March 4, 2025

EMERGING THREATS

Black Basta

UPDATE 03/04/2025: A significant leak of internal chat logs from within Black Basta ransomware group has provided the community with a glimpse into their operations, including further information regarding their capabilities, tools and motivations. It was released via JSON file on February 11, 2024 by a Telegram user named ExploitWhispers, and contained around 200,000 chat messages dated between September 2023 and June 2024. Black Basta is considered one of the most impactful Ransomware groups of recent years, and this event rivals the 2022 leaks that affected the Conti ransomware gang in 2022. With newly discovered information uncovered due to these leaks, threat hunters at Intel 471 have updated the collection with newly uncovered TTPs (Tactics, Techniques and Procedures).

THREAT SUMMARY

UPDATE 03/04/2025: A significant leak of internal chat logs from within Black Basta ransomware group has provided the community with a glimpse into their operations, including further information regarding their capabilities, tools and motivations. It was released via JSON file on February 11, 2024 by a Telegram user named ExploitWhispers, and contained around 200,000 chat messages dated between September 2023 and June 2024. Black Basta is considered one of the most impactful Ransomware groups of recent years, and this event rivals the 2022 leaks that affected the Conti ransomware gang in 2022.

With newly discovered information uncovered due to these leaks, threat hunters at Intel471 have updated the collection with the following TTPs (Tactics, Techniques and Procedures):

- Reconnaissance via Discovery tools (such as ifconfig.exe, netstat.exe, ping.exe) and WMIC abuse
- Defense Evasion with the utilization of temp directories, abuse of the BITS (Background Intelligent Transfer Service) component, and tampering of Windows Defender
- Credential access with the usage of the Mimikatz tool
- Command and Control access provided via the AnyDesk application
- PowerShell abuse for the downloading of files and execution
- Data exfiltration taking place through Rclone utility usage
- Persistence achieved via Schedule Task creation

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.

Intel 471 References:

Malware Campaign: The pursuit of alternatives to QBot: Actor Tramp pushes campaigns featuring Bokbot, DarkGate, Pikabot loaders

Malware Campaign: Qbot returns with new lures and links to Black Basta

Actor builds team to conduct ransomware attacks, seeks reliable operators

Actor continues to provide underground call service for ransomware operators, reveals methods; Possibly engaged in Black Basta ransomware operations

Actor builds team to conduct ransomware attacks, claims to operate ALPHV aka BlackCat, BlackSuit, Black Basta, LockBit malware

Black Basta (aka BlackBasta) ransomware group members reveal operational details

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 victim\u2019s 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 ".basta" 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 "vssadmin.exe" and to prevent system recovery.

RELATED HUNT PACKAGES

Rclone Activity - Potential Data Exfiltration

https://hunter.cyborgsecurity.io/details/use-case/7b8b354f-8f5b-41ba-bc26-786dcaae6439

Suspicious Scheduled Task Created - Execution Details Contains Scripting Reference

https://hunter.cyborgsecurity.io/details/use-case/9a4fa42f-57dd-4449-b0c0-a1dd0976b17a

WMIC Windows Internal Discovery and Enumeration

https://hunter.cyborgsecurity.io/details/use-case/bc0fd59c-4217-46a7-a167-764727118567

Autorun or ASEP Registry Key Modification

https://hunter.cyborgsecurity.io/details/use-case/8289e2ad-bc74-4ae3-bfaa-cdeb4335135c

Microsoft Defender Antivirus Disabled via Registry Key Manipulation (Powershell ScriptBlock Logging Detection)

https://hunter.cyborgsecurity.io/details/use-case/988a4e5f-1968-43f2-9c91-f316cf031707

Powershell Command Used to Stop VM on Hyper-V Host - Potential Ransomware Precursor

https://hunter.cyborgsecurity.io/details/use-case/4d8a68de-c019-400d-93da-9d523a47d9de

Potential Abuse of Built-in Network Tools for Network and Configuration Discovery

https://hunter.cyborgsecurity.io/details/use-case/4e5b3d8c-fa7a-40ec-a966-5229d8df38e6

Potential Exfiltration - Common Rclone Arguments

https://hunter.cyborgsecurity.io/details/use-case/f075c217-783e-459a-aeb4-42ea91e07af7

Living Off The Land Technique - Esentutl.exe

https://hunter.cyborgsecurity.io/details/use-case/dd2fd4e0-dab9-47cd-b1ba-8aa3b63a7af9

Excessive Windows Discovery and Execution Processes - Potential Malware Installation

https://hunter.cyborgsecurity.io/details/use-case/6d1c9f13-e43e-4b52-a443-5799465d573b

Mimikatz Non-Interactive Execution

https://hunter.cyborgsecurity.io/details/use-case/9d76a729-5c52-46e4-980c-221fe6f089a0

