# International hacking ring executes $1 billion banking breach

James J. Giszczak, Dominic A. Paluzzi | Monday, February 16, 2015

Kaspersky Lab, an Internet security firm, confirmed that an international hacking ring made up of hackers from Russia, Ukraine, China, and Europe stole as much as $1 billion from more than 100 banks in 30 countries, including the United States, in what could be one of the biggest banking breaches ever.

*The New York Times* first **reported** on the incident, quoting Chris Dogget from Kaspersky Lab as follows: "This is likely the most sophisticated attack the world has seen to date in terms of the tactics and methods that cybercriminals have used to remain covert."

**The method**

Kaspersky claims they uncovered that hackers secretly installed spying software on bank computers via phishing schemes and other methods to infiltrate the banks' systems. Those methods – coined "Carbanak" – eventually learned how to mimic bank employee workflows. "This allowed [the hackers] to see and record everything that happened on the screens of staff who serviced the cash transfer systems," Kaspersky said. "In this way the fraudsters got to know every last detail of the bank clerk" work and were able to mimic staff activity in order to transfer money and cash out."

The breach was dormant for about "two to four months" while it gathered information about the banks' operations before it struck. Once enough information was gathered, the hackers were then able to use that knowledge to make transfers into bank accounts they had created for the theft, and transfer that money into fake accounts to dispense cash from ATMs. This happened a few ways. Sometimes, it was changing an

account balance, and then transferring the excess funds into fake accounts. Other times, it would spew cash out of ATMs while one of the hackers was waiting beside the machine to collect the spoils.

It is unclear whether the attackers are expanding their efforts to other regions of the world, but it is possible. It is said that the “attacks remain active.” While the names of the banks hit have not been disclosed at this point, it is believed that JP Morgan Chase is on that list.

It appears that each individual bank suffered losses between $2.5 and $10 million. At the $10 million mark, however, it looks like the hackers packed up their nefarious tools and moved on to the next target. This may explain why the theft went undetected for so long.

**Phishing emails**

While this may be one of the largest, most sophisticated, banking breaches ever, the means for attack are not new, though the ante has certainly been upped. We have long known that a major cause of breaches occurs through employee-targeted phishing emails. As the **Verizon Data Breach Investigations Report** pointed out, most breaches fit into one of nine patterns, and “[t]he most prolific is the old faithful: spear phishing.” As demonstrated by this breach, these phishing emails and the malware used are becoming ever more sophisticated, difficult to detect, and hard to combat.

**Be prepared**

While educating employees on phishing emails is certainly something every company should be doing at this point, education is not foolproof to “human error.” It stands to reason that these attackers are exceptionally smart and will eventually break through any system's defenses. As such, companies need to take other precautions and be prepared when a breach hits.

Again, preparation and training are critical. While human error creates many opportunities for the thieves, this type of exposure can be dramatically reduced. You can never remind your employees enough to watch out for those phishing e-mails. It is also a good practice to send out “test” phishing e-mails to see who will “bite” on the bait. For those who do, additional training is necessary! Take the time now to reduce your exposure.

For more information, please contact one of the attorneys listed below.

**James J. Giszczak**

**Dominic A. Paluzzi**