‘I Was Running Two Parallel Lives’: An Ex-Secret Service Agent Opens Up About Going Undercover To Catch Cybercriminals

therecord.media/i-was-running-two-parallel-lives-an-ex-secret-service-agent-opens-up-about-going-undercover-to-catch-cybercriminals/

January 5, 2021

Dmitry Smilyanets
January 5, 2021

Editor’s Note: When many people think of the U.S. Secret Service, they picture the unruffled agents who protect the president and other dignitaries. But the agency’s founding mission—and one that it still carries out—is to safeguard the U.S. financial system from counterfeiting and other crimes. Over the last few decades, many of those crimes have shifted online: Hackers breach companies for financial information, sell stolen credit card numbers, encrypt corporate data until a ransom is paid, and trick victims into wiring funds to scam accounts. As a result, cybercrime has become the focus of much of the Secret Service’s work, and the agency plays a key role in investigating a range of computer-related incidents.

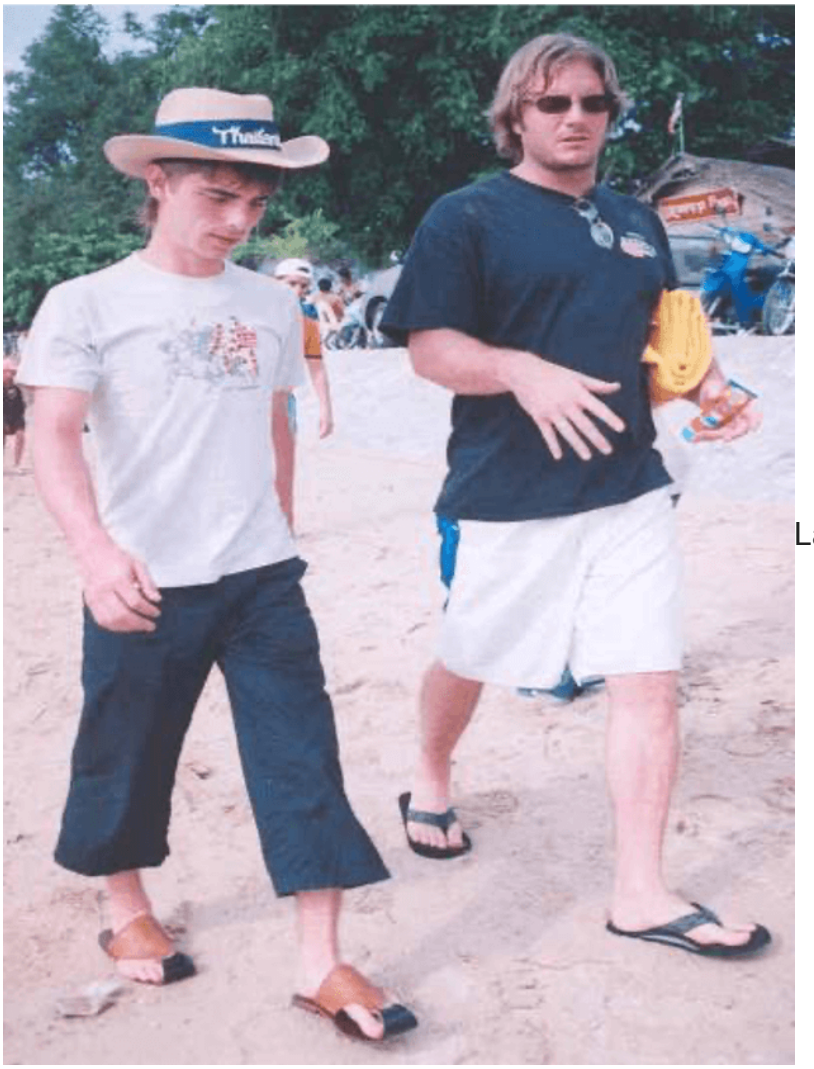
The details of this work sometimes emerge in court cases and law enforcement actions. Secret Service agents are often the ones who investigate and arrest high-profile hackers, darknet vendors, and other perpetrators of computer-related crime. But much of their work happens in the shadows, with undercover agents, million-dollar bounties, and other methods that can sound like they’re lifted from the pages of a spy thriller.

