IN THE UNITED STATES DISTRICT COURT

FOR THE DISTRICT OF DELAWARE

UNITED STATES OF AMERICA	)	
	)	
	)	
v.	)	Criminal Action No. 13-78-GMS
	)	
NATHAN LEROUX,	)	
	)	
Defendant.	)	

GOVERNMENT'S STATEMENT OF FACTS

Had this matter gone to trial, the United States would have proved the following beyond a reasonable doubt through witnesses, testimony, and other competent and admissible evidence:

For a period that stretched from January 2011 through April 2014, members of an international hacking group agreed to and did conduct numerous unlawful intrusions into the protected computer networks of various technology companies involved in the online gaming industry. Between January 2011 and September 2012, Defendant Nathan Leroux was part of this hacking group, which also included Defendants David Pokora, Sanadodeh Nesheiwat and Austin Alcala [collectively "the Hacking Group"].

Much of the Hacking Group's criminal activity targeted Microsoft Corporation's then-unreleased Xbox One gaming console, the Xbox Live online gaming platform, and popular games available for such. The Hacking Group primarily victimized Microsoft and its software development partners, including but not limited to Epic Games, Inc., Valve Corporation, Activision Blizzard, Inc., Electronic Arts, Inc. and other companies. Members of the Hacking Group also targeted other companies for cyber attacks, including Sony, Inc. and Autodesk, Inc.

In general, the Hacking Group members obtained and maintained access to the victim

companies' computer networks through various methods, including SQL injection and the unauthorized use of valid log-in credentials that had been harvested from companies. Once inside the networks, the Hacking Group members accessed and exfiltrated unreleased software, software source code, trade secrets, and other confidential and proprietary information. Hacking Group members also stole financial account and legal information relating to the companies (but not their customers) and certain employees of such companies. The Hacking Group stored this stolen data on their own devices and/or on servers they leased and controlled in various locations, including California, New Jersey, Texas, Utah, and at least four foreign countries.

During their hacking sessions, Hacking Group members utilized instant messaging, VOIP and remote and shared desktop applications to communicate with each other and to jointly engage in the hacking activities. These applications allowed them to write and talk to each other in real time, and to see and control any selected group member's computer screen as they accessed and navigated through the computer networks of the victim companies. They also used a hacked Comcast modem, possessed and controlled by Defendant Nesheiwat, to gain Internet access while obfuscating their Internet Protocol addresses.

Cyber Intrusions and Theft Targeting Computer
Networks of Zombie Studios

Prior to November 2012, Defendants Leroux, Alcala, Pokora, along with D.W., participated in remote desktop intrusions into the computer network of Zombie Studios. They stole network log-in credentials, proprietary and confidential information.

On or about July 29, 2012, for instance, Hacking Group members, including Defendant Nathan Leroux, utilized TeamViewer software to intrude into the computer network of Zombie Studios. During this intrusion, co-conspirator D.W. accessed pre-release software and software builds for gaming software being developed by Zombie Studios, as well as personally identifying

information of Zombie Studios' employees. D.W. transmitted the means of identification, including the name, social security number, home address, and tax documents, of a Zombie employee to another Hacking Group member. D.W. subsequently submitted credit card applications in the names of the Zombie employee and a family member for limits of $15,000 and $10,000. D.W. additionally attempted to open a "Lendingclub.com" liability account in the name of the employee for approximately $20,000.

On or about July 31, 2012, Hacking Group members participated in a Remote Desktop Protocol intrusion into the computer network of Zombie Studios. During this intrusion, D.W. accessed pre-release software builds for gaming software being developed by Zombie Studios through computers and network assets controlled by Zombie Studios and/or its employees. D.W. and his co-conspirators accessed approximately 18 computers, websites, accounts, and/or network shares using unauthorized credentials. Data accessed during this intrusion included multiple software products produced by, or licensed to, Zombie Studios.

Cyber Intrusions and Theft Targeting
the Microsoft Game Developer Network Portal

In or about 2011 and 2012, Microsoft and its development partners were designing a next-generation Xbox gaming console, which Microsoft later named "Xbox One," as well as software to be used with the new Xbox console. Microsoft operated a "Game Developer Network Portal" ("GDNP"), which was an online system allowing prospective developers of games for Microsoft's Xbox and other gaming platforms to access, through an authentication system, pre-release Xbox operating system development tools and software. Microsoft controlled access to the GDNP by, among other methods, imposing licensing and other requirements for authorized users to be registered with Microsoft. In addition, Microsoft administered separate access enclaves within GDNP for more-restricted data.

Microsoft also provided developers with access to a software platform, known as

"PartnerNet," to refine video game creation. Microsoft controlled access to PartnerNet by, among other methods, licensing and providing authorized network users with an "Xbox Development Kit" ("XDK"), which is a non-retail unit used to access PartnerNet.

Beginning in or about January 2011, Defendants Leroux, Nesheiwat, Pokora and other Hacking Group members engaged in incidents of unauthorized access into Microsoft's computer networks, including GDNP's protected computer network, during which they stole log-in credentials, trade secrets, and intellectual property relating to the Xbox gaming system. In particular, Hacking Group members accessed GDNP with valid, but stolen, accounts associated with legitimate Microsoft software development partners.

