Data Theft

INSPIRING DATA SECURITY

David Marques
E-mail: DMarques@DRC.pt
Morada: Rua Alexandre Herculano, Edifício Central Park, 1 - Piso 7, 2795-242 Linda-a-Velha | Coordenadas GPS: 38o 43' 02.17'' N, 09o 14' 16.50'' O
Telefone: 707 200 017 | Telefone: (+351) 214 146 810 | Serviço de urgência: (+351) 964 944 112 | Fax: (+351) 214 146 819 |

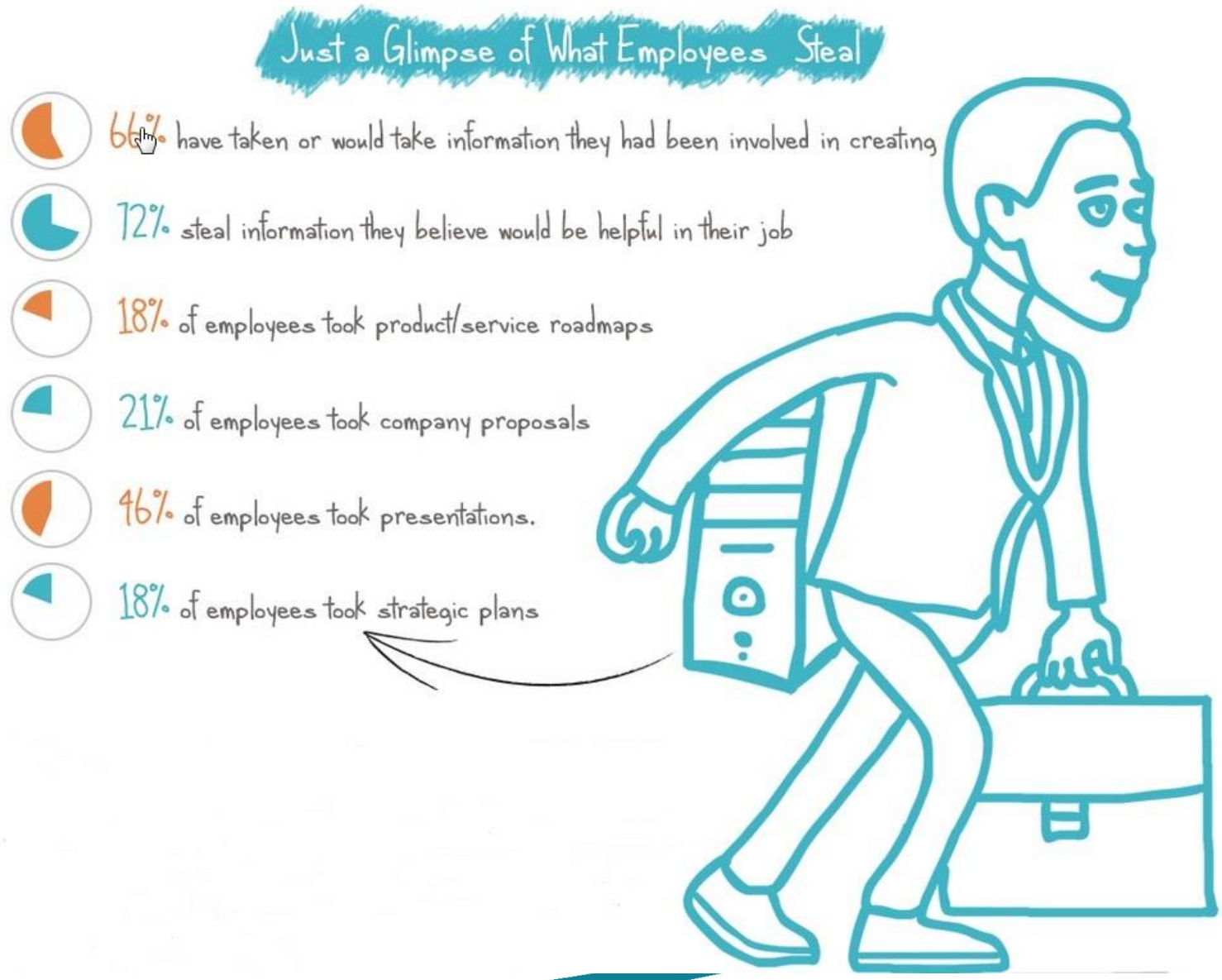
Agenda | Digital Forensics

- Intro
- Why?
- Portuguese Law
- How?
- Evidence
- Countermeasures

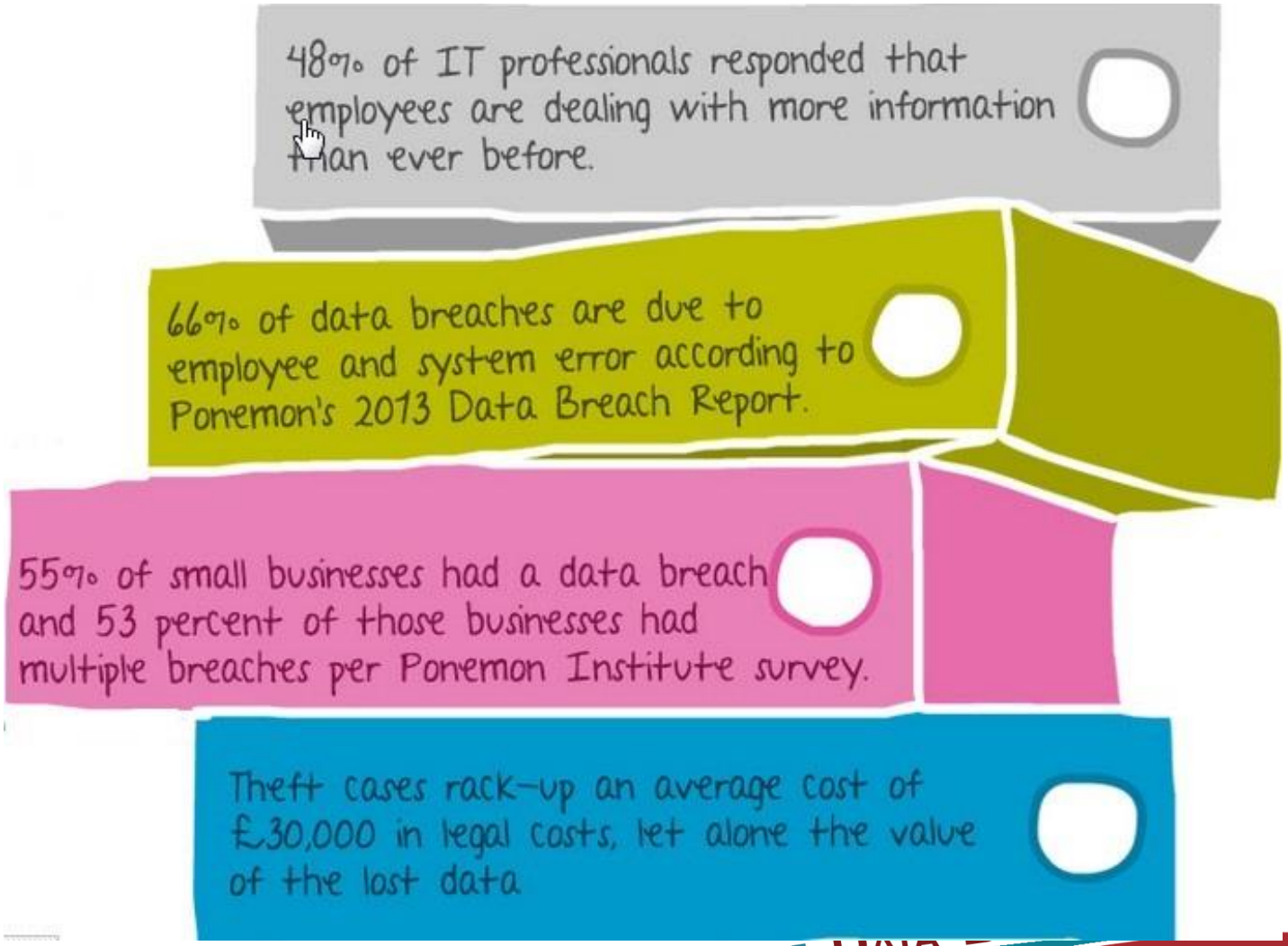
Intro

Is this a real problem?