Until recently, Richard LaTulip was one of the Secret Service's special agents who went undercover to better understand cybercriminals. On occasion, he would even befriend hackers. "I opened the door and there on the other side was the target standing with a liter of vodka… a gift from their home country," he recalled. LaTulip, who left the agency in July to join the private sector, opened up about his experiences at the Secret Service in a recent interview with Recorded Future expert threat intelligence analyst Dmitry Smilyanets. The two first met in 2012, when Smilyanets himself was interviewed by LaTulip in relation to his involvement in a major data breach investigation. The interview below was conducted via email, and has been lightly edited for clarity.

Dmitry Smilyanets: You recently retired and are now a civilian after 22 years of service with the U.S. Secret Service. Do you miss your badge yet?

Richard LaTulip: When I reflect back and contemplate my career, I can honestly say it was a rewarding and meaningful experience. Along the way, I was able to contribute at all levels, gained a lot of invaluable knowledge, and traveled extensively. During this time period, I met a wide range of people, professionally and privately. These opportunities left an impression in my life and it was regardless of the length of time spent with these people. For example, some I may only have spent hours with, others were moments in time, and still others whom I now consider friends impacted my life because I learned from their experiences, gained an understanding from their perspective, understood more about their cultures and this allowed me the unique opportunity to grow as a person and to mature. Far too often we move through life; experience unique things and forget to stop and truly appreciate the experience and opportunity. This prepared me for the other adventures in my life I had yet to know or understand or even knew were coming my way. During my career, I learned how to better appreciate people, places, cultures, and countries. This has made me a better person and I am forever thankful for this chance. But your question was do I already miss the badge? To some degree, I will always miss the badge. Working as a special agent was a large part of who I am and what I represented. However, because I was fortunate enough to be employed by the U.S. Secret Service, I feel I can now take these experiences and share them with others. This is a new page in a long novel, and I am looking forward to meeting new people and continuing to grow and share.

DS: What were some of your most exciting experiences at the Secret Service? Which were most challenging?



LaTulip (right) engaging with a suspect on a 2006 undercover mission in Thailand. *Courtesy of Richard LaTulip*

RL: My career spanned 25 years, but 22 years were with the U.S. Secret Service so as one can imagine I had a lot of exciting experiences. But I can say the most exciting was working the various cybercrime investigations and of course this included my time working on the various underground online forums. From 2005 through approximately 2009, I worked online as an undercover U.S. Secret Service agent who purported to be a buyer of stolen data. In order to establish a level of credibility, I relied on the guidance of an informant. This informant was and had been working in the underground community for a period of time and became established within a specific group of online cybercriminals. The informant provided a level of bona fides within the community and I was able to seize this opportunity and expand upon it. The informant was by my side often, then not too much, and then at various points in time to assist in the investigation, but we'll come back to this later.

Working online as a cybercriminal by night and then a U.S. Secret Service agent by day represented challenges that are not easy to explain. I had to translate the successes from the online world to understandable and meaningful language to those who have not experienced nor understood the challenges. In addition, and unlike what is seen at times in the movies or TV, I was writing reports, recording evidence, documenting online

conversations, participating in conference calls with USSS headquarters representatives. You know, all the nitty-gritty work that is not as glamorous but was required to ensure a successful investigation and eventual successful prosecution.

Anyhow, the informant and I worked odd hours because the case was global. We needed to match time zones and seize on the opportunities when others, the target of the investigation, were online and working. Now talking online and creating rapport behind a computer represented challenges but our goal was different. Our goal was to be the first investigation, at that time, to take our online behind the computer undercover world, the digital world, and turn this into real-world operations. We planned and designed the case so we would travel, as needed, too far away destinations and meet face-to-face with those with whom I was speaking to online on a regular basis. Obviously, this presented unique challenges—we contemplated “the Who” to meet, “the where” to meet, and tempered this with “Where” we were able to meet. The planning and preparing for this style of operation was exciting, demoralizing, interesting, stressful, and rewarding all at the same time.

Because I was able to establish a positive relationship with the informant—one that, in my opinion, was based on mutual respect and understanding of each other—I feel because I gained the respect of the informant this translated to a higher level of devotion and more energy was invested to meet the investigative goals. Again, we speak of challenges, on one hand you have those that live in the world of law enforcement, those who chose an opposite path than those in law enforcement, and then the rest of the world. So, if you were going to be successful, you needed to have a unique personality, in order to bridge the gap between the rest of the world and those who chose the other side of law enforcement. One needed to establish a level of mutual respect. I will say not everyone is geared for this and to be able to work between these worlds is not easy. But for me, I saw it differently. I saw everyone, probably because of my fortitude to travel extensively, as good people—some just chose a different direction, but still they are good people. Therefore, I did everything in my power to never treat anyone differently or treat them in a way I would not want to be treated. For me, this worked well because when I spoke with a member of law enforcement—U.S. or International, a citizen or a “cybercriminal”—I treated them all with the same level of respect.

