MURDERBOARD

HOW IT ALL BEGAN

TALES OF THE CRYPT-OH.
BOOK ONE

KLAUDIA »JINXX« ZOTZMANN-KOCH
RENÉ »LYNX« PFEIFFER

FEATURED BY
DEEPSEC

Cover design: Klaudia Zotzmann-Koch

CONTENTS

PREQUEL

WHERE CRIME FICTION, PRIVACY AND IT-SECURITY COME TOGETHER

It was a warm summer day when I got a call from an acquaintance who wanted to hire me for data protection coaching with one of his clients. Besides crime writing, I also work in data protection, helping self-employed people and small businesses to set up their websites and also their internal processes in a data protection-compliant way and so on. Perhaps a somewhat strange mixture: crime fiction and data protection. But actually it's not on a closer look, and which will—hopefully—become apparent in the course of the following four blog posts. My friend's inquiry was about a suspicion that information was leaking out of the company and being used by the competition.

I prepared quite a long list of questions, which was partly fed by my experience in data protection, but also by seven years of experience as a project manager in web development. I showed the question list to René, who works as a freelance pentester. Maybe some of you know him from the privacy podcast episode on „Pentesting" or also some of his talks at PrivacyWeek. It took a good half hour, then I got the answer: „Looks complete". And I thought to myself: crime writer and IT-sec—a perfect mix for such a job! Criminalistic thinking can help to convict criminals. What would I attack if I were targeting a small company or even an individual?

A little later I got another message: “Make a murder board! A classic who – against whom – when – where – why.“

I thought: “I told you so, crime writer and IT-sec.”

And a third message followed: “I have an idea! Let’s write a murder board blog post series together!“

And here we are: where crime fiction, privacy and IT-security come together.

By the way, we are: René “Lynx” Pfeiffer, IT-security expert and organizer of the annual DeepSec conference, which brings together experts in IT-security and offers a select workshop and lecture program. And me, Klaudia “jinxx” (or “jinxxproof”) Zotzmann-Koch, author, podcast host, privacy expert and co-organizer of the annual PrivacyWeek since 2016.

You might wonder why we’re taking forever to write a blog post series. The answer is quite simple: we want to show you that #onlinecrime is much more common, easy and diverse than you might think. Add to that my experience from many workshops in schools, community colleges, self-organized webinars and more, that the questions asked are always the same in all age groups from 12 to 92. Plus the unanimous opinion that „I’m far too uninteresting for them“, with no further definition of who „they“ are. And of course the ubiquitous „I have nothing to hide,“ which reads more like „I don’t want to deal with this topic“ and points to a popularity comparable to counting calories or testicular cancer. Above it all hovers a blind faith in technology; an expectation of salvation that technology can and will solve all our problems if we just let it. Coupled with naïve guilelessness toward companies and institutions, but also toward authorities and the state.

We want to show you what is currently (spring 2021) actually possible and workable, how difficult or easy it is, and what interests are behind it. And we want to prepare some entertaining reading minutes. The topic is serious, but at least it can be told entertainingly.

CHAPTER 1
TRACES

THE TIME FACTOR

Traces are the „metadata“ of an act, a course of action, a communication or even a presence or having been there. They show us that something happened, but often also how something happened. We consider traces always in retrospect, because they have to be there first in order to be considered. The time interval between the emergence of traces and their observation can vary. In 2017, for example, researchers investigated how Ötzi, a mummy from the ice of the Ötztal Alps, came to his death about 5,300 years ago and thus solved a murder with a slight time delay[1].

But some traces also disappear. Not only the well-known traces in the sand … Also we can't detect e.g. knockout drops in the victim's blood already 24 hours after they drank them.

There are also traces that are not recognized as „disturbing factors“. They fit into the picture and do not cause any frowning by trained observers. A classic „looks like an accident“. Or the death of aged persons, which surprises no one but delights heirs.

