'Silence' hackers hit banks in Bangladesh, India, Sri Lanka, and Kyrgyzstan

By Written by Catalin Cimpanu, ContributorContributor July 3, 2019 at 4:17 a.m. PT

Group-IB

See als

-

A group of hackers specialized in attacking banks has hit again, and this time they've breached four targets in Asia, respectively in Bangladesh, India, Sri Lanka, and Kyrgyzstan, security researchers from Group-IB have told *ZDNet*.

The only incident that is currently public is one impacting Dutch Bangla Bank Limited, a bank in Bangladesh, which lost more than $3 million during several rounds of ATM cashout attack that took place during the month of May, according to local media reports [1, 2].

Silence group expands beyond Europe

In a report shared with *ZDNet* prior to publication, Group-IB tied the Dutch Bangla Bank incident to a group of hackers known as "Silence."

The group, which *ZDNet* previously covered in a September 2018 piece, has been active since 2016 and has historically targeted banks in Russia, former Soviet states, and Eastern Europe.

According to Rustam Mirkasymov, Head of Dynamic Analysis of Malicious Code at Group-IB, this is the first time the group has ventured into Asia.

Dutch Bangla Bank hack tied to Silence infrastructure

Mirkasymov told *ZDNet* that Group-IB has been able to tie the Dutch Bangla Bank hack to Silence's server infrastructure.

"Group-IB has the ability to actively track cybercriminals' infrastructure of this and other financially motivated cybercriminal groups," he told *ZDNet* in an email. "This all gives us visibility to indefinitely confirm that an infected machine inside the bank's network was communicating with Silence' infrastructure."

"In this case, we discovered that Dutch Bangla Bank's hosts with external IPs 103.11.138.47 and 103.11.138.198 were communicating with Silence's C&C (185.20.187.89) since at least February 2019," Mirkasymov told *ZDNet* in an email.

According to the researcher, the group appears to have deployed the eponymously named Silence malware on the bank's network, with modules for running malicious commands on infected hosts and setting up proxy servers to disguise malicious traffic.

The group appears to have used this access to orchestrate coordinated funds withdrawals from the bank's ATMs.

How these attacks occurred is currently unknown. A YouTube video unearthed by local media shows two men (later identified as Ukrainians) visiting Dutch Bangla Bank ATMs, making a phone call, and then withdrawing large sums of money. ATM cashouts using Dutch Bangla Bank ATMs occurred on May 31, but before that, crooks also used cloned cards with the data of Dutch Bangla Bank customers to withdraw money from ATMs in Cyprus, Russia and Ukraine.

This suggests the Silence group might have used their access to the bank's network to facilitate and allow large ATM cashouts without triggering alerts, most likely by deploying their custom-built Atmosphere malware on systems that ran ATM-specific software.

Two other Bangladesh banks also hit

Bangladesh local media reported that two other local banks -- NCC Bank and Prime Bank -- also faced similar issues as Dutch Bangla Bank, but they managed to avert financial losses. It is unclear if Silence was involved in those attacks as well.

Group-IB said Silence did hit banks in three other countries -- India, Sri Lanka, and Kyrgyzstan -- but could not disclose their names.

In September 2018, Group-IB said the group had only been successful in attacks against CIS and Eastern European countries, but that they were sending spear-phishing emails to banks all over the world.

Today's report shows the group was eventually successful in compromising other targets outside their normal operational zone.

According to the Group-IB report on the Silence hacker group from September 2018, the group is a small two-person operation, with one member being suspected of being part of the cyber-security industry.

However, Mirkasymov told *ZDNet* that "it is possible that the gang's structure might have changed" since the report's release. Mirkasymov said his company has recently found out that one of the Silence developers had wrote the "FlawedAmmyy loader" malware as a third-party developer for other cyber-criminal operations.

This article will be updated later today with a link to the Group-IB report, once it becomes publicly available.

The FBI's most wanted cybercriminals

Related malware and cybercrime coverage:

- US Cyber Command issues alert about hackers exploiting Outlook vulnerability
- New Dridex malware strain avoids antivirus software detection
- New Silex malware is bricking IoT devices, has scary plans
- Florida city fires IT employee after paying ransom demand last week
- Facebook abused to spread Remote Access Trojans since 2014
- Ten years later, malware authors are still abusing 'Heaven's Gate' technique
- More than 3B fake emails sent daily as phishing attacks persist **TechRepublic**
- Game of Thrones has the most malware of any pirated TV show **CNET**