But where is this all going or where did it end within three months, we were able to arrange the first International meetings which are a completely different and interesting story on their own.

Now, I spoke about a lot of what I did but let’s not forget everything I did or accomplished relied on the guidance, assistance, goodwill, hard work, and determination of my colleagues in the USSS, other U.S. government agencies, and international partners. Without this assistance and goodwill, I would not have been able to achieve this level of success. However, what I described to you was the most exciting and challenging time in my career.

DS: You were not just a Special Agent—you were one of the most experienced in the Service's Cyber Intelligence Section. Can you please explain the significance of CIS? What are the main differences between CIS and the Criminal Investigative Division?

RL: So, to understand the significance I should start by explaining the CID. In the U.S. Secret Service, there are several different divisions, and CID is one of the divisions. CIS is an investigative section within CID. Over time, CIS has gone through several name branding changes. However, the assessment was that the USSS field offices had a lot of responsibilities, management identified a gap, and determined the USSS needed a group of dedicated professionals who either assist or manage the USSS's most significant investigations. From the beginning, management's vision was that CIS will be reserved for the USSS's most accomplished investigators and specifically designed to investigate, locate, identify, and arrest the advanced persistent threat. This same group of dedicated professionals is not only tasked with managing significant investigations, but these agents were also tasked with debriefing the arrested top-tiered cybercriminals, building relationships with international partners, managing significant operations, act as liaisons with federal prosecutors, working with federal, state, and local partners and ultimately crunch the data. Reality is inside the data, and from the data is how the APT is eventually identified and arrested. With this group focusing on top-tiered cybercriminals, they quickly established themselves as subject matter experts. This elevated the status, added value, and over time gained the respect from our partners specifically as it relates to investigative matters performed by members from CIS. I spent just over three years at CIS, and during this time I was fortunate enough to participate at all levels in a variety of significant investigations. This provided opportunities to debrief a wide range of cybercriminals and liaison with our many international partners. My knowledge expanded, interview techniques were sharpened, and my analytical skills refined. With this additional experience, I again continued to progress and gain a higher level of personal and professional growth. I believe this growth was key to help solidify relationships, and guided me through some of the most interesting results and experiences of that time.

DS: If you were the director of USSS, how would you improve the cyber intelligence process and cybercrime investigations?

RL: This is an interesting question and one that is not easy to answer. To be Director of the USSS' would be challenging, rewarding, and an honor. The USSS has a long and prestigious history. Along the way there have been some missteps, but the USSS learned from this and ultimately became a better organization. When I think back on my career, I know the men and women who served in the USSS take pride in their work, understand the magnitude of the responsibility, know the importance of properly implementing the mission, represent the organization with pride, and carry out its mission with honor. Ultimately, when we speak of the USSS we must recognize this organization is charged with and required to successfully manage two distinctly different missions. On one hand, we have the mission the USSS is most known for: protection. This mission means the USSS is responsible to protect the U.S.

President, Vice President—current and former—those designated by the U.S. President, and international heads of state while in the United States. When we speak of investigation within the USSS, it is unique. I say this because we are ultimately an agency with two missions, both of which are very important, and neither can be forgotten when we contemplate the organization as a whole. Since the USSS has the responsibility of a dual mission, I believe an approach that will holistically help the organization is to create three verticals: protection, investigation, and support. Each vertical will have domains, but ideally protection and investigations only focus on that specific mission. Protection, the larger of the verticals, along with those who work within this vertical, only are assigned protective missions that support the vertical. The agents would be regionally positioned, in fewer locations but located in the larger cities. Ideally, these larger cities have regional airport hubs, which can lower travel costs, and then the Agents work and travel from there to support the region.

