How law enforcement can stay a step ahead of hackers

Dmitry Smilyanets

April 27, 2021

Cybercrime presents a range of challenges for law enforcement officials around the globe. Investigating and responding to these incidents requires technical expertise, the ability to see beyond borders, and the willingness to pursue cases when attribution may be incredibly difficult, just to name a few.

“Generally, [law enforcement agencies] know who the traditional criminals are, but have a hard time to prove what they are doing. In cyber, this is turned around,” says Erik van de Sandt, operational specialist with the Dutch National Police’s National High Tech Crime Unit. “They know what crimes are committed, but not who are behind these acts.”

Van de Sandt, who holds a Ph.D. in computer science and serves as an honorary research fellow at the University of Bristol's Cyber Security Research Group, both chases cybercriminals and studies them. He talked to Recorded Future expert threat intelligence analyst Dmitry Smilyanets recently about how cybercriminals avoid detection and the changes police departments need to make to pursue them. The interview was conducted via email and has been lightly edited for clarity.

Dmitry Smilyanets: How would you rate law enforcement's ability to catch cybercriminals?

Erik van de Sandt: There is, unfortunately, a digital divide between law enforcement agencies. Agencies do not have the same cyber capabilities. Let's focus on those who excel in their work. In my opinion, several teams, departments, and agencies—the FBI, U.S. Secret Service, the U.K.'s National Crime Agency, Germany's Federal Criminal Police Office to name a few—truly understand their role within and added value for the broader cybersecurity community. They closely collaborate with the cybersecurity community, while showing the self-confidence and authority that conducting truth-seeking investigations for prosecution purposes are the sole responsibility of governments.

Attribution—who did what—is both science and art. Police investigators are specialized in making statements about reality that go beyond a reasonable doubt. But attribution is not an easy practice, and law enforcement agencies (LEAs) are increasingly depending on collaboration with the cybersecurity community. That is a blessing: many companies and institutions want to confront crime as well. Generally, these stakeholders have a far better sight on victims and attack infrastructure. Ultimately, LEAs too have to fill in the Diamond model—actors, capabilities, infrastructure, and victims—but rigorously, without making a single mistake. So ultimately, LEAs are about diligence, about checking and re-checking assumptions, verifying and falsifying hypotheses, until we can make factual statements, while the private security industry is about efficiency. That might be a field of tension, but I have experienced so many situations in which LEAs and cyber threat companies were actively collaborating while acknowledging these differences. The major challenge is when identified suspects are in a jurisdiction where extradition is difficult, and this happens regularly. Therefore, LEAs must formulate alternative interventions such as disrupting criminal infrastructure, seizing assets, assisting victims, or writing threat analyses.

National High Tech Crime Unit
Central Criminal Investigations Division

The Dutch National Police’s National High Tech Crime Unit focuses on complex cybercrime investigations.

DS: In your view, is it harder to catch cybercriminals than other types of criminals? If so, what factors make it more difficult and how can the police overcome them?

EvdS: There is a causal relation between on the one side the complexity of the security of criminals, and on the other side the duration and complexity of police investigations. While there is academic, corporate, media, and political attention for attacks by the ‘bad guys’ and cybersecurity of the ‘good guys,’ the security practices of cybercriminals are largely known unknowns. Unless we know what cybercriminals secure, against whom, and to what extent, formulating effective offensive countermeasures—i.e., investigations—is a challenge.

The bad guys acknowledge the importance of security. Organized cybercrime and traditional crime both put a lot of resources in protecting their members and crimes. There is nowadays a complete underground economy for deviant security products and services. The security measures of both traditional and cybercriminals are comparable. Both distribute their assets over multiple jurisdictions, apply deception, use trust and distrust mechanisms, etc. Yet the emphasis and implementation might differ. Cybercriminals, for example, obviously rely more on offensive technical security measures like DDoS-attacks to cover digital tracks, RATs to spy on co-conspirators, etc. But traditional criminals are catching up, and I expect that the distinction between traditional organized crime and organized cybercrime will blur even more in the next few years. From an investigative point of view, the big difference between traditional and cybercriminals is their manifestation in the physical world. Generally, LEAs know who the traditional criminals are, but have a hard time to prove what they are doing. In cyber, this is turned around. LEAs know what crimes are committed, but not who are behind these acts.

