



CSIRT, Cyber Extortion DDoS Attacks & Forensics

John Walker
SBLTD

Nottingham Trent University

Session ID: HT-210

Session Classification: Intermediate

RSACONFERENCE
EUROPE 2012

Introduction - Employment

- Royal Air Force



- RAF Newton, Laarbruch, ASU Wittering, HQP&SS (Germany), HQP&SS (SR), Falklands, Marham, Newton, 399SU, JARIC – working within Investigations, Sigint, Comint, & Talent Keyhole (TK) Compartments

- Logica - BAe
- General Motors
- Experian
- Contracts for various Clients



Introduction - 2

- Worked in both Public and Private Sectors
- Military/Intelligence background of 20+ years
- Police background – PACE, Investigations
- Expert Witness support for Clients
- Covert & Overt operations
- Commercial Investigations
- Originated Forensics Course for NTU
- Delivered CSIRT, & First Responder Forensics



Landscape - CrimeWare Campaign

RSA Warns of New Attacks September 2012
(Tracy Kitten reporting).

Underground CrimeWare Campaign Plan's 'Substantial' Attack!

<http://ffiec.bankinfosecurity.com/interviews/rsa-warns-new-attacks-on-banks-i-1681>

October 12: Anonymous takes down multiple Swedish government sites in massive DDoS attack!



The Onslaught of the Cyber Threat



***William Hague* – September 2012:**

“Cybercrime is one of the greatest global and strategic challenges of our time.”

"It has never been easier to become a cyber criminal. today, such attacks are crisscrossing the globe from north to south and east to west - in all directions, recognising no borders, with all countries in the firing line."



Scott McNealy - 1999

In 1999 Scott McNealy (then CEO of Sun) was criticised for saying:

‘Today, people have less privacy online than ever’

Looking back at past events & predictions of the future, may one conclude this to be equally applicable to **Security** in 2012?



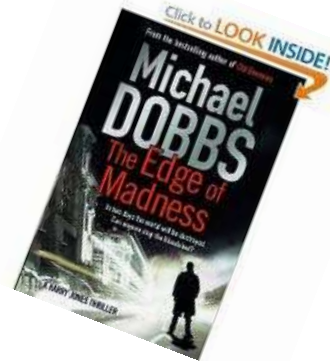
Declaration of CyberWar (CyberConflict)

Unrestricted Warfare: Qiao Liang, Wang Xiangsui

Beijing: PLA Literature & Arts Publishing House, February 1999

‘The great masters of warfare techniques during the 21 st century will be those who employ innovative methods to recombine various capabilities so as to attain tactical, campaign & strategic goals’

Yier Tierfude



Tit-for-Tat of CyberWar/CyberConflict

Iran has tightened Cyber Security since impact in 2010 by Stuxnet Worm, which Tehran believes was planted by their arch-adversaries – *whoever they may be?*

September 12 - Iran: Attack against infrastructure & communications companies – forcing limited Internet.

Mehdi Akhavan Behabadi, Secretary of the High Council of Cyberspace.



Confusion of Objectives

For *laudable* reasons, PCI-DSS, and other related Standards evolved, to drive *Governance, Compliance, & Security*. They are tools to provide visibility, and drive to assure the business is doing the right thing.

However, there have been [*are*] occasions where, for example, *security* has suffered reduction of resource in order to satisfy a 'Tick-in-the-Box', Dashboard orientated compensatory controls, without necessarily interfacing, communicating, or addressing the sub-technological control(s).



State of Denial

A state of denial has existed for years:

- The **Computer Virus** posed no threat!
- The **Computer Worm** was not possible!
- **SPAM** was not to be considered as dangerous!
- **Cell Phone Security** was not a security issue! (*CSA Report 2012*)
- **Computer Crime** was declining!
- The computer can't be used as a **weapon**!
- **CyberWar/CyberConflict** is a product of imagination!
- The National Infrastructure is **immune** from Compromise!
- The good-guys are **winning** the battle against Cyber Crime/Attacks



External Actors

- Clearly Hackers
- Serious-and-Organized-Crime
- Drive-by-Hackers
- Hacktivists
- Individuals
- State Sponsored Activities
- The *Collusionist*
- Industrial Espionage
- Cyber Radicals



What do they look like?



Cloud & Outsourcing

Many opportunities, but poor *T&C's* of engagement can, and have caused exposure to a number of organisations.

As in the **Cuckoos Egg**, Third Parties were the key to unauthorised incursion – nothing has really changed in the last 20 years!



The Internal Threat

Threats can arrive in many forms. However, based on some real-time, *real-world* observations, one big area of potential exposure is that of bad security practices and skills within the area of Operational Security, and at times higher levels of Security Management where there may be *disjoint* between the levels of understanding between *soft*, to *technological* security.