Intro



Intro



Intro

39% of IT professionals worldwide were more concerned about the threat from their own employees than the threat from outside hackers.

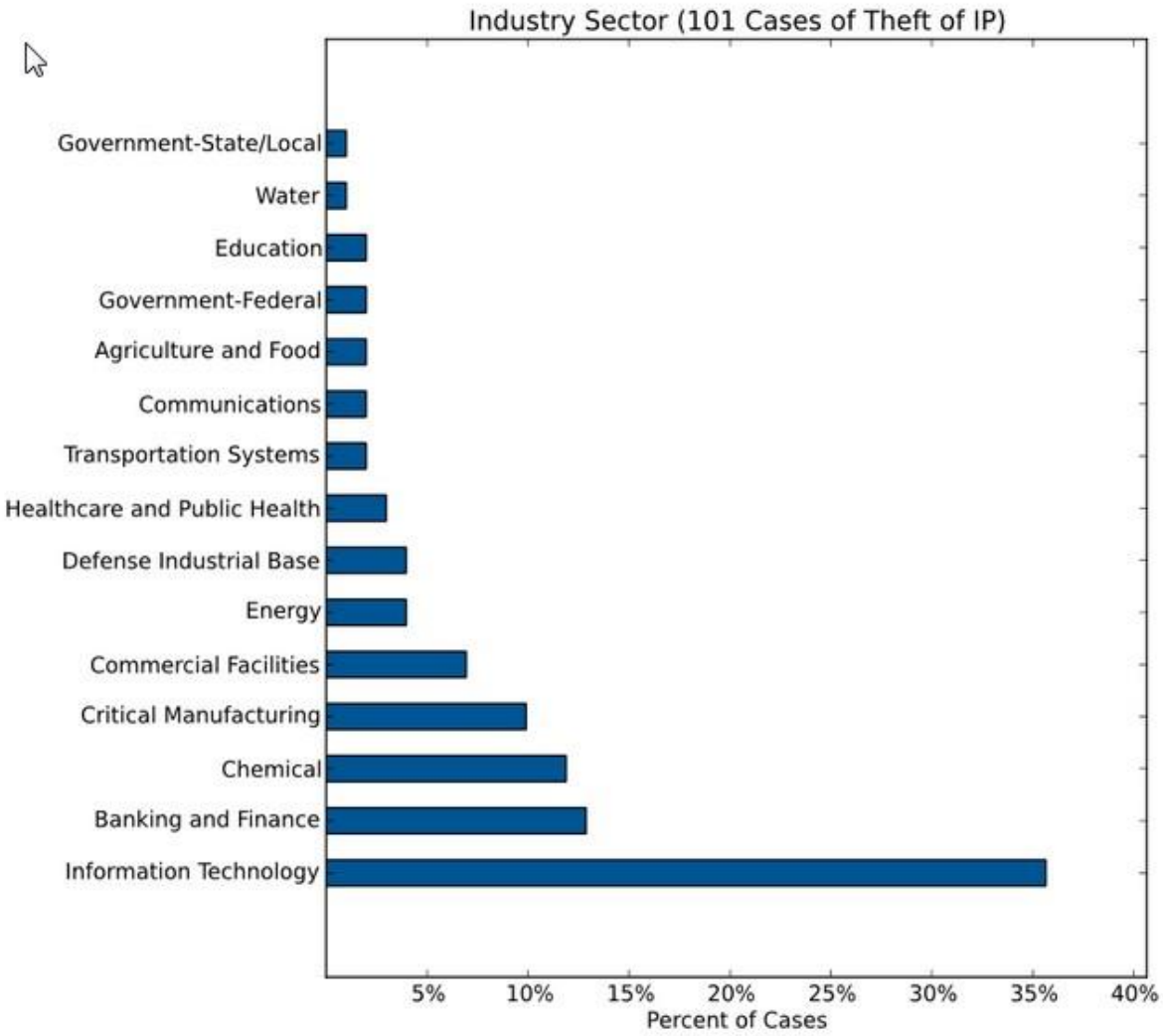
20% of IT professionals said disgruntled employees were their biggest concern in the insider threat.

