IMPORTANT CYBERSECURITY NEWS: LOTUS PANDA HACKS SOUTH EAST ASIAN GOVERNMENTS WITH BROWSER STEALERS AND SIDELOADED MALWARE

Vairav Cyber Security News Report

Date: April 22, 2025

Vairav Cyber Threat Intelligence Team

Vairav Technology Security Pvt. Ltd.

Thirbam Sadak 148

Baluwatar, Kathmandu

Phone: +977 4541540

Mobile: +977-9820105900

Email: sales@vairavtech.com

EXECUTIVE SUMMARY

A recent cybersecurity incident involving the Chinese state-sponsored threat group Billbug (also known as Lotus Blossom, Lotus Panda, Bronze Elgin) has resulted in the compromise of multiple organizations across Southeast Asia. The attackers infiltrated a government ministry, an air traffic control organization, a telecoms operator, a construction company, a news agency, and an air freight organization. By leveraging sophisticated techniques such as DLL sideloading and deploying custom malware, Billbug aimed to conduct extensive espionage activities. Security experts are advising organizations to take preventive measures to mitigate the risk.

DETAILS OF THE INCIDENT

Description of the Cyber Threat: Between August 2024 and February 2025, the Billbug group conducted a targeted intrusion campaign against various organizations in Southeast Asia. The attackers employed multiple new custom tools, including loaders, credential stealers, and a reverse SSH tool. They utilized DLL sideloading techniques, exploiting legitimate software from Trend Micro and Bitdefender to load malicious DLLs. Additionally, a new variant of the Sagerunex backdoor, exclusively used by Billbug, was deployed to maintain persistence within the compromised networks.

Identification: The campaign was documented by Symantec's Threat Hunter Team in April 2025. Indicators of compromise (IOCs) used in this campaign were also identified in a recent blog by Cisco Talos, confirming the involvement of the Billbug group.

Threat Actor: Billbug is a long-established advanced persistent threat (APT) group believed to be operating on behalf of Chinese interests. The group has been active since at least 2009 and is known for targeting entities in Southeast Asia and the United States.

Affected Entities/Industries:

- Government ministry
- Air traffic control organization

- Telecommunications operator
- Construction company
- News agency
- Air freight organization

Potential Impact: The compromise of these organizations could lead to significant risks, including:

- Unauthorized access to sensitive information
- Operational disruptions
- Financial losses
- Reputational damage

Exploitation Methods:

- DLL sideloading using legitimate software (Trend Micro's tmdbglog.exe and Bitdefender's bds.exe)
- Deployment of custom malware tools such as ChromeKatz and CredentialKatz
- Use of reverse SSH tools for remote access
- Modification of registry entries for persistence

RELATED THREAT INTELLIGENCE & IOCs

Malware Hashes (SHA256)

- *4b430e9e43611aa67263f03fd42207c8ad06267d9b971db876b6e62c19a0805e*
- *2e1c25bf7e2ce2d554fca51291eaeb90c1b7c374410e7656a48af1c0afa34db4*
- *6efb16aa4fd785f80914e110a4e78d3d430b18cbdd6ebd5e81f904dd58baae61*
- *ea87d504aff24f7daf026008fa1043cb38077eccec9c15bbe24919fc413ec7c7*
- *e3869a6b82e4cf54cc25c46f2324c4bd2411222fd19054d114e7ebd32ca32cd1*
- *29d31cfc4746493730cda891cf88c84f4d2e5c630f61b861acc31f4904c5b16d*
- *461f0803b67799da8548ebfd979053fb99cf110f40ac3fc073c3183e2f6e9ced*
- *b337a3b55e9f6d72e22fe55aba4105805bb0cf121087a3f6c79850705593d904*
- *54f0eaf2c0a3f79c5f95ef5d0c4c9ff30a727ccd08575e97cce278577d106f6b*

- *b75a161caab0a90ef5ce57b889534b5809af3ce2f566af79da9184eaa41135bd*
- *becbfc26aef38e669907a5e454655dc9699085ca9a4e5f6ccd3fe12cde5e0594*
- *2da00de67720f5f13b17e9d985fe70f10f153da60c9ab1086fe58f069a156924*
- *f9036b967aaadf51fe0a7017c87086c7839be73efabb234e2c21885a6840343e*

RECOMMENDED ACTIONS

Immediate Mitigation Steps

- Identify and isolate affected systems to prevent further spread.
- Update antivirus and endpoint detection systems with the latest IOCs.
- Conduct a thorough review of network logs for signs of unauthorized access.

Security Best Practices

- Implement strict access controls and least privilege principles.
- Regularly update and patch all software and systems.
- Educate employees on recognizing phishing attempts and suspicious activities.

For Advanced Security Teams

- Deploy advanced threat detection tools to monitor for anomalous behavior.
- Conduct regular penetration testing to identify potential vulnerabilities.
- Establish an incident response plan to quickly address future breaches.

ADDITIONAL RESOURCES AND OFFICIAL STATEMENTS

- https://thehackernews.com/2025/04/lotus-panda-hacks-se-asian-governments.html
- https://www.security.com/threat-intelligence/billbug-china-espionage

CONTACT US

Vairav Technology Security Pvt. Ltd.

Cyber Defender from the land of Gurkha

Thirbam Sadak 148, Baluwatar

Kathmandu, Nepal

Phone: +977-01-4541540

Mobile: +977-9820105900

Email: sales@vairavtech.com

Website: https://vairavtech.com