Silence: Moving into the Darkside

By Dmitry Volkov, CEO at Group-IB

Archived: 2026-05-01 02:10:03 UTC

Group-IB has exposed the attacks committed by Silence cybercriminal group. While the gang had previously targeted Russian banks, Group-IB experts also have discovered evidence of the group's activity in more than 25 countries worldwide. Group-IB has published its first detailed report on tactics and tools employed by Silence. Group-IB security analysts' hypothesis is that at least one of the gang members appears to be a former or current employee of a cyber security company. The confirmed damage from Silence activity is estimated at 800 000 USD.

Download full version of the report Silence: Moving into the Darkside

In August 2017, the National Bank of Ukraine warned state-owned and private banks across the country about a large-scale phishing attack. The threat actor used an exploit from the arsenal of the state-sponsored hacker group APT28. However, the tool, as Group-IB discovered, was modified to target banks. It also appeared that the authors of the phishing emails had in-depth knowledge of reverse engineering.

At the time, the National Bank of Ukraine linked the attack with a new wave of NotPetya ransomware outbreak, but these were not pro-government hackers. Initial impressions would indicate that the targeted attack was on par with the works of Cobalt or MoneyTaker. This hypothesis went unproven. On investigation, the adversaries were a young and active hacker group, who, like young smart technical specialists, learned very fast and from their own mistakes.

The new threat actor group was eventually named **Silence**. They were identified and named first in reports by Anti-Virus vendors, however, until the publication of this report, no detailed technical analysis of Silence or their operations has been conducted.

Silence is a group of Russian-speaking hackers, based on their commands language, the location of infrastructure they used, and the geography of their targets (Russia, Ukraine, Belarus, Azerbaijan, Poland, and Kazakhstan). Although phishing emails were also sent to bank employees in Central and Western Europe, Africa, and Asia). Furthermore, Silence used Russian words typed on an English keyboard layout for the commands of the employed backdoor. The hackers also used Russian-language web hosting services.

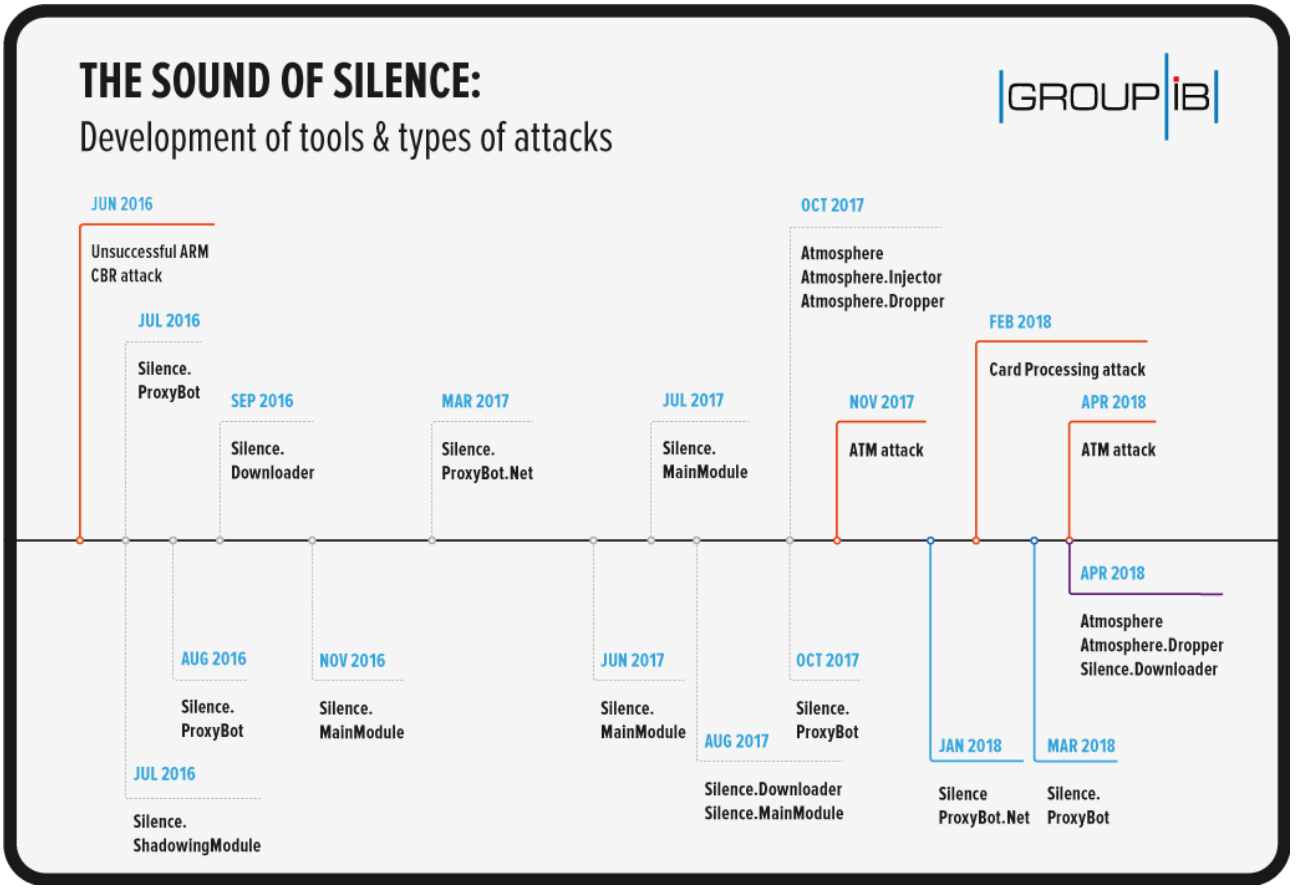
Financially motivated APT groups which focus efforts on targeted attacks on the financial sector such as — Anunak, Corkow, Buhtrap — usually managed botnets using developed or modified banking Trojans. **Silence is**

