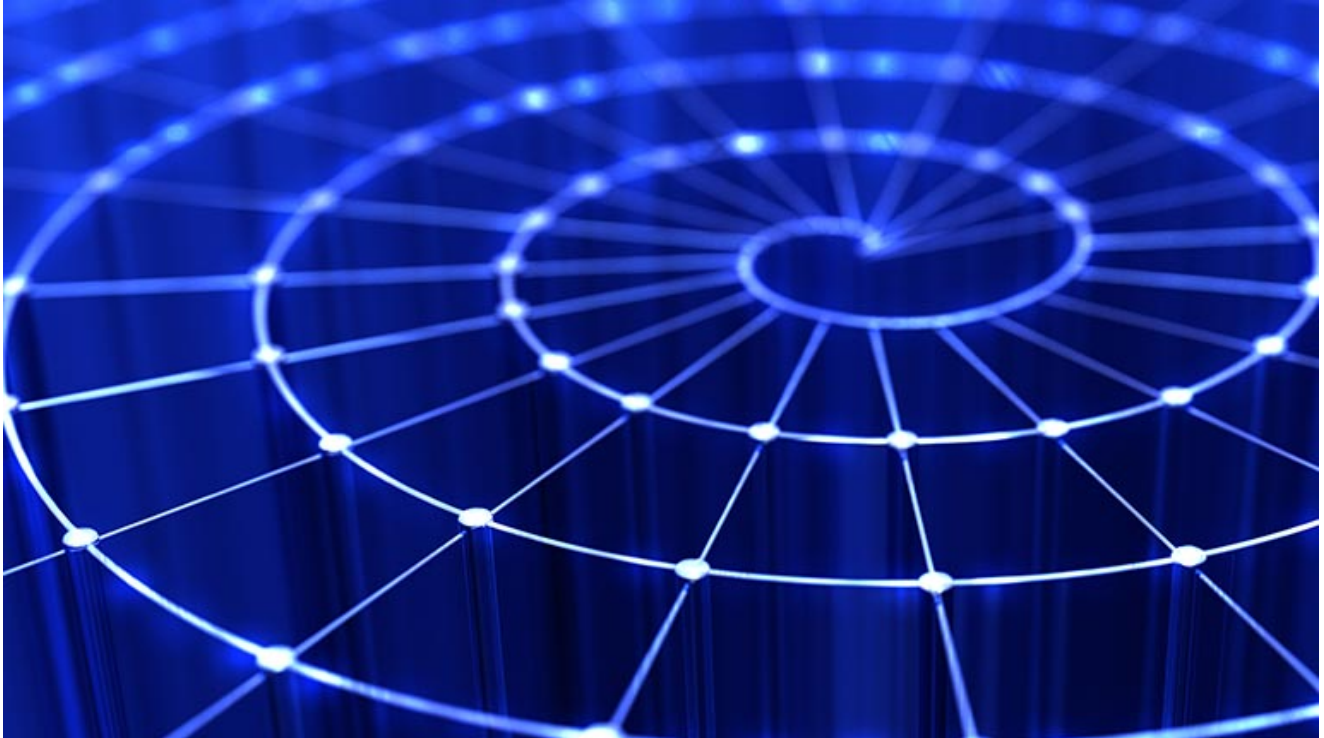


It's getting hot in here! Unknown threat group using Hades ransomware to turn up the heat on their victims

[accenture.com/us-en/blogs/cyber-defense/unknown-threat-group-using-hades-ransomware](https://www.accenture.com/us-en/blogs/cyber-defense/unknown-threat-group-using-hades-ransomware)



Cyber Defense

March 26, 2021

Share

Executive Summary

- An unknown financially motivated threat group is using the self-proclaimed Hades ransomware variant in cybercrime operations that have impacted at least three (3) victims since December 2020.
- Known victims include a large US transportation & logistics organization, a large US consumer products organization, and a global manufacturing organization.
- Tactics, Techniques and Procedures (TTP) employed to compromise a victim network, escalate privileges, move laterally, evade defenses, exfiltrate data and deploy Hades ransomware are relatively consistent with other well-known ransomware operators, using a combination of commodity tooling and various living-off-the-land techniques.