The concept is the same for investigations, however the investigative vertical is smaller and will have more postings in the U.S. Of course, the support vertical is just that—support. But this will provide support for both the investigative and protective vertical. Another experience I had during my career is the USSS statistically does not promote or seek out opinions of personnel who devote their career to the investigative mission. I believe if verticals were created, then those who work in those verticals will promote within the vertical. This will assist in development as management will be more aligned to the concerns of an investigative agent. Diversity was always a focus but, in my opinion, this rarely included a difference of thought. To be truly diverse I would believe we need to have different positions, experiences, and thoughts. I saw mostly that promotions focused mainly on a similar line of thoughts. Again, this is just an opinion and frankly, some items are easier said than implemented, but I truly believe to holistically move an organization forward we must include more well-thought-out ideas which include at times a difference of thought. This, in turn, can have a positive effect on an organization’s morale and for a period of time, the USSS suffered a moral issue.

DS: I know one of the areas you investigated was Eastern-European hackers. If you can, please share a couple of the more exciting stories from your undercover days. What are some of the most important skills for successful undercover operatives online?

In Ukraine on a 2018 assignment to debrief cybercriminals. *Courtesy of Richard LaTulip.*

RL: So, I have reflected on this over time and of course my thoughts change along with the opinions. What is or were some of the most important skills that assisted me during my undercover days? Was I successful because I was that believable? Was it my upbringing? Was it luck? Or was it because I was social enough and experienced enough to be able to straddle the line between being a special agent during the day and a cybercriminal during the evening? Actually, it could have been one, two, a combination, or none of them. Bottom line, this is historical because everything is different today. However, at that time, this was something not so well known to law enforcement in general. Cybercrime as we think of it today was much different during this time. Yes, a computer was involved, so you had the technology. And of course online instant messaging was not new, but as widely distributed as this technology is in today's environment, the answer, at that time, was no.

So we looked for a skimmer, which was popular at the time but dangerous for those who worked this type of criminal activity. I say dangerous because of how closely connected an individual was to the stolen credit card data. But to now see in the wild people using full track data that was compromised via a network intrusion? This was new to law enforcement, and to be honest we had to get caught up. Luckily for everyone involved, the cybercriminal was having just a difficult time. Can you imagine: "Hey world, I have just hacked a company and

stole full credit card track data. I am offering $5.00 per track. Anyone?" I recall in some of the debriefs with hackers, them telling me how in the early days they were having trouble vending the stolen data. People were not so trusting. Can you imagine? "Let me understand, you want me to send money to I do not know who or where, oftentimes halfway around the world to a city I never heard of and in exchange I will get full credit card track data? Yeah right." That was often the answer. Most people, during those initial days, were not trusting hackers. So to counter, the hackers gave away data. The hacker received, as payment, cigarettes, alcohol, or very insignificant amounts of money. This did not last long. When you consider what is in the news today, one can now understand how far we have progressed and imagine how much a hacker earns today.

So, going back to when I started and proposed undercover operations specifically to move from the digital world, which was the most common type of undercover operation, and to move that operation to the real world… This was not something most organizations were contemplating, especially at a global level. I would say from the introduction—early 2000s—to when we operated—mid-2000s—we knew more, understood the areas the cybercriminals operated, so this operation was not a simple move into our "backyard." In order to be successful, we were getting on airplanes and going to far-off distant locations. This was a big deal, not just for the USSS, but for everyone in law enforcement, and so we put our heads together, thought about what we needed, and focused on the task at hand. Remember, this was new to law enforcement. The USSS had a policy, but this policy was not designed for international in-person real-life undercover operations. At that time, the USSS had no official training program, so everything we did was going to be groundbreaking, exciting, challenging, stressful, and extremely dangerous. We, in fact, heavily relied on our international partners, and fortunately for me and those involved we had reliable, dedicated, and trustworthy partners.

To set the stage we needed to brainstorm and answer all types of questions and come up with answers. One of the bigger questions—please remember we were not always dealing with individuals who had the highest set of morals—was related to the consumption of drugs. For example, if offered, do I accept, take, and consume drugs? Well, this was easy for me, I have never taken drugs, therefore I was not going to start today. But I needed to develop rapport so this meant I could not be the first one to bed. So, I focused on other areas in order to develop that required level of rapport. Understanding the cultures helped focus on the plan of action. If the target was from an Asian culture, then we focused on gambling, eating, and hanging at nightclubs. If the target was from a Western culture, then we focused on beaches, eating, and hanging at nightclubs. Small difference, but one had to understand the audience. Following that we needed to find that place in which the target wanted to go. This often meant tropical resorts and those that can supply the typical things most cultures and people would want. Gambling, girls, booze, bars, sandy beaches, warm weather, and clear clean blue water. Sometimes you could not get everything on the list—but gambling, bars, good food, and girls were a must, and easier to check off the list.

