



June 2016 Chapter Meeting

Venue: Georgian Suite, Buswells Hotel, Molesworth St., Dublin 2

Date & Time: June 1st at 16:00

Chair proposed Ordinance Survey Ireland, Seconded by David Cahill
Chair proposed Nostra, seconded by Richard Liddle

First Speaker John Ryan – Zinopy on Crypto-Ransomware

This included an excellent interactive poll that John conducted that was very well received by those present.

Ransomware is costing Irish businesses €600M per annum, huge technical skill shortage, this contributes to a 3-6 month that average APT is on a network.

First Ransomware was discovered in 1989, not a new problem, but newly monetised. It affects all industries, including those with huge security investment, largest impact on systems without admin / user segregation.

Why is popular

- Less risk than other data extraction
- Very lucrative
- Uses bitcoin
- Can be bought as a service, with good customer support

Healthcare systems in USA a major target, not yet in Europe but is likely. Master Boot Records, Apple and Linux devices now targeted.

Major attack vector, drive-by malvertising on reputable sites.

Ran by Organised Crime

- Lucrative
- Multilingual and multi-level support
- Tracking of news to 'adjust' their product to suit market
- Targeted audience, including background checks of their affiliates

Affects all countries, >10,000 users per month pay, campaigns average \$34M, 20% of Irish companies admit to being affected, believe this is very under-reported

Concerns

- Damage to brand
- Data loss
- Staff seen as being biggest vector for attack, but still not trained often or well enough, if at all

Options for Protect – it is an arms race and they are winning

- Backup and Restore
- Anti-Virus
- Patch and compliance management
- Network segmentation
- Content filtering
- Advanced malware protection



- Least privilege access
- Threat extraction

After the Break Tony Clarke (tony.clarke@owasp.org) from OWASP asked member to consider joining an initiative into Women in Cyber Security, only 11% of people in Cyber Security are women and there are 1.5 million open security roles across the world. Please contact Tony if you want to get involved.

Richard Harris -FireEye: Overview of the threat landscape

2015 was the year of retail breaches, median days before compromise discovered is going down, but still high. It is still nearly a year on average from breach until full public disclosure.

Business disruption attacks and PII theft on increase.

Routers and switches a major new vector for attacks, including pushing images to SDNs

Incident responses:

- Confirm
- Humans can be unpredictable, deal with caution
- Timing is critical
- Stay focused
- Evaluate risk of confronting attacker
- Engage legal, PR, forensics FIRST and have a plan
- Consider all options
- Ensure segmentation and backups
- After an event – gap analysis, Improve security
- Once you have been attacked and paid, you will be target again by same attackers and others

EMEA specific

Political, Industrial espionage, financial services are all on increase

Turkey, Spain, Israel, Saudi, Belgium, Luxembourg, Germany and UK major targets

Virtuals – Defence, government, financial services, energy / utilities and telcos main targets. Financial Services and government growing quickest, financial services biggest increase in APTs

Malware, ransomware both increasing both in volume and sophistication

APT phishing still on the increase, impersonating IT or Security being a big vector, attackers working on ordinary calendar week, Wednesday is busiest, weekends are quieter.

System integrators and third parties are being a major vector for APT attacks, one SI can lead to multiple systems being breached. Look at SLAs, plans, multi-factor authentication



We then retired to the Oak Bar for our annual quiz, which as always was a great success, a big thanks to all the members and associates below for their gifts.

The charity raffle raised €335 for Dublin Simon Community

Prizes courtesy of:

Asystec Limited
BCC Risk Advisory
Buswell's Hotel
Ernst & Young Global Limited
Espion
IBM
Integrity 360
ISAS
Logicalis
Microsoft
Threatscape
Ward Solutions
Workday
Zinopy



Meeting Attendance record 01/6/16:

Company	Name	Company	Name
Aib	Ashley Hewitt	Menlo Security	Jason Steer
Aib	David Cahill	Kbc	Cillian Fagan
CBI	Niall Mcevoy	Isas	Martim Kerrigan
Aer Lingus	Richard Liddle	Zinopy	Lolly Tondani
Asystec	Joe Montgomery	Aib	Richard Nealon
ICON Plc	Tony Clarke	ESB	Chris Madden
Bnym	David Torres	Zinopy	John Ryan
Bnymellon	Dom Gentile	Smbc Aviation Capital	Martina Costelloe
Logicalis	Marcus Reid	Health And Safety Authority	Barry Young
Logicalis	John Bailey	Hpress	Joanne Bailey
CIE	Tim Wilson		
Threatscape	Eddie Lyons	F5 Networks	Dave Burke
Threatscape	Darren Campbell	Pwc	Rebecca Hughes
Asystec	Michael Spillane	Pwc	Thomas Reidy
Asystec	Peter O' Connor	Pwc	John Noonan
Ordnance Survey	Joe Lynch	Aib	Declan Tobin
Espion	Neil Ryan	Capita	Philip Thompson
Espion	Iain Cuthbertson	Capita	Colin English
Bhconsulting	Neha Thethi	Bord Gais Energy	Frank O'reilly
Ibm	Rory Harte	Nostra	Senan Largey
Menlo Security	Simon Haylock	Asystec	Brendan Mcphillips
Tim Wilson	CIE		

Members are reminded to sign the attendance records, so that CPE's can be verified.

2016 Committee

Martina Costelloe, SMBC	martina.costelloe@smbc.aero	John Clarke	john.clarke@workday.com
David Cahill, AIB	david.a.cahill@aib.ie	Karin Mulvihill, BNY	Karin.Mulvihill@bnymellon.com
Niall McEvoy, CBI	niall.mcevoy@centralbank.ie	Richard Liddle, Aer Lingus	richard.liddle@aerlingus.com
Declan Tobin, AIB	Declan.A.Tobin@aib.ie	Brian Molony, VHI	brian.molony@vhi.ie