NCA
National Crime Agency

Intelligence Assessment

Pathways Into Cyber Crime

National Cyber Crime Unit / Prevent Team

Purpose

There are a number of young people in the UK that are becoming involved in cyber dependent crime. Current understanding of pathways and motivations into this type of crime is limited. This report is limited by the relatively small number of debriefs involved. NCCU's continuing debrief project will inform any future versions.

This report aims to:

- Collate, summarise and analyse offender debriefs and NCA intelligence to help identify motivations and pathways into cyber crime.
- Review academic studies in this area.
- Use this understanding to identify key intervention points where NCA resources should be targeted.
- Identify gaps in understanding and propose recommendations.

This report concerns pathways into cyber-dependent[1] crime. Cyber-dependent crimes (or 'pure' cyber crimes) can only be committed using a computer, computer networks or forms of information communications technology. The NCA's National Cyber Crime Unit focuses on cyber-dependent crime.

Initial Findings

- A number of UK teenagers who we assess as unlikely to be involved in traditional[2] crime are becoming involved in cyber crime.
- To date there has been no socio-demographic bias amongst offenders or those on the periphery of criminality.
- Availability of low-level hacking tools encourages criminal behaviour.
- Autism spectrum disorder (ASD) appears to be more prevalent amongst cyber criminals than the general populace though this remains unproven.
- Offenders begin to participate in gaming cheat websites and 'modding' (game modification) forums and progress to criminal hacking forums without considering consequences.
- Financial gain is not necessarily a priority for young offenders.
- Completing the challenge, sense of accomplishment, proving oneself to peers is a key motivation for those involved in cybercriminality.
- Offenders perceive the likelihood of encountering law enforcement as low.
- Cyber crime is not solitary and anti-social. Social relationships, albeit online, are key. Forum interaction and building of reputation drives young cyber criminals.
- Positive opportunities, role models, mentors can deter young people away from cyber crime.
- Targeted interventions at an early stage can steer pathways towards positive outcomes.

[1] 'Cyber-dependent' definition from McGuire, Dr. Mike and Dowling, Samantha. *Cyber Crime: A Review of The Evidence.* Home Office, 2013, Report 75.

[2] 'Traditional' crimes are regarded as those typically recorded within Home Office police recorded crime and are generally thought of as committed in offline environments, for example, theft, fraud, sexual or harassment offences.

Intelligence base

Debriefs

Until recently there has been limited intelligence sourced directly from cyber criminals arrested by the NCA and UK law enforcement in general. The NCCU Prevent team has begun to conduct extensive behavioural debriefs with former cyber criminals.

Eight debriefs of individuals involved in cyber criminality have been undertaken so far. They have all been subject to a caution, community sentence or imprisonment. All debrief subjects were interviewed with their full knowledge and consent as to the purpose of the interview.

The debriefs followed a semi-structured format with the lead officer guiding the conversation whilst allowing the subject to describe their journey into cyber crime in their own words.

This interview structure is the most satisfactory tool for gaining detailed information where the topics being discussed were open-ended in terms of the range of possible answers.

Cease & Desist Visit Intelligence Collation

Over 80 cease & desist visits have been co-ordinated or carried out directly by NCCU Prevent since November 2013. The aim is to visit individuals who have been identified as being involved in the fringes of cybercriminality and advise them to desist their activities.

NCA has attempted to use these visits as a tool to collect qualitative intelligence from the individuals visited. Officers conducting visits have been provided with questions to ask subjects regarding their background, motivations and behaviours in this area. The data offers insight into the behaviours or those on the periphery of cyber crime.

It is important to clarify that those visited are not cyber criminals. They have not been through the criminal justice system and are not guilty of any offences.

Limitations

The debriefs undertaken and the cease & desist visit interviews completed have relied fully on voluntary participation by the subjects. It is not possible to corroborate the qualitative aspects of the responses given.

Debriefs have only been conducted with a subset of cyber-dependent criminals, those who have been caught and/or arrested and those who agreed to be interviewed.

Debriefs only occurred with offenders from the UK, so it is not possible to extrapolate the findings to other countries without further research.

The intelligence collection period for this report is November 2013 to April 2016.

Confidence Statement

We have medium confidence in our assessment that financial gain is not necessarily a prime motivation for young UK cyber offenders. This is due to the difficulty in corroborating self-reported offender motivations. We assess there is no reason to doubt the veracity of debriefs, details have been corroborated where possible and have been shown to be accurate accounts.	**Medium**
We have medium confidence in our assessment that early intervention can change the course of offending. Although reported by many ex-offenders to be a key driver in their desistance we cannot rule out other factors.	**Medium**
We have high confidence in our assessment that a number of UK teenagers who would not otherwise be involved in 'traditional' crime are becoming involved in cyber crime. This is due to extensive experienced officer feedback and lack of previous convictions or records amongst UK cyber offenders.	**High**

Introduction

Young People & Entry into Cyber crime

Cyber crime attracts young offenders. 61% of hackers begin hacking before age 16[3]. The average age of suspects and arrests in NCCU investigations in 2015 was 17 years old[4]. The average age of arrest of those involved in NCA drugs cases in 2015 was 37 and the average age of arrest of those involved in NCA economic crime cases in 2015 was 39 years old[5].

