HADES ransomware operators continue attacks

JUNE 29, 2021

SHARE

RISE FROM THE ASHES! HADES RANSOMWARE OPERATORS CONTINUE TO PROLIFERATE ATTACKS, DEPLOYING NEW VARIANTS ALONG THE WAY.

Accenture Security – Cyber Investigations, Forensic & Response (CIFR), Accenture Cyber Threat Intelligence (ACTI)

Executive Summary

- In March 2021, Accenture Security identified a previously unknown financially motivated threat group using the self-proclaimed Hades ransomware variant in cybercrime operations that impacted multiple victims.
- Since the March reporting, additional victims have been targeted in the consumer goods & services, insurance, and manufacturing & distribution industry verticals.
- Accenture security assesses with a moderate-to-high level of confidence that in addition to the Hades variant, the threat group has added at least one new ransomware variant to their arsenal, Phoenix Cryptolocker, possibly to deter attribution claims or campaign links.
- Tactics, Techniques and Procedures (TTPs) employed by the threat group have remained relatively consistent over time, including significant overlap in intrusion sets across known victims.
- However, some unique and destructive actions were observed across intrusions, such as targeted enumeration of cloud environments and destruction of cloud-native backups or snapshots.

- Accenture Security assesses with moderate confidence that the threat group does not operate under an affiliate-based model or ransomware as a service (RaaS) operation.
- While previous industry reporting by Crowdstrike and SecureWorks attribute the operations to Evil Corp and Gold Winter respectively, Accenture Security is not yet able to confidently make attribution claims based on observed intrusion clusters.

The information outlined in this blog is based on collection from CIFR incident response engagements, threat intelligence insights, Open-Source Intelligence (OSINT), and various media and industry reports.

This is a developing story; additional technical analysis of the intrusion clusters, attacker TTPs and Indicators of Compromise (IOCs) will be released to the community in a separate blog post.

Summary & timeline update

Accenture Security assesses with a moderate-to-high level of confidence that a previously reported unknown threat group is now using multiple ransomware variants in cybercrime operations that have impacted at least seven (7) victims. Based on collection sources, the threat group has been in operations since at least December 2020 and has continued to target victims through May 2021. Accenture Security also analyzed the group's activities in the context of attribution, victimology, and TTPs employed based on collection from industry publications, OSINT and incident response data. Accenture Security assesses the group's operations are well underway, and their activity will likely continue to proliferate into the foreseeable future, impacting additional carefully selected victims.

Victimology update

Based on our collection sources, we are currently aware of at least seven (7) victims spanning multiple industry verticals. Consistent with previous reporting, all known victims are large multi-national organizations with annual revenues exceeding $1 billion USD. The profiles of the known victims continue to be a consistent indicator of Big Game Hunting, with target selection and deployment methods aimed toward high-value payouts.

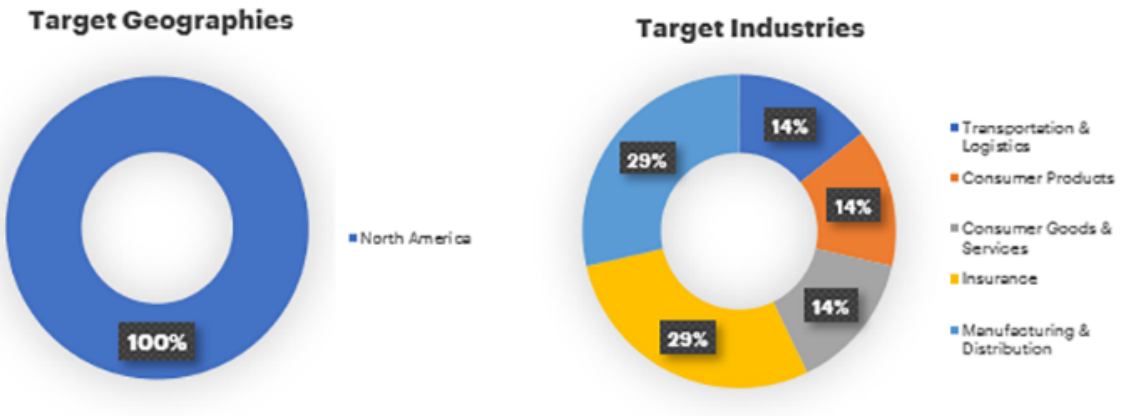

Figure 1 – Target Geographies & Industries

Commonalities across intrusions

Despite the numerous similarities in the potentially linked intrusion sets described herein, there are very few similarities between the victims themselves beyond geography. This includes few overlaps in industry vertical, political ideology, or public status.

As previously noted, the most significant commonality between victims is that they all fall into the category of “big game ransomware targets”[12], large companies with the perceived ability to pay larger ransoms demanded by the threat actors.
In all cases, the threat actors used a relatively standard toolkit with only minor variations, including but not limited to the following:

- Credential access via VPN and SocGholish malware delivered via a malicious Google Chrome update were found to be the primary infection vectors across victims.
- Advanced IP scanner was utilized for reconnaissance.

