BSides Liverpool Conference

29/06/2019

Abstract

BSides is a community driven event built for and by information security community members. BSides Liverpool held its inaugural conference on 29th July 2019 and this report will outline my experience and learnings from the day, with some in-work applications. NB: Opinions are my own and the statements made about vendors/software/hardware are correct as far as I'm aware.

> Miles Eastwood

Opening Key Note – Focus on your malware, not infrastructure!

By Omri Segev Moyal

This talk centred around the use of automation tools in security research, namely the dissection of malware of exploits. However, as the research becomes quicker there arises a new problem with the maintenance and support of the supporting secure infrastructure for the automation. It was claimed that security researchers needed to spend precious time on their infrastructure and its hostile environment rather than on their target goal.

A category of cloud computing, FaaS (Function as a Service) provides a cost effective and low maintenance solution to the problems stated above and by using the model, a “serverless” architecture can be achieved. FaaS works by providing a platform where customers can develop, run and manage application functionalities, only incurring charges when the infrastructure is in use – a pay for processing model if you will.

With cloud providers such as Amazon with AWS (Amazon Web Services) Lambda offering FaaS, security researchers can spend time creating exploits and testing malware with the infrastructure being supported by a large vendor. For the vendor, they now have a model whereby spare processing/memory/storage can be sold as a service – reducing computing waste and opening a new line of income.

Cyber Threat Intelligence – Askari Blue

By Matthew Haynes (@MrMDHaynes)

It's all well and good having Cyber Threat Intelligence (CTI) but the focus should be on the whole Threat Intelligence (TI) picture – there are many different forms on intelligence but it is of most use when provided in a timely manner to a team/individual where it can be actioned.

Some useful terminology and structure around threat intelligence was presented:

- Data is collected and processed to become information. Information needs to be analysed to become intelligence.
- Intelligence Lifecycle:

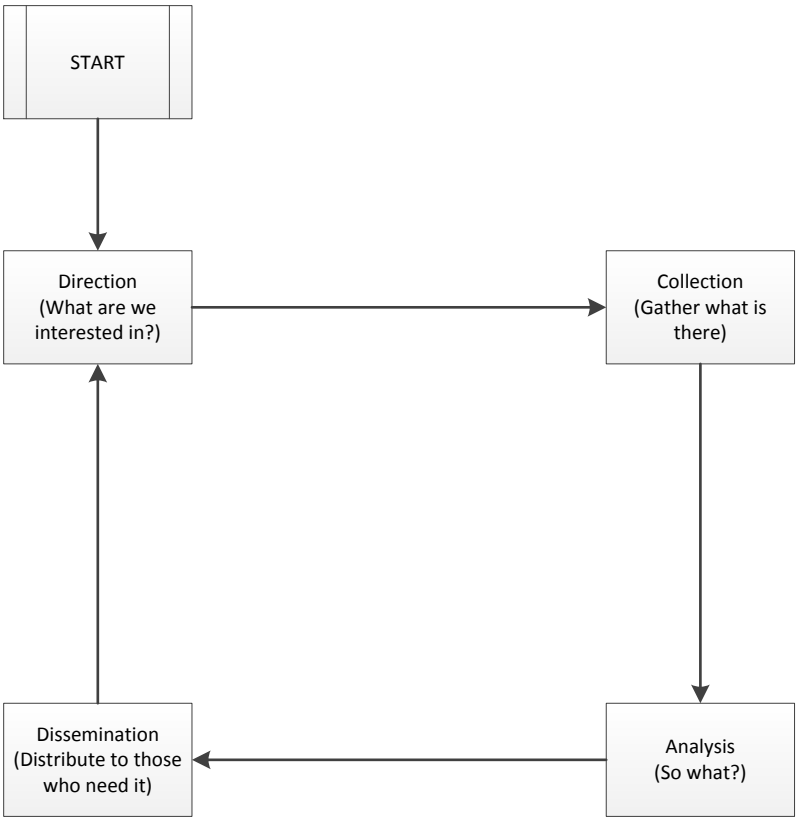

Figure 1 - Intelligence Lifecycle

Something that was explained as part of the other terms for intelligence sources was Most Likely Course of Action (MLCoA) and Most Dangerous Course of Action (MDCoA). These terms aren't always explicit in our RMADS but present a useful way of highlighting what we believe is likely to occur and what actions we are most concerned about threat actors making.

