Dorme” in un modo piu` sofisticato (*stalling code*)

Procrastinare

```
SYSTEMTIME SystemTime;

DisableThreadLibraryCalls(hdll);
GetSystemTime(&SystemTime);
result = SystemTime.wMonth;
if (SystemTime.wDay + 100 * (SystemTime.wMonth + 100 * (unsigned int)SystemTime.wYear)
    >= 20120101)
{
  uint8_t* pmain_image = (uint8_t*)GetModuleHandleA(0);
  IMAGE_DOS_HEADER *pdos_header = (IMAGE_DOS_HEADER*)pmain_image;
  IMAGE_NT_HEADERS *pnt_header = \
      (IMAGE_NT_HEADERS*)(pdos_header->e_lfanew + pmain_image);
  uint8_t* entryPoint = pmain_image + pnt_header->OptionalHeader.AddressOfEntryPoint;
  result = VirtualProtect(entryPoint, 0x10u, 0x40u, &flOldProtect);

  if (result)
  {
    entryPoint[0] = 0xE9;
    entryPoint[1] = (uint8_t)((uint8_t *)loadShellCode - entryPoint - 5);
    entryPoint[2] = (uint8_t)(((uint8_t *)loadShellCode - entryPoint - 5) >> 8);
    entryPoint[3] = (uint8_t)(((uint8_t *)loadShellCode - entryPoint - 5) >> 16);
    entryPoint[4] = (uint8_t)(((uint8_t *)loadShellCode - entryPoint - 5) >> 24);
    result = VirtualProtect((LPVOID)entryPoint, 0x10u, flOldProtect, &flOldProtect);
  }
```

Procrastinare

```
1 unsigned count, tick;
2
3 void helper() {
4   tick = GetTickCount();
5   tick++;
6   tick++;
7   tick = GetTickCount();
8 }
9
10 void delay() {
11   count=0x1;
12   do {
13     helper();
14     count++;
15   } while (count!=0xe4e1c1);
16 }
```

Figure 1. Stalling code found in real-world malware (W32.DelfInj)

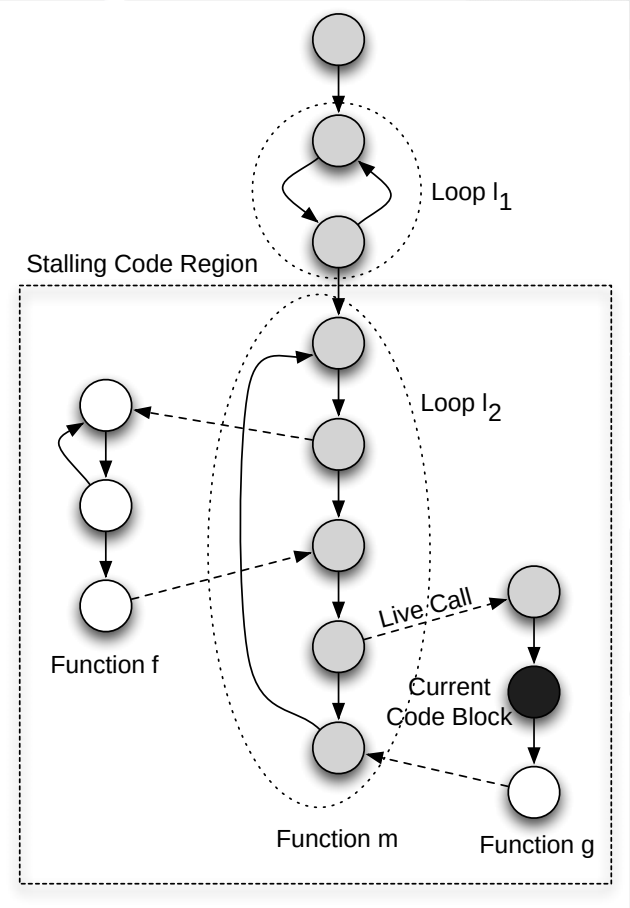
Macchina reale - Qualche millisecondo
Anubis – Dieci ore

Aggirare stalling loop

- Mitigare stalling loops
  1. Rilevare che il programma non fa progressi
  2. Modalita` passiva
     - Trovare il loop che e` attivo
     - Ridurre il logging per questo loop (finche` non e` interrotto)
  3. Modalita` attiva
     - Quando la riduzione del logging non e` sufficiente
     - Interrompere attivamente il loop
- Controlli di progresso
  - Basati sul monitoraggio delle system call:
    troppi errori, troppo poche chiamate, sempre le stesse, …

Modalita` passiva

- Trovare i blocchi di codice per cui possiamo ridurre il logging
  - Costruisci il control flow graph dinamico
  - Esegui l'algoritmo di rilevamento del loop
  - Identifica i blocchi attivi e archi
  - Identifica il primo loop attivo
  - Marca tutte le regioni raggiungibili da questo loop



