Department of Justice

UNITED STATES DEPARTMENT OF JUSTICE PRESS CONFERENCE

Wednesday, February 17, 2021, 11:30 AM Eastern

PARTICIPANTS

Marc Raimondi – Spokesman
John Demers - Assistant Attorney General for National Security
Tracy Wilkison - Acting United States Attorney for the Central District of California in Los Angeles
Kristi Johnson - Assistant Director in Charge of the FBI's Los Angeles Field Office
Jesse Baker - Special Agent in Charge of the Los Angeles Field Office for the U.S. Secret Service under Homeland Security

PRESENTATION

Operator
Good day and welcome to the Department of Justice press conference. All participants will be in listen-only mode. Should you need assistance, please signal a conference specialist by pressing the star key followed by zero.

After today's presentation, there will be an opportunity to ask questions. To ask a question, you may press star then one on your touchtone phone. To withdraw your question, please press star then two. Please note, this event is being recorded. I'd now like to turn the conference over to Marc Raimondi. Please go ahead.

Marc Raimondi
Thank you, Grant. This is Marc Raimondi with DOJ Public Affairs. Thank you all for joining. We're still queuing up people who are calling in, so we started a couple minutes late. Today is on the record. Recording is fine for broadcast or whatever purpose you desire. And live tweeting and so forth is allowed. Everything that we say today is on the record. Those of you who RSVP'd should have already got some products from me, including the press release, some remarks, the wanted posters, and the indictment. If you did not get that, it should be live on our website at justice.gov by now. If it's not, just--if you have the page up, refresh and it should pop up any minute.

We're going to start out with four speakers today. The order of speaking will be John Demers, Assistant Attorney General for National Security, followed by Tracy Wilkison who's the Acting United States Attorney for the Central District of California in Los Angeles, Kristi Johnson, who's

the Assistant Director in Charge of the FBI's Los Angeles Field Office, and then, closed out by Jesse Baker who's the Special Agent in Charge of the Los Angeles Field Office for the U.S. Secret Service under Homeland Security. Following the formal remarks, we'll have a Q&A period where I encourage you to queue up now at star then one.

We'll go through a few questions. And after the last question, you can either drop off or you can stay on. We'll be having a deep dive into the indictment for those interested with two background briefers, who will be referenced as senior justice officials. And that will happen immediately following the last question of the official on the record period. Thanks a lot. And again, please queue up early. And I'll turn it over to John Demers.

John Demers
All right. Great. Thank you very much, Marc. Good morning, everyone. Nice to be back together. Today we're announcing charges following a significant national security cyber investigation first disclosed publicly more than two years ago. As laid out in today's indictment. North Korea's operatives, using keyboards rather than guns, stealing digital wallets of cryptocurrency instead of sacks of cash, have become the world's leading bank robbers. The department will continue to confront malicious nation-state cyber activity with our unique tools and work with our fellow agencies and the family of norms abiding nations to do the same.

We were all back together in September 2018 when the U.S. Attorney's Office for the Central District of California, the same office that's here with us today, with the assistance of the National Security Division, charged the North Korean programmer who was working for the government of the Democratic People's Republic of Korea with conspiring to conduct some of the most damaging cyber-attacks ever, including the November 2014 destructive attack and hack-and-dump targeting Sony Pictures Entertainment over a comedy film they didn't like, February 2016 cyber enabled heist of $81 million in the bank of Bangladesh and other heists, and the May 2017 Global WannaCry 2.0 attack. The events as described in that indictment provided the first indication that the North Korean regime would become focused on, and adept at, stealing money from institutions around the world.

Today the Department unseals an indictment returned by a grand jury in the central district, charging the same DPRK programmer, as well as two newly identified DPRK conspirators, with a campaign of cyber heists and extortion schemes targeting both traditional and cryptocurrencies. The indictment adds to the list of victims since 2018, including continued cyber-enabled heist from banks on four continents, targeting over $1.2 billion.

It also describes in stark detail how the DPRK cyber threat has followed the money and turned its revenue generation sights on the most cutting-edge aspects of international finance, including through the theft of cryptocurrency from exchanges and other financial institutions, in some cases, through the creation and deployment of cryptocurrency applications with hidden backdoors. The indictment refines the attribution of this crime spree to the DPRK military intelligence services, specifically the Reconnaissance General Bureau, or RGB. Simply put, the regime has become a criminal syndicate with a flag, which harnesses it's state resources to steal hundreds of millions of dollars.

In a moment, you will hear more details about the charges and evidence in the case from the acting U.S. Attorney for the Central District, from the Bureau, and from the United States Secret Service. But I want to take a moment to highlight the significance of these charges for the department, the United States, and the international community. As a description of victim entities in the indictment shows, the DPRK's malicious activities are a global problem, requiring global awareness, condemnation, and cooperative disruption. With this indictment and related disruptions, the United States continues to do its part.

First, we continue to shine a light on the global campaign of criminality being waged by the DPRK. Nation-state indictments like this are an important step in identifying the problem, calling it out in a legally rigorous format, and building international consensus. Second, in addition to educating the U.S. public and international community about this activity, we're also targeting the networks through which the DPRK is cashing out its ill-gotten gains. As will be described in more detail by my colleagues, the Department has obtained custody over a dual U.S.-Canadian National who organized the laundering of millions of dollars stolen by the DPRK hackers. He has agreed to admit his role in these criminal schemes in a plea agreement, and he will be held accountable for his conduct.