And then there are the traces that online crimes leave behind. „IP addresses“ and „log data“ may sound more cryptic than footprints, cardiac arrhythmias or „direction from which the arrow came“, but they are just as revealing.

Time is ubiquitous not only in crime or physics. Computers depend on clocks. Thus, de facto clocks and looking at them are constant companions in the digital world. Pretty much all tools used for programming allow a simple view of the current time. Times or timestamps, as we call them, are an excellent Ariadne's thread digitally. You can always orient yourself by this.

A HARMLESS BEGINNING

Leon is a student and has a tight wallet. His computer is broken, and he urgently needs a new one. So he goes to a computer store that also offers refurbished devices. He buys a refurbished laptop and trades in his defective device as a spare part.

DATA CARRIER

Eventually, something has to be stored permanently. By permanent, computer science understands the so-called non-volatile memory, which can store bits and bytes for a certain time even without a power supply. The digital clay tablets can take various forms. Storage began with magnetic data carriers such as tapes, floppy disks and rotating metal discs. Optical data carriers (CD, DVD, BluRay) accompanied this. Modern media use computer chips that memorize, i.e. store, small electrical charges. The actual process of storage leaves traces as magnetic fields, electric fields or material properties, depending entirely on the method.

Forensics on and at data carriers deals with accessing and analyzing stored data. The copy plays a central role, since we carry all investigations out on copies of the original. The aim is to prevent unintentional changes during the analysis. Exactly what we can read from which medium and how depends heavily on the technology used. We find traces everywhere, if one does not have a melting furnace at hand for cover-up. Even broken CDs can contain data fragments on the fragments. This sounds a lot like movies and television, but occasionally it’s just a matter of small amounts of data like passwords, logins, keys or metadata. Even small pieces of the whole can be sufficient.

NETWORKS

When we send data over a network, it is divided into smaller parts and transported individually via many intermediate stations. You can think of it as a delivery that is sent in a series of manageable packages. These packets can, of course, each create traces. On the one hand, the individual stations could create copies of the packages. There is also the digital sender and receiver. Which point communicates with which other point can be recorded as well. With more complex protocols, additional data is added. For example, a web server can record which end point (meaning: which end device) retrieved which data and when. From this, for example, we can derive the purpose of the transmission.

These traces do not always have to be automatically collected and stored. However, the data necessary for the traces always arise, whether they are stored or not.

FILES AND MESSAGES

Digital and analog, information is always available in defined portions. File folders and books correspond to files. Notes, postcards and letters correspond to messenger messages and e-mails. All of this can be arranged in any way – sorted, chaotic, in one place (i.e. on one device), distributed across multiple locations or people. Sifting through and properly connecting these finds is a fine art and requires experience. With luck, files carry time information in or on them. Emails often also have a history of time and place information in their content, if they are complete (i.e. with envelope and postmarks on them).

Meanwhile, Leon's defective laptop is taken apart at the dealer. Spare parts storage in the literal sense. They disposed of the defective main board, and put the remaining parts like keyboard, screen, hard drive, touchpad and more into boxes with other keyboards, screens, hard drives and touchpads and wait for a new use. First, they use the screen as replacement part in another laptop, then the hard drive. This is formatted, and the system reinstalled. And with that, the repaired device is ready for its next lifetime.

Metadata

Metadata is structured data that describes certain characteristics of the actual data. They provide context and help to understand and process the data describing them. Metadata alone can be very revealing. One can infer relationships, for example. Who is in contact with whom is quite interesting. Often, metadata relates to communication. Additionally to the communication partners, there is sometimes a description of the content. In investigations, the general rule of thumb is: the more metadata, the better.

We are familiar with metadata from everyday life. Telephone numbers, the device identifier of cell phones or e-mail addresses are examples. They rarely contain any personal information, but we can assign them to people.

[1] https://www.wissenschaft.de/geschichte-archaeologie/oetzi-es-war-heimtueckischer-mord/

CHAPTER 2
INVESTIGATIONS

LETTERS AS WINDOWS TO THE WORLD

When young people discover the world, they are often happy to receive mail. Who doesn't like it when others think of you? Once the love letters from the crush have undergone the metamorphosis into heartless letters with windows, we realize: Money rules their content, just like in this story.

