The Unseen One: Hades Ransomware Gang or Hafnium

awakesecurity.com/blog/incident-response-hades-ransomware-gang-or-hafnium/

March 29, 2021

Threat Intelligence from Hades Incident Response Engagements

When you talk about ransomware threat actors, the image that is conjured up is one of ruthless mercenaries looking to make a quick buck. Unfortunately, much of the security industry operates under this assumption, and perhaps fails to look at broader motives and deeper breaches. Over the past two weeks, we have seen two posts from CrowdStrike and Accenture respectively documenting the Hades Ransomware Gang. While we agree with many of the technical conclusions in these posts and have observed many of the same tools, we believe there is more to the Hades story. Our incident response engagements with Hades and other threat actors has us increasingly convinced that ransom is not the only objective for at least some of these gangs. With that perspective, we are engaging the community to share our analysis. As we encountered the Hades threat actor, they appeared to exhibit a number of characteristics that were at once unlike other ransomware gangs, almost amateurish in a sense, while at the same time showing the type of sophistication and obfuscation that is more the forte of nation-state based advanced persistent threats (APT). Our “spidey sense” certainly went off but given the extremely limited threat intelligence on the Hades ransomware gang across the community as a whole, it was difficult to paint the full picture. However, as our experience with this threat actor has increased, we have been able to identify a set of defining characteristics that lead us down the path of challenging the conventional wisdom surrounding at least one ransomware gang. Perhaps the other gangs have similar alternate motives that we have not collectively picked out.

In this post we will break down several aspects we saw during our incident response engagements including:

- Industries and Geography
- Leak Sites

- Tactics and Tools
- Forensic Practices
- Intelligence Gaps
- Detecting the Techniques

As you will see below, in responding to this threat actor we uncovered evidence tactics, techniques and procedures that can be attributed to multiple sophisticated adversaries including Hafnium group, the threat actor Microsoft says is behind the recent Exchange Server hack. Based on a forensic timeline we built across multiple engagements, we believe there is significant evidence that points to one of two possibilities:

- An advanced threat actor is operating under the guise of Hades;
- Multiple independent actors just coincidentally compromised the same environment, potentially due to weak security practices in general.

Background

Arista's Awake Labs' incident response team had the opportunity to help several of the organizations impacted by Hades with their incident response needs. Some may already be familiar with the Hades Ransomware attack on Forward Air Trucking Giant Attack in December 2020, however at the end of 2020 there were several other victims. With such a limited number of publicly disclosed victims of the Hades group, we have a unique perspective with data that has not been available to anyone else. As you will see below we uncovered evidence of multiple nation-state and ransomware actors tools and techniques, while at the same time observing behaviors that are uncharacteristic of a sophisticated ransomware adversary.

Hafnium and Other Potential Connections to Hades

As we responded to multiple Hades ransomware attacks over the last few months, the lack of logging and forensic data sometimes hampered our ability to identify the initial access point into the network. The one exception being a possible Hafnium compromise. Our team was pulled in after the compromise and encryption to review the situation and in this one case a Hafnium domain was identified as an indicator of compromise within the timeline of the Hades attack. Moreover, this domain was associated with an Exchange server and was being used for command and control in the days leading up to the encryption event. The domain, p[.]estonine[.]com/p?smb, was identified by a third party forensic firm first engaged by the victim. Based on their analysis this domain was first seen in a Hades attack in December 2020. Clearly at this point the vulnerability in Exchange had not been publicly disclosed but this attack time frame aligns more closely with the DevCore vulnerability discovery date. This clearly provides evidence of the attack prior to January 2021, which has been the consensus until now.

In addition to Hafnium and the Hades gang, some victims showed evidence of other threat actors. While we were not able to forensically determine the direct connection to the Hades attacks, we are providing a summary of these discoveries in case this intelligence is relevant to future Hades attacks.

TimosaraHackerTeam (THT) Tools and Techniques

Remnants of the TimosaraHackerTerm (THT) ransomware group, named after a town in Romania, were identified in one or more environments, a few weeks prior to the Hades attack. The THT situation mirrored almost exactly the details in a Sensors Tech Forum Remove THT posting from March 2020. Awake Labs also saw the use of BestCrypt as mentioned in a blog post by id-ransomware in June of 2018. In short, we saw the following activities.

