Cyber criminal journeys to support forensic investigation and response deployment

In less than 20 years the Internet has affect the way society and humans operate. Worldwide internet usage increased from almost nothing in 1994 to more than 3.5 billion users worldwide at the beginning of 2014 (Internet Usage and World Population Statistics, 2014). In addition to humans, internet connectivity extends to digital devices. Indeed, more "things" are connected to the Internet than people. Gartner reports that the number *of* internet connected devices will reach 4.9 billion in 2015 while predicting 25 billion for 2020 (Gartner, 2014).

Expanding Internet connectivity has translated into a growing emphasis on the strategic importance of cyberspace to enable achieving fundamental objectives in contemporary societies: innovation, collaboration, productivity, competitiveness and leadership (Sharma, 2010). The expansion of cyber functionalities has, however, also opened up new opportunities for people to carry out criminal activities online, and/or to use the Internet as a medium for their criminal objectives. The advantages of the Internet come with risks. While organisations and individuals are exploiting its business benefits they may not realise that cyberspace confers the same benefits on those who wish to attack them. Hacker groups, criminal organisations and espionage units worldwide have access to powerful, evolving capabilities, which they use to identify and target their victims and commit cyber crimes. Today cyber criminals operate at the scale and sophistication of a global industry. The activities of modern cyber criminals often appear to have clear business objectives. Cyber crime has various aspects: attack planning, development and sale of tools, execution and generation of personal gain for the criminals. As a result of this complexity, in order better to understand cyber crimes, while developing and deploying measures to fight against it, it is important to understand its core mechanics as well as the thought processes and activities that characterise its cycles.

A useful tool to investigate cyber crimes and help develop effective countermeasures can be provided by criminal journey mapping. Journey mapping is a methodological tool that has been traditionally used in customer experience (Shostack, 1984) and criminology with the name of crime scripts (Brayley et al 2011). A journey describes all events and experiences that specific individuals or organisations go through to reach a goal or fulfil a need. A journey consists of events that describe what has happened and experiences that describe how the person or organisation involved felt during these events. Events and experiences are then translated into a visualisation map to show the full event process, key steps as well as positive and negative events. This tool is often used by strategy consultancies and public organisations to shape customer strategies and public service transformational programmes[1]. In the cyber crime context journey mapping can be used to describe all events and

[1] For instance in 2005, the UK government set out to transform public services. As part of this process, they focused on customer insight techniques such as customer experience journey mapping (UK Cabinet office, 2010)

experiences that cyber crime victims and perpetrators go through to fulfil their needs and/or objectives within the Internet over a given period of time.

As part of the emerging efforts to better understand and describe the events and experiences that cyber crime perpetrators and victims go through during a cyber crime we have developed cyber journeys from perpetrators and victims' perspective. In this first part of our article we have focused on the perpetrators and deployed crime scripting techniques[2] to develop eight journeys, which represent a selection of the most experienced and common cyber crimes across several industry sectors, mapping the key actions of their perpetrators. A script is a predetermined, stereotyped sequence of actions that define a well-known situation in a particular context (Borrion 2013). Our focus within the scripts has been on the crime itself rather than the contextual causes of crime or the law enforcement actions following the crime. This is because the key steps and cycle of cyber crimes can offer immediate and practical clues to support the investigation of cyber crimes, while also helping identify opportunities to manage risks and responses. Key steps within the cyber criminal cycle can also assist in the identification of *key points* or *gates* where to deploy responses (Borrion 2013). For example, by graphically presenting the typical sequence of events constituting a cyber crime that has been derived from mapping multiple instances of that type of crime, forensic analysts are able to identify specific metaphorical *gates* the criminal pass through if their crimes are to succeed. Once these points are identified, the logic is that those seeking to prevent such crimes will now better understand where best to focus their energies, whether this be through legislative/regulatory changes, the development of new technological applications, the behaviour modification of potential victims, and/or increased monitoring by Law Enforcement Agencies (LEAs) so as to detect, deter and/or capture the cyber criminals.

