Steptoe

Episode 252: In the cyber adversary Olympics, it's Russia for the gold and North Korea (!) for the silver

Stewart Baker: [00:00:07] I am flabbergasted that the North Koreans are second.

Dmitri Alperovitch: [00:00:12] That is the other big revelation, that North Koreans were second, China third, Iran fourth, and all criminal groups put together were in fifth place with almost 10 hours to breakout on average. Initially, it was surprising to me too. I certainly expected China to be in second place. But I have to say, in thinking this through, it is not a surprise. The North Koreans have been at it for 20 years. When you think about how they recruit people into their cyber forces, there is a great deal of selection that happens. The best kids in high school get into college. The best people in the class get sent into the cyber forces. The other thing I think is important to point out about North Korea is I actually think that they are the most innovative actor in cyberspace bar none. They are the first ones, if you look at the history, to have been using destructive attacks to accomplish coercion and achieve their objectives. They were the first ones to use information operations! We focus so much on Russia, but two years before Russia, we had Sony. And I think the US government and most of us in the industry fundamentally misunderstand Sony because we so much focused on the destructive element of Sony Pictures attack that we forgot that they stole emails and leaked them to WikiLeaks. Two years before Russia! And now you have North Koreans engaging in massive cybercrime in terms of breaking into banks and stealing hundreds of millions of dollars on unprecedented scale. So in terms of actually achieving objectives in cyber, I think they are the best out there.

Stewart Baker: [00:01:39] [Music] Welcome to Episode 252 of The Cyberlaw Podcast, brought to you by Steptoe & Johnson. Thank you for joining us. We're lawyers talking

technology, security, privacy, and government. And any resemblance between the views expressed here and the views of our clients or our friends or our firm is purely coincidental. I'm gonna be interviewing today Dmitri Alperovitch, who's the co-founder and CTO of CrowdStrike, who's been on here several times before and whose company just released its 2019 Global Threat Report with some really interesting stuff in it. Welcome, Dimitri.

Dmitri Alperovitch: [00:02:18] Thank you.

Stewart Baker: [00:02:18] And for the News Roundup, we'll let Dmitri talk too, but Maury Shenk from our European technology and cybersecurity beat in London. Welcome, Maury.

Maury Shenk: [00:02:32] Good to be here, Stewart.

Stewart Baker: [00:02:33] And we'll give you Weaver! Nick Weaver, senior researcher at the International Computer Science Institute and a lecturer at UC Berkeley. Welcome, Nick.

Nick Weaver: [00:02:45] Thank you.

Stewart Baker: [00:02:45] And I'm Stewart Baker, formerly with NSA and DHS, the host of today's program, holding the record for returning to Steptoe & Johnson more times to practice law than any other lawyer. Jumping right in: the story that I wanted to cover, because it's kind of a law story, is that police are using "reverse location search warrants" to compel Google to tell them who was in the neighborhood of a particular crime when the crime occurred. And not surprisingly, Slate and a host of NGOs like EFF [Electronic Frontier Foundation] and the ACLU are trying to say, "That's just shocking." And I have to say I just don't get it. I don't see what's wrong with finding this. There's a notion that we ought to be able to identify the person before we can do a search warrant. But the fact is we've radically limited the numbers of people who are going to

get searched or are going to fall under suspicion when we say we want to find people who are in this location at this time. Nick, tell me I'm wrong.

Nick Weaver: [00:04:02] No, because the problem is this data is collected at all. So Google has a data collection attitude that would make NSA lawyers embarrassed. So, among other things, their apps collect location tied to identity, and if it's there and searchable with probable cause, it makes sense to search. And so I think these are concerning searches, but the target of the ire is wrong. The target of the ire should be those who are collecting these dossiers on everybody on the planet in the first place, not that, "Hey, law enforcement realizes you can take advantage of these dossiers that said companies are producing on everybody on the planet."

Stewart Baker: [00:04:56] Dmitri?

Dmitri Alperovitch: [00:04:56] Can I just ask: how is this different from getting data from telcos that have cell tower records of who is in an area?

Stewart Baker: [00:05:03] It's even easier. It was even easier to get cell tower dumps than any of the stuff that people are now complaining about here. And the cell tower dumps were delivered on the theory that this is information that belonged to the phone company and you could subpoena, so asking for a search warrant here at all is a substantial improvement in the amount of protection that data privacy gets. And Google actually has a second rule apparently in which they say, "We're only going to give you anonymized, hashed data so that you can identify that a person was here, and then you can go look for the next crime and see if there's any overlap between the person who was at the first crime and the second." And then they'll tell you who it was, but otherwise they might not. So it is kind of a surprise that this is attracting a lot of unfavorable attention.

Nick Weaver: [00:06:02] The other thing is with tower dumps is these days tower dumps mostly are done with warrants because of fallout from *Carpenter*.

Stewart Baker: [00:06:14] Right.

Nick Weaver: [00:06:14] But tower dumps do not have the precision that Google has. Tower dumps, unless you're doing like E-911 tracking, give you people within a couple-kilometer radius. This can get you within a 50-meter radius.

Stewart Baker: [00:06:31] And maybe soon better than that. I absolutely agree, but this is goalpost moving. Everybody was celebrating that in *Carpenter* they were requiring a warrant. Now people are saying, "A warrant? That's not good enough." So we'll have this fight as the ACLU tries to get us shocked about things that never shocked us when Google did it and never shocked us before when the police did it but now suddenly has to be shocking. Alright. Speaking of shocking, the UK House of Commons select committee, I guess it is – certainly it has every party known to man – has issued a report on disinformation and fake news. I have said the quick summary on this is: because Leave [Campaign] won, everybody in Britain must hate Facebook, and because Trump won, everybody in the United States must hate Facebook. And so this is a long, extended attack on social media, much of it aimed at Facebook. Maury, how seriously is this being taken in the UK?

Maury Shenk: [00:07:45] Well, I think it's being taken pretty seriously, and as you might predict, Stewart, I don't fully agree with the high-level summary. Those of us who are more left-y think that disinformation is having a big effect for the forces who think foreigners are dangerous rather than "let's all do it together." But it is a pretty – the report is rather sensationalistic. It reads kind of like an investigatory report. It spends a lot of time on Facebook privacy scandals. It spends a lot of time on election manipulation in the UK, US, elsewhere, places like St. Kitts and Nevis. And it identifies a number of bad actors like Cambridge Analytica and some affiliated companies. And it's a very highly regulatory set of recommendations about more power for regulators, a digital levy to pay for them, etc., etc. So I agree with you that it's rather extreme, if not with the overall summary of where it's going.