The skill barrier to entry into cyber criminality is lower than it has ever been. Off-the-shelf hacking tools, which require very limited technical expertise to utilise, are available at little to no cost for the user.

Many illegal products are advertised openly on low level hacking or gaming forums. Video guides and step by step tutorials on how to use these products are readily available on the open web.

[3] F. Bosco (2012), Hackers' Profiling Project, UNICRI

[4] Suspect data used because of insufficient arrest data.

[5] Figures compiled from NCA PPR Performance Team.

These circumstances have created an environment in which more young people are becoming involved in cyber crime.

Emboldened by a perceived anonymity and lack of visible law enforcement presence online, lower level cyber criminals can continue to progress their offending unchecked. The debrief analysis below has shown that many offenders cross from non-criminal online behaviour into outright illegality without considering or fully comprehending the transgression and its consequences.

Only a small number of low-level cyber criminals will go on to reach the higher level of the very technically skilled cybercriminal. Nonetheless, it is important to note that the proliferation of off-the-shelf hacking tools and services has brought the ability to cause significant harm within reach of the young and relatively unskilled cybercriminals.

Example

The DD4BC group extorted money by DDoS-ing a company's website and then issuing a demand to pay a fee or the DDoS attacks would continue. The extortion group did not have their own botnet infrastructure in place but were actually using commonly available DDoS/booter services to launch attacks.

Academic Literature Review conclusions

A limited academic literature review is contained in Annex A.

Limitations

The UK government delineates between cyber-dependent and cyber-enabled offences. This distinction is not usually recognised or adopted by academia, and there is little consensus as to the agreed definition of a cybercriminal. Many academics will create their own taxonomy of cybercriminality at the outset of their studies.

Conclusions

Although it may be difficult to draw conclusions from such disparate studies, several key findings emerge:

- Conquering the challenge, proving oneself to the group and intellectual satisfaction are more important motivations than financial gain, though this may change over time if the subject continues their criminal hacking.
- Offenders consider the risk of being caught as low.
- Many offenders see criminal hacking as a victimless crime.
- Deterrence and early interventions can have an impact on this target group.
- Although a link between cyber crime and autism spectrum disorder is suspected this has yet to be proven.

Analysis of Cease & Desist Intelligence

NCCU has co-ordinated national intervention campaigns targeting individuals involved in, or on the periphery of cyber crime but who have been judged not to meet the threshold for arrest.

Cease and desist visits entail a face to face meeting with officers, who outline the individual's alleged connection to criminality and then warn and advise the individual to cease and desist their activities or face potential consequences relating to the associated offences.

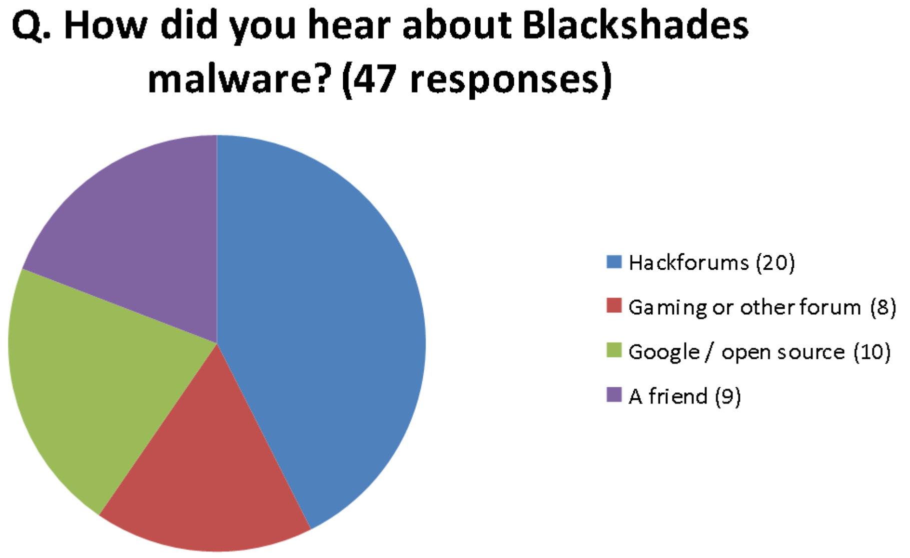
Over 80 cease and desist visits have been carried out or co-ordinated by NCCU since November 2013. In addition to serving cease and desist notices, officers were asked, where possible, to gather qualitative intelligence regarding motivations and pathways into subjects' activities. NCCU Prevent team provided a number of questions for the attending officer to answer.

The focus of the questions differed in each operation:

- For Operation DERMIC officers were tasked with finding out how the subjects had become aware of the Blackshades RAT.
- For Operation VIVARIUM the officers were asked to ascertain how the subjects first became interested or involved with computers and technology.

