Huellas en la Memoria para Análisis de Malware

Mateo Martínez

intel Security

Mateo Martínez
@mateomartinez1
www.foundstone.com

- **Consultor en McAfee Foundstone**
  - Pentesting / Ethical Hacking
  - Social Engineering
  - Code Review
  - Incident Response
  - Entrenamientos Ultimate Hacking
- **OWASP Uruguay**
  - OWASP Days
  - OWASP Latam Tour
  - OWASP AppSec Latam 2012 (2015)
- **Certificaciones:**
  - CISSP
  - ISO 27001 Lead Implementer
  - PCI QSA
  - ITIL
  - MCP

Teoría

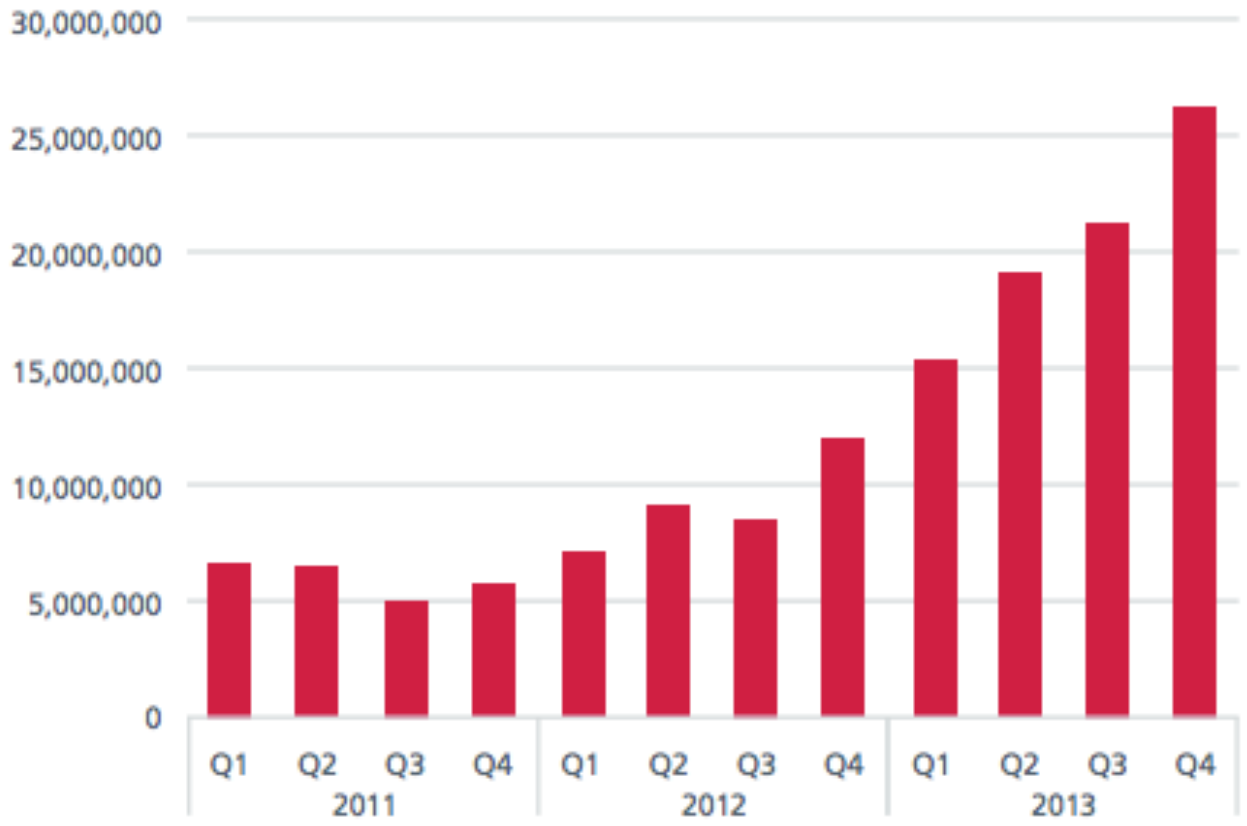
- Malware
- Respuesta ante Incidentes
- Forense Digital
- Herramientas

