Sophos MTR in Real Time: What is Astro Locker Team?

news.sophos.com/en-us/2021/03/31/sophos-mtr-in-real-time-what-is-astro-locker-team/

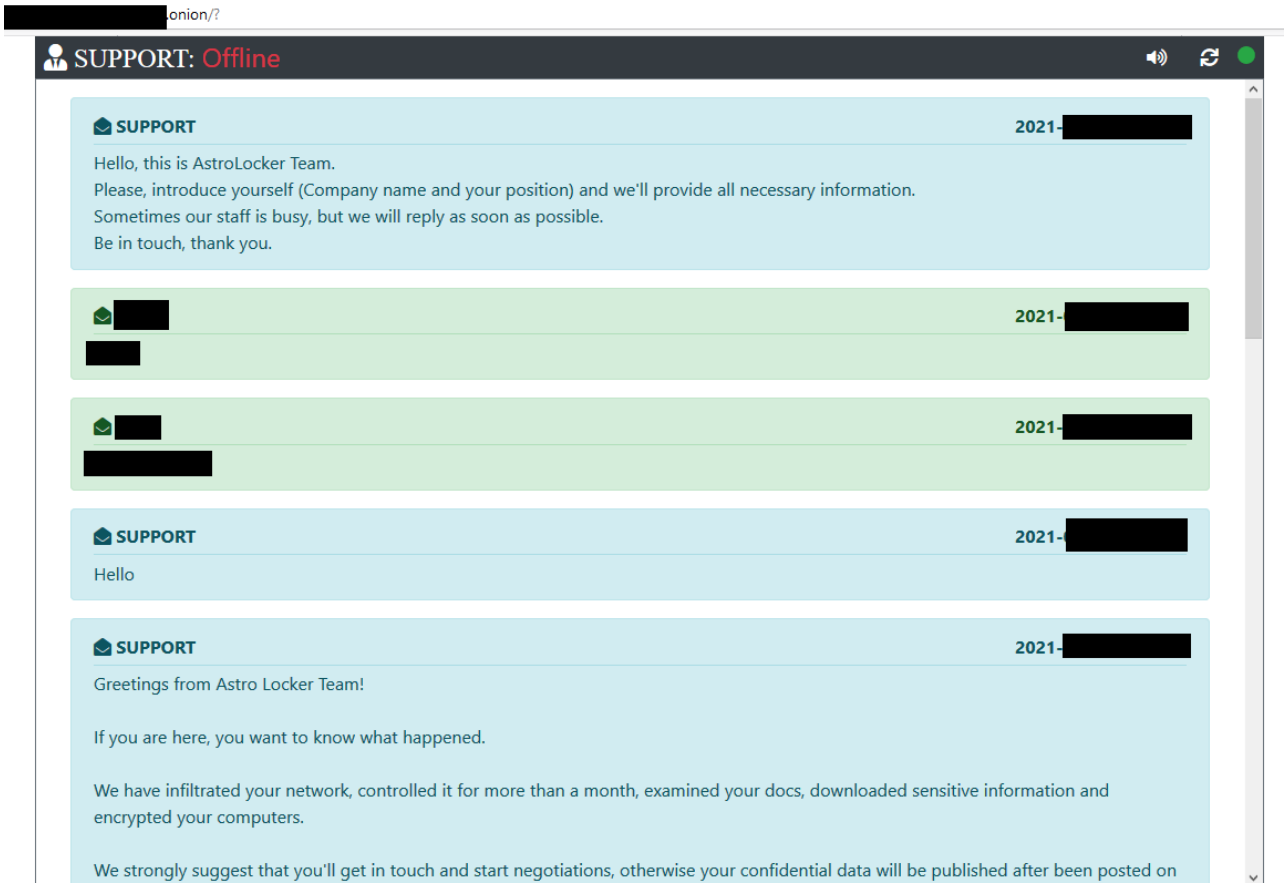
Michael Heller March 31, 2021

A recent incident with a new Sophos Managed Threat Response (MTR) customer has raised questions about the Mount Locker ransomware group and the relationship it has with Astro Locker Team.

A ransomware detection for Mount Locker kicked the MTR team into gear and what they found was surprising. The first detection made it clear what the team was dealing with: rundll32 executing locker_64.dll – Mount Locker ransomware.

MTR moved quickly to stop the attack on unsecured devices and ensure the ransomware group was banished from the organization's network. Throughout the incident all evidence – from the tactics, techniques, and procedures (TTPs) used, to the files involved, and even the ransom note left behind – pointed to this being the work of the Mount Locker group.