Stewart Baker: [00:08:43] Well, you obviously are farther left than I am, which is not hard. But a large chunk of this is just saying, "Facebook was present when the results that the Left doesn't like prevailed in elections, and therefore, Facebook must pay because we never want to have that happen again."

Maury Shenk: [00:09:05] I think it's an attack on the Facebook business model. So they're not saying these things are illegal necessarily. Some of them are breaches of Facebook's terms of service, but there's a lot of people out there who are criticizing Facebook's business model and its effect on our society. And I think that's the point of view that the report takes.

Stewart Baker: [00:09:24] Well, it's fair enough to criticize some aspects of the business model, and that's a social media problem generally. But I think the real juice in the report is we're shocked to discover that sometimes the Right wins elections, and we have to adopt measures to make sure that doesn't ever happen again. Alright. Speaking of never happening again: the last two months there've been unfolding scandals under the heading "DNSpionage" in which there have been significant compromises of DNS security in ways that have advanced a lot of Middle Eastern intelligence collection. Nick, how serious was this, and what should we be thinking about it?

Nick Weaver: [00:10:15] This is a very serious set of attacks. So as far as we know – and there's the great CrowdStrike analysis, and then Brian Krebs took advantage of some of the indicators to make a public report on other affected targets. Let's start with the fundamental problem of secure communication is: who do you trust? And so when you set up your domain, you have to trust your registrar – that is, the persons that are talking to the DNS infrastructure to set things up, and that's really the root of trust for everything. And so if your DNS registrar is compromised or your account with the registrar is compromised, somebody can trivially redirect all communication intended to you through them, decrypt it, re-encrypt it, because they can get cryptographic authorizations with the certificate authorities. And now they're able to basically intercept every communication – Web, email, etc. – destined for your target.

Stewart Baker: [00:11:33] So a lot of the victims of this were governments in the Middle East: Jordan, Kuwait, Albania, UAE, Lebanon, Iraq. As you go through the list, you start to imagine you have a pretty good –

Dmitri Alperovitch: [00:11:49] Iran was missing.

Stewart Baker: [00:11:50] Yeah, Iran was missing. Exactly. And so is Israel. So you kind of wonder, but you don't wonder much, who the attackers were. But if you were the Jordanian government and you had a domain, wouldn't you be kind of surprised to discover that all of the communications from other parts of the government are coming into you through Germany instead of through the mechanisms that it used to use?

Dmitri Alperovitch: [00:12:18] So what they did was actually very smart. They changed the records to point at their servers for very brief periods of time so it wasn't continuous. They were sampling the data. So it was actually very, very difficult to detect, and even systems that had DNS monitoring weren't able to pick it up even when they were using multiple providers. But the real problem is that – and we've known this for many decades now – is that the Internet is basically built on quicksand. A lot of these protocols we rely on, like DNS, like BGP for routing, are really fundamentally insecure, were never built with security in mind, and everything we've built on top of it, bolt-on security, really relies on those things working well. So, as Nick mentioned, if you're using encryption, if you're using certificates, but you're able to compromise the certificate authority and then use DNS to redirect the traffic, you can read all the encrypted traffic. And that's exactly what these adversaries were able to do. So we do have a fundamental problem here. We've known about it for many years. None of this, what we saw here, was surprising in terms of how it was done. We've known that this was possible for a long period of time. It was surprising, I guess to some, that it was actually done.

Stewart Baker: [00:13:25] How valuable would full implementation of DNSSEC actually be in combatting this kind of attack?

Dmitri Alperovitch: [00:13:34] So it actually did stop some of the attackers, but only because they didn't try to mess with DNSSEC. The final problem is that if you access the registrar, you can change the public key that's available, and of course, then your DNSSEC is own'd.

Stewart Baker: [00:13:47] You're toast.

Dmitri Alperovitch: [00:13:48] So you're absolutely toast. And this is a problem when you trust a third party, like the certificate authority, like the registrar withholding valuable data and being the authority of entity for that data, [if] they get hacked, we're all screwed.

Stewart Baker: [00:14:00] And what are the prospects that the DNS providers, the certificate authorities here, are going to suffer some of the same pain that DigiNotar suffered when its CA [certification authority] key was stolen?

Dmitri Alperovitch: [00:14:18] We'll have to see. I don't think there'll be lasting effects because the reality is most of them are very vulnerable. So it's not like there's a gold standard out there.

Stewart Baker: [00:14:25] It could've happened to anybody.

Dmitri Alperovitch: [00:14:26] Yep.

Stewart Baker: [00:14:28] Alright. Nick, any last minute thoughts?

Nick Weaver: [00:14:31] I thought that was well put. And welcome to the Internet.

Stewart Baker: [00:14:38] Yeah. There's always somebody who doesn't care quite as much about your security as you do.

Nick Weaver: [00:14:43] Who you have to rely on because they're in the root of trust.

Stewart Baker: [00:14:48] Yeah. Alright. So the Swiss have come up with a mechanism for voting online, and it's proving pretty controversial. Nick, I can guess what your ultimate recommendation here is, but what was wrong with the Swiss system?

Nick Weaver: [00:15:09] Well, there's the high level of they were just trying to do Internet voting, which is such a bad idea that XKCD has a classic cartoon on the subject. And then there was the implementation which is apparently – let's put it this way – the Charlie Foxtrot you expect from online voting systems where bad theory meets bad practice meets bad code meets plenty of 0 of 1 fraud scenarios where you can make Mickey Mouse win by 10 million votes.

Stewart Baker: [00:15:45] Yeah, the XKCD thing was right on point. It said if you ask elevator engineers how safe elevators are, they'll tell you about all the multiple failsafe devices that make it almost impossible for the elevator to fail. If you do the same thing with people who make civilian aircraft, they'll give you a similar speech, maybe not quite as self-confident. And then if you ask security engineers about Internet voting, they immediately hold up a cross, a bag of garlic, and run for the door.

Dmitri Alperovitch: [00:16:23] But I think that highlights the difference between safety and security, that with safety we're worried about act of God type situations and not an active adversary that's trying to circumvent, which is a problem we face in voting.