Práctica

- Adquisición de memoria
- Análisis de memoria
- Análisis de malware

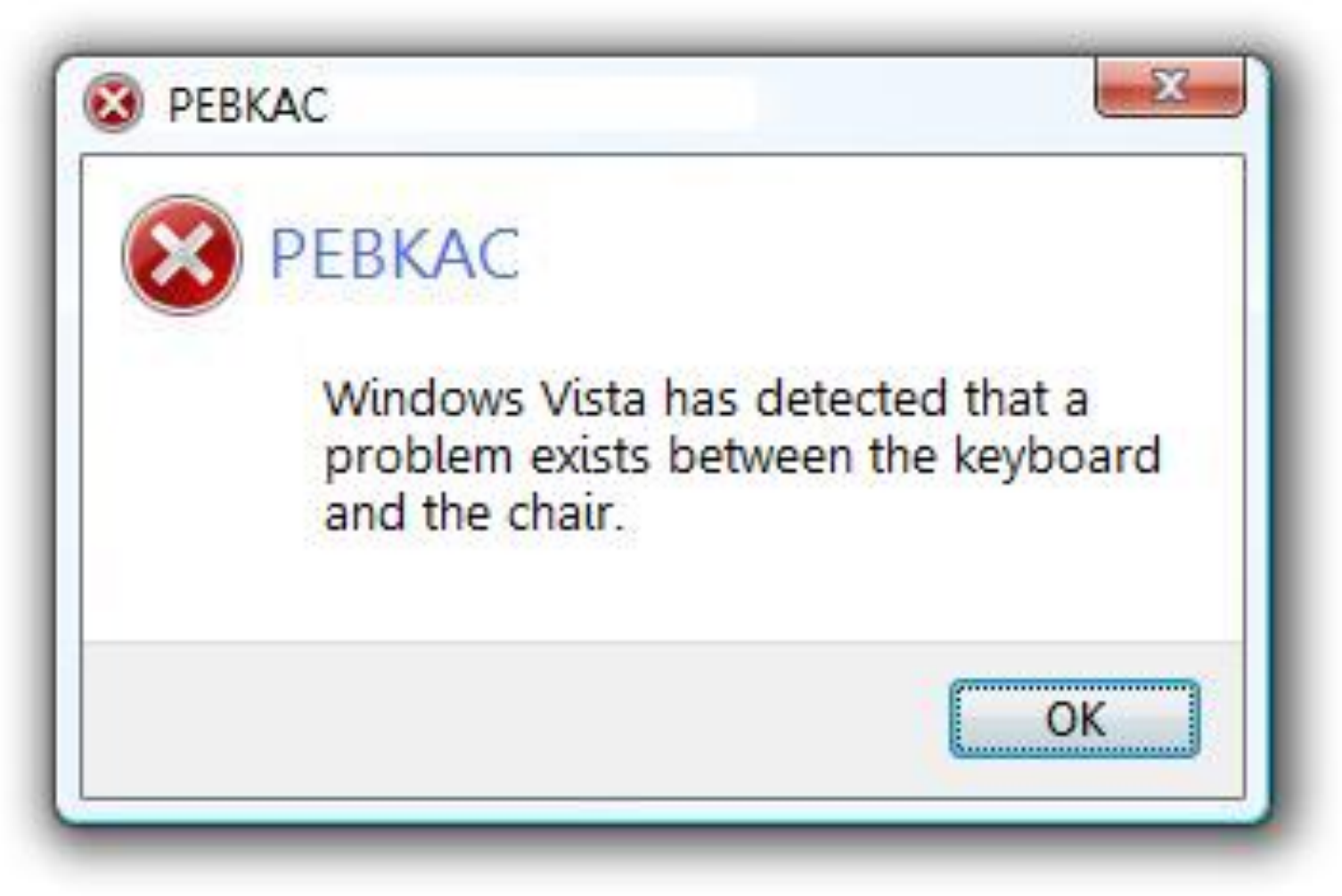
Malware

NEW MALWARE



Source: McAfee Labs, 2014.

El mayor vector de infección…



El **RFC 2828** define un **Incidente** como:

"Un evento de seguridad en el que la política de seguridad ha sido desobedecida o vulnerada"

http://www.ietf.org/rfc/rfc2828.txt
(212 páginas)

Principio de intercambio de Locard

"Every contact leaves a trace"

Dr. Edmond Locard
(13 diciembre 1877 – 4 mayo 1966)

Práctica Actual de Respuesta ante Incidentes

- Adquirir de lo más volatil a lo menos volatil
- El malware residente en memoria no puede analizarse a partir de una imágen de disco
- La memoria puede contenter claves de información que haya sido cifrada en el disco

El RFC 3227 define el orden básico para recolectar:

- Memoria del Sistema
- Archivos temporales (swapfile / paging file)
- Procesos y conexiones de red
- Información de routeo & ARP Cache
- Adquisición de Discos (Forense)
- Logs Remotos & Datos de Monitoreo
- Configuración física & Topología de Red
- Backups

http://www.ietf.org/rfc/rfc3227.txt

(10 páginas)