*A Journalist friend of mine asked a set of International Hackers about their high levels of Cyber Skills that they possessed & used to compromise targets – their response was ‘**it is more a case of the targets insecurity being the point of leverage**’*

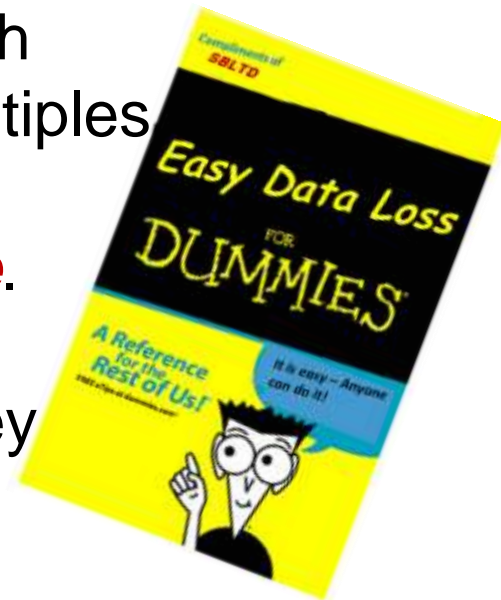


Real-Time Case History - 1 - DLP

Company 'A' - an organisation residing in a very sensitive commercial business environment, storing high volumes of user credentials, & processing multiples of financial transactions via card & account transactions – **with a history of compromise.**

To accommodate protection to their assets they made considerable investment in DLP.

Testing was conducted, & located 22 exposures, ranging from promiscuous protocols, privilege management, through to poor Workstation configurations – this DLP was *totally* ineffective



Real-Time Case History - 2 - Trust

In this case we consider the level of ultimate trust with post & appointments like the **CISO**. In Case No 2, we have a set of events which saw the appointed *professional* fall into dispute with the Executive.

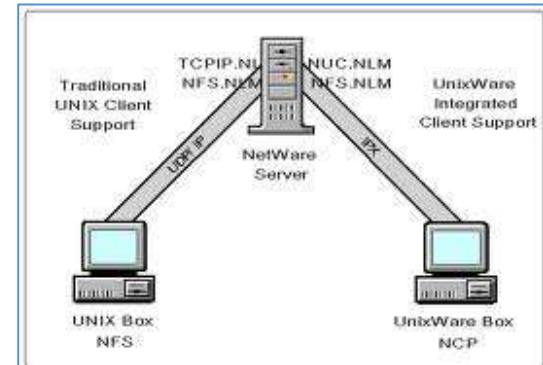
Within hours of a top floor meeting our CISO had visited the local computer outlet, and then busily started to download files from the company LAN!

A true case of concern for the impacted business, as well as the Profession in relation to Ethics – They remained in post!



Real-Time Case History - 3 - SAMBA /Cloud

An interesting, long-standing Exposure. Notwithstanding Company 'B' conducted ongoing Pen Testing over years, it was never identified that the majority of **PCI-DSS** transactions, data, & other sensitive assets were on, and passing over an Insecure **SAMBA Share**!



And it was never appreciated that **PCI** assets, & other sensitive data had been subject to **unauthorised migration** into an **insecure, unencrypted Cloud**, mixed in with other **collocated** organisations data!



Real-Time Case History - 4 - Printers

This organisation invested considerable investment to secure their Classified Assets, and deployed virtualised systems – wish, no data-assets on the shop floor – problem was, they overlooked the MFD!

The MFD (Multi Functional Device) – not just a printer, but a Computer, **Print Server**, **IP addressable** device, along with its **Hard Drive** of **300 gb** +, and with no **Physical Security** – how do they fit in with, say, a Secured **CITRIX** Deployment?



Real-Time Case History - 5 - MetaData

Major branded organisation engaged with massive UK Project, supporting *Commercial, Government, & Public* interests, suffering *significant exposure* from inadvertent publication of Metadata – notwithstanding they are located in the *security* arena, even *post* awareness, nothing changed, & still suffer exposure four months on!!



Leaking masses of data – Email addresses, machine information, IP addresses, Document Paths, Logon ID and much more.....



Real-Time Case History - 6 - The Euro MP

Euro MP Compromised:

- Computer
- Cell Phone
- Environment (Spectrum)

Solution:

- Spectrum Analysis
- Logical Investigations
- Disinformation



Advanced Threats

Considering the consequence of existing exposures within any environment, one must consider what the implications of the **advanced threats** in the form of **Active Persistent Threats (APT)** A subject of discussion by Kaspersky in 2012, & the **Advanced Evasion Techniques (AET)**, a threat researched by StoneSoft in 2010.

But this is nothing new, as the Concept has been around Since VB93 ----->



In this case, the threat posed by ‘Encapsulated Packets’



What is Classified as an AET?

Under the Research Banner of the **NTU School of Computing & Informatics**, researching *trends*, recent security incursions, & attacks targeting top brand organisations, it may be inferred that some form of Advanced threat, like the **AET** does exist, but it does not have a single *identity, look or feel*, or a *static-profile*, which may be defined as:

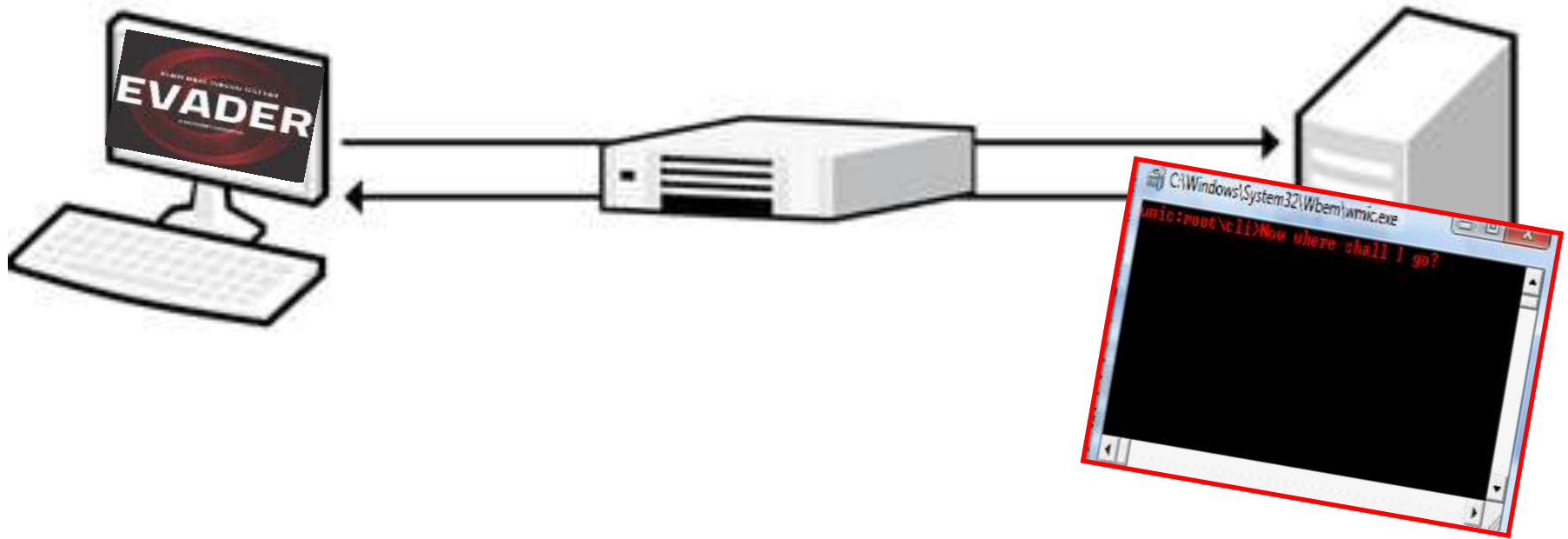
‘Mechanisms by which known attack conditions are subjected to an altered profile, to cloak their recognised signature, or condition from external and/or internal protective-security devices & applications, in order to circumvent detection.

In other words, it is feasible that a security device accommodated with the *latest detection signature* for a *known* condition—say, **Conficker**—may be considered up-to-date, even though the known malicious condition(s) may circumvent their protection capabilities.



Attacks in Action

Having witnessed the concept of evading up-to-date fully patched Firewalls, the research was conclusive as to the potential threat.



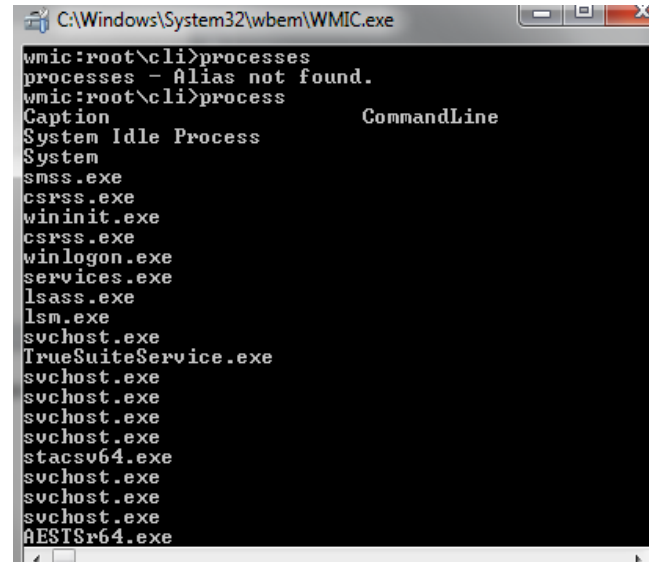
Exposed Points of Leverage - 1

Once compromised by an attack
It is a matter of finding out just how
much the internal users are trusted.

wmic:root\cli>

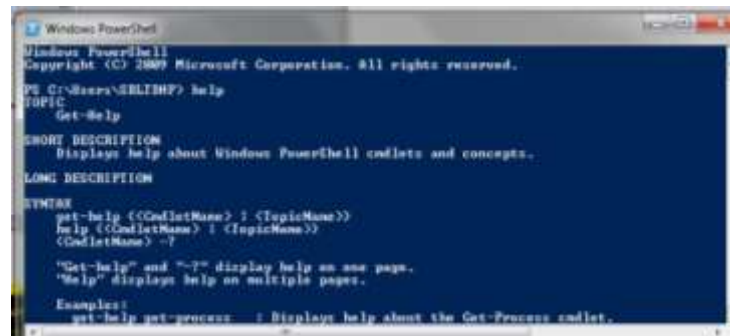
Ask the System – are you listening:

**Confidential
Secret
Client in Confidence**



```
C:\Windows\System32\wbem\WMI.exe
wmic:root\cli>processes
processes - Alias not found.
wmic:root\cli>process
Caption                               CommandLine
System Idle Process
System
smss.exe
csrss.exe
wininit.exe
csrss.exe
winlogon.exe
services.exe
lsass.exe
lsm.exe
svchost.exe
TrueSuiteService.exe
svchost.exe
svchost.exe
svchost.exe
svchost.exe
stacsu64.exe
svchost.exe
svchost.exe
svchost.exe
svchost.exe
AESTSr64.exe
```

powershell



```
Windows PowerShell
Microsoft PowerShell
Copyright (C) 2009 Microsoft Corporation. All rights reserved.
PS C:\Users\BLENTH> help
TOPIC
    Get-Help
SHORT DESCRIPTION
    Displays help about Windows PowerShell cmdlets and concepts.
LONG DESCRIPTION
SYNTAX
    get-help ((Get-ListName) | <TopicName>)
    help ((Get-ListName) | <TopicName>)
    <Get-ListName> -?
"Get-help" and "??" display help on one page.
"help" displays help on multiple pages.
Examples
    get-help get-process -? Displays help about the Get-Process cmdlet.
```



Exposed Points of Leverage - 2

The HP Smart Server, a useful piece of technology – use with a **Dynamic URL** and here is one useful appliance to park data.