Leon has a habit. When walking back from the mailbox, he likes to feel the meaning of the contents of letters with his fingers. Here, it's the letter from the credit card bill. And it has grown to several meaty millimeters. Leon hopes for a change in the terms and conditions. However, after opening it, it turns out that, unfortunately; it is a list of payments. He can barely remember the individual items. There are just too many—and most of them are not from him! In the column of numbers, various amounts have lined up and marched in lockstep to the total. He neither knows the items nor the companies claimed to have been paid by him. Slowly, sanity returns. Leon searches his wallet, but all the cards are still there. Then he reaches for the phone and has the credit card blocked.

Over the next few days, Leon is pretty busy applying for a new credit card and canceling payments. Besides his studies and his part-time job, this eats up a hell of a lot of time and nerves. Especially the latter. Two resources that are finite for all of us and, in Leon's case, would have been better spent elsewhere.

What happened to him?

ACCOUNTS AND CARDS

The answer to this question begins with the use of the credit card. In the analog world, you think about when you used the card where and for what purpose. Often, that's manageable and tied to geographic locations. Digitally, this becomes more difficult because online merchants often offer the option of storing credit card details in user accounts. This automatically creates a link to the access data of these accounts. If you are logged in, you can make payments from this platform. In most cases, it requires a login and password for online accounts. Under some circumstances, an e-mail address is used as a login. In contrast to the physical credit card, one must now clarify which online account is responsible for a payment. Was the online portal compromised? Was the password too weak? Or did someone gain access to the email account?

In Leon's case, several possibilities are conceivable. Affected accounts may have become part of a data leak. With bad luck, the platforms that „lost" the data don't know about it yet. So they can't investigate the matter. Another possibility is malware on the devices that were used. Resourceful malicious code looks on systems for stored accounts, browser history, in documents and other usable data. These are smuggled out and analyzed in the attackers' command centers. Usually, there are entire campaigns behind such attacks, which are well prepared and organized.

SOCIAL MEDIA ALTER EGO

Social media postings move the world, especially when ex-presidents tweet. You know your own timelines. Some people look for trustworthy sources, follow them, and in this way have created human filters for information that are supposed to control the daily flow of facts. Trust forms networks.

The cell phone rings. Leon picks up.

„Are you completely stupid now? Why do you post such nonsense! I hope you're drunk! „, it comes to him without greeting. Several minutes of incomprehension follow and cannot be cleared up. Simply hung up. After the third call, the picture forms. According to his friends, his Twitter account published things that were racist and not suitable for minors. He immediately sets out to find the cause, but realizes that his login no longer works.

This incident is not fiction and has happened to many people. Chains of trust in social networks are worthwhile targets, especially when a clear name requirement still leads to public identification. Account credentials are usually compromised through theft. Malware looks for active accounts to grant access to third parties. Leon's example is still a harmless case, albeit very embarrassing for him as the affected party. It's not just about public messages, but also about direct communication (so-called „direct messages" on Twitter, Instagram, Mastodon or similar messages). How is Leon or I supposed to know if someone is reading?

Many providers report when the last login is not plausible. Some always report when you logged in with which device from where (geographically or network-wise). This only helps if you also register this information and irregularities become visible. We usually recommend so-called two-factor authentication (2FA). Here, the login needs a second channel that provides a code for verification. This can be a classic SMS. But there are also code generators that deliver time-based numbers that change every minute. You start the generator with a value that is stored in the respective online account. If someone steals the access data, the second factor is (hopefully) missing and the other person still cannot log in, even though they could capture the login and password.

Leon didn't have 2FA for his Twitter account. Until that day, he thought it was only for privacy fanatics and people who had something to hide.

