The Quarterly Magazine for Digital Forensics Practitioners

Issue 19 • May 2014

DIGITAL FORENSICS / MAGAZINE

WIN! a signed book

by Mark Osborne

NTP DDOS

DNS to NTP DDOS Conversion – Magic!

How to convert a DNS DDOS program to an NTP DDOS program by changing a few lines of code...

Latest News, 360 Book Reviews, IRQ *& much more inside!*

PLUS!

Cyber Skills
Xbox Tested
Memory Forensics
Analyze DI

9 772042 061004 19
Issue 19 / £14.99 TR Media

CYBER FORENSICS – INCIDENT RESPONSE

CSIRT, First Responder Capabilities, Cyber Forensics and Incident Response, are topics high on the agenda, but low in capability, says John Walker...

/ ADVANCED

Our world still suffering from the fallout of the economic downturn; businesses, organisations and individuals are feeling the financial effects, but there is one sector that seems unaffected and is enjoying significant growth; generating billions in revenue, and looking forward to a long and prosperous future. Welcome to the world of e-crime! There has also been much recent debate about the levels of cyber-risk faced by individuals, businesses, governments, and all levels of the interconnected 'Global Village'. The basic fact however is rather simple:

'If you or your business use the Internet, then you are potentially vulnerable, and exposed to the possibility of criminal exploitation.'

But then having recognised this state of imposition, we may have actually played into the hands of the criminal element by our very passive acceptance of dealing with the early signs of the onslaught of attacks. Over the last decade the profession of IT/Cyber Security has been very much focused on defending and protecting assets, but when it came to a security incidents, or events, in my experience it was not so much about acquiring evidence and artefacts, but more a case of keeping the operational lights on. However, whilst such a mission was to be approached in the interest of those always on, and always available services, that approach has done very little to gather any statistics of information about encountered threats, and to a large extent was neglect which played into the hands of Cyber Criminals and Hackers alike. As an example from the real world, consider the financial institution that encountered regular DoS [Denial-of-Service] attacks coming through a well-known Chinese newspaper site, of the same profile, and at the same time every single day, which on occasions then changed its profile, but nevertheless continued. However, as it was possible to packet-shape the adverse connections, they were simply put to one side, tolerated, and left to continue their illicit attempts to cause chaos, which they eventually did.

Figure 1 is the actual example downloaded from the Firewall Logs that shows the event in flow.

/ FIRST RESPONDERS & THE CSIRT

For many years now, the Forensic Science Society has been recognised as a leader in the field of Forensic Science and has published multiples of well researched academic reports on subjects ranging from wet sciences [body fluids], ballistics, though to fingerprinting techniques. However, at a meeting held at their Harrogate Offices in 2013, it was agreed that, given 99.9% of crimes now tend to have some direct, or indirect association with some form of technology, be that, laptop, cell phone, or other forms of electronic [digital] storage or communications, it would seem to make good sense to incorporate the element of 'Cyber Forensics', and 'First Responder Cyber Response Capabilities' into their areas of interest, and on 2nd February 2014 the first of many events encompassing this specialised subject was convened in York, thus emphasising just how important this topic has become to all elements of society, and not just those engaged in the world of IT.

The blatant facts of the matter are however, when it comes to the CSIRT, First Responder Capabilities, Cyber Forensics and Incident Response, whilst these topics are high on the agenda of discussions, they would seem to be low in the capability stakes, and as such

Date(s)	Time	Attacker	Target	Region	Size of Attack	Duration	Impact	Comments
Various	Various	See below.	See below.	******	See below.	24 hours	FW detected Bad Packets, and logged - alerted encountered Syn attack. CPU process consumed to 60 percent of capacity (normal operational consumption is <>24 percent).	Attack was constructed of Bad Packets, which were generated seemingly from the ******** (*****). Presumption is this IP was spoofed. FW auto self-protected against Syn attack. It is also possible that the location that the attack has been generated from has been subject to a zombie impact on their networked environment.