Stewart Baker: [00:16:34] Yes. And it is certainly the case that if you wanted to cause an elevator to fall –

Dmitri Alperovitch: [00:16:42] There are trivial ways of doing that.

Stewart Baker: [00:16:43] You could do that. In fact, I was unsuccessful at this, but I made an effort about 10 years ago when we first got talking elevators to figure out if I could hack into the system that announced the floor so that I could make personal

comments about partners who were on that floor. Luckily, I failed completely in that effort, which is why I'm still at Steptoe & Johnson. Alright.

Nick Weaver: [00:17:08] One thing I'd like to add on the elevator analogy is that sabotaging an elevator's safety systems probably requires physical access as well. So sabotaging a thousand elevators requires breaking into a thousand elevators, compared with sabotage of a pure electronic system where changing a thousand votes is the same effort as changing one.

Stewart Baker: [00:17:37] Fair enough. Well, my favorite aspect of the implementation was that the system was really complicated to put together. It'd be easy to screw up, not deliberately but just because it was such a complex integration. And the commenting on the code says, "Oh, be really careful here." And I thought, "If we just solve our security problems with more comments like that, life would be easy." Alright. Facebook. Title III. This is a kind of beneath-the-bedclothes fight that has been going on for a long time. It was a fight over a Title III order against Facebook that has never seen the light of day. The court rejected the Title III order, refused to enforce the order that the Justice Department wanted to pursue, so Facebook won. And then a bunch of NGOs – and maybe the *Washington Post* as well – asked the court to disclose what the fight had been about, at least in part. Facebook supported the in-part or whole as civil society groups wanted. And so we now have this bizarre story in which we don't know what the court is talking about, but the court is very clear that it's not going to disclose anything about the decision beyond the fact that there was one. Nick, what's your sense about what it was that the parties were fighting about?

Nick Weaver: [00:19:28] The problem is it's one of two situations. It's either this what – so background on Facebook Messenger. Facebook Messenger has two modes. It either has a mode where Facebook sees everything because it's going through the Web interface, or the phone-to-phone only mode, which is solidly end-to-end encrypted. And we don't know what the government was asking for. And one of the weird things about the decision is I think the judge is slightly misinformed. So, in the end, it came down to we can't separate out the criminal investigation stuff from affecting sources and

methods. The problem is the source and method is: either it's trivial and Facebook managed to fight the warrant on some other grounds, or it's impossible without forcing Facebook to change the code for the Messenger, which would have huge public implications.

Stewart Baker: [00:20:38] That would be the re-fight of the FBI v. Apple debate.

Nick Weaver: [00:20:47] Yes.

Stewart Baker: [00:20:47] I wondered if it was possible that instead they were trying to get Facebook to add somebody to the group that was being used and obfuscate the fact that they'd added the FBI to the clandestine MS-13 murder squad communications.

Nick Weaver: [00:21:08] That wouldn't work because the Messenger encryption library underneath Facebook Messenger already considers that as a threat model. You could use that against Apple, but you can't use that against Facebook Messenger because there's an almost-but-not-quite-hidden feature where I can go, "Let's see everybody else's keys and make sure that nobody else was added in."

Stewart Baker: [00:21:35] Okay. People can see this, but if they're sloppy gangbangers, maybe they wouldn't notice.

Nick Weaver: [00:21:42] Yeah. But all it takes is one person noticing it, and it falls apart. Do you think the government would tolerate a Title III order where you say, "Oh, and there's a chance that the Title III wiretap will not only be discoverable by the target but the target will be able to announce that, 'Hey, you're doing these Title III wiretaps.'"

Stewart Baker: [00:22:06] So those are the choices. We don't know what this fight was about. But since Facebook won and the government lost, my guess is it was one of the more dramatic requests rather than one of the more benign requests. Maury, *The New York Times* says that India is emulating China in its Internet regulation. Do you buy that?

Maury Shenk: [00:22:35] Well, not 100%, but to a significant extent. We're seeing more and more countries adopting really strict – well, broad and discretionary – restrictions on what can be controlled online. Even in Europe people are talking about harms-based control of Internet content. And China, Russia, Turkey have very strict controls, and India has proposed some regulations, which look quite likely to be adopted, that are heading much more that direction.

Stewart Baker: [00:23:03] You could just as easily have said that India is emulating Germany or the EU.

Maury Shenk: [00:23:11] They're going further than that.

Stewart Baker: [00:23:15] Really? Maybe on encryption. Right? They clearly have said, "We want to be able to decrypt some of these communications," but other than that, it's kind of, "We want to make sure that disinformation and illegal and harmful and unduly sexy speech doesn't get promulgated."

Maury Shenk: [00:23:32] Although, the definition of unlawful content appears to be much broader in these India regulations than in Europe. Also, India is weakening intermediary protections. In Europe we still have the Commerce Directive where you know if you're just a conduit or a host, you have a lot of immunities. And India is proposing to significantly weaken existing similar immunities.

Stewart Baker: [00:23:55] Although, I will note that that UK report says that we absolutely need controls on illegal and harmful speech, and the harmful of course is inconsistent with the values of the great and the good in southeast England. But the notion that stuff has to be suppressed that isn't illegal is pretty common across Europe, isn't it? And frankly, increasingly common in the US.

Maury Shenk: [00:24:26] Oh, yeah. There is a wide discussion about Internet harms, but it's directed at stuff like child pornography and terrorist content and destabilizing

political content as well. I still don't think it's as broad as what they're discussing in India, where it's really a vehicle for broad social control like you have in China.

Stewart Baker: [00:24:47] Okay. I want to make this public announcement: The Cyberlaw Podcast has been working on artificial intelligence. And we have the coolest artificial intelligence tools in the world. They're so good, we're not going to tell you about them. That is what OpenAI more or less said. They said, "We're working on this mechanism for taking a sentence or two and turning it into an entire riff. And the AI takes the sentence or two and does the riffing. And it's so good it scares the hell out of us, and so we're not going to release the code or the training modules that produced it." Nick, I actually looked at the riffs, and they aren't that good.

Nick Weaver: [00:25:31] Yeah, it's better. The Markov [chain] bot style stuff just keeps getting better and better. And it also depends on who you want to riff against. So if you want to do fake Fox News, that's gonna be easier than fake NPR because you're going to have to do more content that's semantically right. But even so, it's –

Stewart Baker: [00:25:56] [Laughter] So you're saying the sentences are shorter and the multi-syllabic words are less common on Fox?

