Two Hacking Groups Seen Targeting Materials Sector in Asia



Symantec has published two blog posts to warn organizations about advanced persistent threat (APT) actors targeting the materials sector in Asia.

The most prominent of the hacking groups is Winnti, also known as APT41, Barium, Blackfly, Bronze Atlas, Double Dragon, Wicked Panda, and Wicked Spider, a Chinese state-sponsored threat group active since at least 2007, engaging in both cyberespionage and financially motivated attacks.

The recently observed operation, which was carried out in late 2022 and early 2023, targeted two subsidiaries of an Asian conglomerate in the materials and composites sector, likely for intellectual property theft.

As part of the attacks, the APT was seen using the Winnkit backdoor, Mimikatz, and multiple tools for credential dumping,

screen capture, process hollowing, SQL querying, memory dumping (ForkPlayground), and proxy configuration.

In a separate attack, Symantec observed a materials research organization in Asia being targeted by a previously unknown threat actor called ‘Clasiopa’, which does not appear to be affiliated with other APTs.

Clasiopa likely gained access to the targeted organization by brute forcing public facing servers and used a diversified set of post-exploitation tools, including the Atharvan remote access trojan (RAT), a modified version of the Lilith RAT, the Thumbsender hacking tool, and a custom proxy tool.

According to Symantec, the threat actor checked the IP addresses of the compromised machines and attempted to disable endpoint protections, used the backdoors to build lists of files and exfiltrate them, cleared logs, and created a scheduled task to list file names.

Furthermore, Clasiopa appears to have used legitimate software from Agile and Domino in the attack, but it is unclear whether the attackers deployed the tools or abused existing installations.

Based on commands received from its operators, the Atharvan backdoor can download arbitrary files from a server, execute files, and configure communications with the command-and-control (C&C) server.

The modified Lilith RAT, on the other hand, can kill and restart processes, execute remote commands and PowerShell scripts, and kill and uninstall itself.

Analysis of Atharvan uncovered a Hindi mutex and a password that could suggest Clasiopa is based in India, but Symantec notes that these could be false flags deliberately planted by the threat actor.

Related: Chinese Cyberespionage Group ‘Billbug’ Targets Certificate Authority

Related: New Chinese Cyberespionage Group WIP19 Targets Telcos, IT Service Providers

Related: Meta Disrupted Two Cyberespionage Operations in South Asia

Two Hacking Groups Seen Targeting Materials Sector in Asia