- VSS Admin was used to clear shadow copies of the local machine
- Bitlocker or BestCrypt (bcfmgr) was used for encryption on the local machines
- External IP connection was made to Romania IP 185[.]225[.]19[.]240

For the THT IOCs, the IP address mentioned from Romania was observed between October and November 2020 with malicious behavior and associated with two new files tracked on VirusTotal.

File MapsBroker.exe

> SHA-256:
> ed3dc1c727e5de77e3700cd2da699d46e3590dc98f8cabca7a70fd9e6e73977a

Oracle.bat

> SHA-256: 2fb5766af3d68c210e62518263b2f29ca4c50100c99b6979c3d0e19f05af6a39

It was also reported with malicious behavior by open intel communities on October 30, 2020 (Figure 1).

DATE CHECKED	URL	HOSTNAME	SERVER RESPONSE	IP
Oct 30, 2020	http://185.225.19.240/	185.225.19.240	200	185.225.19.240
Oct 30, 2020	http://185.225.19.240/dmenconsvc.dll	185.225.19.240	200	185.225.19.240

Figure 1: TimosaraHackerTeam IOCs

Hades Gang: Tactics, Techniques and Procedures

Industries and Geographies

Our analysis and intelligence shows that there was relatively a small number of organizations that were hit by the Hades ransomware gang. While there could be more, it is interesting to note that no other victims have been publicly identified in the media or via the known Hades

leak methods (more on this below).

The focus of this gang also appears to be mostly with a few industries. As mentioned above, a logistics provider has been publicly mentioned as a victim. Our intelligence shows that most of the other organizations have a focus in manufacturing, and more specifically those in the automotive supply chain as well as those with insulation products.

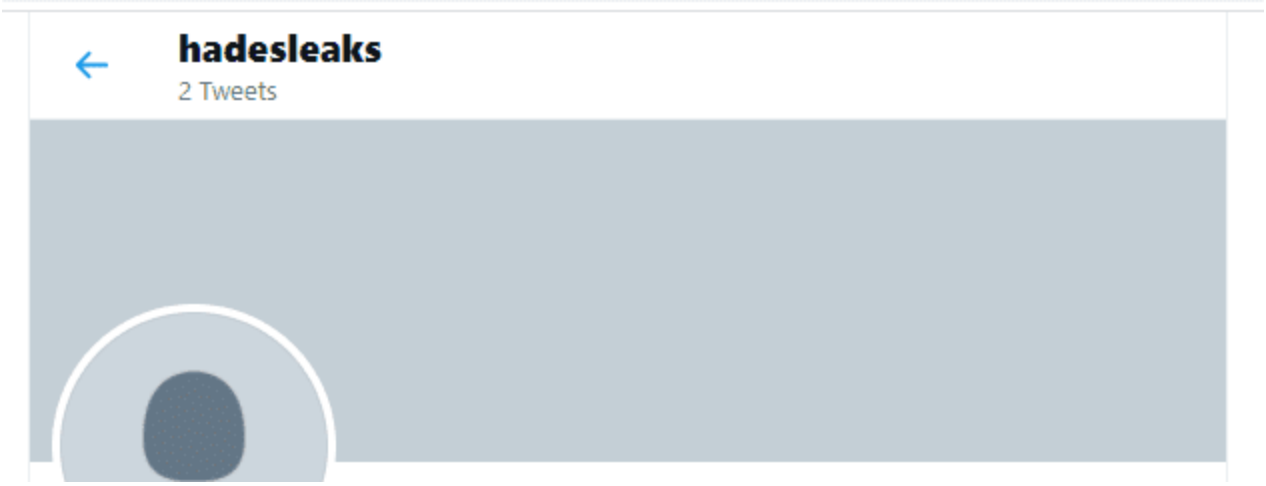
The locations of the attack were slightly dispersed as each of the companies were global in their operational footprints. While these organizations were impacted across multiple geographies, we have evidence to suggest that the ransomware attack was focused on the geographies below :

- Canada
- Germany
- Luxembourg
- Mexico
- United States

While other ransomware gangs do target specific verticals, they usually run larger campaigns where the goal is to compromise several organizations with the hope of higher payouts. Hades' relatively narrow targeting does stand out as unique comparatively.