"The Chief"

By Peter Bleksley

After an interesting talk on his background, Peter Bleksley (best known as "The chief" from the TV Show "Hunted") had a plea for help. After giving up the show where he attempts to find wannabe fugitives, he's turned his hand to finding real fugitives and was looking for support in his latest endeavour to find Kevin Parle (**suspected** murderer).

His plea centred on the recruitment of "cyber detectives" to help find Mr Parle. Whilst something that is a worthwhile task, it was concerning that there was a 'by any means necessary' undertone.

One ~~Man~~ Person Army – MileIQ, Microsoft

By Kashish Mittal (@IAmKMittal)

This talk focused on how to instil security and a security culture in start-up companies where it hasn't been considered before.

Awareness and education are key for instilling a culture of security within an organisation, with new start-ups the key window is 30-90 days after starting. In this window there should be 3-5 key wins made that show the importance of security but also are of limited detriment to existing users. After

the initial window, when coming across a new area the process should be to secure, document, repeat as creating repeatable processes and documenting them helps create standards – with end users potentially able to carry out the work.

An idea that has worked amongst the organisations Kashish has worked for is the introduction of 'Security Champions'. Users who are more bought into security than the average and can champion the cause as well as provide advice after receiving appropriate training. It was suggested that there should be one champion per team, one per location (in geographically disparate organisations) or one per twenty full time employees. This is made successful by having an executive (board) level sponsor and perks that the champions can buy into.

The logs don’t work, they just make it worse – LMNTRIX

By Ian Murphy

The current trends in the security landscape are suggesting that the previous high focus area of prevention is no longer where the focus should be.

Too much focus on prevention causes the following problems:

- Alert fatigue – the sheer number of logs about everything over saturates the reporting and important events get lost in the noise.
- Tough to identify hackers on the network – no post breach strategy.
- Lack of evidence – no post breach forensic capability.
- Lack of skills/resource – no breach validation capability.

There are three fundamental truths that need to be accepted:

1. You will be breached.
2. The human factor is the weakest link – "there is no patch for stupidity."
3. Insecure software is eating the world.

Organisations need to mature through the following levels:

1. Architecture.
2. Passive Defence.
3. Active Defence.
4. Intelligence.
5. Offence (perhaps not for us though).

Compliance does not equal security. The basics need to be in place and be right, and then the drive should be from prevention to intelligence-driven security and big data security analysis.

“New talk who dis” – Kryptos Logic

By Jamie Hankins (@2sec4u)

This was a very interesting and engaging talk on the emergence and spread of WannaCry globally. Whilst mainstream media reported predominantly on the effects of the outbreak in terms of the NHS (as a high profile and severely affected organisation), it was interesting to understand the full scope of infection and the work needed to stop it.

The use of sink holes to prevent to prevent malicious activity was eye opening and the amount of work required to run them for a major incident was impressive – 90+ hours over 5 days engaging with law enforcement and those affected.

The Beer Farmers

A dissection of some of the ethical issues around data/information privacy and exploit releases. This drew on a couple of recent(ish) high profile cases; the Facebook-Cambridge Analytica data scandal Google’s release of a Windows 7 zero-day exploit, even when Microsoft had informed them a patch was being developed.

Other discussion points were around the scale of private information leakage from nearly every platform that uses it, reinforcing that nothing is “unhackable” – despite the claims by many company’s marketing schemes and various Kickstarter campaigns.

Closing Keynote – Machiavelli’s guide to InfoSec!

By Aaron <<Finux>> Finnon (Vindler GmbH)

A heavily concept based presentation for the closing keynote which was an attempt at drawing parallels between that which is presented in Machiavelli’s *The Prince* and secure practices/culture.

The parallels, somewhat tenuous at times, followed a trend of highlighting a need for an enterprise wide inclusivity in secure practices where security should arm/empower individuals so that they are almost partisan-esque. Additionally, the keynote focused on a topic mentioned previously in the day – fortresses are often built to protect from sudden attacks and those on the inside, if a ruler (security professional) fears his subjects (users) more than foreign invaders (threat sources/actors), they should build fortresses.