SharePoint On-Line



Or:

Tonido Plug



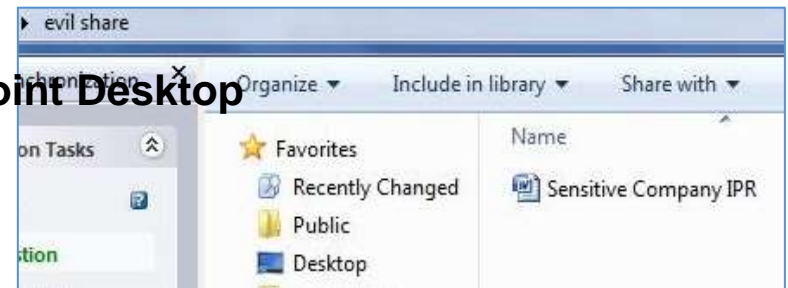
DropBox



Office 2010



SharePoint Desktop



PogoPlug

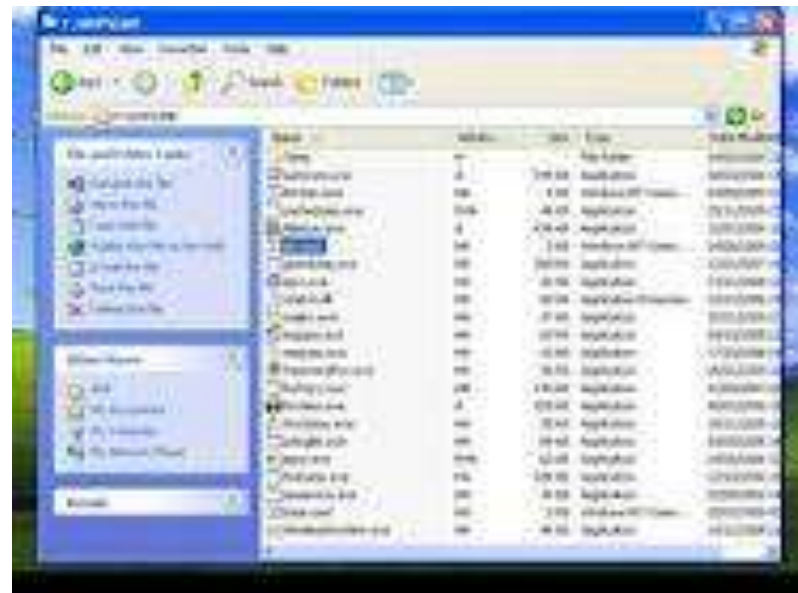


Exposed Points of Leverage - 3

A mass of powerful tools available to track & compromise systems & applications through interfaces – easy to obtain, and very easy to use.

Or obtain them as CaaS – CrimeWare-as-a-Service.

Or deliver to target via Social Engineering.



And credit to Rik Fergusons excellent Trend Micro Video on the web



Smart Malware - Duqu!

Malware is becoming *smarter, evasive, and targeting.*

Remember the **DroneBug!**



Jumping a ride with classified systems Was this 'Duqu'

*No matter, the security ramifications of any malicious code in such sensitive environments, where they may monitor conversations, catch coordinates, or access, what is referred to as **Ephemeris Data** is significant to National & International Security!*



Cyber Extortion

Comment: ?????? down most of the afternoon which doesn't bode well for Cheltenham. I believe they are under some sort of Cyber Attack and this is probably an attempt to extort money from them - probably a **DDoS** attack.

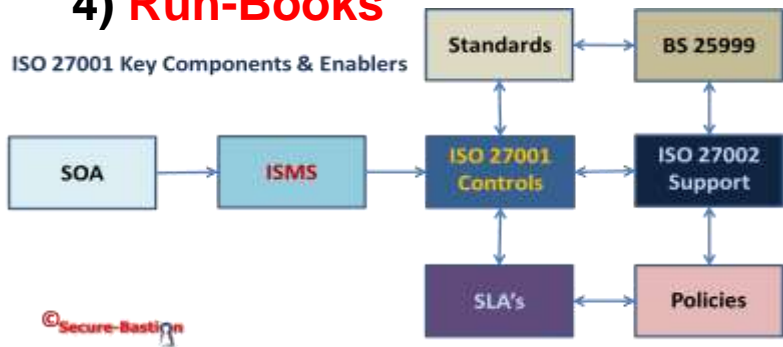
The reason it hasn't been publicised, I believe is because it would cause fear among the clients. An example



The CSIRT

When an incident impacts, no matter in what guise it arrives, this is *not* the time to be unprepared, doing the *Headless Chicken Dance*.

