DUTCH-BANGLA BANK COMPROMISED BY THE NOTORIOUS SILENCE GANG

Bangladesh Cyber Heist 2.0: Silence APT goes global

Singapore, 03.07.2019 – Group-IB, an international company that specializes in preventing cyber attacks, has established that Silence, a Russian-speaking cybercriminal group is likely to be behind the brazen attack on Dutch-Bangla Bank's ATMsresulting in the theft of $3 million, the amount reported by the local media. The actual amount of money stolen could be much higher. This is one of Silence's most recent international attacks which, indicates that the gang has expanded its geography and has gone global, focusing now on APAC markets.

Thefinal stage of the brashcyber attack, which started months earlier, took place in Dhaka on May 31, 2019, according to the local media reports. In CCTV footage posted by local newspapers two Ukrainian mules with their faces covered are seen withdrawing money from Dutch-Bangla Bank's ATMs. They made phone calls every time before withdrawing money, which immediately prompted Group-IB's Threat intelligenceteam's interest and indicated that this could likely beinvolvement of an organized financially-motivated cybercriminal group rather than simple skimming attack. At the time, Group-IB Threat Intelligence team was already aware that Silence had been carrying out operations in Asia.

Group-IB has been tracking Silence and their infrastructure since 2016 and published a report "Silence: Moving into the darkside" in September 2018 which was the first to describe the group's tactics and tools in detail. The information gathered by Group-IB's Threat Intelligence team and comprehensive knowledge about Silence's infrastructure suggested that Dutch-Bangla Bank's hosts with external IPs 103.11.138.47 and 103.11.138.198 had been communicating with Silence's C&C (185.20.187.89) since at least February 2019. During the attack on Dutch-Bangla Bank, the cybercriminals likely used the following Trojans - Silence. Downloader (aka TrueBot), Silence.MainModule (MD5 fd133e977471a76de8a22ccb0d9815b2) which allows to execute remote commands covertly and download files from the compromised server, and Silence.ProxyBot (MD5 2fe01a04d6beef14555b2cf9a717615c), which executes the tasks of the proxy server and allows the attacker to redirect traffic from a hidden node to a backconnect server via compromised PC.

Once they gained access to the bank's infrastructure, Silence went on to the next stage of the attack – money withdrawal. One of the instances was shown on the CCTV from May 31 published by the local media. Based on the TTPs used by Silence, the money could have been stolen in one of two ways: the hackers could have either compromised the bank's card processing system or used the custom Atmosphere software,a set of tools for ATMs jackpotting. The detailed description of Silence's toolset is available in Group-IB's report "Silence: Moving into the darkside". "What we see now is that Silence is continuing to shift their focus from the CIS and neighbouring countries to international markets," comments Rustam Mirkasymov, Head of Dynamic Analysis of Malicious Code at Group-IB. "Having tested their tools and techniques in Russia,Silence has gained the confidence and skill necessary to be aninternationalthreat to banks and corporations. Asia particularly draws cybercriminals' attention. Dutch-Bangla Bank is not the first Silence's victim in the region. In total, we are aware of at least 4targets Silence has attacked in Asia recently."

About Silence
Silence is an active though very small group of Russian-speaking hackers. Group-IB first detected the group's activity in 2016. Over the course of their 'work', Silence attacked bank management systems, card processing systems, and the Russian interbank transfers system (AWS CBR). The gang's targets are mainly located in Russia, Ukraine, Belarus, Azerbaijan, Poland, and Kazakhstan, although phishing emails were sent to bank employees in Central and Western Europe, Africa, and Asia. Recently, Group-IB has detected Silence shifting their focus from the CIS and neighbouring countries to international markets. The report "Silence: Moving into the darkside" was published in September 2018 and was the first to describe the group's tactics and tools.

About Group-IB
Group-IB is a leading provider of solutions aimed at detection and prevention of cyberattacks, online fraud, and IP protection. Group-IB's Threat Intelligence system has been named one of the best in class by Gartner, Forrester, and IDC. Group-IB's technological leadership is built on the company's sixteen years of hands-on experience in cybercrime investigations around the world and 55 000 hours of cyber security incident response accumulated in the largest forensic laboratory in Eastern Europe and a round-the-clock center providing a rapid response to cyber incidents—CERT-GIB. Group-IB is a partner of INTERPOL, Europol, and has been recommended by the OSCE as a cybersecurity solutions provider. Group-IB is a member of the World Economic Forum.

In Bangladesh Group-IB is working with Dhaka Distributions to protect local customers against most advanced cybercriminal groups. Dhaka Distributions current and potential customers have opportunity to enhance their cybersecurity capabilities with Group-IB's Threat Detection System for adversary-centric detection and proactive threat hunting, powered by Group-IB Threat Intelligence which is a unique source of tailored, actionable and reliable data on threat actors and major types of malware used by cybercriminals.

For more information, please contact:

Nika Komarova
Head of Corporate Communications
komarova@group-ib.com

Sergei Turner
Communications Manager
turner@group-ib.com

+65 31593798
pr@group-ib.com
https://www.group-ib.com
https://www.group-ib.com/blog
Twitter | LinkedIn

DHAKA DISTRIBUTIONS IS THE ALLIANCE PARTNER FOR GROUP-IB IN BANGLADESH.