"Product" "Interface" "Origin" "Type" "Action" "Service" "Source" "Destination" "Protocol" "Source Port" "Attack Name" "Information"

"8Oct2005" "23:56:16" "SmartDefense" "eth3c0" "**********_01" "Log" "Drop" "5708" "xx xxx xx xx" "xxx xx xxx xx" "tcp" "http" "Bad packet" "TCP flags: SYN-ACK-URG; Attack Info: TCP header corrupt"

Figure 1.

“IT IS ABSOLUTELY ESSENTIAL THAT THE PRACTICES ARE DELIVERED WITH SOLID KNOWLEDGE AND DISCIPLINES TO ENSURE THE APPLIED METHODOLOGIES, ACQUISITIONS, AND CASE MANAGEMENT PROCESSES ARE ROBUST AND CONSISTENT ON EACH OCCASION, EVENT OR INCIDENT AS IT IS ENGAGED.”

COPINE SCALE

This is a rating system created in Ireland and used in the United Kingdom to categorize the severity of images of child sex abuse. The scale was developed by staff at the COPINE (“Combating Pedophile Information Networks in Europe”).

a] The ability to contain Artifacts such as logs, traces, events, Dynamic Memory, eMail and of course where appropriate screen shots

b] Methodologies and capabilities should be in place to underpin the acquisition of evidence and artifacts ensuring that the associated integrity is preserved

c] Have the capability to assess the Taxonomy of the attack type to understand its early implications

d] Have agreed policies, processes, and procedures in place which will be applied when engaging an incident

e] Deploy a system which support case management/handling

f] Follow processes which mandate the security handling, bag-and-tagging, and storage of acquired artifacts

g] Have interfaces established with external agencies [e.g. Law Enforcement]

h] Have the right tools in place to support response to an incident

i] And last but not least – ensure that the members of the CSIRT First Responders are trained, proficient, and are capable of using the procured toolsets

Figure 2.

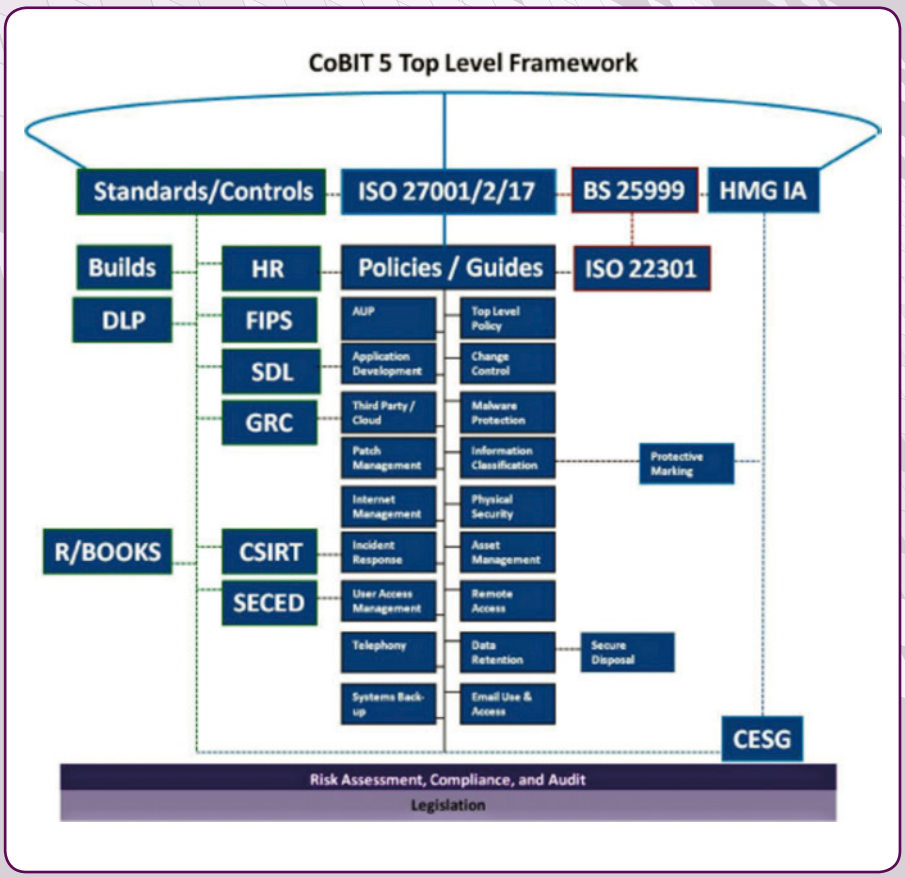

Figure 3.

much does get missed, damaged, or is just ignored for sake of expediency, a position which must change. That said of course, there are also expectations out of many directives that require some form of investigative and incident response underpin, not forgetting the assertions born out of PCI-DSS.