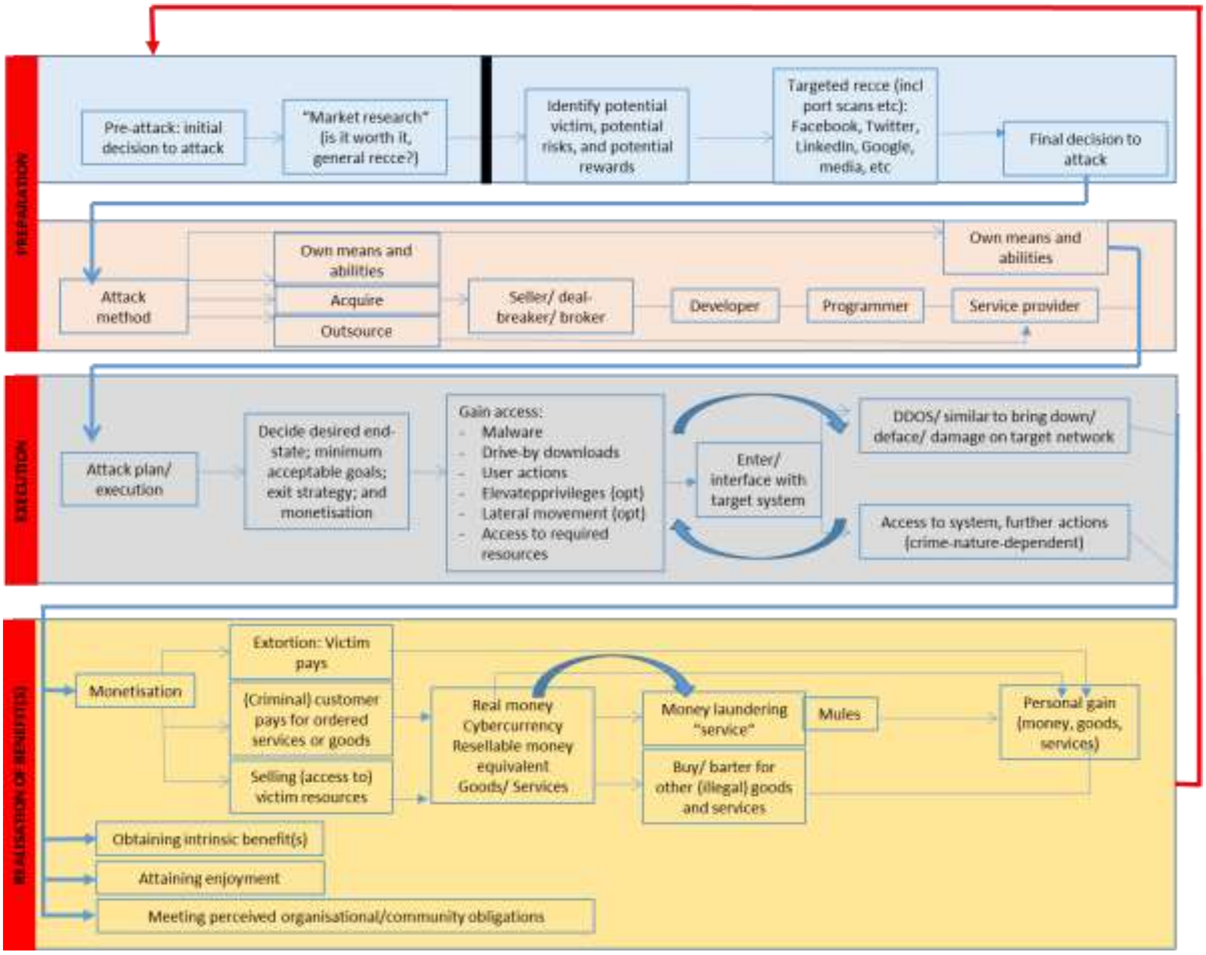
General cyber criminal journeys

There are various levels of scripts and selection depends on the script's intended application (Brayley et al 2011). Figure 1 represents a high-level journey map detailing a general crime cycle from the criminal's perspective. From this general depiction, more detailed maps can be drawn focussing on specific forms of cyber attacks by removing any superfluous steps. The benefits for investigators of producing this visual representation of the general cycle are that; (a) by identifying the commonalities inherent to the conduct of seemingly disparate cyber crimes we expose the underlying sequence of events that underpin the majority of cyber crimes, and (b) by comparing detailed maps of multiple different cyber attacks against this general crime cycle those tasked with defending against such attacks can see best where to focus their resources for maximal effect.

