Group-IB's new report on Silence: Damage from Silence APT operations increases fivefold

Archived: 2026-05-01 02:31:31 UTC

Group-IB, a Singapore-based cybersecurity company that specializes in preventing cyberattacks, has exposed the most recent campaigns carried out by Silence, a Russian-speaking APT group, in the new "Silence 2.0: Going Global" report. Group-IB experts discovered that Silence have significantly expanded their geography and increased the frequency of their attacks. Additionally, the total confirmed amount of funds stolen by Silence has increased fivefold since the publication of Group-IB's original report, and is now estimated at USD 4.2 million. Group-IB's Threat Intelligence team has also revealed a link between Silence and TA505 group and identified that Silence has made a number of changes to its TTPs and enhanced its arsenal, as a result of being in the spotlight of security researchers for some time now. Given that the gang represents a growing threat, both of Group-IB's reports on Silence ("Silence: Moving into the darkside" and its sequel, "Silence 2.0: Going Global") have been made publicly available to help cybersecurity specialists with proper attribution and prevention of new incidents. Group-IB has limited some of the data in the reports that could hinder investigations into the group's cybercrimes.

Silence going global. Larger geographical scope of attacks

Prior to April 2018, Silence's target interests were primarily limited to 25 post-Soviet states and neighboring countries. Since the report "Silence: Moving into the darkside" was released in September 2018, Group-IB's Threat Intelligence team has detected at least 16 new campaigns targeting banks launched by Silence. In 2019 alone, Silence has infected workstations in more than 30 countries across Europe, Latin America, Africa, and Asia. Since Group-IB's original report was published, the total confirmed damage has increased more than fivefold, from just USD 800,000 to USD 4.2 million. In July, Group-IB experts reported that Silence was likely to be the perpetrator behind the brazen attack on Dutch-Bangla Bank, when money mules supposedly connected to Silence were caught on CCTV footage withdrawing money from the bank's ATMs. Other recent successful attacks attributed to Silence and known to Group-IB's specialists, were detected in India (August 2018), Russia (February 2019, Russian "IT Bank"), Kyrgyzstan (May 2019), Russia (June 2019), Chile, Ghana, Costa Rica, and Bulgaria (July 2019). The cybercriminals are particularly drawn to Asia, which is where Silence conducted one of their biggest reconnaissance campaigns to date.

Within the sound of Silence. New tools and techniques uncovered

The emails you never sent

Like most APTs, Silence uses phishing emails to infect their victims. In October 2018, however, Silence implemented new tactics: the gang began sending out reconnaissance emails as part of a preparatory stage for their attacks. Silence's "recon" looks like a "mail delivery failed" message that usually contains a link without a malicious payload. Such "recon" emails allow cybercriminals to obtain a list of valid emails for future attacks and get information about the cybersecurity solutions used by a targeted company all the while remaining undetected.

Group-IB's Threat Intelligence team identified at least three major reconnaissance campaigns. These campaigns spread across Asia, Europe and post-Soviet countries with more than 170,000 "recon" emails sent. The biggest campaign focused on Asia: since November 2018, Silence sent out close to 80,000 emails to organizations in Taiwan, Malaysia, South Korea, the UAE, Indonesia, Pakistan, Jordan, Saudi Arabia, Singapore, Vietnam, Hong Kong, and China. Another large-scale campaign, which began in October 2018, was carried out in Russia and the post-Soviet states. Silence's European "recon" campaign was the smallest: in October 2018, the group sent out less than 10,000 reconnaissance emails to UK-based financial organizations.

New tools in the gang's arsenal

Silence's global expansion attracted the attention of cybersecurity researchers leading the cybercriminals to grow more cautious and introduce changes to their toolset to complicate detection. Notably, at the initial infection stage, in addition to their infamous primary loader Silence.Downloader (aka TrueBot), the cybercriminals started using Ivoke, a fileless loader, written in PowerShell. Ivoke was detected by Group-IB's Threat Intelligence team in May 2019, when Silence sent out phishing emails purporting to be from a bank's client with a request to block a card. Interestingly, Silence started using fileless tools much later than other APTs. This supports the initial hypothesis that Silence have spent their time "catching up": first studying the approaches of other groups, and then customizing them to their needs.