TREASURES OF THE NETWORKS

Most of the time, everything evolves around money. In the digital world, however, other aspects come into play. Goods and monetary assets are more diverse. Valid bank accounts, credit cards, access to e-mail accounts or similar resources such as social media profiles indirectly represent assets that are stolen and traded. The picture on such incidents gets distorted in the process. After all, we humans like to think, „Why are they after me? «. Or „I'm far too uninteresting for them". But that's not always the point. You also become a target if you have resources that are interesting. Real email senders are popular, of course, because they increase the credibility of a fake email. Even access to websites is a sought-after commodity because the criminals can store data for their actions there or on the web servers behind the website. It recently happened to an acquaintance that his blog was used to distribute Emotet. The file with the malicious software was put on his server, and from all over the world the file was retrieved via phishing mails and downloaded to the computers of people who had clicked the link in the e-mail. All because of a non-updated plugin in the WordPress he uses to run his blog.

Automation multiplies the added value. Many a scam e-mail may have caused amusement or amazement. But if only a fraction of a percent of millions of emails fall for the scam, then the bottom line doesn't look bad at all. All the downloads of the Emotet file speak for it. The same applies to the other areas. Of course, we can block stolen credit cards and change account passwords. But to do that, the theft has to be noticed first. In the digital world, data is not simply „gone" or

„disappeared“; it is copied, which means that unauthorized access is not noticed immediately. It only becomes noticeable when the copied access data is actively used. And that can be an unknown number of others who retrieved the data from wherever and are now using it.

„Follow the money“ is therefore still valid. Cui bono? The concept has just to be extended to values.

VIRTUAL MOTIFS

Besides money and revenge, there are other motivations for digitized criminals. One factor that is difficult to accept is simply resources. This also means computing power. Anything that has access to the Internet and can execute code is a target. It becomes even more interesting if it is poorly secured or barely monitored. Almost anything called „IoT“ („Internet of Things,“ networked things like toothbrushes, cameras, coffee makers, heating thermostats or bathroom scales, etc.), falls into this category. Another good example is an old computer (or smartphone). It may also be a server, whether in the cloud or self-operated. Old is relative; It is enough that it runs software without security updates, while the physical thing itself can be brand new (IoT). If the system has storage space, can run programs, and may use the Internet, it's interesting because it can serve as a springboard for further actions.

This approach allows to disguise the origin of attacks. The origin is rarely the direct source of incidents. For those affected, of course, it is no consolation to be bycatch.

For investigations, it is important to establish relationships. Is a victim the actual target, a means to an end, or a deliberate deception? Occasionally, there are false leads laid in order to steer the assignment of the perpetrators in a certain direction.

INVESTIGATIONS

Catherine Miller is a police officer. Cybersecurity, the people with the nimble Internet connections and the pre-installed Tor browser for investigations in the so-called darknet. For some time now, one name has been coming up in her mind again and again: Leon Dragic. Katharina is still not sure whether he is the victim or rather the perpetrator. It would be a lot of chutzpah if he had rented all the servers from which malware spreads on the net with his actual name. But it wouldn't be the first time a guy thought he was invulnerable or untraceable. So far, she's gotten them all. Some just took longer. And the list of notes on Leon is slowly but surely getting longer.

THE RED THREAD

A common thread in motifs is benefits. What is the benefit of a compromised system or account? This is not the same question as "cui bono?". Rather, the question of who benefits from an attack for obfuscation. What is the benefit of a system itself? What can it see, e.g. what does it have access to? With IoT devices, a coffee machine might see a lot of other devices on the same network. Or what data is going over that network. It may also see cell phones that may not be logged into the same Wi-Fi, but are communicating with the coffee machine via the Bluetooth interface. And depending on what else the marketing agency that built the app for the coffee machine needs for "marketing purposes", it may also see the phone book on the cell phone, the photos, data from other apps stored on the SD card, and perhaps the data from the device's sensors such as accelerometer or position sensor.