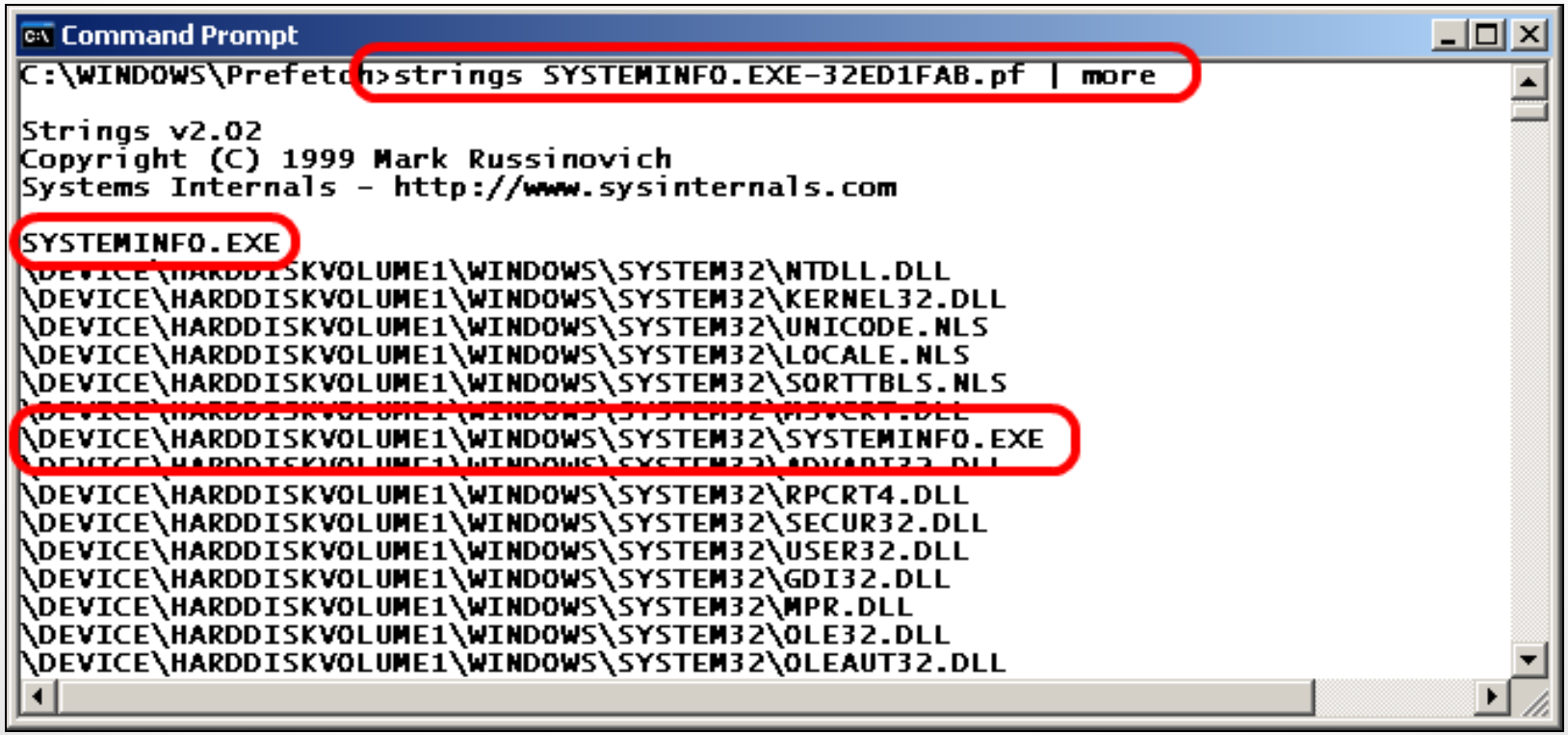
Información a revisar

- Archivos de Logs
- Procesos de Sistema
- Archivos ocultos inusuales
- Backdoors
- Tareas Programadas
- Nivel de Parches
- Relaciones de confianza
- Archivos temporales
- SWAP Files
- Reconstruir papelera de reciclaje
- Reconstruir el pool de impresión
- Extraer correos y archivos adjuntos
- Historia de navegación web
- Aplicaciones instaladas