The basic facts of the matter are that every organisation or business which wishes to preserve the integrity of their assets, needs to have a capability deployed into their area of operation. As a starter checklist the following elements are my top areas of interest which need to be provisioned.

Figure 2 represents a list of the essentials that are required to furnish a robust capability to underpin CSIRT operations

To provision the overall internal service, it is absolutely essential that the practices are delivered with solid knowledge and disciplines to ensure the applied methodologies, acquisitions, and case management processes are robust and consistent on each occasion, event or incident as they are engaged. It is equally important that the fundamental processes of engaging a case are always followed. These, I refer to as the 3Ps, which are Process, Process, and Process. Why? Well here, as most lawyers will tell you, when such cases fail it is not so much around the technical facets, or artefacts, but some break in process, say mishandling an artefact, failing to follow the chain-of-custody, or by corrupting a hard drive with some unintentional writes onto the media under investigation. For this reason, the origination of documentation in the form of CSIRT Policies, Procedures, Case Handling, and even Run-Books

[Playbooks] can represent critical components of the established CSIRT, ensuring that no matter which member of the team initiatives, or picks up the investigation, they are following, and applying, as far as is practicable, consistent guidelines devoid of dangerous interpretation.

At Figure 3 is an example of an established CSIRT Framework based on CoBIT, encompassing the ISO/IEC 27001, and PAS 555 as appropriate to deliver the enterprise wide service, which in this case also necessitates inclusion of CESG directives.

It is, of course, equally important to appreciate the external factors, which feed into the internal mission of incident response, with one high value resource is a document circulated by ACPO [Association of Chief Police Officers] in the form of the Good Practice Guide for Computer Based Electronic Evidence.

Clearly to cover every eventuality in an article of this size is simply not possible, but one area I feel is incumbent upon me to introduce is the methodologies, and styles of handling which are applied when encountering, what is loosely referred to as Child Pornography. However, before we look at this known, and what would seem to be considered as a growing problem, let us clarify that the actual term which is applicable to images, descriptions, and other such materials in this category are actually 'Child Abuse Materials'. In the last 5 years, I have consulted with organisations on this subject, and to my astonishment in the majority of cases they have not understood the criminal implications of mishandling such materials, had failed on multiple occasions to report such discoveries, and in one of the worst cases of all, a Nottingham based organisation established within the Financial Security Sector had their CISO almost dedicated to receiving, and reviewing any trapped images, including those in this category. With the last example, the matter got even more serious, as when such materials were proven to be interesting, they were further shared with other members of the team, thus compounding the legal implications related to handling such objects [artefacts].

3	Erotica	Surreptitiously taken photographs of children in play areas or other safe environments showing either underwear or varying degrees of nakedness.
4	Posing	Deliberately posed pictures of children fully clothed, partially clothed or naked (where the amount, context and organisation suggests sexual interest).
5	Erotic Posing	Deliberately posed pictures of fully, partially clothed or naked children in sexualised or provocative poses.
6	Explicit Erotic Posing	Pictures emphasising genital areas, where the child is either naked, partially clothed or fully clothed.
7	Explicit Sexual Activity	Pictures that depict touching, mutual and self-masturbation, oral sex and intercourse by a child, not involving an adult.

Figure 4.

