Arete

Observations on Midnight Group's Fraud Campaign Resurgence

March 24, 2023

Table of Contents

Executive Summary 3

Key Takeaways 3

Background 3

How is the Midnight Group Identifying Victims? 5

Conclusion 6

Executive Summary

Arete's research recently discovered a fraud campaign by a re-emerging actor dubbed "Midnight Group" specifically targeting organizations who previously fell victim to ransomware attacks. Midnight Group operations date back as far as 2019, but recently their operational tempo has increased dramatically. Interestingly, the re-victimized organizations experienced the initial attacks at the hands of over five distinct threat actor groups. Victims of this fraud campaign receive emails claiming the Midnight Group was behind the original ransomware attack, and their data will be posted on the dark web if they do not pay. At the time of this reporting, at least 15 current or previous Arete clients received this fraudulent email.

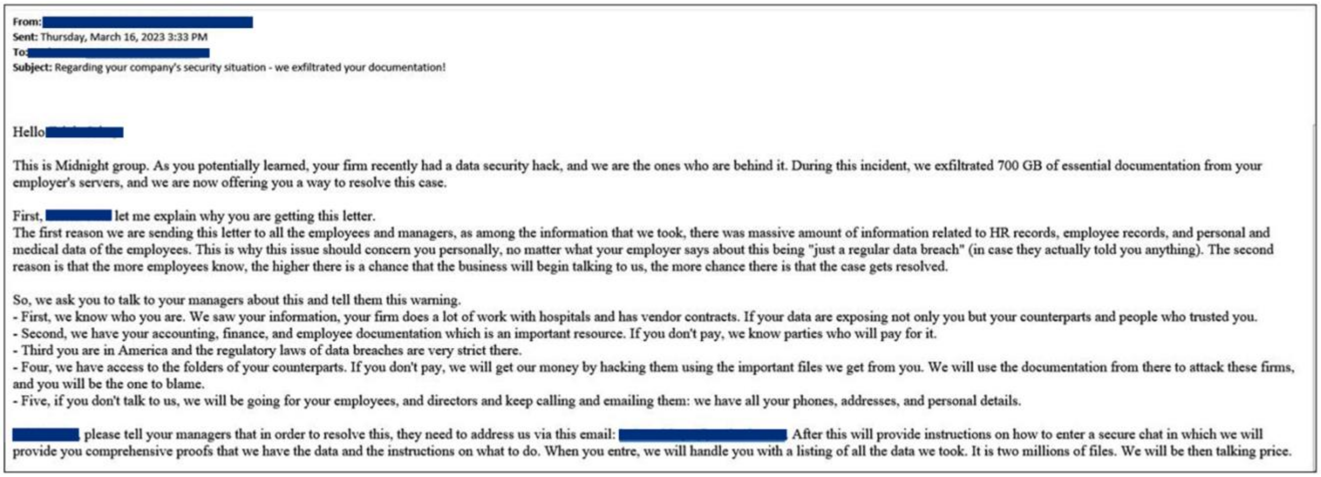
Key Takeaways

- The Midnight Group threat actor is identifying victims of ransomware attacks, even when the victims are not publicly available.
- The Midnight Group claims to have exfiltrated between 700GB–900GB of data, even in cases where no data exfiltration occurred, or a different amount of data was exfiltrated.
- Contacted individuals appear to have been identified on the victim's public website.
- In several instances, the threat actor claimed to be associated with different ransomware operations (e.g. Surtr and Silent Ransom), but these threat actor groups were not involved in the original ransomware attack suffered by the victims.

Background

Arete's Cyber Threat Fusion Center identified victims of previous ransomware campaigns receiving suspicious emails claiming to have exfiltrated data and intending to leak their data unless payment is made to the threat actor. The extortion email makes vague claims regarding the victim's customer base, exfiltrated data, and ancillary threats should the ransom not be paid. The Midnight Group requests that the victim contact them via email for proof of exfiltration (POE) before initiating negotiations.

The Midnight Group contacts easily identifiable individuals from the victim organization's public-facing website. Common roles receiving this email include sales, business development, and executive team members. In addition to claiming to be the original threat actor, they also claim the Midnight Group exfiltrated 700GB-900GB of data, even when data exfiltration did not originally occur during the ransomware attack.



From: [redacted]
Sent: Thursday, March 16, 2023 3:33 PM
To: [redacted]
Subject: Regarding your company's security situation - we exfiltrated your documentation!

Hello [redacted]

This is Midnight group. As you potentially learned, your firm recently had a data security hack, and we are the ones who are behind it. During this incident, we exfiltrated 700 GB of essential documentation from your employer's servers, and we are now offering you a way to resolve this case.

First, [redacted] let me explain why you are getting this letter.
The first reason we are sending this letter to all the employees and managers, as among the information that we took, there was massive amount of information related to HR records, employee records, and personal and medical data of the employees. This is why this issue should concern you personally, no matter what your employer says about this being "just a regular data breach" (in case they actually told you anything). The second reason is that the more employees know, the higher there is a chance that the business will begin talking to us, the more chance there is that the case gets resolved.