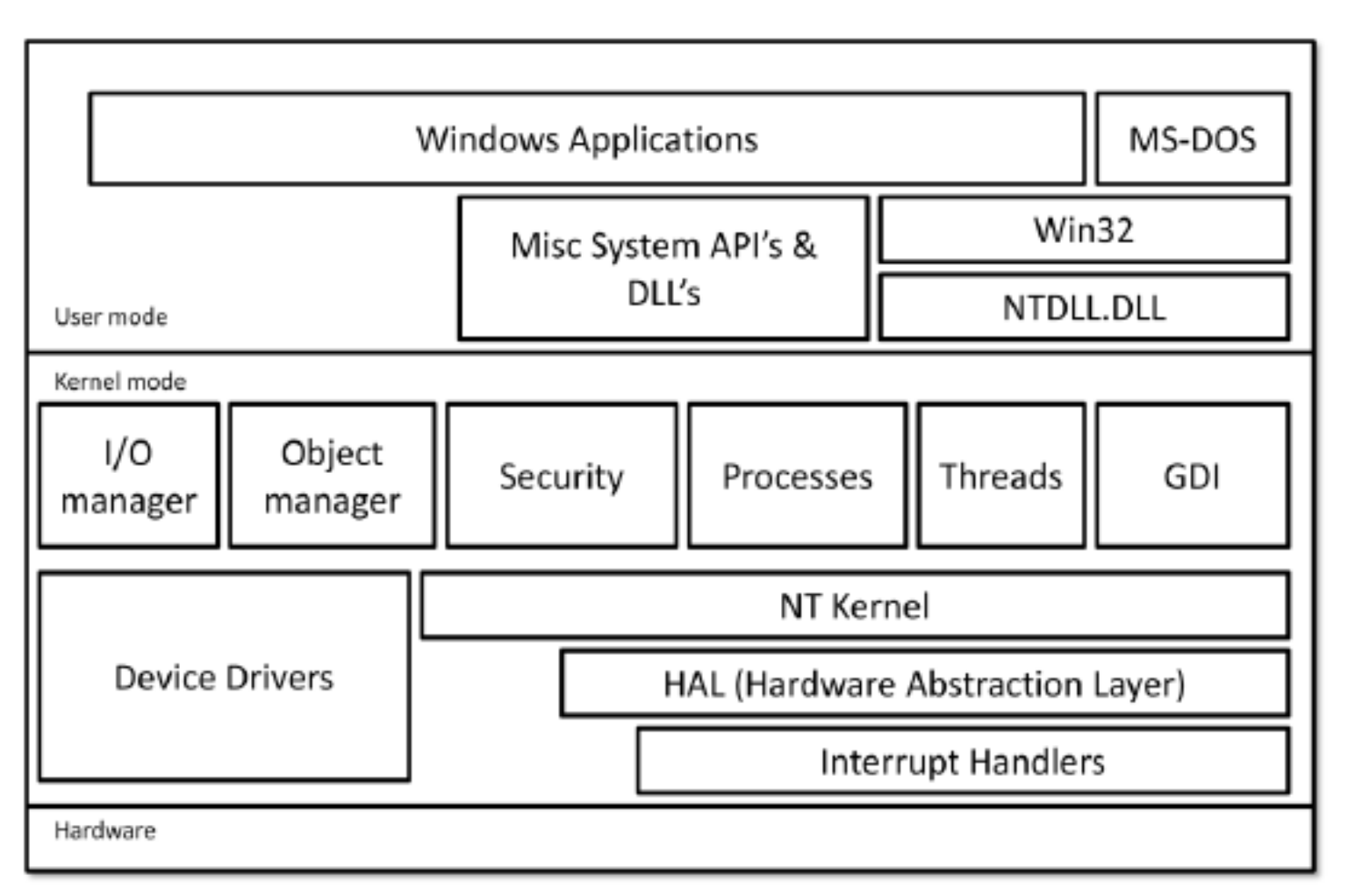
Windows Prefetch

Es un registro de los últimos 128 programas ejecutados en un sistema.