DS: What resources (tools, skills, etc.) do the most successful cybercrime police units invest in?

EvdS: Simple answer: successful agencies invest in data science. We launched a white paper with the first framework for data scientific investigations in March 2021. The framework is called CSAE (pronounced as ‘see-say’, and an abbreviation of Collect, Store, Analyze, and Engage). While CSAE focuses on LEAs, the framework is helpful for the academic and corporate sector as well. Our data science approach is mixing the social/behavioral perspective of traditional investigators, technical perspective of digital (forensic) investigators with the numerical perspective of police officers with a mathematical background. Together, they are able to collect raw data, normalize and convert data into information, analyze the information and create intelligence, and eventually make factual statements about reality and execute a range of interventions. These interventions go beyond the prosecution of suspects, and include disruption of TTPs, victim assistance, and damage mitigation. We explain in detail how data science is used in all four phases to create sight (i.e., hindsight, foresight, insight, and oversight) what to collect, what to store, what to analyze and what interventions are needed. We have developed, tested and implemented this framework for the last five years, and not only applied it to financially-driven cybercrime, but also drugs-trafficking and child abuse images. I can truly say that the Dutch police now regards ‘big evidence’ as an opportunity, rather than a challenge.

DS: You’ve worked on many cases that crossed international borders. Indeed, cybercrime is often considered a crime that knows no borders. What are some of the biggest obstacles when working across borders, and how do you overcome them?

EvdS: Policymakers, politicians, and legislators have done a lot to promote legal and organizational harmonization such as signing international treaties and promoting operational collaboration. So, in most instances, LEAs are allowed to share evidence with international partners and they know with whom they need to align their operations. But then a new problem arises and everybody who participated in operational meetings recognizes the following challenge. Generally, the output formats of one agency cannot be an input for another agency because all agencies use different systems, software, formats, and data schemes. In practice, colleagues make exports in spreadsheets because that is the only format their counterpart accepts. So what we miss is technical harmonization. Technical harmonization is about shared ethics and resources, and establishing technically uniform norms, criteria, methods, and principles to process evidence by law enforcement agencies. We have had some major technological breakthroughs at the Dutch National Police, such as very advanced ETL-tooling [extraction, transformation, and loading]. We share these key technologies, including corresponding data schemes, with other law enforcement agencies in liberal democracies. That’s why we love industry standards such as MISP, Diamond, CRISP-DM, and the Intelligence Cycle. CSAE builds upon these standards to push forward the new field of data scientific investigations.