different. Even at the beginning of their journey, in the summer of 2016, Silence was not able to hack banking systems and actually seemed to learn on the job by carefully analyzing the experiences, tactics and the tools of other groups. They tried new techniques to steal from banking systems, including AWS CBR (the Russian Central Bank's Automated Workstation Client), ATMs, and card processing.

From circumstancial analysis over two years of attacks, it appears that Silence group members have worked or are currently working in legitimate information security activities. The group has access to non-public malware samples, patched Trojans available only to security experts and also TTP changes suggest that they modify their activity to mimic new attacks and red teaming activity.

Group-IB researchers were tracking Silence throughout this period and conducting response following incidents in the financial sector. During this monitoring period a phishing email was sent to CERT-GIB (Computer Emegency Response Team of Group-IB). This was analysed and confirmed to be from Silence. Challenge accepted, Group-IB engaged.

This report details the results of our investigation, review of attacks and thefts by Silence, analysis of their tools, tactics and procedures used to target financial institutions. This report serves as a contribution to the Whitehat Security community from Group-IB and provides technical descriptions of the methods and technologies that can be used to detect and track this group. We have also included a detailed analysis of the toolset created by Silence and associated Indicators of Compromise (IoC), YARA and IDS rules.



Silence is a new threat to banks

Group-IB detected the first incidents relating to Silence in June 2016. At that time, the cyber criminals were just beginning to test their capabilities. One of Silence's first targets was a Russian bank, when they tried to attack AWS CBR. After this, the hackers "took a moment of silence". It was later discovered that this is standard practice for Silence. They are selective in their attacks and wait for about three months between incidents, which is approximately three times longer than other financially motivated APT groups, like MoneyTaker, Anunak (Carbanak), Buhtrap or Cobalt.