The expanding network of cyber criminals is increasingly operating like any legitimate, sophisticated business network. While there is an element of

[2] We have developed the script with the help of desktop research and insights from a group of experts

opportunism, often modern cyber criminals seem to have clear (business) objectives when starting their actions. The cyber criminals seem to know what kind of information they are searching for, what end-results they want to achieve, and how to reach these established goals, and they are sometimes willing to spend a lot of time in research and in planning their actions (CISCO 2014). These factors are reflected in the composition of the general crime cycle.



PREPARATION
Pre-attack: initial decision to attack
"Market research" (is it worth it, general recce?)
Identify potential victim, potential risks, and potential rewards
Targeted recce (incl port scans etc): Facebook, Twitter, LinkedIn, Google, media, etc
Final decision to attack
Attack method
Own means and abilities
Acquire
Outsource
Seller/ deal-breaker/ broker
Developer
Programmer
Service provider
Own means and abilities
EXECUTION
Attack plan/ execution
Decide desired end-state; minimum acceptable goals; exit strategy; and monetisation
Gain access:
- Malware
- Drive-by downloads
- User actions
- Elevateprivileges (opt)
- Lateral movement (opt)
- Access to required resources
Enter/ interface with target system
DDOS/ similar to bring down/ deface/ damage on target network
Access to system, further actions (crime-nature-dependent)
REALISATION OF BENEFIT(S)
Monetisation
Extortion: Victim pays
(Criminal) customer pays for ordered services or goods
Selling (access to) victim resources
Real money Cybercurrency Resellable money equivalent Goods/ Services
Money laundering "service"
Mules
Buy/ barter for other (illegal) goods and services
Personal gain (money, goods, services)
Obtaining intrinsic benefit(s)
Attaining enjoyment
Meeting perceived organisational/community obligations

Figure 1: General Crime Cycle

Cyber crime can be seen as a process where resources are required and decisions are taken at different stages in that process. In conceptualising and mapping cyber crimes we have divided these into three phases, being; the *preparation*, *execution*, and *realisation of benefits* phases.

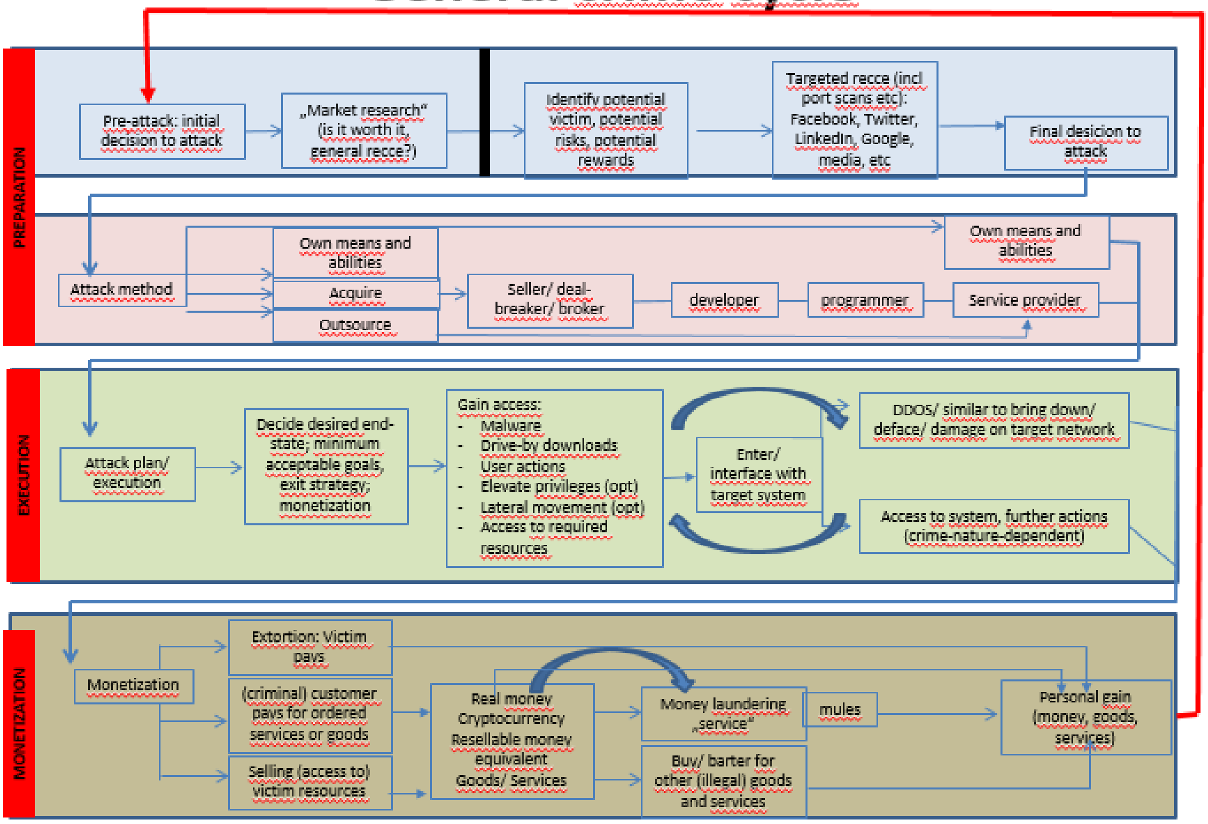
The preparation phase has two main components. Firstly the criminals need to decide to conduct the crime; this may be an opportunistic decision or may include "market research" in the sense of determining and weighing the costs and benefits of their options. The second component requires the identification of the potential victims and attack methods, the conducting of targeted reconnaissance and finally deciding to execute the criminal act. The attack itself can then be executed in three ways, such that the criminal either; (1) uses their own existing means and abilities, (2) they acquire the respective means from other criminals, or (3) they outsource the crime by paying another criminal to conduct it as a service. Regardless of the option taken there are specific forums, markets and online stores to assist the criminal here.

