Helge Naber
Montana Bar Id. 7059
NABER PC
300 Central Avenue Suite 320
Great Falls Montana 59401
Phone (406) 452 3100
Fax (406) 452 6599
ATTORNEY FOR DEFENDANT

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MONTANA
GREAT FALLS DIVISION

	*	
UNITED STATES OF AMERICA	*	CR 08-33-GF-CCL-3
Plaintiff	*	
vs.	*	**DEFENDANT KUZMENKO's**
	*	**MEMORANDUM IN SUPPORT**
JEVGENIJS KUZMENKO	*	**OF SECOND MOTION TO**
Defendant	*	**DISMISS**
	*	

Defendant JEVGENIJS KUZMENKO, by and through counsel, hereby respectfully submits his Memorandum in Support of his First Motion to Dismiss for Lack of Probable Cause, and reasons as follows:

FACTUAL BACKGROUND

1. Between about December 20, 2007, and about January 11, 2008, an Co-Defendant Robert Borko effected a series of unauthorized intrusions into a private computer system belonging to D.A. Davidson Companies ("DADCo.") in Great Falls, Montana, retrieved personal and financial account information from D.A. Davidson Companies' customers, and stored such information on another computer believed to be under the control of Co-Defendant Robert Borko. See <u>Affidavit in Support of Request for Extradition of Jevgenijs Kuzmenko</u> ¶5 attached hereto as *Exhibit 1*.

2. On January 16, 2008, a senior employee of DADCo. Received an email from Co-Defendant Borko with the following content:

> "Mr. Morrison,
> Dadco web applications have several security vulnerabilities, which make possible access to your database and to your internal network. Please see an attached file with 20,000 records of your clients accounts – (Account Number, SSN, First Name, Last Name, Address, City, Zip, FC ID, Date of Birth, Account Asset Type, Account Value). Other clients records (more than 300k) as well as other sensitive date also be accessed.
> Davidson Companies is very respectfull financial services provider, hundreds of thousands of clients trust you their money, it's not good when any person have ability to look inside your Database. Do you agree with me that the vulnerabilities must be fixed as soon as possible? I offer you a full report on all the security vulnerabilities found on Dadco, my services as independent IT security consultant and the garantee that all aquired data will be deleted from my computer. I hope you not want to involve FBI here and we can have agreement like businesman." See U.S. Secret Service Investigative Report [undated] authored by USSSRA O'Neil (Govt. Bate-Stamp 00004) attached hereto as *Exhibit 2*.

3. In a subsequent email to another DADCo. employee, Co-Defendant Borko stated:

> "Donn,
> My name is Robert Borko, I'm independent IT security consultant. Michael Morrison advised me to contact you in regard to vulnerabilities in Dadco network, i believe Michael have already forwarded you my previous emails and you know the matter.
>
> The help i want to offer you include:
> 1. The full and detailed report on all vulnerabilities found on your network.
> 2. Advise on fixing the vulnerabilities + advises on how to garantee your network protection in future.
> 3. 6 Month free support on IT security questions, email or icq at your choise.

> 4. Garantee that all data aquired from Dadco network will be deleted from my computer.
> 5. Long time relations if you are interested in them.
>
> The price for the services is 80k usd, 40% should be paid in advance, 60% after you get the security report, the aquired data is destroyed when the final payment is made. Payment method is Western Union (several transfers) or bank wire, WU is prefered.
>
> I'm interested in you to benefit from our relations and have a good impression of it as many of my previous clients.
>
> Regards,
> Robert"

See id. at Govt. Bate-stamp page 00006.

4. DACo. ultimately agreed to retain Co-Defendant Borko's services, and further communications concerning further details of the services and transactions, including DACo. executing a service agreement with Co-Defendant Borko ensued. See id. at Govt. Bate-stamp pages 000010-000011. In further email exchanges on February 6 and February 8, 2008, in order to facilitate payment of the agreed-upon contract price, Co-Defendant Borko gave DADCo. the name Defendant Kuzmenko's name as the beneficiary of the first Western Union transfer in the amount of $1,500.00 directed to Western Union in the Netherlands. See id. at Govt. Bate-stamped pages 000015-000016.