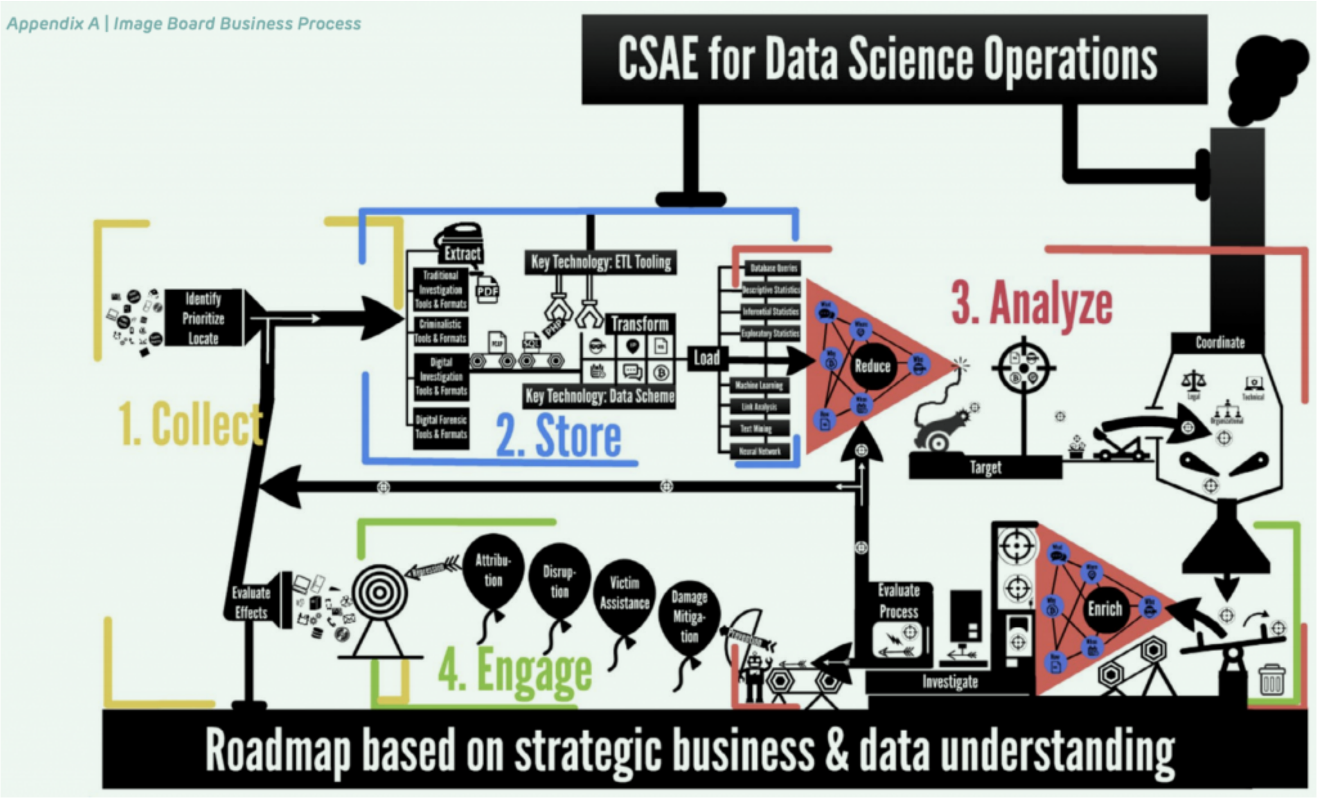
> I expect that the distinction between traditional organized crime and organized cybercrime will blur even more in the next few years.”

DS: Does having something like the EU make it easier to go after cybercriminals within its borders?

EvdS: Yes definitely. The EU and Europol are examples of legal and organization harmonization. It is nice to come together under a single roof and meet international colleagues that share the same passion as you. I am always happy when we detect a malicious server or identify a suspect within the EU because you’re certain that a preservation or an arrest will be a fact. The downside is, again, the lack of a shared language for (data scientific) investigations. Imagine sitting for days in the same room with colleagues of 27 member states who all try to explain their business process… If you would make a movie of that part of our job, the movie would be categorized as ‘comedy’ rather than ‘thriller.’ CSAE was truly inspired to solve that problem and push towards technical harmonization.

DS: It seems like governments focus their indictments on state-sponsored APT groups, while ransomware operators and other criminals are a lower priority. Do you agree? If so, do you think the average citizen stands more to fear nation-state actors or criminal groups?