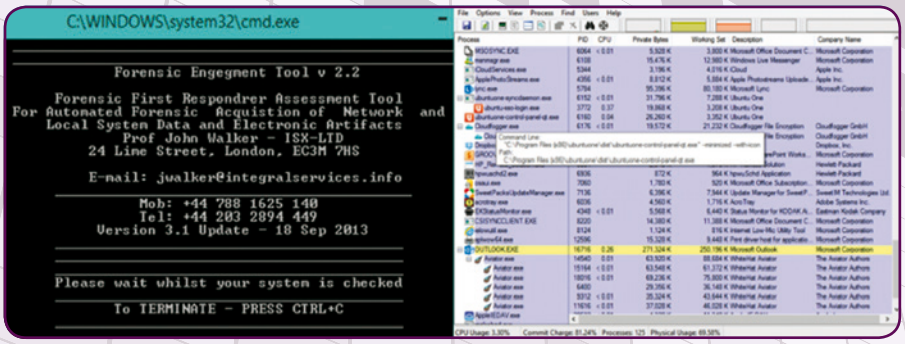

Figure 5.

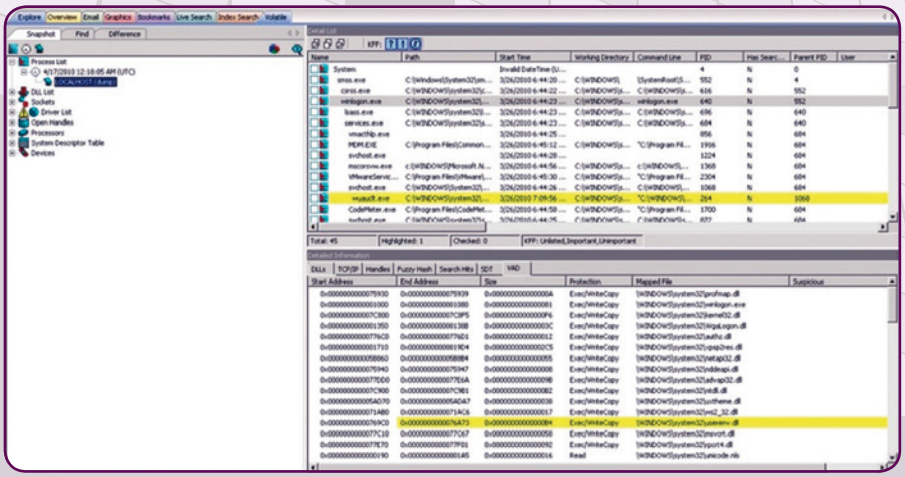

Figure 6.

Given the legal, and reputational ramifications of an organisation encountering and mishandling materials in this category, it is of paramount importance that the deployed CSIRT has the required capabilities to engage, and to assure that any such encountered and acquired materials are subject to correct classification, and that they are handled in accord with the implicated criminal law and legal aspects. To address this element of the CSIRT, we have augmented a number of organisations with the required level of internal training, with further underpin of Policy, and the associated Run-Books [Playbooks] detailing what process the First Responder should follow, including the categorisations listed under the COPINE 1–7 scales, See Figure 4.

We can see an extract from the COPIN Scale, along with the associated descriptions of the objects, and the related assessment.

It is my personal belief that the most important part of a CSIRT, or First Responder engagement is that of the applied processes and policies, and supporting documentation to assure that a righteous path is always consistently followed, and that there are always applicable processes in place to preserve the integrity of any acquired information, artefacts, or other forms of materials which represent evidential interest.

With the assertion that the correct level of skill set is in place we then move on to the tools, utilities, and applications which may be employed to underpin the

mission of technological engagement, acquisition of images, and other such First Responder requirements.

When we enter this area of discussion, we get closer to the 'B' World [Budget] with the focus on what is the cost? However, contrary to popular opinion a basic CSIRT does not have to cost an arm and a leg. The first important questions to be answered of course are:

a) What is to be encompassed by the CSIRT, and
b) What initial funding is available to underpin its deployment

With question a) The business needs to clarify if they are going for implementation of a fully capable internal CSIRT capability, with all the required bells and whistles; or could it be that the organisation is looking to provision a light-touch CSIRT Team with reliance on an external provider under contract, or other such on-the-fly services, such as those offered by Access Data, outsourcing elements of the CSIRT when you need it.

