BY [ASHLEY POST](http://www.insidecounsel.com/author/ashley-post)JULY 26, 2013

Five hackers have been charged in what’s being called the biggest data breach in U.S. history.

Yesterday, federal prosecutors announced that they’ve indicted five cyber criminals responsible for a hack that cost targeted companies more than $300 million. Prosecutors say the five men, who are from Russia and Ukraine, stole and sold at least 160 credit card numbers. Two of the suspects are in custody.

The hacked companies include Nasdaq, Visa Inc., J.C. Penney Co., JetBlue Airways Corp. and Carrefour SA.

According to authorities, each of the men had specialized tasks—two hacked into networks, another mined them for data, another provided anonymous web-hosting services to hide the group’s activities, and another sold the stolen data and distributed the profits.

“This type of crime is the cutting edge,” New Jersey U.S. Attorney Paul J. Fishman said in a statement. “Those who have the expertise and the inclination to break into our computer networks threaten our economic wellbeing, our privacy and our national security.”

# U.S. indicts hackers in biggest cyber fraud case in history

BY [**DAVID JONES**](http://blogs.reuters.com/search/journalist.php?edition=us&n=david.jones&) AND [**JIM FINKLE**](http://blogs.reuters.com/search/journalist.php?edition=us&n=jim.finkle&)

(Reuters) - Federal prosecutors said on Thursday they have charged five men responsible for a hacking and credit card fraud spree that cost companies more $300 million and two of the suspects are in custody, in the biggest cyber crime case filed in U.S. history.

They also disclosed a new security breach against Nasdaq, though they provided few details about the attack.

Other companies targeted by the hackers include a Visa Inc licensee, J.C. Penney Co, JetBlue Airways Corp and French retailer Carrefour SA, according to an indictment unveiled in New Jersey.

Authorities have been pursuing the hackers for years. Many of the breaches were previously reported, though it appeared the one involving Nasdaq OMX Group Inc was being disclosed for the first time.

Prosecutors said they conservatively estimate that the group of five men from Russia and Ukraine helped steal at least 160 million payment card numbers, resulting in losses in excess of $300 million.

Authorities in New Jersey charged that each of the defendants had specialized tasks: Russians Vladimir Drinkman, 32, and Alexandr Kalinin, 26, hacked into networks, while Roman Kotov, 32, mined them for data. They allegedly hid their activities using anonymous web-hosting services provided by Mikhail Rytikov, 26, of Ukraine.

Russian Dmitriy Smilianets, 29, is accused of selling the stolen data and distributing the profits. Prosecutors said he charged $10 for U.S. cards, $15 for ones from Canada and $50 for European cards, which are more expensive because they have computer chips that make them more secure.

The five hid their efforts by disabling anti-virus software of their victims and storing data on multiple hacking platforms, prosecutors said. They sold payment card numbers to resellers, who then sold them on online forums or to "cashers" who encode the numbers onto blank plastic cards.

"This type of crime is the cutting edge," said New Jersey U.S. Attorney Paul J. Fishman. "Those who have the expertise and the inclination to break into our computer networks threaten our economic wellbeing, our privacy and our national security."

The indictment cited Albert Gonzalez as a co-conspirator. He is already serving 20 years in prison after pleading guilty to helping mastermind one of the biggest hacking fraud schemes in U.S. history, helping steal millions of credit and debit cards.

Prosecutors say the defendants worked with Gonzalez before his arrest in Miami, then continued on a crime spree after his capture.

Drinkman and Smilianets were arrested in June 2012, while traveling in the Netherlands, at the request of U.S. authorities. Smilianets was extradited last September and is expected to appear in New Jersey Federal court next week. Drinkman is awaiting an extradition hearing in the Netherlands.

Prosecutors declined comment on the whereabouts of the other three defendants.

Tom Kellermann, a vice president with security software maker Trend Micro, said he thinks the prospects are dim that they will be caught because authorities in some countries turn a blind eye to cyber criminals.

"There is an enormous shadow economy that exists in Eastern Europe. In some countries, sophisticated hackers are seen as national assets," he said.

Kalinin and Drinkman were previously charged in New Jersey as "Hacker 1" and "Hacker 2" in a 2009 indictment charging Gonzalez in connection with five breaches.

NASDAQ BREACH

The U.S. Attorney's Office in Manhattan announced two other indictments against Kalinin, one charging he hacked servers used by Nasdaq from November 2008 through October 2010. It said he installed malicious software that enabled him and others to execute commands to delete, change or steal data.

