Ticket: 473845
Incident: Tangerine Yellow
Date: 2/16/2019 10:14:44
Description: Pineapple RAT analysis
Status: Assigned

MD5 = dcf574b977e291e159b3efeddc9e5075
SHA1 = bc50bfce0ad9753a6be7448e350a15c1b7f719cc
SHA256 =
18548a48f2c30070dc3982bb04ab004a9491aa5c1933ad73a84c0de1d816cd13
Filename = winspoo1.exe **Defense Evasion - Masquerading (T1036)**

Analysis notes:

C2 protocol is base64 encoded commands **(Command and Control - Data Encoding (T1132))** over https **(Command and Control Standard Application Layer Protocol (T1071))**. The RAT beacons every 30 seconds requesting a command.

So far the following commands have been discovered and analyzed:
UPLOAD file (upload a file server->client)
DOWNLOAD file (download a file client->server) **Command and Control - Remote File Copy (T1105)**
SHELL command (runs a command via cmd.exe) **Execution - Command-Line Interface (T1059)**
PSHELL command (runs a command via powershell.exe) **Execution - Powershell (T1086)**
EXEC path (executes a program at the path given via CreateProcess) **Execution - Execution through API (T1106)**
SLEEP n (skips n beacons)

Sandbox execution artifacts for winspoo1.exe

Network traffic:
10.1.1.1:12442 -> 8.8.8.8:53 (query A www.m1tre.org)
8.8.8.8:53 -> 10.1.1.1:12442 (response A www.m1tre.org A 129.83.44.12)
10.1.1.1:24123 -> 129.83.44.12:443 **Command and Control - Commonly Used Port (T1043)**
129.83.44.12:443 -> 10.1.1.1:24123
10.1.1.1:24123 -> 129.83.44.12:443
129.83.44.12:443 -> 10.1.1.1:24123
10.1.1.1:24123 -> 129.83.44.12:443
129.83.44.12:443 -> 10.1.1.1:24123
10.1.1.1:24123 -> 129.83.44.12:443
129.83.44.12:443 -> 10.1.1.1:24123

10.1.1.1:24123 -> 129.83.44.12:443
129.83.44.12:443 -> 10.1.1.1:24123

File activity:
Copy C:\winspoo1.exe -> C:\Windows\System32\winspool.exe **Defense Evasion - Masquerading (T1036)**

Registry keys added:
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\winspool REG_SZ "C:\Windows\System32\winspool.exe" **Persistence - Registry Run Keys (T1060)**