Operation DERMIC – 2014

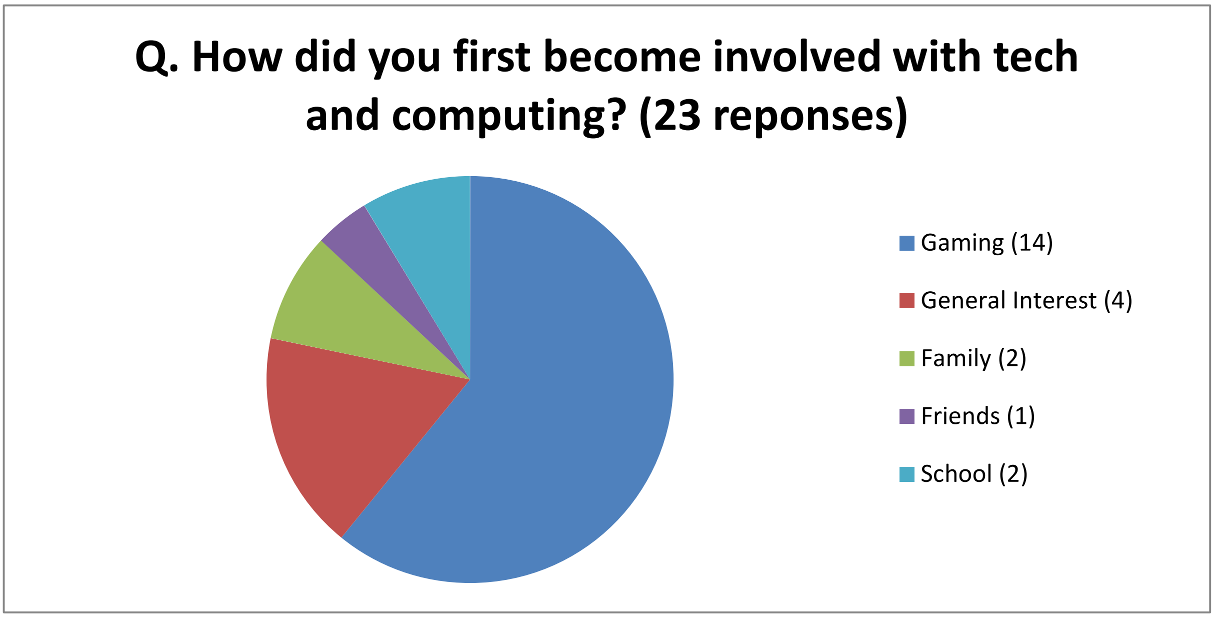
Operation DERMIC was an investigation into the customers of Blackshades malware. Blackshades was a Remote Access Trojan with a variety of malicious features that allowed users to take control of a victim's computer and then steal data or manipulate computer functions at will (e.g. view and record victims webcam). The customer list was triaged based on the amount and seriousness of the malware purchased and deployed. There were 21 arrests in the UK. Cease & desist visits were carried out across the UK by NCCU and Regional Organised Crime Unit (ROCU) officers.



Blackshades was an explicitly criminal set of tools and services. The purpose of asking customers this question was to ascertain how users became aware of the existence of this criminal tool and how accessible it was to the average internet users. As the results illustrate, the majority of users (60%) learned about Blackshades on a forum (71% of these on one specific site, Hackforums.net). 21% individuals found out about Blackshades by searching the internet for information on a particular service that then linked them back to the Blackshades product. 19% of users claim they wanted to buy the product after hearing about it from a friend.

Operation VIVARIUM – 2015

Operation VIVARIUM was an investigation into the customers of Lizardstresser.su, a website offering a DDoS-for-hire service. Customers were triaged based on the amount of money they had spent on the service and number of times they were seen to have used the service to launch DDoS attacks. In the UK, six people were arrested and 28 cease & desist visits have been completed. The average age of those visited was 19 years old.



The results reinforce the debrief intelligence, illustrating that the majority of those engaged in, or on the periphery of, cyber crime, become involved via an interest in computer gaming. We assess that it is likely that these results would be replicated across all UK individuals engaged in cyber-dependent criminality.

Education, Industry & Positive Pathways

Children in the UK are being encouraged to learn more about programming and technology, which NCA sees as a positive change. Any NCA activity or any law enforcement message should make it clear to parents and young people that an interest and aptitude for programming and technology is beneficial, for them personally and for the UK as a whole. The UK needs creative and skilled cyber professionals.

CREST workshop[6]

In September 2015 NCCU hosted CREST (the ethical security and penetration testing industry body) and security specialists from CREST member companies. The workshop was convened so that NCCU could draw on the experiences and knowledge of attendees, to improve understanding of the motives of young people who might move from an interest in coding and gaming to hacking and illegal activities.

