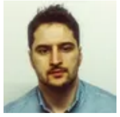
New Silence hacking group suspected of having ties to cyber-security industry

zdnet.com/article/new-silence-hacking-group-suspected-of-having-ties-to-cyber-security-industry/

Home Innovation Security

New Russian-speaking "Silence" group linked to the theft of at least $800,000 from Russian and Eastern European banks and financial institutions.



Written by Catalin Cimpanu, Contributor on Sept. 5, 2018 silence-group.jpg

Group-IB

At least one member of a newly uncovered cybercrime hacking group appears to be a former or current employee of a cyber-security company, according to a new report released today.

The report, published by Moscow-based cyber-security firm Group-IB, breaks down the activity of a previously unreported cyber-criminal group named Silence.

According to Group-IB, the group has spent the last three years mounting silent cyber-attacks on financial institutions in Russia and Eastern Europe.

The group went undetected for years, mainly because of its predisposition for using legitimate apps and tools already found on victims' computers, in a tactic known as "living off the land."

But Silence also created their own tools, such as:

- Silence-- a framework for infrastructure attacks;

- Atmosphere--a set of software tools for attacks on ATMs;
- Farse--a tool to obtain passwords from a compromised computer;
- Cleaner--a tool for logs removal.

These tools, coupled with the group's lay-low tactics helped it go under the radar for far longer than many of its counterparts.

See also: Windows utility used by malware in new information theft campaigns

Following a year-long investigation into the group's modus operandi, Group-IB says the group has been linked to hacks going as far back as 2016.

The first recorded hack attributed to Silence took place in July 2016. The hack was a failed attempt to withdraw money via the Russian inter-bank transaction system known as AWS CBR (Automated Work Station Client of the Russian Central Bank).

"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," Group-IB explained in its report.

However, the bank's remediation efforts weren't up to par, and Silence regained access to the same bank's network a month later, in August 2016. This time, they took another approach.

"[Silence] 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," Group-IB said.

But the Silence group didn't stop after these initial clumsy hacking attempts. They did manage to hack into a bank and finally steal some money, more than a year later, in October 2017.

According to Group-IB, the group stopped attempting to wire money using the AWS CBR system and switched to targeting the bank's ATM control systems, making ATMs spew out cash (known as jackpotting) at desired hours.

Investigators say that Silence stole over $100,000 during their first successful cyber-heist. Other hacks following the same pattern were later discovered and traced back to the Silence group in the following months, such as the theft of over $550,000 in February 2018, and another $150,000 in April 2018.

See also: FIN6 returns to attack retailer point of sale systems in US, Europe

The group is nowhere as successful as other criminal groups known to target financial institutions, such as Cobalt, Buhtrap, or MoneyTraper, all linked to multi-million dollar heists.

The reason, according to Group-IB experts, is that Silence is only a two-man operation --hence, they don't have the same vast human resources to throw at their targets as other groups do.

This is the reason why it took them more than a year to develop the Atmosphere malware they used in the 2017 and later ATM money-dispensing attacks.

silence-attacks.png

Timeline of Silence attacks and tools

Group-IB

But it was when Group-IB researchers analyzed the group's entire malware arsenal that they discovered that despite being a two-man group, Silence was actually pretty good at what it did.

Researchers say the group was very efficient at crafting spear-phishing emails. These spear-phishing emails used exploits for the following Windows and Office vulnerabilities CVE-2017-0199, CVE-2017-11882+CVE-2018-0802, CVE-2017-0262, CVE-2017-0263, and CVE-2018-8174.

The exploits implanted the Silence modular malware framework on victim's systems. The group would use locally installed tools for reconnaissance and lateral movement, and would only deploy Atmosphere when they knew they infected the proper computer that ran ATM-specific software.

When needed, the group would also manually modify malware developed by other crooks, such as the Kikothac backdoor, the Smoke downloader, or the Undernet DDoS bot.

Group-IB says that these modifications to third-party malware are what led its researchers to reach the conclusion that at least one of the Silence group members used to, or still works, in the cyber-security industry.

silence-members.png

Group-IB

Group-IB codenamed the Silence group's members as The Developer and The Operator. They say the former developed or modified all the group's malware, while the latter was the one using them to infect banks and carry out the hacks.

The Developer, in particular, showed advanced knowledge of malware families and reverse engineering skills, but lacked the knowledge to write top-quality code from scratch --a typical trait of most security researchers, who spend most of their time reverse engineering other people's code, rather than writing their own.

"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," said Dmitry Volkov, Chief Technology Officer and Head of Threat Intelligence at Group-IB.

"[The Developer] knows exactly how to develop software, but he does not know how to program properly."

See also: This malware disguises itself as bank security to raid your account

As for Silence's origin, Group-IB believes the two are based either in Russia or another Russian-speaking country.

"Group-IB experts concluded that 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)," the Russian cyber-security firm said today in a press release.

"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."

Group-IB did not share the names of the hacked banks but only said that "successful attacks currently have been limited to the CIS and Eastern European countries," although the group sent spear-phishing emails to banks all over the world.