InSideCopy: How this APT continues to evolve its arsenal

blog.talosintelligence.com/2021/07/sidecopy.html

By Asheer Malhotra and Justin Thattil.

- Cisco Talos is tracking an increase in SideCopy's activities targeting government personnel in India using themes and tactics similar to APT36 (aka Mythic Leopard and Transparent Tribe).
- SideCopy is an APT group that mimics the Sidewinder APT's infection chains to deliver its own set of malware.
- We've discovered multiple infection chains delivering bespoke and commodity remote access trojans (RATs) such as CetaRAT, Allakore and njRAT.
- Apart from the three known malware families utilized by SideCopy, Talos also discovered the usage of four new custom RAT families and two other commodity RATs known as "Lilith" and "Epicenter."
- Post-infection activities by SideCopy consist of deploying a variety of plugins, ranging from file enumerators to credential-stealers and keyloggers.
- **Talos is releasing a new, detailed paper on SideCopy's operations today, which you can read here.**

What's new?

Cisco Talos has observed an expansion in the activity of SideCopy malware campaigns,

targeting entities in India. In the past, the attackers have used malicious LNK files and documents to distribute their staple C#-based RAT. We are calling this malware "CetaRAT." SideCopy also relies heavily on the use of Allakore RAT, a publicly available Delphi-based RAT.

Recent activity from the group, however, signals a boost in their development operations. Talos has discovered multiple new RAT families and plugins currently used in SideCopy infection chains.

Targeting tactics and themes observed in SideCopy campaigns indicate a high degree of similarity to the Transparent Tribe APT (aka APT36) also targeting India. These include using decoys posing as operational documents belonging to the military and think tanks and honeytrap-based infections.

How did it work?

SideCopy's infection chains have remained relatively consistent with minor variations — using malicious LNK files as entry points, followed by a convoluted infection chain involving multiple HTAs and loader DLLs to deliver the final payloads.

Talos also discovered the usage of other new RATs and plugins. These include DetaRAT, ReverseRAT, MargulasRAT and ActionRAT. We've also discovered the use of commodity RATs such as njRAT, Lilith and Epicenter by this group since as early as 2019.

Successful infection of a victim results in the installation of independent plugins to serve specific purposes such as file enumeration, browser password stealing and keylogging.

So what?

These campaigns provide insights into the adversary's operations:

- Their preliminary infection chains involve delivering their staple RATs.
- Successful infection of a victim leads to the introduction of a variety of modular plugins.
- The development of new RATs is an indication that this group of attackers is rapidly evolving its malware arsenal and post-infection tools since 2019.
- The group's current infrastructure setup indicates a special interest in victims in Pakistan and India.

Analyses and IOCs

You can read a detailed analysis of Sidecopy operations in our new research paper here. You can also find a detailed list of IOCs here and here.

- Win.Dropper.njRAT-9876129-0
- Win.Downloader.FList-9875630-0
- Win.Downloader.FileSearcher-9875631-0
- Win.Downloader.UPirate-9875632-0
- Win.Trojan.Johnnie-9875495-0
- Win.Trojan.Zapchast-9875496-0
- Win.Trojan.Zapchast-9875497-0
- Win.Keylogger.Xeytan-9875498-0
- Win.Keylogger.Lagger-9875499-0
- Win.Trojan.DetaRAT-9875325-0
- Win.Trojan.EpicenterRAT-9875326-0
- Win.Trojan.ReverseRAT-9875329-0
- Win.Trojan.Meterpreter-9875304-0
- Win.Trojan.Lilith-9875305-0
- Win.Trojan.PasswordStealer-9875308-0
- Win.Trojan.Chromer-9875310-0
- Win.Trojan.AllakoreRAT-9875300-0
- Win.Trojan.AllakoreRAT-9875301-0
- Win.Trojan.ActionRAT-9874905-0
- Win.Trojan.AllaKoreRAT-9874917-0
- Win.Malware.Generic-9874177-0
- Win.Packed.Trojanx-9874176-0