The infected servers did not include the trading platform that allows Nasdaq customers to buy and sell securities, prosecutors said. Officials with Nasdaq said they could not immediately comment.

A source with knowledge of the breach said on Thursday the indictment was not related to a 2010 attack that Nasdaq had previously disclosed, which was targeted against Directors Desk, a service used by corporate boards to share documents and communicate with executives, among other things.

The source, who asked to remain anonymous due to the sensitivity of the matter, said that hackers appear to have used their access to the firm's network to create their own landing page on a Nasdaq website, where users were directed when they wanted to change their passwords.

The second indictment filed against Kalinin in Manhattan, which was unsealed on Thursday, charged that he worked with a sixth hacker, Russian Nikolay Nasenkov, 31, to steal bank account information from thousands of customers at Citibank and PNC Bank from 2005 to 2008, resulting in the theft of millions of dollars.

MAKING PROGRESS

Mark Rasch, a former federal cyber crimes prosecutor, told Reuters that the arrests show that law enforcement is making progress in identifying those responsible for major cyber crimes.

"They involve dozens or even hundreds of people huddled over computer terminals all over the world in a common purpose of stealing of disseminating credit card numbers," said Rasch, who was not involved in bringing the case.

Among the breaches cited in the New Jersey indictment, prosecutors charged that the group was responsible for the theft of more than 130 million credit card numbers from U.S. payment processor Heartland Payment Systems Inc beginning in December 2007, resulting in approximately $200 million of losses. That was the same case for which Gonzalez was convicted and which was the largest case of its kind before the latest indictments.

Heartland released a statement praising authorities for their work: "We hope that this indictment further delivers the message that prolific hacking organizations worldwide will be pursued and charged for crimes such as this one."

The indictment charged that they took approximately 30 million payment card numbers from British payment processor Commidea Ltd in 2008 and 800,000 card numbers from Visa Inc's licensee Visa Jordan in 2011.

An attack on Global Payment Systems that begin in about January 2011 resulted in the theft of more than 950,000 cards and losses of about $93 million, according to the indictment.

It charged the ring with stealing approximately 2 million credit card numbers from French retailer Carrefour SA, beginning as early as October 2007 and said the theft of card numbers from Dexia Bank Belgium resulted in $1.7 million in losses.

Other victims included Dow Jones, Wet Seal Inc and 7-Eleven Inc, according to prosecutors.

Dow Jones said in a statement that there was "no evidence" that information of Dow Jones or Wall Street Journal customers information was compromised as a result of the breaches.

Officials with Carrefour, Global Payments and JCPenney declined comment.

(Reporting by David Jones and Jim Finkle; Additional reporting by [John McCrank](http://blogs.reuters.com/search/journalist.php?edition=us&n=john.mccrank&),[Christian Plumb](http://blogs.reuters.com/search/journalist.php?edition=us&n=christian.plumb&), [Phil Wahba](http://blogs.reuters.com/search/journalist.php?edition=us&n=phil.wahba&), [Beth Pinsker](http://blogs.reuters.com/search/journalist.php?edition=us&n=beth.pinsker&), Varun Aggarwal, [Jennifer Saba](http://blogs.reuters.com/search/journalist.php?edition=us&n=saba&), Beth Gladstone, Aman Shah and David French; Writing by Jim Finkle; Editing by [Scott Malone](http://blogs.reuters.com/search/journalist.php?edition=us&n=scott.malone&),[Alden Bentley](http://blogs.reuters.com/search/journalist.php?edition=us&n=alden.bentley&) and [Claudia Parsons](http://blogs.reuters.com/search/journalist.php?edition=us&n=claudia.parsons&))

**It was one of the most sophisticated**[**cyber crime**](http://www.channel4.com/news/cybercrime-a-bigger-threat-than-nuclear-attack)**campaigns ever mounted: a hacking spree that snared millions of victims worldwide and netted the gang behind it as much as half a billion pounds. Not content with raiding the bank accounts of their victims, the thieves blackmailed them, and then hijacked their computers to snare even** more targets.

The criminal network behind it has now been hit by a global police operation. **Channel 4 News** was given exclusive access to the UK's National Cyber Crime Unit (NCCU) as it helped in the take-down of the GameOver Zeus Crew, a notorious group of computer criminals believed to be based in Russia.

Phishing emails

The gang used carefully crafted phishing emails to trick its way on to victims' machines, often masquerading as urgent messages from HMRC or Companies House. Some corporate victims told**Channel 4 News** that the emails included specific details about their company to add to their authenticity.