5. Co-Defendant Borko further advised DADCo. that "people picking up the money don't know where the money from[.] They just get the WU trsnfer [sic] information." See id. at Govt. Bate-stamped page 000014. They had no knowledge of the origin of the funds transferred, or of the reason why the transfer was made. See U.S. Secret Service Investigative Report [undated] authored by USSSRA O'Neil (Govt. Bate-Stamp 000014) attached hereto as *Exhibit 2*.

6. Though someone with knowledge of the transfer contacted Western Union in the Netherlands on or about February 14, 2008, no one picked up, or attempted to pick up, this February 14, 2008-transfer. See Affidavit in Support of Request for Extradition of Jevgenijs Kuzmenko ¶8 attached hereto as *Exhibit 1*.

7. On February 18, 2008, Defendant Kuzmenko was arrested in Eindhoven/Netherlands. See U.S. Secret Service Investigative Report dated April 24, 2008 authored by USSSRAIC McDonough (Govt. Bate-Stamp 00040) attached hereto as *Exhibit 3*. Defendant Kuzmenko was arrested under a provision of the U.S.-Dutch Extradition Treaty, which allows for the preliminary arrest of a suspect physically present in the state from which extradition is requested ("the Requested State"). See U.S. Department of Justice Request for Provisional Arrest dated Feb 19, 2008 (Govt. Bate-Stamp 000340-000343) attached hereto as *Exhibit 4*. Such request was supported by factual allegations that Defendant Kuzmenko "made an attempt to pick the money and failed". See id. at Govt. Bate-Stamp 000341.

8. On February 20, 2008, all Dutch charges against Defendant Kuzmenko were dismissed by a Dutch court, and Defendant Kuzmenko remained detained based solely upon the provisional arrest and expedition request. See U.S. Secret Service Investigative Report dated April 24, 2008 authored by USSSRAIC McDonough (Govt. Bate-Stamp 00040) attached *hereto as Exhibit 3.* He was finally extradited to the United States in October 2009, and has remained in continuous custody since his arrival.

LEGAL ANALYSIS

I. Count II of the Indictment Against Defendant Kuzmenko Should be Dismissed Because No Threat of Economic Harm Was Made Against DADCo. and Its Fear Thereof Was Not Reasonable.

In Count II of the Indictment, Defendant Kuzmenko is charged with (aiding and abetting) economic extortion of DADCo., in violation of 18 U.S.C. §§1951, 2.

The elements of economic extortion are a threat of economic harm that is made with the purpose of obtaining money from the victim that puts the victim in reasonable fear of economic harm. See. U.S. v. Marsh, 26 F.3d 1496, 1500 (9th Cir. 1994). To find criminal liability for aiding and abetting such a threat, the prosecution must prove that the defendant specifically intended such threat to be made and took take some action in furtherance of such intent. *Cf*. U.S. v. Nelson, 137 F.3d 1094, 1104 (9th Cir. 1998).

Here, there was no threat of economic harm because Co-Defendant Borko's proposal to enter into a consulting agreement with DADCo. did not contain any threatening *conditio sine qua non* in case DADCo. would not accept his proposal. See U.S. Secret Service Investigative Report [undated] authored by USSSRA O'Neil (Govt. Bate-Stamp 00004 and 00006) attached hereto as *Exhibit 2*.

The emails show an offer a guaranty that the acquired data would be deleted from Co-Defendant Borko's computer. They did not contain any threats that the data would be published, disseminated, compromised, or otherwise abused if DADCo. turned down the offer. There is no evidence that the original data found on DADCo.'s servers were destroyed, tampered with, access to them in any way hindered, or that DADCo. was in any way blocked or prevented from their use. As far as the duplicate data retrieved by Co-Defendant Borko are concerned, they may have been stored on Co-Defendant Borko's computer forever or they may have been deleted regardless. Lastly, there was no mentioning that the intrusion would have been made public, thereby compromising DADCo.'s reputation or harming any other proprietary or economic interest.