- Of note, we observed significant effort by the threat group to disable or bypass endpoint defenses, including Endpoint Detection and Response (EDR) tooling, using both custom tooling and hands on keys approaches.
- We assess with moderate confidence that the group's operations have just begun, and that Hades activity will likely continue to proliferate into the foreseeable future, impacting additional victims.

The information outlined in this blog is based on collection from CIFR incident response engagements, Open-Source Intelligence (OSINT), and various media reports. This is a developing story; additional details will be released to the community when available.

Summary & timeline

An unknown threat group is using the self-proclaimed Hades ransomware in cybercrime operations that have impacted at least three (3) victims. Based on collection sources, the threat group has been in operations since at least December 2020 and has continued to target victims through March 2021. Accenture Security also analyzed the group's activities in the context of attribution, victimology, and TTPs employed according to OSINT and incident response data. Accenture Security assesses the group's operations have just begun, and their activity will likely continue to proliferate into the foreseeable future, targeting additional victims.

Victimology

We are currently aware of 3 victims, all of which are large multi-national organizations with annual revenues exceeding \$1 billion USD. The profiles of the three (3) known victims are a strong indicator of Big Game Hunting, with target selection and deployment methods aimed toward high-value payouts. This also may explain the relatively low number of known victims since Hades was first identified publicly in December 2020.

Industries impacted so far based on known victimology include:

1. Transportation & Logistics
2. Consumer Products
3. Manufacturing & Distribution

Furthermore, we identified additional Tor hidden services and clearnet URLs via various open-source reporting pertaining to the Hades ransomware samples. For all analyzed samples, the ransom notes identified instruct the victim to install Tor browser and visit the specified page. The Tor pages differ only in the Victim ID that is provided, indicating each Tor address may be uniquely generated for each victim. Accenture Security identified a total of six (6) of these addresses, indicating there could be three (3) additional victims we are unaware of at this time.

<<< Start >>>



Hades
ransomware.

Contact Us

We have hacked your network, downloaded and encrypted your data.

You can recover your data and prevent data leakage to the public.

For further details contact us via [TOX](#) messenger:

COPYRIGHT © HADES

Figure 1—Hades ransomware tor site

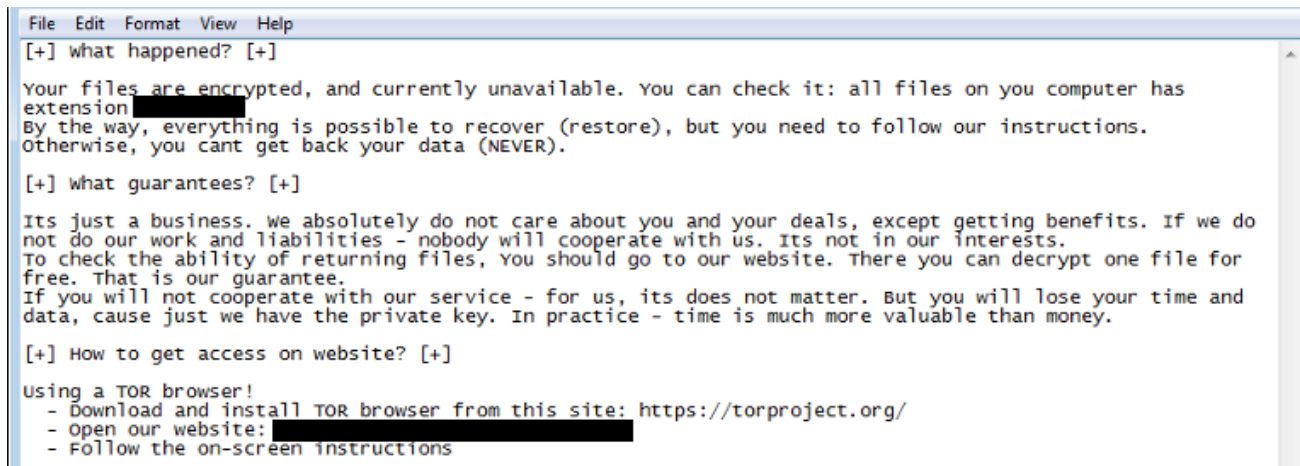
<<< End >>>

Hades ransomware operations

At this time, it is unclear if the unknown threat group operates under an affiliate model, or if Hades is distributed by a single group. Under an affiliate model, developers' partner with affiliates who are responsible for various tasks or stages of the operation lifecycle, such as distributing the malware, providing initial access to organizations or even target selection and reconnaissance. However, based on intrusion data from incident response engagements, the operators tailor their tactics and tooling to carefully selected targets and run a more "hands on keyboard" operation to inflict maximum damage and higher payouts.

In addition, we identified similarities in the Hades ransom notes to those that have been used by REvil ransomware operators, where portions of the ransom notes observed contain identical wording. The differentiating factors in the ransom notes are the operators' contact information and the formatting of the ransom notes. While the ransom notes are similar, we do not have any evidence to suggest the threat groups or operations have any overlap at this time.

<<< Start >>>

A screenshot of a ransomware ransom note displayed in a text editor window. The window has a menu bar with 'File', 'Edit', 'Format', 'View', and 'Help'. The text of the note is as follows:

```
[+] what happened? [+]
Your files are encrypted, and currently unavailable. You can check it: all files on you computer has
extension [REDACTED]
By the way, everything is possible to recover (restore), but you need to follow our instructions.
Otherwise, you cant get back your data (NEVER).

[+] what guarantees? [+]
Its just a business. we absolutely do not care about you and your deals, except getting benefits. If we do
not do our work and liabilities - nobody will cooperate with us. Its not in our interests.
To check the ability of returning files, you should go to our website. There you can decrypt one file for
free. That is our guarantee.
If you will not cooperate with our service - for us, its does not matter. But you will lose your time and
data, cause just we have the private key. In practice - time is much more valuable than money.

[+] How to get access on website? [+]
Using a TOR browser!
- Download and install TOR browser from this site: https://torproject.org/
- Open our website: [REDACTED]
- Follow the on-screen instructions
```

Figure 2—Hades ransomware ransom note

<<< End >>>

The below provides a high-level summary based on analysis of Hades ransomware samples:

- Creates a copy of itself at the path %appdata%\[created folder]\[create file with no extension] with a variable folder and file name.
- Relaunches itself using the command line parameter go
- Deletes itself and its copy using the following command structure where %s is the path to file executable: “cmd /c waitfor /t %u pause /d y & attrib -h "%s" & del "%s" & rd "%s"”
- Unpacks an executable in memory and executes it (i.e., the unpacked Hades sample)
- Deletes shadow copies through “vssadmin.exe Delete Shadows /All /Quiet”
- Traverses local directories and network shares looking for files to encrypt and skips files with specified extensions or strings
- Adds an extension (different for each sample) to files that it encrypts and drops a ransom note with file name “HOW-TO-DECRYPT-[extension].txt”
- As previously noted, the ransom note includes a URL to a TOR site for ransom instructions

In addition, based on significant code overlap found in Hades samples with other known variants, Crowdstrike assesses that the new variant is a successor to WastedLocker ransomware and possibly linked to Evil Corp operations.

Compromise activity & detection opportunities

Initial access

The primary method for initial access into the victim’s network appears to be internet-facing systems via Remote Desktop Protocol (RDP) or Virtual Private Network (VPN) using legitimate credentials.

