United States Department of Justice

National Security Division Press Conference

Tuesday, September 16, 2020

CORPORATE PARTICIPANTS

Jeff Rosen - *Deputy Attorney General*

John Demers - *Assistant Attorney General for National Security*

Michael Sherwin - *Acting U.S. Attorney for the District of Columbia*

James Dawson - *Acting Assistant Director in Charge of the FBI's Washington DC Field Office*

David Bowdich - *FBI Deputy Director*

PRESENTATION

Marc Raimondi
Thank you for being here. We are going to have a press conference today announcing APT41, which is Advanced Persistent Threat. We're going to have four speakers. We're going to start out by the Deputy Attorney General. Then we're going to be followed by the DC U.S. Attorney, Michael Sherwin, followed by the FBI Deputy Director, David Bowdich. And then Assistant Director in Charge of the Washington field office, FBI, James Dawson. Also on stage but not speaking, but available for Q&A is the Assistant Attorney General for National Security, John Demers.

The way that the press conference will work, is they will each come out and make brief remarks. We'll ask the operator to open the line for questions, follow the operator's instructions on how to do that. All questions are coming in through the phone line because this is a virtual press conference. You'll get one question and if you need a follow up, just re-queue, but we're probably not going to get through all of the questions in the initial phase of the press conference. But we are doing, immediately following the press conference, when the principles leave, and the cameras go down, those on the phone line are welcome to remain behind for a case briefing, and then we will get to all of your questions.

So, we're gonna be back in about a minute. So, I'd like, operator, please keep the line open, and we'll be right back, and we'll go right into a start. Thank you.

Jeff Rosen
All right. Well, good morning. Thanks for being here today. I'm Jeff Rosen, and with me, are FBI Deputy Director David Bowdich; Assistant Attorney General for National Security, John Demers; Acting U.S. Attorney for the District of Columbia, Michael Sherwin; and Acting Assistant Director in Charge of the FBI's Washington DC Field Office, James Dawson.

We're here today to announce coordinated, wide ranging actions to disrupt the malicious cyber activities of a group commonly referred to as Advanced Persistent Threat 41 or APT41, as well as a related international criminal enterprise involving APT41 actors. Cyber security experts have referred to APT41 activities as one of the broadest campaigns by Chinese cyber espionage actors in recent years.

We are announcing today, multiple efforts to disrupt these activities. First and foremost, is that we have unsealed three indictments that collectively charge five Chinese nationals with computer hacking and charged two Malaysian nationals for helping some of those hackers target victims and sell the fruits of their hacking.

Our charges allege two distinct categories of criminal conduct. First, as the core of APT41's computer hacking, the Chinese defendants targeted well over 100 victims worldwide in a variety of industries and sectors that are sadly part of the standard target list for Chinese hackers. These criminal acts were turbocharged by a sophisticated technique referred to as a supply chain attack, in which the Chinese hackers compromised software that providers around the world had and modified the providers' code to install backdoors that enabled further hacks against the software providers' customer's.

Second, and as an additional method of making money, several of the Chinese defendants compromised the networks of video game companies worldwide. That's a billion dollar industry

and defrauded them of the in game resources. Two of the Chinese defendants stand accused with two Malaysian defendants, of selling those resources on the black market through their illicit website.

Now, in addition to these unsealed indictments, I'm pleased to announce that through the cooperation of the Malaysian law enforcement authorities, the two Malaysian defendants were arrested on Sunday evening, and now face extradition proceedings. So, we have the indictments and two arrests. Identifying those responsible and holding them account is our primary mission. But criminal investigation and prosecution alone are not enough to make the internet safer.

So, there's a third part of today's announcement. Specifically, in addition to these criminal charges, and the two arrests, the Department of Justice and the FBI have been working with seven private sector partners, including Microsoft, Facebook, Google, Verizon Media, and others, to identify and neutralize the computer infrastructure that APT41 uses to conduct its crimes. It's virtual private servers, malware, malicious domains, and other tools.

We have done this through a combination of public and private actions, including technical measures to block this threat actor from accessing victim's computer systems, issuing a public safety announcement outlining their tactics, techniques, and procedures to aid network defenders. And by taking control of, or otherwise disabling, their accounts pursuant to court orders and Terms of Service violations. The bottom line is that we have used every tool at the department's disposal to disrupt these APT41 activities.

Now, ideally, I would be thanking Chinese law enforcement authorities for their cooperation in the matter and the five Chinese hackers would now be in custody awaiting trial. Unfortunately, the record of recent years tells us that the Chinese Communist Party has a demonstrated history of choosing a different path, that of making China safe for their own cyber criminals, as long as they help with its goals of stealing intellectual property and stifling freedom.

Less than two months ago, Assistant Attorney General Demers was at this podium to announce an indictment in another hacking case, in which the Chinese government tolerated the defendants' criminal activity because those defendants were willing to work on behalf of the Chinese intelligence services. And here we are again.

In this case, one of the Chinese defendants is accused of boasting to a colleague that he was "very close" to the Ministry of State Security and would be protected "unless something very big happens". The Hacker and his associates agreed not to "touch domestic stuff anymore." We know the Chinese authorities to be at least as able as the law enforcement authorities here and in like-minded states to enforce laws against computer intrusions, but they don't do so.

But know this, no country can be respected as a global leader while paying only lip service to the rule of law and without taking steps to disrupt brazen criminal acts like this. No responsible government knowingly shelters cyber criminals that target victims worldwide in acts of rank theft. Responsible nations not only condemned criminal conduct, they routed out and punish it. Responsible nations disavow criminals within their borders and bring them to justice. Responsible nations work with other countries law enforcement authorities to ensure that justice is served in a court of law. The PRC has done none of these things.

