Billbug: Intrusion Campaign Against Southeast Asia Continues

By About the Author

Archived: 2026-04-05 18:19:56 UTC

The Billbug espionage group (aka Lotus Blossom, Lotus Panda, Bronze Elgin) compromised multiple organizations in a single Southeast Asian country during an intrusion campaign that ran between August 2024 and February 2025. Targets included a government ministry, an air traffic control organization, a telecoms operator, and a construction company.

In addition to this, the group staged an intrusion against a news agency located in another country in Southeast Asia and an air freight organization located in another neighboring country.

The attacks involved the use of multiple new custom tools, including loaders, credential stealers, and a reverse SSH tool.

The campaign is one of the findings documented in the Threat Hunter Team's new whitepaper - *Relentless Force: China-linked Espionage Actors*

Attribution

The activity appears to be a continuation of a campaign first documented by Symantec in December 2024, where multiple high-profile organizations in Southeast Asian countries were targeted. While it was clear that Chinese actors were behind the attacks, attribution to a single actor could not be determined.

However, a recent blog by Cisco Talos detailing recent Billbug activity contained indicators of compromise (IOCs) used in this campaign, indicating that it was the work of Billbug.

Sideloaded Malware

In several of the intrusions, the attackers used legitimate software from Trend Micro and Bitdefender to load malicious loaders, using the technique known as DLL sideloading.

One of the legitimate executables used for sideloading was a Trend Micro binary named tmdbglog.exe (SHA246: f9036b967aaadf51fe0a7017c87086c7839be73efabb234e2c21885a6840343e). This was used to sideload a malicious DLL named tmdglog.dll (SHA256: b75a161caab0a90ef5ce57b889534b5809af3ce2f566af79da9184eaa41135bd). Analysis of tmdglog.dll revealed that it was a loader that read, decrypted, and executed the contents of the file C:\Windows\temp\TmDebug.log. It then logged the execution progress to C:\Windows\Temp\VT001.tmp.

Another legitimate executable used was a Bitdefender binary named bds.exe (SHA256: 2da00de67720f5f13b17e9d985fe70f10f153da60c9ab1086fe58f069a156924). This was used to sideload a malicious DLL named log.dll (SHA256:

54f0eaf2c0a3f79c5f95ef5d0c4c9ff30a727ccd08575e97cce278577d106f6b). Analysis of log.dll concluded that it was another loader which read and decrypted the contents of the file winnt.config. It then started the process C:\Windows\system32\systray.exe and injected the decrypted contents to it.

Several variants of log.dll were used in the campaign, but only one was retrieved for analysis. The same Bitdefender binary was also used to sideload a file named sqlresourceloader.dll, which was also not retrieved. It is unknown if this is related to the loader analyzed or a different tool.

Sagerunex Backdoor

The attackers also used a new variant of the Sagerunex backdoor, a custom tool that is exclusively used by Billbug. The variant (SHA256: 4b430e9e43611aa67263f03fd42207c8ad06267d9b971db876b6e62c19a0805e) appears to be related to variants of Sagerunex documented by Cisco in February 2025. As documented by Cisco, the attackers created a persistence mechanism by modifying the registry to ensure that it would run as a service.

New tools

Among the new tools deployed were two designed to steal credentials from the Chrome web browser. Deployed tools included:

- **ChromeKatz** – Capable of stealing both credentials and cookies stored in Chrome
- **CredentialKatz** – Capable of stealing credentials stored in Chrome
- **Reverse SSH Tool** – Custom tool capable of listening for SSH connections on Port 22

Other Tools

The attackers deployed the publicly available Zrok peer-to-peer tool, using the sharing function of the tool in order to provide remote access to services that were exposed internally.

Another legitimate tool used was called datechanger.exe (SHA256: b337a3b55e9f6d72e22fe55aba4105805bb0cf121087a3f6c79850705593d904). It is capable of changing timestamps for files, presumably to muddy the waters for incident analysts.

Background

Active since at least 2009, Billbug has largely focused on Southeast Asia, targeting governments and military organizations in particular.

The group first came to public attention in 2015 when Palo Alto published a report on its activities in Southeast Asia, linking it to over 50 different attacks over a period of three years. Its campaigns used spear-phishing emails and convincing lure documents to deliver the custom Trensil (aka Elise) Trojan.

In 2018, Symantec published an investigation on the group's activity, detailing an attack on a large telecoms operator in Southeast Asia. The attackers used PsExec to install a previously unknown piece of malware (Infostealer.Catchamas). The discovery of this attack led to the discovery of further attacks against the communications, geospatial imaging, and defense sectors, both in the U.S. and Southeast Asia. During that

investigation, Symantec referred to the actor as Thrip, but we subsequently determined that Thrip and Billbug were most likely the same group and began tracking all activity under the Billbug name.

In 2019, Symantec published another report on the group, detailing the use of two previously unseen backdoors known as Hannotog (Backdoor.Hannotog) and Sagerunex (Backdoor.Sagerunex). Targets of this campaign included at least 12 organizations in Hong Kong, Macau, Indonesia, Malaysia, the Philippines, and Vietnam. In addition to military targets, the group also attacked organizations in the maritime communications, media, and education sectors.

Billbug remained active in subsequent years. In November 2022, Symantec published new research on the group, highlighting an attack on a digital certificate authority in an Asian country. The targeting of a certificate authority was notable because the attackers could have accessed certificates and used them to sign malware, helping them to evade detection. Compromised certificates could also potentially be used to intercept HTTPS traffic.

Learn more about Billbug and other Chinese threat actors in our comprehensive whitepaper:
Relentless Force: China-linked Espionage Actors

Protection/Mitigation

For the latest protection updates, please visit the Symantec Protection Bulletin.

Indicators of Compromise

If an IOC is malicious and the file is available to us, Symantec Endpoint products will detect and block that file.

4b430e9e43611aa67263f03fd42207c8ad06267d9b971db876b6e62c19a0805e – Sagerunex
2e1c25bf7e2ce2d554fca51291eaeb90c1b7c374410e7656a48af1c0afa34db4 – ChromeKatz

6efb16aa4fd785f80914e110a4e78d3d430b18cbdd6ebd5e81f904dd58baae61 – ChromeKatz

ea87d504aff24f7daf026008fa1043cb38077eccec9c15bbe24919fc413ec7c7 – ChromeKatz

e3869a6b82e4cf54cc25c46f2324c4bd2411222fd19054d114e7ebd32ca32cd1 – CredentialKatz

29d31cfc4746493730cda891cf88c84f4d2e5c630f61b861acc31f4904c5b16d – CredentialKatz

461f0803b67799da8548ebfd979053fb99cf110f40ac3fc073c3183e2f6e9ced – Reverse SSH tool

b337a3b55e9f6d72e22fe55aba4105805bb0cf121087a3f6c79850705593d904 – Date changer

54f0eaf2c0a3f79c5f95ef5d0c4c9ff30a727ccd08575e97cce278577d106f6b – Loader

b75a161caab0a90ef5ce57b889534b5809af3ce2f566af79da9184eaa41135bd – Loader

becbfc26aef38e669907a5e454655dc9699085ca9a4e5f6ccd3fe12cde5e0594 – Suspected loader

---