This prosecution demonstrates the commitment of the Department to ensuring that those who conspired with the DPRK hackers will face justice. The Department was also able to seize and expects to ultimately return almost $2 million stolen by the DPRK from a New York-based financial services company. This follows on similar seizure actions announced in March and August 2020, in which the U.S. Attorney's Office for the District of Columbia seized and froze approximately $8.5 million dollars of cryptocurrency. These cryptocurrency seizures and prosecution of a high-level money launderer collectively represent important steps in disrupting the DPRK hackers and their money laundering networks and illustrate the department's commitment to repatriating stolen funds before they reach the DPRK.

Third, the United States is empowering network defenders. As you will hear, the prosecutors and investigators have, throughout this investigation, worked closely with victims and intended victims of the DPRK hackers and have provided these victims with information about avoiding and remediating infections. This work continues today. Accompanying this announcement, the FBI and the Department of Homeland Security, Cybersecurity and Infrastructure Security Agency, with the assistance of the Department of the Treasury, are releasing a Joint Cybersecurity Advisory and Malware Analysis Report regarding the DPRK as a malicious cryptocurrency application. The criminal investigation leading to today's indictment obtained that information for distribution to our network defenders. Further, the context provided in today's indictment underscores the necessity of paying attention to this advisory and its recommendations.

Fourth, the allegations in today's indictments inform and empower the international community so that they can not only join us in condemning this activity but also helped to stop it. In that regard, the European Union's July 2020 sanctions related to the to the Lazarus Group were a welcome development. We commend the EU for its initial efforts to impose consequences for state sponsored malicious cyber activities. Now it's time for other nations that wish to be regarded as responsible actors to step up.

The conspirators described in today's indictment are alleged to have been working, at times, from locations in China and Russia. The DPRK has also utilized Chinese over the counter cryptocurrency traders and other criminal networks to launder the funds. Just as the United States has disrupted the DPRK's crime spree through arrests, forfeitures, and seizures, the time is beyond ripe for Russia and China, as well as any other country whose entities or nationals play a role in the DPRK revenue generation efforts, to take action.

The Department's criminal charges are uniquely credible forms of attribution. We can prove these allegations in open court beyond a reasonable doubt using only unclassified, admissible evidence. And they are the only way in which the Department speaks. If the choice here is between remaining silent while we at the Department watch nations engage in malicious norms violating cyber activity or charge these cases, the choice is obvious. We will charge them. Before I turn this over, I would like to thank the agents at the FBI in Los Angeles, Charlotte, and Raleigh, the Secret Service in Savannah, Los Angeles, and DC, and the prosecutors in Los Angeles, and here in NSD for stepping up to the plate to play their part. Tracy?

Tracy Wilkison
Thank you. Good morning. My name is Tracy Wilkison. And I'm the Acting United States Attorney here in Los Angeles. Thank you all for joining us today. Nearly two and a half years ago, we charged a North Korean computer programmer in a criminal complaint with being a member of a conspiracy that conducted sophisticated cyber attacks around the world on behalf of the North Korean government. The indictment unsealed today by my office represents a significant development in this case, adding two more North Korean defendants and alleging a series of criminal schemes beginning in 2014 and continuing through last year.

The indictment alleges that the three defendants were part of the North Korean regime, specifically, that they work for the Reconnaissance General Bureau, a military intelligence agency. The hackers charged in the indictment were members of units known in the cybersecurity community as Lazarus Group and Advanced Persistent Threat 38. While the cyber security community recognizes these two as different North Korean groups, the criminal investigation has revealed that these groups were part of a single conspiracy that worked under the North Korean military to destroy computer systems and to steal money and information, offer revenge, and to finance the criminal regime.

The indictment we're announcing today builds on the charges in the 2018 complaint, which described how members of the conspiracy were responsible for several highly destructive and well-known computer intrusions, including the cyber attack on Sony Pictures Entertainment right here in our community. The indictment includes these intrusions and cyber attacks but greatly expands the scope of the allegations to include entirely new types of schemes in which the hackers attempted to steal hundreds of millions of dollars. And some of these intrusions occurred as recently as a few months ago, using newly identified strains of malware uncovered by the FBI as part of this investigation.

Count one of the indictment alleges several new hacking schemes. First, building off the allegations in the complaint, the indictment alleges a series of cyber heist targeting banks around the world. The hackers typically gained access to a bank's computer network and sent secure

messages through the SWIFT system that is used to transfer money between banks. The indictment alleges that these attacks sought to steal more than $1.2 billion from financial institutions around the world, most recently from a bank in Malta in February of 2019.

Second, the indictment alleges ATM cash out schemes in which the hackers used malware to take control of bank ATMs, allowing for limitless cash withdrawals. This scheme, referred to by the U.S. Government and Cybersecurity Advisement as FASTCash, allowed co-conspirators to withdraw $6.1 million from one bank alone.

Third, the indictment states that the North Korean hackers engaged in cyber extortion in which they would gain access to computer systems and then steal data or deploy ransomware that would demand payment.