So, you can take three additional observations from this conference today. First, the Chinese government has the power to help stop crimes like this. Second, the Chinese government has made a deliberate choice to allow its citizens to commit computer intrusions and attacks around the world, because these actors will also help the PRC. But third, the Department of Justice will do everything it can to disrupt these crimes by exposing the techniques, tactics and procedures used by APT41, by enabling the private sector to disable them, and by working with our law enforcement colleagues all around the globe, to arrest the hackers when we can, as with the two today.

We appreciate our partnerships with the private sector. As I said, in this instance, including Microsoft, Facebook, Google and Verizon media. And our partnerships with foreign law enforcement partners, who have been a force multiplier in these fights against international criminals. Such partnerships send a clear message that governments and the private sector are prepared to work together to defend against significant cyber threats.

Today, on top of all the measures I've mentioned already, we are exposing this threat to the international community, to cybersecurity experts, and to the greater public. And we will never stop pursuing the individuals responsible for these alleged criminal acts, here and abroad, and anywhere they travel. Now at this point, I will turn the podium over to acting U.S. Attorney, Michael Sherwin, who will discuss the allegations in the indictments in greater detail.

Mike?

Michael Sherwin
Thank you, sir. Alright. Ladies and gentlemen, the scope and sophistication of the crimes alleged in these three indictments that we unsealed this week are really unprecedented for several reasons. As previously mentioned, hundreds of corporations and thousands of individual accounts were targeted by these Chinese hackers and causing upwards, estimated, millions of dollars in damages.

Now, what makes these indictments more troubling and more interesting to some degree, is the fact that we now see these hallmarks of hackers targeting, in addition to the standard corporations that were targeted, business institutions, universities, we also see online gaming companies, which the Deputy Attorney General just mentioned, is a billion dollar industry. So, this is a new target rich environment in which hackers are targeting.

And as we'll go through with these indictments, the Chinese hackers are working in concert with the two Malaysians to, not only hack into these online digital gaming companies, but then essentially fence and sell digital currencies, tokens, coins, on gaming platforms to third parties, and essentially victimizing these online gaming companies and laundering those proceeds back to the Chinese.

So, the first indictment, ladies and gentlemen, the Zhang indictment, deals with to Chinese nationals and there's really two criminal schemes related to this first indictment. The first criminal scheme is the basic brute force type hacking that we've seen in other cases. But this scheme also involved, as the Deputy Attorney General just mentioned, this supply chain attacks, in which the Chinese hackers, in a very sophisticated way, would hack into software companies, insert malicious malware, that software then would be sold to innocent third parties for corporate use. But the software is a Trojan horse, which allowed the hackers to then get into

the third party databases and steal more proprietary information. And that's seen and elicited throughout that first indictment.

In addition to that, that first criminal scheme that we outlined in that first indictment, we also see another scheme in which these two Chinese hackers were working in concert with the two Malaysians, in which they were targeting online gaming companies throughout the world. And once they would target these online gaming companies, as many people know, especially if you have kids, there's a lot of coins, tokens, digital currency, involved in a lot of these online games. They would steal that digital currency, they would then work with the two Malaysians that are cited in indictment number two, that would then essentially fence and sell that stolen digital currency online to other innocent third parties.

So, this is again, troubling because we see this as unfortunately a new area in which hackers are exploiting, and its a billion dollar industry, and I'm sure this isn't the end. We're going to see much more of this criminal conduct, unfortunately. The third indictment, ladies and gentlemen, deals with three Chinese nationals, very similar to the allegations in the first indictment with the two Chinese nationals. Very basic allegations of brute force hacking.

But what's interesting in the third indictment, ladies and gentlemen, is there's a reference to Shang Doug 40 (SP), which is a Chinese corporate entity which is closely linked to the Chinese government, does work for them. And it has close contacts with the Chinese People's Republic Army and also the Chinese Military Security Apparatus. So, in terms of that third indictment, we see hacking, we see the theft of the proprietary information. And again, hundreds of corporations targeted throughout the world, with millions in losses.

So these three indictments, ladies and gentlemen, essentially are trying to telegraph to the world that the Department of Justice, the FBI, the U.S. Attorney's Office will fix, find, and indict cyber criminals in any corner of the world, be it Malaysia, China, Eastern Europe, Western Europe, and bring them to justice here in the District of Columbia.

Without much more to say, I want to first of all, thank the AUSA’s that weren't involved in this case, in the U.S. Attorney's Office. And also, the amazing and extraordinary work of the FBI, in working this case up, because it was very sophisticated and involved a tremendous amount of effort by the Bureau.

So, right now, I'm going to turn over the podium to Deputy Director, David Bowdich. Thank you.

David Bowdich
Alright. Thank you, Mike. Alright. Good morning. I've been up here all too often, with my partners from the Department of Justice, talking about hackers, in particular, Chinese hackers. And here we are again. We're here today to tell these hackers and the Chinese government officials who turned a blind eye to their activities that their actions are, once again, unacceptable, and we will call them out publicly.

We've been fighting the cyber threat for years now. And all too often, it's been a game of whack a mole. We investigate one hacker group, and we quickly uncover another hacker group. We disrupt one nation’s state adversary targeting our infrastructure and our intellectual property, and very quickly we are oftentimes exposing another side of that nation state actor, or another nation state actor as well.

Some days it seems like a never ending battle. But cyber is one of our highest priority. In fact, the FBI's new enterprise strategy highlights how important it is to us. The FBI's priority number two is to protect to the United States against foreign intelligence, espionage, and cyber operations.

Our number three priority is to combat significant cybercriminal activity. And we've been taking a closer look at what the FBI can bring to this fight. Our cyber strategy, in a nutshell, is designed to impose both risk and consequences on our adversaries. In plain English, we want to make it more difficult and more painful for hackers and criminals to do what they're doing. And the best way for us to do that is by leveraging our unique authorities, our unique capabilities, and our enduring relationships, not just in the U.S., but throughout the world.