Several of the attendees admitted that they had been involved with or on the periphery of cyber crime earlier in their lives. All participants said that at some point in their lives someone had made a positive intervention of the kind that helped them move into the

[6] www.crest-approved.org/wp-content/uploads/CREST_NCA_CyberCrimeReport.pdf

cyber security industry; and that without this intervention they may not have realised that such a career was possible. Some suggested that they might otherwise have been tempted towards illegal activity online.

Participants cited the importance of role models, at school and in their personal lives, who had proved to be positive influences, recognising and encouraging their talent and helping them find the path that eventually led to their current roles. Many also acknowledged the importance of education in helping them enter the industry.

Participants were asked what they thought were the key motivations, characteristics and influences of people engaged in cyber crime:

- A sense of belonging through hacking forums and online communities.
- A desire to prove oneself to the group.
- A desire to improve one's skills, to solve the difficult problems.
- Financial gain is often only a secondary motivation.
- Some young people may also want to use their skills to further political ends.
- Often the main motive for doing something illegal is simply that it presents an interesting challenge.

Conclusions

Conclusions have been drawn from the analysis of the offender debriefs (detailed transcripts are contained within the annex), cease and desist intelligence gathered, a review of the academic literature, and engagement with law enforcement and industry partners.

A number of UK teenagers (overwhelmingly male[7,8]) who we assess as unlikely to be involved in traditional crime are becoming involved in cyber crime. Experienced officer feedback has indicated that those involved in cyber-dependent criminality in the UK would not be the type of individuals who would engage in offline, traditional crime, such as theft or burglary.

To date there appears to be no socio-demographic bias amongst offenders. Debriefs have taken place with people from various financial and demographic backgrounds. This finding is mirrored in the 80+ cease & desist visits carried out by officers since 2014. A more detailed approach to investigating this finding will form part of future research work.

Very little skill is needed to begin criminal activity online. With tools such as booters and Remote Access Trojan (RAT) users can make a small payment (or often no payment) and begin breaking the law. The ready availability of step by step tutorials and video guides only make the transition into criminality easier. As outlined in the debriefs, once the law is broken, subsequent transgressions become easier.

Autism spectrum disorder appears to be more prevalent amongst cyber criminals than the general populace, though this remains unproven. Anecdotal evidence from the officers arresting and interviewing those involved in cyber-dependent cases has often led to suggestions that ASD is more prevalent amongst cyber criminals. The

[7] 94% male, Bosco, F., 2012. *Hackers' Profiling Project,* s.l.: UNICRI.
[8] No females have been arrested by NCCU for cyber-dependent crime as of February 2016.

Ledingham & Mills paper points to clear reasons that may support the connection, but concludes that more research is needed.

A large proportion of offenders begin to participate in gaming cheat websites and 'modding' (game modification) forums and progress to criminal hacking forums. As outlined in the debriefs and reinforced in cease & desist responses, a common pathway into cyber criminal activities is via online gaming cheat and modding forums.

Financial gain is not necessarily a priority for offenders. Industry interviews, debriefs, and academic literature suggest that money is not the sole or even key driver of behaviour in the majority of UK offenders. However, financial motivation should not be discounted. The rise of off-the-shelf hacking tools that can be used to make money illegally may lead to a rise in low-skilled offenders who are involved in cyber crime purely for financial gain.

Completing a challenge, a sense of accomplishment and proving oneself to peers are key motivations for those involved in cybercriminality. These factors are repeated throughout the debriefs and academic literature, as the main reason young people begin and continue hacking. An 18 year old who was arrested for obtaining unauthorised access to a US government site said *'I did it to impress the people in the hacking community, to show them I had the skills to pull it off…I wanted to prove myself…that was my main motivation'.*[9]

Law enforcement activity does not act as a deterrent, as individuals consider cyber crime to be low risk. Illegal activities are discussed openly on many open forums. Forum users offer guides and tips for new users. The law and its consequences are rarely discussed and if the topic is raised it is generally dismissed. Debrief subjects have stated that they did not consider law enforcement until someone they knew (or had heard of) was arrested. For deterrence to work, there must a closing of the gap between offender (or potential offender) with law enforcement agencies functioning as a visible presence for these individuals.

Cyber crime is not solitary and anti-social. Social relationships, albeit online, are key. Forum interaction and building of reputation scores drives young cyber criminals. The hacking community (based largely around forums) is highly social. Whether it is idolising a senior forum member or gaining respect and reputation from other users for sharing knowledge gained, offenders thrive on their online relationships. The debriefs highlighted the sense of value that some offenders felt by demonstrating their technical prowess for the group. This in turn helped to fuel their drive and desire to learn and accomplish more.

Positive role models, mentors and opportunities are key to deterring young people away from cyber crime. Debrief subjects lacked a positive role model who could steer them towards a positive pathway. Role models will often be the cyber criminal at the top of ladder the young people are trying to climb. Ex-offenders who managed to cease their activities and gain an education or career in technology have credited this change to a positive mentor, or someone who gave them an opportunity to use their skills positively.