- 1) Policies
- 2) Procedures
- 3) TOR's
- 4) Run-Books

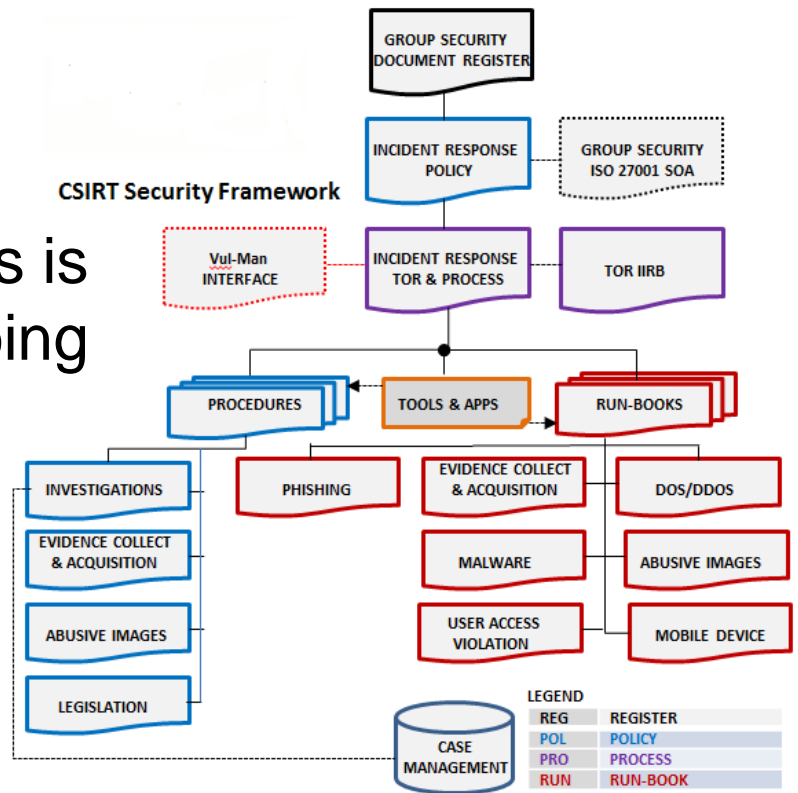


5) Case Management Systems

6) Reporting

7) End-to-End, Cross Site Ownership

8) Event After Care



The Pragmatics of Cyber Forensics

With current levels of *acknowledged* Cyber Crime, & Adversity
It is essential to have ***First Responder Capabilities*** to react &
engage with any *actual, suspected, or inferred* event(s), or
security incident(s).

Operational Underpin:

- *Policies*
- *Process*
- *Training*
- *Tools*
- *Information*
- *Communications*



Differing Levels of Robustness

Cases will differ, with some dictating more ***procedural, formalised rigour*** than others.

commission	17/05/2012 16:34	File folder	
Leads	17/05/2012 16:34	File folder	
Legal	17/05/2012 16:34	File folder	
MASTER SALES 2	17/05/2012 16:34	File folder	
Mon meeting	17/05/2012 16:34	File folder	
New Folder	17/05/2012 16:34	File folder	
new xxxxx world	17/05/2012 16:34	File folder	
!Fw_ showcase of email software	17/05/2012 16:35	E-mail Message	8 KB
1 personal sales plans & comm Debbie	11/07/2006 16:48	Microsoft Excel 97...	38 KB
1 Roy personal sales plans & comm	11/07/2006 15:41	Microsoft Excel 97...	47 KB
3 yr growth plan-	05/07/2006 14:12	Microsoft Excel 97...	481 KB
360 Degree Feedback Tool - MKS Man...	05/07/2006 07:57	Microsoft Word 9...	52 KB
Bex_F1_car	14/08/2006 12:34	JPG File	1,208 KB
Chris XXXXXX visit to XXXXXX itinerar...	31/07/2006 17:21	Microsoft Word 9...	20 KB
Detailed marketing budget DS	28/06/2006 08:31	Microsoft Excel 97...	39 KB
Existing 20056 fwd liability	11/07/2006 07:44	Microsoft Excel 97...	144 KB
Forum Banner_Des 4	31/05/2006 08:10	Shockwave Flash ...	28 KB
Fw_ [CM] Re_ Your invitation to the la...	17/05/2012 16:35	E-mail Message	5 KB
Fw_ [CM] Re_ Your invitation to the la...	17/05/2012 16:35	E-mail Message	2 KB
install_flash_player	31/05/2006 08:43	Application	931 KB
Jude c d	17/05/2012 16:35	E-mail Message	109 KB



First Responders - FRAT.BAT



```
C:\Windows\system32\cmd.exe

FRAT
NT/XP/VISTA/Win7
Forensic First Responder Assessment Tool
For Automated Forensic Acquisition of Network and
Local System Data and Electronic Artifacts
John Walker - SBLTD
Wilsthorpe Road, Breaston, Derbyshire
E-mail: sbltd@sbltd.onmicrosoft.com

Mob: 0788 1625 140
Tel: 0870 3929198
Version 3.1 Update - 18 Sep 2012
Mod F - SBLTD

Please wait whilst your system is checked

To TERMINATE - PRESS CTRL+C

Press any key to continue . . . .
```



FRAT Reporting

Automated generation of reports, written directly you the USB Path.