We want to build on the innovation that has helped the FBI and our partners adapt and evolve to meet the evolution of threats throughout the past century. We've got to change the cost benefit analysis of criminals and nation state actors who believe they can compromise United States networks, steal U.S. financial and intellectual property, and hold our critical infrastructure at risk, all without imposing risk to themselves.

Indictments are only one way in which we do that. But often, that's all we can do. We indict the criminals, we come up here on stage, and we call them out publicly. This time, as Deputy Attorney General stated earlier, due in a large part to the efforts of our folks here, but also in a large part to our Malaysian law enforcement counterparts, we have two people in custody. And we are seeking their extradition, to bring them to the U.S. to face these charges.

The cyber threat is not a problem that any one agency can address by itself. So central to our strategy is, the role the FBI plays as an indispensable partner, to our federal counterparts, our foreign adversaries, and our private sector partners. We want to make sure we're doing everything we can to help our partners do what they need to do. And the private sector, and the partnerships that have been developed over time, cannot be understated. They're an incredibly important component in the cyber fight.

That means using our role as a lead federal law enforcement agency with law enforcement and intelligence responsibilities to not only pursue their actions, but those of the adversaries overseas. To enable our partners, to defend networks, to attribute malicious activities, to sanction bad behavior, and to take the fight to our adversaries overseas as much as we possibly can.

To that end, later today, we will be distributing a flash message to our private sector partners and our foreign partners. A flash message essentially provides the expertise necessary, and the technical expertise necessary, for them to defend their own networks. We believe it will be helpful in not only detecting but mitigating APT41's malicious activities.

Before I wrap up, I want to remind you what I have said almost every time we've been up here at the podium when it comes to an indictment of Chinese hackers. Our concern is not with the Chinese people. Our concern is not with the Chinese Americans. But specifically, our concern is with the Chinese Communist Party. Confronting this threat effectively does not mean we should not do business with the Chinese. It does not mean we should not host Chinese students. And it does not mean we should not welcome Chinese visitors or coexist with China on the world stage as a country.

What it does mean, is that when China violates our criminal laws, and our international norms, we will call them out. We're going to work together with our partners at home and abroad, in law enforcement and in the private sector, to stop brazen cybercrime and hold people accountable. The cyber threat is daunting, but with the tailored approaches that we've put together in each situation to bring together the right talent, and the patriotic people, their tools and the authorities we've been provided at the right times, we have the ability to understand and combat the cyber threat.

So, let me talk about those people. I want to quickly call out our special agents, our analysts, our computer scientists, and quite frankly, the prosecutors, that worked on this case and work on these cases on a day to day basis. These cases are tedious; they are detailed; they require a significant level of expertise, and they require more than anything, tenacity. I want to thank them for their work for the American people.

To the hackers, I want to tell you, whether you're in the U.S. or whether you're overseas, just because you have not yet seen an indictment, does not mean that there is not a prosecutor, working with a group of agents and supporting cast, putting together an indictment for you as we speak.

Thank you. Next up, I want to introduce our acting as Assistant Director in Charge of the Washington Field Office, Jim Dawson.

Jim Dawson
Good morning and thank you Deputy Director, Bowdich. Today's actions charging five China based and two Malaysia based hackers, demonstrate the tenacity of the FBI's Washington field office and our government partners to ensure all criminals are held accountable for their actions, no matter their location.

We are committed to bringing justice to all victims of cybercrimes. These hackers compromised the computer networks of more than 100 companies around the world. These intrusions allowed hackers to steal source code, customer account data, and personally identifiable information. Using their access, the hackers not only compromised an individual company, but also used their access to compromise a company's customers, extending the effects of their crimes.

These actions were often conducted using, maintaining, and communicating with computer and internet infrastructure located in the United States. Several of these defendants also defrauded video game companies through manipulation of in game resources to increase their illicitly obtained income. These four profit criminal activities took place with the tacit approval of the government of the People's Republic of China.

This investigation is another example of the blended threat increasingly seen in cyber investigations. To address these threats, the FBI brings together its expertise in criminal national security, and cyber investigations, to bring justice to these actors who attempt to take advantage of the supposed anonymity and lack of geographical limits of cyberspace.

The companies and individuals victimized by these criminals are located around the world. Their crimes transcended borders, which is another reason the FBI and our partners must work together to bring these individuals to justice, no matter where they might reside. In this case, we're immensely grateful to the Malaysian government for their willingness to assist us with the arrest and extradition of two of these hackers.

In addition to the Malaysian government, we would also like to thank the private sector companies who have taken proactive measures to harden their network vulnerabilities utilized by these actors. Notably, we are unable to extend any gratitude to the Chinese Communist Party, or to the government of the People's Republic of China, which was unwilling, or unable, to address the egregious cyber-criminal activity of its citizens.

As always, the FBI will continue to work with its partners to identify those who conduct cyber-attacks against our nation, bring their actions to light, and hold them responsible, wherever they are. Thank you.

And I'll yield the podium to Deputy Attorney General Rosen.

Jeff Rosen
So, let me add my thanks to both the FBI for the outstanding work by the entire team there, and to our lawyers at both the National Security Division and the U.S. Attorney's Office. It's outstanding work, and on behalf of the Department, I want to express my appreciation for that as well.

I think at this point, we'll (INAUDIBLE) questions.

Operator
Thank you. We will now begin the question and answer session. To ask a question, you may press star, then one, on your telephone keypad. If you're using a speakerphone, please pick up your handset before pressing the keys. To withdraw your question, please press star, then two. We ask that you please state who you are directing your question to.

At this time, we'll pause momentarily to assemble our roster. And our first question will come from Eric Tucker with the Associated Press. Please go ahead.