[9] Pattenden, Mike 2015, 'The Biggest Teenage Hackers'. *The Times* October 29

Targeted interventions at an early stage can steer potential offenders towards positive outcomes. Several interviewees stated that an early intervention by law enforcement would have forced them to rethink and make them realise that their online world had real world consequences. A CREST workshop participant commented that in criminal forums there was an air of invincibility. The participant felt that any engagement with law enforcement would have left a lot of forum members very surprised and concerned.

Proposals for further activity:

Four recommendations to enhance the pathway report findings for future versions:

1. **More offender debriefs needed:** A continued programme of offender debriefs is needed. This will either back up the conclusions made in this report or offer new insights into the pathway into cyber crime. NCCU working with ROCUs to actively seek debrief subjects and will continue to document its findings.

2. **Increased international partnership working:** NCCU needs to work with international law enforcement partners to share debriefs and knowledge gained from reports such as this. Can lessons learned from this report be used to reduce the international threat to UK? Are potential intervention points the same as in the UK? Is the pathway outlined in this report transferrable to other countries and cultures?

3. **In-depth autism study to take place:** The anecdotal evidence regarding autism spectrum disorder is not sufficient to infer any link or association between ASD and cyber crime. A more in-depth study is underway by Rebecca Ledingham and Bath University in conjunction with the Research Autism charity. NCCU will be offering support and findings will be fully integrated into any future pathway reports.

4. **Utilise expertise of academia to further research:** NCCU is in the early stages of engagement with a small number of universities. The aim is to test the conclusions in this report to thorough academic standards and improve and alter the methodology and conclusions where necessary.

Key recommendations following from the conclusions drawn:

1. **Continue and increase volume Prevent activity:** NCCU Prevent should continue to conduct and mainstream volume Prevent work with ROCUs and police forces. This would include cease & desist visits, letters, and emails with those on the periphery of cyber crime. The academic literature review and the debriefs confirm that perception of the risk of law enforcement intervention remains low in the criminal hacking community.

2. **Increase law enforcement presence in entry-level criminal forums:** As shown in the debriefs and the cease & desist intelligence analysis, such forums play a key role in the development of young cyber criminals. Illegal activities and services are discussed and exchanged openly.

3. **Degrade the marketplace for ‘gateway’ criminal services:** Services such as ‘booters’ and ‘RATs’ should be seen as gateway hacking tools. NCCU needs to continue to develop methods to combat the marketplace for these tools.

4. **Work with the video gaming industry to deliver Prevent activity:** It is clear that the majority of cyber criminals, or those on the periphery of cyber crime, are also online gamers (as the cease & desist analysis shows, many got into computing and technology via their interest in gaming). This, of course, does not mean all gamers are cyber criminals. GameTrack estimate that 40% of the UK population play video games[10]. Current statistics concerning the US population shows that 49% play video games, although only 10% of this group identify as ‘gamers’[11] (we judge it very likely that these numbers would be replicated in the UK). Targeting Prevent communications at the UK version of this 10% who identify as ‘gamers’ could be an effective way of spreading awareness of cyber crime and its consequences, as well as signposting positive alternative pathways available. NCCU Prevent have set up a project that aims to build partnerships and deliver Prevent activity with the video games industry.

5. **Improve cyber crime resources available for schools and teachers in UK:** Better, earlier, education on cyber crime and its consequences, cyber ethics, victims is needed in the UK. Current curriculum provision and teacher knowledge is limited. NCCU Prevent proposes setting up an education advisory board with key stakeholders to help develop and deliver content for schools and teachers.

6. **Create a toolkit of positive diversions that can be made available to young people on the periphery of offending:** As the workshop with CREST and industry professionals showed, a positive mentor or positive opportunity at a young age can make the difference and steer at-risk individuals away from cyber crime and towards a successful education or career in the tech industry. There are many positive diversions currently available, from the national Cyber Security Challenge to local coding clubs or industry sponsored internships. NCCU Prevent is working to catalogue these and create a toolkit of appropriate diversions that Prevent subjects can be signposted towards. In addition to this, NCCU are working with industry and academia to set up specific positive diversion options as required. These options could also be used to prevent re-offending.

Annex A

Analysis of offender debriefs

Subject 1 - Sold DDoS tools and Botnet services. Member of hacking collective.
Subject 1 became interested in gaming when he was 13 years old. He played Call of Duty on the Xbox and was not initially interested in using a PC.

He would search out and share cheats for Xbox games. Subject 1 spent a significant amount of time on a popular gaming forum and community website. He became

[10] GameTrack Digest Quarter 1 2016
[11] Duggan, Maeve. ‘Gaming and Gamers.’ Pew Research Center. December 2015.

interested in 'modding'[12] and would identify new cheats and hack for games.

‘...sharing this knowledge gave me credibility and popularity.’

Subject 1 enjoyed meeting other gamers and enjoyed building his credibility with them. He was motivated to build a good reputation in his gaming community. He began to frequent more forums, including Hackforums.net[13].

‘I was driven by my curiosity, I wanted to understand the best modifications and cheats.’