With b) of course, it may be that there is an identified cost which may be used to procure the required set of tools. Thus, what is in the pot will very much dictate what you can procure, so let us consider the opportunities:

Option 1: At option one we may consider what can be achieved at zero cost. In this are there are those in-house tools which may be leveraged to run an early investigative triage, or the utilisation of tools like the very capable Process Explorer which is an excellent tool for investigation of dynamic states and the investigation of active Malware infestations, see Figure 5.

In Figure 5, we see the comparison between an in-house developed, complex acquisition tool, and the free Process Explorer utility.

ACPO GUIDE

The Association of Chief Police Officers (ACPO) Good Practice Guide for Computer Based Electronic Evidence. The main principles of the ACPO Good Practice Guide for Computer Based and electronic Evidence.

Option 2: With option 2 we can look to those professional tools which are used by International Law Enforcement, and Security Professionals, and these come in various flavours and costs, and it really does here ask the question as to what spend is available to furnish the required level of technological solutions. With focus on provisioning support for Windows, in this area I am introducing two well-known vendors, and they are Paraben, and Access Data who supply multiple solutions to enable the CSIRT Forensics element to a global user base. Figure 6 below is an example of the Access Data application FTK [Forensic Toolkit] running in anger against a test case.

Figure 6 is a screen shot of the commercially available and very powerful, all-encompassing Forensic Toolkit [FTK] which is provided by Access Data.

Option 3: This option is considering engaging an external provider who may act on behalf of the organisation to provision services at time of an incident, or at time of an event being identified. However, notwithstanding the approach here has migrated the CSIRT operational capability out of the organisation, there will still remain the requirement for the early capability to engage the incident, capture all the required details, and information, and of course to acquire any artefact and discoveries in a process orientated manner. Thus it is still recommended that there are documented processes and procedures in place to ensure the early stage process secures the integrity of the event, and thereby maintains the subsequent investigation.

GOOD GUIDANCE

It is always, of course, of high value to follow some form of recognised Best Practice Guidance, and in this area I would recommended obtaining a copy of PAS 555. Published in 2013, it addresses Cyber Security and Incident Management, and provides a very solid cornerstone upon which to rest the aspiration of delivering a robust CSIRT, First Responder Capability. This, along with the ancillary activities which make up the big picture, the ISO/IEC 27001 high level guidance, and relationships to the ACPO Guide already introduced in this article can provide the commercial organisation with a very effective entry level capability to furnish their business with a robust solution.

CONCLUSION

Security incidents and events for some organisations are known every day occurrences, whilst for others there may be events which occur, but go unnoticed until such time the impact becomes obvious to them or their clients. Nevertheless the posed cyber threats are now well evidenced by multiples of well-documented security compromises and attacks against very high profile organisations, along with the unwanted fallout of adverse press, and losses of reputational pride. It may thus also be asserted that the onslaught of cyber-attacks, and crime will continue to escalate, and it may be more a case of when it happens to you, and not if. However, no matter the acceptance of the need to establish some form of CSIRT capability, from my experience, I have observed one very clear fact, the time to decide that such a capability is required is not at the time of encountering an event.

AUTHOR BIOGRAPHY

John Walker is a Visiting Professor at the School of Computing and Informatics, Nottingham Trent University (NTU), owner and CTO of SBLTD, a specialist Contracting/ Consultancy in the arena of IT Security and Forensics, and Security Analytics, the Director of Cyber Research at the Ascot Barclay Group. He is also activity involved with supporting the countering of eCrime, eFraud, and on-line Child Abuse, an ENISA CEI Listed Expert, an Editorial Member of the Cyber Security Research Institute (CRSI), the Chair of the ISACA London SAG, and in July 2012 was appointed Member of the ISACA International Guidance & Practices Committee (GPC), and is a Fellow of the British Computer Society (BCS). John is also a practicing Expert Witness in the area of IT, and the originator, and author of a CPD/MSc Module covering Digital Forensics and Investigations.

John

Digitally signed by John
DN: cn=John, o=ISX, ou=ISX, email=jwalker@integralservices.info, c=GB
Date: 2014.05.05 17:15:13 +01'00'