Eric Tucker
Yes. Hi. Thank you so much. I suppose this question is perhaps best directed to the Acting United States Attorney, Michael Sherwin. I was wondering if you could please elaborate on two different things. One, is the connection that you alleged between this hacking group in the Chinese government. I'm trying to determine whether it's a, sort of, a test connection or more of a direct link.

And also, for, sort of, the nonprofit hacking related efforts, what do you think is the primary motive that you're seeing, in terms of the intrusions that are targeting universities and think tanks, and elements like that? Thank you,

Jeff Rosen
Mike, come on up.

Michael Sherwin
Yes. So, I want to start off by saying in neither, in any of these three indictments, do we blatantly allege that these acts were state sponsored. However, the caveat is this, in those indictments you have to ask two questions. One, who is doing the hacking, and who is being hacked. Now, the general nature of that hacking was for personal benefit with those defendants.

However, if you parse through those indictments, you're going to see some targets that were not corporations. You see targets such as pro-democracy groups, you see targets such as democracy think tanks and universities. Now, a hacker for profit is not going to hack a pro-democracy group. This is a breadcrumb that shows that these individuals were working for private, personal gain, yes, but they also were proxies.

That's a conclusion you could draw for the Chinese government. Why can we say that? We can say that for a few reasons. One, as alleged in the indictment, some of the lead defendants boasted and mentioned that they had communications and contacts with the state apparatus of China. They also mentioned that, and again, I believe it's in the third indictment, the Zhang indictment, that it is okay to target externally internationally, but a no go domestically.

So, that's showing that there is some tacit approval, or there's some tacit direction that they're getting from the Chinese government. Did I address all of your questions, sir?

Eric Tucker
Yea.

Operator
Thank you. And the next question will come from Dustin Volz with the Wall Street Journal. Please go ahead.

Dustin Volz
Hi, thanks so much for doing the call. Two quick questions on the so called supply chain attacks. That seemed like a pretty interesting mechanism used here. Can you just give us more details about, sort of, how widespread that was in the campaign, or how many of those victims were impacted by that approach of compromising the software companies that were then injecting updates to third parties?

And then on the companies that were helpful in the investigation, Facebook, Microsoft, Google, and Verizon, any more details just about how that assistance worked, how long they were involved? And is there any evidence that any of them were themselves targeted or compromised by this campaign?

Jeff Rosen
Okay. So, those are important aspects. Why don't we take them separately? Mike, you want to address first the supply chain attacks, because that is a very important element here?

Michael Sherwin
As again, I'll be brief, but as mentioned earlier, these supply chain attacks did occur in the conduct related to these indictments. However, this isn't the first time we've seen that. This isn't a novel type of a hacking attack. We've seen this before over the past several years. So that's not novel, but it is sophisticated. And most of that was, as mentioned, malware would be inserted into that software that would then be sold to third parties. That creates backdoors, so you could further exploit those customers that purchased that software.

Unknown Speaker
About the cooperation in the private sector.

Michael Sherwin

Sure. I mean, I think on that, we're not going to say more than what we've already said publicly and, in the indictment, in terms of the cooperation we've gotten from the private sector. But we're obviously very grateful, both to those who were named and those who were not named.

Jeff Rosen
And I think I just said in the big picture, that's an important part of what we do in these kind of situations, is the partnership with the private sector is extremely important to our ability to both deal with the cases and try to protect the internet. Next question.

Operator
Thank you. And that question will come from Nick Schifrin with PBS. Please go ahead.

Nick Schifrin
Thank you very much for doing this. I wanted to go back to the intersection of espionage and politics. Can you talk more about the MSS connection, whether you believe this is a real connection or whether it was just a bit of a brag? And when you say proxy, can you talk more about the nature of the targeting, not only against pro-democracy Hong Kong activists, but also India and Vietnamese computer networks? That seems to be two governments that the Chinese have had difficulties with, and the U.S. has been trying to ally with recently. Thanks.

Michael Sherwin
Sure. Briefly, I'll essentially say what I stated before. So, look, there's no explicit allegation that this was state sponsored. However, people that are hacking for profit do not target some of the entities that are listed in those indictments. For example, the pro-democracy groups, the other universities.

For example, in that third indictment, there was hacking of essentially thousands of students at a Taiwanese University. That is a hallmark that is a trademark of espionage. That's what espionage, that's what Intelligence Service used to harvest data, individuals that they could spot and target. Again, this is evidence circumstantial when you build it all together, when you follow all the breadcrumbs, those breadcrumbs, in general, a theory could be that that leads to the Ministry of State Security.

Jeff Rosen
I think the U.S. Attorney answered that very well and there's not a lot I have to add. I would say, that as I mentioned earlier, we are seeking the extradition of these two Malaysian subjects. Whether or not any other country gets involved in that and tries to block that in any way, will be interesting to watch.

I do want to follow up also on the private sector aspect that was asked earlier. Look, the reality is, for many decades, we've talked about our private sector partners, first with law enforcement and then in the intelligence community. But today, the private sector partnerships that we have developed throughout the country are absolutely essential. And just because we have some very talented people working in the private sector, does not mean they are not every bit as patriotic as those of us working in the U.S. government.

Operator
And the next question will come from David Spunt with Fox News. Please go ahead.

David Spunt

Sure. Thank you for taking my question, everybody. This is for FBI Deputy Director, David Bowdich. Sir, I could sense your frustration when you came up to the podium and you talked a little bit about this being like whack a mole. My question for you is, when you deal with people in China and you arrest people in China, they're not playing ball, and they're not helping you guys out to extradite these people. I mean, sure two from Malaysia are going to come back. But talk to me about the frustration to put these wanted posters out here, countless wanted posters, and not have any help from anybody in China to get these people to the United States.

David Bowdich
Sure. I can address at least part of that question. First off, it is incredibly frustrating. And I think that the Deputy Attorney General's points earlier about asking for Chinese assistance, and relying upon them, it was a very salient point for all of us to think through.

