Issued 11/1/17

New Trojan 'Silence' Uses Stealth to Attack Banks

Security researchers have discovered a new attack against financial organizations, in which hackers break into their infrastructure and stay lurking for months to learn their internal procedures before starting to steal money. Because of the extended period of time when attackers monitor and learn the behavior of their victims, researchers have dubbed the Trojan program used in this attack "Silence."

The cybercriminals behind Silence are not the first to incorporate stealthy techniques normally associated with cyberespionage and APT threats. In 2014, a cybercriminal group called Carbanak used similar methods to infect more than 100 financial institutions worldwide and steal $1 billion. Then, in 2016, Kaspersky researchers reported similar operations launched by two other gangs that used malware programs known as Metel and GCMAN. The Silence gang first compromises some machines at the targeted organizations, using methods that have yet to be determined, with the goal of gaining access to employee email accounts. The group then uses compromised accounts to send malicious spear-phishing emails to other employees, launching a multistage attack.

Those rogue emails seen by the Kaspersky researchers carry Microsoft Compiled HTML Help (CHM) files embedded with malicious code. When opened, the files execute rogue JavaScript code, which then downloads a malicious VBS script from an URL and runs it. The VBS script installs a malware dropper that connects to a command-and-control server and

downloads multiple payloads that act as modules, each with different functionality. One module continuously takes screenshots of the victim's desktop and builds a real-time video stream for the attackers that allows them to monitor the employee's activity. Another module allows attackers to execute Windows shell commands on the machine.