PTA Security Advisory-No: 52

10, May 2019

Summary

Targeted Malicious RAR file titled as 'LEA LIVE SYSTEM.rar' is spreading in telecom sector of Pakistan. The RAR file contains an executable by the name SETUP.EXE that has a malware hidden in it. Running this file executes the malware in the background, which results in compromise of your operating system.

Analysis

- Name of files: SETUP.exe, alan321.exe, WindowsFormsApplication2.exe
- Malware type: Windows x86 PE Executable based exploit
- Antivirus detection rate: 20/56 common Antivirus programs
- CVE: New Variant

C & C Servers

The malware appears to be using dynamic DNS (No-IP) for communicating with external sources.

Host	PORTS
alan321.ddns.net	1955/TCP
alan321.ddns.net	1955/TCP

Key Indicators of Compromise:

- Uses PORT 1955 (non standard) TCP Port for communication

Hash Value

MD5: 0206ee0f182e49c34b822ab913c11c72
SHA-1 :845c8043732561311128c525c12fb3a1897837a1
SHA 256: 8f1b56e71a010b7b8e0021548ec30d7d31e10f8a6ea187988235dedc8b38c412
SHA 256: c0085eb467d2fc9c9f395047e057183b3cd1503a4087d0db565161c13527a76f

Registry Values

1	HKU\S-1-5-21-3369207043-1486425347-397435451-1000\di: "!"
2	HKU\S-1-5-21-3369207043-1486425347-397435451-1000\Environment\SEE_MASK_NOZONECHECKS: "1"
3	HKU\S-1-5-21-3369207043-1486425347-397435451-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CEBFF5CD-

	ACE2-4F4F-9178-9926F41749EA}\Count\P:\Hfref\Gnun\Qbjaybnqf\Yrn Yvir Flfgrz\PQE Fbsgjner\FRGHC.rkr: 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF FF FF FF FF 90 A2 6D 68 A8 04 D5 01 00 00 00 00
4	HKU\S-1-5-21-3369207043-1486425347-397435451-1000\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{CEBFF5CD-ACE2-4F4F-9178-9926F41749EA}\Count\P:\Hfref\Gnun\nyna321.rkr: 00 00 00 00 00 00 00 00 01 00 00 00 8D 00 00 00 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF 00 00 80 BF FF FF FF FF 00 00 00 00 00 00 00 00 00 00 00 00
5	HKU\S-1-5-21-3369207043-1486425347-397435451-1000\Software\Microsoft\Windows\CurrentVersion\Run\Window Update Complaint: ""C:\Users\Username\alan321.exe" .."

Capabilities of Malware:

Malware tests for the Internet connectivity by opening www.google.com in a browser. It opens notepad.exe and chrome.exe to disguise itself as a legitimate process. It pops up a fake installation failure to support the legitimacy. The Malware connects with the host machines for communications through port 1955. It also has the ability to terminate debugging and task manager in the effected system.

Recommendations:

- Whenever possible, run software with minimal access rights and privileges.
- Use licensed antivirus and regularly obtain its latest updates with its real-time scanning capabilities enabled.
- Only use licensed software and avoids download/use of crack and pirated software.
- Designate PoC from your security / network team (if yet not designated), for seeking assistance and reporting security issues.
- Block the host communicated and URL accessed by the malware.
- Incase if indicators of compromise are found in the system, please disconnect the computer from internet and reinstall the operating system.
- In case of any incident, please report to this office.