As far as our counterintelligence mission and our cyber mission, yes, much of our work is done against Chinese Communist Party individuals or Chinese Communist Party affiliated individuals. Yes, it's incredibly frustrating. And the reality is, there are those out there who do not believe indictments are effective. I would counter that strongly for many reasons.

First and foremost, we know about the travel of some individuals who participate in this type of activity. They know that if they are indicted, they are at great risk if they travel outside their country. We have proven that through the long arm of the law, and that may sound like an overused phrase, but I truly believe in it in these international cases. And so, it does restrict their travel.

It also puts them on notice. And it has been successful in many cases, not just with Chinese Nation State Adversarial Actors, but also with other Adversarial Nation State Actors, where we are able to actually reach them, bring them back to the U.S., and run them through the adjudication process. Is it frustrating? Yes, it is. Are our folks dogged and tenacious, and will they continue to be, yes, they will.

Jeff Rosen
Let me supplement that with just two quick points. This is a case where, thanks to our partnership with the Malaysian government, we have two people who perhaps thought they were beyond our reach. And they've been arrested. We still have to have them extradited. But people who think that there are safe havens, need to think pretty carefully about that. Because as I said in my initial remarks, we will pursue people. Not just here, but abroad, wherever they travel. And this is a case, or set of three cases really, in which the victims are worldwide and affected countries all over the globe.

So, there will be many people interested in finding these defendants. And we hope to find the opportunity to try them in a court of law and present the evidence beyond a reasonable doubt. One more?

Operator
Thank you. And that question will come from Kadhim Shubber, with the Financial Times. Please go ahead.

Kadhim Shubber
Hi, there. Thank you for doing this call. I had a question for Acting U.S. Attorney, Sherwin. Can you just tell us a little bit about the compromised government networks in India and Vietnam?

What was targeted or stolen or disrupted there? And also, about the attempt to compromise government networks in the UK, and what the hackers were targeting there?

Michael Sherwin
At this point, we cannot exceed the four corners of those indictment, again, into details. Obviously, as the case proceeds, more details would come out. But at this point, we just have to (INAUDIBLE) the allegations. And yes, those nations' infrastructures were targeted. And obviously, as previously mentioned, I think in a question a couple minutes ago here, those nations are not friends of China. So, it's no mystery, or it's not surprising that some of their infrastructure was targeted.

Jeff Rosen
So, I hate to end on one that that we have some limits on what we can say. So, why don't we do one more?

Operator
Thank you. And that question will come from Alex (INAUDIBLE) with (INAUDIBLE) News. Please go ahead.

Alex
My questions. Just wanted to ask, do you have a sense of the extradition timing, in terms of, the Malaysian government was obviously very cooperative in arresting them. But do you have any sense on when these two Malaysian businessmen will see the inside of the U.S. courtroom?

Jeff Rosen
I think this is a somewhat complicated subject, but we'll see if John Demers can offer any thoughts.

John Demers
Well, I don't want to get ahead of the process there in Malaysia. Obviously, they, these two defendants, will have a right to raise whatever claims they'd like to try to fight the extradition. I imagine they will try to fight the extradition. And we'll just have to let the Malaysian process play itself out. But it certainly will be months before they get over here.

But in the meantime, they've been arrested over there. Thanks.

Jeff Rosen
Well, thanks very much, everybody. And let me just mention that we do plan a backgrounders, as well. So, while I'm going to have to depart, some of the folks that can provide many more of the specific details and address some of the background things will now be available. And we'll go to that.

Operator
Thank you. Once again, if you'd like to ask a question, please press star, then one.

Marc Raimondi
Alright. Thank you, everybody, for joining. This marks the end of the formal part of the press conference. The cameras can shut down now. And then in about one minute, we're going to start with a backgrounder. We're going to have some of the prosecutors working on the case

come up and make some brief remarks. But then we will get through every media question, every on topic media question that you have.

So, if you are still in the queue, I apologize you didn't get your question asked, but you are more than welcome to ask any question you want now. Thank you.

Alright. Again, the attribution is Senior Justice Department Official. And the purpose of this is to round out the knowledge of these three different indictments. And so, I'm going to turn it over to one of my colleagues from the U.S. Attorney's Office, Washington DC.

Senior Justice Department Official
I think we'll start with the AUSA's walking through some details of the case. Just as they mentioned earlier, there are three charging documents. And so, I think it's helpful to help you all navigate some of the key accusations and allegations in those charging documents.

Senior Justice Department Official
Sure. Again, good morning. So, there are three, in separate indictments. The first indictment was returned in August of 2019. That's the indictment. That's an indictment titled United States of America versus Zhang Hao Ran and Tan Dailin. The second indictment, I'm just going to refer to them by case caption, by lead defendant.

The second indictment that we'll discuss is United States versus Wong Ong Hua and Ling Yang Ching that was returned in August 2020. And the third indictment that we've referred to is United States versus Zhang Li Zi (SP), Chen Diwan (SP), and Fu Truong (SP). And that was also returned in August 2020.

The first indictment United States versus Zhang Hao Ran and Tan Dailin, alleges that the two defendants engaged in two distinct types of criminal conduct. Generally speaking, referred to in the indictment as a computer hacking conspiracy and a video game conspiracy. The computer hacking conspiracy is consistent with what the principle discussed earlier during the live press conference, in which they were accused of conspiring to commit computer intrusions around the world, targeting high technology organizations and similar organizations.

The second type of conduct alleged in the United States versus Zhang Hao Ran and Tan Dailin indictment, alleges that they conspired to profit from hacking video game companies, including by using their hacked computer access at video game company networks to obtain and generate illegally obtained Digital Goods related to video games that they could then sell.