Persistence

The use of legitimate credentials, service creation, and distribution of Command and Control (C2) beacons across victim environments through the use of Cobalt Strike and Empire, so far appear to be the predominant approach used by the unknown threat group to further their foothold and maintain persistence. In addition, the threat actors operated out of the root of C:\ProgramData where several executables tied to the intrusion set were found.

Privilege escalation

Credential harvesting and subsequent privilege escalation achieved through the use of tooling and manual enumeration of credentials.

Defense evasion

Impeding defenses was achieved through use of domain administrator credentials and includes the following:

- Batch script that leverages wevtutil.exe to clear event logs on impacted hosts
- Disabling Anti-Virus (AV) products on endpoints, as well as manually disabling Endpoint Detection & Response (EDR) tools and prevention policies through the user interface
- Modification of Group Policy Object (GPO) to disable windows audit logging

Discovery

Observed multiple methods for internal network reconnaissance, such as various reconnaissance scripts and tools used to collect network, host, and domain information.

Lateral Movement

Lateral movement accomplished via compromised accounts obtained during internal reconnaissance activities. Remote Desktop Protocol (RDP) was also leveraged for host-to-host lateral movement.

Exfiltration & impact

Prior to deploying Hades ransomware, the unknown threat group has employed the 7zip utility to archive data that was then staged and exfiltrated to an attacker-controlled server hosted in Mega[.]nz cloud infrastructure, leveraging the MEGAsync utility. In addition to data theft, actors deploy Hades ransomware to encrypt files identified on the victim network. Hades operators leverage this approach for "double-extortion" tactics.

Mitigation recommendations

- Ensure robust crisis management, incident response and disaster recovery plans are in place in the event of a data breach or ransomware incident.
- Consider developing continuity of operations plans (COOP) that account for ransomware or wiper attacks that can impact business operations.

- Maintain best practices against ransomware, such as patching, firewalling infection vectors, updating anti-virus software, employing a resilient backup strategy (e.g., 3-2-1, 3-2-2, etc.), implementing strict network egress policies, and using application whitelisting where feasible.
- Install and update anti-virus software to proactively identify and protect against malware.
- Consider deploying Endpoint Detection and Response (EDR) across the environment, targeting at least 90% endpoint and workload visibility.
- In addition to a robust password policy, use MFA where possible for authenticating corporate accounts to include remote access mechanisms (e.g., VPNs)
- Secure Remote Desktop Protocol (RDP) connections with complex passwords, virtual private networks (VPNs) and Network Level Authentication (NLA), if RDP connections must be used.
- Patch infrastructure to the highest available level, as threat actors are often better able to exploit older systems with existing vulnerabilities.
- Encrypt data-at-rest where possible and protect decryption keys and technology.
- Do not store credentials in files and scripts on shared locations
- Where possible, deny caching of credentials in memory (e.g., Credential Guard)
- Train users of all systems to positively identify and safely handle e-mails that could be part of a phishing campaign.

MITRE ATT&CK techniques observed

Tactic	Technique
Initial access	T1133: External Remote Services T1078: Valid Accounts
Execution	T1059: Command and Scripting Interpreter T1086: PowerShell T1035: Service Execution
Persistence	T1078: Valid Accounts T1050: New Service
Privilege escalation	T1055: Process Injection T1078: Valid Accounts
Defense evasion	T1078: Valid Accounts T1036: Masquerading T1027: Obfuscated Files or Information T1070: Indicator Removal on a Host T1562: Impair Defenses
Credential access	T1110: Brute Force T1003: Credential Dumping

