ultraviolet

THREAT REPORT:

RansomHub Ransomware

Services Performed By:
UltraViolet Cyber
Casey Latham
(443) 351-7630
info@uvcyber.com

Published Date:
June 13, 2024

Contents

1 Executive Summary

RansomHub is a threat actor group offering a Ransomware-as-a-Service (RaaS) business model to affiliates for quick entry into, or expansion in, cybercrime. Regardless of the possibility of RansomHub being a re-branded operation, they have hit the cybercrime scene fast and hard. Already, they have reportedly successfully attacked several large organizations with Ransomware, ending in extortion for the victims. The Ransomware-as-a-service business model allows RansomHub to grow due to the low barrier of entry. The growth and availability of ransomware from RansomHub is a cause for alarm for all organizations and enterprises.

2 Technical Analysis

RansomHub is possibly a re-branded threat actor group coming out of the Knight ransomware gang. The Register reports that their activity over the last three months has grown exponentially.[i] Recent attacks include Christie's Auction House, Telco and healthcare companies. Utilizing the RaaS business model allows any bad actor to purchase the ransomware service and quickly get up and running. This can be defined as an affiliate model.

The RansomHub ransomware has been observed "… abusing the ZeroLogon elevation-of-privilege vulnerability (CVE-2020-1472) in Microsoft's netlogon remote protocol…"[ii] for initial entry. However, no ransomware attack protection or identification should be limited to one attack vector. Once entry is established the bad actors will utilize legitimate tools to map out the victim's network and devices. This is a common way for bad actors to leverage intelligence, as companies utilize the same software internally in some cases. This makes the network traffic appear legitimate.

Even with legitimate traffic, Enterprises can still detect a malicious file within a network. Unfortunately, RansomHub already thought of that and is reportedly utilizing Gobfuscate to hide its malicious code.[iii] This makes detection of the code difficult, and Ransom Hub's current success is evidence of that. Once the ransomware is deployed on a device, encryption begins. After encryption, an insidious extortion note is dropped on the victim machine.

Symantec researchers have pointed out a very alarming fact while investigating and releasing information about RansomHub's ransomware. Symantec states, "A unique feature present in both Knight and RansomHub is the ability to restart an endpoint in safe mode before starting encryption."[iv] Unique indeed. This means that security controls, like anti-virus, will not be loaded while the ransomware is completing its operations, allowing for a smooth encryption operation.

The growth of RansomHub is alarming because their RaaS solution has been verified effective, as evidenced by the recent successful and newsworthy attacks. The safe mode operations of the ransomware make it especially lethal. The affiliate model, still growing in bad actor circles, allows for a low barrier to entry which enables cybercrime groups to expand quickly. Enterprises need to equip their organizations with robust perimeter defenses and educate users about the dangers of opening any unknown files.

3 What UltraViolet Cyber is Doing

- UltraViolet Cyber regularly updates our IOC database to ensure alerting is up to date
- Monitoring commands that are associated with malicious activity from threat actors
- Monitoring network logs for traffic to known malicious sites

4 What Customers Can Do

- Keep perimeter devices up to date with firmware and detections
- Educate users on ransomware and the dangers of opening unknown files
- Develop or maintain a ransomware recovery strategy

5 References

Lyons, J. (2024, June 5). What is RansomHub? Looks like a Knight ransomware reboot. *The Register*. https://www.theregister.com/2024/06/05/ransomhub_knight_reboot/

RansomHub: New Ransomware has Origins in Older Knight. (2024, June 5). Symantec Enterprise Blogs. https://symantec-enterprise-blogs.security.com/threat-intelligence/ransomhub-knight-ransomware

Small, Z. (2024, May 30). *After Hack, Christie's Gives Details of Compromised Client Data*. The New York Times. https://www.nytimes.com/2024/05/30/arts/design/christies-hack-client-data.html

[i] Lyons, J. (2024, June 5). What is RansomHub? Looks like a Knight ransomware reboot. The Register. https://www.theregister.com/2024/06/05/ransomhub_knight_reboot/
[ii] Ibid.
[iii] Ibid.
[iv] RansomHub: New Ransomware has Origins in Older Knight. (2024, June 5). Symantec Enterprise Blogs. https://symantec-enterprise-blogs.security.com/threat-intelligence/ransomhub-knight-ransomware