Range from 10 to 100+ pages of output.

```
File Edit Format View Help
Folder PATH listing
Volume serial number is 0013F8D8 9A66:25CC
I:.
AAAATools
    AAAAPS
    AAAAmd5
ACCOUNTS
Force user logoff how long after time expires?:      Never
Minimum password age (days):                        0
Maximum password age (days):                        120
Minimum password length:                             8
Length of password history maintained:               10
Lockout threshold:                                   6
Lockout duration (minutes):                          60
Lockout observation window (minutes):                5
Computer role:                                       WORKSTATION
The command completed successfully.

SERVER CONFIGURATION
WORKSTATION CONFIGURATION
Computer name                                         \\xxxxxxxxx\F4J
Full Computer name                                   xxxxxxxxxxxx\F4J.xxxxxxxx.uk
User name                                             xxxxxxxxxxxx

Workstation active on
```

If you are interested in a copy, just ask



Cyber Forensics - Documents - 1

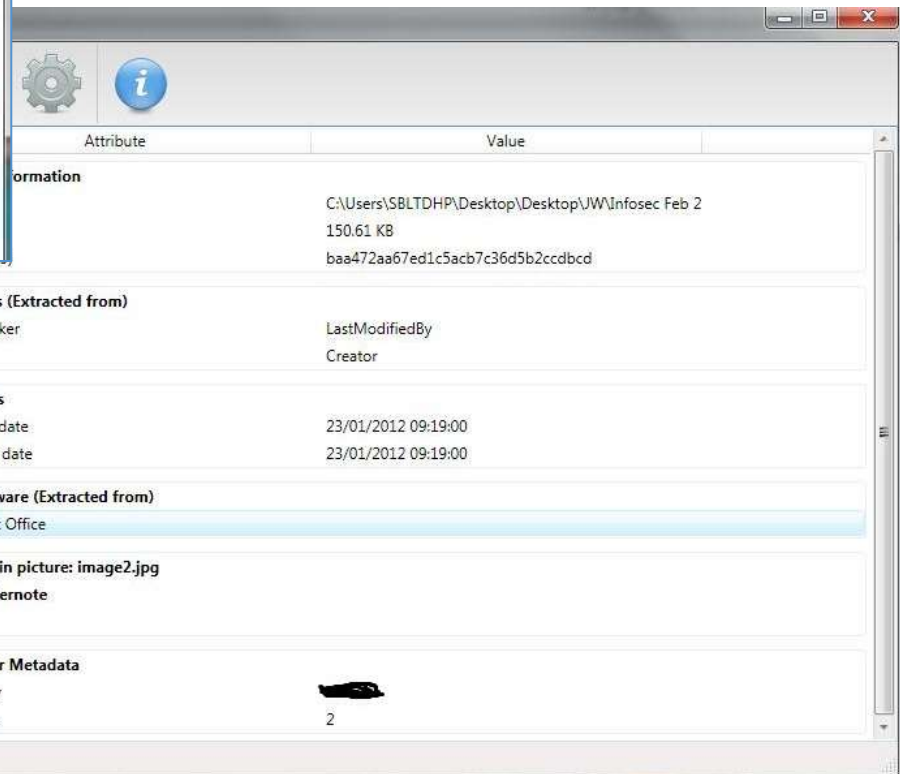


Low cost, easy to use tools to support teams of varying levels of skill



Cyber Forensics - Documents - 2

MetaData can be a rich discovery in any Investigation.

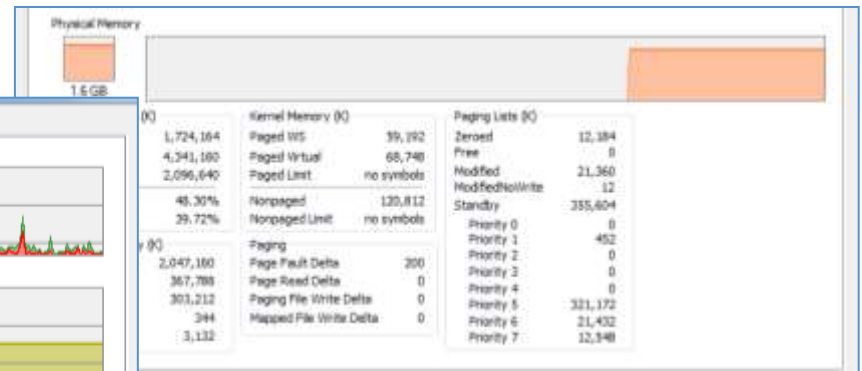
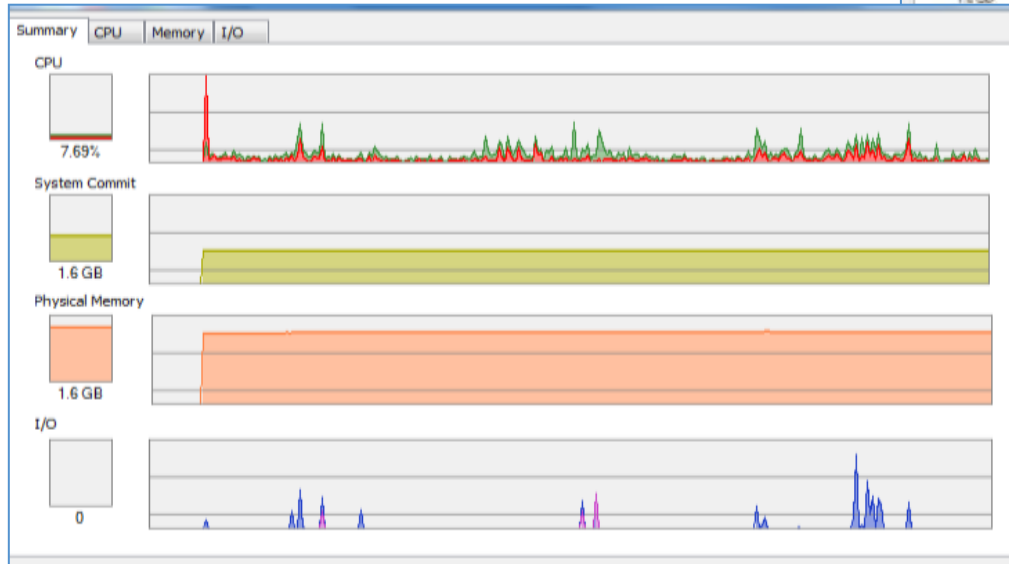


It can also be a great asset for any attacker who may be 'Footprinting' a target.