Intro

2014 IT Threat Predictions

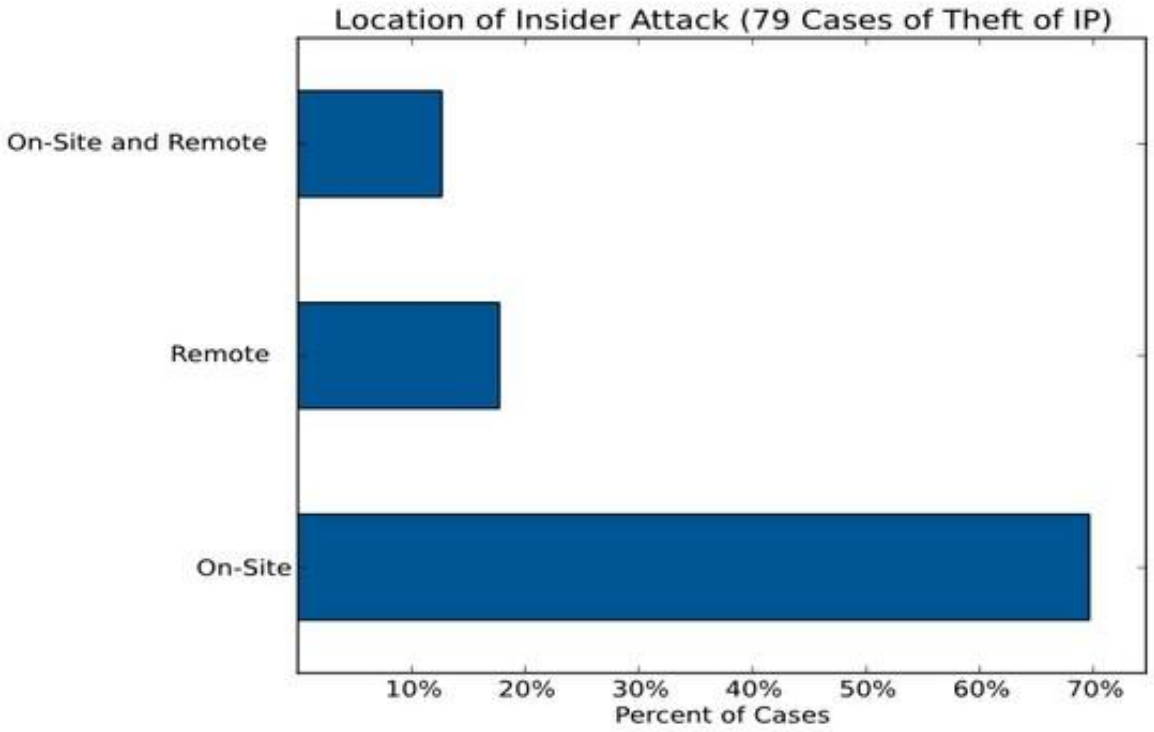
- Lower level malware will be seen as big danger, as small businesses are often not prepared and such attacks go unreported.
- Data will not just be stolen, destruction of data could play its part in 2014 as well.
- Cyber criminals in 2014 will find newer uses for tried-and-true attacks and will focus on your 'weakest' line of defense which is employees.

Intro



Source: CERT CMU

Intro



Source: CERT CMU

Intro

- Trusted business partners accounted for over 17% of attackers (i.e., 98 of the 103 cases) and former employees accounted for 21%. (Employment status was known in 100 of the 103 cases)
- Over 30% of insider theft of IP cases were detected by non-technical means, while fewer than 6% cases were detected by a software solution.
- The financial impact of these attacks is substantial. The impact was over $1,000,000 USD in 48% of cases and over $100,000 in 71% of insider theft of IP cases. (Financial impact was known in 35 of the 103 cases)

Source: CERT CMU

Why?