The execution phase starts with an attack plan. In the plan the criminal decides upon a desired end-state, their minimum acceptable goals, and monetisation and exit strategies. During the attack, the criminal gains access to victim's resources through any number of means, including malware, drive-by downloads, user actions, etc. Once the criminal gains access to the victim's system, they will map the compromised network, and/or deploy additional malware. Thereafter the criminal enters or interfaces with the target system and based on their desired and decided goals and end-states they take commensurate actions.

The realisation of benefits phase involves obtaining either *intrinsic* or *extrinsic* benefits. Intrinsic benefits include such things as enjoyment, self-satisfaction, peer-approval, status, feeling of revenge, or (in relation to hacktavism or government sponsored espionage) pride or justification. Extrinsic benefits including direct monetary gain (where the victims monetary assests are stolen, or the victim pays the criminal directly in cases of extortion, such as ransomware or DDoS extortion schemes) or indirect monetary gain whereby the victim's resources can be turned to tangible assets which are traded or sold.

There is a potential fourth stage sitting before the *preparation phase*; being the **Motivation phase**, whereby the would-be criminal makes the conscious decision to engage in a criminal act. While this decision is conscious, this does not imply it is necessarily well-reasoned, rational, or considered, in that the time between realising an opportunity exists to commit a cyber crime and making the decision to commit that crime may be incredibly short, and hence akin to a crime of opportunity. However, when developing our general crime cycle of criminal journeys we have removed the *motivation stage* and reverted to the three stage model depicted here. This does not imply the motivation of criminals is unimportant, especially when developing protection measures or considering changes to the regulatory environment. Rather, for the purposes of mapping the structure of the crime journeys themselves, while the motivation of the individual criminal may profoundly affect the particular choice of cyber crime to engage in, it does not materially affect the steps required to successfully complete that chosen crime. Hence incorporation of the motivation stage is not required to produce our criminal journeys here.

General crime cycle



PREPARATION

Pre-attack: initial decision to attack

„Market research“ (is it worth it, general recce?)

Identify potential victim, potential risks, potential rewards

Targeted recce (incl port scans etc): Facebook, Twitter, LinkedIn, Google, media, etc

Final desicion to attack

Attack method

Own means and abilities

Acquire

Outsource

Seller/ deal-breaker/ broker

developer

programmer

Service provider

Own means and abilities

EXECUTION

Attack plan/ execution

Decide desired end-state; minimum acceptable goals, exit strategy; monetization

Gain access:
- Malware
- Drive-by downloads
- User actions
- Elevate privileges (opt)
- Lateral movement (opt)
- Access to required resources

Enter/ interface with target system

DDOS/ similar to bring down/ deface/ damage on target network

Access to system, further actions (crime-nature-dependent)

MONETIZATION

Monetization

Extortion: Victim pays

(criminal) customer pays for ordered services or goods

Selling (access to) victim resources

Real money
Cryptocurrency
Resellable money equivalent
Goods/ Services

Money laundering „service“

mules

Buy/ barter for other (illegal) goods and services

Personal gain (money, goods, services)