Furthermore, the concept of hacking into a computer system, then revealing the intrusion, and seeking employment is hardly new or necessarily criminal. See ABC News Article "Hacking Their Way to a Job?" published Apr 17, 2009 attached hereto as *Exhibit 5*; BBC News Article "iPhone hacker lands software job" published Nov 26, 2009 attached hereto as *Exhibit 6* and Washington Post Article "The Hacker Fair" published Jan 6, 2010 attached hereto as *Exhibit 7*. Thus, even if there was a perceivable threat, it did not create a reasonable fear of economic loss.

In any event, all communication to and from DADCo. was initiated and entertained solely by Co-Defendant Borko. See U.S. Secret Service Investigative Report [undated] authored by USSSRA O'Neil (Govt. Bate-Stamp 00001 *et.seq.*) attached hereto as *Exhibit 2*. Defendant Kuzmenko was not involved in such communications, either directly or in an aiding capacity, nor did he knew of them or intended them to be relayed. See id. Therefore, Count II of the Indictment, as far as it pertains to him, should be dismissed.

II. Count V of the Indictment Against Defendant Kuzmenko Should be Dismissed Because He Did Not Undertake An Overt Act to Carry The Offense.

Defendant Kuzmenko is charged with receiving, possessing, disposing, or concealing money obtained from the acts of extortion, in violation of 18 U.S.C. §§875, 880 (Count V).

Defendant Kuzmenko did not attempt to pick up the February 14, 2008-transfer to Western Union in Eindhoven. See Affidavit in Support of Request for Extradition of Jevgenijs Kuzmenko ¶8 attached hereto as *Exhibit 1*. He did not approach Western Union outlet to attempt receipt of the transfer made to him as the designated beneficiary. There is no proof that he ever even contacted Western Union in order to do so; all that is known is that "someone with knowledge" contacted Western Union, but it is unknown who this "someone" is. See id. Defendant Kuzmenko was arrested by Dutch authorities in the apartment in which he stayed at the time. See U.S. Secret Service Investigative Report [undated] authored by USSSRA O'Neil (Govt. Bate-Stamp 00024) attached hereto as *Exhibit 2*. He had no knowledge of the source of the funds, or the reason why he was designated as their recipient. See U.S. Secret Service Investigative Report [undated] authored by USSSRA O'Neil (Govt. Bate-Stamp 000014) attached hereto as *Exhibit 2*.

Thus, there is no evidence that Defendant Kuzmenko received, or attempted to receive, any money from Western Union in Eindhoven. Therefore, Count V of the Indictment against him should be dismissed.

III. Count I of the Indictment Against Defendant Kuzmenko Should be Dismissed Because There Is No Offense for Which Commission He Conspired With The Co-Defendants.

As shown above, there is no evidence that Defendant Kuzmenko committed, or attempted to commit any criminal act. Person cannot be convicted of under 18 U.S.C. §371 of conspiring to commit a crime against the United States when the facts reveal that there could be no violation of a statute under which the conspiracy is charged. See U.S. v. Galardi, 476 F.2d 1072, (9th Cir. 1973).

WHEREFORE, Defedant Kuzmenko respectfully moves the Court to dismiss Counts I, II, and V of the Indictment against him.

Counsel for Defendant has conferred with Counsel for Plaintiff earlier, and counsel for Plaintiff indicated that he will resist this motion.

Counsel for Defendant estimates that the time sufficient for a hearing would be one hour.

Respectfully submitted this 5th day of February, 2010.

NABER PC

/s/ Helge Naber
Helge Naber
Montana Bar Id. 7059
300 Central Avenue Ste. 320
Great Falls, Montana 59401
Telephone (406) 452 3100
Facsimile (406) 452 6599
ATTORNEY FOR DEFENDANT

CERTIFICATE OF COMPLIANCE

Pursuant to L.CR. 12.1(e), counsel for Defendant Kuzmenko hereby certifies that this MEMORANDUM IN SUPPORT OF SECOND MOTION TO DISMISS contains 1,746 words and is thus compliant with the word limit by L.CR. 12.1(b).

