

24.11.2021

CYBERSECURITY ANALYST INTERVIEW:

What would be in your experience the biggest risks, speaking in terms of crime, that we are currently facing through the internet?

Yes, here, well, I would start by saying that it depends a lot on the threat agent because it is not the same thing, for example, for a State actor who may have other motivations or final objectives, for example, more oriented towards cyber war or cyber espionage, or operations of influence, this type of action, than, for example, criminal organisations or hacktivist groups who may have other objectives, more oriented towards interrupting a service or a website or an infrastructure or leaking information, for example, or damaging the image of a company. And there, well, we would also have what would be the insiders or disgruntled staff of the company itself, but above all in general, what we are seeing, for example, at the level of fraud is obviously one of the most booming cybercrimes, at the level of impersonation of a person's digital identity for different purposes, whether impersonation of a social network, for example, or physical identities to then carry out some procedure online, or well, threats, for example, it is also another of the services that we are also requested to identify who is behind a certain smear campaign or towards certain people, so the range is very varied, but many of them are mainly based on social engineering techniques, on attacking the weakest link, which in the end are people, and with few means, a lot can be achieved, as in the case of phishing or ransomware to introduce malicious code into a company.

And in that sense, what kind of security or preventive measures could cybersecurity specialists provide us with in relation to these crimes that are taking place in the online environment?

When we talk about cybersecurity, we should include the cyber-intelligence aspect because intelligence should, or rather, cybersecurity should rely on cyber-intelligence to improve its capabilities, especially in terms of detection, prevention and response. And there, well, as I said, intelligence can do a lot in terms of preventing, detecting and learning from previous cases, There are threats such as those I mentioned earlier that will always be there, but the idea is to minimise the risk by minimising those deficiencies that we know we may have and that we can somehow protect and take measures, and there from a digital patrol that would allow us to monitor multiple sources of information and detect certain patterns or certain activities, detect them in time to be able to take measures and then also in the event that certain incidents or crimes occur in the subsequent investigation and that is also where a lot of work is done and many specialists are required to be able to extract the information that is required and at the time and time and in the form that is also always urgent,. And then as I said, to learn from certain types of patterns, certain types of crimes, certain campaigns, and if I know for example that in the Dark web, for example, certain IP addresses are being moved or identified and moved, or a certain exploit is being sold and exploited in a unit. I can think that someone may exploit it massively and therefore I can already prevent that this campaign is coming and take measures accordingly, see if I am affected, etc., this for example, we detected, at the time, Spanish IP addresses that were moving on the dark web that had a specific port, that had a service that they were exposing, and specifically it was for example a remote desktop, they were moving around on the dark web and shortly after that explosion occurred and if we are able to detect it, because for example, in this case, it also affected entities such as the Bank of Spain or the Ministry of the Interior or the "red.es" network. This is, of course, what we brought to the

attention [of the competent authorities], but it requires this work, above all proactive work, to anticipate the crime, that is where we can do a lot or should do a lot.

And do you know in all your work that the pandemic has affected the fact that crimes are moving more to the Internet? And have you noticed in all your work if the pandemic has moved more crimes to the Internet?

Yes, absolutely, in fact there are figures around, some say that it has increased by more than 30% and even others say that it is higher, and indeed because cyber criminals have become increasingly professionalised and in the end they know how to adapt to the situation and they know that if there is a pandemic and companies encourage teleworking, well, in the end what they can do is where they are going to attack, they are going to attack the platforms that you use to have these meetings, or they are going to be able to elaborate attacks directed against those people that they already know they are at home, they are not in the business environment with their measures and protections and that each user is going to have different measures. And then, in addition, for example, we have also seen this in terms of disinformation campaigns or fake news, taking advantage of the COVID pandemic., If I know that many people are going to look for information because they are worried and are going to search on Google for example about COVID or vaccines, what they are going to do is create specific pages that give you an answer to what you are looking for and somehow manage to infect you or steal information or disinform you directly, so they learn and adapt to the context in which they find themselves and the pandemic did indeed increase crime.

And in all this that we are talking about, how difficult is it to investigate or prove this type of crime, such as [human] trafficking or other transnational criminal offences, when it comes to cybercrime?

Well, unfortunately there are many problems, it is a difficult question, there are many difficulties precisely because of the idiosyncrasies of the crime itself, for example the ubiquity, the fact that an attack can be carried out in parallel and at the same time in multiple different countries and each with its different problems. So from identifying or defining or determining which is the competent jurisdiction that can take charge of, for example, transnational crimes that cross borders and that in the end each country has different legislation, unfortunately the problem of cooperation also makes it very difficult to share the information that is available, if it is already difficult within the same country between different security forces and bodies, then between different countries and different services, even more so.

And above all, I would say that one of the biggest problems is the attribution of the crime. It is possible to detect and obtain information, from which IP or from which avatars or which identities they are [operating], but to attribute it or associate it to which person, to a specific name and surname or to a specific company or organisation, that is where the difficulty lies, because even though I say, even though we can locate it in a specific geographical area, it may even be third parties. Even if the mafias have hired others within the same country or attacks to that flag, then there are many factors that make investigations really complicated, although this should not be an impediment for us to continue betting, on the contrary, we should see more means to be able to improve this capacity.