The thought of visibility and access inevitably leads to chains of trust, which is also a goal. Friends of friends are always interesting because they trust each other. They use this for email or even SMS scams in all shapes and colors. Plausible senders wash messages clean. The damage is only worse when attackers have full access to other accounts.

CHAPTER 3

SERIAL HACKERS

ORGANIZED CRIME OR GRAND THEFT DATA

MOTIVATIONS AND MOTIFS OF THE “COSA DATA”

Elevate data to a valuable commodity and it gets automatically traded, hoarded, stolen and counterfeited. We can use digital processes both legally and illegally, just like the economy in the physical world. However, cyber crime is about much more than data. Accounts with certain privileges also represent value because they act as a multiplier. For example, a simple e-mail account with stored contacts (address book or even the contact data in existing e-mails). This has several properties at once: Identity, trust and an archive of messages. The archive can be searched directly for valuable data. The identity can be used for fraud with the help of the trust of the contacts to get further access to more accounts and data.

Motivation is—on balance—always something like a benefit or profit. Data sold directly has an immediate benefit.

More often, data is obtained in several steps.

METHODS: ORGANIZED AND NEAT

The organization in digital crime follows analog models. There are service providers for all roles and stations that are necessary. You will find everything that you would find in a well-established company. There are technicians, marketing, a helpdesk for victims (with extortion software—yes, indeed!), notaries, traders, security experts, banking and whatever else they need in business. This structure implies the procedure and preparation of operations. Something like dramaturgically prepared scenes, where within a few minutes of hectic keyboard strokes entire IT systems are riddled with holes, exists only on television or in imaginary books. Reality is much simpler and very routine.

VALUES OF THE SHADOW ECONOMY

The shadow world is full of service providers offering their respective expertise. This results in an accurate reflection of the legal economy. Opportunities for business arise from the collaborations. Fraud campaigns collect data from victims via email sends. This data is compiled into databases. These go to refiners, who refine the raw data through verification and classification. By the way, you don't even have to click a link in an email for your email address to be added to the convolute. Emails often contain „tracking pixels" and it is enough to open (or preview) the email to trigger tracking and report to the sender that this email has been opened. So, just by viewing the email, one confirms it is a real and active email address that can be resold. This increases the value of the individual records. The goods prepared in this way are then passed on to traders who offer the products on marketplaces. There, besides the traders and buyers, there are notaries and payment service providers (up to and including banks and money launderers), who ensure that the transactions are processed securely. One crow may not peck out another's eye, but it's better to be safe than sorry. After all, you probably don't know each other.

THE USUAL SUSPECTS

Or maybe they do know each other. The usual suspects. Like the 30 to 80 people on Catherine Miller's watch list. She surfs the usual sites day in, day out, monitoring the offers and the people offering them. Nicknames are always changing, and people are constantly joining or dropping out. But the „hard core" is always there, under some name or another. For most of her job, she doesn't even have to start the Tor browser, most of it happens on the regular Internet. Among the newcomers, there is an "ldra002" since last month. Seems to be quite active. She puts the name on her list.

CHAPTER 4

TROJAN HORSES

OR: STATE HACKING

FEEDING PIGEONS IN THE PARK: ESPIONAGE

Knowledge is power. Knowing nothing makes one envious when looking at the model of modern information societies. The natural application of networks that transport information is espionage. So the Internet early made acquaintance with it. The aspect of smuggling messages in and out of an area is obvious. It also involves breaking through security measures to gain access to protected information.

Whereby large parts of our own information are much less protected than we would like or even be aware of. The e-mails mentioned above are always in plain text and therefore are visible to everyone. An unknown number of third parties read them on the way from sender to recipient and assess this information. And all the information we have in accounts on US platforms (photos, more or less public postings, direct messages, etc.) is viewable by authorities in the US and anyone who cooperates with the US. It would not be the first time that people may not enter a country because of a social media posting or a direct message on a platform.