Leak Sites

As incident responders know it is common for ransomware actors to set up leak sites for their data, but what was interesting about Hades is that they used methods for both their leaks and their drop sites that would likely be taken down within a very short time. There was very little sophistication in this setup, something that stands apart from other ransomware actors. For example, if you look up @hadesleaks on Twitter today you will see the response "No results for "@hadesleaks". However, as recently as December 2020 / January 2021, there were a few victims mentioned including the trucking giant (Figure 2). Additionally, we observed that this actor chose multiple different sites for their leaks, with the only consistency being the Twitter account used to broadcast the message naming the victims.



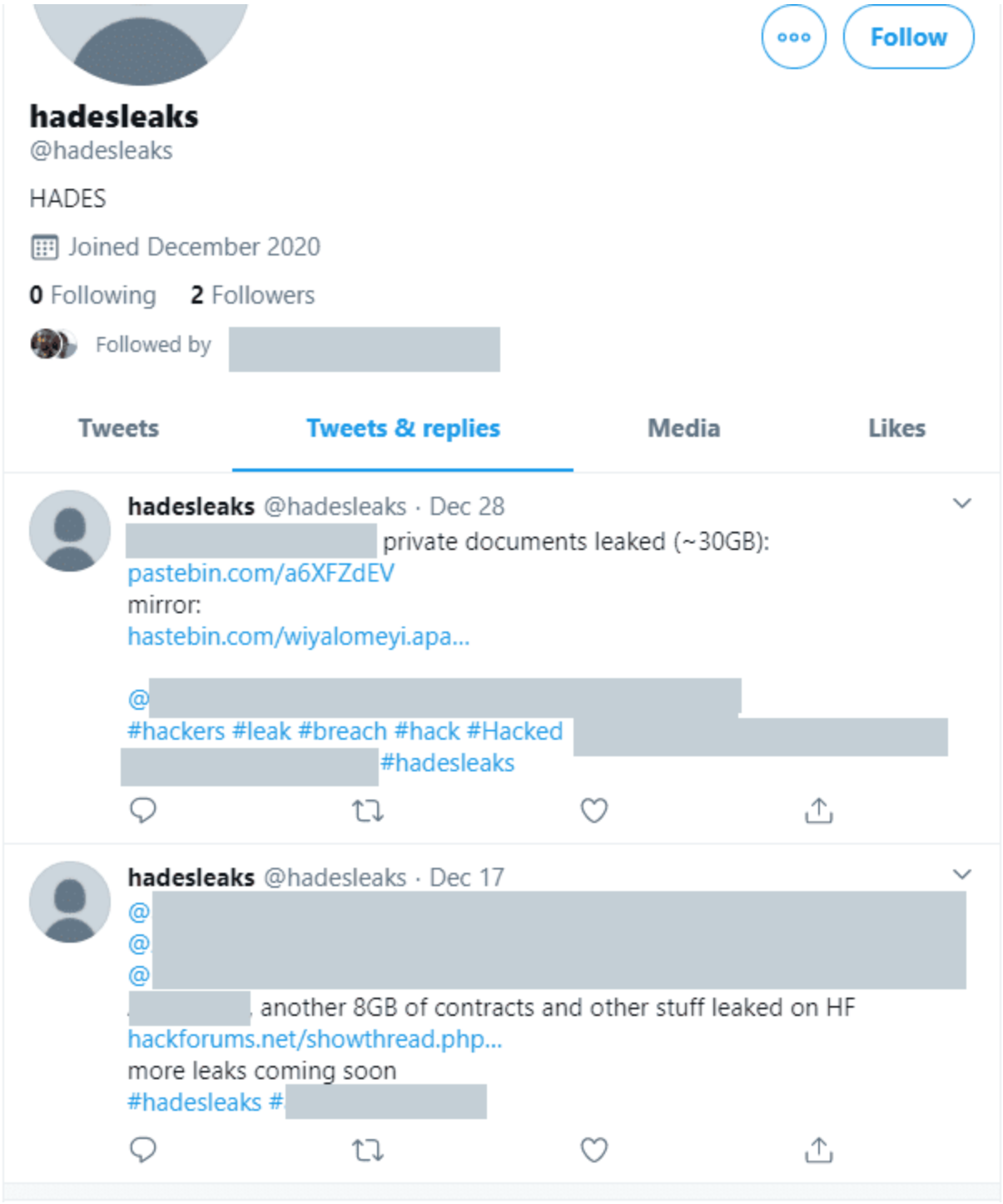


Figure 2: hadesleaks Twitter

For instance, in the first posting on Dec 17th, the leak site “hackforums” was used (Figure 3). But very quickly this site was rendered inaccessible within the forum.