The second indictment vs. Wong Ong Hua and Ling Yang Ching. And I should mention at this point that all of the names, the surnames are going to be the first names listed. So, in the first indictment Zhang Hao Ran, the surname is Zhang. Tan Dailin, the surname is Tan. And that's true for all three indictments.

The second indictment Wong Ong Hua and Ling Yang Ching, that indictment, those two defendants are the Malaysian individuals that have been arrested and were previously discussed. They are accused of racketeering, racketeering conspiracy, and all essentially related to fraud and computer hacking directed at the video game companies. The indictment alleges that Wong and Ling were principals at a company called SEA Gamer Mall in Malaysia. And that SEA Gamer Mall had an online platform to sell video game related items. And so, it

was an easy place for hackers who have access to video game company networks that provides a platform that they can monetize that access because they can sell goods for profit.

The third indictment, United States versus Zhang Li Zi, Chen Diwan, and Fu Truong, those charges are about the three individuals at a company called Chung Du 404 (SP) Network Technology, which is a company based in the PRC, are registered in the PRC, and they're accused of racketeering conspiracy, conspiracy and computer hacking related offenses for the broad range of targeting.

They are not accused of conspiring with the two Malaysians. However, as alleged in the indictment against Zhang, Chen, and Fu, they did work with in the past and had collaborated with Zhang Hou Ran and Tan Dailin. The common link between the three indictments is Zhang Hou Ran and Tan Dailin, specifically who are mentioned in all three indictments. And also, the fact that all five of the Chinese actors have conducted, or participated in, computer hacking that the InfoSec community has tracked as APT41, or Barium, in other various labels.

It was outlined in the indictments and what I'll say all three together. Obviously, there are the differences that we just talked about. But first, let's talk about the breath. The breath is extensive. It includes foreign governments. It includes universities around the world. It includes targets of value, which are the video game companies, which we talked about, which is a separate part of the conspiracy.

But I think focusing on individual pieces is also helpful, to know how they were going about doing it. So, we talk about companies, we talked about providers, telecommunications providers, we're talking also about a number of companies, based in the United States and internationally, through which these companies were able to manipulate software, get into networks, and obtain access to other companies around the world.

As part of the other part of the activity, which included taking over computers for basically minting Bitcoin, and other types of cyber currencies, taking over computers for that particular value and purpose. So, this is broad, extensive, we refer to the crypto jacking as part of that. In the indictment, you hear 20,000 computers being tossed around as a number, very easily. So we're talking about thousands of computers around the world, not just video games.

Obviously, the video game conspiracy has its own set of victims, which are talked about in the indictment, some of which are the supply chain attack as well. And including the victims there, you're talking not just about the companies, but also their vendors and other people associated with those companies and people who played those games.

Senior Justice Department Official
Just a few more items to highlight and various indictments before we'll turn it over to questions. When it comes to techniques, I know there's some questions about that during the general press conference. These actors use a wide variety of techniques, including spear phishing Emails. They use stolen or forged software signing certificates to masquerade malware as legitimate software in order to evade detection.

These actors, some of the Chinese actors employed command and control dead drop domains, which is basically websites they created. And their malware would go to those websites and there would be some hidden code on those websites that would provide the malware with instructions.

They also took advantage of publicly available exploits, including a number of common vulnerabilities and exposures that are listed in those indictments. So, those for folks who aren't familiar with those, those are vulnerabilities in computer systems that have been identified by the private sector, by security researchers, that patches are available for those products and those exploits. But these actors, obviously, were able to find many victims who had not patched their systems.

With regard to the video game conspiracy, I talked a lot about that already, but these actors also use supply chain attacks to target video game companies. One of the questions during the press conference was, how widespread are these supply chain attacks? In the 2020, indictment of the three Chinese individuals at Cheng Du 404, the indictment actually walks through in some pretty good detail, at least one of those supply chain intrusions. But I want to also point out in the video game related activity, the actors also conducted supply chain intrusions against the video game industry.

A few other techniques that are noteworthy in the video game conspiracy. Obviously, they create fake accounts. The actors would hack into the videogame companies and modify or generate digital goods to assign to those accounts, which then would be sold. But the actors were also very active in monitoring the video game companies' fraud detection efforts. They were in the system, they could see what those video game companies are doing to try to prevent these activities, so they could adjust their own activities accordingly to evade detection.

We also saw them sabotaging other criminal groups that were in those networks, in order to harm their criminal competition. I think that's generally it, just time periods of the conduct. The criminal hacking conduct, the non-video game conduct started in about May 2014. And continued to August of this year, which is the date of the grand jury. And then the, yes, for the August 2020 indictment that is, and for the video game conduct that began in around June 2014 and continued to August of this year, which is the date of the grand jury, that the grand jury returned the indictment.

With that, those details out laid out there, I think we'll take some questions for any issues that folks would like to further dig into.

Operator
Thank you. Once again, if you'd like to ask a question, please press star, than one. At this time, we'll just pause momentarily to assemble our next roster. And the first question will come from Nick Schifrin with PBS. Please go ahead.

Nick Schifrin
Hey, guys, sorry to beat a dead horse on this. But just wondering if you could put any meat on the bone on questions that we've kind of circled around, which is the connection with Chinese government priorities. Whether you can describe maybe how successful the Indian and Vietnamese hacks were, the nature of the Taiwanese students, and maybe the nature of those Hong Kong pro-democracy activists, and the nature of the targeting of them? Thanks.

Senior Justice Department Official
Sure, I mean, for the most part, we do have to stick with the allegations in the indictment. The indictment was very specific in some of these areas. In particular, when you're asking about the

targeting of foreign governments, I would point you to the August 2020 indictment against the three hackers, Zhang, Chen, and Fu.