Modalita` attiva

- Interrompere il loop
  - Trova il salto condizionale che conduce fuori dalla regione white-listed
  - Inverti la condizione la prossima volta che il salto viene eseguito
- Problema
  - Il programma potrebbe successivamente usare variabili che sono scritte dentro il loop
  - Se invertiamo semplicemente il salto, le variabili non avranno il valore corretto e il programma fallisce

```
1 // H4X0r: make sure delay loop was not interrupted
2 void check() {
3  if (count!=0xe4e1c1) exit();
4 }
```

- Soluzione
  - Marca tutte le variabili scritte dentro il loop
  - Traccia tutte le variabili che sono marcate (taint analysis)
  - Quando il programma usa una di queste variabili, estrai una slice che ne calcola il valore, esegui la slice, e forza il valore nell'esecuzione originale

Risultati sperimentali

Description	# samples	%	# AV families
base run	29,102	–	1329
stalling	9,826	33.8%	620
loop found	6,237	21.4%	425

- **1,552 / 6,237 stalling samples reveal additional behavior**
- **At least 543 had obvious signs of malicious (deliberate) stalling**

Description	Passive			Active		
	# samples	%	# AV families	# samples	%	# AV families
Runs total	3,770	–	319	2,467	–	231
Added behavior (any activity)	1,003	26.6%	119	549	22.3%	105
- Added file activity	949	25.2%	113	359	14.6%	79
- Added network activity	444	11.8%	52	108	4.4%	31
- Added GUI activity	24	0.6%	15	260	10.5%	51
- Added process activity	499	13.2%	55	90	3.6%	41
- Added registry activity	561	14.9%	82	184	7.5%	52
- Exception cases	21	0.6%	13	273	11.1%	48
Ignored (possibly random) activity	1,447	38.4%	128	276	11.2%	72
- Exception cases	0	0.0%	0	82	3.3%	27
No new behavior	1,320	35.0%	225	1,642	66.6%	174
- Exception cases	0	0.0%	0	277	11.2%	63

Conclusioni

- Malware e` un componente essenziale di attacchi mirati oggigiorno
- Analisi automatizzata di malware deve risolvere alcune sfide chiavi
  - Evasione e` una sfida critica
- Tipi di evasione
  - Rilevamento di ambiente virtualizzato
  - Rilevamento del sistema di analisi
  - Impedire l'analisi
- Ci sono tecniche per affrontare certi tipi di evasione in maniera generale

Mission

Advisory
Storage
Security

Sinergy è il partner per costruire la ***platform as a services,*** specializzato nella Consulenza, nel Disegno, nella Realizzazione e Gestione di Infrastrutture ICT *business critical.*

Il nostro Approccio

1. ADVISORY

- Customer Business Needs
- IT &Security Advisory
- Gap Analysis & Remediation Plan
- Compliance

2. DESIGN & IMPLEMENTATION

- Project Planning
- IT Design, Transition & Operation
- Solution Integration
- DC Transformation
- Private Cloud

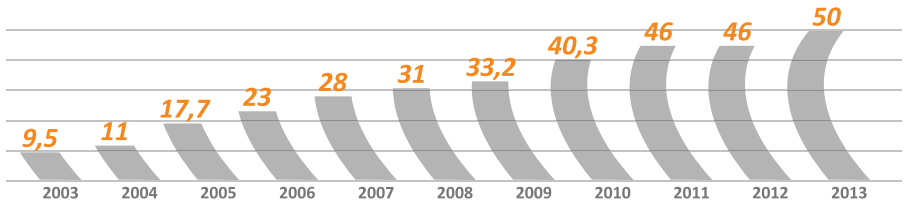
3. MANAGED SERVICES

- IT Service Management
- Flexible Managed Services
- IT & Security Governance
- NOC

Continuità e Solidità

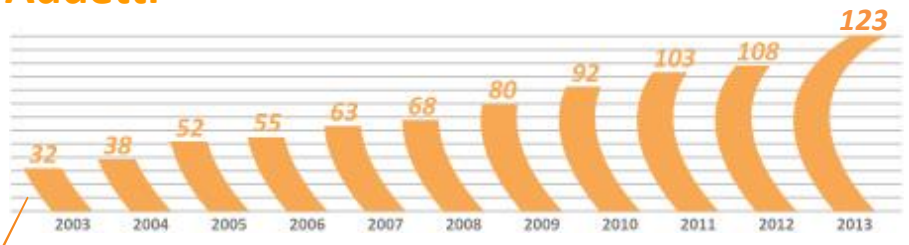
Le nostre sedi

Fatturato totale in mln di €



€ 50 milioni al 2013

Addetti



123 professionisti cui 73 technical specialist

SINERGY 20 1994-2014 da sempre con la stessa passione

Il Team Security
Consulenti d'alto livello

Il team di Security è composto da 25 professionisti con consolidata esperienza ed elevati skill professionali.

Certificazioni

ISO 27001 Certified
CISSP Certified Information Systems Security Professional
CISA
CRISC
CISM
COBIT 5
PMP Project Management Professional
Offensive Security OSCP
C|EH Certified Ethical Hacker
ITIL

Il team

Consulting

- Security Advisor
- Ethical Hacker

Professional services

- Senior Architect
- Technical Expert

SINERGY

More info:
m.ceccon@sinergy.it
www.sinergy.it