- It’s easy...
- Personal benefit...
- Disgruntled employees...
- Judicial System
- Lack of information classification...
- Misunderstood between what’s Intelectual Property (Company Info vs Personal Info)

Law

"Is this a Crime?"

Código do Trabalho: Artigo 128, nº1, alinea f)
"Guardar lealdade ao empregador, nomeadamente não negociando por conta própria ou alheia em concorrência com ele, nem divulgando informações referentes à sua organização, métodos de produção ou negócios."

Law

Lei do Cibercrime (Lei nº 109/2009)

Artigo 4º

Quem, sem permissão legal ou sem para tanto estar autorizado pelo proprietário, por outro titular do direito do sistema ou de parte dele, apagar, alterar, destruir, no todo ou em parte, danificar, suprimir ou tornar não utilizáveis ou não acessíveis programas ou outros dados informáticos alheios ou por qualquer forma lhes afectar a capacidade de uso, é punido com pena de prisão até 3 anos ou pena de multa.

Law

Lei do Cibercrime (Lei nº 109/2009)
Artigo 5º

Quem, sem permissão legal ou sem para tanto estar autorizado pelo proprietário, por outro titular do direito do sistema ou de parte dele, entravar, impedir, interromper ou perturbar gravemente o funcionamento de um sistema informático, através da introdução, transmissão, deterioração, danificação, alteração, apagamento, impedimento do acesso ou supressão de programas ou outros dados informáticos ou de qualquer outra forma de interferência em sistema informático, é punido com pena de prisão até 5 anos ou com pena de multa até 600 dias.

Law

Lei do Cibercrime (Lei nº 109/2009)

Artigo 6º

Quem, sem permissão legal ou sem para tanto estar autorizado pelo proprietário, por outro titular do direito do sistema ou de parte dele, de qualquer modo aceder a um sistema informático, é punido com pena de prisão até 1 ano ou com pena de multa até 120 dias.

Law

Código Penal (Crimes contra a propriedade)
Artigo 203º (Furto)

Quem, com ilegítima intenção de apropriação para si ou para outra pessoa, subtrair coisa móvel alheia, é punido com pena de prisão até 3 anos ou com pena de multa.

How?

Do you need to be a geek?

How?

Does not seem so...

How?