- PSexec was used for lateral movement and deployment of the ransomware.
- The threat actors also made heavy use of Remote Desktop Protocol (RDP) for lateral movement.
- Mimikatz was used for credential access.
- Similar batch files used to disable Microsoft Windows Defender and other antivirus software, stop services and clear even logs.
- Threat actors often operated out of the root of C:ProgramData where several executables tied to the intrusion set were found.
- Consistent use of Cobalt Strike.
- Commonalities in C2 domains were found across intrusions.
- In at least two (2) intrusions, targeted destruction of backups prior to encryption.
- 7zip utility was used to archive data that was then staged and exfiltrated to an attacker-controlled server hosted in Mega[.]nz cloud infrastructure, leveraging the MEGAsync utility.

Hades ransomeware operations

Accenture Security assesses that careful target selection and a unique approach to victim communication, combined with a “lone wolf” approach, also may explain the relatively low number of known victims since Hades was first identified publicly in December 2020. Lone wolf ransomware groups typically operate outside of the affiliate-based model and don’t consistently participate in RaaS operations. However, this doesn’t necessarily mean they are not a well-resourced group in and of themselves. In addition, consistent with analysis published by SecureWorks, the ACTI team did not identify related activity on underground forums and criminal marketplaces, further supporting our assessment.

Based on updated 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. This includes multi-million-dollar (USD) ransom demands, and in at least two (2) instances, successful payment. However, while portions of each intrusion chain may seem “novel” in nature, their approach suggests a moderate level of operational and technical sophistication, as the operators leverage a mostly standard toolkit and often use “noisy” approaches for reconnaissance. In at least one instance, the targeted

organization successfully deterred the attack before impact, so the intended action on objectives are unknown.

Compromise Activity & Detection Opportunities

Initial Access
The primary methods for initial access into the victim's network includes internet-facing systems via Remote Desktop Protocol (RDP) or Virtual Private Network (VPN) using legitimate credentials, as well as SocGholish malware delivered via fake Chrome browser updates.

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, seem to be the predominant approach used by the threat group to further their foothold and maintain persistence.
In addition, consistent with previous reporting, 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 to include mimikatz and manual enumeration of credentials found within files.

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
- Modification of GPO to disable windows audit logging
- Manually disabling Endpoint Detection & Response (EDR) tools and prevention policies through the user interface

Discovery
Observed multiple methods for internal network reconnaissance, including various

reconnaissance scripts and tools such as Advanced Port Scanner 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) and PSexec were also leveraged for host-to-host lateral movement.

In one incident, the threat actor installed a custom build of Chrome.exe and leveraged the native browser capabilities to manually target the victim's cloud environments. This activity included enumeration of high-value accounts and targeted destruction of data and backups through the cloud management console.

In addition, the attempted use of KeeThief for lateral movement was observed. This tool is often used by threat actors to abuse credentials stored in KeePass databases. Specifically, threat actors deployed an instance of KeeThief.ps1—an open-source PowerShell package written in 2016 designed to compromise credentials stored in memory on a system with an open KeePass database.

Command and Control
In most of the recent incidents, the threat actors utilized the ubiquitous Cobalt Strike post-exploitation framework for command and control within the impacted environments with at least two (2) external beacons per environment. Command and control was also established using remote manipulator system [3](RMS).

Exfiltration & Impact
Prior to deploying 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 ransomware with PSexec to encrypt files identified on the victim network. The operators leverage this approach for "double-extortion" tactics.

Mitigation recommendations

- Ensure a robust crisis management and incident response plan 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 spread across the business.
- Employ a resilient backup strategy and architecture using a “no-silo” approach.
- Avoid opening or downloading suspicious links from external sources until confirming legitimacy.
- Maintain best practices against ransomware, such as patching, updating anti-virus software, implementing strict network egress policies, and using application whitelisting where feasible.
- Install and update anti-virus software to proactively identify and protect against malware.
- Deploy Endpoint Detection and Response (EDR) across the environment, targeting at least 90% workload visibility.
- Employ a strong corporate password policy.
- Use MFA where possible for authenticating corporate accounts to include remote access mechanisms and security tools. Admin accounts should be cross-platform MFA enforced.
- 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 related keys and technology.
- Do not store credentials in files and scripts on shared locations.
- Close password management applications after use.
- Where possible, deny caching of credentials in memory (e.g., Credential Guard).
- Hunt for attacker TTPs to proactively detect and respond to a ransomware attack in order to mitigate impact.

MITRE ATT&CK techniques observed

Tactic	Technique
Initial access	T1133: External Remote Services T1078: Valid Accounts T1189: Drive-by Compromise

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

If you have an incident or need additional information on ways to detect and respond to cyberthreats, contact a member of our CIFR team 24/7/365 by phone 888-RISK-411 or email CIFR.hotline@accenture.com

[1]https://arstechnica.com/information-technology/2019/10/fbi-warns-of-major-ransomware-attacks-as-criminals-go-big-game-hunting/ [2]https://www.ic3.gov/Media/Y2019/PSA191002

[3]https://malpedia.caad.fkie.fraunhofer.de/details/win.rms

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

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.