However, something odd happened when the investigators followed the link included in the ransom note. Upon following the TOR link, MTR investigators were presented with a chat directly with the "support" team for the ransomware who introduced themselves as the "AstroLocker Team" and also the "Astro Locker Team."



Following up on this new lead, an MTR expert found the Astro Locker leak site and, while there was no listing there for the impacted organization of this case, other interesting links surfaced.

When comparing the Astro Locker leak site to the Mount Locker leak site, investigators noted that all five of the organizations listed on the Astro Locker site were also listed as victims on the Mount Locker site. Digging in further, the size of the data leaks on all five matched and shared some of the same links to the leaked data.

Looking at the matching links more closely, Sophos experts noticed one last connection: some of the leaked data linked on the Mount Locker site was being hosted on the Astro Locker onion site: http[:]//anewset****.onion

While it is unclear what the relationship is between Mount Locker and Astro Locker, defenders should consider both when dealing with a ransomware attack.

“In recent incidents where Sophos experts investigated and neutralized an active Mount Locker attack, we noticed various techniques that suggest these attackers are not as sophisticated as other ransomware groups like Ryuk, REvil and DoppelPaymer,” Peter Mackenzie, manager of Sophos’ Rapid Response team said. “It is possible that the Mount Locker group wants to rebrand themselves to create a new and more professional image, or

it could be an attempt to kickstart a true ransomware-as-a-service program. Regardless, if any organizations become a victim of 'Astro Locker' in the future, they should investigate the TTPs of both Mount Locker and Astro Locker."

Ransomware relationships and branding

It is known that Ragnar Locker is affiliated with Mount Locker in some way but doesn't appear to be part of the Mount Locker ransomware-as-a-service (RaaS). Although Ragnar is the more skilled ransomware group and the two groups don't overlap in TTPs or malware, Mackenzie said it was possible there were "back end" services being shared, including access to target networks.

The connection between Mount Locker and Astro Locker is clearer insofar as they both use Mount Locker ransomware, the same ransom note, and share some TTPs, such as using services to execute commands and batch scripts. Creating scheduled tasks called 'updater' and 'regsvr32' as well as hiding some of their files in the same location: C:\Users\\Music\.

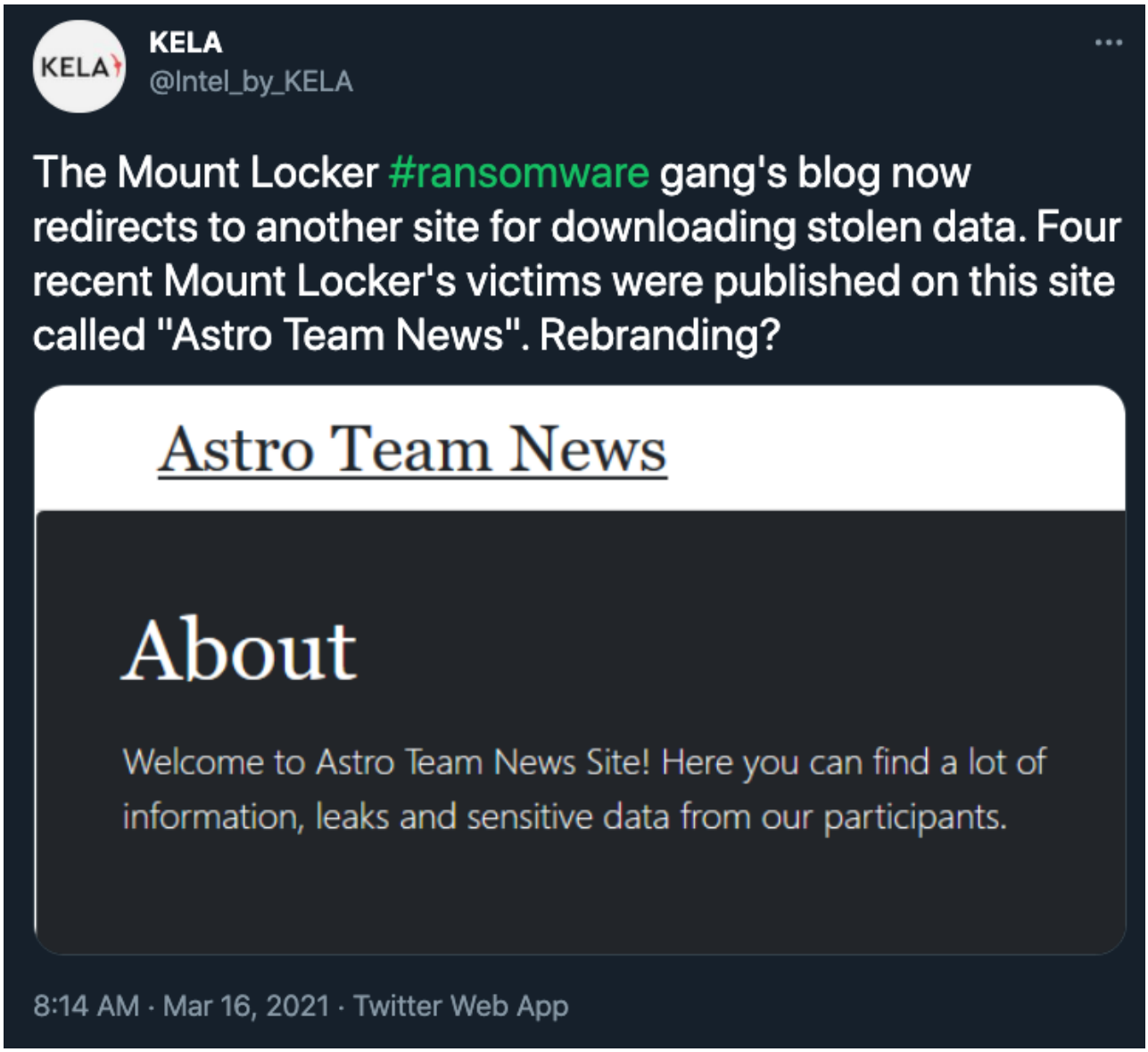
Astro Locker:

