Thrip: Ambitious Attacks Against High Level Targets Continue

By About the Author

Archived: 2026-04-05 13:02:33 UTC

Since Symantec first exposed the Thrip group in 2018, the stealthy China-based espionage group has continued to mount attacks in South East Asia, hitting military organizations, satellite communications operators, and a diverse range of other targets in the region.

Many of its recent attacks have involved a previously unseen backdoor known as Hannotog (Backdoor.Hannotog) and another backdoor known as Sagerunex (Backdoor.Sagerunex). Analysis of the latter has revealed close links to another long-established espionage group called Billbug (aka Lotus Blossom). In all likelihood, Thrip and Billbug now appear to be one and the same.

Since we last published on Thrip in June 2018, the group has attacked at least 12 organizations, all located within South East Asia. Its targets have been located in Hong Kong, Macau, Indonesia, Malaysia, the Philippines, and Vietnam.

The group has attacked a diverse range of targets over the past year, most notably military targets in two different countries. It has also attacked organizations in the maritime communications, media, and education sectors.

One of the most alarming discoveries we made in our original Thrip research was that the group had targeted a satellite communications operator and seemed to be interested in the operational side of the company, looking for and infecting computers running software that monitored and controlled satellites. Significantly, Thrip has continued to target organizations in the satellite communications sector, with evidence of activity dating to as recently as July 2019.

New malware provides more leads

Much of this recent activity was uncovered by Symantec following the discovery of a Thrip tool, a backdoor called Hannotog which appears to have been used since at least January 2017. It was first detected in an organization in Malaysia, where it triggered an alert for suspicious WMI activity with our Targeted Attack Analytics (TAA) technology, available in Symantec Endpoint Detection and Response (EDR).

TAA leverages artificial intelligence in order to comb through Symantec's vast data and spot patterns associated with targeted attacks. It is capable of automatically flagging incidents that would otherwise have taken thousands of hours of analyst time to identify.

TAA allowed us to uncover Hannotog and from there, our expert threat hunting team built out a profile of the adversary's tools, tactics, and procedures. This allowed us to identify other organizations that have been compromised by Thrip, allowing us to build up a complete picture of the group's most recent activities.

Hannotog is a custom backdoor which provides the attackers with a persistent presence on the victim's network. It has been used in conjunction with several other Thrip tools, including Sagerunex, another custom backdoor providing remote access to the attackers, and Catchamas (Infostealer.Catchamas), a custom Trojan deployed on selected computers of interest and designed to steal information.

In addition to custom malware, Thrip has made extensive use of dual-use tools and living-off-the-land tactics. These include:

- Credential dumping
- Archiving tools
- PowerShell
- Proxy tools

The Billbug link

Since Symantec first uncovered Thrip in 2018, we've found strong evidence linking it to the Billbug group.

What ties the two groups together is the Sagerunex backdoor. This malware appears to be an evolution of an older Billbug tool known as Evora. By comparing strings and code flow between the two, we found that:

- The code for logging in both is the same
- The logging string format is similar, Evora is just more verbose
- The log name for both starts with "\00EV"
- The command and control (C&C) communication code flows are similar

Billbug is a long-established espionage group, active since at least January 2009. Similar to the Thrip sub-group, the wider Billbug group is known for specializing in operations against targets in South Asia.

Billbug's targets are usually compromised by either spear-phishing emails or watering hole attacks. The group's spear-phishing attacks have tended to use exploits in Microsoft Office and PDF documents to drop its malware onto victims' computers. To date, many of the group's targets have been governments or military organizations.

Wider picture

Thrip appears to have been undeterred by its exposure last year, continuing to mount espionage attacks against a wide range of targets in South East Asia. Its link to the Billbug group puts its activities into context and proves its attacks are part of a broader range of espionage activity heavily focused on (but not limited to) governments, armed forces, and communications providers.

Symantec's TAA was the catalyst for both our initial discovery of Thrip in 2018 and the discovery of new tools and victims in 2019. Without TAA's artificial intelligence, it is quite likely that the group's activities may have gone undetected for a lot longer.

Protection/Mitigation

Symantec Endpoint Detection and Response (SEDR), which contains TAA technology, automatically detects Thrip-related activity.

In addition to SEDR, Symantec's Managed Endpoint Detection and Response (MEDR) service leverages automated attack hunting provided by analytics as well as Symantec analyst security expertise to remotely investigate and contain incursions by adversaries such as Thrip in Symantec customer networks.

The following protections are also in place to protect customers against Thrip attacks:

File-based protection

- Backdoor.Hannotog
- Infostealer.Catchamas
- Backdoor.Sagerunex

Threat Intelligence

Customers of the DeepSight Intelligence Managed Adversary and Threat Intelligence (MATI) service have received reports on Thrip and Billbug, which detail methods of detecting and thwarting activities of this group.

Indicators of Compromise
