Quick Heal
Security Simplified

Advanced Targeted Attacks Set Sights on Philippines Financial Companies

Overview

The Quick Heal Threat Research Labs have observed several targeted attacks aimed towards private sector companies and financial institutions from the Philippines over the last few days. These attacks spread through spam emails which contain malicious executable files as attachments within them.

What is notable about these attacks is that once the components are executed by victims, the malicious payloads cleverly avoid detection. They ensure that they do not activate automated analysis systems of network security products. These detections confirm the rise of trends wherein malware authors are using advanced Anti-VM (Virtual Machine) and Anti-Sandbox tricks to bypass automated analysis security software.

Moreover, these payloads are specially built to carry out surveillance over users to capture keylogs, screenshots and to steal login credential information.

Capabilities of the Targeted Attack

The mechanism of this targeted attack is quite similar to the technique used by previously seen APTs (Advanced Persistent Threats). Once all the components have been decrypted and downloaded onto a victim's machine, the remote attacker gains full access and he is capable of performing the following malicious activities:

- Steals credentials of Outlook and Live Mail accounts
- Performs keylogging activities
- Takes screenshots
- Copies clipboard data
- Downloads and executes other malicious components

Analysis of the Malicious Attachments

The malicious attachments that have been discovered contain executables which are named "fraudulent trns.exe". This name entices curious users to click on the file and spread the payload further into the system. The available file header information indicates that the file was created on 2nd August, 2015. After the payload has entered the system, it communicates with an external C&C (Command & Control) server and shares confidential information from the infected machine.

C&C Remote Server Details

After analyzing the C&C server details, the following observations have been made regarding this attack:

- The C&C server panel is active with the name “KeyBase Web Panel”
- This panel is hosted on “elley080.com”
- The IP address is 85.159.237.152 and 60 other sites are hosted on IP address
- The registrant name “Jocelyn Santosd” appears to be of Philippine origin
- The IP location located in Roosendaal, North-Brabant region, Netherlands

Conclusion

This targeted attack is aimed specifically at financial organizations and other institutions from Philippines. Analysis of this targeted attack has further shown how this advanced threat is armed with Anti-VM, Anti-Emulation and Anti-Sandbox mechanisms to avoid automated analysis. The file creation date is a little more than 10 days old, which shows that this is a new attack still in progress.

For more information contact:

Adfactors PR Pranali Nimkar +91 9820168532 / +91 9820531932 pranali.nimkar@adfactorspr.com	Quick Heal Technologies Pvt. Ltd. Nikhil Khatri +91 9881-489-689 nikhil.khatri@quickheal.co.in