Usage of chmod to Enable Execution - Potential Payload Staging

https://hunter.cyborgsecurity.io/details/use-case/dfbdc565-a37c-472b-a4c7-6c0e5325b255

Rundll32 Run Without Arguments

https://hunter.cyborgsecurity.io/details/use-case/f4e1ba57-3c1f-44ce-a320-f3e61a7ed389

Remote Services - SMB Share mounts/admin shares/scanning

https://hunter.cyborgsecurity.io/details/use-case/29b036ae-4879-4509-a0ac-65d46ea76cf1

Microsoft Defender Antivirus Disabled via Registry Key Manipulation (CommandLine Execution)

https://hunter.cyborgsecurity.io/details/use-case/6e56bf47-7f67-4cba-b71c-323d831bf68c

Suspicious Scheduled Task Created - Encoded PowerShell Payload Executed From Registry

https://hunter.cyborgsecurity.io/details/use-case/709d156f-5712-4854-833c-659acaa52b28

Atera Agent utilized for Unauthorized Remote Access

https://hunter.cyborgsecurity.io/details/use-case/b479f6b2-b14c-4667-be40-6ec310dbd934

RDP Enabled Via NETSH

https://hunter.cyborgsecurity.io/details/use-case/6322023c-8874-41f2-aa0b-c6600d47398c

Remote WMI Command Attempt

https://hunter.cyborgsecurity.io/details/use-case/9f2e163b-4f26-4972-b3d5-31c0b24b98a0

Suspicious bcdedit Activity - Potential Ransomware

https://hunter.cyborgsecurity.io/details/use-case/8a4f0a60-2b55-4dfd-8788-8691e11e1ca1

Local Data Staging - ADFind.exe

https://hunter.cyborgsecurity.io/details/use-case/1fe16ece-e03d-444e-bebc-fcd2bab5c974

Excessive Windows Discovery CommandLine Arguments - Potential Malware Installation

https://hunter.cyborgsecurity.io/details/use-case/8bb5819f-06a4-4e5d-9099-e43115601999

Microsoft Defender Antivirus Disabled via Registry Key Manipulation

https://hunter.cyborgsecurity.io/details/use-case/81d218e6-0c53-42c4-9275-4aac0eef5bc6

Suspicious Child Process - Calc.exe

https://hunter.cyborgsecurity.io/details/use-case/C6455152-2801-4060-A060-F9250CB87C5A

Shadow Copies Deletion Using Operating Systems Utilities

https://hunter.cyborgsecurity.io/details/use-case/2e3e9910-70c1-4822-804a-ee9919b0c419

Regsvr32 Running Files from Temp Directories

https://hunter.cyborgsecurity.io/details/use-case/6d3f3c9e-0a8a-4d8c-9c1c-369ae94d3aad

AnyDesk Execution from Abnormal Folder - Potential Malicious Use of RMM Tool

https://hunter.cyborgsecurity.io/details/use-case/93F71607-F35D-4AA6-AEC9-C2F8A62CBD8A

RELATED LINKS

Black Basta Emerging Threat Collection

MITRE CONTEXT

- Tactic Names:
  - Credential Access
  - Defense Evasion
  - Execution
  - Impact
  - Initial Access
  - Discovery
  - Persistence
  - Collection
  - Lateral Movement
  - Command and Control
  - Exfiltration
- Technique Names:
  - Exfiltration Over Alternative Protocol
  - Regsvr32
  - System Network Configuration Discovery
  - Service Stop
  - External Remote Services
  - Ingress Tool Transfer
  - Remote System Discovery
  - NTFS File Attributes
  - Disable or Modify Tools
  - Registry Run Keys / Startup Folder
  - NTDS
  - Scheduled Task
  - Data from Local System
  - Rundll32
  - Windows Management Instrumentation
  - Portable Executable Injection
  - Remote Access Software
  - Linux and Mac File and Directory Permissions Modification
  - LSASS Memory
  - Inhibit System Recovery
  - Exfiltration to Cloud Storage

    - SMB/Windows Admin Shares
    - Disable or Modify System Firewall
- Exploit Vulns:
    - CVE-2024-3400
    - CVE-2021-1675
    - CVE-2021-4436
    - CVE-2023-4966
    - CVE-2021-34527
- Technique IDs:
    - T1562.004
    - T1047
    - T1105
    - T1218.010
    - T1016
    - T1490
    - T1018
    - T1053.005
    - T1219
    - T1222.002
    - T1218.011
    - T1489
    - T1133
    - T1564.004
    - T1003.001
    - T1005
    - T1562.001
    - T1547.001
    - T1003.003
    - T1567.002
    - T1055.002
    - T1048
    - T1021.002

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
6. https://blog.bushidotoken.net/2025/02/blackbasta-leaks-lessons-from-ascension.html