Discovery	T1083: File and Directory Discovery T1082: System Information Discovery T1087: Account Discovery T1482: Domain Trust Discovery T1135: Network Share Discovery T1069: Permission Groups Discovery T1018: Remote System Discovery T1016: System Network Configuration Discovery
Lateral movement	T1076: Remote Desktop Protocol T1028: Windows Remote Management
Collection	T1005: Data from Local System T1039: Data from Network Shared Drive
Command & control	T1043: Commonly Used Port T1105: Remote File Copy T1071: Standard Application Layer Protocol
Exfiltration	T1002: Data Compressed T1048: Exfiltration Over Alternative Protocol
Impact	T1486: Data Encrypted for Impact T1489: Service Stop

Indicators and detections

We are publishing indicators to help organizations identify both the Unknown Threat Group's TTPs and the Hades Ransomware variant itself. As this is a developing story, additional indicators will be released, when available.

As mentioned before, it should be noted that the threat actors often operated out of the root of C:\ProgramData where several executables tied to the intrusion set were found.

Tactic	Technique
Attacker tooling	PortQuery—Recon Advanced Port Scanner—Recon Cobalt Strike—Lateral Movement, C2 PowerShell Empire MEGAsync—Exfiltration

Attacker infrastructure	185[.]162[.]131[.]99 185[.]250[.]151[.]33 currentteach[.]com newschools[.]info 185[.]63[.]253[.]131 8[.]208[.]22[.]215 82[.]148[.]28[.]9 8[.]208[.]16[.]206 119[.]18[.]58[.]41
Exfiltration	mega[.]nz MEGAsync
Ransomware binary	e657ff4838e474653b55367aa9d4a0641b35378e2e379ad0fdd1631b3b763ef0 ea310cc4fd4e8669e014ff417286da5edf2d3bef20abfb0a4f4951afe260d33d 0dfcf4d5f66310de87c2e422d7804e66279fe3e3cd6a27723225aecf214e9b00 fe997a590a68d98f95ac0b6c994ba69c3b2ece9841277b7fec9dfaa6f589a87

A special thanks to the following individuals who also contributed: Jon Begley, Alison Ali, Curt Wilson, Nancy Strutt, Leo Fernandes, Max Smith and the Accenture Cyber Investigation & Forensic Response (CIFR) team.

Accenture Security

Accenture Security is a leading provider of end-to-end cybersecurity services, including advanced cyber defense, applied cybersecurity solutions and managed security operations. We bring security innovation, coupled with global scale and a worldwide delivery capability through our network of Advanced Technology and Intelligent Operations centers. Helped by our team of highly skilled professionals, we enable clients to innovate safely, build cyber resilience and grow with confidence. Follow us @AccentureSecure on Twitter or visit us at www.accenture.com/security

Accenture, the Accenture logo, and other trademarks, service marks, and designs are registered or unregistered trademarks of Accenture and its subsidiaries in the United States and in foreign countries. All trademarks are properties of their respective owners. All materials are intended for the original recipient only. The reproduction and distribution of this material is forbidden without express written permission from Accenture. The opinions, statements, and assessments in this report are solely those of the individual author(s) and do not constitute legal advice, nor do they necessarily reflect the views of Accenture, its subsidiaries, or affiliates. Given the inherent nature of threat intelligence, the content contained in this report is based on information gathered and understood at the time of its creation. It is subject to change. Accenture provides the information on an “as-is” basis without representation or warranty and accepts no liability for any action or failure to act taken in response to the information contained or referenced in this report.

Copyright © 2021 Accenture. All rights reserved.



Eric Welling

Security Delivery Senior Manager

As the CIFR North American lead, Eric helps clients prevent and recover from cyber critical incidents.

Follow me:



Jeff Beley

Security Innovation Principal

Jeff has 20 years of IT experience with a focus on infosec. He is a senior incident response and threat hunt lead on the CIFR team.

Follow me:



Ryan Leininger

Senior Manager – Accenture Security

Follow me:



Accenture Cyber Threat Intelligence

Subscribe to Accenture's Cyber Defense Blog [Subscribe to Accenture's Cyber Defense Blog](#)

[Subscribe](#)
