Chasing Lazarus: A Hunt for the Infamous Hackers to Prevent Large Bank Robberies

By Kaspersky

Published: 2017-04-05 · Archived: 2026-04-02 12:02:26 UTC

Kaspersky Lab has published the results of its more-than-year-long investigation into the activity of Lazarus – a notorious hacking group allegedly responsible for the theft of 81 million dollars from the Central Bank of Bangladesh in 2016.

Kaspersky Lab has published the results of its more-than-year-long investigation into the activity of Lazarus – a notorious hacking group allegedly responsible for the theft of 81 million dollars from the Central Bank of Bangladesh in 2016. During the forensic analysis of artefacts left by the group in South-East Asian and European banks, Kaspersky Lab has reached a deep understanding of what malicious tools the group uses and how it operates while attacking financial institutions, casinos, software developers for investment companies and crypto-currency businesses around the world. This knowledge has helped to interrupt at least two other operations which had one goal - to steal a large amount of money from financial institutions.

In February 2016, a group of hackers (unidentified at that time) attempted to steal $851 million USD, and managed to transfer 81 million USD from the Central Bank of Bangladesh. This is considered to be one of the largest, most successful cyber heists ever. Further investigation conducted by researchers from different IT security companies including Kaspersky Lab revealed a high chance that the attacks were conducted by Lazarus – a notorious cyber espionage and sabotage group responsible for a series of regular and devastating attacks, and known for attacking manufacturing companies, media and financial institutions in at least 18 countries around the world since 2009.

Although several months of silence followed the Bangladesh attack, the Lazarus group was still active. They had been preparing for a new operation to steal money from other banks and, by the time they were ready, they already had their foot in a financial institution in South East Asia. After being interrupted by Kaspersky Lab products and the following investigation, they were set back for another few months, and later decided to change their operation by moving to Europe. But here too, their attempts were interrupted by Kaspersky Lab's security software detections, as well as the quick incident response, forensic analysis, and reverse engineering with support from company's top researchers.

Lazarus Formula

Based on the results of the forensic analysis of these attacks, Kaspersky Lab researchers were able to reconstruct the modus operandi of the group.

- **Initial compromise:** A single system inside a bank is breached either with remotely accessible vulnerable code (i.e. on a webserver) or through a watering hole attack through an exploit planted on a benign website.

Once such a site is visited, the victim's (bank employee) computer gets malware, which brings additional components.

- **Foothold established:** Then the group migrates to other bank hosts and deploys persistent backdoors – the malware allows them to come and go whenever they want.
- **Internal reconnaissance:** Subsequently the group spends days and weeks learning the network, and identifying valuable resources. One such resource may be a backup server, where authentication information is stored, a mail server or the whole domain controller with keys to every "door" in the company, as well as servers storing or processing records of financial transactions.
- **Deliver and steal:** Finally, they deploy special malware capable of bypassing the internal security features of financial software and issuing rogue transactions on behalf of the bank.

Geography and Attribution

The attacks investigated by Kaspersky Lab researchers lasted for weeks. However, the attackers could operate under the radar for months. For example, during the analysis of the incident in South-East Asia, experts discovered that hackers were able to compromise the bank network no less than seven months prior to the day when the bank's security team requested incident response. In fact, the group had access to the network of that bank even before the day of the Bangladesh incident.

According to Kaspersky Lab records, from December 2015, malware samples relating to Lazarus group activity appeared in financial institutions, casinos software developers for investment companies and crypto-currency businesses in Korea, Bangladesh, India, Vietnam, Indonesia, Costa Rica, Malaysia, Poland, Iraq, Ethiopia, Kenya, Nigeria, Uruguay, Gabon, Thailand and several other countries. The latest samples known to Kaspersky Lab were detected in March 2017, showing that attackers have no intention of stopping.

Even though attackers were careful enough to wipe their traces, at least one server they breached for another campaign contained a serious mistake with an important artefact being left behind. In preparation for operation, the server was configured as the command & control center for the malware. The first connections made on the day of configuration were coming from a few VPN/proxy servers indicating a testing period for the C&C server. However, there was one short connection on that day which was coming from a very rare IP address range in North Korea.

According to researchers, that could mean several things:

- The attackers connected from that IP address in North Korea
- It was someone else's carefully planned false flag operation
- Someone in North Korea accidentally visited the command and control URL

The Lazarus group heavily invests in new variants of their malware. For months they were trying to create a malicious toolset which would be invisible to security solutions, but every time they did this, Kaspersky Lab's specialists managed to identify unique features in how they create their code, allowing Kaspersky Lab to keep tracking the new samples. Now, the attackers have gone relatively quiet, which probably means that they have paused to rework their arsenal.

"*We're sure they'll come back soon. In all, attacks like the ones conducted by Lazarus group show that a minor misconfiguration may result in a major security breach, which can potentially cost a targeted business hundreds of millions of dollars in loss. We hope that chief executives from banks, casinos and investment companies around the world will become wary of the name Lazarus,*" said Vitaly Kamluk, Head of Global Research and Analysis Team APAC at Kaspersky Lab.

Kaspersky Lab products successfully detect and block the malware used by the Lazarus threat actor with the following specific detection names:

- HEUR:Trojan-Banker.Win32.Alreay*,
- Trojan-Banker.Win32.Agent*

The company is also releasing crucial Indicators of Compromise (IOC) and other data to help organizations search for traces of these attack groups in their corporate networks. For more information go to Securelist.com

We urge all organizations to carefully scan their networks for the presence of Lazarus malware samples and, if detected, to disinfect their systems and report the intrusion to law enforcement and incident response teams.

To learn more about financial attacks by Lazarus group, read the blog post available at Securelist.com or watch the video.