EvdS: I agree, but we have to put this observation into context. Cybercrime exploded over recent years, and COVID accelerated events even more. Although governments have invested in cybercrime units, the growth is quite linear as compared to the exponential growth of cybercrime. It takes time to hire, train, and build new investigation teams. There is a bright side to the story—look for example at the Netherlands. In the past, my own team—the National High Tech Crime Unit (NHTCU)—had to do all types of cybercrime investigations, from fake pop-up web shops to DDoS attacks. We also successfully investigated ransomware and set up the No More Ransomware Project. But such projects are very labor-intensive and gladly Europol adopted the project. Nowadays, all regional police units in the Netherlands have fully functioning teams. On a national level, the regional cyber team of ‘Oost-Brabant’ set up a Dutch Ransomware Task Force and are responsible for ransomware investigations. This really helps the NHTCU to focus on financially-driven APTs and large cybercrime-as-a-service providers such as Emotet. So, while the NHTCU focuses on harm to large companies and vital infrastructure, regional units focus more on harm to citizens and small and medium enterprises. Ransomware, unfortunately, harms society as a whole, and therefore the NHTCU closely collaborates with the regional unit of ‘Oost-Brabant.’ By the way, this region is an economic powerhouse that holds a very high number of innovative companies (ranked 15th in the world based on the number of patents). This creates a range of opportunities for the regional police unit. So, I am convinced that regional units are not lesser national units. If properly equipped, they will create their own niche, specialization, and network.



A depiction of the CSAE process, or Collect, Store, Analyze, and Engage.

DS: Cryptocurrency has made ransomware attacks especially hard to trace, and there have been relatively few arrests in this area compared with the size of the damages. What's the solution?

EvdS: What I find fascinating is the concept of time. Cryptocurrencies are just a decade old, but revolutionized the commission and protection of crime. Against that background, legislators, politicians, and policymakers have to come up with a range of interventions to regulate this new sector. The next step is the enforcement of these regulations. Supervisory and compliance institutions have to figure out how such a new sector works, who the bad apples are, and if the sector is able to apply self-governance. Then there is the ultimum remedium of criminal investigations, and LEAs should indeed focus more on financial trails. Really good technical LE units tend to be poor in financial investigations and vice versa. But I have seen the first examples of successful multidisciplinary LE teams, so I think the number of investigations against crypto money laundering schemes will slowly increase. At the same time, there are parts of the world where there is no regulation or enforcement at all. As a consequence, these jurisdictions become 'crypto safe havens.'

DS: You published a very comprehensive work, *The Technical Computer Security Practices of Cyber Criminals*—how would you summarize the security measures the threat actors implement to avoid prosecution?

EvdS: While the protective practices of cybercriminals are not necessarily deemed criminal by law, security policies and mechanisms of cybercriminals frequently deviate from prescribed bonafide cybersecurity standards. As such, my study is the first to present a full picture on these deviant security practices, based on unique access to confidential sources related to some of the world's most serious and organized cybercriminals. Besides describing the protection of crime and the criminal, the observed practices are explained by the economics of deviant security: a combination of technical computer security principles and microeconomic theory. The new security paradigm lets us realize that cybercriminals have many countermeasures at their disposal in the preparation, pre-activity, activity, and post-activity phases of their tactics, techniques, and procedures (TTPs). Their controls are not only driven by technical innovations, but also by cultural, economic, legal, and political dimensions. Deviant security is very much democratized, and indeed one of the prime causes of today's efficiency and effectiveness crisis in police investigations. Yet every modus operandi comes with all kinds of minor, major, and even unavoidable weaknesses, and therefore suggestions are made how police investigations can exploit these vulnerabilities, while serving and protecting citizens.

DS: What are the most common mistakes cybercriminals make? What was the most epic one, in your experience?

EvdS: I have so many examples… But generally, I like the 'I-cannot-tell-my-girlfriend-about-what-I-do-for-a-living-but-nevertheless-I-came-up-with-a-set-of-rules-that-she-did-not-obey-such-as-not-using-my-computer-for-personal-stuff' related mistakes. What I also like are really complicated deviant security schemes that in theory are brilliant but are poorly executed in practice. I can really imagine somebody passionately telling a co-conspirer how to protect a TTP, only to imagine the frustration when he/she finds out that his/her partner lacks the same enthusiasm… Ultimately, human beings, including criminals and myself, are imperfect and prone to error.

> I have so many examples… But generally, I like the 'I-cannot-tell-my-girlfriend-about-what-I-do-for-a-living-but-nevertheless-I-came-up-with-a-set-of-rules-that-she-did-not-obey-such-as-not-using-my-computer-for-personal-stuff' related mistakes."