Nick Weaver: [00:26:05] It's not just that. It's that you could easily imitate Tucker Carlson with just, "Oh, my God, the brown hordes are coming," and riffs thereof. It takes a little more nuance to do NPR, except for the "give us more money" part.

Stewart Baker: [00:26:23] [Laughter]

Dmitri Alperovitch: [00:26:24] Although, to throw a little bit of cold water on the whole AI hype, there was a great tweet that I saw last week that said, "What is the difference between machine learning and artificial intelligence? If it's written in Python, it's machine learning. If it's written in PowerPoint, it's artificial intelligence."

Nick Weaver: [00:26:39] [Laughter]

Stewart Baker: [00:26:39] [Laughter] That makes perfect sense. Alright. We'll see. Eventually I'm sure OpenAI will release what it's done, but I think we've got a ways to go before we have to be really scared of AI riffing on bits of text. Alright. Why don't we turn if we can, unless – we had a few stories that we were thinking about covering. Maury, Nick, any of those stories that you really want to be heard on?

Nick Weaver: [00:27:11] Yes, on the YouTube one.

Stewart Baker: [00:27:14] Yeah. So YouTube is taking a lot of grief because the comments on a bunch of kids' athletic and gymnastic programs are written by what looks like pedophiles saying, "Oh, go to minute four, second 20, and she does the splits. It's so great," and nasty stuff like that. And advertisers are saying, "We don't want our ads appearing next to comments like that."

Nick Weaver: [00:27:47] The situation's actually worse. It's that once you get on to one of these videos, YouTube's recommendation engine continues down this rabbit hole, and this is a symptom of YouTube's larger problem. You optimize for engagement. You're going to engage specific communities, whether it's anti-vax crazies who don't care that their unvaccinated kids may kill others to QAnon to jihadis to this. And I'm not sure if there's a way to solve the radicalization problem inherent in recommendation models.

Stewart Baker: [00:28:29] Yeah. So the drive to extremes that recommendation engines send you down is very real because there is something – and it could be it drives you towards extremes of weightlifting, it drives you towards extremes of home knitting, or it drives you toward extremes of sexual perversion. And part of this is just it's human nature. Right? They're telling you what other people who looked at this video went on to look at, and those people went on to look at other extreme things precisely because that was their nature. I see the phenomenon. It bothers me. And yet I think it's more humanity than the recommendation engine that's at fault here.

Nick Weaver: [00:29:26] Actually, I think it's both. So what happens is you get multiple feedback loops here where you have the recommendation engine radicalizing humanity and humanity radicalizing the recommendation engine.

Stewart Baker: [00:29:42] Fair enough. As soon as people realize there are other people like them, they get more confident in the values that they share, even if they aren't very attractive values, and so there is a reinforcing effect. So I see the problem. I'm not sure the answer is to say, "Stop doing recommendations," 'cause there's an awful lot of value in those recommendations and an awful lot of subcultures that we're perfectly happy to have continue to prosper. So figuring out when you should stop or moderate your recommendation engines strikes me – maybe because I am a minority in this regard, at least in Silicon Valley – they would cheerfully take three-quarters of my views and say, "We'll never recommend anyone look at those." And so the idea that they should be saying, "People with views like yours should not be able to find each other online" is troubling.

Maury Shenk: [00:30:46] So, Stewart, I'll just jump in on the Lauri Love story in the UK to say a powerful message for wannabe hackers out there: that if you hack into US government websites, even if you don't get extradited to the United States, you probably won't get your encrypted devices back.

Stewart Baker: [00:31:01] Yeah. Talk about chutzpah! He had all this stuff he'd stolen from the United States government, and he said, "What's on my computer? Can I have my computer back now that you've decided not to send me to the United States because I got Asperger," as if that were an excuse. And at least they said no, although I actually think they should have given it back to him with a key logger built in, and then they could have figured out everything that he took and then maybe they have more evidence to prosecute him on.

Nick Weaver: [00:31:34] Or only allow unencrypted data.

Stewart Baker: [00:31:37] Yeah, that could be too. Okay. Dmitri Alperovitch. Dmitri's been on the program many times before. He's always got great, thoughtful views about cybersecurity. And the 2019 Global Threat Report from CrowdStrike had some really interesting stuff in it. Dmitri, can you give me the elevator summary of the report? What are the things that really struck you from this report?

Dmitri Alperovitch: [00:32:04] Yeah. So the report covered what we saw last year in terms of major actors, major events that were taking place, but probably the most novel thing that we did this year is put together an adversary ranking, at least of the major countries that are involved in cyber activity that we had seen. And this is something that I've been asked to provide many times, and I'm sure you have: who is the best out there? We spent a lot of time thinking about what's the right way to do ranking, and pretty quickly we rejected the idea of looking at tools for a couple of reasons. One, you can buy tools, so just because you're a country with billions of dollars to spend doesn't mean I'm going to put you at number one. But also, probably just as importantly, the adversaries often don't use the best tools when they break in, so they use what they need to achieve their objective. So that didn't seem like the right way to rank it. So we started thinking of how do you actually rank people? How do you determine who's got the best folks and who's best at it operationally? We came up with this metric called breakout time, which is really how rapidly can they break out of a beachhead that they establish. The idea is that anyone can spearphish. Lots of people in an organization get people to click. In our tests, when we do phishing tests, we see that on average about 30% of the people in any organization will click on just about anything.

Stewart Baker: [00:33:19] You're doing great if you get down to 20.

Dmitri Alperovitch: [00:33:21] Exactly. So getting in is not the problem. But getting to your actual objective once you get someone to click on a link takes a lot of effort because you have to figure out how to get there, what privileges you need, what credentials you need, where to go. Just imagine yourself in the shoes of someone who is starting a new job. You've got the IT department telling you where the resources are, how to get your machine set up, and anything else. As an adversary, you have none of

that benefit. You still have to figure it out. And we thought that whoever is fastest at doing that, whoever has the shortest breakout time, really is fantastic operationally.

Stewart Baker: [00:33:53] So let me ask you just a question because I didn't understand from reading the report how you measured it: did you kind of find compromises and then walk backwards to see how they got in and how long it took them to get to the full compromise?

