2024-05-15

HUNTER

EMERGING THREATS

BLACK BASTA RANSOMWARE AND THREAT GROUP

Black Basta Ransomware and Threat Group (originally seen in 2022) is known to encrypt files on a victim's computer or network, and hold data "ransom" until the victim pays the attacker for the decryption key/software. Further, the group utilizes a double extortion tactic - which means that after the data is encrypted and held ransom, there also exists a threat of publishing the data (which was exfiltrated before encryption) to the public. Financially motivated and Russian-speaking, **Black Basta** operates under the Ransomware-as-a-Service (RaaS) model and has targeted many countries worldwide; including the United States, Japan, Australia, The United Kingdom, Canada and New Zealand.

CYBORG SECURITY

THREAT SUMMARY

Black Basta Ransomware and Threat Group (originally seen in 2022) is known to encrypt files on a victim's computer or network, and hold data "ransom" until the victim pays the attacker for the decryption key/software. Further, the group utilizes a double extortion tactic - which means that after the data is encrypted and held ransom, there also exists a threat of publishing the data (which was exfiltrated before encryption) to the public. Financially motivated and Russian-speaking, **Black Basta** operates under the Ransomware-as-a-Service (RaaS) model and has targeted many countries worldwide; including the United States, Japan, Australia, The United Kingdom, Canada and New Zealand.

On May 10, 2024, a joint report from CISA (Cybersecurity & Infrastructure Security Agency) and the FBI (Federal Bureau of Investigation) was released, detailing the major activity from the **Black Basta** ransomware threat group between April 2022 and May 2024. During this time period, the threat group targeted over 500 entities across North America, Europe and Australia (the report noting they affected 12 out of 16 critical infrastructure sectors). The report highlighted the increased risk to healthcare organizations, with researchers observing an increase in attacks targeting the sector due to their size and potential impact. The joint report was released in collaboration with HHS (Department of Health and Human Services Services) and MS-ISAC (Multi-State Information Sharing and Analysis Center), and provided TTPs (Tactics, Techniques and Procedures) and IOCs (Indicators of Compromise) that were. identified to be used in the wild.

SYNOPSIS

Black Basta Ransomware, operating under a RaaS (Ransomware as a Service) model and first identified in 2022, employs TTPs (Tactics, Techniques and Procedures) that begin with typical initial access techniques - such as phishing emails that contain malicious attachments or links, compromised websites or exploitation of known vulnerabilities. Recently, a **Black Basta** affiliate has been observed to send an overwhelming amount of spam emails to victims, which transitions to the malicious actors to make calls to the victims posing as IT staff. During the conversation, they offer help with the spam emails and ask the victim to download a remote support tool - if successful and with access to the victimâ€™s machine, the malicious actor runs script(s) masquerading as software updates.

After initial access is obtained, **Black Basta** operators have been observed to perform network scans and reconnaissance - specifically mentioned in the CISA report, SoftPerfect (netscan.exe) in order to survey the network. Other techniques that have been observed by researchers include usage of BITSAdmin and PsExec in order to conduct lateral movement, as well as other tools such as Splashtop, Screen Connect, and Cobalt Strike beacons to assist. Additionally, the CISA report mentions operator usage of Mimikatz for credential scraping and privilege escalation.

Subsequently, actors have been observed to use Rclone and/or WinSCP for file exfiltration before the encryption of data across local and network drives begins. Actors then disable antivirus products (in some instances using a tool called Backstab) in order to mitigate any interferences and begin encrypting files - appending **â€œ.bastaâ€** to files encrypted and dropping ransom notes containing instructions to contact the group via a specified URL. After completion, operators have been observed to delete volume shadow copies via â€œvssadmin.exeâ€ and to prevent system recovery.

HUNT PACKAGES

SUSPICIOUS SCHEDULED TASK CREATED – EXECUTION DETAILS CONTAINS SCRIPTING REFERENCE
https://hunter.cyborgsecurity.io/research/hunt-package/9a4fa42f-57dd-4449-b0c0-a1dd0976b17a

AUTORUN OR ASEP REGISTRY KEY MODIFICATION
https://hunter.cyborgsecurity.io/research/hunt-package/8289e2ad-bc74-4ae3-bfaa-cdeb4335135c

MICROSOFT DEFENDER ANTIVIRUS DISABLED VIA REGISTRY KEY MANIPULATION (POWERSHELL SCRIPTBLOCK LOGGING DETECTION)
https://hunter.cyborgsecurity.io/research/hunt-package/988a4e5f-1968-43f2-9c91-f316cf031707