Now, this dovetails into an interesting side note. Of course, everyone wanted to go to tropical resorts. I mean how many people are interested in going to some far-off destination and not doing anything interesting? Well, some management started complaining and indicating why we are always going on these types of operations. So as the relationships grew and were becoming more popular, I was invited to a destination that was not a resort. More of a city tour but not so popular with tourists. I thought to myself, excellent! Here is the opportunity to show we are not only seeking what is considered by some as a government-paid holiday. However, the response by the same who complained was now why would anyone go here on a holiday. So, this message was clear—no way of winning, so let's just keep focusing on what works and go to the beach resorts.

In essence, I was running two parallel lives; these lives had to intersect at times, just so I could keep everything straight in my own mind but reflect back on what I was just mentioning. This will all make sense soon. On one of the operations, we decided to meet and hang out at one of the beach resorts. Of course, nothing was running smoothly, and we were waiting for the target's arrival. Delays and timing were not matching to what was spoken or planned for earlier in the planning stages. As you can imagine, some people were getting nervous. Thoughts raced through some minds—maybe the operation was compromised or maybe the target just decided, last minute, to not travel. Anything was possible, but then out of nowhere a knock at the door. I opened the door and there on the other side was the target standing with a liter of vodka. The vodka was a gift from their home country. This was not expected, as I thought—really everyone thought—I would get an instant message or similar type of notification. Regardless, none of that mattered, we were in play and moving. Thankfully, we did not move too far, just to the lobby for a late dinner along with some drinks. Finished with that, one thought was, "Ok, this is ending, everyone from the flight must be tired and in need of some sleep." Just as I thought this, there was an invitation to continue drinking in the room. Who was I to say no? It can't be me who goes to bed first, so off to the target's suite. This was not optimal, however it was a positive sign I was to be trusted. And trust is the place we wanted to be specifically with this target. Once inside, it was right back to a good conversation and drinks. This was going on now for a while and the minibar was getting low, so it was on to stronger drinks. Regarding the conversation, it was my intention to speak about new topics, old topics, and ensure we intertwined business into the discussions. Anyhow, I was relating a personal story—of course, the names and locations were changed but nonetheless still something that occurred in real life. The target keenly listening to my story immediately understood it was not something that aligned with what I spoke about online. So he called me out and challenged my story and asked why there was a difference. At this point, one can say, I was uncovered and exposed. Remember as well that it was late, we had more than one drink, and I was for the most part alone with the target. Thinking quickly or being a magician of words could have been the difference between success and failure. And failure was not an option. Another topic to consider, which at times is beyond a person's control, is nonverbal communication. What did I look like from the target's perspective? Was I sweating, twitching, or did my eye blink one too many times? Moments may have seemed longer than they actually were, but then again we did have

more than one drink, so this all could have been normal. Regardless, in the end none of it mattered. In retrospect, I was too quick to respond and everything I stated just resonated. Everything I stated was the truth, plain and simple. I lied. To understand completely, the online world is what you want it to be. Trust is as deep as all the 1s and 0s that make up the internet. I can be what I want to be when I want to be it and how I want to be. So deeper than mere words, “I lied” was the second stage of the conversation. The reason for the lie was simple—we spoke online. Today we sit in front of each other and have an opportunity to really know each other. The online world is filled with lies, and misstatements. This is real life now, face-to-face. Now is the time to build real trust and understanding of each other. Everything was true and the target knew it, participated in it, and understood it. So on to more important items. More conversation drifted on into the night and early morning hours. We watched the sun come up and after there was no more to drink it was off to bed. I think this was when everyone decided it was time to work the other more hidden aspects of the operation in shifts. No one was interested in staying up all night.

Now I know you asked for a few, but I will save the other stories for another time and place.

DS: Who are the top five cybercriminals on your list? Which hacking groups do you think are the most dangerous currently?