With respect to any connections between the defendants and the Chinese governments, there are connections between the companies. The company Chung Du 404, that are alleged in the indictment, the indictment alleges that Chung Du 404 itself claimed publicly that its customers included Chinese government organizations. That's listed in the indictment.

But beyond that, we would have to, or at least I would have to, defer to the comments previously made by the four principles.

Operator
And the next question will come from Evan Perez with CNN. Please go ahead.

Evan Perez
I'd wondered if you could provide any kind of estimate on the monetary losses by some of these customers. I think one of the indictments in the Asian indictment, mentions people, obviously goods and so on, being bought with some of the stolen cybercrime currency, I guess is what they were using.

And then secondly, the Deputy Director of the FBI, I think, I think Mr. Bowdich is the one who mentioned that the Chinese government was unwilling or unable to assist on this. Can you give us a little bit of a context on what that means? I mean, what efforts were made to get the Chinese government to arrest these people? Or was there any such conversation had? Or was this just based on past behavior by the Chinese government?

Senior Justice Department Official
So, I'll take I'll take first, the lost related question, or the damages related question, then turn it over. With respect to the losses, so the companies, the victims that were being targeted here were primarily organizational victims. And even when there were individual victims, it's the targeting refers to their industry, or their politics.

With respect to the organizational victims, the losses are going to be in the multiple millions of dollars. If you can look at the indictment there, there is not an overall summary of what the total losses are, which is perhaps incalculable. But with the specific example of manufacturer number two, which is discussed in the August 2020 indictment against the three individuals. Manufacturer number two in paragraph 32, suffered costs exceeding $1 million. That's just one victim, one victim that's described in the indictment.

And there are many, many, many more. And so, we would estimate that you could infer that there's going to be multiple millions and multiple 10s of millions of damages, if you were able to get the full scope. But the allegations in the indictment are pretty specific, justice to the one.

Senior Justice Department Official
Yeah. Yeah. With respect to the to the video game allegations, in March 2015, there's just a snapshot. It’s on the, let’s see, it’s gonna be--deep into the indictment, I'll find it. But on page 12 of the indictment against Wong and Ling, there's a discussion of just in a three month period, in relation to one victim and one video game, 3,000,779,440 of an unknown currency is paid to Zhang Hao Ran and his wife.

That's just a three month snapshot of the amount of money that was being made. At that point, the currency isn't specified in the indictment. But if that were, just in that three month period, if that were either in Malaysian currency or Chinese currency, it's going to be hundreds of thousands of dollars just to one of the hackers during one three month period of time.

Senior Justice Department Official
On the Chinese government question, we did not reach out to Chinese authorities for assistance in this case. Our attempts to work with China on joint law enforcement operations against cyber actors go back years. We know what lies down that road, denials and obfuscation.

We've made comments before about how we've requested assistance in other hacking cases from the Chinese government and received no meaningful response. At this stage, the department justice has alleged, through its cases, not this one, but other ones, that the Chinese government has breached this 2015 commitment to cooperate on cyber investigations, and not to sponsor economic espionage. And I think, we see no use in pursuing that route at this point in time, until we see different actions by the Chinese government.

Senior Justice Department Official
Next question, please.

Operator
Thank you. Our next question will come from Anthony Leake with Chronicle Fashion Guide. Please go ahead.

Anthony Leake
Yeah. Thank you, guys, for taking my call. My question is more about, one of you guys mentioned, it was some pro-democracy websites that were hacked into. Were any pro-republican websites hacked into, and how extensive was the video game in hacking? Because I know they pretty much talked about the Chinese earlier, but they didn't really go into more of the video game aspect, which you said was a billion dollar business.

Senior Justice Department Official
I'll take the first question. There are no allegations in this charging document about the targeting of domestic U.S. political organizations.

Senior Justice Department Official
The political targeting that was discussed is political dissidents that were particularly in Hong Kong and elsewhere in areas of interest that would naturally be of interest to the Chinese government and not domestic U.S. political issues.

Senior Justice Department Official
Could you repeat the other question, if you're still on the line?

Anthony Leake
Yes. My question was more about you guys. The first guys alluded to the video gaming hacking, and they said it was a billion dollar business. But he didn't say what video games were targeted, how they went about targeting of video games. They did mention something about the currency, but it didn't go into more about what video games, what interests two of the Chinese hackers, and how they actually went about doing it.

Senior Justice Department Official
As it relates to the video game victims, obviously in the indictment, they've been anonymized. And part of the effort of prosecuting cases like this is to get victims to cooperate with us. It is a billion dollar industry. There are a number of videogame companies who were targeted. It's not just one alone. And obviously, that has an economic fact impact on their businesses, but we can't go beyond what is in the indictment, in terms of identifying and naming them individually or the games in which were compromised.

Anthony Leake
Alright, so will you be releasing a copy of the indictment? Because when I got the email, it didn't have a copy of the indictment.

Senior Justice Department Official
It does. If you look at the top of the press release, which if you don't have it, you can get it at justice.gov, there will be links to the three indictments and other materials. Next question, please.

Operator
And the next question will come from Caitlin Yilek with Zenger News. Please go ahead.

Caitlin Yilek
Hi, was the targeting of video game companies solely for financial purposes?

Senior Justice Department Official
So, with respect to the allegations in the indictment, the allegations in the indictment focus on the monetary aspect, of the indictments, focus on the monetary aspect of targeting video games. However, just as a general matter, and not specific to the indictments in this case, as a general matter, if a hacker successfully compromises a company's networks, including companies such as video game companies, which do have valuable technology, valuable intellectual property, and referenced earlier, were code signing certificates, things that helped software, including malicious software, if it's used improperly, to look innocent. And so, there could be multiple reasons why hackers would target video game companies. The indictments, here are focused on the use of the money aspect.

Operator
And the next question will come from Mark Hosenball with Reuters. Please go ahead.