During one interaction on a forum Subject 1 got into an argument with a fellow user over a game, which led to the individual disrupting Subject 1's internet connection. Subject 1 was motivated to understand how this could be done so began to research what software was required to take fellow gamers offline. He found a 'booting' programme and began to use it. Subject 1 watched tutorials on Hackforums and YouTube to learn how to use the software. He began to spend an increasing amount of time on Hackforums.net.

Once he had mastered the booting software he began to learn about Remote Access Trojans. Subject 1 said Dark Comet was very popular on Hackforums and very easy to get hold of. Subject 1 also wanted to learn about botnets and how to build them. He started building IRC botnets and would provide bots for other users. He progressed onto how to use servers to grow botnets.

As his proficiency increased, Subject 1 began to help other members of hackforums.net develop their skills. He said he felt this allowed him to earn trust and respect on the forums and he liked the feeling he got when he helped others learn. His reputation score grew as he provided more advice and services for other users.

‘...the more my reputation increased, the more I felt I could interact with the smarter members’.

Subject 1 claims that users never discussed criminality or the consequences of crime.

‘...there was a relaxed atmosphere. We felt at ease discussing botnets and other hacking tools’.

Subject 1 was learning legitimate skills, such as web hosting, while he was engaged in his illicit hacking activities. He claims that he began to help web hosting companies address weaknesses in their systems. Subject 1 again claimed that he was not motivated by money but by an appetite to perfect his skills.

Subject 1 looked up to a senior user on Hackforums because of his high reputation. They had lots of conversations online and the senior user offered to teach Subject 1 and give him access to the closed forum he ran. In return, Subject 1 helped to

[12] A mod or modification is the alteration of content from a video game in order to make it operate in a manner different from its original version.

[13] www.hackforums.net is the largest entry-level forum with over 5 million messages. It provides users with information on gaming, computers and hacking tutorials. Hackforums users are given reputation scores based on their contributions and interactions on the site.

maintain botnets for the senior user. Subject 1 got paid a small amount for this role.

‘*...it was more interesting than working for a company...it gave me a feeling of power.’*

Subject 1 did not think about potential victims and felt removed from any consequences. He said that he did not think what he was doing was criminal and did not worry about law enforcement. The volume of people engaged in similar activity seemed to make it acceptable to him.

‘...there were so many others doing the same thing.’

The first time he recognised that he was involved in crime and that there may be consequences for his actions was when he saw the media reporting around Blackshades (a Remote Access Trojan – 21 arrests in UK).

Subject 1 claimed a warning from law enforcement would have made him stop his activities. He felt that there should be more regulation of forums like Hackforums.net.

Subject 2 – arrested for Computer Misuse Act 1990 offences

Subject 2 claims his initial desire was to learn and increase his knowledge for its own sake. He claims he had no desire for financial gain and just went on forums to answer questions that other members had asked.

‘I get a bee in my bonnet trying to understand how things work.’

Subject 3 – Convicted of Computer Misuse Act offences against large corporations and government agencies

Subject 3’s interest began when he was aged 8. After his father bought him a computer subject 3 would spend most of the day playing games. He became interested in coding and by age 14 was finding vulnerabilities in websites, and eventually began to commit cyber crime.

‘...sometimes law enforcement was discussed in forums but people didn’t care about the consequences.’

Subject 4 – Jailed for Fraud Act offences – Moderator of criminal forum

From the age of 11 Subject 4 was fascinated with how computers worked. Over a period of time he rose to be the moderator in a criminal services forum. Subject 4 said he would never think of stealing a bag or wallet in the real world but he thought the chances of getting caught were low.

‘With the anonymity I thought I was invincible.’

Subject 5 – recruited by senior hacker to assist criminal activities

When Subject 5 was 14 years old he had stopped going outside and spending time with friends so that he could game online. Due to gaming cheats and modding learned in forums he became so good that he lost interest in games and moved onto other hacking forums. He became a moderator of one such criminal forum. Subject 5 says he did not consider the consequences of what he was involved in.

‘...I had built up my computer world to be my main focus, it was an alternative to the real world.’

Subject 6 – jailed for Computer Misuse Act offences

Subject 6 was not interested in online gaming but he was obsessed with becoming a ‘hacker’ from a very young age. He spent hours and hours on various forums learning and honing his skills. Form the beginning Subject 6 claims to have been motivated by the technical challenge of any particular problem. He was manipulating and creating malware because it interested him.

‘I didn’t recognise the term “malware”, it was just programming of code for a purpose.’

Subject 7 – jailed for Computer Misuse Act 1990 and Fraud 2006 offences.

Subject 7 became interested in computers after lessons at school aged 9. He played games on the family computer and learned about cheats online to enhance his playing ability.

He was suspended from school at age 13 for gaining admin rights to the computer system in order to upload games for his fellow pupils to play.

‘…it made me popular, I enjoyed the feeling’.

Curiosity and an urge to learn about how online processes worked drove his interest. At age 14 Subject 7 was spending a significant amount of time on the computer.

