Magdeburger Journal zur Sicherheitsforschung

Gegründet 2011 | ISSN: 2192-4260
Herausgegeben von Stefan Schumacher
Erschienen im Magdeburger Institut für Sicherheitsforschung
http://www.sicherheitsforschung-magdeburg.de/publikationen/journal.html

This article appears in the special edition »In Depth Security – Proceedings of the DeepSec Conferences«.
Edited by Stefan Schumacher and René Pfeiffer

Without a Trace

Cybercrime, who are the Defendants?

Edith Huber and Bettina Pospisil and Walter Seböck

Since 2006, cases of computer crime in Austria have been recorded in official crime statistics under the collective term »Cybercrime«. While the authors also analysed the solved cybercrime cases of the last ten years (2006 - 2016) this article focuses on the unsolved cases which occurred during this period. Thus, those cases in which the Vienna Criminal Court did not reach a verdict are analysed through a file analysis conducted by an interdisciplinary team. The aim of the article is to gain more insight in the phenomenon cybercrime. Special focus lies in the actors of cybercrime (offenders and victims) as well as the heterogeneous approaches and motivations of offenders.

Keywords: Cybercrime, Law, Unsolved Cases

Citation: Huber, E., Pospisil, B. & Seböck, W. (2019). Without a trace: Cybercrime, who are the defendants? *Magdeburger Journal zur Sicherheitsforschung*, *17*, 938–942. Retrieved June 29, 2019, from http://www.sicherheitsforschung-magdeburg.de/uploads/journal/MJS_063_Huber_Cybercrime.pdf

1 Introduction

If we look at the past 12 years, we can see that cybercrime cases are on the rise. For example, the Austrian crime statistics for 2006 counted 3,257 reported cases. Ten years later, in 2016, there were already 16,804 reports (Federal Ministry of Interior 2018). It should be kept in mind, that the phrase ›cybercrime - offense‹ can only be described based on its context, since its description is always dependent on the respective legal framework of the state. Regarding traditional offences, there is no misunderstanding as to what this could mean in concrete terms. For example, it is clear to everyone what a murder or a car theft is. In the case of cybercrime, things look a little different.

Basically there are two types of cybercrime:

Type 1: Cybercrime in the narrower sense (Core Cybercrime or Cyberdependent Crime)

This definition includes all offences that do not exist offline in any variant. This category of cybercrime includes attacks against the confidentiality, integrity and availability of networks, devices, data and services in these networks. These include hacking, cybervandalism, virus spreading, etc.

Type 2: Cybercrime in the broader sense (Non-cyberspecific Cybercrime or Cyberenabled Crime)

Offences that fall under this category can also exist offline. These include offences such as credit card misuse, information theft, money laundering, copyright infringement, cyberstalking and the use, distribution and making available of child pornography, etc. (McGuire, Dowling 2013).

However, these definitions always refer to the national context and must therefore always be considered within the legal and cultural framework. Europol has started an attempt to define a common description for cybercrime:

a. The intensity of cybercrime depends on cultural, legal, economic and regional factors;

b. Traditional methods of fighting crime are no longer effective here. Electronic ›evidence‹ is often spread across several places in the world, making it difficult to find the perpetrators;

c. In a world of cloud computing, the legislature will have to consider what evidence could be used to convict offenders in order to ensure effective prosecution;

d. Harmonisation of national laws is needed to facilitate prosecution in an international environment, and

e. Cybercrime prevention must be a priority in all countries (UNODOC 2013).

In many cases, the offenders could not be caught. This can also be seen regarding the cybercrime cases in Austria. In the next sections, the authors are offering a closer look into the unsolved cybercrime cases in Vienna.

2 Research design and methodical approach

The aim of this project was, to gather new information about the unsolved cases of cybercrime and the current situation in Austria (Vienna). Therefore, the research questions focus on the actors as well as on the procedures and techniques, which the players used. In this article, the authors focus on one subarea of findings: the actors of cybercrime.

The research questions - which is dealt with in this article – are the following two:

1. Who are the defendants of cybercrime?
2. Who are the victims of cybercrime?

To answer these research questions, the authors conducted a court file analysis (Dölling, 1995) of the offenses prosecuted at the Vienna Criminal Court between 2006 and 2016. Therefore, all cases that fit into the legal framework[1] of a cybercrime case were taken into account. Regarding these paragraphs 5408 cases got prosecuted between 2006 and 2016 at the Vienna Criminal Court. When, in a first step, excluding the 399 solved cases, there are 5009 unsolved cases left. In a second step, the research team excluded the cases of identity theft and the – for different reasons - not valid cases. After choosing a sample of 20% the research team ended up with 88 cases with 128 defendants in it.

