MITRE-ID: G0091

Name: Silence

Country: Unknown

Description:

Silence is a financially motivated threat actor targeting financial institutions in different countries. The group was first seen in June 2016. Their main targets reside in Russia, Ukraine, Belarus, Azerbaijan, Poland and Kazakhstan. They compromised various banking systems, including the Russian Central Bank's Automated Workstation Client, ATMs, and card processing.

TTPs:

Resource Development:

* Teh group obtained and modified versions of publicly-available tools

Initial Access:

* The group has used compromised credentials to log on to other systems and escalate privileges.
* Silence has sent emails with malicious DOCX, CHM, LNK and ZIP attachments.

Execution:

* The group has used RAdmin, a remote software tool used to remotely control workstations and ATMs
* Silence has used PowerShell to download and execute payloads.

Persistence:

* The group used HKCU\Software\Microsoft\Windows\CurrentVersion\Run, HKLM\Software\Microsoft\Windows\CurrentVersion\Run, and the Startup folder to establish persistence.
* The group has used compromised credentials to log on to other systems and escalate privileges.

Defense Evasion:

* The group has named its backdoor "WINWORD.exe".
* The group can create, delete, or modify a specified Registry key or value.

Credential Access:

* The group has used the Farse6.1 utility to extract credentials from lsass.exe.

Discovery:

* The group has used Nmap to scan the corporate network, build a network topology, and identify vulnerable hosts.

Lateral Movement:

* The group has used RDP for lateral movement

Collection:

* The group can capture victim screen activity.
* The group has been observed making videos of victims to observe bank employees day to day activities.

Command and control:

* The group has used ProxyBot, which allows the attacker to redirect traffic from the current node to the backconnect server via Sock4\Socks5.
* The group has used port 444 when sending data about the system from the client to the server.