Bank of America	USD 374,855.12 | US Dollar
USD 374,855.12 | US Dollar	EUR 334,569.44 | Euro
BL0401 - Commercial Banking	EL0201 - External Theft & Fraud
US - United States	North America
Loss Event	Published in media 16 May 2019

BoA suffers losses of USD 375,000 following cyberattack using GozNym malware

As of 16 May 2019, Bank of America (BoA) has suffered damages of at least USD 375,000 (EUR 335,000) as result of a cyberattack perpetrated by a criminal network responsible for infecting tens of thousands of computers worldwide with GozNym malware. The malware, often transmitted through malicious links in phishing emails, enabled the cybercriminals to steal customer online banking credentials and attempt to make fraudulent fund transfers.

On 16 May 2019, the US Department of Justice (DoJ) announced that it had dismantled the criminal network as part of an international law enforcement operation. The group attempted to steal around USD 100 million from victims in the US and around the world. Victims other than BoA included Brookline Bank and Comerica Bank which suffered losses of USD 41,000 and USD 28,000 respectively.

According to the BBC, GozNym malware is a hybrid of Nymaim software, which is designed to discreetly install malware on to a device, and Gozi, a Trojan which contains techniques aimed at stealing financial information. According to the indictment released by the DoJ, GozNym would capture victims confidential personal and financial information by keystroke logging and/or web injects, which are fake online banking pages displayed while the victim is browsing the web, in an effort to trick the victim into entering online banking information.

The DoJ said that the victims of the crimes were mainly US businesses and their financial institutions. Financial institutions in the US first noticed fraudulent activity in and around late 2015, according to the indictment. The indictment included examples of attacks on 13 victims from businesses such as an asphalt and paving business in Pennsylvania and a law firm in Washington, D.C. The network gained access to their online bank accounts held at institutions including BoA, Wells Fargo, and Comerica Bank.

With regards to BoA, the group succeeded in causing losses of USD 374,855.12 to the bank in three transactions. In the first example, a phishing email was sent to the firm on or around 16 February 2016, inviting the recipient to click a link to view an invoice. Clicking the link installed GozNym malware, and on 25

February 2016 the criminals accessed the bank account of the employee and attempted to transfer USD 97,520 from the victim's BoA account to an account controlled by the criminals. This resulted in a loss of USD 76,178.12.

In the second example, conspirators accessed the account of a distributor of neurosurgical and medical equipment, and succeeded in transferring USD 98,900 to a Santander Bank account controlled by a member of the group. In the third example, the conspirators gained access to the bank account of a provider of electrical safety devices, and transferred USD 199,777 to an account in Georgia.

In the other examples of specific attacks given in the indictment, the criminal network often gained access by sending emails concerning invoices with links that installed GozNym malware. After gaining access to online bank accounts, they made attempts to fraudulently transfer USD 3.2 million in 38 transactions.

On 16 May 2019, the US Attorney's Office for the Western District of Pennsylvania unsealed an indictment charging 10 members of the GozNym criminal network. They were charged with conspiracy to commit computer fraud, wire and bank fraud, and money laundering. The members of the group, along with an eleventh person who had already been charged, reside or resided in Russia, Georgia, Ukraine, Moldova and Bulgaria.

The DoJ noted that this criminal conspiracy exemplified the concept of "cybercrime as a service". The defendants advertised their specialised technical skills and services on underground, Russian-language online criminal forums, and the individuals then formed the GozNym network.

The law enforcement operation involved co-operation between the US, Georgia, Ukraine, Moldova, Germany, Bulgaria, Europol and Eurojust. Five of the named defendants remain in Russia as fugitives from justice, but co-operation from international authorities enabled the extradition of the remaining defendants to the US.

Author: Isha Pearce **Published Date:** 17 May 2019 **Last Update:** 21 May 2019

O.R.X | News

ORX News reference: 8602
ORX Standard: Banking

Published In Media	Occurrence - From	Occurrence - To	Discovery Date	Recognition / Settlement
16 May 2019			01 January 2015	

Boundary Risk Other Risk	**Industry Event**	**Scenario** SC0024 - Cyber-Related Fraud
Product PD0603 - Commercial Bank Accounts	**Process** PC1004 - IT Security	**Event Closed** No
ORX Member Yes	**Role of Firm** LS0307 - Position Taking (Principal)	**Jurisdiction / Choice of Law** LS0101 - United States of America
Cause 1 CS0102 - Assault by Criminals / Terrorists	**Cause 2**	**Cause 3**
Counterparty LS0212 - Not Identifiable	**Environmental Volatility** LS0406 - Not Identifiable	**Provision** No

Source(s)

https://www.justice.gov/opa/pr/goznym-cyber-criminal-network-operating-out-europe-targeting-american
https://www.justice.gov/opa/press-release/file/1163066/download
https://www.bbc.co.uk/news/technology-48294788

Related links