MITRE-ID: G0072

Name: Honeybee

Country: Unknown

Description:

The group G0072/HoneyBee has been replaced by Operation Honeybee (v1.0).

Operation Honeybee was a campaign that targeted humanitarian aid and inter-Korean affairs organizations from at least late 2017 through early 2018. Operation Honeybee initially targeted South Korea, but expanded to include Vietnam, Singapore, Japan, Indonesia, Argentina, and Canada. Security researchers assessed the threat actors were likely Korean speakers based on metadata used in both lure documents and executables and named the campaign "Honeybee" after the author's name discovered in malicious Word documents.

TTPs:

Resource Development:

* attackers created email addresses to register for a free account for a control server used for the implants.
* the threat actors stole a digital signature from Adobe Systems to use with their MaoCheng dropper.

Initial Access:

* the threat actors deployed malware that used API calls

Execution:

* threat actors relied on a victim to enable macros within a malicious Word document
* threat actors ran sc start to start the COMSysApp as part of the service hijacking and sc stop to stop and reconfigure the COMSysApp

Persistence:

* threat actors installed DLLs and backdoors as Windows services
* the threat actors used a batch file that modified the COMSysApp service to load a malicious ipnet.dll payload and to load a DLL into the svchost.exe process.

Defense Evasion:

* the threat actors used Base64 to encode files with a custom key
* the threat actors deployed the MaoCheng dropper with a stolen Adobe Systems digital signature

Discovery:

* the threat actors used a malicious DLL to search for files with specific keywords

Collection:

* the threat actors collected data from compromised hosts

Command and control:

* the threat actors downloaded additional malware and malicious scripts onto a compromised host
* the threat actors had the ability to use FTP for C2

Exfiltration:

* the threat actors uploaded stolen files to their C2 servers

Reference:

https://attack.mitre.org/campaigns/C0006/