The emails included an attachment or link, and when the recipient clicked on it they were infected with GameOver Zeus, a powerful new virus. It first checked whether the computer's keyboard was set up in Russian, and if not, it installed a more complex virus which gave the criminal gang complete control over the machine.

"Anything you can do on your computer, they can do on your computer without you knowing," said Stewart Garrick, who has led the NCCU's investigation into the gang. "I know of more than 15,000 computers in the UK infected with this right now."

The virus was used to blackmail victims, steal cash from their accounts, and then force the infected computer to snare other victims.

It gave the criminals real-time access to the victim's entire online life: **Channel 4 News** was shown how the hackers can record videos of everything that appears on the screen, gather passwords for websites, and even switch on the webcam.

Extortion campaign

Blackmail is a key tactic, and the gang was behind a global extortion campaign that snared doctors' surgeries, lawyers and even police stations. It used the virus to launch Cryptolocker, which scrambles the victims' files and gives them deadline to pay a ransom of hundreds of pounds to get them back.

Eunice Power, a chef in Co Waterford, found the contents of her laptop scrambled. "This big red screen appeared saying 'your files have been encrypted'. I checked the files and it was all gobbledy-gook, one after the other. I unplugged it thinking that would sort it out but it didn't.

"At this point it was flashing up an amount of time, I had 72 hours to pay a ransom. I had an external back-up which was plugged in at the time so that was all encrypted. I could feel perspiration coming out through me. I didn't believe anything could be so evil."

The blackmailers demanded payment in the virtual currency Bitcoin. As Mrs Power struggled to make the payment work, the countdown hit zero.

"I lost everything: family photos, accounts, payroll, everything. If someone had robbed my house it would have been easier. It was devastating," she said.

Her folders are still intact, meaning she can see which photos and documents she lost, but when she tries to open them, she is confronted with incomprehensible code.

Bank accounts targeted

Blackmail is just one option: the thieves' main target is internet banking.

"They want to monetise the investment they've made in getting into your machine," said Don Smith of Dell SecureWorks, which has spent years tracking the gang. "They are absolutely after dollars, pounds and euros."

Once installed the virus waits for the computer to connect to online banking, and then alerts the criminal, who can manipulate what the victim sees on screen, throwing up fake pages and tricking them into authorising transfers out of their account.

**Protecting yourself**  
  
With the criminals' network disrupted, now is the time to protect your computer. There are three things you need to do:  
  
1. Update your operating system (this is Microsoft Windows if you own a PC, or Mac OS if you have an Apple machine).  
  
2. Install, update and run anti-virus software. There are many options but try to buy it as a physical CD - that way you don't risk downloading from a dodgy website.  
  
There is more advice on the government's [Get Safe Online](https://www.getsafeonline.org/) website

"They are able to inject pages between the user and their bank without anyone being any the wiser," said Smith. "They can ask for extra login credentials, ask for credit card numbers, anything to get the victim to a point where money can be transferred out."

One of the victims was AEV, a varnish factory in Birkenhead. One of its employee's computers was infected with the virus after clicking on an email.

The thieves' fake webpages convinced her that her bank login had failed, and that she needed to use the keypad which is normally used to make transfers. Unwittingly, by using the keypad she authorised two payments to accounts in the Ukraine and Cyprus.

Utter horror

"We lost £100,000 in under three minutes," said AEV Managing Director Jonathan Kemp. "We started the day normally, and by the end of it there was utter horror."

The business eventually got the money back from the bank, but in the meantime, after it went public, it was contacted by dozens of other fellow victims.



"The phone started ringing. Eventually we ended up with 40 or 50 businesses that had been hit. I calculated the losses at something like £3.5m," said Mr Kemp.

Millions of victims

In fact, there are millions of victims around the world. Once infected, a victim's computer becomes part of the criminals' network. It can be used to send instructions to other hacked machines, and to send phishing emails to snare more targets.

This weekend, the NCCU, in co-operation with tech companies, the FBI and other forces around the world, moved in to break up the network. They reprogrammed the infected computers to stop them communicating with each other, and then with the help of internet companies hit the hackers' fallback network of command computers which can send instructions to the hacked machines.

Global

"This is the biggest operation I've been involved with in 28 years in law enforcement," said Mr Garrick. "We're taking unprecedented steps, and it's truly global in scale."

The NCCU's hope is that if it can stop the GOZ Crew's virus network from receiving updates, it will give software and anti-virus firms a chance to catch up. Users can then update their software, run anti-virus programmes, and protect themselves from the gang.

"It's a window of opportunity," said Mr Garrick. But with the criminals able to vanish into cyberspace at the press of a button, it seems inevitable they will return soon with newer, smarter tactics.