MITRE-ID: G0026

Name: APT18

Country: China

Description:

APT18 is a threat group that has operated since at least 2009 and has targeted a range of industries, including technology, manufacturing, human rights groups, government, and medical.

TTPs:

Initial Access:

* The threat actors leverage legitimate credentials to log into external remote services.

Execution:

* The group uses cmd.exe to execute commands on the victim’s machine.
* The group actors used the native at Windows task scheduler tool to use scheduled tasks for execution on a victim network.

Persistence:

* The group establishes persistence via the HKCU\Software\Microsoft\Windows\CurrentVersion\Run key.
* The group actors leverage legitimate credentials to log into external remote services

Defence Evasion:

* The group actors deleted tools and batch files from victim systems.
* The group obfuscates strings in the payload.

Discovery:

* The group can list files information for specific directories.
* The group can collect system information from the victim’s machine.

Command and Control:

* The group can upload a file to the victim’s machine.
* The group uses HTTP and DNS for C2 communications.

Reference:

https://attack.mitre.org/groups/G0026/