Silence before the storm: Russian speaking hacking group is attacking banks in Sub-Saharan Africa

Monday, 13th January 2020; Kaspersky security researchers have reported on thousands of notifications of attacks on major banks located in the sub-Saharan Africa (SSA) region. The malware used in the attacks indicates that the threat actors are most likely to be an infamous Silence hacking group, previously known to be responsible for the theft of millions of dollars from banks across the world.

The Silence group is one of the most active Advanced Persistent Threat (APT) actors, which has carried out a number of successful campaigns targeting banks and financial organisations around the Globe. The typical scenario of the attack begins with a social engineering scheme, as attackers send a phishing e-mail that contains malware to a bank employee. From there the malware gets inside the banks' security perimeter and lays low for a while, gathering information on the victim organisation by capturing screenshots and making video recordings of the day to day activity on the infected device, learning how things work in the targeted banks. Once attackers are ready to take action, they activate all capabilities of the malware and cash out using, for example, ATMs. The score sometimes reaches millions of dollars.

The attacks detected began in the first week of January 2020 and indicated that the threat actors are about to begin the final stage of their operation and cash out the funds. To the date, the attacks are ongoing and persist in targeting large banks in several SSA countries.

Kaspersky researchers attribute the attacks to the Russian speaking Silence group based on the malware used in the attacks, which was previously used solely in the group's operations. In addition, the language of the malware is Russian: threat actors attempted to slightly cover this fact by typing Russian words using the English keyboard layout.

"Silence group has been quite productive in the past years, as they live up to their name; their operations require an extensive period of silent monitoring, with rapid and coordinated thefts. We noticed a growing interest of this actor group in banking organisations in 2017 and since that time the group would constantly develop, expanding to new regions and updating their social engineering scheme," said Sergey Golovanov, security researcher at Kaspersky. "We urge all banks to stay vigilant, as apart from the large sums Silence group also steal sensitive information while monitoring the Banks activity as they video record screen activity. This is a serious privacy abuse that might cost more than money can buy."

Kaspersky detects the malware used in the operation as HEUR:Trojan.Win32.Generic,PDM:Exploit.Win32.Generic

To protect from this and similar attacks, we advise financial organisations to apply the following measures:

- Introduce basic security awareness training for all employees so that they can better distinguish phishing attempts.
- Monitor activity in enterprise information systems information security operations center.
- Use security solutions with dedicated functionality aimed at detecting and blocking phishing attempts. Businesses can protect their on-premise email systems with targeted applications inside the Kaspersky Endpoint Detection and Response or use the Kaspersky Anti Targeted Attack platform.
- Provide security teams with access to up to date threat intelligence data, to keep pace with the latest tactics and tools used by cybercriminals.
- Prepare an incident response plan to be ready for potential incidents in the network environment.