3 Findings

The defendant

When taking a closer look at the defendants in the unsolved cases, it is obvious, that a huge average of them stays unknown (63%). This is one of the main reasons, why these cases cannot be solved. Regarding the cases where the defendant is known, it is possible to paint a picture of an »ideal-type« (in a statistical sense) of defendant. Commonly he is male and single. He is about 34 years old and an Austrian citizen. In most of the cases, the defendant has no previous conviction and has an ordinary level of education. This »ideal-type« already shows that there is no special attribute, which can be linked with the cybercriminal as such.

Most unsolved cases (more than 40%) can be classified as »identity theft«. This is an extension of the classic theft crime. Whereas cash used to be stolen, today it is credit cards or ATM cards. Since this is only an extended form of classic petty crime and not a special feature of cybercrime, these files were not further

[1] 118a: Unlawful use of a computer system, 119: Breach of telecommunication confidentiality, 119a: Improper interception of data, 123: Reconnoitring of trade and business secrets, 124: Reconnoitring of trade and business secret to the benefit of a foreign country, 126a: Damage to electronic data, 126b: Disrupting the operation of a computer systems, 126c: Misuse of computer programs or login data, 148a: Commercial Fraud, 225a: Counterprinting public authentification marks

analysed. To get a more specific picture regarding the different types of defendants but also the approaches taken, the cases need to be classified. This differentiation can be conducted best regarding the motivation of the defendant. In doing so, the authors differed five types of cybercrime, that already occur in Austria (Huber, Pospisil, Hötzendorfer, Löschl, Quirchmayr, Tschohl, 2019):

- Type I: Revenge crime
- Type II: Financial crime
- Type III: Show-off crime
- Type IV: Conviction crime
- Type V: Follower crime

These types of cybercrime differ from each other not just regarding the motivation of the defendant, but also in their approach, the way in which they chose their victims and the damage they caused. With 43% the revenge crime is the most common type of cybercrime, not getting solved in Austria, followed by the financial crime (29%) and the show-off crime (12%). The last two types, the conviction crime (5%) and the follower crime (4%) had not been that often, till now. In the following, the motivational types will be illustrated based on variables.

Type I: Revenge crime

B separates from A, who longs for revenge. Due to the former trust relationship, A knows the password that B uses for different accounts (Facebook, email account …). A gets access to the accounts, changes the password, looks into private data, deletes and modifies it or posts degrading texts and photos in B's name.

The majority of unsolved cases can be assigned to the category »revenge crime«. The defendant wants to take revenge on a victim. He often uses social media to carry pictures and information about the victim into cyberspace. The victim is always a private person and there is almost always a kind of »relationship« between perpetrator and victim. This can be a love relationship, or an acquaintance relationship. Many cases of cyberstalking fall under this category. Defendants of this type commonly do not have any specific technical expertise, but uses the insider knowledge he/she has from a former trust-relationship. The defendant usually operate alone and out of a personal feeling of jealousy, revenge or others more. Thus, the attack is commonly a targeted one and the victim is generally a private person. In these cases of revenge crime, the vulnerability is usually the naivety and unawareness of the victim. The offence is in most of the cases a data breach or an attack on networks. As consequence of the revenge crime, victims usually suffer under mental harm and the loss of information as well as the loss of reputation.

Type II: Financial crime

A wants to make quick money. He/she buys some email-addresses from employees of huge enterprises online and sends out a so called »pishing mail«. B, the assistant of the CEO in a huge enterprise, receives this mail with the request that he/she has to transfer a huge amount of money, to a bank account he/she does not know. The request seems to come from the CEOs mail-address and is handled as top secret. B is uncertain, but does not want to make something wrong and transfers the amount of money to A.

Defendants of the type financial crime usually have at least basically technical expertise, and are aware of simple cover-up measures, such as wrong IP addresses. They commonly operate in groups and search for an open vulnerability to conduct the financial crime. Thus, the defendants typically do not has a relationship with the victim, which can be a company as well as a private person. In most of the cases, the vulnerability – the defendant is searching for – is the unawareness or naivety of the victim. Typical examples are social engineering and phishing attacks, in which the defendant encourages the victim to disclose confidential information. After the attack, most victims suffer from financial damage, especially reinstatement costs.