Mark Hosenball
Hello, thank you. A couple questions. First of all, going back to the video games issue, we are hearing that maybe a company called Electronic Arts, one of the company's targeted in this hacking, and we're wondering if that's correct? But also whether they're popular FIFA soccer sports game series was one of the video games that they were hacking into?

Separately, we'd like to also know whether your view is that the Tik Tok deal with Oracle, where byte dance still has the majority of Tik Tok, would that be acceptable to the Justice Department? It's a little bit off track but not entirely.

Senior Justice Department Official
With respect to identification of victims, we're not going to identify any victims, we're not going to confirm or deny any speculation about who the victims might be, or what video games might

have been affected. It is important that we use the justice system to vindicate the rights of victims. But in that process, to the extent possible, we respect the privacy of victims, and that's why the allegations that are legally necessary are in the indictments, but we're not going to identify any victims.

Senior Justice Department Official
We're going to focus this background on the allegations in the charging document, not address any other inquiries to the Department of Justice Office of Public Affairs.

Senior Justice Department Official
Thank you. Next question.

Operator
And that question will come from Shannon Vavra with CyberScoop. Please go ahead.

Shannon Vavra
Hi, there. Thanks again for doing this phone call. I just wanted to double check and see if you could clarify. FireEye has recently announced another sweeping campaign related to APT41 in March. Could you go into detail about DOJ's coordination efforts with FireEye on these indictments? And could you clarify if they're separate? The timing appears separate, but I just want to hear your take on that. Thank you.

Senior Justice Department Official
So, in this matter, we have certainly engaged all over with the private sector, whichever people are either interested or affected as victims, or are also folks who might have expertise in the areas. We're not going to address FireEye, or any other company that we didn't already publicly announce.

I will say that the engagement of Microsoft, Facebook, Google, Verizon, it reflects the nature of the threat, the significance of these charged defendants, as well as the APT41 threat group, generally, and we thank them for their participation. But with respect to FireEye, we don't have any comment.

Shannon Vavra
Thank you.

Operator
And the question will come from Michael Costner with NBC News. Please go ahead.

Michael Costner
Yes, thank you. I was just trying to understand a little bit about how that digital currency was sold. When they obtained the currency and then you said to third party, so how is it sold? How did they do that?

Senior Justice Department Official
It is a complicated fact pattern. I think the best way to answer it succinctly is to say, SEA Gamer Mall, the company that is named in the indictment against Wong and Ling, sells those types of items in in a variety of ways. And the gist of the business model, or at least the relevant part of their business model, is to sell digital goods, such as either game currency itself, or game

playing accounts that have the currency already stored inside them, one way or the other, they would be trying to sell that through their own online platform.

The online platform there works, sort of, like a typical ecommerce site. You can go to the website and make purchases. How they affect the purchases, or what particularly is sold is going to vary according to the different video games. And I imagine the marketplace, what they're willing to pay.

There was a question about how they generated, as well. So, again, similar answer, it's a complicated fact pattern that depends on the victim in the video game. But basically, the allegations here are that obtaining one way or the other, illegally obtaining digital goods, whether it's coins, or accounts with the coins, or axes, or I don't even know whatever the digital goods are. It's not really specified in the indictments here, but it's just digital goods that can help enhance the game playing experience.

Those can be generated in a number of ways. For example, if the hacker has access to a corporate database of accounts and can change the values in the accounts, would be, I think, the simplest of the examples. But other examples would depend on the type of video game, the type of thing that is interesting to the market. And it's important too, as was mentioned earlier, that the hackers would use their access to monitor the fraud detection groups of the video game companies so that they could avoid detection. And also, that they could use their access, essentially, to cut out the criminal competition by taking action inside the network against competitors.

Operator
And the next question will come from Andres Triay with CBS news. Please go ahead.

Andres Triay
Hey, guys, thanks for doing this. Did you seize any assets, cryptocurrency, or bank accounts or anything, and how much was that?

Senior Justice Department Official
We can’t comment about any other monetary seizures at this time. I can say, as part of the overall effort, we have engaged in a number of seizures around the world, with assistance of private partners and also foreign governments to assist in getting us to where we need to be. Which is to deter this threat, and to defeat it wherever possible, which means seizing C2 domain names, it includes seizing accounts controlled by the hackers and individuals associated with them, so they can't continue to be a threat from those same accounts.

Andres Triay
And by seizing, you mean you froze them, or you actually took control of them?

Senior Justice Department Official
With respect to the accounts, it would depend on the nature of the account, but in some cases, it would just be shutting down an account and cutting off access to infrastructure, such as a server that the hackers are actively using for current hacking operations. And so, in the United States that would be either a takedown by a provider, which has observed a violation of its terms of service or affected that through seizure warrants and legal process.

Andres Triay

Thank you.

Unknown Speaker
Last question.

Operator
And that question will come from Shannon Vavra with CyberScoop. Please go ahead.

Shannon Vavra
Hi, there. Thanks again for taking our questions. I just wanted to ask one more, which is, were these announcements of these indictments today coordinated with the Department of Homeland Security and FBI as announcements earlier this week on MSS hackers using commonly known vulnerabilities? The announcement today mentions that these attackers have also used commonly known vulnerabilities that are (INAUDIBLE) Thank you.

Senior Justice Department Official
I'm not going to speak specifically to coordination with the announcement you're referring to. But I think, generally, you can expect when we have these types of cases, that there is a wide ranging coordination across the government, the United States government, with our interagency partners, to handle these threats. And so, that release was broad. It referred to MSS, I think, at large, which I think is a broader threat than specifically the one described in this group, in these cases. Thank you.

Shannon Vavra
Thank you.

Unknown Speaker
Thank you. Thank you everyone for calling in. This now concludes the backgrounder. You may now disconnect.

United States Department of Justice
Tuesday, September 16, 2020, 11:00 AM