Banco de Chile Wiper Attack Just a Cover for $10M SWIFT Heist

The wiper malware affecting 9,000 workstations and 500 servers inside Chile's largest financial institution turns out to have been a distraction.

A cyberattack against Chile's largest financial institution last month, which reportedly destroyed 9,000 workstations and 500 servers, was actually cover for a larger plot to compromise endpoints handling transactions on the SWIFT network. When the dust settled on the attacks, investigators said $10 million was stolen from Banco de Chile and funneled off to an account in Hong Kong.

On Sunday, the bank's general manager Eduardo Ebensperger told Chilean media outlet Pulso that the late-May attack allowed adversaries to complete four separate fraudulent transactions on the SWIFT system before the heist was discovered.

"We found some strange transactions in the SWIFT system (where banks internationally remit their transactions to different countries)," Ebensperger told the outlet. "There we realized that the virus was not necessarily the underlying issue, but apparently [the attackers] wanted to defraud the bank."

The initial attack was carried out using a wiper malware that Ebensperger described as a "zero-day virus" that had never been seen in the wild. However, in report published Tuesday by Flashpoint, analysts discovered that the code is actually a modified version of the Buhtrap malware component known as kill_os. The module renders the local operating system and the Master Boot Record (MBR) unreadable by erasing them.

After reverse-engineering the codebase, Flashpoint analysts found that the Chile-attack malware, dubbed "MBR Killer," was identical with only minor modifications to Buhtrap's kill_os. For instance, the Buhtrap code, which was leaked onto the Dark Web in February, contains an almost identical Nullsoft Scriptable Install System (NSIS) script as the unpacked Banco de Chile malware (NSIS is an open-source system used to build Windows installers).

This revelation could potentially help with attribution: The Buhtrap malware and its components, including MBR Killer, were previously used by a Russian-speaking hacker collective in attacks against multiple financial institutions in Russia and the Ukraine, Flashpoint noted.

However, the attribution behind the Banco de Chile attack remains uncertain.

"It is notable, however, that Chilean financial institutions were targeted entities by the Lazarus Group, which was linked to North Korea, during the compromise of the Polish Financial Supervision Authority website in 2017," Vitali Kremez, director of research, told Threatpost in an interview. "More specifically, the breached website was filtered to serve payloads to only targeted IP ranges associated with financial institutions of interest to the group."

He added, "the above-referenced indicators point to two possible groups behind – purported North-Korean affiliated group Lazarus and the known Russian-speaking sophisticated criminal group Buhtrap."

It's also possible, researchers said, that it's an entirely different copycat group making use of Buhtrap's leaked source code.

Meanwhile, Ebensperger said that a forensic analysis conducted by Microsoft attributed the attack to either Eastern European or Asian groups. Further, Ofer Israeli, CEO of Illusive Networks, said via email that he too believes the North Korea-linked Lazarus Group, which is thought to have carried out the SWIFT attacks in Bangladesh in 2016, is behind it all.

"Targeting financial organizations is part of their long-term strategy and compromising global financial networks via small to medium-sized banks in Central and South America whose cyber-defenses may be less sophisticated poses a higher probability of success," he explained.

In any event, Banco de Chile is the latest victim in a string of cyber-attacks targeting payment transfer systems. For instance, in May, Somewhere between $18 million to $20 million went missing during unauthorized interbank money transfers in Mexico's central banking system.

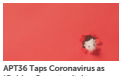
"Third-party providers of payment and transfer systems have become one of the most effective attack vectors for hackers trying to siphon money from banks," said Fred Kneip, CEO at CyberGRX, via email. "We've seen the SWIFT Network under attack for years now, and just last month hackers targeted the Mexican central bank SPEI interbank transfer system."

He added, "A large international bank has tens of thousands of third parties in their digital ecosystem, but hackers have figured out that it only takes one weak link to make millions of dollars. Understanding the level of risk exposure introduced by all third parties is important, but that becomes even more critical for a Tier 1 partner like a transfer system provider."

Share this article:

Hacks | Malware

SUGGESTED ARTICLES



APT36 Taps Coronavirus as 'Golden Opportunity' to Spread Crimson RAT

The Pakistani-linked APT has been spotted infecting victims with data exfiltration malware.

March 17, 2020

Activities of a Nigerian Cybercriminal Uncovered

Rise and fall of a Nigerian cybercriminal called 'Dton,' who made hundreds of thousands of dollars in a 7-year campaign, outlined in new report.

March 27, 2020

Coronavirus-Themed APT Attack Spreads Malware

The APT group was spotted sending spear-phishing emails that purport to detail information about coronavirus – but they actually infect victims with a custom RAT.

March 13, 2020

DISCUSSION

Ambarish on August 4, 2018

SWIFT is sleeping and has to come out of the illusion that they are secured. It's a fact now and bankers across the globe should realize sooner then later

INFOSEC INSIDER

A Practical Guide to Zero-Trust Security
January 13, 2020 2

7 Tips for Maximizing Your SOC
December 31, 2019 5

Mean Time to Hardening: The Next-Gen Security Metric
December 30, 2019 4

Combining AI and Playbooks to Predict Cyberattacks
December 26, 2019 1

The Case for Cyber-Risk Prospectuses
December 24, 2019