C:\Windows\Prefetch> strings *filename*

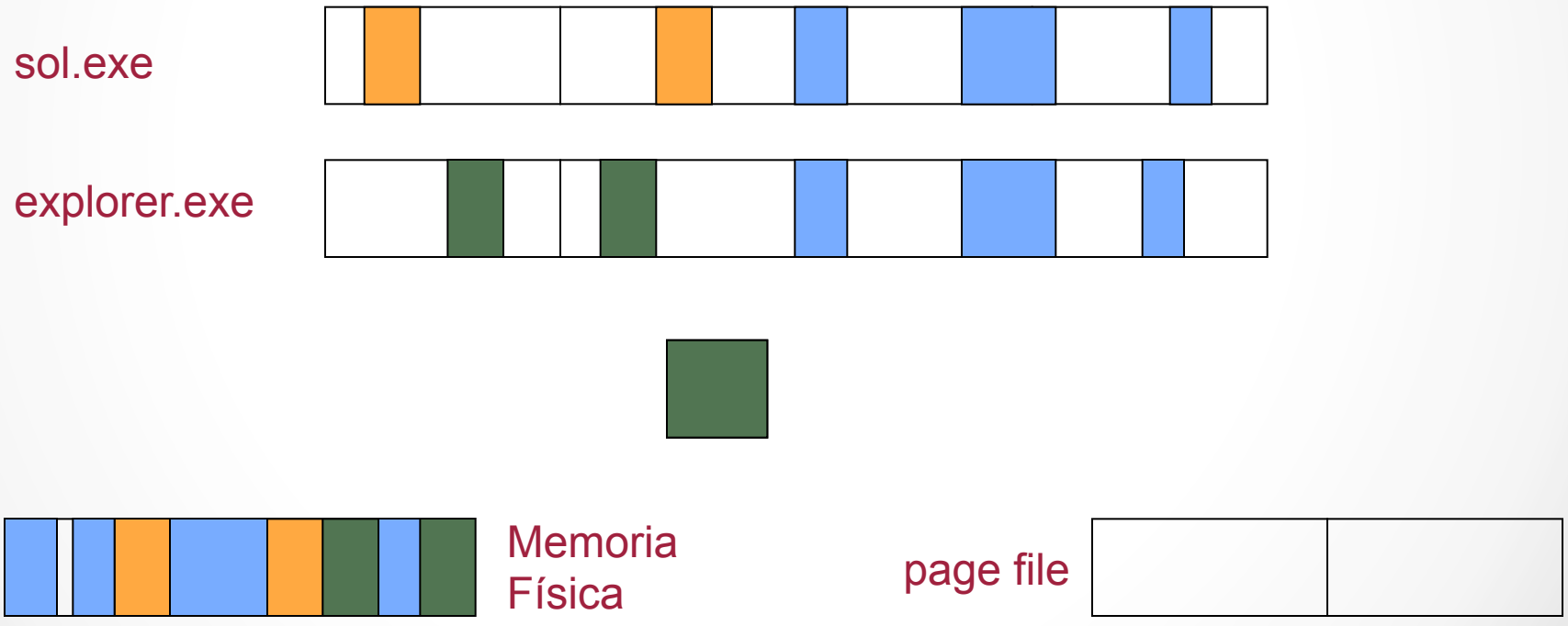


¿Qué contiene la memoria en Windows?



The Page File

Los datos se pueden mover al pagefile para liberar espacio



Pagefile.sys

- No se puede copiar directamente ya que el SO lo está "utilizando"
- Una opción es la herramienta FGET de HBGary
- FTK Imager es otra opción (pero es una GUI)

Dumping System Memory w/Software

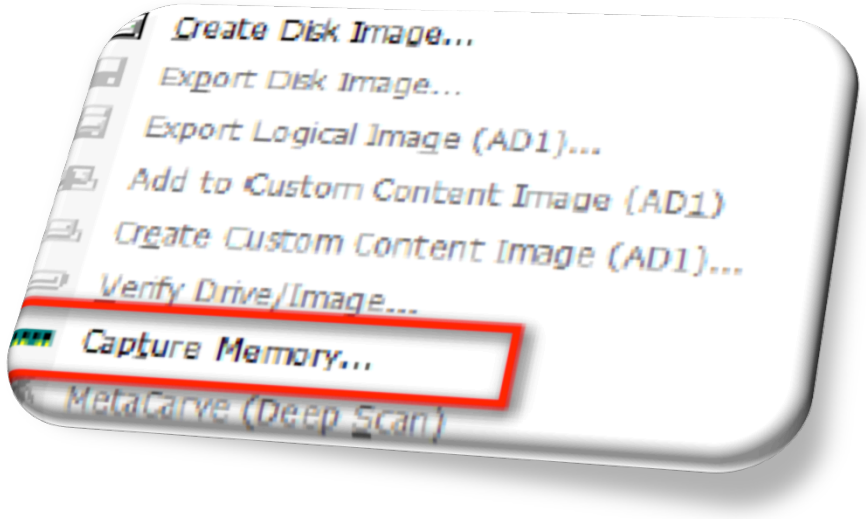
En Windows, se accede a la memoria física a través de \\.\PhysicalMemory and \\.\DebugMemory devices

Herramientas

- Moonsols/win32dd
- FTK Imager
- FD.exe (HBGary)
- KnTDD
- Encase Enterprise
- F-response