In Bangladesh, while teaching a cybersecurity and digital evidence collection class to the Bangladeshi police. *Courtesy of Richard LaTulip.*

RL: I do not really prescribe to or have a “top five” cybercriminal list. I have seen and experienced a lot to know that at any moment, any number of people can be today’s most highly sophisticated and successful hacker. As you know, there are a lot of intelligent and at times self-taught programmers, analysts, and cybersecurity penetration testers, and the list goes on and on. Some have chosen to use these skills to ensure the internet is a safer place for everyone. Others, for their own reason, have chosen a different path. I was fortunate enough, during my career, to arrest and debrief some of whom we termed as the most

successful online cybercriminals. With this success, some believed we made an impact. And to some extent, we did make an impact. These cases—and a lot I was not involved with in any capacity—were impactful. However, I knew it was only a matter of time before any cybercriminal's position was filled by another cybercriminal. Also, the world is highly competitive. Some want a level of fame and fortune, add in that today's world is also dependent on social media, which translates to status. This status is where some seek to be confirmed and validated. Move from the open social media and dive deeper into the "dark web" and we find forums. These forums have all types of members—some are legendary, some are ok with being amongst the crowd, and then others want to become legendary. When I was working online undercover, I thought most, not all, aligned with me, about the forums. The forums were more or less social media websites but in another format.

What I just spoke about extends to criminal hacking groups—they are all potentially dangerous. Hacking groups all have various levels of talented coders, programmers, or support personnel. These groups have time on their side and can slowly examine networks, find weaknesses, can leverage off-the-shelf penetration testing programs to assist in exploitation, and eventually over time are successful. When I was working in law enforcement, some took it personally; I never took this type of crime personally. They had chosen their career path and I had chosen mine. Their job was to be successful and create havoc online, exfiltrate something of value, and monetize the item of value. My job, at that time, was to correlate the intrusion to the individual who I needed to identify, locate, and arrest. As you know, this was without regard to where the person was located, so long as they compromised or utilized infrastructure in the U.S Regardless, I enjoyed my career, and I had a lot of success.

DS: What is your opinion of state-sponsored hackers and groups? How does the Russian GRU and FSB recruit new talent, in your opinion? Do they run these recruits or do they control them in other ways?

RL: I have many opinions about state-sponsored hackers or groups. However, I think everyone has an opinion and most probably the answer is "it depends." Regardless you can be sure that talent is everywhere and just like in most nations, there are those who desire to serve their respective countries. National pride is something I have seen interwoven into the underground community. For example, when online one can sense an "Us-vs-Them" ideology. Some will immediately think "us" means the online criminal community and "them" most definitely can mean law enforcement, the corporate world, or other injustices, perceived or real. However, this is not entirely what I am speaking about. The way some criminal actors write—in the online posts, links to articles—one can feel at times the "us" is them and their country and the "them" means most other countries. I gather from this information that to a degree they believe they are serving their country. I have even read, from historical chats, of online cybercriminals who claim by day to be hacking Western companies, but at night receive direction and are working on campaign X or Y for their country. Ultimately, the pride of the nation can be a method of recruitment.

Other recruitment methods can be very simple—for example, conducting investigations that will cross paths with top-tier talent. I also know from experience top tier talent will inadvertently post a “here I am” sign right on their homes. Not literally, but if you are from a small village and typically are seen cruising around on public transportation or driving an outdated vehicle, and then tomorrow everyone in the town sees you driving a brand-new Mercedes, Porsche or BMW… Well, this attracts the attention of everyone in the town, which includes those who work in security services. From here the next steps are not too difficult for an inquisitive and well-trained investigator to understand something is afoot.

Regarding the direction of a new recruit, I would surmise the officer or agent provides guidance, including over-the-shoulder direction. In addition, the person could be brought into the larger group, including a place to work from and operational funding. It is not a secret that oftentimes nation-state cybercriminal actors are well-funded and trained and—since the task is mission-specific—patient.

DS: In your view, how sophisticated are ransomware operators and their affiliates?

RL: My opinion is they are very adaptive, are able to adjust tactics, and overcome various obstacles. Yes of course you will have your one-offs, but overall the groups are very well organized. All of this leads to one conclusion: Certain ransomware groups are sophisticated. We have seen over time, referring to what I previously mentioned, an adjustment to tactics and deployment methodologies. This transformation did not happen overnight. For example, when ransomware was first deployed, it was encryption followed by a ransom demand. The demand was preset and pretty much this was forwarded to any victim. This lasted for a period of time, but the groups were successful, and they were successful at getting rather handsome cryptocurrency payments. So, companies prepared for the possible ransomware deployment cross-network. This assisted corporations specifically when the victim corporation refused to pay the ransom demand. So, as the pendulum swings from one side to the other this meant the advantage was to the corporation’s benefit. The ransomware groups added a new fold that could not be so easily ignored. Groups started exfiltrating corporate data followed by an encryption event and ransom demand. This demand usually identified the theft of proprietary data, but as with before the demand was for a predetermined amount of cryptocurrency. And the cat-and-mouse game continued as each side postured and adjusted. In today’s environment, we are seeing specifically-crafted ransom demands, a key indicator of pre-attack victim research. Also comes threats to release or vend data to competitors, as well as the burning of infrastructure. Some ransomware groups even have blogs where they name and shame the latest victims, provide levels of decryption support and allow for “victim” feedback related to the successful decryption of data. With their success, the techniques translate to other less sophisticated groups entering the market. Inside the dark web community, the information is shared, which includes profits. Profits other cybercriminals imagine or desire to have, and so they join the already crowded field of ransomware. I even know of hacking groups changing the entire business platform, switching the gears so-to-speak, and moving wholly to ransomware