Process Exploration

Immediate Visibility of System



Behaviours
Resource
Malware Activity etc

www Sysinternals: www.sysinternals.com [PARLIAMENT\walkerjb]

Process Find Users Help

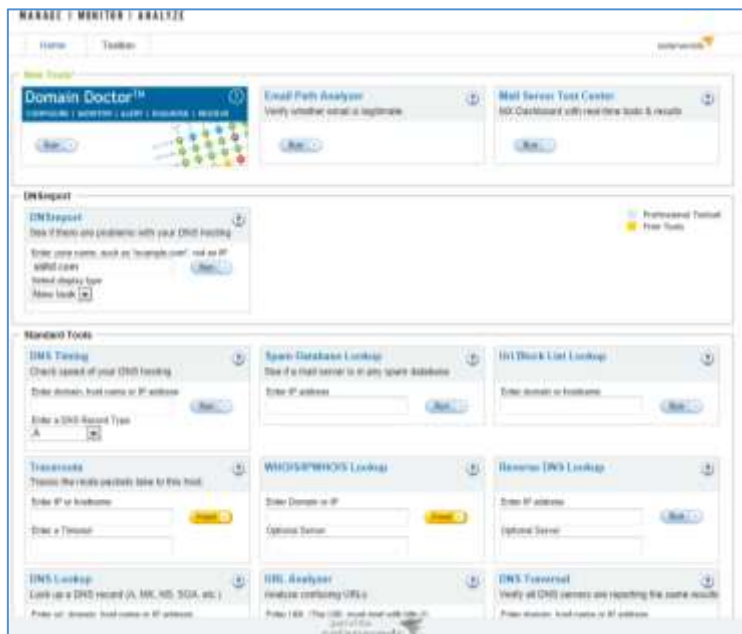
	PID	CPU	Private Bytes	Working Set	Description	Company Name
...	1836		2,112 K	3,196 K		
...	2008		352 K	1,456 K		
...	352		1,848 K	4,384 K		
...	2068		2,700 K	4,632 K		
...	2096		30,468 K	20,596 K		
PretorClient.exe	2596		2,164 K	1,644 K	PretorClient MFC Application	
...	2224		1,132 K	2,648 K		
...	2240		3,840 K	4,224 K		
...	2260		8,364 K	5,312 K		
...	2356		1,768 K	1,628 K		



DNS Tracing



Investigations involving remote site activity will require Triage to follow-up discoveries – **DNSstuff** is a quick & easy tool to use.



Overall Results: **2** FAIL **3** WARNING **27** PASS **4** INFO

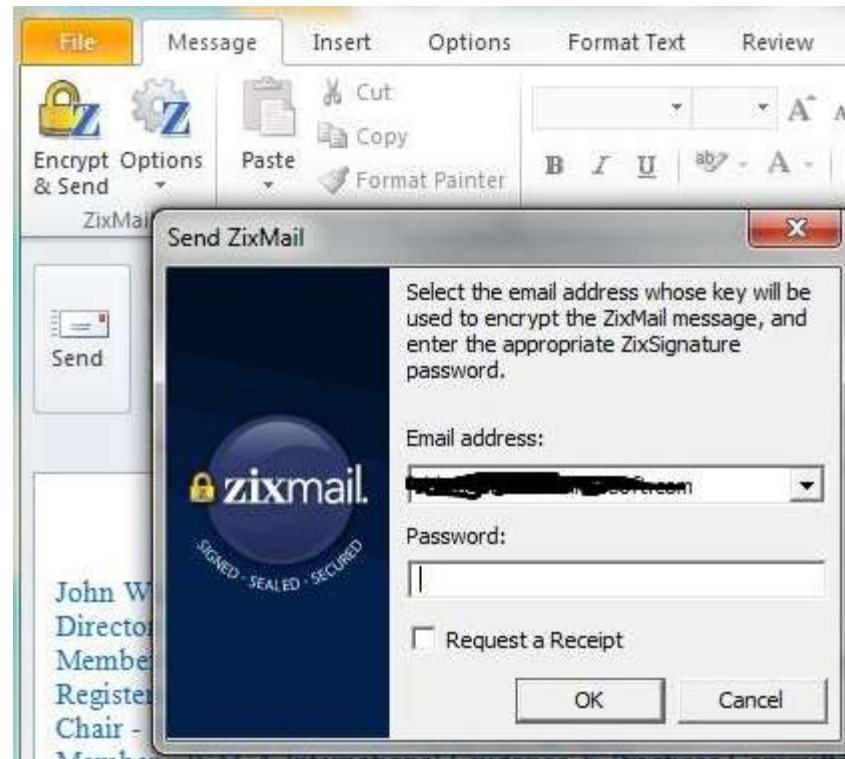
Status	Test Name	Information
PASS	Parent zone provides NS records	Parent zone exists and provides NS records. This is good because some domains, usually third or fourth level domains, such as 'example.co.uk' do not have a direct parent zone. This is legal but can cause confusion. The NS Records provided are (nameserver Address TTL): dns1.name-services.com 98.124.152.1 dns2.name-services.com 98.124.157.1 dns3.name-services.com 98.124.153.1 dns4.name-services.com 98.124.154.1 dns5.name-services.com 98.124.154.1
PASS	Number of nameservers	At least 2 (RFC 1035 section 5 recommends at least 3), but fewer than 8 NS records exist (RFC 1035 section 2.6 recommends that you have no more than 7). This meets the RFC minimum requirements, but is lower than the upper limits that some domain registrars have on the number of nameservers. A larger number of nameservers reduce the load on each and, since they should be located in different locations, prevent a single point of failure. The NS Records provided are: dns1.name-services.com 98.124.152.1 TTL=172800 dns2.name-services.com 98.124.157.1 TTL=172800 dns3.name-services.com 98.124.153.1 TTL=172800 dns4.name-services.com 98.124.154.1 TTL=172800 dns5.name-services.com 98.124.154.1 TTL=172800