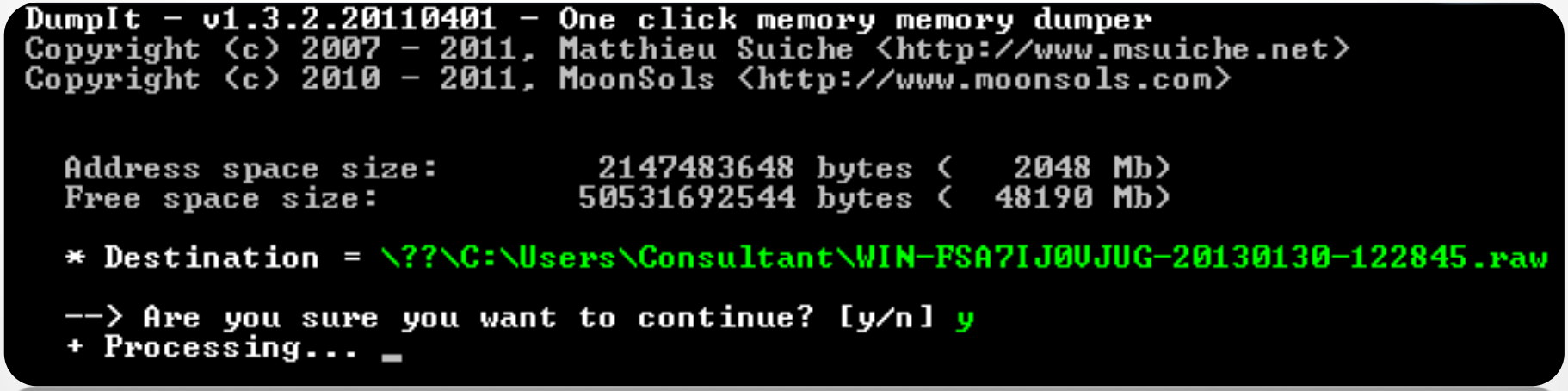
Dumping System Memory w/Software

FTK Imager: File → Capture Memory



Dumping System Memory w/Software

Moonsol's DumpIT



Dumping System Memory w/ Hardware

- Con Firewire, el OHCI controller puede leer y escribir los primeros 4 GiB de memoria
- Ver : http://www.storm.net.nz/projects/16

Analizando Dumps de Memoria

Volatility

- Advanced memory forensics framework
- Es un script en Python
- Es posible escribir plugins propios
- Varios plugins de detección de malware
- Versión 2.3.1
- Gratis!

Yara

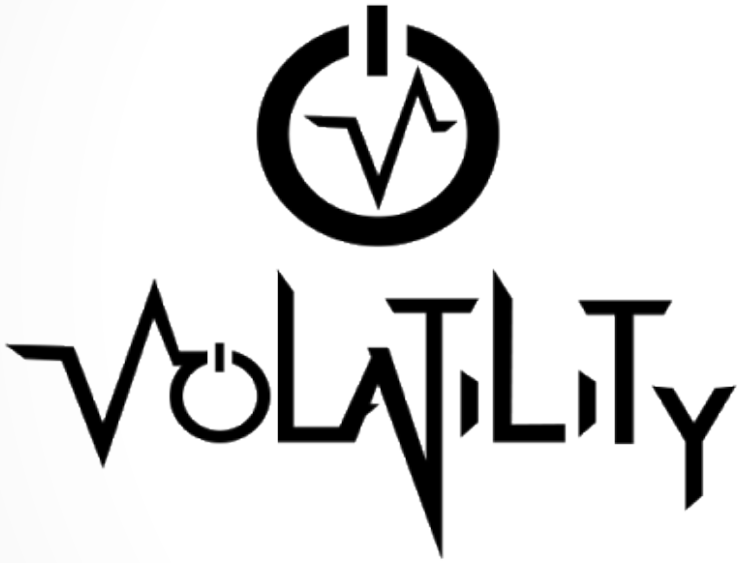
- Malware plugins para Volatility

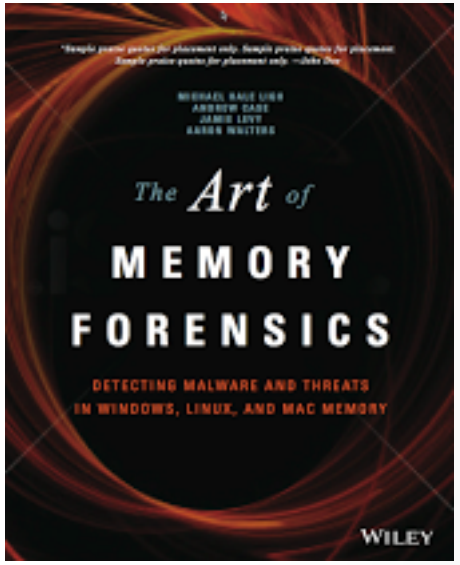
Analizando Dumps de Memoria

Plugins de Volatility para análisis de malware:

- malfind
- svcscan
- ldrmodules
- impscan
- apihooks
- idt
- gdt
- orphanthreads
- callbacks
- driverirp
- psxview