Dmitri Alperovitch: [00:34:07] So last year we detected 30,000 major intrusions across lots of industries and governments and countries, and in those 30,000 intrusions where we actually had adversary moving laterally, where they didn't get shut off by the company quickly enough, we looked at those and said, "Okay. When was the first time that they actually had code execution inside the target network, and how long did it take them to actually get off that system and move laterally?" So that was the measurement for breakout time. There are a couple of caveats that I have to mention because not every adversary may have necessarily motivation to move fast, although as defenses are getting better and better, I do think that that is going to become a bigger priority for organizations because if you get detected quickly and ejected, you don't accomplish your mission. So what we're seeing is that adversaries are trying their best to move as quickly as possible. But the ranking came out to be really, really interesting.

Stewart Baker: [00:35:05] Right. So now we're going to do a little drum roll. [Drum roll]

Dmitri Alperovitch: [00:35:07] Exactly.

Stewart Baker: [00:35:09] Let's open the envelope! Who gets the "Strikie" for the year for the best time to breakout?

Dmitri Alperovitch: [00:35:17] Perhaps unsurprisingly, it was Russia. And I have to note that we didn't measure Western intelligence agencies simply because we didn't have data on the operations. We almost never see them targeting our customers for obvious reasons because we don't have a lot of customers in Iran, North Korea, China,

and Russia. And I would expect that they would be at the top of the list, far eclipsing even Russia. But what was most interesting about Russia is how fast they were. They were eight times as fast as their nearest competitor, the country that was in second place, and their breakout time was 18 minutes. So if you think about it from a defender's perspective, that's how long you have to basically contain the incident – 18 minutes – before you have a major breach on your hands. And that again emphasizes that speed is everything in cybersecurity. It is a race against the adversary. And when you're facing the Russians in particular, you have to be really, really fast.

Stewart Baker: [00:36:07] I wonder if it says something about how they're organized, too, that maybe the Russians are more kind of the fighter pilots of cyberspace. They are determined to go in and do everything that needs to be done, as opposed to bit players who say, "My job is to take this beach, and then the next guy will take the cliffs, and the next guy will take the hedgerows after that." Is it possible that the Russians just have some really good all-around players who once they get in can quickly pivot to compromising the rest of the system, whereas other folks have to do it in a more pedestrian way?

Dmitri Alperovitch: [00:36:51] It is possible that in other countries you have teams that you have to do handoffs and there's delays because of that. But one thing to note here is that there was actually a great deal of variance between individual teams within each country. So even in the case of Russia there were slower teams or faster teams, and that's something that we struggle with.

Stewart Baker: [00:37:09] Are you getting emails from people who say, "My bonus depends on you naming me"? [Laughter]

Dmitri Alperovitch: [00:37:13] [Laughter] Exactly. Next year's CrowdStrike report is your goal for whether you get a bonus or not. But I think it is important to understand that every country is going to have an A team and a B team. Generally speaking, we actually see that civilian intelligence agencies are much better than militaries. So in the case of Russia, for example, SVR [Foreign Intelligence Service] is better operationally

typically than GRU [military intelligence]. Same is true in China: MSS [Ministry of State Security] is better than PLA [People's Liberation Army], and so forth. In general, I think it's because in militaries – and this is true in the US as well – people move around too much. In the civilian agency, you get into the job, and you may be in that job for 20 years and you have opportunities to learn from others and really build up your expertise, where in the military you're a tank commander one day, you're a cyber operative the next, and maybe you're an artillery guy the year after that. And it's just hard to become really, really professional at that. I know the US military is struggling with this right now.

Stewart Baker: [00:38:07] I'm not at all surprised that the Russians would be first. I am flabbergasted that the North Koreans are second.

Dmitri Alperovitch: [00:38:15] That is the other big revelation, that North Koreans were second, China third, Iran fourth, and all criminal groups put together were in fifth place with almost 10 hours to breakout on average. Initially, it was surprising to me too. I certainly expected China to be in second place. But I have to say, in thinking this through, it is not a surprise. The North Koreans have been at it for 20 years. When you think about how they recruit people into their cyber forces, there is a great deal of selection that happens. The best kids in high school get into college. The best people in the class get sent into the cyber forces. In China, you just have way too many people, so you can blend in and be average. They certainly have some good people, but with so many people, it's hard for everyone to be the best. And in general, even if you look at Five Eyes [Australia, Canada, New Zealand, the United Kingdom, and the United States], I would say, pound for pound, some of the smaller agencies are better than the US because they just can't afford to have anyone who is average. When you only have five people in New Zealand, each one of those better be a rock star if you want to accomplish your mission. So in general, I think the small organizations are more nimble and have better people as a result. But the other thing I think is important to point out about North Korea is I actually think that they are the most innovative actor in cyberspace bar none. They are the first ones, if you look at the history, to have been using destructive attacks to accomplish coercion and achieve their objectives. They were the first ones to use information operations! We focus so much on Russia, but two

years before Russia, we had Sony. And I think the US government and most of us in the industry fundamentally misunderstand Sony because we so much focused on the destructive element of Sony Pictures attack that we forgot that they stole emails and leaked them to WikiLeaks. Two years before Russia!

Stewart Baker: [00:39:58] Yeah. The Russians clearly were just drafting behind the North Koreans.

Dmitri Alperovitch: [00:40:02] Yeah, exactly. And now you have North Koreans engaging in massive cybercrime in terms of breaking into banks and stealing hundreds of millions of dollars on unprecedented scale. So in terms of actually achieving objectives in cyber, I think they are the best out there.

Stewart Baker: [00:40:16] Wow. You think that others are going to – do you think the Russians will be next to start stealing money?

Dmitri Alperovitch: [00:40:21] Well, we certainly have criminal groups that are doing that in Russia. So far, on the nation state level, we haven't seen a lot of evidence of that, although there is a blending of the two where in the case of Yahoo, of course, we had criminal groups that the FSB [Federal Security Service] co-opted that were also on the side putting money in their pockets as they were executing national security priority missions.

Stewart Baker: [00:40:42] So I'm under the impression the last time I looked at the Verizon Report it was still the case that the time from compromise to discovery of compromise was measured in months. So does it matter really whether you're dealing with somebody who can compromise you in 18 minutes or in nine hours?