DS: How do you see the threat landscape changing in the next 5 to 10 years?

EvdS: Well, the future is today, and I described several trends in my new book *The Deviant Security of Cyber Crime*. More centralization towards, and collaboration between, a few big cybercriminal key players. More professionalization, specialization, and niche players. More disruptive actions without any regard for human costs. More acceptance of cybercrime as a legitimate job in some parts of the world. More state-involvement as cybercrime becomes a political tool in an ever-increasing multipolar world. And all of this against a background of an ever-increasing number of cybercriminals and increasingly complex—thus vulnerable—networks and systems.

DS: What is your opinion on ransomware? What is the most effective method to combat ransomware?

EvdS: Society as a whole still does not take information security seriously. Apparently, corporations immediately save on information security during economic crises, while more individuals are drawn into crime during such times of hardship. Dmitry, I knock every now and then on the door of Recorded Future for a chat. We discussed ransomware in the past, and your analysis is spot on when you said that this is one of the biggest threats. Unauthorized access to networks is nowadays fully monetized by criminals, with ransomware as the icing on the cake. Companies will end up with all their data stolen, paying a high price for ransom, while their customers are victimized because of compromised client databases. So, a proactive stance on information security is key, including cyberthreat intelligence for a larger group than only those who can afford it. When an incident occurs, collaboration is vital and this is going in the right direction. But I also see a growing number of legitimate companies that make a living out of ransomware attacks such as insurance companies, emergency response teams, and even startups that focus on ransomware negotiations. Time will tell whether these new kids on the block will collaborate with the broader cybersecurity community, or not.

DS: What industry do you worry about the most? Who do you feel is least prepared for cyberattacks?

EvdS: There are quite some companies in the world with large revenues and a low number of employees that nobody knows. These companies seem to be interesting targets because they really focus on making a profit and try to avoid overhead, including security. Just a personal anecdote: in the Netherlands, we have many companies in the agriculture industry that fit within this profile. Once, I had to call such a company on a Friday evening because we received intelligence that their email system was compromised. Because of CEO fraud, €200,000 was wired to China. An assistant gave me the cell number of—let us say—CEO Peter. His company had a turnover of over a billion euros a year while only employing 20 people at their HQ. When I told him how much was lost, Peter was relieved: only €200,000! But he also told me frankly that his company was putting all their efforts in acquisitioning companies around the world, and this incident was just the downside of that strategy.

DS: There have often been fears expressed about collaboration between more traditional organized crime groups and cybercriminal groups. Have you ever seen instances of cooperation between the two?

EvdS: In 2013, the NHTCU investigated a case where Dutch drug traffickers deployed a hacker to access the network of the port of Antwerp. Since then, we have had a number of cases where traditional criminals relied on cybercriminals, mostly hackers-for-hire. But this will change—traditional criminals, such as drug traffickers, need bulletproof internet connections, servers, communications, payments, etc. CyberBunker is a nice example of this pattern. I am also curious how the cybersecurity industry will respond to this trend.

DS: Tell me a secret, what was the most exciting case you investigated?

EvdS: In October 2021, I will celebrate my 12 ½ years in ‘cyber’ service, a milestone! Generally, our job ensures that you will have a lot of exciting stories that you cannot share. Although I experienced cases that involved espionage, hundreds of millions of stolen dollars, and massive undercover ops, an investigation against a bulletproof hoster was emotionally more satisfying. I generally focus on intelligence and the preparatory investigative phase, and I overlooked that these suspects were also involved in the commercial distribution of child sexual abuse images. My initial feelings of guilt were replaced by absolute pride when my extremely talented colleagues successfully investigated all crimes committed, including those against children. Although it was their success, you feel part of a team with a mission, and that’s what motivates me to work at the Dutch National High Tech Crime Unit.

Mission-driven and Russian-speaking intelligence analyst with type A personality. Dmitry has twenty years of experience and expertise in cybercrime activity that includes being a former member of an elite Russian-based hacking organization.