Service Name: PrpOJqmErkoJtAAg – random 16-character string
Service File Name: %COMSPEC% /C echo whoami ^> %SYSTEMDRIVE%\\WINDOWS\\Temp\\FaUocMGJjmCAbJMr.txt > \\WINDOWS\\Temp\\uxvbnnSkrkOMnsJg.bat & %COMSPEC% /C start %COMSPEC% /C
Scheduled Task Name: updater
Action: regsvr32.exe /i C:\Program Files\Google\Drive\wininit64.dll

Mount Locker:

Service Name: xGGXJTFBQlzNTVTT
Service File Name: %COMSPEC% /C echo whoami ^> ZSYSTEMDRIVE%\WINDOWS\Temp\pkLneFsUyHywIUwZ.txt > \WINDOWS\Temp\sloKuaTCIYITTPwM.bat & %COMSPEC% /C start %COMSPEC% /C \WINDOWS\Temp\sloKuaTCIYITTPwM.bat
Scheduled Task Name: updater
Action: C:\Users\\AppData\Local\Google\Chrome\User Data\FileTypePolicies\archs64.dll

"A few outside sources that have noticed the connection between Mount Locker and Astro Locker and suggested it may be a close affiliate relationship. Mount Locker has been reported to be running RaaS, but it has never been clear how many affiliates were in the program," said Mackenzie. "Astro Locker, as a significant branded group to be part of a Mount Locker RaaS, could imply Mount Locker is attempting to speed up a transition to becoming a RaaS, or it could even be that the Mount Locker group is using the Astro name to pretend they have a big new affiliate.



“Branding is a powerful force for ransomware groups,” Mackenzie added. “Good branding can come from a single threat group being skilled at hitting high value targets and avoiding detection – such as DoppelPaymer – or by running a successful RaaS network – like Sodinokibi or Egregor. Powerful branding with ransomware groups can strike fear in targets and lead to a higher likelihood of payouts.

“Mount Locker has proven itself as a less sophisticated ransomware group, so a pivot to an affiliate program might be a way to create a new brand and move up the hierarchy of threat groups.”

IOCs

Mount Locker/Astro Locker ransomware, on its own, is unable to bypass the CryptoGuard feature of Sophos Intercept X; Our endpoint products may detect components under one or

more of the following definitions: Troj/Ransom-GFR and Malware/Generic-S. Network protection products like the Sophos XG firewall can also block the malicious C2 addresses to prevent the malware from retrieving its payloads and completing the infection process.

IoCs relating to these threats can be found on the SophosLabs Github.

Special thanks to John Carlo Adriano, Colin Cowie, Blake Bowdoin, Jordon Carpenter, and Peter Mackenzie for their efforts in detecting, investigating, and responding to these threats.