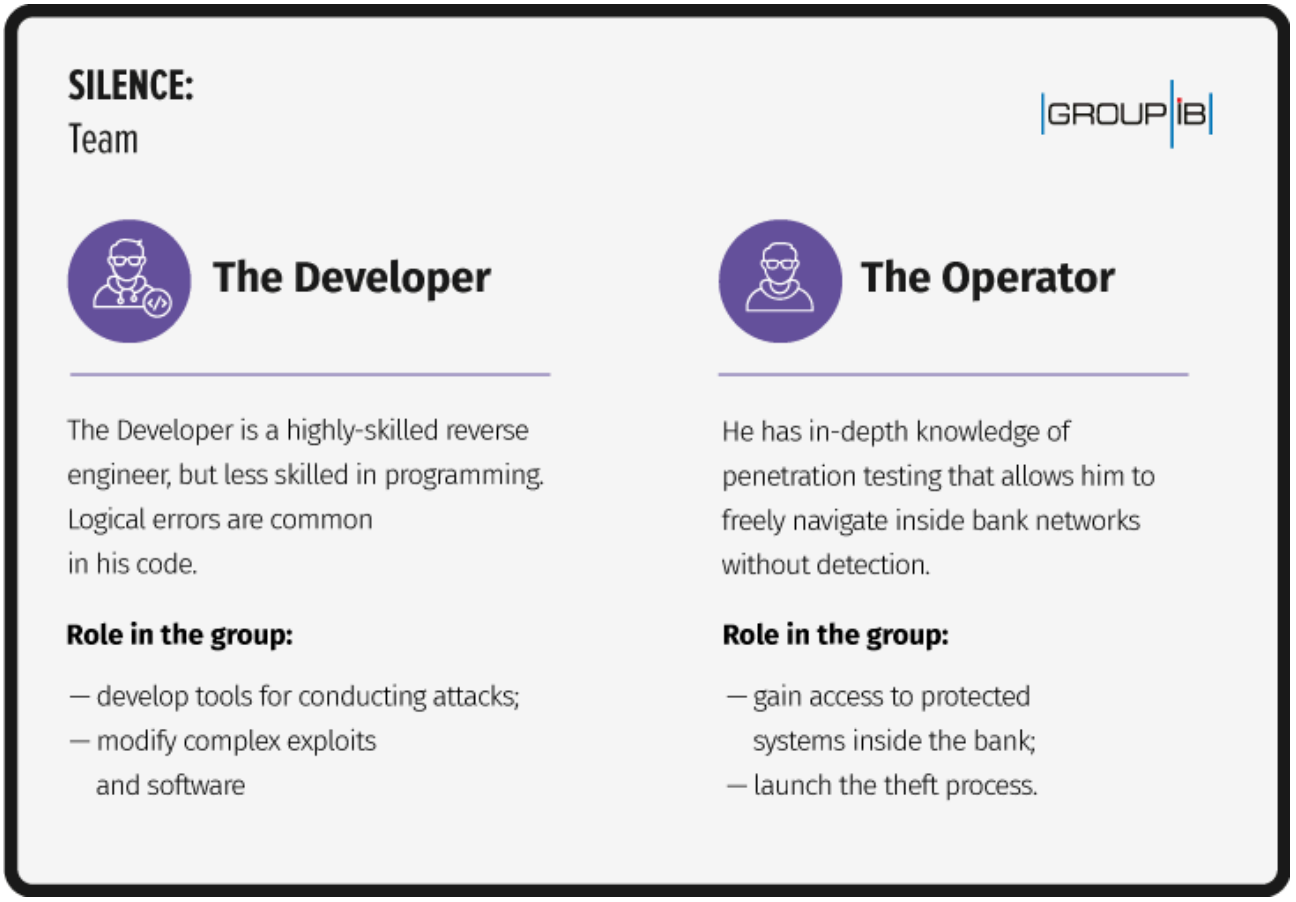
The reason for this is that Silence is a small group. In years of cyber intelligence and investigations, it is the first time that Group-IB has encountered this kind of structure and role-based group. Silence members constantly analyze the experience of other criminal groups. They try to apply new techniques and ways of stealing from various banking systems, including AWS CBR, ATMs, and card processing. In a short period of time they studied not only direct types of hacking, but also supply-chain attacks. In less than a year, the amount of funds stolen by Silence has increased five times.

Team

Our hypothesis is that the Silence team has two clear roles: the Operator and the Developer. Presumably, the Operator is the group leader. He acts like a penetration tester, who has in-depth knowledge of the tools for conducting penetration testing on banking systems. This knowledge allows the group to navigate easily inside the bank. It is the Operator who gains access to protected systems inside the bank and then conducts the theft.