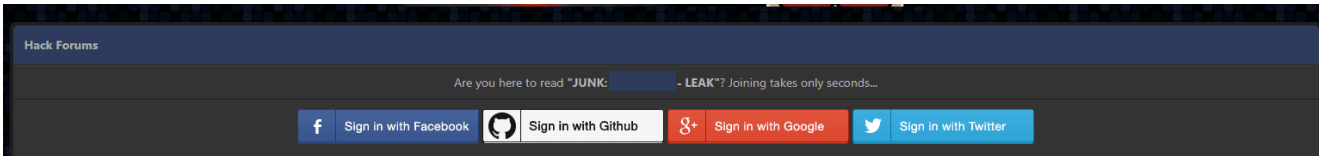


Figure 3: hackforums Dec 17 leak

Eleven days later in their next post, we see the Hades gang use both pastebin and a mirror hastebin (Figure 4). Both sites today say “This page is no longer available.” The pastebin and the hastebin site were removed.

In both these sites we see the files hosted on “mega.nz,” a cloud storage provider, which we will provide more context about later.

Figure 4: Pastebin Hades Leak site

As for the Twitter account, Awake Labs and several other organizations requested that it be suspended. On or about January 1, 2021 the account was in fact suspended by Twitter (Figure 5) leaving the actor to find other mechanisms to inform the world of its leaks. As of this writing the account continues to be locked out.

Figure 5: Hadesleaks Twitter Captured on January 2, 2021

When we downloaded and looked at the data from the leak sites and compared it to what our incident responders forensically identified as being exfiltrated, it appeared as if the data on the leak sites was not the most consequential data the actor could have leaked. The data

chosen for the leak was a very limited set with little repercussions to the victims. Meanwhile the exfiltrated data was very different containing large amounts of data focused on manufacturing processes. The question that therefore arises, what was the objective of stealing the crown jewels but disclosing less significant bits of information? Did they hold back on publicly sharing the most valuable data because they had alternate means to monetize the proprietary secrets?

We know the actor requested amounts in the range of $5 to $10 million of ransom and was very slow to respond to some individuals. In some cases, they may not have responded at all. In fact, one Twitter user even claimed "TA never responds." If there were only a few organizations attacked, why would it take so long to respond to requests for ransom? Was there another potential motive here? Why haven't we seen Hades since?

Tactics and Techniques

Our analysis identified many of the actors' techniques used during the attack.

MITRE ATT&CK® Tactic	Techniques
Resource Development (TA0042)	Malware compilation Obtain Capabilities: Malware – T1588.001
Execution (TA0002)	Execution of the malware (Ransomware) Malicious File – T1204.002 Winexe tool for remote execution System Services: Services Execution – T1569.002
Credential Access (TA0006)	Use of service and admin level accounts Valid Accounts – T1078
Discovery (TA0007)	GUI navigation of shares and directories Network Share Discovery – T1135 Query session command qwinsta Remote System Discovery – T1018
Lateral Movement (TA0008)	Remote desktop login Remote Desktop Protocol – T1021.001 Transfer of malware (Ransomware) via PsExec Lateral Tool Transfer – T1570
Collection (TA0009)	7zip and Zip used to compress data prior to exfiltration Archive Collected Data – T1560 Search of local file systems and databases Data from network Share Drives – T1039 Data from Local System – T1005 Archived files staged for extraction Data Staged: Local Data Staging – T1074.001

Command and Control	Hafnium domain DNS communication – T1071.004
Exfiltration (TA0010)	Mega.nz Cloud Storage Provider Exfiltration Over Web Service: Exfiltration to Cloud Storage – T1567.002
Impact (TA0040)	Ransomware Data Encrypted for Impact (T1486)

Forensic Practices

Resource Development

During our review, Awake was able to identify timestamps within the AppCompatCache that showed binary modifications. The actor appeared to be compiling the ransomware binary at the same time the data was exfiltrating out of the environment.

Execution

We identified execution of the malware, which was achieved via PsExec, through the RecentApps entry, Registry Key LastWrite times and the creation of new services on the remote systems it was run against.

The data we have also shows the usage of the tool winexesvc.exe in one environment which has been used by other actors in the past for remote execution.

- SHA-256: be582632770b52fd6c4a5d375c73f150b42199e81e3c138f6fab243316ff9e07
- SHA-256: a9e2d7c4c796eedb69f3847b44981a13e32a454d324412962a0dc825460b2c90
- SHA-256: 1b5f182ea9e224e8e7f33c7df247b05292de6f4e65381aca0d5e626cf9b00c8

This software was seen initially executed on an Exchange system.