NABER PC

By __/s/ Helge Naber_________________________
300 Central Avenue Ste. 320 • Great Falls, MT 59401

- Clerk of District Court via CM/ECF
- Ryan Archer Esq.

US ATTORNEY's OFFICE
316 North 26th Street
Billings Montana 59101

CERTIFICATE OF ELECTRONIC SERVICE

This is to certify that the foregoing MEMORANDUM IN SUPPORT OF MOTION TO DISMISS was duly submitted to the CM/ECF System of the trial Court named in this action, and submitted to counsel for the plaintiff by facsimile transmission on February 5, 2010.

NABER PC

By __/s/ Helge Naber__________________________
300 Central Avenue Ste. 320 • Great Falls, MT 59401

abc NEWS

Hacking Their Way to a Job?

17-Year-Old Behind Recent Twitter Worm Offered Job After Claiming Responsibility

By KI MAE HEUSSNER

April 17, 2009—

For the social networking darling Twitter, it was a headache and potential threat. But for the young man behind the computer worm that attacked the micro-blogging site this week, it was a fast track to a job.

Called both "Mikeyy" and "StalkDaily," the pesky computer program crashed the tweet-fest for the first time over the weekend, leaving thousands of unwanted messages in its wake.

Infected accounts not only displayed posts left by Twitter users and their followers, but messages directing users to StalkDaily.com and saying things such as "Mikeyy I am done&," "Twitter please fix this" and "Twitter hire Mikeyy."

Well, Twitter did not hire "Mikeyy." But, it looks like someone else will hire 17-year-old Michael "Mikeyy" Mooney.

The teenage programmer told ABCNews.com that after claiming responsibility for the attacks, two companies contacted him with job offers.

And though leading computer security experts do not endorse hacking as way to gain the attention of potential employers, Mooney is hardly the only young programmer to score a job after making headlines for a hack.

A Way to 'Get My Name Out There'

The Brooklyn, N.Y., high school senior told ABCNews.com that he started programming in the sixth grade and over the past few years he's developed about five computer worms. In the ninth grade, he says he was expelled from school for half a year after breaking into the county's school network.

Creating worms is something of a hobby, he said. But in the case of the Twitter worm, it was also something else. "It was a little bit to show the developers of Twitter that there was a problem," Mooney said. "I did the worm to get my name out there & to like companies, not just general people. Since Twitter is so big they'll know who I am for the future."

Mooney said he created the worm because he wanted to prove to Twitter that its site was vulnerable before someone else exploited the flaw and caused more harm.

'Grey Hack' Was a Service?

His attack was a "grey hack," he said, that went over the line but didn't pilfer or store any personal information belonging to Twitter users. Mooney said Twitter hasn't contacted him but said he and his parents have retained a lawyer.

"I'm really getting a bad reputation from it but at the same time people are taking into consideration that even though I did some harm I didn't cause any damage," he said.

Among the negative comments and e-mails, he said, he's also received a number of positive ones, including the job offers.

Travis Rowland, founder and CEO of exqSoft Solutions, a custom Web applications development company, confirmed that he'd offered and that Mooney had accepted a job with his company, starting immediately.

"I contacted him after I saw what he did to Twitter and asked him," Rowland said, adding that Mooney will be doing security analysis and Web development.

The way he sees it, Twitter wasn't paying attention to a basic vulnerability in its system and Mooney's hack was a service.

Mooney Could Have Caused More Trouble But Didn't

Twitter did not immediately respond to requests for comment from ABCNews.com, but said on its blog that it "takes security very seriously and we will be following up on all fronts." It also said that it has identified and secured all of the compromised accounts.

With the knowledge Mooney obtained, Rowland said he could have caused more trouble but chose not to.

"In my opinion, he could have stored the user information on their profiles but he didn't," Rowland said. "He didn't use it to steal personal information."

By hiring Mooney, Rowland isn't only getting new talent but publicized talent, "and I think that's a good thing for our company," he said.