Type III: Show-off crime

A is part of the hacker group »XY«. The members of the group are bored by their daily life and want to show the world their technical skills. To attract high attention they search for vulnerabilities in critical infrastructures like national authorities. They find one in the security-system of authority B and launch a SQL injection and a Distributed Denial of Service attack on B. Thus, the group modifies sensitive data and influences the functionality of the system. Finally, they post their procedure as well as the open vulnerability of the authority and the sensitive data on an online platform to show their success.

The defendants of this type are typically younger men and usually act in groups of more. They commonly have technical expertise and have a rather complex approach compared to the defendants of the other motivational types. Defendants of the type show-off crime, also use cover-up measures, such as the TOR-network or VPN-encryption. The attack itself is in most cases based on tools, but could also be a D(D)oS-attack. Moreover, it is commonly not a targeted attack, because the defendants are searching for a vulnerability. The aim of the group is not a special information or victim, but to gain attention for their attack. Therefore, in most of the cases the victim is an authority or a company of public interest. As consequence of the attack, the victims suffer from reinstatement costs as well as from the loss of reputation and sensitive data.

Type IV: Conviction crime

A is a member of the religious perpetrator group »YX«. This group wants to spread their radical conviction to find new followers. Thus, they need a platform and search for open vulnerabilities on homepages. They find one and use technical attacks to gain access to the homepage of B. After doing that, they delete the existing content of the homepage and instead display Djihad fighters with machine guns and their religious message.

Defendants of the type conviction crime commonly have a various level of IT expertise and so is the complexity of the approach. They normally act in a group of more with the same conviction. The group usually attack homepages of private persons as well as companies, because their aim is not to gain information or harm the victim, but to spread their conviction and ideals. Thus, the defendants of this type normally do not have a relationship to their victim. As consequence of the attack, the victims commonly suffer from the loss of information as well as the loss of reputation because of the radical contents presented on their homepage.

Type V: Follower Crime

A is part of various forums with technology interested persons in it. One day other members of one of this forum brag about having cracked B's system and post instructions, vulnerabilities and sensitive data in the forum. A is curious and follows the instructions given. A gets access to the email account of B, reads the emails and changes the password, just because he/she can.

The defendant of the type follower crime, commonly has basically technical knowledge, but is not an expert in the field. Moreover, he/she takes part in special interest groups/communities and has therefore access to existing information about vulnerabilities. The defendant uses this information out of a lack of awareness or out of curiosity. The follower crime needs another crime to occur, usually the show-off crime. Thus, the attack is commonly not targeted and the defendants do not have a relationship with the victim, who could be anyone who was the victim of the enabler in the first place.

4 The victim

Regarding the unsolved cases of cybercrime prosecuted between 2006 and 2016 at the Vienna Criminal Court, we can generally distinguish in two groups of victims: private individuals and institutions. While private individuals mean individuals, groups of private persons and persons of public interest, the institutions mean companies as well as agencies. Private individuals more often (58%) become victims, and there nearly as often woman (53%) as men (47%). The individual victim is about 39 years old (mean) and unawareness as well as a lack of security measures are common vulnerabilities. If an institution becomes a victim (42%), it is usually no critical infrastructure (64%) and has no reporting obligation following the NIS directive (96%). The most common vulnerabilities are publicly known vulnerabilities and the lack of security measures.

5 Conclusion

When analysing the files at the Vienna Criminal Court, we found out, that a lot of information regarding the cyberattack is missing. To illustrate this, we need to take a closer look on the process of a cyberattack. According to Hutchins, Cloppert and Amin (2011), a cyberattack can be divided into seven phases: reconnaissance, weaponization, delivery, exploitation, installation, command & control and actions on objectives. Strung together, these phases are called »Cyber Kill Chain« and shown in Fig: 1.

If a case gets charged at the Criminal Court, in most cases the victim itself recognized the cyberattack. In these cases the defendant is usually already in the last phase of the Cyber Kill Chain, because the process before is much more difficult to get aware of. Out of a scientific perspective, it would be very useful, to gather information to the process before, but this information is hard to find in any of the files. With this knowledge, it would be possible to raise our knowledge about the specific approach of a defendant. To get this information, it would be necessary to raise the investigations to a new level.

Therefore, it would be necessary to raise the knowledge of the society as a whole as well as the knowledge of the responsible persons in the investigation process. The main problem is a vicious circle leading from unsolved cases to the difficulty to learn from these complex cases. The origin are the responsible persons in the investigation process, who (1) do not already know enough about the topic of cybersecurity. This lack of basic knowledge leads to (2) a lack of knowledge regarding investigation methods that could be useful when facing high tech crimes like cybercrime. If the possible capacities - regarding the investigation – are not exhausted, this leads to (3) a lack of information about the approach of the defendant and a lack of information about the case as a whole. This lack moreover leads to the problem (4) that the case cannot be solved and in the next stage, (5) this information gets lost for further cases, to learn from it. So the cycle closes, because it is (1) not possible to gather new information about the topic cybercrime and our general knowledge cannot be improved.