Analizando Dumps de Memoria





https://code.google.com/p/volatility/

Analizando Dumps de Memoria

Identificar imágen

Plugin: imageinfo

Identificar Procesos Sospechosos

Plugin: pslist & psscan

Identificar conexiones activas

Plugin: connections, connscan2, socks, sockscan2

Identificar archivos y dll`s sospechosas

Plugin: dlllist, files, fileobjscan

Analizando Dumps de Memoria

 # volatility pslist –f memorydump.name

Name	Pid	PPid	Thds	Hnds	Time
System	4	0	87	748	1970-01-01 00:00:00
smss.exe	528	4	3	21	2014-04-19 08:42:57
csrss.exe	584	528	13	604	2014-04-19 08:43:06
winlogon.exe	616	528	22	536	2014-04-19 08:43:13
services.exe	660	616	16	316	2014-04-19 08:43:14
lsass.exe	672	616	21	415	2014-04-19 08:43:14
svchost.exe	836	660	21	203	2014-04-19 08:43:14
explorer.exe	854	543	13	245	2014-04-19 08:43:14
svchost.exe	888	660	12	321	2014-04-19 08:43:14
lsass.exe	928	854	72	1282	2014-04-19 08:43:16
svchost.exe	1016	660	1	7	2014-04-19 07:43:16

LAB TIME!

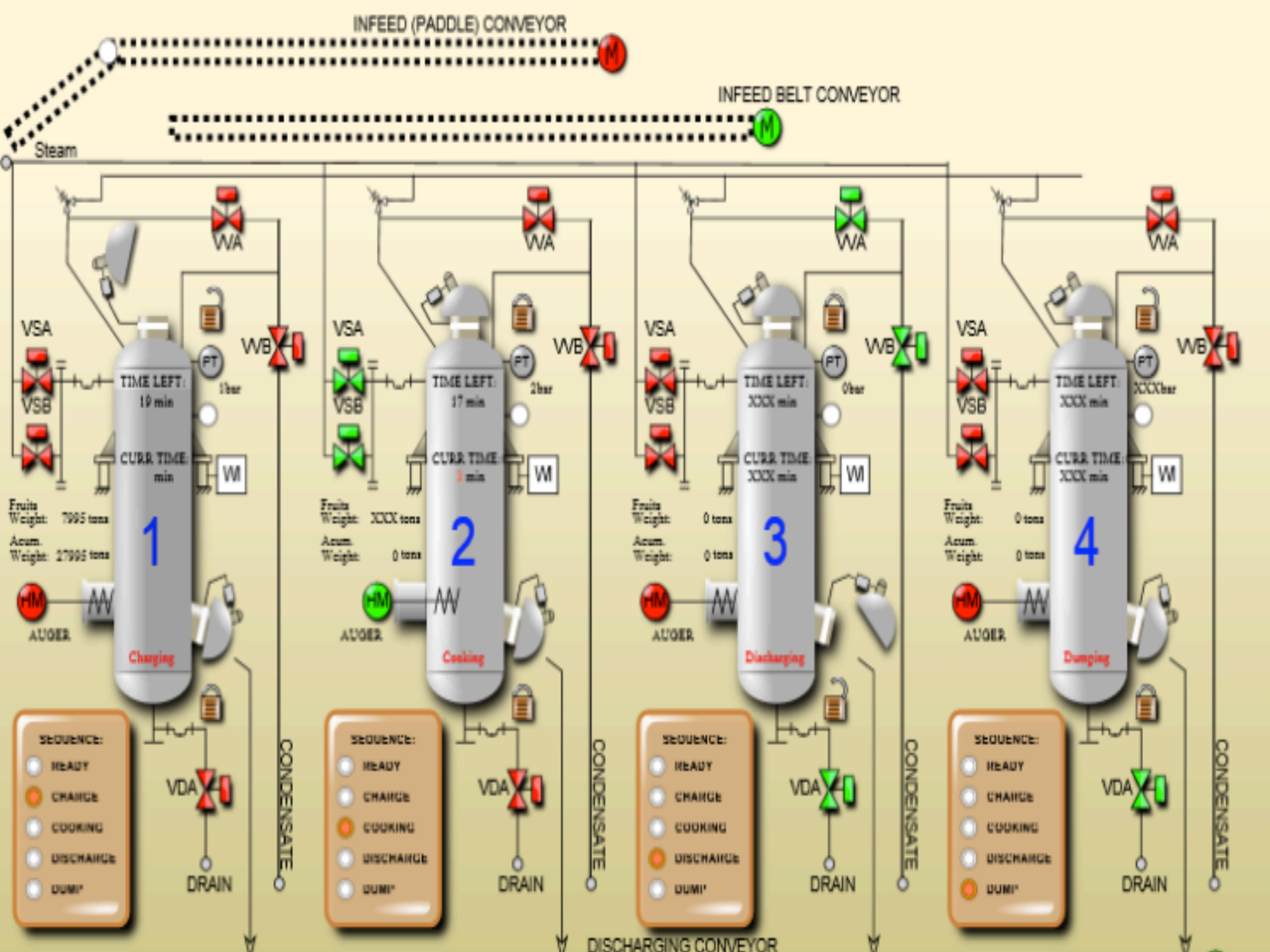
LAB TIME!

