MITRE-ID: G0054

Name: Sowbug

Country: Unknown

Description:

Sowbug is a threat group that has conducted targeted attacks against organizations in South America and Southeast Asia, particularly government entities, since at least 2015.

TTPs:

Execution:

* The group used command line during its intrusions.

Defense Evasion:

* The group named its tools to masquerade as Windows or Adobe Reader software, such as by using the file name adobecms.exe and the directory CSIDL\_APPDATA\microsoft\security.

Credential Access:

* The group has used keylogging tools.
* The group has used credential dumping tools.

Discovery:

* The group identified and extracted all Word documents on a server by using a command containing \* .doc and \*.docx. The actors also searched for documents based on a specific date range and attempted to identify all installed software on a victim.
* The group listed remote shared drives that were accessible from a victim.

Collection:

* The group extracted Word documents from a file server on a victim network.
* The group extracted documents and bundled them into a RAR archive.
* The group has used keylogging tools.

Reference: https://attack.mitre.org/groups/G0054/