CHAIN OF COMMAND

Martin B. from A. earns his money as a contractor. He has a small company under which he offers good old IT services: Setting up printers, maintaining the networks of small businesses, occasionally building a website for individual entrepreneurs. That doesn't make a lot of money, but it provides a valid umbrella for his actual business. Martin B. takes care of a couple of command & control servers that are used by several large campaigns on the net to control and manage malware. He doesn't know the names of his clients. The last three had given long strings of letters and numbers as their nicknames. He gets his money from changing number accounts in different crypto currencies. Most of the time, these accounts exist for only a few days. He has given up trying to track them. He doesn't even want to know. Martin B. keeps using different nicknames and different number accounts himself at irregular intervals. One for each incoming payment. He rarely uses a nickname or number account twice. At the moment he is on the road as „ldra002". And his mission is to spin up a new command & control server for a malware called Ryuk. The specifications given to him are impressively large, and the job gives good money. Presumably his clients have something bigger in mind with it. Martin B. doesn't ask. Asking is bad for the business. Instead, he randomly pulls out one of the recently purchased credit cards from the digital file box and rents a virtual server for 21 days from a major provider. He smiles when he reads the name: Leon Dragic. How funny and very fitting for his current pseudonym. Already the day after tomorrow he will use another one—far earlier than Leon would get the bill.

EXPLOSIVE APPS—SABOTAGE

With sufficient digitization, we can leave both the production of goods and the destruction of production facilities to the machines. Where once you had to laboriously smuggle explosives and have them planted by agents, today you can have that done by software. Industrial facilities such as power supplies, energy transport by pipelines, chemical or nuclear processing, manufacturing or related constructs are vulnerable to failure. It is also possible to interfere with measurement and control processes to force deliberate decisions out of machines based on false values. This type of digital sabotage rarely manifests in spectacular explosions. More like a production coming to a standstill or exhibiting a serial defect. The best sabotage goes unnoticed for a long time.

For the execution of such perfidious attacks, one can assign one's own people or hire silent service providers for a lot of tax money.

One topic we should address at this point is the so-called „state Trojan"—a piece of software that carries many problems. Starting with the fact that we now live in a society in which those in power have a fundamental distrust in all citizens and we are all under a general suspicion of planning the next terrorist attack. Followed by a spyware to be foisted on all of our most personal devices. We mean our smartphones.

That this software exists at all, brings all kinds of problems. For example, finding a way for malware to get access to the right data in the first place. With unsecured or minimally secured devices like IoT devices, this is easy. But our cell phones, which are targeted by governments because they are our personal communication hub, are quite a different level, because they are usually well secured. To get "root privileges" (super admin, quasi "god mode") there, you have to find a really fat (and therefore expensive) security hole. And those exist. It has a reason that the manufacturers of our devices release security updates now and then to close freshly found security holes and to keep the operating systems and apps secure as well as they can. However, there is a large black market, where security holes are sold to the highest bidders. If you have read this far, you won't be surprised. Criminals always find ways to compromise devices. Unlike security researchers, who basically do the same thing but report their findings to manufacturers and help them close the loopholes and make the world a little safer for everyone, the criminals make money out of it. And cui bono? Who is buying into these gaps? Other criminals and governments, who use them to build state Trojans against their own citizens. A highly problematic black market is not only kept alive, they actually fuel it with our tax money.

In application, such spy programs are then also problematic. On the one hand, legally, because a malware for communication monitoring needs really deep rights on a cell phone. For example, if it is to read communication data in secure messengers, it must be able to read the content on the sender's device before encrypting it. A secure messenger sends the data „end-to-end encrypted", i.e. the content of the message can only be read at both ends by the sender and the recipient. On the way in between, you can see that a message exists, but the content is not readable from the outside, only „character salad". Malware that is supposed to be able to read message content before it is encrypted and forward it to the outside world needs super admin rights on the cell phone. And with that, it can read everything that happens on the device, including the phonebook, photos, content in other apps, listen in on phone calls, and whatever else the device can do. That's much, much more than the authorities are actually allowed to do, but it's technically impossible for the software to do less than that.