Dmitri Alperovitch: [00:40:59] So we tracked that statistic as well. It's called dwell time in the industry, and depending on the company you use, I think on average everyone's around the same, which is about 90 days from detection of an incident to actually determine how long they've been in there. But that statistic is fundamentally misleading

because us and the other firms out there do it based on incident response [IR], and the incident responses are really the cases where things have failed. Right? The victim has been compromised, and for every IR that we do, there are literally thousands of cases where the company is actually able to mobilize and quickly stop the breach, so that data, I think, is highly biased. It's still useful to track, but it doesn't tell the full story.

Stewart Baker: [00:41:39] Okay. So what you're really saying is that people need an internal IR capability that can respond in hours.

Dmitri Alperovitch: [00:41:46] You need to respond quickly. And something that I've been promoting is a set of metrics that I think every organization should adapt, which is a way to measure how fast you are, and I call it the 1-10-60 rule. What is your average time to detection of an incident, average time to investigation, and average time to respond? And the best companies we work with try to detect in one minute on average, investigate in 10 minutes, and remediate and contain in one hour. Now clearly, if you're facing the Russians that break out in 18 minutes, you can't even wait an hour. But on average, if you start tracking what your metrics are – time to detect, time to investigate, time to remediate – and driving that down and reporting that at the board level, at the CO level, quarter after quarter, that is a great way to hold people accountable. I would love nothing more than in the federal government for every agency to provide every quarter or at least on an annual basis what are their averages for time to detect, time to investigate, time to remediate, and we can see who is doing better than others and who is going in the other direction, despite all the budgets and people that –

Stewart Baker: [00:42:42] Of course, at this point you're advertising, "Oh, yeah. Kick me." [Laughter] But, yes, I take your point. Let me ask this: thinking about tools, are there tools that could say, "Look, there are certain things that people are looking to break out routinely do." Is there a way to slow down some of those processes in the face of suspicious but not clearly malicious activity?

Dmitri Alperovitch: [00:43:09] Sure. And that's another caveat with the report is that obviously it's a lot easier to break out when the network is Swiss cheese versus one

that's much more hardened, but it averages out because the networks who were targeted by all these adversaries had a mix of really hardened target networks and not so much. And really I think what shows in terms of the Russian ability to be fast is how agile they are, how quick they're on their feet, because, as you know, in any military plan, the plan goes out the window at first contact with the enemy. Well, the same is true in cyber. You land on a system. You don't know where you're going to land. Is it fully patched? Does it have local admin credentials on the box? Is a user logged in? So you have to quickly adapt and try various things that –

Stewart Baker: [00:43:53] It's like that TV show *Naked and Afraid*. Right? They drop you in with no clothes, and you're supposed to live off the land. [Laughter]

Dmitri Alperovitch: [00:44:00] Exactly right. And what makes the Russians so good is that they're able to adapt to the environment and use different tools. Right? It's not that they have some magic silver bullet that just allows them to break out every time. In fact, virtually every adversary most of the time uses Mimikatz. I call it the AK-47 of cyber. Every single adversary group we've seen has used it at one point or another, but they don't rely on it exclusively. And they know that in cases where it's not working, they need to try something else, and that ability to quickly pivot and do something different is what separates the great from the just average.

Stewart Baker: [00:44:36] So the other thing that I noticed in the report: you talked a little bit about the difference between malware compromises and malware-free compromises. And there were striking differences between industries between whether people were mainly compromised with malware or malware-free attacks. Can you explain what the difference is and why that might be the case for some of these industries?

Dmitri Alperovitch: [00:45:01] So in general, we have seen a major trend on the part of many adversaries to try not to use malware because malware is noisy. Any time you have an unknown program running in your environment, it can trigger suspicions. So the best thing to do is live off the land.

Stewart Baker: [00:45:14] This is the success of signature-based and SIEM [security information and event management] tools. As soon as something funny starts happening, a team that's well prepared starts to see it.

Dmitri Alperovitch: [00:45:24] Yeah. Less signature-based and more endpoint detection and response [EDR] type of tools. EDR tools out there, they record everything that's going on so you can start to look at anything that's anomalous. So adversaries have for a while now been adopting tools like PowerShell and common Windows programs that they can use to achieve those objectives without bringing anything into the environment that there would be foreign to that environment could trigger suspicions. It is interesting that in some industries we're seeing a lot more of the malware-free attacks than in others. I think it's more dependent on which adversaries are more likely to target them and which ones prefer that type of tool kit. In a lot of criminal cases, we still see a lot of malware being used, a lot of Trojans, a lot of ransomware –

Stewart Baker: [00:46:04] Because they're spray and pray typically.

Dmitri Alperovitch: [00:46:08] Exactly. They don't need to hit every single one. In target intrusions where you really care about not being detected quickly, you may use more living-off-the-land tradecraft.

Stewart Baker: [00:46:18] So if that's the case, I mean just look at this list, it looked to me as though actually the people who were least likely to get malware-free attacks were pharmaceuticals and oil and gas and financial. Those are folks where I would have expected they had pretty sophisticated defenses, and yet they seem to be attacked mainly with malware attacks.

Dmitri Alperovitch: [00:46:44] I have to tell you, Stewart, this is the biggest misconception that I've seen where the idea that some of these industries are so good at cybersecurity. It really is a general rule of thumb of what I've seen: the bigger the

organization, the worse they are. Too much bureaucracy. Too much consensus. It's not about the budgets and the people. But look at DoD, for example. They're horrible at cybersecurity, despite the fact that they're spending more than any other organization on the planet and have more people. It's just too hard when you've got different fiefdoms and authorities and everything else, and we're seeing that in some of the largest organizations out there. But the biggest thing that I've seen that makes an effect is really the investment of the leadership, of the CO, of the boards of directors. They don't really need to understand the technical details, but if they're giving you the support to say, "We're not going to go into that country and do business there," or "We're going to make these changes to business process that may impact our revenue because cybersecurity is more important," those are the organizations that as a rule of thumb are doing really, really well. And those that take the approach of "Cybersecurity is for that guy in IT to figure out and secure us," those are the ones that you see on the front pages of newspapers reporting major breaches.

Stewart Baker: [00:47:50] Okay. So new participants – at least they were new to me – that you talk about in this, not exactly surprises but still interesting: India, Pakistan, South Korea, Vietnam. My guess is that most of those were goaded into this by discovering that they'd been had by their principal geopolitical adversary. What's your take on the skills and targeting of those different new entrants?

Dmitri Alperovitch: [00:48:23] South Korea is actually very good, as you would expect. Very technological society. Learned a lot from close cooperation with the US military obviously.