In fact, some agents involved in the investigation report the difficulty of [identifying] the person who commits the crime anonymously and this is a little bit what I was commenting on. And we would also like to ask you what kind of tools, if we already have them today or they are in process, could be used to put an end to this?

I think that tools are often given a capacity or a magic that in the end they do not have, magic does not exist in these cases and there is no perfect tool either. It is true that we need tools because the volume of information that we need to manage and access is tremendous, so in order to be able to provide coverage, we need tools that allow us to extract and homogenise the information and that can represent it, so that we can then interpret it. There are no tools as such, for example, I want to de-anonymise a Twitter account and see who is behind the Twitter account and there is no tool to do it, there are no tools, there are different tools with different purposes, that by crossing the different results of them and carrying out manual research, it could be possible to do it. Moreover, each case is particular and each case is a world and the same technique does not mean that it will give results in all of them, but there are possibilities to identify them, but it always depends a lot on different factors. If they do it well and they know how to do it, which is more and more common because they are professionals, it costs more really, if it is done well, they have tools to be able to hide and configure different options even within the platform itself and secure their environment so as not to be traced, but always the more crimes they commit, , the more actions that are committed, there is always the possibility of human error and that is where we can enter or we can take advantage of that situation. I mean, in the end, more than tools, I think that what is required are analysts with that expertise to be able to carry out their analysis, to be able to connect the dots and know how to identify relationships that allow them to be traced, but surely it is a much more manual process.

In our case, for example, which we also do, politicians who receive threats or, for example, we were monitoring the last general elections or the climate summit, and there, of course, you have to handle a significant volume of information and, in this case, there are not only threats against critical infrastructures or against headquarters but also the people behind them and what kind of movements could be behind them, not only behind these people. Sometimes you don't get to a name and surname but you can get to a telephone number, an email address and in that case, well, the security forces do have the capacity to take the next step and in the end I believe that it is a combination or there should be a combination of different entities to be able to provide a more effective solution.

As this project is being developed, as I said, in three European countries, we would like to ask each of the people we interviewed, from their experience or their professional point of view. What would be the strengths or weaknesses, in this case in Spain, when it comes to investigating this type of crime, how are we in terms of investigation or how would you say we are, if we are at the forefront, if we are far behind?

Yes, I think that in the end, as far as weaknesses are concerned, I think that everyone has the same, what we were talking about at the level of, well, the characteristics of ubiquity, anonymity, that feeling of impunity that they may have and that encourages more and more people to join in because they see that the number of crimes, of complaints is very small in relation to the real volume and even so, of what is reported, very few end up being convicted, but it is true that comparing, for example, we have experience with Latin America, we have an

office in Bogota and from there we offer a service. It is true that in terms of capabilities and experience, perhaps not so much in Europe, but with Latin America there is an abysmal difference in terms of experience and knowledge of tools, techniques, training. And I believe that we are there and I would not say that we have nothing to envy to countries around us in the European Union and in fact knowing the people we have within the Security Forces and Intelligence Services, I believe that we have for example the Telematic Crime Group of the Guardia Civil is very powerful, with J. S. at the helm and with very few resources they do a lot, they work wonders, as do the National Police.

So I think that the strength, on the one hand, it is at the cybercrime level, on the one hand it is the experience we have in rcrime and cybercrime for historical reasons, but above all I think that the strength at a global level is the access or exploitation of open sources, the increasing exposure that we all have and that, whether we like it or not, practically obliges us to be there, it also makes it easier to identify those relationships that are so necessary or to identify certain profiles or certain activities, for better or worse. I believe that the use of OSINT and HUMMINT techniques, in combination with other disciplines, is, I think, it is basic and it is really what everyone is betting on because everything happens and moves on the Internet and not only on the Internet, but also a lot on social networks.

Speaking of financial institutions because they are also an important part of the project with the idea that they can be involved in the investigation or detection of crimes, would you consider that they are currently prepared to identify suspicious activities and at the same time be able to report them properly or coordinate with law enforcement agencies?

It's not really an area I'm that familiar with either. I know that they have certain indicators, and surely they could improve those risk indicators in terms of this specific problem, because perhaps they are more focused on other areas or the problems that they perhaps encounter the most, is that someone can supplant the online identity of your electronic banking because your accounts have been stolen, or credit card leaks that move on the Dark web, or several users connect at the same time from different geographical areas, or follow a standard pattern of activity, or connect at a certain time that was not the usual one, or make a certain movement. So it is very well worked out historically, but perhaps, as I said, I don't know much about this, but perhaps it would be interesting to have indicators at a higher level, for example, what happens if someone, users or customers of the institution receive significant income that is withdrawn a few hours later from an ATM or from the institution; patterns of common activity, for example of people who live at the same address or who are registered with certain characteristics, such as telephone or email, at the end of the day these are indications. The problem I think is that even if these cases are reported, one of the problems is that also at the level of the Security Forces, and I am sure that they will comment on this, is the lack of means and resources. For example, I was commenting before about the Grupo de Delitos Telemáticos [Telematic Crime Group], there were 30 people until recently, I know that with J. S. they wanted to be 100, but of course, even so, let's say that cyber criminals are growing at a much faster rate, and in the end they have to prioritise and rather than the preventive work they would have to carry out, I think it will be more in response to the problems they already have to provide a solution, rather than to prevent them.

