Gozi Virus Press Conference
Prepared Remarks of U.S. Attorney Preet Bharara
January 23, 2013

Good afternoon. My name is Preet Bharara, and I am the United States Attorney for the Southern District of New York.

Today, we announce federal charges against three top international criminals. As alleged in the unsealed documents, these men ran a modern-day bank robbery ring. But, as we have seen with increasing frequency, their bank heists required neither a mask nor a gun, but a clever computer program and an Internet connection.

In an information-age update on Willie Sutton, cyber criminals target banks too – because that's where the money still is.

As alleged, this ring conceived, developed, and spread a notorious bit of computer malware known in cyber circles as the Gozi Virus.

The Gozi Virus is essentially a Trojan horse for computers – narrowly tailored and specially designed to infect computers of unsuspecting users to steal their online banking credentials.

As we allege, the Gozi Virus has infected at least a million computers around the world, including 40,000 in the United States, and many more in Germany, Great Britain, Poland, France, Finland, Italy, Turkey and elsewhere. It has led to the theft of tens of millions of dollars from bank accounts of individuals and businesses.

Specifically, today we announce charges against three men who were at the top of this criminal cyber ring:

1. Nikita Kuzmin, also known by the online nickname "76," is a Russian national who conceived of the Gozi Virus and ran a business that rented the virus out to others. He was, essentially, the "idea man." Kuzmin has pled guilty to serious federal cybercrime charges. He has been cooperating with the government and assisting our investigation.

2. Dennis Calovskis, known by the online nickname "Miami," is a Latvian national who wrote some of the computer code that made the Gozi Virus so effective. Calovskis was arrested in Latvia last month.

3. Mihai Paunescu, also known appropriately by the online nickname "Virus," is a Romanian national who ran a so-called "bulletproof" hosting service that enabled cyber criminals throughout the world to spread the Gozi Virus and other malware and to commit numerous other cyber crimes, as well. Paunescu was arrested in Romania in November 2012 and was indicted in this district last week.

The charges against all three of these defendants were unsealed earlier today.

Now let me briefly describe the allegations in the indictments unsealed today.

As alleged, in 2005, Nikita Kuzmin first conceived of the Gozi Virus – malicious computer code or "malware" that could be used to steal the bank account information of individuals and businesses on a large scale. Kuzmin created a list of technical specifications to make the Gozi Virus effective, but he could not do it alone – he needed specialists with expertise and he needed a forum to market and sell his product.

If you take a look at the chart to my right, it basically lays out the scheme as set forth in the various charging documents. As I mentioned, Nikita Kuzmin, who we essentially describe as the "mastermind"of the entire operation, conceived of the virus and figured out what the specifications should be, but he wasn't a person who was able to write the source code himself, so he essentially got another individual, who was referred to as a "co-conspirator" in the documents, to write the source code.

Beyond that, what was clever about this operation as alleged in the charging documents was that they would modify the virus for particular uses of cyber criminals depending on how they wanted to use it, and how they wanted to steal money from banks. So he would further develop a relationship with other people including the individual we describe as "Miami" to do something called web injects which I'll describe in a moment, as depicted on the chart to my left.

After that was all done, the folks at the top of the scheme needed to figure out a way to get the virus to the actual other cyber criminals who were going to be able to use it to steal money from banks, and that was done over what was basically an internet bizarre for criminals, cyber criminals, called 76 Service. And in that forum, cyber criminals could either buy the software, buy the computer program, or lease it, sometimes for prices up to $50,000, plus a cut of the profits back to the mastermind, and then they were the ones who would actually send out spam to infect unsuspecting computers and then steal bank information, and thereby steal money from banks from unsuspecting individuals.

But of course, in order to be able to do that, as alleged in the charging documents, you needed to have a cloak, some kind of cover, and that's where the third defendant we mentioned comes in, Mr. Paunescu, aka "Virus." He was basically the host of what we call a "bulletproof" host and, as the name implies, that was a place where individuals could send forth spam and other nefarious emails to unsuspecting computers from behind a cloak of anonymity, so it would be very difficult for people to trace back where that was coming from. I'll spend a couple minutes more on that in a moment so you have a better sense of what that was.

So at that point, everything is set, and individuals would get spam email from behind the cloak of a "bulletproof" host, and if a person decided to open up a spam email, and typically it was a PDF as we described in the indictments, that PDF would be opened, and then the individual computer would become infected. There was a key-logging mechanism in the virus, and it would specifically try to find out if the computer was visiting an e-banking website, and it would make sure to take the information, including password information and other information so that bank

money could be stolen. And then that back information went back to the cyber criminals and the money went back to the cyber criminals, as you might imagine.