Stewart Baker: [00:48:31] Plus getting pwn'd and pwn'd and pwn'd. [Laughter]

Dmitri Alperovitch: [00:48:32] Exactly. Vietnam is getting very, very good. And Vietnam is actually the biggest concern because they're getting very active in IP theft issues, trying to emulate China, and they're sort of the next big economy that's trying to bring manufacturing and improve domestic capabilities. India and Pakistan are mostly going after each other, so we see less of them in other areas of the world. But certainly

Vietnam and South Korea are the ones that I recommend for Western companies to keep an eye on.

Stewart Baker: [00:49:04] So the Indians and the Iranians often cooperate, not as overtly as you might think, but is there any sign that there's been a TTP [tactics, techniques, and procedures] sharing in that sphere?

Dmitri Alperovitch: [00:49:21] What you have in the region in general is contractors that are basically mercenaries for hire, and you have a number of companies in India that have worked all over the Middle East doing operations for various Middle Eastern countries. So you see some of that, perhaps not directly sponsored with the government, but at least with a government closing their eyes to that activity. So I don't think it's intelligence-to-intelligence-agency cooperation, at least we haven't seen that yet. But certainly cooperation amongst people and resources.

Stewart Baker: [00:49:53] Okay. So the other thing that I was struck by as I went through the report was how often you said, "Oh, and then they compromised credentials. Maybe they got hashes, and they took them offline and whacked that 'em until they could compromise 'em, or they just got 'em in plaintext with man-in-the-middle attacks or logging attack." Isn't it time everybody was using two-factor authentication for everything corporate?

Dmitri Alperovitch: [00:50:20] Well, and we've seen attacks where two-factor is being broken via social engineering attacks, so that's not a panacea either. It certainly raises the bar. But don't think that just because you're using two-factor you're immune. And the Russians in particular are very, very good at prompting you for two-factor and then using man-in-the-middle attack to basically pass it onto the ultimate service. So we are seeing greater adoption of two-factor, but it's not solving the problem. And most of the time, your Windows credentials are not being protected by two-factor. Very few organizations are doing that. And that's where we're seeing sort of the fuel, if you will, for breaking out is this theft to those credentials that allows you to move laterally across the network.

Stewart Baker: [00:51:01] So this is kind of an interesting side note, and I don't know how seriously to take it: one of the stories we didn't talk about today was that the DPRK [North Korea] is attacking Russian targets, and at the same time, the Russians are pretending to be the DPRK when they do some of these intrusions. What's going on there? Is there some subterranean conflict that we just aren't seeing, or is this just the Russians having fun and the DPRK wanting to pwn anybody who neighbors them?

Dmitri Alperovitch: [00:51:37] Well, when you've got friends like these, who needs enemies? But the reality is that this is just another indication that the alliance like what we have with the Five Eyes and even with NATO does not exist amongst our adversaries. They don't trust each other. The Chinese have been going after Russia for many years now, stealing their defensive technology, oil and gas espionage, and the North Koreans are doing the same. No one trusts each other in that region, and they're all keeping an eye on each other. With regards to the Russians, we've seen them try to pretend to be DPRK in the case of Olympic Destroyer, the attack on the Olympic Games.

Stewart Baker: [00:52:09] And that was a sad attempt at false flag, wasn't it?

Dmitri Alperovitch: [00:52:12] Yeah. In general, these false flag attempts are very, very basic. It seems like someone just pulls a couple of strings from some malware that they had seen and adds it to the code, thinking that perhaps –

Stewart Baker: [00:52:22] It'll give them deniability maybe?

Dmitri Alperovitch: [00:52:24] Well, someone may fall for it, but in reality, no one actually does. It's really, really hard to do a good false flag operation where you replicate everything that the other adversary is doing. And even in the case of the attack on the Olympic Games, all you had to do was ask why would North Korea attack the Olympic Games when they're in the midst of their charm offensive, they're sending people and teams over to South Korea and the sister of Kim Jong-un? There was only

one country that was banned from the Olympic Games, and you know it was pretty clear who might be responsible.

Stewart Baker: [00:52:56] And look, 95% of the time, just asking *cui bono* – who is interested in these things, these targets – tells you who did it. But there are limits to common sense, and we learned those limits when we decided that Saddam Hussein was acting like a guy who was hiding his WMD program when, in fact, he was hiding the fact that he didn't have one anymore.

Dmitri Alperovitch: [00:53:19] It's a good clue. It's not enough. And you have to have more evidence for sure, but generally, it can point you into the right direction to pursue. Just like any time you do a criminal investigation, the first thing you ask is who has a motive. That's not everything, but it's a good start.

Stewart Baker: [00:53:35] Right. Always ask who's the spouse. [Laughter] Okay. Just two other things that I want to ask about. You talked about Russian and Chinese upstream attacks, and I wanted to hear a little bit more about how those work and how much of a threat they are.

Dmitri Alperovitch: [00:53:55] Absolutely. And the Justice Department did a great indictment of this recently with MSS operatives. They were accused of going after managed security service providers – managed service providers in general, not just security – and this is something that we've seen for a while now for a number of years from the Chinese, and in some cases the Russians, where they're trying to get into the supply chain, they're trying to compromise either service vendor or the software vendor – NotPetya was a great example of that where they targeted the MeDoc application that was used in Ukraine for filing taxes. So this is something that is a big trend and something that is increasingly worrying to companies because you can be fantastic at securing your perimeter, if you have a supply chain vendor or contractor that's not secure, they can be the way in for the organization. So we will see a lot more of those going forward.

Stewart Baker: [00:54:42] Yeah. That is for sure a big worry. What about the telecom – you talked a little bit about telecom company attacks also as upstream attacks?

Dmitri Alperovitch: [00:54:53] Yeah, telecom industries are some of the most targeted out there. As you can imagine, every nation state wants to get in and tap communications, get to the lawful intercept –

Stewart Baker: [00:55:02] It's all NSA thing.

Dmitri Alperovitch: [00:55:02] Communications to see if that government is watching. Perhaps there are assets in country. So just a wealth of information, and with SS7 and all those capabilities, there's phenomenal attacks you can launch against others through that medium. And that's why, I guess in this country and across our allies, there's so much discussion around Huawei and 5G because if you turn over the keys to your adversary for those types of communications, what's the point of even trying to protect them?