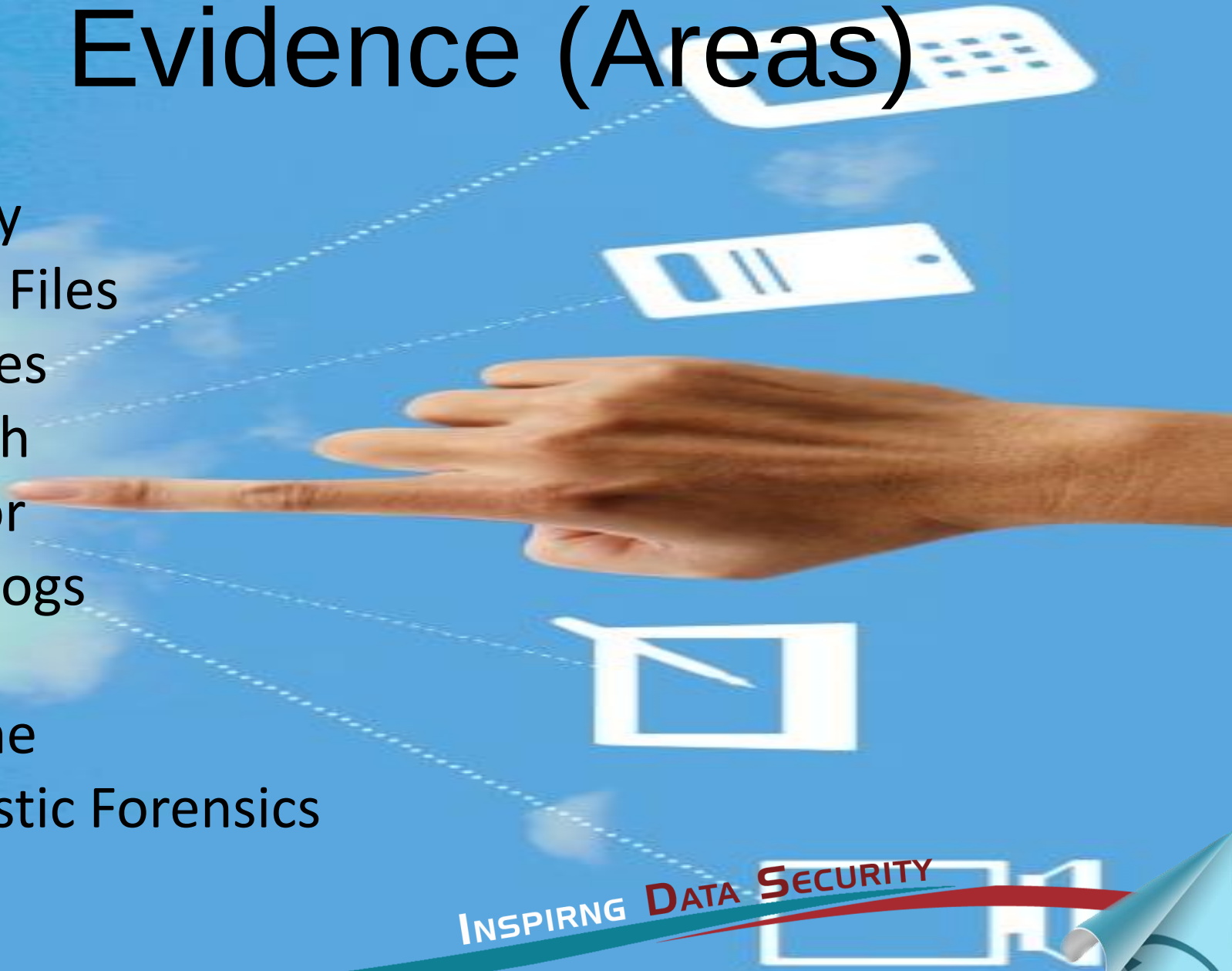
Does not seem so...

How?

Does not seem so...

Evidence (Areas)

- Registry
- Recent Files
- Link Files
- Prefetch
- USBStor
- Event Logs
- E-Mail
- Timeline
- Stochastic Forensics



Registry

Windows Registry is a hierarchical database that stores configuration settings and options on Microsoft Windows operating systems. It contains settings for low-level operating system components and for applications running on the platform that have opted to use the Registry. The kernel, device drivers, services, SAM, user interface and third party applications can all make use of the Registry. The Registry also provides a means to access counters for profiling system performance.

Registry

Root Keys

- HKEY_LOCAL_MACHINE - stores settings that are specific to the local computer.
- HKEY_CURRENT_USER - stores settings that are specific to the currently logged-in user
- HKEY_CLASSES_ROOT - contains information about registered applications, such as file associations and OLE Object Class IDs, tying them to the applications used to handle these items.
- HKEY_USERS - contains subkeys corresponding to the HKEY_CURRENT_USER keys for each user profile actively loaded on the machine

Registry

Files

Path – %SystemRoot%\System32\Config\

- Sam – HKEY_LOCAL_MACHINE\SAM
- Security – HKEY_LOCAL_MACHINE\SECURITY
- Software – HKEY_LOCAL_MACHINE\SOFTWARE
- System – HKEY_LOCAL_MACHINE\SYSTEM

Path – %USERPROFILE%\

- Ntuser.dat – HKEY_USERS\<User SID> (linked to by HKEY_CURRENT_USER)

Registry

Tools

Open Source

- Forensic Registry EDitor (fred) - "Forensic Registry EDitor (fred) is a cross-platform M$ registry hive editor" by Daniel Gillen
- libregfi - The regfi library is a read-only NT registry library which serves as the main engine behind the reglookup tool
- reglookup — "small command line utility for reading and querying Windows NT-based registries."
- regviewer — a tool for looking at the registry.
- RegRipper — "the fastest, easiest, and best tool for registry analysis in forensics examinations."
- Parse::Win32Registry Perl module.
- python-registry Python module.
- Registry Decoder offline analysis component, by Andrew Case
- RegDecoderLive live hive acquisition component, by Andrew Case
- libregf - Library and tools to access the Windows NT Registry File (REGF) format
- Registryasxml - Tool to import/export registry sections as XML
- kregedit - a KDE utility for viewing and editing registry files.
- ntreg a file system driver for linux, which understands the NT registry file format.

