The Silence group

Reference: Memo [191025-1] – Version: 1.0
Keywords: Silence group, banks, ATM, jackpotting, mules
Sources: Publicly available sources, partner security team

Key Points

- Russian origin cyber-criminal group Silence is attacking banks and financial institutions.
- Starting in 2016, the group has improved its tools and escalated its activities to attack worldwide.
- Its capabilities make it a potentially serious threat currently and in the future.

Summary

The criminal group Silence has been active since at least 2016, progressing in a slow pace, targeting banks and financial institutions primarily in Eastern Europe and CIS countries. Since August and September 2019 it has been implicated in cyber-criminal activities with a financial nexus in more than 30 countries worldwide (including Asia and Latin America) and observed in several EU countries as well. Specifically, the group aims to penetrate bank IT systems which are used for automatic teller machine (ATM) control and management. Silence has demonstrated persistence in its operations and willingness to improve its tools and operational security processes in order to avoid detection. The group's members likely have knowledge of IT security procedures and use it to bypass protection mechanisms. Overall, in the period September 2018 to August 2019 at least 16 Silence campaigns have been observed[1].

Silence group campaigns start by the unusual step of sending numerous empty emails (faking non-delivery reports) to several recipients at organisations of interest. Depending on the (automated) responses they receive back they can compile recipient lists and better focus their next steps. The actual attack email messages contain download links to the group's signature piece of malware, the *Silence downloader* (also known as *Truebot*), received from the Command and Control (C2) infrastructure. Another tool used is a PowerShell-based fileless loader called *Ivoke*. One more PowerShell script, called *EmpireDNSAgent* (based on the *Empire* framework and *dnscat2*) is used for moving inside the organisation. The actor is also making use of pre-existing operating system tools (a practice called "living off the land"). The final goal is to reach the systems controlling ATM machines. Control is achieved with other two pieces of malware: the *Atmosphere* trojan and *xfs-disp.exe*.

At the ATMs Silence either increases withdrawal limits for the group controlled cards or disables the ATM information flow from the bank's payment switch, the system that monitors and authorises transactions, to the core banking systems. Normally such transactions are protected by PCI-DSS regulations as well as encryption of IT system communications. Silence has shown a preference to attack banks that do not implement any of these. The group uses "mules" to channel the funds from the commandeered ATMs.

Communications with the C2 infrastructure and command relay, take place via the *ProxyBot* malware.

The *Silence downloader*, shows a strong resemblance to the *FlawedAmmyy* remote access trojan, operated by the TA505 threat actor (also tracked by the name Indrik Spider), to the extent that security researchers believe they have both been developed by the same individual of Russian origin. For this, as well as other indications, it is highly likely that the Silence group is of Russian origin as well.

The Silence group's activities intensified and turned their attention towards Europe since the beginning of 2019. Initially, UK financial institutions were targeted. However, in the August and September campaigns Slovenian organisations also received lure emails with the same objectives. Silence also apparently attacked a Bangladesh-based Dutch bank earlier in 2019.

Comments

This is a group that started slow since its first appearance in 2016, initially operating in an environment "closer to home" (the CIS countries). It has now gradually gathered expertise and confidence to develop its capabilities and escalate its activities worldwide. It's possible that it may use the same capabilities and tools to extend to other areas of cyber-crime.

[1] https://www.group-ib.com/resources/threat-research/silence-attacks.html

Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.