deployment. Anyhow, this is not something to be ignored and corporations must account for the potential compromise. Otherwise, when the music stops, the unprepared will be left with very few options.


In Israel on a 2019 assignment to debrief cybercriminals. *Courtesy of Richard LaTulip.*

DS: You are currently working in cybersecurity for the private sector—does your experience as a federal agent help you? What are the biggest threats to your industry, and what will be your major focus in the new role? Are you prepared for the new challenges?

RL: I spent a long time working for the government, almost exclusively conducting investigations related to financial and computer crimes. Over my career, I worked undercover targeting cybercriminals, investigated online cybercriminals, debriefed vendors of stolen data or products, hackers, bot herders, and others, worked as a diplomat in Europe and in the U.S. Secret Service's Cyber Intelligence Section. I also participated in the U.S. Secret Service's critical systems protection program. Along the way, I picked up several advanced certifications which include the ISC2 Certified Information Systems Security Professional (CISSP) and ISACA's Certified Information Security Manager (CISM). So, I feel I am prepared for new challenges and look forward to them. I know I have a lot to still learn and this is exciting for me. I feel when you stop learning, sit back, and relax you are already

missing the issues. Missing an issue can be the difference between successfully thwarting or succumbing to a cybersecurity event. I also know part of my responsibility is to share my experiences with industry leaders, provide the information that can be leveraged to make a well-informed decision. As I have learned, providing the wrong information at the wrong time leads to incorrect decisions. To be valuable, the information has to be timely, informative, and relevant otherwise the information becomes useless. Our leaders need honest, at times blunt, evaluations of the current state. Otherwise, decisions may not include a holistic approach that positively affects the company. My new role or mission will be to support business leaders and I know, as I explained, that my past experiences will be essential for this success. In addition, I will say it does not matter where you work—the threat landscape is applicable to all parts of the industry. Corporations that ignore or believe it will not happen to them are simply ignoring the facts and the data. Whether working in the government or private industry we must be serious, understand the adversaries, apply best practices, incorporate defense-in-depth, and diligently review, analyze, and interpret the data. In the data will be the artifacts and these artifacts tell the story to the analyst or forensic investigator who then needs to dig deeper and interrogate the network.

DS: Tell me a secret.

RL: I should have been a cryptocurrency millionaire… I guess I need to give some context for you to understand completely. While working undercover I was involved in, among other things, moving money. This, of course, was used to purchase stolen data. And to move money I used all types of methods, which included traditional—such as bank transfers—and non-traditional methods—such as e-Gold, Liberty Reserve, or cryptocurrency. These were, depending on the time period, the accepted forms of payment. But working in the government meant this was extra work. I had to account for every dollar and how one day I could be up and then the next day I was down. It was frustrating and time-consuming to say the least. Anyhow, I participated in the community and the community was all-in when the market shifted to cryptocurrency. So just like everyone online I positioned myself as a “true believer” in cryptocurrency. Behind the scenes, I did not trust cryptocurrency. I had many chances to invest and instead I did the opposite. I mean I was following the rise of cryptocurrency, but I felt, “Where is the value? Where is this going? What coin do I buy?” And so time got away and my trust or lack thereof did not change. Thus, as opposed to investing a few thousand dollars, not much really, and get say 20 or 30 coins, I purchased none of them. Not to mention probably many other opportunities to continue and purchase additional coins. Anyhow, the cryptocurrency bus pulled up and asked me to get on board. I saw the destination but, not being a true believer, I did not get on board. Today one can see the record prices for cryptocurrencies, and I think back—I should have boarded that cryptocurrency bus.

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.