Commercial

- Regisry Manager
- Abexo Free Regisry Cleaner
- Auslogics Registry Defrag
- Alien Registry Viewer
- NT Registry Optimizer
- iExpert Software-Free Registry Defrag
- Registry Recon
- Registry Undelete (russian)
- Windows Registry Recovery
- Registry Tool

Recent Files

(NTUSER.DAT) Gets user's Adobe Reader cRecentFiles values

Most recent PDF opened: Sat Dec 20 13:03:15 2014 (UTC)

- c1 /C/Data/04 - Courses/Security/02 - SSL.pdf
- c10 /E/[O`Reilly] - Beautiful Code - [Oram, Wilson].pdf
- c11 /E/eBooks/kyrylkov-ms-thesis.pdf

Link Files

- Contains information about itself (names, dates)
- Contains information about the target file (names, dates)
- Can be carved from unallocated space
- Has a owner
- Contains information about volume name and path

Prefetch Files

Each time you turn on your computer, Windows keeps track of the way your computer starts and which programs you commonly open. Windows saves this information as a number of small files in the prefetch folder. The next time you turn on your computer, Windows refers to these files to help speed the start process.

Prefetch Files

Prefetch files contain the name of the executable, a Unicode list of DLLs used by that executable, a count of how many times the executable has been run, and a timestamp indicating the last time the program was run.

USBStor

5 Keys to understand USB Devices

- ***SYSTEM\CurrentControlSet\Enum\USBSTOR***

Contains Vendor, Model and SN of the USB

\ControlSet001\Enum\USBSTOR\Disk&Ven_WD&Prod_Elements_10B8&Rev_1007\575836314543335 94B4E3737&0\Properties\{a8b865dd-2e3d-4094-ad97-e593a70c75d6}\00000005

USBStor

5 Keys to understand USB Devices

- ***SYSTEM\MountedDevices***

Match SN of USB device to drive letter

USBStor

5 Keys to understand USB Devices

- ***NTUSER.dat\Software\Microsoft\Windows\CurrentVersion\Explorer\MountPoints2***
- ***Which user was logged in and active when the usb device was connected***

USBStor

5 Keys to understand USB Devices

- ***ROOT\Windows\inf\setupapi.dev.log***
- ***When the device was first connected (Local System Time, not UTC)***

Event Logs

The value os Event Logs depends a lot on which Logs are enable and if there's any retension of Logs.

- Logon / Logoff
- Object Access
- Account Management
- Application
- Etc

E-Mail

Used to send IP files to personal email

- ***E-mail clients (Outlook, etc)***
- ***Rebuild internet pages from temp files (webmail)***

Timeline

A timeline is a way of displaying a list of events in chronological order, sometimes described as a project artifact.

Timeline

User Comms	Web Based E-mail	E-mail	Calendar	Chat / Webmail Memory Artifacts	Chat and IM		
File Download	Open / Save MRU	E-mail	Skype History	Index.dat/ Places.sqlite	Downloads.sqlite		
Program Execution	UserAssist	LastVisited MRU	RunMRU Start->Run	MUI Cache	Win7 Jump Lists	Prefetch	Services (EVT)
File Opening/ Creation	Recent Files	Office Recent Files	Shell bags	Link Files	Jump Lists	Prefetch	Index.dat file://
Deleted File or File Knowledge	XP Search - ACMRU	Win7 Search – WordWheelQuery	Last Visited MRU	Thumbs.db	Vista/Win7 Thumbnails	Recycle Bin	Browser Artifacts
Physical Location	Timezone	Wireless SSID	VISTA/Win7 Network History	Cookies	Browser Search Terms		
USB Key Usage	Key Identification	First/ Last Times	User	Volume Name	Drive Letter	Link Files	P&P Event Log
Account Usage (SAM)	Last Login	Last Failed Login	Last Password Change	Group Membership			
Account Usage (EVT)	Success / Fail Logons	Logon Types	RDP Usage	Account Logon/ Authentication	Rogue Local Accounts		
Browser Usage	History	Cookies	Cache	Session Restore	Flash & Super Cookies	Suggested Sites	Memory Fragments of Private Browsing