Although some companies might be wary of hiring a rogue programmer, Rowland said he himself could have fallen in a similar category. Now 24 years old, he started programming in his teens.

He couldn't disclose many details but said he once worked in military intelligence and "landed that position in a similar fashion." He said he couldn't disclose what agency he worked for or any other details.

Hacker Have Valuable Skills

And Rowland and Mooney have company.

Just last month, a New Zealand teenager, Owen Thor Walker, who helped a crime gang hack into more than 1 million computers worldwide and skim millions of dollars from bank accounts, landed a job as a security consultant for a telecom company, The Associated Press reported.

In hiring Walker, the company said Thor had the skills that senior executives needed to understand security threats.

And one of the most notorious hackers of all time, Kevin Mitnick, was just 17 when he was first arrested for computer crime.

He broke into computer systems at Novell, Motorola, Sun, Fujitsu and other firms, stealing their software and crashing their machines. He was caught, for the last time, in 1995.

He served four years but now runs his own computer security firm and has written two books including "The Art of Intrusion."

Highly-Publicized Hacking Stories Not the Norm

But many computer security experts caution that these examples aren't the norm.

"Anybody that would release any kind of thing into the wild is not someone we'd ever want to be associated with," said Kevin Haley, the director of security firm Symantec's security response team.

He told ABCNews.com that while security firms obviously look for smart people who understand what unlawful hackers do, there's no need to actually let a worm go out into the wild.

Chris Boyd, the director of malware research for FaceTime, a Belmont, Calif. IT security, management and compliance company, said if young programmers like Mooney spot flaws, there are better ways of alerting companies than exploiting them to make a point.

"Part of security research -- part and parcel of it -- is that companies will ignore you when you bring [flaws] to their attention," he said. "It takes time. If he doesn't want to deal with that, maybe this isn't the field for him."

Yet there are hundreds of thousands of teenagers wreaking all kinds of havoc online, he said, and the ecosystem that supports their Internet mischief rewards illicit hacking.

"There is something that's being perpetuated -- if you go on any number of teen hack forums, there's a section on there that lists the top ten hackers that ever lived. Quite a few of those guys made their ways into a respectable living," Boyd said.

Black Hat Route Is a Myth

But by no means, he emphasized, is the recommended or most effective route. Of the hundreds of people he knows in the security world, none were ever black hats. (In computing lingo, black hats are those who penetrate computers without authorization for profit, fun or protest. White hats, sometimes called "ethical hackers," are computer security professionals hired by companies whose intent is to keep computers and networks safe.)

"It's a bit of a myth, I think that you have to go down the black hat route," he said.

Dan Kaminsky, a computer security consultant for Seattle-based IOActive, Inc., who unveiled a major Internet flaw to the security community last summer, agrees.

"Building a serious career is about giving people reasons to hire you, not reasons not to," he said.

He also highlighted that hackers will likely make less money because the firms hiring them know that they're likely blackballed from other companies.

The public only hears about the hackers that went on to successful careers -- not the ones that never recovered from digital transgressions -- but they're hardly in the majority.

"It's easy to blow something up. But how many people can really crank down to do substantial research to help remedy a problem?" he asked. "That's harder, that makes it more impressive."

BBC NEWS

iPhone hacker lands software job

The 21-year-old hacker who wrote the first iPhone worm has landed a job developing software for the phones.

Ashley Towns wrote Ikee, a self-propagating program that changed the phone's wallpaper to a picture of 80s pop singer Rick Astley.

Mr Towns has now been employed as a iPhone application developer for Australian firm mogeneration.

Ikee was not malicious but paved the way for a more serious variant which targeted users of the online bank ING.

"It leaves a nasty taste that he has been rewarded like this, yet has not even expressed regret for his actions," Graham Cluley of Security firm Sophos told BBC News.

Mr Towns said that he had created the virus to raise the issue of security. He has not faced any criminal charges.

'Wild worm'

It was designed to exploit jail-broken phones, where a user has removed Apple's protection mechanisms to allow the phone to run any software.