Another new tool in Silence's arsenal is a previously unknown PowerShell agent based on Empire and dnscat2 projects, dubbed EmpireDNSAgent or simply EDA by Group-IB's Threat Intelligence team. The Trojan is used during the lateral movement stage and is designed to control compromised systems by performing tasks through the command shell and tunneling traffic using the DNS protocol. This program was first discovered in March 2019 by Group-IB and was detected during Silence's most recent attacks on banks in Chile, Bulgaria, Costa Rica and Ghana. In addition to its custom Atmosphere Trojan, designed to remotely control ATMs, Silence started using xfs-disp.exe which is also a Trojan deployed during the attack execution stage. The Trojan was allegedly used in the attack on the Russian IT Bank in February 2019.

Silence has also changed their encryption alphabets, string encryption, and commands for the bot and the main module. Moreover, the actor has completely rewritten TrueBot loader, the first-stage module, on which the success of the group's entire attack depends. Due to ongoing investigations, the new report features the detailed analysis of two of Silence's recent attacks, as well as descriptions of their TTPs.

Alleged connection between Silence and TA505

Group-IB researchers believe that there might also be a connection between Silence and TA505, another presumably Russian-speaking threat actor first named by researchers from Proofpoint. According to media reports, TA505 recent attacks were targeting individuals working at financial organizations in the US, the United Arab Emirates, and in Singapore. FlawedAmmyy, a sophisticated RAT that provides full access to infected machines, is reported to have been used in these TA505 attacks. A comparative analysis of Silence.Downloader and FlawedAmmyy.Downloader revealed that these programs were developed by the same person a Russian speaker who is active on underground forums. That said, the infrastructure used for the FlawedAmmyy attacks differs greatly from Silence's attacks, most likely means that the attacks are not connected.

Three years ago, when we started tracking Silence, its members were young and highly motivated hackers taking their first tentative steps in cybercrime by attacking banks and financial organizations in the post-Soviet states and neighboring countries. Early on, Silence showed signs of immaturity in its TTPs by making mistakes and copying practices from other groups. Since then, Silence have evolved into one of the most sophisticated threat actors targeting the financial sector not only in Russia, but also in Latin America, Europe, Africa, and especially Asia. Since our original report was released, the confirmed damage from their operations has grown significantly, while the geography of Silence's attacks expanded, and some of their tools and techniques have changed. The growing threat posed by Silence and their rapid global expansion, prompted us to make both reports publicly available for the very first time in order to help cybersecurity specialists with proper attribution and detection of Silence's attacks at early stages all over the world.

Rustam Mirkasymov

Group-IB Head of Dynamic Analysis of malware department and threat intelligence expert

About Group-IB

Established in 2003, Group-IB is a leading creator of predictive cybersecurity technologies to investigate, prevent, and fight digital crime globally. Headquartered in Singapore, and with Digital Crime Resistance Centers in the Americas, Europe, Middle East and Africa, Central Asia, and the Asia-Pacific, Group-IB delivers predictive, intelligence-driven defense by analysing and neutralizing regional and country-specific cyber threats via its Unified Risk Platform, offering unparalleled defense through its industry-leading Cyber Fraud Intelligence Platform, Cloud Security Posture Management, Threat Intelligence, Fraud Protection, Digital Risk Protection, Managed Extended Detection and Response (XDR), Business Email Protection, and External Attack Surface Management solutions, catering to government, retail, healthcare, gaming, financial sectors, and beyond. Group-IB collaborates with international law enforcement agencies like INTERPOL, Europol, and AFRIPOL to fortify cybersecurity worldwide, and has been awarded by advisory agencies including Datos Insights, Gartner, Forrester, Frost & Sullivan, and KuppingerCole.

For more information, visit us at www.group-ib.com or connect with us on LinkedIn, X, Facebook, and Instagram.

Discover our podcasts to hear from leading voices on Masked Actors and Fraud Intel, where top cybersecurity experts share real-world experiences, emerging trends, and practical insights to help you stay one step ahead in the fight against cyber crime.