- Muchos procesos iguales (lsass.exe)
- Prioridad de Procesos
- Pocas DLLs
- Malfind Plugin
- DLLs Ocultas
- Mutex
- Nuevos Archivos
- Conexiones
- Kernel Drivers

?

Siemens' SCADA software
Siemens SIMATIC WinCC/STEP 7
CVE-2010-2772
+4 Vulnerabilidades en MS Win
14 Plantas de Enriquecimiento

STUXNET


INFEED (PADDLE) CONVEYOR
INFEED BELT CONVEYOR
Steam
WA
VSA
VSB
WB
PT
TIME LEFT:
19 min
CURR. TIME:
min
WI
Fruits Weight: 7995 tons
Acum. Weight: 27995 tons
1
HM
AUGER
Charging
SEQUENCE:
READY
CHARGE
COOKING
DISCHARGE
DUMP
VDA
DRAIN
CONDENSATE
TIME LEFT:
17 min
CURR. TIME:
min
Fruits Weight: XXX tons
Acum. Weight: 0 tons
2
Cooking
TIME LEFT:
XXX min
CURR. TIME:
XXX min
Fruits Weight: 0 tons
Acum. Weight: 0 tons
3
Discharging
TIME LEFT:
XXX min
CURR. TIME:
XXX min
Fruits Weight: 0 tons
Acum. Weight: 0 tons
4
Dumping
DISCHARGING CONVEYOR

En el Lab ni miramos…

- RPC server
- Tareas programadas
- UPX packing
- Certificados digitales falsificados…

Alerts Feed

ICS-ALERT-14-099-01C : Situational Awareness Alert for OpenSSL Vulnerability
ICS-ALERT-14-015-01 : Ecava IntegraXor Buffer Overflow Vulnerability
ICS-ALERT-13-304-01 : Nordex NC2 – Cross-Site Scripting Vulnerability
ICS-ALERT-13-259-01 : Mitsubishi MC-WorX Suite Unsecure ActiveX Control
ICS-ALERT-13-256-01 : WellinTech KingView ActiveX Vulnerabilities
ICS-ALERT-13-164-01 : Medical Devices Hard-Coded Passwords
ICS-ALERT-13-091-01 : Mitsubishi Electric Automation MX Buffer Overflow
ICS-ALERT-13-091-02 : Clorius Controls ICS SCADA Information Disclosure
ICS-ALERT-13-016-01A : Schneider Electric Product Vulnerabilities (Update A)
ICS-ALERT-13-016-02 : Offline Brute-Force Password Tool Targeting Siemens S7
ICS-ALERT-13-009-01 : Advantech WebAccess Cross-Site Scripting

http://ics-cert.us-cert.gov/alerts

ABB (Multiple, Buffer Overflow)	**Arbiter** (Denial of Service)	**C3-ILEX** (Multiple)	**EMERSON** (Buffer Overflow)
GE (Multiple)	**HONEYWELL** (Buffer Overflow)	**ICONICS** (Multiple)	**INVENSYS** (DLL Hijack, ActiveX, Buffer Overflow)
OSISOFT (Buffer Overflow)	**ROCKWELL** (Multiple PLC Vulnerabilities)	**SCHNEIDER** (Remote Auth bypass, multiple)	**SIEMENS** (XSS, Buffer Overflow)

http://ics-cert.us-cert.gov/alerts

Nombre	Fecha de alerta	Fecha de Parche	Meses
abb_1	10 oct 2011	22 feb 2012	+4
indusoft_*	27 apr 2011	16 nov 2011	+7
ifix_1	06 feb 2011	07 nov 2011	+9
rtip_1	17 oct 2011	22 aug 2012	+10
ifix_2	17 oct 2011	03 aug 2012	+10

La infraestructura crítica no puede parar
(99% de los casos)

La prioridad es la disponibilidad y timing

Existen vulnerabilidades desconocidas por los Vendors y otras (muy) conocidas

Hay que perfeccionar la respuesta ante Incidentes

Referencias:

- http://mnin.blogspot.co.uk/2011/06/examining-stuxnets-footprint-in-memory.html
- http://blogs.technet.com/b/markrussinovich/archive/2011/03/30/3416253.aspx

Muchas gracias!

Mateo Martínez
@mateomartinez1

intel Security