Tracking the inputs and outputs of extortion groups is a significant part of the puzzle as we continue to research the growing web of threat actors. It is essential to understand the mechanisms and patterns used by these groups to perpetrate their crimes.

**Conclusion**

The SentinelOne malware contains a hardcoded list of folders and files that are to be excluded from encryption. The ransomware also attempts to determine whether it is running in a specific debugger. The search list includes `C:\Windows\explorer.exe`, `C:\Windows\System32\MDMHost.exe`, `C:\Windows\System32\iexplore.exe`, and `C:\Windows\System32\WindowsUpdate.exe`. If it finds any of these processes, it will not encrypt the files associated with them.

The ransomware attempts to remove volume shadow copies (VSS) using the following command:

\[ \text{Ransomware would detect and prevent malicious behaviors and artifacts associated with Good Day/ARCrypter ransomware.} \]

In particular, we found a series of ransom notes that all include the email address MikLYmAklY555[@]cock[.]li. Some of the portals have been revealed in previous research by Cyble.

In July and August of 2023, we observed multiple new TOR-based URLs being staged for use by the Good Day group. Each portal is intended for a different language and contains a unique URL for the victim to download a ransom note.

The Cloak leak site first appeared in August of 2023 and currently lists 23 victims. Many of these victims are marked as "sold" and their respective data is available for purchase on the Cloak blog site. They also mention specific company names that can be found on the Cloak blog site.

In the case of sample URLs, we have observed that the Cloak data sales and leaks with Good Day through publicly viewable chats on the group's TOR-based victim portals.

We expand on several unique Good Day ransom notes and victim portals and share our analysis of a sample associated with a URL lead. Good Day ransomware, a variant within the ARCrypter family, was first observed in-the-wild in May of 2023. Between June and August of 2023, we continued to monitor this group and their payloads.

Observing the URLs found in ransom notes and the existing structure of the victim blog sites, we are able to firmly establish the nature of the tie between these two entities. Our analysis shows that Good Day ransomware victims are being threatened with having their data leaked or sold on the Cloak website. This intimidation tactic is used to coerce the victim into paying the ransom.

In particular, we found a series of ransom notes that all include the email address MikLYmAklY555[@]cock[.]li. Some of the portals have been revealed in previous research by Cyble.

In July and August of 2023, we observed multiple new TOR-based URLs being staged for use by the Good Day group. Each portal is intended for a different language and contains a unique URL for the victim to download a ransom note.

The Cloak leak site first appeared in August of 2023 and currently lists 23 victims. Many of these victims are marked as "sold" and their respective data is available for purchase on the Cloak blog site. They also mention specific company names that can be found on the Cloak blog site.

In the case of sample urls, we have observed that the Cloak data sales and leaks with Good Day through publicly viewable chats on the group's TOR-based victim portals.