Fourth, the indictment contains significant allegations about the development and spread of a series of malicious applications, purportedly for trading and storing cryptocurrency, but which were actually designed to give the North Koreans a backdoor into computer systems. The indictment specifically identifies many of these malicious cryptocurrency applications, some of which were still being developed only a few months ago. Such an application was allegedly used in a cryptocurrency heist in August of 2020 to steal from a company in New York.

In total, the indictment alleges three cryptocurrency thefts totaling $112 million.

Count two in the indictment discusses another scheme related to cryptocurrency. In 2017 and ‘18, the North Koreans developed a digital token called Marine Chain, which would trick investors into purchasing ownership interest in marine shipping vessels, such as cargo ships, not knowing that they would be providing cash to an outlaw regime. The Marine Chain token, supported by a blockchain, not only would have given the North Koreans controlling interest in shipping vessels, it would allow them to obtain funds from abroad and skirt U.S. sanctions that were placed on the regime.

The scope of these crimes by the North Korean hackers is staggering. They are the crimes of a nation-state that has stopped at nothing to extract revenge and obtain money to prop up its regime. We chose to unseal the indictment today for several reasons, one of which was the related announcement of a criminal case against the money launder Ghaleb Alaumary who is being prosecuted by my office and is in custody in the Southern District of Georgia. This high-level and trusted money launderer for the North Korean hackers has agreed to plead guilty to conspiring to launder funds from both cyber heists and ATM cash outs. According to a plea agreement that was unsealed today, Alaumary conspired to steal and then launder tens of millions of dollars for the North Koreans and other criminals.

I also want to make very clear to the victims of these crimes that we stand with them. For years, agents and prosecutors here in Los Angeles have collaborated with private cybersecurity companies to analyze the methods of attacks and to arm potential victims with information that will help them to avoid future attacks. This morning, we are building upon that work through the issuance by the FBI and the Department of Homeland Security of a Joint Cybersecurity Advisory

and Malware Analysis Report on a family of cryptocurrency malware produced by the North Koreans.

This analysis is designed to provide the cybersecurity community, and the public, with information about identifying this malware, avoiding intrusions, and remedying infections. In addition, we are continuing to do everything we can to make the victims whole. Last week, we obtained warrants to seize cryptocurrency worth nearly $2 million that was stolen by the North Korean hackers from a financial services firm in New York. Those funds will go back to the victim.

This in-depth investigation involves a number of law enforcement entities, cooperation across agencies and countries, and tireless efforts by all involved. I want to compliment and thank the outstanding agents with the FBI and the Secret Service. I also want to acknowledge two prosecutors in my office who have worked for years on this investigation. Assistant United States Attorney's Anil Antony and Kal Shobaki of our Cyber and Intellectual Property Crimes Section. Thank you very much.

Marc Raimondi
Go ahead, Kristi.

Kristi Johnson
Okay. Very good. Good morning. My name is Kristi Johnson. I'm the Assistant Director in Charge of the FBI's Los Angeles Field Office. The threat posed to the people of the United States, United States interests abroad, and worldwide targets by cyber criminals operating at the behest of North Korea is alarming. But we are facing this threat head on with a variety of resources. A cadre of dedicated prosecutors and investigators including special agents, analysts, computer scientists have continued to build this case since 2014. This talented team has worked tirelessly on this investigation. This case makes clear the extent North Korean adversaries will go to harm our citizens, our businesses, and our foreign allies to generate money for the regime and attempt to weaken our society, our industries, and our economy.

As my colleagues have pointed out, this wide range of intrusions and attacks are attributed to programmers working for the DPRK. Please know that when we assign attribution to a particular cyber aggressor, we do so with high confidence while relying on very solid evidence. The indictment outlines a broad range of cyber crimes attributed to these defendants, all three of which are North Korean citizens who were members of the Reconnaissance General Bureau, a military intelligence agency of the DPRK, which conducts criminal computer intrusions.

Arrest warrants have been issued in the federal court in Los Angeles for three defendants: Jon Chang Hyok, Kim Il, and Park Jin Hyok. They are considered fugitives from justice. The wanted posters can be found at fbi.gov. They are believed to be located in North Korea. However, anyone within the United States with information about their specific whereabouts should contact their local FBI office. Anyone outside the United States should contact their nearest United States Embassy. If you believe you have been a victim of these or similar acts, or you are witness to these or similar activities, please contact the FBI.

I'd like to highlight the cooperation the FBI received from various victims of these attacks as well as from cybersecurity companies and our foreign partners, all of which we could not do this type of investigation without. Victim information gleaned from each attack, including tactics, techniques, and procedures used by the perpetrators is used and shared with other potential targets and victims in order to mitigate damage and prevent future intrusions. As has been mentioned by my colleagues, the FBI and DHS, in coordination with Treasury, have issued a Joint Cybersecurity Advisory and Malware Analysis Report, which have been made available to you. Regarding North Korean cryptocurrency malware, this important advisory expands on the North Korean cyber threat referred by the U.S. government as HIDDEN COBRA. The Advisory and Malware Analysis Report identifies specific malware and indicators of compromise related to the AppleJeus family of malware.