So, we ask you to talk to your managers about this and tell them this warning.
- First, we know who you are. We saw your information, your firm does a lot of work with hospitals and has vendor contracts. If your data are exposing not only you but your counterparts and people who trusted you.
- Second, we have your accounting, finance, and employee documentation which is an important resource. If you don't pay, we know parties who will pay for it.
- Third you are in America and the regulatory laws of data breaches are very strict there.
- Four, we have access to the folders of your counterparts. If you don't pay, we will get our money by hacking them using the important files we get from you. We will use the documentation from there to attack these firms, and you will be the one to blame.
- Five, if you don't talk to us, we will be going for your employees, and directors and keep calling and emailing them: we have all your phones, addresses, and personal details.

[redacted], please tell your managers that in order to resolve this, they need to address us via this email: [redacted]. After this will provide instructions on how to enter a secure chat in which we will provide you comprehensive proofs that we have the data and the instructions on what to do. When you entre, we will handle you with a listing of all the data we took. It is two millions of files. We will be then talking price.

Figure 1: Midnight Group Ransom Email

As the campaign progresses, tactics by the Midnight Group vary slightly. In several cases, the threat actor claimed to be associated with well-known ransomware operations such as the Silent Ransom Group and Surtr. However, in cases where Arete has visibility into both the initial ransomware operator and the threat actor behind the fraud campaign, the threat actors did not align. This corroborates Arete's understanding that the Midnight Group does not have significant insight into the previous ransomware attack. Arete identified the following factors, which contribute to an organization's heightened susceptibility to targeting by the Midnight Group:

- An organization appeared on a threat actors' data leak site (DLS).
- An organization is in active communications with a ransomware actor.
- An organization suffered a ransomware attack, but there was no data exfiltration.
- An organization made payment to the initial ransomware actors for decryption.

How is the Midnight Group Identifying Victims?

While it is currently unclear how the Midnight Group is receiving information on victims affected by various ransomware operations, Arete contemplates several possible scenarios:

Hypothesis one – Collaboration with initial threat actors

It is possible the actors behind the Midnight Group paid or otherwise convinced the initial threat actors to share their victim information. This would explain the Midnight Group's ability to contact victims still in active communication with the initial threat actors.

Counterpoint: The likelihood of the Midnight Group convincing multiple actors to divulge the information of victims who previously paid ransoms or are actively in communications with hopes of receiving payment is low since it would cause a significant hit to the actor's reputation and decrease the chance of future victims paying the ransom.

Hypothesis two – Victim information is collected from publicly available sources

The Midnight Group could passively collect information by monitoring threat actor data leak sites and open-source information such as social media, news articles, and security researchers' blogs. This would be the path of least resistance for the Midnight Group to launch its fraud campaign.

Counterpoint: There are several instances where either the original threat actors are still in active communications with the victim, or the ransom payment was made to the threat actor and the victim was never publicly disclosed.

Hypothesis three – The Midnight Group gained access to a netflow collection toolset to identify potential victims

It is possible the Midnight Group gained access to a netflow collection tool that continuously captures netflow information from the internet. This could allow the Midnight Group to monitor actor command and control (C2) infrastructure and identify potential victims.

Counterpoint: Access to these netflow collection toolsets can be expensive and difficult to obtain. Additionally, creating a proprietary toolset with similar functionality would require a strong background in multiple technical disciplines. The likelihood of the actors behind the Midnight Group having the ability to conduct these operations is low.

Hypothesis four – The Midnight Group gained access to a government or private centralized reporting database for ransomware activity

It is possible the Midnight group gained access to a centralized database where victim information is stored. This could give the Midnight group access to ransomware victim information, but not in-depth details of the ransomware operation, as seen with the fraud campaign.

Counterpoint: Ransomware reporting databases would primarily be maintained by government organizations. It is unlikely the Midnight Group possesses the technical aptitude required to obtain access to these databases.

Hypothesis five – The Midnight Group gained access to multiple ransomware organizations' infrastructure and identified victims that are not publicly available

It is possible the Midnight Group was able to gain access to various threat actors' infrastructure and extract the victim information through offensive measures. Many threat actors, such as Hive, who was recently the subject of a major law enforcement operation, struggled with security hygiene throughout their affiliate programs, leaving them exposed to offensive operations.

Counterpoint: The recipients of the Midnight Group's emails were victims of at least five different ransomware operations, which, at this time, are not currently believed to be operated by a single overarching cybercrime group:

- Quantum Locker
- Timisora hacking team (THT)
- Black Basta
- Luna Moth
- Black Cocaine

Based on this information, it is unlikely the Midnight Group gained victim data from each of these actors' infrastructure.

Conclusion

Based on the available evidence, Arete assesses it is unlikely Midnight Group's claim of being behind the original ransomware attacks is true. The vague accusations of data exfiltration recycled between victims and the contacting of publicly available individuals within victim organizations further cement the idea that this is merely a fraud campaign. Arete has attempted contact with the group and, upon initial contact, was instructed to contact the threat actor using an email address from the company domain. Once completed, the threat actor did not respond or give POE, building on the assessment that the actor does not have exfiltrated data from the victims' environments.

Importantly, the ability to identify victims in active negotiations is a novel tactic not previously identified by Arete. Fraudulent attempts of data extortion will likely continue to plague organizations affected by cybercrime and cause reputational damage to threat actors. Additionally, while the Midnight Group operations have persisted throughout the years, the sudden uptick in operational tempo and target identification is notable. We continue to monitor this threat for developments in the threat actor's capabilities and tactics.