US banks face 'credible' hacker threat, researchers say

December 13 2012

Dozens of US banks face a "credible" threat from hackers based in Eastern Europe who are planning large-scale attacks next year, a security firm said in a report released Thursday.

Dozens of US banks face a "credible" threat from hackers based in Eastern Europe who are planning large-scale attacks next year, a security firm said in a report released Thursday.

The report released by McAfee Labs supports the conclusions of researchers at another security firm, RSA, which first drew attention to the campaign expected to target 30 US financial institutions.

McAfee, owned by Intel, said the so-called Project Blitzkrieg "is a credible threat to the financial industry and appears to be moving forward as planned."

The hackers, who have been traced to servers hosted in Ukraine and led by an individual nicknamed vorVzakone, have already used the malware to steal at least $5 million since 2008, according to McAfee and RSA.

The McAfee report said it sees a real threat in early 2013 despite some speculation in the security community that the project had been dropped after being exposed.

"McAfee Labs believes that Project Blitzkrieg is a credible threat to the financial industry and appears to be moving forward as planned," McAfee researcher Ryan Sherstobitoff said in the report.

"Some recent reports argue that vorVzakone has called off this attack because it has been made public. Yet it is possible that the publicity may merely drive his activities deeper underground."

McAfee said the attack "combines both a technical, innovative back-end with the tactics of a successful, organized cybercrime movement."

An early pilot project "infected at a minimum 300 to 500 victims across the United States," according to McAfee.

Mor Ahuvia of the security firm RSA said in an October blog post that the series of Trojan attacks is set to be carried out by "100 botmasters" taking over control of infected computers.

Ahuvia said the attackers plan to use malware called "Gozi Prinimalka," which is a term derived from the Russian word meaning "to receive."

Earlier this year, several US banks appeared to be targeted by so-called denial of service attacks, which aim to bring down websites by flooding the networks with data requests.