Estimates suggest there could be up to 25,000 jailbroken phones in Australia, whilst up to 10% of the more than 55m iPhones and iPod Touches devices sold worldwide are thought to be cracked.

It specifically targeted those handsets with SSH (secure shell) installed, a program that enables other devices to connect to the phone and modify the system and files.

The worm was able to infect those phones where the owners had not changed the default password after installing SSH.

It could be removed by changing the phone's password and deleting some files.

After it was found circulating "in the wild", a second worm was discovered. Mr Cluley said it was "based" on Mr Town's code and targeted people in the Netherlands who used their iPhones for internet banking with Dutch online bank ING.

The new worm redirects the bank's customers to a lookalike site with a log-in screen. It can also be used to remotely control the phone without the users permission.

Analysts said that it was designed with a "clear financial motive".

Mr Towns is the latest in a long line of programmers to find employment after a high-profile hack.

In 2008, New Zealand computer hacker Owen Thor Walker was hired by a telecommunications company as a security consultant.

He had previously pleaded guilty or being part of an organisation that was thought to have caused millions of dollars worth of damage.

"We interviewed Ashley, assessed him with our iPhone developer test - which he passed with flying colours - and we employed him today," said a spokesperson for mogeneration.

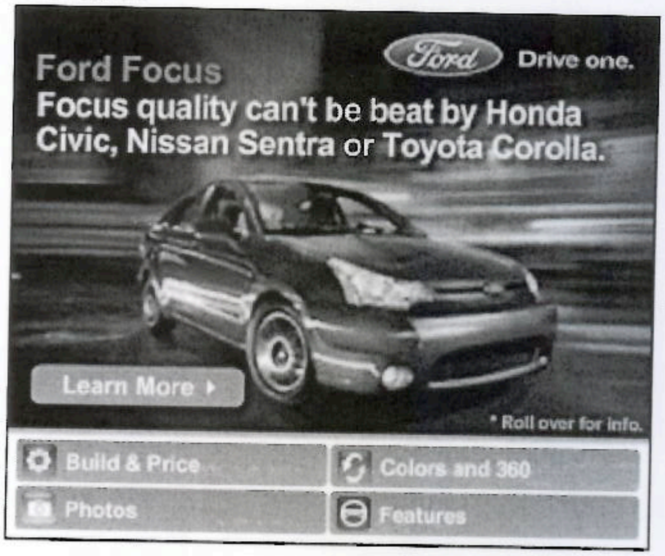
Story from BBC NEWS:
http://news.bbc.co.uk/go/pr/fr/-/2/hi/technology/8380265.stm

Published: 2009/11/26 11:24:47 GMT

The Washington Post

The Hacker Fair: Where Job-Hunting Developers Get A Chance Show Off Their Skills

Jason Kincaid
TechCrunch.com
Wednesday, January 6, 2010; 9:44 PM



For most people on the prowl for employment, job fairs are something of a mixed blessing. Yes, they can sometimes lead to job opportunities. But it's often very difficult to separate yourself from the dozens (or hundreds) of other prospective applicants in attendance ? at the end of the day, you're probably just another resume in the stack. The Hacker Dojo, a community center that caters to developers in the Mountain View area, is looking to turn that model on its head with *The Hacker Fair*. Where developers actually get to show off their coding talents to the employers in attendance.

Here's how they describe it:

At the Hacker Fair, the job seekers are the ones giving demonstrations, and the recruiters are the ones walking around.Think of it as a "science fair" where the "science projects" are the developers' personal and side projects, the "judges" are recruiters, and the "prizes" are interviews and hopefully job offers!

The event will be taking place on January 16th from 10am ¿ 1pm, in Mountain View CA (you can find more details on signing up here). It will be attended by some of Silicon Valley's most well known companies, including Yahoo, Microsoft, Mozilla, Yelp, and plenty more. Microsoft is even sponsoring breakfast.

For those who attend, feel free to let us know how it goes in the comments. I'm guessing a few of the hackers may get creative with their projects, and employers won't know what to expect, which should make things even more interesting.