And last, but not least, the problem where application and purchase of vulnerabilities coincide: The provability. Who says that criminals have sold this one vulnerability (or even the many) only to this one government? It is possible for anyone with enough money to buy anything on a black market. And private individuals or highly professional criminals like the ones we described above can afford three-, four- or even five-figure sums. Now, if anyone can create malware, it will be hard to argue that certain evidence is really from a particular person. We remember admin rights: anyone can forge photos, GPS histories, and more through malware and associated access rights to mobile devices. Suddenly evidence is no longer evidence. The question is, who wants to tell which story? What was done with this device, where was it present, what is it supposed to have seen or heard?

And because we have already spent so much tax money on such software, we have to use it, otherwise it would all have been for nothing. Surprisingly enough, 80 million Germans and 8 million Austrians are not planning terrorist attacks on a daily basis. They also don't organize in child molester rings. Most of them don't even know where to look on the net for instructions on how to build highly explosive things or for photographs that are rightly forbidden. And they have never heard of the Tor browser for accessing the so-called Darknet. Actually, most of them are also happy not to have anything to do with all this stuff and just live their normal lives. So what to do with this nuclear first-strike weapon? They find a few sparrows in extortion and drug and property crimes[1]. And other European countries don't think their own populations are so dandy either when they advocate independence from the central state[2].

In the end, what remains is that governments keep mobile devices insecure for everyone for a state-planned purpose against a few criminals. Worldwide. For tax money. And that opens the door for criminals to do whatever they please with all our devices.

THE FIFTH DIMENSION—WAR AND PROPAGANDA

First, we waged war on the land. Then came the water. The air is still young as a theater of war. Space is even younger. In the last few decades, the Internet has joined the ranks. The military calls the world of digital warfare, or „cyber warfare," the fifth dimension. We fight it with software that either defends against attacks or carries them out. One combines elements of information security (or insecurity) with the dictates of military missions. Including espionage and sabotage.

We often forget information sovereignty in this topic. The manipulation of information is just as much a part of the whole. Influencing news, political decisions, elections or public opinions can have serious consequences. Language becomes a weapon in this process, and the Internet is the delivery system. What is fatal about this kind of manipulation is that even a temporary presentation of messages can have an effect.

STATE HACKING IN INVESTIGATIONS

Where there's investigation, digital chips sometimes fall. This also applies to the digital part of investigations. Unfortunately, that's where forensics meets information security. The basic task of information security is to prevent attacks, the tapping of data and the compromising of systems. Organized crime or the attacks of nations, however, do not abide by laws. Often discussed in this context is therefore the so-called „hack back" or „hacking back" in attacks. This involves actively counterattacking the real or alleged perpetrators of an attack. The controversy here is whether one actually catches the right people or only passers-by or unsuspecting deputies who are involved in the attack. Another issue is the loss of trustworthiness of online platforms and digital infrastructure when backdoors are introduced to access data and digital activities. The major argument for backdoors is the protection of data through encryption. However, seatbelts with predetermined breaking points are no longer. Said backdoors can be used by investigators and criminals alike. We will all be the losers.

IMPLICATIONS AND CONSEQUENCES FOR INFORMATION SECURITY

Information security is to protect digital data and infrastructures. The tools required for this are barriers that protect the digital assets from unauthorized access. These include secure encryption, protection of transport and storage location, and restricted access to data and systems. The quality of protection depends on the means available.

Third party access to IT systems or data can only be achieved with a backdoor or designated access permissions. If one would like to protect oneself from access by third parties, only weak points or duplicate keys remain for investigators and attackers. This then makes it impossible to implement information security. The technology does not value access ethically. Access by third parties remains an intrusion or attack. The context decides. IT specialists can hardly determine the context when there are signs of access before data is copied. In purely technical terms, there is also no such thing as good or evil access. Access to data remains value-neutral. Any weakening of security measures weakens the capabilities of the defenders.