‘My mum was happy that I wasn’t out on the streets all day and night’.

Subject 7 used online tutorials to increase his knowledge of code and programming. Frequenting gaming forums learning cheats led him to Hackforums. He began to learn about hacking and botnets. After some time he paid to access VIP areas, and similar, forums.

After high school Subject 7 began an NVQ in web design but found it hard to focus and felt unchallenged. He kept up his interest in gaming, cheats and game bots and said this interest outweighed his interest in the legitimate training he was receiving.

Subject 7 worked odd jobs but was increasingly spending time up to 70% of his time online. He claims his aim when frequenting hacking forums was to increase his reputation score.

‘I looked up to those users with the best reputations’.

As his skills increased over time he said he was motivated to become a better hacker than his rivals. He would 'nag' other users within the forums for information on different tools and ways of infecting other users.

Subject 7 claimed he did not think about the offences he was committing and was not overly concerned about any law enforcement presence. He did not think he would be targeted or caught for using botnets. The more he became involved in 'darker' cyber activity he did say that his perception of risk increased. He did seem to be slightly confused about what was legal and what was illegal. Subject 7 did not speak about his online activity to people offline.

‘I didn’t consider victims, you don’t see real people behind it [his criminal actions]’.

Subject 8 – jailed for Computer Misuse Act offences.

Subject 8 got his first family computer aged 10 and was immediately fascinated. He wasn't interested in school and when he did show up he wouldn't pay attention. He said most of what he learnt was from online searches in class.

Subject 8 enjoyed playing online games against people around the world. Through online forums he met people who would cheat on games by modding them. He wanted to be able to have these skills and began to learn about programming. By the age of 13 he had self-taught the skills required to be able to reverse engineer most games.

Subject 8 was participating in forums, where he learnt that all software, like games, had bugs that could be manipulated. He started to speak to other people online who were also interested in the weaknesses of software. A fellow forum member introduced him to Remote Access Trojans.

'…money was not a motivation. I just wanted to use the tools to prank and joke around with people'.

Forums were competitive and addictive environments and subject 8 felt his knowledge was good. People would post problems to solve and it would be a race against each other to see who could come up with the solution first. Subject 8 said that sometimes people would offer money for these solutions, but he wasn't interested in that side of it.

Although he spent all his time in his room, subject 8 says his parents were happier that he was in the house because it was better than being out on the streets or in a gang. His parents had no idea about his online actions, his online life was secret. He liked being online cause nobody could see or judge him and he could be whoever he wanted.

Subject 8 claims that the boundary between legal and illegal online activity was blurry for him. There were different 'underground' groups in the cyber community and they would all hack and prank each other.

'…I was aware that some of what we were doing was illegal but because they were all doing it I never really thought about the law or police.'

An example of the kind of pranks he would do is 'swatting'[14], an attempt to get armed police to arrive at the home of a rival believing there to be a critical incident underway.

Subject 8 said that with hacking, once you've broken the law it gets easier to do so. The next time you think 'what does it matter?' He said there was a feeling of invincibility and that he was always chasing the next hacking high.

'I thought "no one is coming for me", everyone was doing it and getting away with it.'

Subject 8 says that cybercriminals feel detached from their crime, with no feeling or

[14] 'Swatting' is the act of deceiving an emergency service (via such means as hoaxing an emergency services dispatcher) into dispatching an emergency armed response to the victims address based on the false report of an ongoing critical incident.

understanding of the consequences to the victim. He felt that defacing a website and pranking is not seen as the same as defacing or vandalising something in the offline world.

In the online communities that Subject 8 was part of, the perception of the police's effectiveness in combatting cyber crime was low.

'…the general opinion was that police don't have the time or level of understanding of cyber for us to worry about.'

Subject 8 said law enforcement is still way behind and only scratching the surface of what goes on online.

After being released from prison Subject 8 has found difficulty attaining employment in cyber security because there is a trust issue.

Subject 8 thought a visit from law enforcement officers at an early stage would have been the best method to make him stop his activities. He also claimed that coding and programming educational opportunities or scholarships would have helped him by providing an outlet for his skills and interests.

Academic Literature Review[15]

Young *et al.* (2007)[16]
Researchers conducted interviews with attendees of the DefCon convention in Las Vegas. DefCon is the largest hacking convention in the world. They found that criminal hackers continued to engage in their activities, despite their knowledge of the severe judicial punishment if apprehended. The criminal hackers believed that there was a low chance of this punishment occurring. (Kirwan & Power, 2013) conclude this is of note as *'severity of punishment has little effect when the likelihood of punishment is low (Von Hirsch et al., 1999) whereas increased likelihood of punishment has been found to work as a deterrent (Killias et al., 2009).'*

Young *et al.* also found that hackers thought the gains from hacking outweighed the potential losses and that this would have to be reversed if offending was to be curbed.