Agile Secure X-Platform Communications

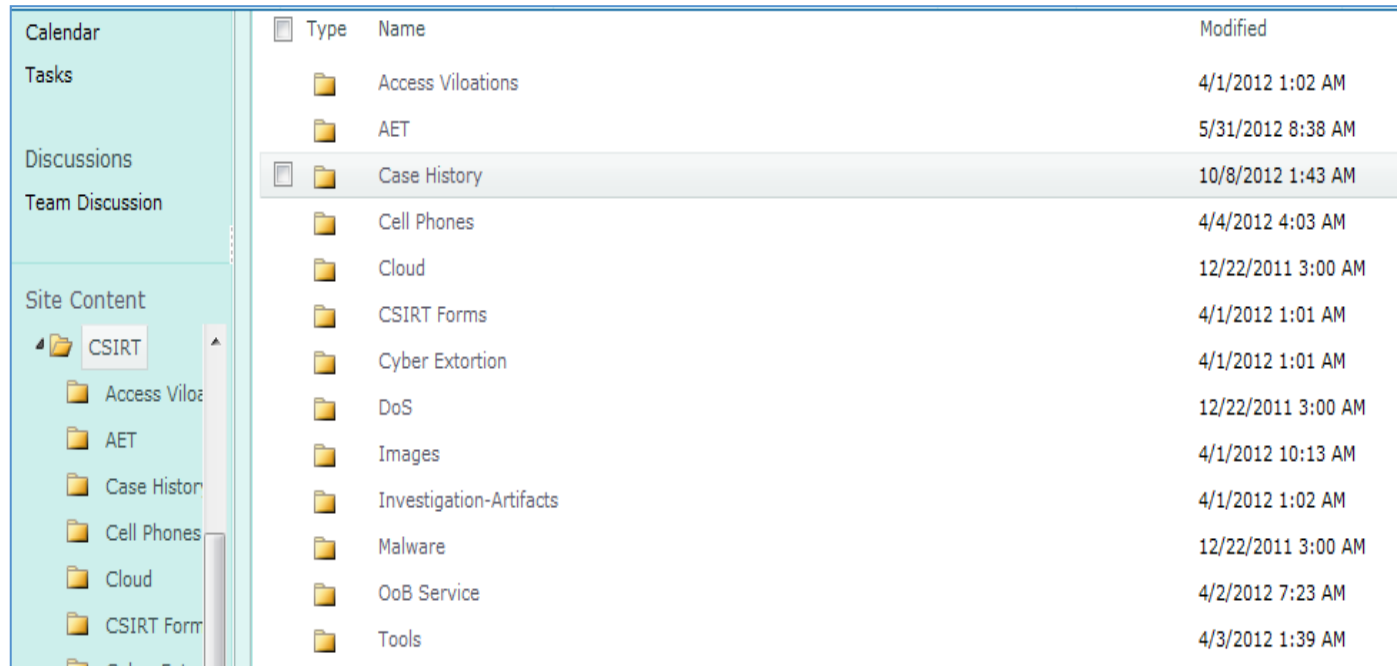
Agile, off LAN, Secure, cross platform forms of communications are at times a must have.

Here, a cost effective solution provisioned by **Zixmail**.



Case Management

It is essential to maintain an in-flow, and post event Case Management System.



Type	Name	Modified
Folder	Access Viloations	4/1/2012 1:02 AM
Folder	AET	5/31/2012 8:38 AM
Folder	Case History	10/8/2012 1:43 AM
Folder	Cell Phones	4/4/2012 4:03 AM
Folder	Cloud	12/22/2011 3:00 AM
Folder	CSIRT Forms	4/1/2012 1:01 AM
Folder	Cyber Extortion	4/1/2012 1:01 AM
Folder	DoS	12/22/2011 3:00 AM
Folder	Images	4/1/2012 10:13 AM
Folder	Investigation-Artifacts	4/1/2012 1:02 AM
Folder	Malware	12/22/2011 3:00 AM
Folder	OoB Service	4/2/2012 7:23 AM
Folder	Tools	4/3/2012 1:39 AM

Buy one, or build it based on an owned application – Here my *SharePoint*.



Conclusions - '*Homogenous Security*'

- The current level of threat is *high*, and in fact are *growing*!
- The vectors of threat should be anticipated to *increase* – after all, *they are on a roll!*
- Baroness Pauline Neville-Jones is correct – we **MUST** get smarter!

We need *joined up thinking*, enhanced levels of Skill, & Cyber Security Awareness, and a joined up ***one-stop-shop of:***

Homogenous Security



Thank You