One more thing about the web inject. As you see in the chart to my left, one of the things that the defendants did in this case, or at least what one defendant was hired to do in this case, was to create a fake welcome page. When an individual would go to his or her bank account, instead of getting a legitimate welcome page, which you see in the left of that chart, they would get a false welcome page, which would then prompt them to give very sensitive information including, as you see on the chart, Social Security information, date of birth information, and pin numbers for their ATM cards – all as part of the charade behind the bullet proof service, so people could figure out what bank information they needed so they could steal the maximum amount possible as we allege.

Back for one second to the "bulletproof host," which I think is an important concept and helps people understand why this is such a difficult thing to track, and such a difficult thing to prosecute, and a difficult thing to investigate, so a lot of kudos to people here who were able to do it.

Notwithstanding its sophisticated and nefarious design, the Gozi Virus would never have been so lucrative for cyber criminals, and so damaging to its victims, were it not for people like Paunescu, one of the defendants in this case.

Just another word about the importance of the so-called "bulletproof host" for this alleged cyber scheme: Notwithstanding its sophisticated and nefarious design, the Gozi Virus would never have been so lucrative for cyber criminals, and so damaging to its victims, were it not for people like Paunescu.

As part of the hosting service, he allegedly provided critical online infrastructure, such as computer servers and IP addresses, to cyber criminals anonymously so that they could commit all sorts of cyber crimes, including spreading the Gozi Virus, with little fear of detection by law enforcement.

In effect, Paunescu functioned as an internet service provider for criminals, one that would protect them from prosecution – that's why his service was allegedly "bulletproof."

Paunescu rented servers and IP addresses from legitimate internet service providers. In turn, Paunescu allegedly rented the servers and IP addresses out to cyber criminals so that they could remain hidden and anonymous to legitimate internet service providers, private-sector security professionals, and above all law enforcement.

If law enforcement ever asked about a suspicious IP address, Paunescu could just say, you're right, I'll cancel it – but then Paunescu could just give the cyber criminal a new IP address unbeknownst to law enforcement.

With Paunescu's alleged help, cyber criminals committed all sorts of crimes including spreading the Gozi Virus, spreading other malware like the Zeus Trojan, conducting distributed denial of

service or DDoS attacks, and sending out spam. As alleged, Paunescu served as both lookout and cover.

Now let me remind everyone that Calovskis and Paunescu are of course presumed innocent unless and until they are proven guilty. We are seeking their extradition and expect that their cases will proceed in Manhattan federal court.

Now, it took nefarious international collaboration to unleash the full destructive power of the Gozi Virus – and it took groundbreaking law enforcement cooperation to bring its purveyors to face justice.

But this case should serve as a wake-up call to banks and consumers alike, because cybercrime remains one of the greatest threats we face, and it is not going away any time soon.

It threatens our financial security and our national security; it threatens individuals, businesses and governments alike; it threatens us from here in the United States and it threatens us from abroad.

That is why investigating and prosecuting cybercrime remains a top priority of this Office and the FBI.

Within the past year, we have charged many significant cyber cases – among other things, we've coordinated an international takedown charging dozens of online identity thieves in over a dozen countries, and we charged a multi-million dollar fraud ring based in Estonia. And in the year to come, we expect to charge many more.

Cyber criminals believe that their online anonymity and their distance from New York render them safe from prosecution. Nothing could be further from the truth, as today's charges demonstrate.

Let me finally introduce our law enforcement team.

I am joined here today by our investigative partner in these extraordinary cybercrime cases and so many others – the FBI: Represented by Assistant Director-in-Charge of the New York Field Office, George Venizelos; Special Agent-in-Charge of the Special Operations and Cyber Branch, Mary Galligan; Assistant Special Agent-in-Charge, Austin Berglas; Supervisory Special Agent Kerry Davis; and Special Agents Katherine Scott, Albert Murray, and Jonathan Perlstein.

DOJ's Computer Crime and Intellectual Property Section with whom we jointly prosecuted the case against Mr. Paunescu.

The NASA Office of the Inspector General.

Further, I want to extend my thanks to our foreign law enforcement partners whose cooperation and support were essential to getting us here today, especially the Latvian and Romanian law enforcement.

Finally, I want to thank the dedicated career prosecutors in my office for their unflagging dedication and consistently outstanding on this case and so many others. They are: Assistant U.S. Attorneys Sarah Lai and Nicole Friedlander, who are led by Deputy Chief of Cyber Crimes in our Complex Frauds Unit, Tom Brown, and Unit Chiefs Michael Bosworth and Richard Tarlowe.

I also want to thank DOJ Trial Attorney Carol Sipperly of the Computer Crime and Intellectual Property Section who worked with us on the Paunescu case.