The Awake team had fun piecing together screenshot artifacts from the RDP bitmap cache (Figure 6 and Figure 7) showing PsExec execution. We were able to validate:

- The user account used to run PsExec and responsible for the service creation on remote hosts
- The option -p <blocked out password> would indicate the partial password for the account was used
- References to “PsEx” and “xec.exe” which are portions of PsExec
- References to C:\data\PsE which we know was where PsExec was run from based on the RecentApp entry
- The option -s to run the remote process in the System account

- The option -f to copy the specified program even if the file already exists on the remote system

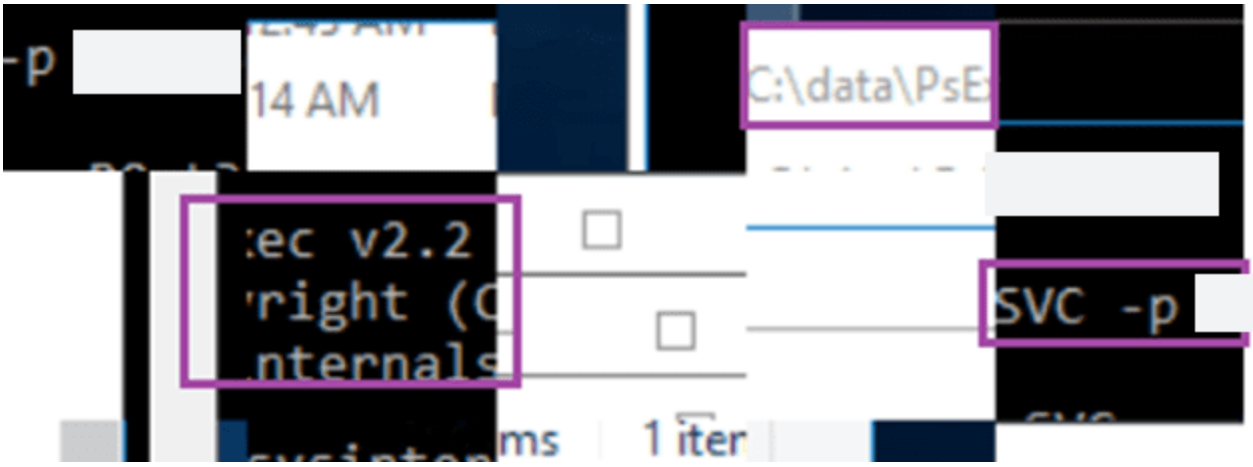


Figure 6: RDP Cache 1

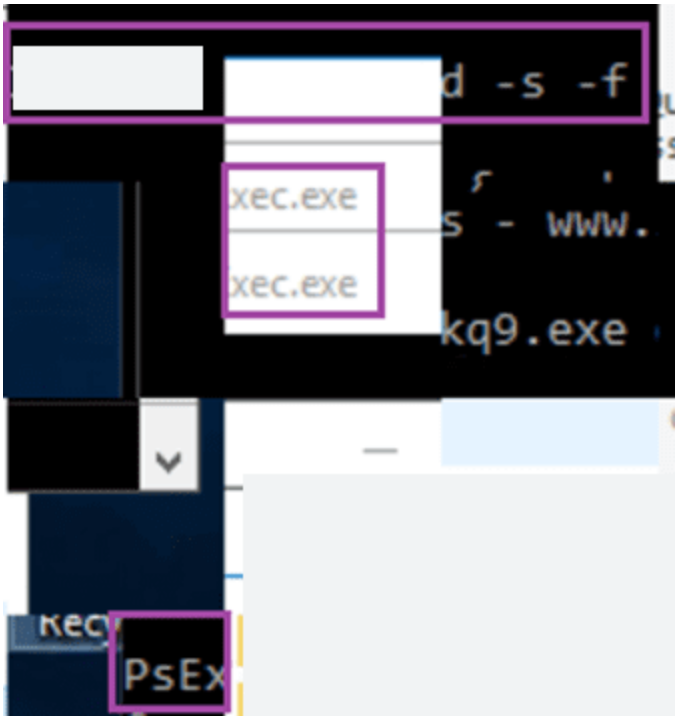


Figure 7: RDP Cache 2

Credential Access

The threat actor also leveraged valid accounts throughout the environments showing there was some level of compromise that enabled them to obtain privileged access. Awake was able to use bitmap cache file entry for RDP typically located in the directory

\Users\<user>\AppData\Local\Microsoft\Terminal Server Client\Cache\

Awake was also able to see JumpList entries for RDP with the associated user id in the directory

\Users\<user>\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations\

These artifacts exposed both service account and privilege admin accounts that were used by the threat actor.