The Developer is a qualified reverse engineer. His advanced reverse-engineering skills do not prevent him from making mistakes while programming. He is responsible for developing tools for conducting attacks and is also able to modify complex exploits and third party software. That said, he patched a little known Trojan that had not previously been employed by other groups. In addition, the Developer has sufficient knowledge of ATM processes, systems and has access to non-public malware samples, which are usually only available to security companies.

A distinctive feature of Silence is their untypical role structure and small size. It appears, this Russian-speaking group includes only two members.



Language

As with most financially-motivated APT groups, the members of Silence are Russian speakers, which is evidenced by the language of commands, priorities in locating leased infrastructure, the choice of Russian-speaking hosting providers and location of the targets.

- The commands of Silence's Trojan are Russian words typed using an English layout:
  htrjyytrn > реконнект (reconnect) htcnfhn > рестарт (restart) ytnpflfybq > нетзадач (notasks)
- The main targets are located in Russia, although phishing emails were sent to bank employees in more than 25 countries of Central and Western Europe, Africa and Asia.
- To rent servers, Silence uses Russian-speaking hosting providers.

Silence, in many ways, is changing the perception of cybercrime in terms of the nature of the attacks, the tools, tactics, and even the members of the group. It is obvious that the criminals responsible for these crimes were at some point active in the security community. Either as penetration testers or reverse engineers. They carefully study the attacks conducted by other cybercriminal groups, and analyse antivirus and Threat Intelligence reports. However, it does not save them from making mistakes; they learn as they go. Many of Silence's tools are legitimate, others they developed themselves and learn from other gangs. After having studied Silence's attacks, we concluded that they are most likely white hats evolving into black hats. The Internet, particularly the underground web, favours this kind of transformation; it is now far easier to become a cybercriminal than 5–7

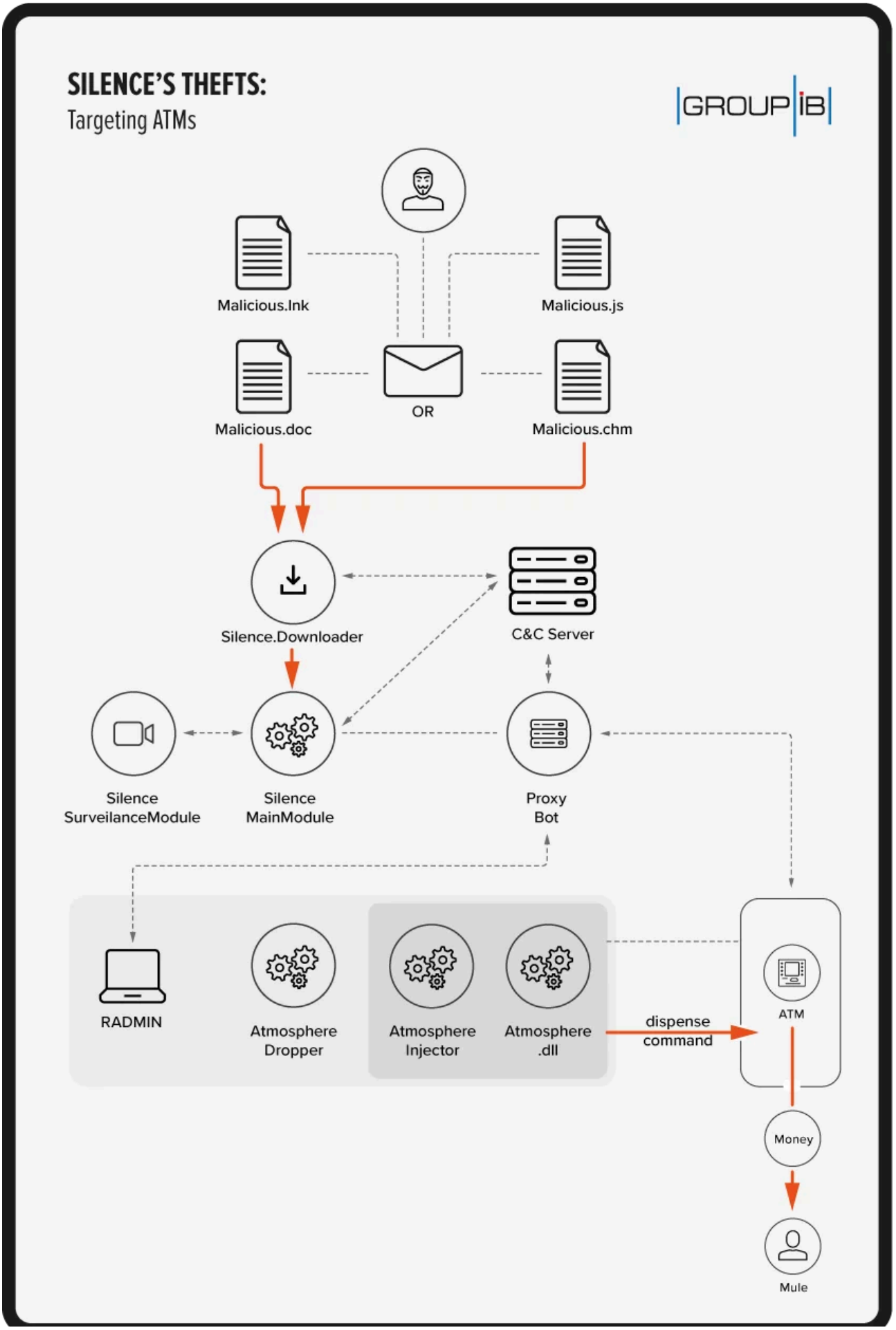
years ago—you can rent servers, modify existing exploits, and use legal tools. It makes things more complicated for blue teams and much easier for hackers.

