HUNTER

EMERGING THREATS

RANSOMHUB RANSOMWARE

RansomHub Ransomware is a malware strain that first emerged in early February 2024. Operating as a RaaS (or Ransomware-as-a-Service), the actor â€œkoley" announced the RansomHub affiliate program on the infamous RAMP cybercriminal forum on February 2nd. The affiliate program entices operators with high commission rates and a wealth of tools, infrastructure and guidance, allowing the less experienced individuals a chance to produce results. Due to the nature of Ransomware-as-a-Service programs, victims have included a myriad of industries and entities. It is worthy to note that operators are instructed not to target systems in China, Cuba, North Korea, Romania and Commonwealth of Independent States countries. The **RansomHub** group has claimed to be responsible for a significantly large number of organizations across the globe, with a large percentage impacting entities within North America and Europe.

THREAT SUMMARY

RansomHub Ransomware is a malware strain that first emerged in early February 2024. Operating as a RaaS (or Ransomware-as-a-Service), the actor â€œkoley" announced the RansomHub affiliate program on the infamous RAMP cybercriminal forum on February 2nd. The affiliate program entices operators with high commission rates and a wealth of tools, infrastructure and guidance, allowing the less experienced individuals a chance to produce results. Due to the nature of Ransomware-as-a-Service programs, victims have included a myriad of industries and entities. It is worthy to note that operators are instructed not to target systems in China, Cuba, North Korea, Romania and Commonwealth of Independent States countries. The **RansomHub** group has claimed to be responsible for a significantly large number of organizations across the globe, with a large percentage impacting entities within North America and Europe.

The malware itself is written in Golang and C++ and leverages advanced evasion techniques and multi operating system support - including Windows, Linux, and VMware ESXi operating systems. Researchers hypothesize that **RansomHub** could be a successor to the Knight Ransomware strain, which was offered for sale on dark web forums in February of 2024 - additionally, there are numerous similarities identified between the two ransomware strains. Recently in August 2024, the **RansomHub** threat group has implemented a new tool in their attacks, dubbed â€œEDRKillShifterâ€. This tool is built to stealthily disable EDR or security tooling installed on a victimâ€™s system and helps operators take control of the system. With the variant continuously evolving, and attacks utilizing **RansomHub** ransomware growing rapidly, it is important to assess, understand and prepare for this malware in our environments.

Intel 471 References:

[TITAN Service Profile: RansomHub ransomware-as-a-service]
(https://titan.intel471.com/report/fintel/83f391baee9c4b57ba3ac7050ab6fc97)

[TITAN Breach Report: Ransomware breach claims reviewed - July 2024]
(https://titan.intel471.com/report/fintel/5cafbab349e6df5044046248695ed3ea)

SYNOPSIS

RansomHub ransomware emerged in February of 2024 as a new Ransomware-as-a-Service (RaaS) and has rapidly become one of the most prolific ransomware strains in the wild. The malware operates pretty similarly to other ransomware strains, however what sets itself apart from other types is its advanced evasion techniques and multi operating system support (which includes Windows, Linux and VMware ESXi). **RansomHub** has been observed to achieve initial access through phishing emails, exploited vulnerabilities, leveraging compromised credentials or even brute force attacks.

After access is achieved, operators execute obfuscated commands and script files that disable antivirus and EDR software to evade detection. A recent tool that has been implemented is the EDRKillShifter binary that loads a legitimate, vulnerable driver that can be exploited and is designed to disable active EDR process and service from a privileged state. **RansomHub** also abuses PsExec and the smbexec.py tool from the impact python suite to move laterally in the compromised environment, as well as tools such as Advanced Port Scanner for reconnaissance.

Operators of **RansomHub** utilize the double-extortion model, which means they will not only encrypt compromised systems, but also threatens to sell or release data that is exfiltrated during the infection. Therefore, after encryption is completed, encrypted files will have a random string of characters appended to their file names and ransom note provided via .txt file. The malware also includes an uncommon ability to restart a victimâ€™s machine in safe mode before the encryption even begins. It is also worthy to note that the malware inhibits system recovery by the deletion or modification of shadow copies via PowerShell.

HUNT PACKAGES

DRIVER FILE CREATED IN TEMP DIRECTORY - POTENTIAL MALWARE INSTALLATION
https://hunter.cyborgsecurity.io/research/hunt-package/120bf3d2-ab6b-4254-b313-4b543e91c177

POWERSHELL COMMAND USED TO STOP VM ON HYPER-V HOST - POTENTIAL RANSOMWARE PRECURSOR
https://hunter.cyborgsecurity.io/research/hunt-package/4d8a68de-c019-400d-93da-9d523a47d9de

UNIQUELY NAMED DRIVER WRITES WITH FILENAMES BETWEEN 4-10 CHARACTERS - POTENTIAL TERMINATOR DRIVER WRITE
https://hunter.cyborgsecurity.io/research/hunt-package/82c57ee1-546f-4727-ad2c-efb909fd0805

WEVTUTIL CLEARED LOG
https://hunter.cyborgsecurity.io/research/hunt-package/7ceada06-54e2-4b44-9dca-b4e8d4ba401d

INTERNET INFORMATION SERVICES RESET VIA CMD - POTENTIAL RANSOMWARE STAGING
https://hunter.cyborgsecurity.io/research/hunt-package/cff6d39a-43c0-4e3b-8618-15587e739319

POWERSHELL MODULE REMOVE-CIMINSTANCE TO DELETE SHADOW COPIES - POTENTIAL RANSOMWARE PRECURSOR
https://hunter.cyborgsecurity.io/research/hunt-package/a66962e7-a44c-47ff-b027-31fc6943ddda

RELATED LINKS
Sign up for free HUNTER access
RansomHub Ransomware Emerging Threat Collection

MITRE CONTEXT

- Tactic Names:
  - Command and Control
  - Privilege Escalation
  - Defense Evasion
  - Persistence
- Technique Names:
  - Exploitation for Defense Evasion
  - Ingress Tool Transfer
  - Kernel Modules and Extensions
  - Exploitation for Privilege Escalation
- Threat Names:
  - RansomHub Ransomware

REFERENCES

1. https://titan.intel471.com/report/fintel/83f391baee9c4b57ba3ac7050ab6fc97
2. https://titan.intel471.com/report/fintel/5cafbab349e6df5044046248695ed3ea
3. https://symantec-enterprise-blogs.security.com/threat-intelligence/ransomhub-knight-ransomware
4. https://www.forescout.com/blog/analysis-a-new-ransomware-group-emerges-from-the-change-healthcare-cyber-attack/
5. https://www.darkreading.com/endpoint-security/ransomhub-rolls-out-brand-new-edr-killing-byovd-binary
6. https://www.bleepingcomputer.com/news/security/ransomware-gang-deploys-new-malware-to-kill-security-software/