We also are aware of at least one environment where Mimikatz was used as a method to extract credentials. This was the same environment with the file winexesvc.exe on the Exchange system where the Hafnium domain was identified.

SHA-256: 31443b7329b1bdbcf0564e68406beabf2a30168fdcb7042bca8fb2998e3f11c5

Discovery

Remote System Discovery was also conducted by the actors via the query session command qwinsta. This command was identified with the Powershell ConsoleHost_history.txt file. The qwinsta command is run to display information about sessions on a Remote Desktop Session Host server.

Lateral Movement

Like many other attacks, administrator and service accounts were used by the actor with PsExec to move lateral from system to system across domains to access and prep files for exfiltration. The actor compromised accounts and then used RDP to navigate throughout the organizations. Once the exfiltration was done, the actor then used PsExec to push the ransomware that encrypted the environments.

Collection

The Hades actors searched local file systems and databases to find files of interest and sensitive data prior to Exfiltration. They also searched and collected data from network shares on remote systems. Common targets of this were accessible shared directories on file servers. Awake identified these activities on multiple systems by analyzing the ShellBags registry artifact.

For the archiving, the actor was identified downloading 7zip from a regular download site. Awake also was aware of the WinRar utility's use at some of the victim organizations. 7zip leaves an archive history in the NTUSER.data registry hive, which provided the ArchHistory value data which when parsed provides the file listings that were archived. The files listed in the ArchHistroy were compared to files we knew were exfiltrated and they matched.

Exfiltration

The exfiltration methods that were concretely identified and used by the Hades gang are not particularly new. For instance, we see in an article from July 2020 where the Mega[.]nz application was used. In this case, we investigated and identified the Hades actor downloading the standard Mega.nz application directly from its main site and using these commonly available tools for exfiltration.

Impact

The actor in more than one instance was particularly destructive. There were several confirmed instances where the actor issued commands such as “kill” to destroy the backup storage systems, rendering the organization incapable of restoring from backup.

Outside of the backup destruction we saw the impact of the encryption across the Microsoft Windows environment. With ransomware we know adversaries encrypt files in large numbers across the network. This was similar in the Hades incidents, we identified cross domain encryption and several different versions of the encryption software used in the Hades incidents. At least one of the files was associated with Sodinokibi ransomware while the others files appear to be associated with a Crypmodng signature.

- SHA-256: ea310cc4fd4e8669e014ff417286da5edf2d3bef20abfb0a4f4951afe260d33d
- SHA-256: 0dfcf4d5f66310de87c2e422d7804e66279fe3e3cd6a27723225aecf214e9b00
- SHA-256: fe997a590a68d98f95ac0b6c994ba69c3b2ece9841277b7fecd9dfaa6f589a87
- SHA-256: 1f7b65834408fad403f4959f3c265751c09dd1d55350a68b1c02b603c145fe48

Detecting the Techniques

The Awake Security Platform detects these threats across the network. In addition, the Awake Labs team can be contacted for detailed forensic investigations. The following is a list of the existing network detection and response (NDR) models that can identify the activity outlined in this article.

Awake Security Detection Models

- Discovery: SMB Admin Share Access
- Lateral Movement: Psexec Like Activity
- Lateral Movement: Interactive Remote Shell Access through PsExec
- Lateral Movement: Remote Desktop Used by Administrator on Non-Admin Device
- Lateral Movement and Execution: Remote Command Execution (psexec, cobalt strike, metasploit, others)
- Download: Possible Ransomware Tool TTPs
- Collection: Device Collecting Several Potentially-Sensitive Files from Destination System
- C2: Highly Suspicious Domain Communicating Repeatedly With Few Devices
- Exfiltration: At Least 1GB of Data Uploaded to Mega
- Impact: Behavior Typical of Ransomware (Numerous New Files Created and Written)

Subscribe!

If you liked what you just read, subscribe to hear about our threat research and security analysis.

Jason Bevis

VP, Awake Labs

LinkedIn