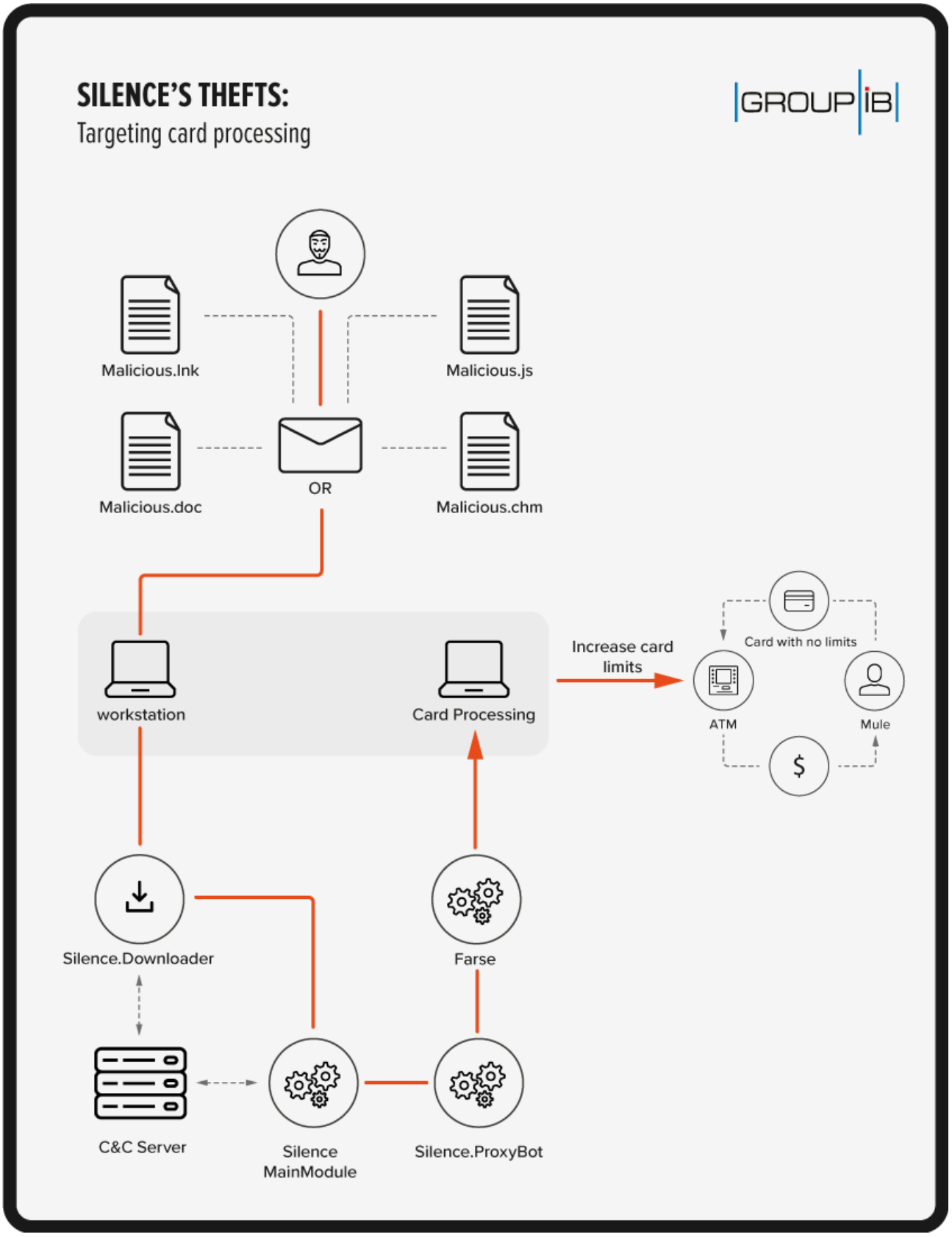
Geography and Timeline of attacks

Silence's successful attacks currently have been limited to the CIS and Eastern European countries. Their main targets are located in Russia, Ukraine, Belarus, Azerbaijan, Poland, and Kazakhstan.

However, some phishing emails were sent to bank employees in more than 25 countries of Central and Western Europe, Africa and Asia including: Kyrgyzstan, Armenia, Georgia, Serbia, Germany, Latvia, Czech Republic, Romania, Kenya, Israel, Cyprus, Greece, Turkey, Taiwan, Malaysia, Switzerland, Vietnam, Austria, Uzbekistan, Great Britain, Hong Kong, and others.

- **July 2016** — A failed attempt to withdraw money via the Russian system of interbank transactions AWS CBR. Hackers gained access to the system, but the attack wasn't successful due to improper preparation of the payment order. The bank's employees suspended the transaction and conducted Incident Response and remediation using their own resources. This resulted in the subsequent incident described below:
- **August 2016** — Another attempt to attack the same bank. Just one month (!) after their failure with AWS CBR, Silence regained access to the servers of the bank and attempted another attack. To do this, they downloaded software to secretly take screenshots and proceeded to investigate the operator's work via video stream. This time, the bank asked Group-IB to respond to the incident. The attack was stopped. However, the full log of the incident was unrecoverable, because in an attempt to clean the network, the bank's IT team deleted the majority of the attacker's traces.
- **October 2017** — The first successful theft by the group that we know about. This time, Silence attacked ATMs and stole over $100,000 in just one night. In the same year, they conducted DDoS attacks using the Perl IRC bot and public IRC chats to control Trojans.
  After the failed attempt with the interbank transactions system in 2016, the criminals did not try to withdraw money using the system, even after gaining access to the servers of AWS CBR.
- **February 2018** — Successful attack using card processing. They picked up over $550,000 via ATMs of the bank's counterpart.
- **April 2018** — In two months, the group returned to their proven method and withdrew funds again through ATMs. During a single night they siphoned about $150,000. This time, the Silence's tools had been significantly modified: they were not burdened with redundant features and ran stably without bugs.


SILENCE'S THEFTS:
Targeting ATMs
GROUP IB
Malicious.lnk
Malicious.js
Malicious.doc
OR
Malicious.chm
Silence.Downloader
C&C Server
Silence
SurveilanceModule
Silence
MainModule
Proxy
Bot
RADMIN
Atmosphere
Dropper
Atmosphere
Injector
Atmosphere
.dll
dispense
command
ATM
Money
Mule



Source: https://www.group-ib.com/blog/silence