

Cyber attacks hit global banks for \$80 mn: study

June 26 2012



A wave of cyber attacks has likely stolen at least \$80 million from bank accounts in Europe, the United States and elsewhere, a security report said Tuesday.

A wave of cyber attacks has likely stolen at least \$80 million from bank accounts in Europe, the United States and elsewhere, a security report said Tuesday.

The joint report by Guardian [Analytics](#) and McAfee said "Operation High Roller" was led by criminals attacking cloud-based servers in a global fraud campaign.

The report from the two US firms said the attacks tried to steal between \$75 million and \$2.5 billion (60 million to two billion euros) from at least 60 banks worldwide.

The ring used "sophisticated" techniques including automation and targeted high-value accounts in Europe before moving to [Latin America](#) and the United States, it said.

"This is a serious new threat that is actively targeting American financial institutions," a statement from Guardian Analytics said.

"To the best of our knowledge the scheme has already netted nearly \$80 million worldwide, and it could be much higher."

The report offers insight into hacking into banks, which is often not disclosed by financial institutions.

"As this research study goes to press, we are working actively with international law enforcement organizations to shut down these attacks," the report said.

In the attacks uncovered earlier this year, the criminals "attempted transfers to mule business accounts as high as 100,000 euros," the report said.

"Where Europe has been the primary target for this and other [financial fraud](#) rings in the past, our research found the thefts spreading outside Europe, including the United States and Colombia."

In the [United States](#), "victims were all companies with commercial accounts with a minimum balance of several million dollars."

In most cases, the victims were found through online reconnaissance and "spear phishing," which uses a fake email to get an account holder's login details and password.

The first attacks affected "a popular bank in Italy and its consumer and

business accounts" and used SpyEye and Zeus malware to transfer funds to a "mule account" or pre-paid debit card where the thief could retrieve the funds quickly and anonymously.

But later attacks showed increased automation and sophistication, in some cases taking over the victim's account without an attacker's active participation. In some cases, the criminals were able to bypass smartcard readers which offer extra authentication used in many European banks.

"This ring adds many breakthroughs: bypasses for physical 'chip and pin' authentication, automated mule account databases, server-based fraudulent transactions," the report said.

It said the attacks hit "every class of financial institution: credit union, large global bank, and regional bank."

In some attacks, transactions were routed through a server in California, but the researchers said they "found evidence of the fraudster logging in from Moscow, Russia, to manipulate some of the transactions."

(c) 2012 AFP

Citation: Cyber attacks hit global banks for \$80 mn: study (2012, June 26) retrieved 26 April 2024 from <https://phys.org/news/2012-06-cyber-global-banks-mn.html>

<p>This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.</p>
--