MITRE-ID: G0098

Name: BlackTech

Country: China

Description:

BlackTech is a suspected Chinese cyber espionage group that has primarily targeted organizations in East Asia--particularly Taiwan, Japan, and Hong Kong--and the US since at least 2013. BlackTech has used a combination of custom malware, dual-use tools, and living off the land tactics to compromise media, construction, engineering, electronics, and financial company networks.

TTPs:

Resource Development:

* The group has obtained and used tools such as Putty, SNScan, and PsExec for its operations.
* The group has used stolen code-signing certificates for its malicious payloads.
* The group has used valid, stolen digital certificates for some of their malware and tools.

Initial Access:

* The group has exploited a buffer overflow vulnerability in Microsoft Internet Information Services (IIS) 6.0, in order to establish a new HTTP or command and control (C2) server.
* The group has used spearphishing e-mails with malicious password-protected archived files (ZIP or RAR) to deliver malware.
* The group has used spearphishing e-mails with links to cloud services to deliver malware.

Execution:

* The group has exploited multiple vulnerabilities for execution, including Microsoft Office and Adobe Flash vulnerabilities.
* The group has used built-in API functions.
* The group has used e-mails with malicious links to lure victims into installing malware.
* The group has used e-mails with malicious documents to lure victims into installing malware.

Persistence and Privilege Escalation:

* The group has used DLL side loading by giving DLLs hardcoded names and placing them in searched directories.

Defense Evasion:

* The group has used right-to-left-override to obfuscate the filenames of malicious e-mail attachments.

Discovery:

* The group has used the SNScan tool to find other potential targets on victim networks.

Lateral Movement:

* The group has used Putty for remote access.

Reference:

https://attack.mitre.org/groups/G0098/