Thrip: Ambitious Attacks Against High Level Targets Continue

symantec.com/blogs/threat-intelligence/thrip-apt-south-east-asia

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.

"Thrip APT group hits targets in Hong Kong, Macau, Indonesia, Malaysia, the Philippines, Vietnam https://symc.ly/2m4FiUv"

Ambitious targets

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.

> Thrip has continued to target organizations in the satellite communications sector, with evidence of activity dating to as recently as July 2019.

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).

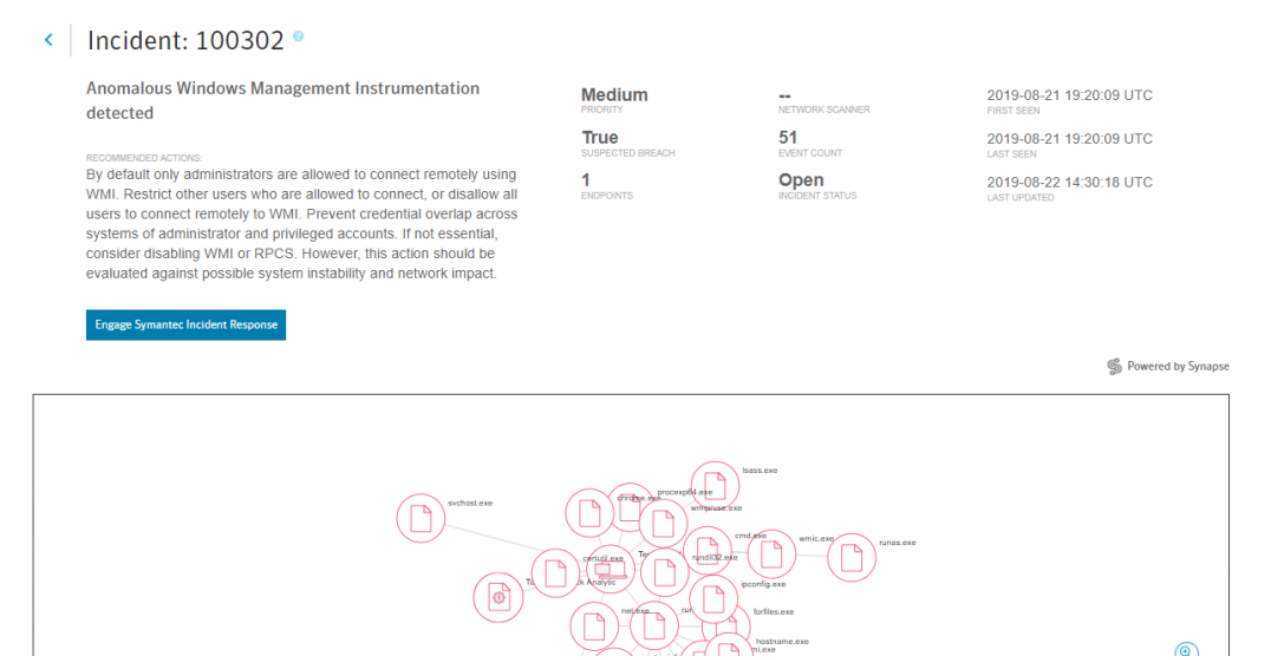

Figure 1. Hannotag was first discovered when it triggered a Targeted Attack Analytics (TAA) alert for suspicious WMI activity

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

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

SHA256	Name
9348eba0582b19c4580491a32457a1904c41c06dee27ed07c86d986d3c98d15c	Hannotog
bd92ce8ef31cd40894b68338d9b71d371936b432b5347d944fad7d9381459761	Hannotog
0d1ecd92570b8ca7b2ffd60271c5f601c08a822197413cf4ffd552a7e2426ff6	Sagerunex
19378dab8b242d94148ad5c48d57d9e45fec5f53b6724155488dd80566a66623	Sagerunex
1e164da9ddd19d0b654e8a60b416c80e82f9bfc0ab35dd262733f4364610c9f4	Sagerunex
27ccd12206d185bf3297df288febf7d47b93ccdc6ec0e5c389ae30da8cac4bf3	Sagerunex
460e11159413b47399aac530433bb00132f54e3859da1f5305977275e37c6153	Sagerunex
5174d45c4e64c5e6abe6639a6a1d6f64bb48b4fb0efdad2b0ea708be7cb82fce	Sagerunex
523f28a364858bd7bb65de7c9e94bbdfbbdb9fe800421c990226662e293a05ea	Sagerunex
76a309691661ed67808a9c438815e9a282495e2e8e0055f2fe40e42bcf002dab	Sagerunex
868f0a1d3764e1c8e03a58caf1d4b8de946671d59b9145e30102ab6540349968	Sagerunex
9530d2df7d340c74f061a1bff87bd2720ff11347b09f05cfb16e4dfd198f0168	Sagerunex
9fd88a5d30fa36d8353cad6ea8b5f867429d39652bf85473de31c39466435775	Sagerunex
c0be532e9fb71e0462f9bfdc8754df320be960b9d510a0b3b6d6cf128c537658	Sagerunex
d45ad71497f48d0d2ebff8ecdcafc9e609b550c0ed76d540d7660dc27785d376	Sagerunex
d54de8e0dc2b58b140f8677be3f0ea3c902dc3f3b112c7350aa95a9cbe24a8af	Sagerunex
d7c6aa114df9be3a1e01c196ca44e929821d6a6316f4754b0933189f98af4fc7	Sagerunex
fe2046e479289b1013eb394f5b3d7a49a419cb98015add3ead0fa87614fe6e38	Sagerunex
3228a0d40222548ea3476b43b13a18ef09f06a4402e3280640ee297533b5a3a0	Catchamas
6b236d3fc54d36e6dc2a26299f6ded597058fed7c9099f1a37716c5e4b162abc	Catchamas
d9131bf2e2e2a80c319ed6ffbe5c726fe30eac50902705096d2610de52a774e2	Catchamas
f14c9c859e12cf70099af098668f849b2ca0e99de6cc62b8569c230f35e36aa5	Catchamas
0fb583b98cb73bd1bda1d60398fc6587a9541fff43d4db6dd172b853dcac1b17	Catchamas
6b01d376b355c56ede966ccf5cca6c8d5616962e67bbf0ddbf7ad395d117fdee	Catchamas
db921a575fa7fd4b0c1b405a54f77d10c73eb1cb1384a27d584d7323e72938b6	Catchamas