I totally agree, in fact, it is the greatest difficulty that they always report, and in this regard, the National Police told us that they were going a bit further, in the sense of capturing patterns of behaviour, of identifying possible trafficking suspects, but I understand that with all the difficulty that this entails, I don't know if this is possible at some point in your experience.

In other words, alerting or having these indicators, yes, it would even be feasible, just as cyber criminals are also at the cutting edge of technology and use artificial intelligence or machine learning techniques or other types of aspects, the good guys also use them, but perhaps not with the power or the capacity because perhaps it is not our business and we do not know how to take advantage of it or we lack resources or there are different actions, no? I think it would be good and we should focus on increasing the detection of this activity, of these patterns of behaviour that the algorithms themselves could detect and generate alerts, which would then have to be investigated later, but at least we should be able to detect this first indication.

I wanted to ask you another question, what do you consider to be the emerging payment channels today, for example, for laundering, laundering money from criminal activities?

As far as money laundering is concerned, it would not be my field, but for example, there have been companies that have published articles about it and there is for example a market in the Dark Web which is Hydra, which is widely used not only to carry out illicit activities, but also to carry out money laundering and, for example, especially from cryptocurrencies, which are used so much and for example, the darkside group that was responsible for the radware that attacked for example the famous oil pipeline in the United States, laundered with cryptocurrencies there, I think it was around 5% of the profit that had been laundered here and in the end what it allows, for example is through here to use different services and convert those cryptocurrencies for example into credit cards or even to withdraw cash in certain locations that are predefined and hidden or other services. In the end I know that this Hydra infrastructure is used a lot there, and that most of the laundering, they talk about 75% approximately is moved there on this platform, which as always, like Sin root or other platforms that have also been closed down, well, for the moment it is holding its own and I think it has been open for 5 years, so we see the difficulty that even if we know that there are illicit activities there, often due to the legislation itself or for various reasons, including geopolitical ones, it is more complicated.

And a last double question and so we close, we would like to know what you would highlight, because it is also your field of expertise, of the application of OSINT techniques to, for example, detect or prevent criminal profiling, as we were talking about, and in relation to all this, what training do you think they would need, for example, law enforcement agencies, public prosecutors, what they would need to improve and what can be provided from your experience.

Well, on the first part of the question, everybody is really using open sources nowadays, isn't it? And it is said that even to get an idea, more than 80% of the intelligence that is generated today by intelligence services or by private analysts or police information units, more than 80%, is generated through open sources because let's say that the benefit is very great with very little cost, and that is one of the facets that we commented before, but above all and going more into the OSINT, HUMMINT, social networks, both these techniques and, for example, graph theory, allow us to represent or identify relationships, which would be for example the main nodes of a criminal network on which we should focus because often the problem is that we have so much information to process that in the end we have to prioritise and focus on where we start the investigation, which is the one that a priori seems to give us more results and we start investigating here and we can do this, these types of techniques allow us to help in this type of analysis and research that often require specific developments for example, because every day new social networks emerge or even criminals use their own social networks and we have to create specific extractors to extract this information from these networks, and then when we talk about information we have to bear in mind that we are not only talking about the text of

publications, increasingly what is on the Internet is more multimedia and more visual and there we have to be able and in fact, for example, we do so, to be able to identify or analyse it, audio videos, and if someone, for example, talks about a certain operation, a key word in a video, then we must be able to analyse it, process it and try to make a certain person appear in a video, which often clashes with the legal aspects, because mass surveillance of the population is not allowed, but for cases such as terrorism or other crimes, for example, facial recognition is allowed, and that is where we can also make a lot of weight.

And the second part of the question was, what can we do to train or what?

That is, what do you think, in order to deal with all this complexity of Internet crime that we are talking about, would the Security Forces, the Public Prosecutor's Office, or any other agent involved in the investigation of these crimes need to be trained?

I believe that, fortunately, the Security Forces are highly trained and that they are also updating themselves internally, but surely they also need support from the private sector to increase these capacities or to contribute with another point of view and other knowledge that they may also have, and above all, it is also very important that jurists also have knowledge of what these threats, these risks, and how they are carried out, what the risks are, how they are carried out, what the methodology is, the modus operandi, what makes them possible and how they are exploited 100%, because in many cases it is true that the younger ones are more involved in day-to-day life but there are cases in which the knowledge is so poor that it is very difficult to make others see or it is easier for them to overturn a particular case because of how it is explained or how a particular case is defended.

So I think that this is where prosecutors and judges need specific training in this type of cybercrime, in techniques and skills as well, I think we can contribute and how we can identify whether or not, or if a piece of evidence is valid or not depending on what, that part is fundamental.