Stewart Baker: [00:55:35] Okay. Last thing that I pulled out of this was a discussion of cybercrime, which is a much bigger concern than nation state intrusions for a lot of people, and the adoption of what was a nation state persistent attack tactic to build enough information so that you could really deliver a ransomware attack or maybe a CEO attack that was very credible and very effective and would guarantee you a lot of money. Can you talk a little bit about the evolution of that kind of attack?

Dmitri Alperovitch: [00:56:12] Absolutely. We call it the "big game hunting" where as opposed to doing the large, widespread attack and seeing who clicks, you're gonna pick a target, you're gonna do some research into who is most likely to pay ransom – maybe they paid ransom in the past, which is one of the reasons people should be hesitant to offer a ransom – but then you actually do old-fashioned intrusions – break in, steal credentials, get domain admin on the network, and then deploy ransomware to lock up as much of the systems as possible. We've seen that in the city of Atlanta. We've seen it in other places. And one group that we track out of Eastern Europe called Ryuk has

actually managed to steal over $4 million from 52 victims. This is actual ransom those paid over the course of the last six months. So great payoff and great ability to do these targeted attacks. And one type of group that we are particularly concerned about are the West Africans, the Nigerians, and folks from Ghana. They're doing these business email compromises where they can actually hack into the network, watch emails between CFO, between accounting people, CEO, emulate an email from one to the other to issue fraudulent wire transfers, figure out exactly what the limits may be, who has authority to approve it, and people have literally lost hundreds of millions of dollars as a result of those attacks.

Stewart Baker: [00:57:31] Yeah. It's scary. Actually what's scary is that $8 million is not a lot of money. I mean, a business that grossed $8 million would be a small business in the United States.

Dmitri Alperovitch: [00:57:44] In six months? I'll take it.

Stewart Baker: [00:57:47] Okay. Alright. Yeah that's $16 million. Okay. But it's discouraging that there are so many attacks and they cost us so much when the motivation to do them is not quite as big. These are not guys with white cats in their lap.

Dmitri Alperovitch: [00:58:05] And these were 52 victims. There are probably hundreds of other victims that chose not to pay a ransom and probably suffered hundreds of millions of dollars in losses.

Stewart Baker: [00:58:12] Alright. So what did I leave out that you want to talk about?

Dmitri Alperovitch: [00:58:15] Well, the one big thing also is us really declaring – and I've said this in the past publicly as well – is that the deal, the Obama-Xi deal –

Stewart Baker: [00:58:24] Ah, is over. Yes.

Dmitri Alperovitch: [00:58:26] The Chinese espionage is back in force, and we're seeing literally on a daily basis targeting Western industries that have no dual-use capability whatsoever. There's no question that what they're stealing – medical research, pharmaceutical, manufacturing data – is not national security priorities. There are those, too, of course, but it's clear that they're back to their old ways of stealing intellectual property for the purpose of economic espionage.

Stewart Baker: [00:58:51] So from the Trump Administration's point of view, just to take the tariffs off, they oughtta say, "The price is you got to stop this. Just go back to the status quo ante. You're obviously doing it because you're mad at us. We understand that, but you've got to stop." Would you know if they did stop?

Dmitri Alperovitch: [00:59:10] Yes, absolutely. So we saw them stop shortly after the deal, and that continued for about a year. A lot of people at the time said, "Oh, maybe you're just not seeing them. Maybe their tradecraft is so good." That was nonsense. Maybe it was so good for a year, and then they went back to their old ways? Makes no sense whatsoever. So absolutely certain that we would pick it up again, and we would be able to actually observe compliance. But it is interesting that that deal was important, even though it didn't last, because it was the first time ever we've actually managed to get an adversary to change their behavior, even if for a short period of time, and I think there are probably lessons to be learned from that. Why did they do that? Because they're really afraid of our sanctions. They were afraid that we were going to undermine their companies and prevent them from being able to do business, not just in the US but all over the world. And we need to find more leverage points against them and other adversaries to actually change their behavior.

Stewart Baker: [01:00:02] Yeah. So it's not that we can't do it. Now that we've got decent attribution, we need to find better retribution to make clear what we will and won't tolerate.

Dmitri Alperovitch: [01:00:15] Deterrence works. You just have to find the right levers to pull on.

Stewart Baker: [01:00:17] Alright. Dmitri, thanks so much for doing this. This was great.

Dmitri Alperovitch: [01:00:23] Thanks for having me.

Stewart Baker: [01:00:23] It was a real pleasure to have you on the show. Thanks to Dmitri Alperovitch of CrowdStrike, to Maury Shenk and Nick Weaver for joining me on the News Roundup. This has been Episode 252 of The Cyberlaw Podcast, brought to you by Steptoe & Johnson. I want to congratulate Dr. Megan Reiss. You're not going to hear her on the program because she has a new job on the Hill working for Senator Romney's foreign affairs committee. So if you're thinking about whether you should participate in The Cyberlaw Podcast, it's good for your career, among other things. Also could get a bounce and launch your own podcast series like Nate Jones and Dave Kris, who have a Rule of Law podcast series. The first episode is up now on the Lawfare Podcast. If you want to suggest somebody else to appear on the program, if you do and they come on, we'll give you a highly coveted Cyberlaw Podcast mug. Dmitri, you probably have several, but we'll give you another one if you want one. Send those suggestions to CyberlawPodcast@Steptoe.com. This week I did get the topics out on Twitter, @StewartBaker, and also up on LinkedIn. Please do rate our show. We're still stuck with one review on Stitcher that didn't like my politics. So if you can tolerate my politics, go there and say, "Yeah, it's alright, even despite them." Also Google Play, Spotify, we'd love to have reviews there as well. Coming up: Gordon Crovitz and Steve Brill, the odd couple of content management at NewsGuard; Elsa Kania, one of our favorite China analysts from the Center for a New American Security; Amy Zegart from Stanford's Hoover Institution; Adam Segal from the Council on Foreign Relations. All upcoming guests on the program. Laurie Paul – soon to depart – is our producer, along with Christie Jorge. Laurie has gotten a better job someplace else. Doug Pickett is our audio engineer. Michael Beaver's our intern. We've given him new responsibilities and more money, so he won't be leaving hopefully soon. And I'm Stewart Baker, your host. We hope you'll join us next time as we once again provide insights into the latest events in technology, security, privacy, and government.