TL;DR or somewhat confused? In a nutshell, disarming citizens (users) sends a message that the ruler (security professionals) do not trust them. Like disarming one’s citizens, building a fortress within the city expresses distrust and shows insecurity. It was argued that no fortress can substitute for the trust and support of the people.

Market Stalls:

PwC

The drive from PwC appeared to be a push on recruitment as there was information on both graduate schemes and roles for experienced professionals. PwC also was advertising that they were running an information security consultancy arm of their organisation which is divided into Cyber Security Advisory, Cyber Threat Operation, Identity and Access Management (IdAM) and Network Information Security.

Besides the sales and recruitment elements, there was an interesting report 'Operation Cloud Hopper' which was published in April this year by PwC in collaboration with BAE Systems. The report centres around APT (Advanced Persistent Threat) 10 (Menupass Team) which has targeted managed IT Service Providers (MSPs) with aims of retrieving intellectual property from both providers and clients. The threat actor is assessed as highly likely of being a China-based threat actor. With the specific targeting of intellectual property on a global scale and general espionage activity it is a clear threat to our organisation, especially with growing interest in the Maritime and Defence sectors by other alleged China-based APTs such as APT1 (Unit 61398 (PLA), Comment Crew), APT3 (UPS Team), APT12 (Calc Team), APT18 (Webky) and APT40. The report is high-level and relatively digestible with a separate technical report. Electronic copies of the repot with technical annexes are available from the PwC website – even with md5 hashes for each element for the paranoid amongst us. For more on the aforementioned APTs, FireEye has a good amount of material for each of them and other nation state attributed APTs on their website.

Sapphire/Tenable

Tenable is perhaps most notable as the vendor of Nessus (arguably one of the most common vulnerability assessment tools and the output from which, when interpreted, can be sold as a consultancy service worth a small fortune).

Sapphire is a platinum tier partner with Tenable (not sure what exactly that means) and from speaking to the Major Accounts Manager, Sapphire is a provider of managed services from a security perspective in a wide range of areas. Notably this included solutions tailored to converged Information Technology (IT)/Operational Technology (OT) systems and there is a solution brief on the joint company's passive and active security solutions – unfortunately no hashes on the download this time and I take no responsibility for integrity of it.

The discussions on the upcoming Industry 4.0 (a new phase in the industrial Revolution that focuses heavily on interconnectivity, automation, machine learning, and real-time data) didn't extract any of the practices employed but solidified that this is a growth area that needs to be planned for, before it's too late.

North West Regional Organised Crime Unit

Nothing of particular note from speaking to the vendor. The information was predominantly was publicly available NCSC guidance on various topics.

TrapX Security

DeceptionGrid™ 6.2 was the latest and greatest offering from TrapX Security, a way by which operational IT assets and connected IoT (Internet of Things) devices are mimicked to create 'Traps'. These 'Traps' are similar to honeypots (data that appears to be a legitimate part of the network but is actually monitored and isolated) and with the DeceptionGrid it is alleged that minimal resources are required to deploy with a 99% accurate reporting rating (as the trap is either activated or it isn't). The software also allows for emulation of industry specific devices such as bespoke OT that we could potentially look replicate. As well as Traps, Deception Tokens (lures) are deployed with threat actors believing they are gaining files, scripts or configurations in an effort to escalate privileges but are instead moving into Traps.

So, how does this actually work? As a threat actor or malware begins to enumerate network access/start to make lateral moves, when they enumerate or access a DeceptionGrid Trap an alert is

raised and the infected assets/network areas are isolated in order to contain the spread. The alert is only raised when the threat actor or malware touches a Trap, so reporting has a high accuracy as the conditions are binary.

Prism InfoSec

The Cheltenham and Liverpool based Prism InfoSec was mainly selling their services in the areas of Cyber Security Assessments (Red Teaming, Pen Testing, Simulated Attacks, etc.), Information Security Consulting (GDPR, Risk Assessments, Maturity Reviews, etc.) and Cloud Security Services (Migrations, Architecture Reviews, Risk Assessments, etc.).

The AntiSocial Engineer

A small company of social engineers/penetration testers/awareness providers that provide services around the human element of both physical and IT security.

The particular area of focus was around the awareness of the way that users are targeted through various ‘ishing’ attacks (phishing, smishing, vishing, etc.) and the ease of physical access by tailgating, and even by dressing in the right theme.