Written by **Bob Adelmann** on February 16, 2015

Russian Cyber-thieves Steal $1 Billion From Russian Banks?

A report released on Monday from Kaspersky Lab to be presented at a cyber-security conference in Cancun, Mexico, revealed a highly sophisticated, well-funded, and immensely patient plan to steal at least $300 million from banks around the world, with estimates that the real losses could exceed $1 billion.

Kaspersky Lab, the fourth largest international provider of sophisticated software to fend off malware attacks, has been tracking the band of hackers known as Anunak or Carbanak for years. The first public exposure of the plot to steal millions at first appeared in late 2013 to be a simple mistake: an ATM in Kiev, Ukraine, started dispensing cash while no one was around. Within seconds, security cameras showed participants in the theft arriving and scooping up the loot and escaping before anyone at the bank could be alerted.

The losses extended far beyond that single ATM, and, according to Kaspersky, represent a quantum jump for the hackers, who stole as much as $18 million in 2014. As *Forbes* noted in December, this is the same group that stole vast amounts of data from Staples, Sheplers, and Bebe, and is now considered to be “one of the most sophisticated cybercriminal groups ever seen.”

Anunak breached the banks’ security systems through very sophisticated phishing techniques that invited bank administrators, thinking they were receiving an innocuous e-mail or announcement from a trusted source, to click on it, allowing background malware not only to enter the computer programming of banks but to stay in the background until it learned all it needed to to manipulate its processes.

Here is one simplistic (and obvious) example of such a phishing attempt, from a phony bank called TrustedBank targeting (in this instance) bank customers:

> Dear valued customer of TrustedBank,
>
> We have received notice that you have recently attempted to withdraw the following amount from your checking account while in another country: $135.25.
>
> If this information is not correct, someone unknown may have access to your account. As a safety measure, please visit our website via the link below to verify your personal information:
>
> http://www.trustedbank.com/general/custverifyinfo.asp

> Once you have done this, our fraud department will work to resolve this discrepancy. We are happy you have chosen us to do business with.

That link, of course, would take the victim to another webpage designed to look official but phony as a three-dollar bill. Once opened, malware would worm its way back into the owner's computer to work its mischief.

In the case of banks, however, the attacks were vastly more complicated and insidious, allowing the hackers to obtain not only screen shots of administrators moving money around, but video of the actual administrators making those moves. After waiting patiently for up to four months, the hackers then would enter the secure system and create phony account withdrawals, substituting temporarily larger account balances and then transferring the phony overage to a hacker's account offshore.

This means that the hackers were able not only to learn their way around inside bank security systems, but also to manipulate international banking systems allowing such transfers to take place without notice. According to Kaspersky, the thefts would usually be less than $10 million, perhaps much less, to avoid or at least delay detection.

These attacks, which are ongoing, represent "the most sophisticated attack the world has seen to date in terms of the tactics and methods that [Anunak is] using to remain covert," said Chris Doggett, managing director of Kaspersky's Boston office.

Several oddities were noted in reviewing the report from Kaspersky and comments related to its revelations. It is estimated that more than 100 banks have been targeted, in about 30 countries, but none has come forward to confirm the attacks. Second, Kaspersky found 178 IP addresses linked to Russian banks on the servers belonging to the hackers, with another 37 linked to banks in the United States. Third, Eugene Kaspersky himself, the head of his international security software firm, lives in Moscow where his company has its headquarters.

A brief look at his background raises additional questions: a brilliant student, Kaspersky graduated at age 22 from the Mathematical Faculty of the Institute of Cyptography, Telecommunications and Computer Science, which just happens to be funded by the Russian Ministry of Defense and by the Russian KGB.

Within five years he began licensing his protective software programs worldwide, which he then developed into his own private company, Kaspersky Lab. A popular speaker, Kaspersky promotes "worldwide action" by governments to create a "non-proliferation" treaty to cover such cyberweapons as those developed by Anunak. Those governments would certainly benefit from knowing what private companies such as his have already learned:

> The private sector — particularly IT and security related industries, and also certain key critical industries for which IT security has long been at the top of the agenda — has a wealth of front line cyber-battle experience, which state bodies will greatly benefit from by having access to.

Once that "non-proliferation" treaty has been signed onto by governments across the globe, Kaspersky believes, they will then be positioned to decide just who will have access to what kind of data through the use of mandatory Internet identification requirements (a cyber ID card), in order to solve the problem that his company just happens to have uncovered. He said,

> I believe the World Wide Web should be divided into three zones. A red zone for critical processes; for operations in this zone an Internet ID should be mandatory.

> Then comes the yellow zone, where minimal authorization is needed; for example, age verification for online shops selling alcohol, or adult stores.
>
> And finally there's the green zone: blogs, social networks, news sites, chats … everything that's about your freedom of speech. No authorizations required.

But all of this is just too pat, too coincidental, for observers not to smell to an agenda behind it. Kaspersky and his Lab have been investigating for years, but it just now comes to light in time for the cyber-security conference in Mexico? And no one else suspected anything was wrong even though hundreds of millions and possibly a billion dollars are involved in this massive theft? Is the KGB-trained Kaspersky, whose cybersecurity company has made him wealthy and who has received a long list of national and international awards and honors for his work, really trying to protect other people's wealth from hacking? And why does his investigation reveal that most of the attacks are on Russian banks instead of U.S. banks, where the real money is?

Critics say it's all too pat not to suspect a rat.

A graduate of an Ivy League school and a former investment advisor, Bob is a regular contributor to The New American *magazine and blogs frequently at www.LightFromTheRight.com, primarily on economics and politics. He can be reached at badelmann@thenewamerican.com*