THE CLICK OF THE HANDCUFFS

Catherine is in a jubilant mood. She and her colleagues have just landed an enormous fish. One of the persons behind a large-scale malware campaign against the Ministry of the Interior is sitting next door in the interrogation room. To their own amazement, he has confessed. What is particularly interesting is who else he had to deal with and who was involved in the affair?

Catherine meticulously goes through her notes again. One name keeps popping up here, too. At the same time in the same place … Leon Dragic. The GPS data on his phone speaks volumes. Four out of seven times he was in the same café and once at a demonstration. She is sure by now that Leon is one of those guys who are too sure of themselves. She found him in photos from two demonstrations. Rips on it quite the mouth.

Catherine sends the warrant to the colleagues who will bring Leon in.

We hope, we could show you, that one aspect is central for internet crime: trust. Trust is a good and long-learned thing between humans since the mammoths. But with all the technology in between us, trust nowadays—sadly—is usually in the wrong places.

The End. (For now.)

[1] https://netzpolitik.org/2021/justizstatistik-2019-polizei-nutzt-staatstrojaner-vor-allem-bei-erpressung-und-drogen/

[2] https://www.golem.de/news/nso-group-spanien-setzt-offenbar-staatstrojaner-gegen-katalanen-ein-2007-149659.html

Sources and Links

https://www.wissenschaft.de/geschichte-archaeologie/oetzi-es-war-heimtueckischer-mord

https://netzpolitik.org/2021/justizstatistik-2019-polizei-nutzt-staatstrojaner-vor-allem-bei-erpressung-und-drogen/

https://www.golem.de/news/nso-group-spanien-setzt-offenbar-staatstrojaner-gegen-katalanen-ein-2007-149659.html

Links to the original blog post series »Murderboard« in Englisch:
https://blog.deepsec.net/murder-board-blog-series-prequel/
https://blog.deepsec.net/murder-board-blog-series-chapter-1-traces/
https://blog.deepsec.net/murder-blog-series-chapter-2-investigations/
https://blog.deepsec.net/murder-board-blog-series-chapter-3-serial-hackers-organized-crime-or-grand-theft-data/
https://blog.deepsec.net/murder-board-blog-series-chapter-4-trojan-horses-or-state-hacking/

Links to the original blog post series »Murderboard« in German:
https://www.zotzmann-koch.com/murderboard-prequel-wo-krimi-privatsphaere-und-it-sicherheit-zusammenkommen/
https://www.zotzmann-koch.com/murderboard-kapitel-01-spuren/
https://www.zotzmann-koch.com/murderboard-kapitel-02-ermittlungen/
https://www.zotzmann-koch.com/murderboard-kapitel-03-serienhacker-organisiertes-verbrechen-oder-auch-grand-theft-data/
https://www.zotzmann-koch.com/murderboard-kapitel-04-trojanischer-amtsschimmel-oder-auch-staatliches-hacken/

DeepSec Blog: https://blog.deepsec.net/

Murderboard-Talk by René and Klaudia at PrivacyWeek 2020 #pw20:
https://media.ccc.de/v/pw20-367-murderboard-wo-krimi-privatsphre-und-it-sicher heit-zusammenkommen

About the Authors

René “Lynx” Pfeiffer, IT-security expert and organizer of the annual DeepSec conference, which brings together experts in IT-security and offers a select workshop and lecture program.

Mastodon: https://chaos.social/@nightlynx

Klaudia “jinxx” (or “jinxxproof”) Zotzmann-Koch, author, podcast host, privacy expert and co-organizer of the annual PrivacyWeek from 2016 to 2021.

Mastodon: https://literatur.social/@viennawriter

Murderboard is *Featured by DeepSec*.

Responsible for the content and design of this book:
© 2022 Klaudia Zotzmann-Koch, 1040 Wien
https://www.zotzmann-koch.com/

You can find more awareness short stories – mostly in German, in English on request at:

https://www.zotzmann-koch.com/stories/

Created with Vellum