POTENTIAL ABUSE OF BUILT-IN NETWORK TOOLS FOR NETWORK AND CONFIGURATION DISCOVERY
https://hunter.cyborgsecurity.io/research/hunt-package/4e5b3d8c-fa7a-40ec-a966-5229d8df38e6

POTENTIAL EXFILTRATION – COMMON RCLONE ARGUMENTS
https://hunter.cyborgsecurity.io/research/hunt-package/f075c217-783e-459a-aeb4-42ea91e07af7

LIVING OFF THE LAND TECHNIQUE – ESENTUTL.EXE
https://hunter.cyborgsecurity.io/research/hunt-package/dd2fd4e0-dab9-47cd-b1ba-8aa3b63a7af9

EXCESSIVE WINDOWS DISCOVERY AND EXECUTION PROCESSES – POTENTIAL MALWARE INSTALLATION
https://hunter.cyborgsecurity.io/research/hunt-package/6d1c9f13-e43e-4b52-a443-5799465d573b

USAGE OF CHMOD TO ENABLE EXECUTION – POTENTIAL PAYLOAD STAGING
https://hunter.cyborgsecurity.io/research/hunt-package/dfbdc565-a37c-472b-a4c7-6c0e5325b255

RUNDLL32 RUN WITHOUT ARGUMENTS
https://hunter.cyborgsecurity.io/research/hunt-package/f4e1ba57-3c1f-44ce-a320-f3e61a7ed389

SUSPICIOUS SCHEDULED TASK CREATED – ENCODED POWERSHELL PAYLOAD EXECUTED FROM REGISTRY
https://hunter.cyborgsecurity.io/research/hunt-package/709d156f-5712-4854-833c-659acaa52b28

ATERA AGENT UTILIZED FOR UNAUTHORIZED REMOTE ACCESS
https://hunter.cyborgsecurity.io/research/hunt-package/b479f6b2-b14c-4667-be40-6ec310dbd934

RDP ENABLED VIA NETSH
https://hunter.cyborgsecurity.io/research/hunt-package/6322023c-8874-41f2-aa0b-c6600d47398c

SUSPICIOUS BCDEDIT ACTIVITY – POTENTIAL RANSOMWARE
https://hunter.cyborgsecurity.io/research/hunt-package/8a4f0a60-2b55-4dfd-8788-8691e11e1ca1

LOCAL DATA STAGING – ADFIND.EXE
https://hunter.cyborgsecurity.io/research/hunt-package/1fe16ece-e03d-444e-bebc-fcd2bab5c974

MICROSOFT DEFENDER ANTIVIRUS DISABLED VIA REGISTRY KEY MANIPULATION
https://hunter.cyborgsecurity.io/research/hunt-package/81d218e6-0c53-42c4-9275-4aac0eef5bc6

SUSPICIOUS CHILD PROCESS – CALC.EXE
https://hunter.cyborgsecurity.io/research/hunt-package/C6455152-2801-4060-A060-F9250CB87C5A

SHADOW COPIES DELETION USING OPERATING SYSTEMS UTILITIES
https://hunter.cyborgsecurity.io/research/hunt-package/2e3e9910-70c1-4822-804a-ee9919b0c419

REGSVR32 RUNNING FILES FROM TEMP DIRECTORIES
https://hunter.cyborgsecurity.io/research/hunt-package/6d3f3c9e-0a8a-4d8c-9c1c-369ae94d3aad

RELATED LINKS
Sign up for free HUNTER access
Black Basta Ransomware and Threat Group Emerging Threat Collection

MITRE CONTEXT

- Tactic Names:
  - Defense Evasion
  - Execution
  - Command and Control
  - Initial Access
  - Privilege Escalation
  - Exfiltration
  - Impact
  - Discovery
  - Persistence
- Technique Names:
  - Registry Run Keys / Startup Folder
  - Hide Artifacts
  - Remote Access Software
  - Disable or Modify Tools
  - Regsvr32
  - Remote System Discovery
  - Disable or Modify System Firewall
  - Exfiltration Over Alternative Protocol
  - NTFS File Attributes
  - Rundll32
  - External Remote Services
  - Inhibit System Recovery
  - System Network Configuration Discovery
  - Linux and Mac File and Directory Permissions Modification
  - Scheduled Task
  - Portable Executable Injection
  - Ingress Tool Transfer

REFERENCES

1. https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-131a
2. https://thehackernews.com/2024/05/black-basta-ransomware-strikes-500.html
3. https://malpedia.caad.fkie.fraunhofer.de/details/win.blackbasta
4. https://www.hhs.gov/sites/default/files/black-basta-threat-profile.pdf
5. https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-blackbasta