An advanced model of hacking, Rennie and Shore (2007)[17]
Rennie and Shore found that early intervention to highlight the consequences and criminality of illegal hacking could reduce its attractiveness to children. Law enforcement could begin identifying the 'early signs' of hacking behaviours and intervening with potential offenders, offering written warnings or 'acceptable behaviour' contracts.

Rennie and Shore state that inexperienced hackers embarking on a criminal career could be put off if the availability of entry-level hacking tools was reduced.

[15] Cybercrime: The Psychology of Online Offenders (Kirwan & Power, 2013) was used to identify multiple studies applicable to cyber-dependent crime for this study.
[16] Young, R., Zhang, L. and Prybutok, V. R. (2007). Hacking into the minds of hackers. *Information Systems Management,* 24, 281-7.
[17] Rennie, L. and Shore, M. (2007). An advanced model of hacking. *Security Journal,* 20, 236-251.

A Sociology of Hackers, Jordan & Taylor 1998[18]

As summarised by Raoul Chiesa et al[19] Jordan and Taylor conclude that the most common motivations lead back to a compulsive attraction to hacking, intellectual curiosity, strong feelings of control/power, and finally the satisfaction derived from the feeling of belonging to a group. The authors conclude that *'the motivations behind hacking seem to lead back to a sort of intrinsic motivation; in other words, the tendency to engage oneself in tasks that are gratifying in themselves are interesting, and can be viewed as a challenge.'*

The Risk Propensity and Rationality of Computer Hackers by Michael Bachmann, TCU, 2010[20]

The study surveyed hackers[21] to see if their rationality and propensity for risk was the same as the average population.

Bachmann found that hackers had a significantly higher than average rationality value compared to the general public. Hackers also reported a significantly higher confidence in the experience-based decision making measure. The study found that hackers prefer a more analytical and rational thinking style than the average person, displaying a higher confidence in their ability to make decisions.

Bachmann's study suggests that effective deterrence might be an effective strategy in dealing with highly rational offenders. Bachmann says *'it is unfortunate that present efforts to curb cyber crimes are not suited to exerting a pronounced deterrence effect'.*

Jonathan Lusthaus, Director, The Human Cyber Criminal Project, Nuffield College, Oxford

In Electronic Ghosts (2014)[22] Lusthaus says that it is vitally important that younger people are taught about the reality of their actions in the virtual world: '*It is something that many cyber criminals often realize too late: Their victims are real, as are the consequences of illegal behavior.'*

Cyber crime Trajectories: An integrated theory of initiation, maintenance and desistance. Alice Hutchings, Computer Laboratory, University of Cambridge[23]

Hutchings does not support the cyber-enabled/cyber-dependent distinction and instead postulates two pathways into cyber crime; the General and the Technical. The technical pathway would include the NCCU's target group and encompass both cyber-enabled and dependent criminals.

Hutchings states that the technical pathway is male-dominated (less than 5% female). McQuade (2006b) examined students' perceptions of being caught for a variety of technology enabled crimes. Respondents believed the likelihood of detection was low, and the punishments for those caught were not severe. In addition, McQuade states

[18] Jordan, T and Taylor, P. (2008). A sociology of hackers. *The Sociological Review*, 46, Issue 4, 757-780.

[19] Chiesa, R. and Ducci, S. and Ciappi, S. (2008). Profiling Hackers: The Science of Profiling as Applied to the World of Hacking.

[20] Bachmann, M. (2010). The risk propensity and rationality of computer hackers. *International Journal of Cyber Criminality,* 4, 643-656.

[21] 'hacker' here means someone who has done a number of technical intrusions, malware distributions etc.

[22] Lustahus, J. (2014) . Electronic Ghosts. *Demcracy: A journal of ideas.,* 31.

[23] Hutchings, A. (2016). Cybercrime trajectories: An integrated theory of initiation, maintenance, and desistance. *T. J. Holt (ed), Crime Online: Correlates, Causes, and Context* 117-140.

that physical removal from the victim allows the offender to deny injury or deny the victim with ease:

‘since they cannot see the Internet or the people who create content, victims, if they are contemplated at all, become faceless entities, computer systems, or perhaps corporations rather than real people whose livelihoods and wellbeing are compromised…’.

Hutchings states that offenders perceive the likelihood of detection as low, and this holds greater weight than the harshness of available punishments. Benefits obtained from those engaged in technical offences include skill development, fun and excitement, social status, power and sexual gratification.

Hutchings says that an interest in gaming and technology can expose potential offenders to the types of online communities that share the information needed to commit cyber crime. This can lead to ‘cyber crime by association’.

Hutchings concludes - '*Although offenders perceive the potential penalties as severe, they have a low opinion about the ability of law enforcement to investigate these matters. They see the chance of detection as being low. Therefore it is the likelihood of detection, rather than the severity of punishment, that is likely to have the greatest effect on offending. Offenders cease their activities when they gain meaningful work or enter a relationship, reflecting the increased cost of their actions on their lives.*'

Handling Instructions

This report is publicly available. There are no special handling requirements and permission is not required prior to further distribution.