Using the stolen log-in credentials of Microsoft's software development partners, Defendants Leroux, Nesheiwat and Pokora, as well as other Hacking Group members, spent hundreds of hours navigating the GDNP and copying files containing or relating to the specialized operating system for the forthcoming Xbox One, including software source code, technical specifications, assembly instructions, and software design and source code writing specifications for use by game developers for the console.

During an online electronic communication session on or about July 13, 2012, Defendants Leroux, Pokora and Austin Alcala, along with other Hacking Group members, discussed using compromised GDNP accounts to steal intellectual property from Microsoft, which they then could sell. They specifically discussed how they might divide the proceeds from such sales. The group discussed their expectation of being able to resell the intellectual property they planned to steal from Microsoft for up to $30,000. During the recorded session, the co-conspirators also stated, among other things:

Pokora: If you do multiple accounts it might raise a flag at GDN overall . . .

And then they might want to implement new security . . .

We don't want that . . .

We still want access to GDN, but we don't want to raise a flag at GDN

...

We just want to make them think that one developer was hacked ...

It'd be too weird if an entire like developer database...cause we want this access for the next generation of consoles as well

Leroux: Hey Austin, if you do, like, start selling some of yours, you should totally let me do that so I can pay for college because I seriously have to do that.

. . . .

Alcala: What do we do if one of us gets caught?

. . . .

Pokora: If you're stealing 12 kits. That's worth a decent amount of money. Microsoft might come after you.

Leroux: With sidecars, it's like, 2.5K each.

Pokora: So with 12 . . .

Leroux: 30K

Pokora: When you steal $30,000 from Microsoft, they might be a bit upset.

. . . .

Alcala: Dave, one of my accounts has access to order one more Durango (*i.e.,* an then-unreleased Xbox One).

Redacted Audio Call of 7/13/12 – "Multiple Accounts" (Ex. 8).

Defendants Leroux and Pokora and other co-conspirators agreed to use this stolen data

and operating system software to manufacture and then sell a counterfeit version of the next generation Xbox gaming console. Defendant Leroux subsequently ordered hardware components from online vendors to build a counterfeit version of the console, which was then being prepared for commercial distribution.

During an online electronic communication conducted on or about July 24, 2012, Defendants Leroux and Pokora and other Hacking Group members discussed a plan pursuant to which a Hacking Group member would travel from Delaware to Defendant Leroux's Maryland residence to obtain custody of the counterfeit version of the next-generation Xbox gaming console that Defendant Leroux built with the stolen intellectual property. They then planned to mail the counterfeit version of the next-generation Xbox gaming console built by Defendant Leroux to an individual located in Victoria, Mahe, Republic of Seychelles, who had agreed to purchase it.

On or about August 9, 2012, FBI Special Agents intercepted the counterfeit version of the next-generation Xbox gaming console built by Defendant Leroux in Delaware. Microsoft subsequently confirmed that this counterfeit version of the next-generation Xbox gaming console contained stolen Microsoft intellectual property.

In or about August 2012, D.W. listed another counterfeit version of the next generation Xbox gaming console for sale on eBay.com. D.W. sold the counterfeit version of the next-generation Xbox gaming console for approximately $5,000. D.W. paid Defendant Leroux a portion of the sales proceeds by giving Defendant Leroux access to D.W.'s credit card, which Leroux used to pay tuition to the University of Maryland.

Also in 2012, certain members of the Hacking Group, including Defendant Nathan Leroux, utilized stolen source code for the game "FIFA 2012," the intellectual property rights to

which are held by Electronic Arts, Inc., to design and employ software that automatically generated the virtual currency used in the FIFA 2012 game through Microsoft's Xbox Live online gaming system. Without the authorization of Electronic Arts, Defendant Leroux would sell bulk quantities (millions at a time) of these "FIFA Coins" online. Defendant Leroux obtained monetary proceeds from these sales, writing to C.K. at one point: "made $15k in a week," and "a few weeks and I should be set for college." Defendant Leroux told C.K. that "the fifa shit makes approx. $30/hr . . . lol . . . per xbox that I have running." Defendant Leroux explained that he was selling the bulk coins on a black wholesale market, and that his buyers then would "sell to whoever at whatever cost they want." Defendant Leroux added: "I don't bother with anything less than a million [coins] at once," to which C.K. replied: "sounds more like a drug operation than a hacking spree lol."

When C.K. asked Defendant Leroux if Electronic Arts or Microsoft was aware of this software exploit, Defendant Leroux responded: "they don't even know its being done lol." Defendant Leroux added: "[Microsoft and Electronic Arts] can't do anything about it either . . . the way its works IMHO is unpatchable without EA losing out on a LOT of money . . . . my little venture isn't enough money out of their pockets for them to even bother lol."

Respectfully submitted,

LESLIE R. CALDWELL
ASSISTANT ATTORNEY GENERAL
U.S. DEPARTMENT OF JUSTICE
CRIMINAL DIVISION

By: James Silver
James Silver
Trial Attorney, Computer Crime &
Intellectual Property Section

CHARLES M. OBERLY, III
UNITED STATES ATTORNEY

By: _____
Edward J. McAndrew
Assistant United States Attorney

Dated: 1/20, 2015, ~~2014~~