AppleJeus refers to a host of related malicious cyber cryptocurrency applications which are further described in the advisory. The Joint Cybersecurity Advisory and Malware Analysis Report provides the cyber security community and the public with information about North Korean malicious cryptocurrency applications in order to prevent compromise and intrusion as well as to remedy infections that have already occurred. As was mentioned by my colleague from the United States Attorney's Office here in California in the Central District, following a 2020 North Korean intrusion and theft from the United States based financial services company, the FBI located and froze approximately $1.8 million United States dollars' worth of cryptocurrency.

Last week, the FBI obtained warrants for the seizure of those stolen cryptocurrencies and is working with the United States Attorney's Office to return the funds to the victim. We cannot investigate these cases in a vacuum. We routinely collaborate with private sector and government partners both domestically and globally. We rely on one another to prevent future intrusions, to address large scale state sponsored attacks, and to impose risk and consequence upon our cyber adversaries. While we have worked with scores of victims and partners on this case, I'd like to specifically thank the following around the globe: various FBI legal attaché offices located in US embassies around the world, our foreign law enforcement partners, and the United States Secret Service. In addition to their assistance in the cyber investigation, the arrests of the money laundering co-conspirators is due to their efforts, and I thank them today.

The FBI extends a great deal of resources training businesses and the public on how to defend their computer systems and networks, the goal of which is to protect from reputational harm and avoid potential financial loss that inevitably results from any large-scale attack. Prevention is the key to protecting your systems. The defendants in this case conducted a range of cyber attacks from simple phishing schemes to highly sophisticated malware creation and everything in between at the behest of the North Korean government.

This case is a perfect example of the destruction that can be caused by a cyber attack and the grave threat these attacks pose to our national security. The FBI will continue to work with our private and public partners to combat these attacks and prevent future ones. Thank you very much. I'd like to turn it over to Special Agent in Charge, Jesse Baker, of the United States Secret Service in Los Angeles.

Jesse Baker

Thank you, Agent Johnson. I appreciate that. Good afternoon. My name is Jesse Baker. That's J-E-S-S-E Baker. And I'm the Special Agent in Charge of the Los Angeles Field Office. It's my honor to represent the Secret Service here today. I know we've already heard from a lot of speakers here about their conspiracy. And I want to draw attention to some of the documents that you have about this specific case with Ghaleb Alaumary and his role as a prolific money launderer as part of this North Korean conspiracy.

Our involvement, when we looked at not only the arrest but ultimately the guilty plea, is looking at this and what was our role. Well, we did what we did since 1865. We follow the money. We did this through the use of technology and really old school detective work. While you've heard about how the suspects use a multitude of complex schemes to steal money, they still have to find a way to move the money. In this case, the money was laundered a variety of ways. We saw that people were directed to move funds between bank accounts, through wire transfers, withdrawing cash from accounts, and ultimately, converting the funds to cryptocurrency where they would then be put into private wallets.

This laundering was sophisticated. It was really extensive. But these methods left an information trail. We really had to collect the dots in order to connect the dots. When I look at this, I really think that this case is like a thousand-piece puzzle, but it's spread out all over the map. In the beginning, the pieces are hard to connect. But you put a few together and, eventually, a clear picture emerges. And that's what we saw here with this case.

And my second point I'd like to cover is that we continue to see a confluence of state and non-state actors in cybercrime. We have a growing alliance between global transnational criminal organizations and those responsible for carrying out state sponsored cybercrime. It's happening with increasing regularity. Oftentimes, it's no longer either criminal groups or nation states. These distinctions have really blurred.

Now, my third and final point is that the extreme complexity of this case required a really robust and inclusive investigative method. When the Secret Service protects the president, we don't just use one specific division. We leverage the skillsets of multiple different groups, both internal and external. And we really modeled this case using those same methods, that same methodology, drawing on the expertise of a, really, a variety of people throughout the agency. It took a lot to get here. And I want to acknowledge that we looked at that through the efforts of the Secret Service Office in Savannah, Georgia, our Global Investigations Operation Center, which we refer to as the GIOC, here in the Los Angeles Field Office, as well as efforts through Miami, New York, and Ottawa.

And I also want to echo what you've heard on the call. You hear this a lot, but it cannot be more true that the importance and strength of our federal partnerships and state local partnerships is critical and key to the successful prosecutions like what you've seen today. In closing, we are very proud of this case. And we are not slowing down. We are full speed ahead. The men and women of the Secret Service will continue our 156-year history of focusing on complex financial crimes for the benefit of the American public. Thanks for allowing me to speak to you today.

Marc Raimondi

All right. Thank you very much, Jesse. Thank you to all our speakers. Again, please queue up pushing star one. And as soon as we get some folks queued up, we'll start the Q&A. When you ask a question, please direct it to either Assistant Attorney General John Demers or Acting U.S. Attorney Tracy Wilkison or Kristi with the FBI or Jesse with the Secret Service, Kristi Johnson or Jesse Baker. If you forget their names, you can just say Secret Service, FBI, or DOJ and we'll figure it out. Thank you. Operator, please open the line for questions now.

QUESTION AND ANSWER

Operator
We will now begin the question-and-answer session. Again, to ask a question, you may press star then one on your touchtone phone. If you're using a speakerphone, please pick up your handset before pressing the keys. To withdraw your question, please press star then two. At this time, we will pause momentarily to assemble our roster. Our first question comes from Del Wilber with the LA Times. Please go ahead.

Del Wilber
Hey. Thanks. This is for John. It's a two-part question. Could you put this scheme, this hacking-- these hacking attacks, in North Korea's overall strategy into the broader context of the cyber threats we're facing? Like China and Russia, they do it differently. It seems that North Korea's after money more than the espionage spurned by China and Russia. And the second question is, it kind of goes to the China/Russia thing, what were these hackers doing in Russia and China, if you can say, and provide a little color about that. Thank you.

John Demers
Thanks, Del. On your first question, I mean, look, I think you've got it. What we see almost uniquely out of North Korea is trying to raise funds through illegal cyber activity. That includes, as reflected in this indictment, the theft of cryptocurrency, the theft of traditional currencies, extortion, cyber extortion schemes, and these marine chain tokens that they had also fraudulently developed.

Their need as a country is for currency because of their economic system and because of the sanctions that are placed on them. And they used their cyber capabilities to get currency wherever they can do that. And that's not something that we really see from actors in China and Russia or in Iran who are after different aspects, whether it's intellectual property or export controlled technology or disrupting our elections. Whatever it is, those countries have different kinds of activity than do the North Koreans. The North Koreans are very focused on this, on their need for currency.

On your second question, I mean, I really can't go into much detail about what they were doing in these countries. But it does highlight the problem that I think some of our other cases have highlighted as well, of Russia and China not only engaging in their own malign cyber activities, but also providing a safe harbor, or a place, for whether it's cyber criminals, or in this case, other nation-state actors to act. And I think, as you know, due to the authoritarian, totalitarian nature of those countries, there's very little of significance that goes on there without those governments knowing about it.

Operator
Our next question will come from--it will come from Ellen Nakashima with the Washington Post. Please go ahead.

Ellen Nakashima
Hi. Thanks. This question is for anyone who feels qualified to answer. Just a couple--actually a couple of questions. How much did the hackers, or defendants, actually, are they accused of actually stealing versus attempting to steal? And secondly, are cryptocurrency exchanges regulated? Are they supposed to follow the Know Your Customer rules the same way banks are? And, if not, are they part of the problem?

Unknown
Tracy, if you want to take the question on the amount.

Tracy Wilkison
Absolutely.

Unknown
Identify yourself.

Tracy Wilkison
This is Tracy Wilkison. I can't really comment on the exact amount of money that the hackers made. But, as set forth in the indictment, the hackers successfully stole $81 million from Bangladesh Bank and conducted other cyber enabled bank heist and ATM cash outs and obtained millions of dollars through extortion and theft of cryptocurrency. And I know that they attempted to steal more than $1.3 billion. Knowing the exact amount that they've received, I can't really comment. I just have that information.

Marc Raimondi
Jesse, do you have anything you want to add to that? (Inaudible) on the regulation piece?

Jesse Baker
When it comes to cryptocurrency, there's certainly a lot of information out there. Can you phrase, Ellen, again, the way you pronounce that sort of and about whether they follow the rules?

Ellen Nakashima
Banks are supposed to ask questions about their customers and who they are and where they come from and basically follow rules of, they call it Know Your Customer rules. And that's an attempt to make sure that they're not doing suspicious transactions. Are cryptocurrency exchanges regulated in the same way, and if not, should they be? Otherwise, how are you going to detect this activity earlier and then recover the money for the victims?

Jesse Baker
Thanks, Ellen. I'll refer any policy decisions about regulations of cryptocurrency and traders to policymakers if you will. I'll speak to a little bit, though, about the techniques because you inferred

there about, how are you going to still catch them. And I think that's what is really great, for example, about the Alaumary case, where he pled guilty today, is that at some point that cryptocurrency is still only codes. It's not worth anything to them until it can be converted to cash. At some point that has to happen. And when that happens, it's going to leave some sort of trail. And we always use legal processes in order to change, to follow the money, like I said in the beginning. It's worthless to them until it's converted to money. At some point, they're going to do that. And there's ways that we can examine that through lawful processes when that happens.

Marc Raimondi
Okay. Thank you. Next question—

Operator
--(Inaudible) comes from Aruna Viswanatha with Wall Street Journal. Please go ahead.

Aruna Viswanatha
Hi. Thanks. Just to follow up on Ellen's question and clarify, so the $1.2 billion figure, that was money that was attempted to be stolen, but you don't have a figure of what was actually stolen? And I think I had heard earlier that a lot of that was taken from, or tried to be taken from, victim banks around the world using fake SWIFT codes. That seems pretty reminiscent of what happened in the Bangladesh Bank heist. Was there some--were they using the same tools that they had used there? Or these were newer methods that tried to get around the improvements that banks had put in place after that heist? And then, also, just to go back, also, to the initial coin offering. That seems like a newer tactic. How is this, with the price of bitcoin so high, is this something you see them trying to do more and more of? How big a deal is this going to be going forward?

Tracy Wilkison
This is Tracy Wilkison. Just on the issue of the amounts of money, I will confirm, yes, that the $1.2 billion is the attempted to steal. The $81 million from Bangladesh Bank is the--actually stolen. And there's specific amounts for individual overt acts as listed in the indictment. And that's available to you. Then, I'll turn the remainder over either to Kristi or to the backgrounder.

Kristi Johnson
Thank you, Tracy. We'll go ahead and push that to the backgrounder for more details.

Operator
Our next question will come from Eric Tucker with the Associated Press. Please go ahead.

Eric Tucker
Yes. Hi. Thank you so much for doing this. I just wanted to clarify about the nature of the conspiracy and the attribution for each of the bullet pointed hacks. Is the allegation that these three gentlemen each played a role in each of those individual hacks and intrusions that are delineated in the indictment, or is that not necessarily the case? I just want to be clear as to--because I appreciate that it's a conspiracy, so wasn't sure you have to establish that.

Tracy Wilkison

This is Tracy Wilkison. Yeah. These individuals are charged in the overall conspiracy. Where there is specific attribution for specific acts, they are named in the overt acts in the in the indictment.

Operator
Our next question will come from Eamon Javers with CNBC. Please go ahead.
Eamon Javers
Hi, everyone. Thanks again for doing the call. Two questions for you if I could. The first one is, I guess, for FBI on the diplomacy aspect of all this. Have you guys seen the North Korean criminal enterprise you're outlining here respond in any way to U.S. diplomatic overtures? That is, the former president of United States was meeting with the leader of North Korea extensively, or a couple of times, in '18 and '19. Did you see any pause during that diplomatic overture, or did this continue unabated through that period of time?

And then, second question is, I know you can't quantify total losses here. Can you quantify just cryptocurrency losses here? And can you narrow that even down to American cryptocurrency investor losses in terms of dollars? Two questions, one on the diplomatic overture and one on the U.S. cryptocurrency losses. Thanks.

Kristi Johnson
Thank you for that question. Kristi Johnson with the FBI. On the first piece, I am going to, for the broader perspective, I will push that back to Mr. Demers back in Washington, DC.

John Demers
Thanks. Hey, Eamon. It's John Demers. I mean, on your first question, I don't think we've mapped the activity of this conspiracy against the timeline of the diplomatic engagements with North Korea. I don't know that we could answer whether there were lulls in this activity during certain times of that engagement, and then, whether it picked up after that. I mean, the North Koreans, overall, have been fairly persistent in their engagement of these types of cyber crimes. But beyond that, I don't--we didn't do a tick tock, month by month or something like that.

Tracy Wilkison
Hi, this is Tracy Wilkison. On the specific question as to the amount of money stolen for--by way of the cryptocurrency heist, that number is alleged in the indictment at $112 million.

Operator
Our next question will come from Claire Hines—

Kristi Johnson
--(Inaudible)

Operator
Go ahead.

Kristi Johnson

Sir, can I just follow up on that? Thank you, Tracy. This is Kristi Johnson with the FBI. We just don't have a breakdown within the U.S. of the losses related to cryptocurrency. But just to shore that up. Thank you.

Operator
Our next question will come from Claire Hines with CBS News. Please go ahead.

Claire Hines
Hi. Thanks so much for doing this. I was just wondering if you could speak at all to the threat assessment or continued threat level that these groups like Lazarus and others still pose to the United States?

Kristi Johnson
This is Kristi Johnson with the FBI. This group, Lazarus Group, does continue to pose a threat across all industries. Thank you.

Operator
Our next question will come from Jerry Dunleavy with the Washington Examiner. Please go.

Jerry Dunleavy
Thanks, guys. I think this is probably for Mr. Demers. My guess is that these hackers, with them being in North Korea, aren't expected to come into U.S. custody. Would DOJ be able to just lay out the benefit (inaudible) in attribution like this and in filing indictments like this even--especially when the people that have been indicted probably aren't going to stand trial?

John Demers
Thanks. Sure. I mean, I expect they won't be traveling here anytime soon, although I wish they would so we could prove all these charges in court. In terms of what the benefits of these indictments are, it's something I've tried to address in the opening remarks. I mean, we do them for a number of reasons. One is educational, to draw attention of the public, and of policymakers to the kind of activity that we're seeing from these different malicious nation-state actors, including, here, North Korea. I think over the course of our indictments, over the course of years, I think the public and policymakers both in the executive branch and in Congress have a much better understanding of the way that these different actors do their work.

The second is to show to these actors that they are not as anonymous as they think they are. As you see in this indictment, you can see photos of the hackers at issue. We've done that in other cases, too. You think you're anonymous behind a keyboard, but you're not. And we lay out how we can prove that attribution, again, not to a nation-state level, not even to a unit level within a military or an intelligence organization, but to the individual hacker. The third is that our charges often enable other agencies to use their tools, whether they're sanctions or otherwise, to bring costs on the hackers and the countries that harbor them or use them.

The fourth is our work with the international community. And we, as this case shows, we do a lot of work on the law enforcement side and on the intelligence side with the international community in order to bring these cases forward. But also working with them to help them impose costs

separately and to call out this activity separately. And you see that in the EU's actions and their sanctions against the Lazarus Groups and against others over the summer.

Those are the first set of EU sanctions for nation-state cyber activity. Significant development, which can be attributed in part to, I think, a lot of the work that we've done together on these cases. And all with a view of creating norms for nation-state behavior in cyberspace, and then, encouraging those countries that are breaking those norms to follow them and--but also warning other countries that may be thinking of engaging in that kind of behavior that we will catch them out and call them out.

Marc Raimondi
Thanks. We have time for one more question. And then, we'll go into the backgrounder. Grant, could you please, whoever's next on the list, give them the last question?

Operator
Sure. Our last question will come from David Shortell with CNN. Please go ahead.

David Shortell
Hi, guys. Thanks for doing this. A couple questions. First, (inaudible) for Tracy. Can you help break out for us the new allegations that we're seeing today regarding the Sony hack and the Bangladesh Bank episode beyond, obviously, the addition of two new co-conspirators. And then, the second question, perhaps for John is we've discussed today the novel and sophisticated tools that these military hackers are using. Can you expand on that a bit? What's the pace of new tools that they're cranking out over in North Korea? And how did their capabilities stack up against other bad or other good actors around the world?

Tracy Wilkison
Hi. This is Tracy Wilkison. First--there's two counts in the indictment. The first count alleges a conspiracy with respect to hacking. And then, the second is a conspiracy with respect to fraud, okay. And in the first count, the new allegations, you have the original allegations regarding the SWIFT system and the cyber heist targeting the banks. And then, it adds in
three additional schemes. One is the ATM cash out scheme where they took control of the bank ATMs and were using that to cash out millions of dollars.

Two is the cyber extortions where they would gain access to the computer systems, steal data, and then, extort money in exchange for the for the data. And then, third is the cryptocurrency allegations where they were designing systems that were supposed to look like they were supposed to trade and store cryptocurrency but were actually giving a backdoor into the system so that they could then steal the cryptocurrency. In addition, in count one, there were additional new bank heists that were added since the time of the complaint. And then, count two is this marine chain cryptocurrency fraud conspiracy where they were developing a digital token to trick people into investing, not knowing that they would be supporting the North Korean regime.

Unknown Speaker
(Inaudible)—

John Demers
--(Inaudible) Hey, David. There's another part to David's question. Hey, David, it's John Demers. As to your other questions, I mean, the North Koreans are among the most sophisticated nation-state cyber actors in the world. They may lack resources, but those that they have they dedicate, in large part, to their cyber program. And they have very good hackers who work for them. And in terms of the pace of their tool development, I don't think I can answer that with any specificity. But they continue to engage in new tool development, and as this shows, cook up new schemes for raising money for the regime. It's a very sophisticated actor. It's a dangerous actor, especially when it comes to financial institutions. And it's one that we're going to continue to investigate and look at.

Jesse Baker
Hi, David. It's, real quick, it's Jesse Baker—

Kristi Johnson
--I'd just like to add. It's Kristi Johnson. Yep. Oh, sorry. Go ahead, Jesse.

Jesse Baker
Just, I'm sorry, just super--real quick, David--

Kristi Johnson
--Okay. Thank you—

Jesse Baker
--It's Jesse Baker from Secret Service. I wanted to acknowledge what you talked about, about the cutting edge. And we've seen that in so many different ways of people, basically, trying to separate you from your wallet. And what I don't want to miss is that we see this in currency. For example, they design new currency. And people are already there trying to counterfeit it. No matter what sort of devices you put in, people will always push the envelope. And because we're so interconnected on these digital tools, they're leveraging that constantly.

But remember, they still have to utilize people outside of the country. As we saw here with this Alaumary case, there are still runners that are come to America, they're going to be taking money out of banks, and this is where we're going to look for them. And I think another final point that is critically important is the social engineering aspect of this. Remember, on business email compromise, how many times have we gotten emails about this? Or click on this link and once you do, the whole system, oftentimes, can be compromised. And I can tell you, people at work hate me because any email that comes to me, I never click. I never click. And I think there's so much, still, out there in education with the public to be so careful and mindful on what we click on and what we do because it is an incredibly key aspect. No matter how advanced they are, social engineering is still a critical component of this.

Marc Raimondi
All right. Kristi, do you have something to add to that—

Kristi Johnson

--Kristi Johnson, here. That's--Yep. Thank you very much. Exactly the point I wanted to make, Jesse. Thank you. And the prevention piece is just critical. It is. It really highlights the need for these malware analysis reports and the cybersecurity advisory that was issued today, just to continue to educate and inform the public and our, all of our partners around the globe. It is the click of the link. Sounds very basic and rudimentary, but if we can educate one more person to not do that and to make sure that they know exactly what they're responding to when they get unsolicited emails or job offers that entice them to click a link that, ultimately, can introduce malware to their system, that's our goal is to continue the prevention efforts. Thank you for allowing me to make this comment.

Marc Raimondi
All right. Thank you very much. We're going to move into the backgrounder now. The principals who spoke earlier, you are free to go. And we'll give it a minute. If you have no interest in the backgrounder, you're welcome to drop off. If you do want to talk to some additional subject matter experts about the indictment, you're welcome to stay on. We'll start out with the Central District of California Deputy Chief of the Cyber and Intellectual Property Crime Section. Speaking first, Anil Antony. And then, we'll have Sean Newell, the Deputy Chief for Cyber for the DOJ's National Security Division will be available to answer your questions as well. These will be--the attribution is senior justice officials for this.

Operator
And if you'd like to ask a question, it is star then one.

Marc Raimondi
Okay. Anil, why don't you start out?

Anil Antony
Sure. Good morning. This is Anil Antony. I'm an Assistant United States Attorney and the Deputy Chief of the Cyber and Intellectual Property Crime Section, as was mentioned, at the U.S. Attorney's Office here in Los Angeles. I'm one of the two prosecutors who obtained the charges against the North Korean hackers and Ghaleb Alaumary. I'll provide a background briefing on two topics. The first is the 2018 complaint as it relates to the indictment that was unsealed today. And the second is additional information about the family of malicious cryptocurrency applications. And then, I'll take any background questions.

As you heard at the briefing a few minutes ago, we've unsealed an indictment that dramatically expands the allegations made in the criminal complaint filed in 2018. To briefly recap, the criminal complaint charged one defendant. And it was supported by a 172-page affidavit that alleged a series of cyber attacks, and also detailed how the defendant was identified and how we were able to trace the attacks back to the source. That complaint, unsealed in 2018, focused primarily on three categories of events.

First, retaliatory cyber attacks targeting the entertainment industry, notably the well-known intrusion that had a devastating impact on Sony Pictures here in Los Angeles, but also targeting of AMC Theaters because a plan to show the movie The Interview. There was also an intrusion at a UK production company, creating a fictional miniseries about North Korea. All that occurred in

2014 and 2015. Second, the complaint discussed certain cyber-enabled bank heists, including the theft of $81 million from Bangladesh Bank and other bank heists from 2015 through 2017, in which the North Korean hackers attempted to steal hundreds of millions of dollars. I know there was a question about more recent hacks. There are additional hacks, as the acting U.S. Attorney clarified, from banks alleged in this indictment stretching from 2017 all the way to 2019.

The third part of the complaint is that it addressed the creation of the highly destructive and indiscriminate WannaCry 2.0 ransomware, which wormed its way through the internet in May of 2017, destroying hundreds of thousands of computers along the way and causing disastrous consequences for many sectors, including healthcare systems that were paralyzed. As described in great detail in the complaint, investigators were able to map the commonalities of these attacks. Many of the attacks involved malware with technical similarities and used the same operational infrastructure, such as computers, IP addresses, and email accounts. All of this conduct is alleged in the indictment as well.

As you know, the two-count grand jury indictment unsealed today charges three defendants, alleges new schemes and numerous new victims, and asserts that the conspiracy continued its illegal activities long after the initial case was announced in 2018. You've heard the broad outline of the allegations from the acting U.S. Attorney. The indictment does not discuss the various schemes with the detail found in the criminal complaint, nor does it discuss investigative steps taken by authorities. That is the nature of an indictment. I won't fill in that detail or retread the ground already covered by the prior speakers, but I will provide some additional details on this case and related mitigating mitigation efforts before we take questions.

In relation to the allegations about malicious cryptocurrency applications, we've identified specific programs, including a number that are part of a family of malware known in the cybersecurity community as AppleJeus, that’s apple as in the fruit, and then, the letters J-E-U-S. Most of the malicious cryptocurrency applications alleged in the indictment, with the exception of one called iCrypto-Fx, were part of the AppleJeus family of malware. These malicious cryptocurrency applications could be used by the North Korean hackers to provide a backdoor to the computers of victims. As alleged in the indictment, the North Korean hackers continued to create new strains of the AppleJeus malicious cryptocurrency applications as recently as a couple months before the indictment was filed.

As you've heard, the impact of these malicious cryptocurrency applications is not simply theoretical. The North Korean hackers used one of the AppleJeus family of malware to steal more than $11 million of cryptocurrency from a company in New York, which is identified in the indictment as the New York Financial Services Company. The first of the new defendants charged today, Jon Chang Hyok, is alleged to have been particularly involved in the creation and deployment of this AppleJeus family of malware. As an aside, the second new defendant charged today, Kim Il, is alleged to have been central to the marine chain token scheme, as well as being involved in thefts from banks and other hacking activity.

Turning back to the AppleJeus malware family, as you've heard this morning, the FBI and Department of Homeland Security issued a joint cybersecurity advisory and malware analysis reports on the AppleJeus family of cryptocurrency malware. The joint cybersecurity analysis

provides detailed information about the AppleJeus family of malware and six specific versions of that application. This analysis is designed to provide the cybersecurity community and the public with information about identifying this malware, avoiding future intrusions, and detecting and mitigating infections. That ends the background remarks, or my background remarks. I'm happy to field any questions at this point.

CONCLUSION

Marc Raimondi
Okay. Can you open the line for questions, please? We have time for about two questions, maybe three. If you don't get your question answered, please email me directly, and we'll get your question answered. Grant, can you open the line for questions? I see that there's several queued up.

All right. I think we're having some technical difficulties. So why don't we just do this. If you RSVP'd, you received an email from me earlier today with the products. Just respond to that email with your question, and we'll get your questions answered and back out to you. Thank you very much. And this background call is complete.