Timeline

date	time	MACB	sourcetype	type	short
39649	0.06115	MACB	Email PST	Email Read	Message 114: Attachment m57biz.xls Opened
7/20/2008	1:27:40	MACB	XP Prefetch	Last run	EXCEL.EXE-1C75F8D6.pf: EXCEL.EXE was executed
7/20/2008	1:27:40	.AC.	NTFS $MFT	$SI [.AC.] time	C:/Program Files/Microsoft Office/Office/EXCEL.EXE
7/20/2008	1:27:40	.AC.	UserAssist key	Time of Launch	UEME_RUNPATH:C:/PROGRA~1/MICROS~2/Office/EXCEL.EXE
7/20/2008	1:28:03	..CB	Shortcut LNK	Created	C:/Documents and Settings/Jean/Desktop/m57biz.xls
7/20/2008	1:28:043	MACB	NTFS $MFT	$SI [MACB] time	C:/Documents and Settings/Jean/Application Data/Microsoft/Office/Recent/Desktop.LNK
7/20/2008	1:28:03	MACB	FileExts key	Extension Change	File extension .xls opened by EXCEL.EXE
7/20/2008	1:28:03	MACB	NTFS $MFT	$SI [MACB] time	C:/windows/system32/winsvchost.exe
7/20/2008	1:28:03		SOFTWARE key	Last Written	SOFTWARE\Microsoft\Windows\CurrentVersion\Run
7/20/2008	1:27:40		Memory Process	Process Started	winsvchost.exe|1556|1032||0x02476768
7/20/2008	1:27:40		Memory Socket	Socket Opened	4|134.182.111.82:443|Protocol: 6 (TCP)|0x8162de98|||
7/20/2008	1:27:40		XP Prefetch	Last run	WINSVCHOST.EXE-1C75F8D6.pf: EXCEL.EXE was executed
7/20/2008	1:28:03	..CB	Shortcut LNK	Created	C:/Documents and Settings/Jean/Desktop/m57biz.xls
7/20/2008	1:28:03	.A..	Shortcut LNK	Access	C:/Documents and Settings/Jean/Desktop/m57biz.xls
7/20/2008	1:28:04	MAC.	NTFS $MFT	$SI [MAC.] time	C:/Documents and Settings/Jean/Application Data/Microsoft/Office/Recent/m57biz.LNK
7/20/2008	1:28:04	..C.	NTFS $MFT	$SI [..C.] time	C:/Documents and Settings/Jean/Local Settings/History/History.IE5/MSHist012008072020080
7/20/2008	1:28:04	..C.	NTFS $MFT	$SI [..C.] time	C:/Documents and Settings/Jean/Local Settings/History/History.IE5/MSHist012008072020080
7/20/2008	1:28:04	MACB	RecentDocs key	File opened	Recently opened file of extension: .xls - value: m57biz.xls

Stochastic Forensics

Stochastic forensics is a method to forensically reconstruct digital activity lacking artifacts, by analyzing emergent properties resulting from the stochastic nature of modern computers.

Stochastic Forensics

The statistical distribution of file systems metadata is affected by such large scale copying. By analyzing this distribution, stochastic forensics is able to identify and examine such data theft. Typical file systems have a heavy tailed distribution of file access. Copying in bulk disturbs this pattern, and is consequently detectable.

Countermeasures

- **Human Resources Motivation**
- **DLP (Data Loss Prevention)**
- **Logs**
- **Security Policies**
- **Audits**

Q & A

Thanks!

David Marques

dmarques@drc.pt

www.drc.pt

INSPIRNG DATA SECURITY