To raise the number of solved cases, it is therefore necessary to raise the knowledge about cybersecurity - on the one hand - in the society as a whole and - on the other hand – regarding the responsible persons in justice and executive.

6 About the Authors

Edith Huber is a Senior Researcher in the field of Security Research. Her research focuses on Cyber Security, CERTs, Information Security, Communication, Cybercrime, Cyberstalking, New Media, Social Science and Criminology. In 2009, she received the federal security prize of Austria. She has a lot of publications and experience in international research projects.

Bettina Pospisil received the B.A. and also the M.A. degree in sociology from the University of Vienna (2014, 2017). In 2015 she was Research Assistant with the Institute of Instructional and School Development at the University of Klagenfurt and at the Institute for Information Management and Control at the Vienna University of Economics and Business.

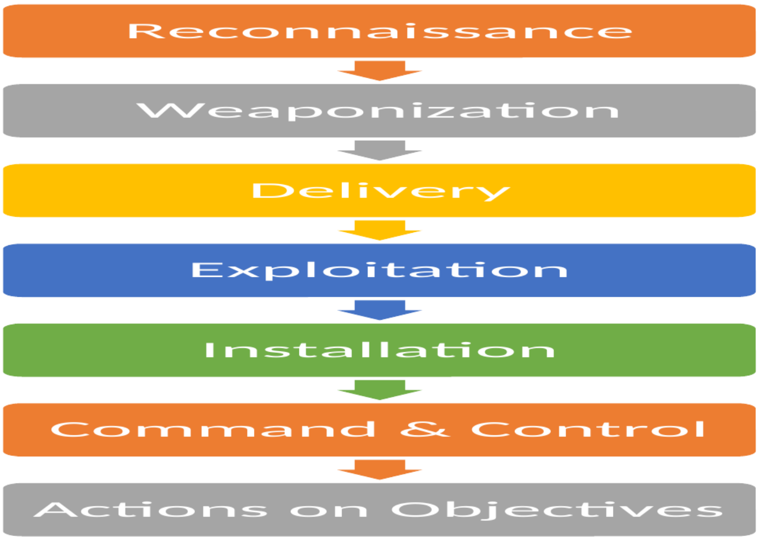

Figure 1: The Cyber Kill Chain

Since 2017 she works as Junior Researcher in different KIRAS and FWF funded projects at the Faculty of Business and Globalization at the Danube University Krems. 2017 she and her colleague received the Innovation Award of the Danube University Krems for the project called »CERT-Kommunikation II«. By now Bettina Pospisil is the co-author of different papers and presented academic lectures at criminological and technical conferences. Her research interest includes the topics Cybersecurity and Crime Studies.

Walter Seböck studied at the University of Vienna as well as at the University of Economy Vienna, Alaska Pacific University and Danube University Krems. He is Assistant Professor for Security Studies, head of the Center for Infrastructural Security at the Danube University Krems and responsible for the development of security courses and security research.

He is a lecturer on Information Security and Security Aspects in the Digital Economy and Industry 4.0 at Lomonosov University in Moscow, Hebei Finance University in China and Xingtai University.

7 Literature

- Dölling, D. (1995): Probleme der Aktenanalyse in der Kriminologie, in: Die Täter-Individualprognose (S. 129–141). Heidelberg.
- Hutchins, E. M., Cloppert, M. J., & Amin, R. M. (2011). Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains. 6th Annual International Conference on Information Warfare and Security.
- Huber, E.; Pospisil, B.; Hötzendorfer, W.; Löschl, L.; Quirchmayr, G.; Tschohl, C. (2019): Without a Trace - Die ungeklärten Cybercrime-Fälle des Straflandesgerichts Wien. In: Schweighofer, E.; Kummer, K.; Saarenpää, A.: Internet of Things. Tagungsband des 22. Internationalen Rechtsinformatik Symposions IRIS 2019. Editions Weblaw: Bern.
- Federal Ministry of Interior (2018) Crime Statistics, Vienna.
- McGuire, M; Dowling, S. (2013) »Cyber Crime: A Review of the Evidence.« https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/246749/horr75-summary.pdf.
- UNODOC. 2013. »Comprehensive Study on Cybercrime.« Wien. http://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf.