JOINT
CYBERSECURITY
ADVISORY

TLP:CLEAR

Co-Authored by:

Product ID: AA24-131A

November 8, 2024

#StopRansomware: Black Basta

SUMMARY

Note: This joint Cybersecurity Advisory (CSA) is part of an ongoing #StopRansomware effort to publish advisories for network defenders that detail various ransomware variants and ransomware threat actors. These #StopRansomware advisories include recently and historically observed tactics, techniques, and procedures (TTPs) and indicators of compromise (IOCs) to help organizations protect against ransomware. Visit *stopransomware.gov* to see all #StopRansomware advisories and to learn more about other ransomware threats and no-cost resources.

Note: Updates to this advisory, originally published May 10, 2024, include:

- **November 8, 2024:** The advisory was updated to reflect new TTPs employed by Black Basta affiliates, as well as provide current IOCs/remove outdated IOCs for effective threat hunting.

Actions for critical infrastructure organizations to take today to mitigate cyber threats from ransomware:

- Install updates for operating systems, software, and firmware as soon as they are released.
- Require phishing-resistant MFA for as many services as possible.
- Train users to recognize and report phishing attempts.

The Federal Bureau of Investigation (FBI), Cybersecurity and Infrastructure Security Agency (CISA), Department of Health and Human Services (HHS), and Multi-State Information Sharing and Analysis Center (MS-ISAC) (hereafter referred to as the authoring organizations) are releasing this joint CSA to provide information on Black Basta, a ransomware variant whose actors have encrypted and stolen data from at least 12 out of 16 critical infrastructure sectors, including the Healthcare and Public Health (HPH) Sector.

This joint CSA provides TTPs and IOCs obtained from FBI investigations and third-party reporting. Black Basta is considered a ransomware-as-a-service (RaaS) variant and was first identified in April 2022. Black Basta affiliates have impacted a wide range of businesses and critical infrastructure in North America,

To report suspicious or criminal activity related to information found in this joint Cybersecurity Advisory, contact your local FBI field office or CISA's 24/7 Operations Center at Report@cisa.gov or (888) 282-0870. When available, please include the following information regarding the incident: date, time, and location of the incident; type of activity; number of people affected; type of equipment used for the activity; the name of the submitting company or organization; and a designated point of contact. SLTT organizations should report incidents to MS-ISAC (866-787-4722 or SOC@cisecurity.org).

Europe, and Australia. As of May 2024, Black Basta affiliates have impacted over 500 organizations globally.

Black Basta affiliates use common initial access techniques—such as phishing and exploiting known vulnerabilities—and then employ a double-extortion model, both encrypting systems and exfiltrating data. Ransom notes do not generally include an initial ransom demand or payment instructions. Instead, the notes provide victims with a unique code and instructs them to contact the ransomware group via a `.onion` URL (reachable through the Tor browser). Typically, the ransom notes give victims between 10 and 12 days to pay the ransom before the ransomware group publishes their data on the Black Basta TOR site, Basta News.

Update November 8, 2024:

Recent techniques include email bombing—a tactic used to send a large volume of spam emails—to aid social engineering over Microsoft Teams and trick victim end users into providing initial access via remote monitoring and management (RMM) tools.

Update End

Healthcare organizations are attractive targets for cybercrime actors due to their size, technological dependence, access to personal health information, and unique impacts from patient care disruptions. The authoring organizations urge HPH Sector and all critical infrastructure organizations to apply the recommendations in the Mitigations section of this CSA to reduce the likelihood of compromise from Black Basta and other ransomware attacks. Victims of ransomware should report the incident to their local FBI field office or CISA (see the Reporting section for contact information).

For a downloadable list of IOCs, see:

- AA24-131A (STIX XML, ### KB) (November 2024 Update)
- AA24-131A (STIX JSON, ### KB) (November 2024 Update)
- AA24-131A (STIX XML, 238 KB) (Initial Version)
- AA24-131A (STIX JSON, 181 KB) (Initial Version)

TECHNICAL DETAILS

Note: This advisory uses the MITRE ATT&CK for Enterprise framework, version 16. See the MITRE ATT&CK Tactics and Techniques section for a table of the threat actors' activity mapped to MITRE ATT&CK® tactics and techniques. For assistance with mapping malicious cyber activity to the MITRE ATT&CK framework, see CISA and MITRE ATT&CK's Best Practices for MITRE ATT&CK Mapping and CISA's Decider Tool.

Initial Access

Black Basta affiliates primarily use spearphishing [T1566] to obtain initial access. According to cybersecurity researchers, affiliates have also used Qakbot during initial access.[1]

Starting in February 2024, Black Basta affiliates began exploiting ConnectWise vulnerability CVE-2024-1709 [CWE-288] [T1190]. In some instances, affiliates have been observed abusing valid credentials [T1078].

Update November 8, 2024:

In May 2024, Black Basta affiliates launched a social engineering campaign in which targeted users were sent a large volume of spam email, often from legitimate sources like website registrations, email subscriptions, and other marketing content. Black Basta affiliates would subsequently call the victim, act as technical support, and offer to fix the issue [T1566.004]. During this process, the actors requested the victim users download a tool for remote access, such as AnyDesk or Microsoft's Quick Assist [T1204]].

In October 2024, this social engineering campaign incorporated the use of Microsoft Teams to contact victims. Black Basta affiliated operators would message the victims from legitimate Microsoft Teams accounts from external organizations, posing as technical support to resolve the email spam issues. Threat actor follow-on objectives remained the same; Black Basta affiliates requested victim users to download tools for allowing remote access.

Update End

Discovery and Execution

Black Basta affiliates use tools such as SoftPerfect network scanner (`netscan.exe`) to conduct network scanning. Cybersecurity researchers have observed affiliates conducting reconnaissance using utilities with innocuous file names such as `Intel` or `Dell`, left in the root drive `C:\` [T1036].[1]

Privilege Escalation

Black Basta affiliates use credential scraping tools like Mimikatz for privilege escalation. According to cybersecurity researchers, Black Basta affiliates have also exploited ZeroLogon (CVE-2020-1472 [CWE-330]), NoPac (CVE-2021-42278 [CWE-20] and CVE-2021-42287 [CWE-269]), and PrintNightmare (CVE-2021-34527 [CWE-269]) vulnerabilities for local and Windows Active Domain privilege escalation [T1068].[1],[2]

Lateral Movement

Black Basta affiliates use tools such as BITSAdmin and PsExec, along with Remote Desktop Protocol (RDP), for lateral movement. Some affiliates also use tools like Splashtop, Screen Connect, and Cobalt Strike beacons to assist with remote access and lateral movement.

Exfiltration and Encryption

Black Basta affiliates use RClone to facilitate data exfiltration prior to encryption. Prior to exfiltration, cybersecurity researchers have observed Black Basta affiliates using PowerShell [T1059.001] to disable antivirus products, and in some instances, deploying a tool called Backstab, designed to disable endpoint detection and response (EDR) tooling [T1562.001].[3] Once antivirus programs are terminated, a ChaCha20 algorithm with an RSA-4096 public key fully encrypts files [T1486]. A `.basta` or otherwise random file extension is added to file names and a ransom note titled `readme.txt` is left on the compromised system.[4] To further inhibit system recovery, affiliates use the `vssadmin.exe` program to delete volume shadow copies [T1490].[5]

Leveraged Tools

See Table 1 for publicly available tools and applications used by Black Basta affiliates. This includes legitimate tools repurposed for their operations.

Table 1: Tools Used by Black Basta Affiliates

Disclaimer: Use of these tools and applications should not be attributed as malicious without analytical evidence to support threat actor use and/or control. Black Basta affiliates were observed using these legitimate tools for intended malicious purposes.

Tool Name	Description
AnyDesk	A remote monitoring and management tool used by Black Basta affiliates to gain access to a victim user's endpoint.
Microsoft Teams	A messaging application used within organizations and maliciously used by Black Basta affiliates to contact employees.
Microsoft Quick Assist	A remote monitoring and management tool used by Black Basta affiliates to gain access to a victim user's endpoint.
BITSAdmin	A command-line utility that manages downloads/uploads between a client and server by using the Background Intelligent Transfer Service (BITS) to perform asynchronous file transfers.
Cobalt Strike	A penetration testing tool used by security professions to test the security of networks and systems. Black Basta affiliates have used it to assist with lateral movement and file execution.
Mimikatz	A tool that allows users to view and save authentication credentials such as Kerberos tickets. Black Basta affiliates have used it to aid in privilege escalation.
PSExec	A tool designed to run programs and execute commands on remote systems.
PowerShell	A cross-platform task automation solution made up of a command-line shell, a scripting language, and a configuration management framework, which runs on Windows, Linux, and macOS.
RClone	A command line program used to sync files with cloud storage services such as Mega.
SoftPerfect	A network scanner (`netscan.exe`) used to ping computers, scan ports, discover shared folders, and retrieve information about network devices via Windows Management Instrumentation (WMI), Simple Network Management Protocol (SNMP), HTTP, Secure Shell (SSH) and PowerShell. It also scans for remote services, registry, files, and performance counters.
ScreenConnect	Remote support, access, and meeting software that allows users to control devices remotely over the internet.

Splashtop	Remote desktop software that allows remote access to devices for support, access, and collaboration.
WinSCP	Windows Secure Copy is a free and open source SSH File Transfer Protocol, File Transfer Protocol, WebDAV, Amazon S3, and secure copy protocol client. Black Basta affiliates have used it to transfer data from a compromised network to actor-controlled accounts.

MITRE ATT&CK TACTICS AND TECHNIQUES

See Tables 2–6 for all referenced threat actor tactics and techniques in this advisory.

Table 2: Black Basta ATT&CK Techniques for Initial Access

Technique Title	ID	Use
Phishing	T1566	Black Basta affiliates have used spearphishing emails to obtain initial access.
Phishing: Spearphishing Voice	T1566.004	Black Basta affiliates have used spearphishing phone and Microsoft Teams calls to trick users into providing initial access.
Exploit Public-Facing Application	T1190	Black Basta affiliates have exploited ConnectWise vulnerability CVE-2024-1709 to obtain initial access.

Table 3: Black Basta ATT&CK Techniques for Privilege Escalation

Technique Title	ID	Use
Exploitation for Privilege Escalation	T1068	Black Basta affiliates have used credential scraping tools like Mimikatz, Zerologon, NoPac and PrintNightmare for privilege escalation.

Table 4: Black Basta ATT&CK Techniques for Defense Evasion

Technique Title	ID	Use
Masquerading	T1036	Black Basta affiliates have conducted reconnaissance using utilities with innocuous file names, such as `Intel` or `Dell`, to evade detection.
Impair Defenses: Disable or Modify Tools	T1562.001	Black Basta affiliates have deployed a tool called Backstab to disable endpoint detection and response (EDR) tooling. Black Basta affiliates have used PowerShell to disable antivirus products.

Table 5: Black Basta ATT&CK Techniques for Execution

Technique Title	ID	Use
User Execution	T1204	Black Basta affiliates have used social engineering techniques to convince users to execute legitimate remote access tools such as AnyDesk and Microsoft's Quick Assist.
Command and Scripting Interpreter: PowerShell	T1059.001	Black Basta affiliates have used PowerShell to disable antivirus products.

Table 6: Black Basta ATT&CK Techniques for Impact

Technique Title	ID	Use
Inhibit System Recovery	T1490	Black Basta affiliates have used the `vssadmin.exe` program to delete shadow copies.
Data Encrypted for Impact	T1486	Black Basta affiliates have used a public key to fully encrypt files.

INDICATORS OF COMPROMISE

Update November 8, 2024:

Many indicators provided in this advisory's initial publication have been removed considering they are outdated. For historic reference, see AA24-131A #StopRansomware: Black Basta (Initial Version).

The IOCs listed in Tables 7–8 were obtained from trusted third-party reporting and are considered most current.

Table 7: Network Indicators

Disclaimer: The authoring organizations recommend network defenders investigate or vet IP addresses prior to taking action, such as blocking, as many cyber actors are known to change IP addresses, sometimes daily, and some IP addresses may host valid domains.

IP Address	First Seen	Description
170.130.165[.]73	October 14, 2024	Likely Cobalt Strike infrastructure
45.11.181[.]44	October 24, 2024	Likely Cobalt Strike infrastructure
66.42.118[.]54	October 15, 2024	Exfiltration server
79.132.130[.]211	October 24, 2024	Likely Cobalt Strike infrastructure

Table 8: Suspected Black Basta Cobalt Strike Domains

Domain	First Seen
Moereng[.]com	October 9, 2024
Exckicks[.]com	October 2, 2024

Update End

MITIGATIONS

The authoring organizations recommend all critical infrastructure organizations implement the mitigations below to improve your organization's cybersecurity posture based on Black Basta's activity. These mitigations align with the Cross-Sector Cybersecurity Performance Goals (CPGs) developed by CISA and the National Institute of Standards and Technology (NIST). The CPGs provide a minimum set of practices and protections that CISA and NIST recommend all organizations implement. CISA and NIST based the CPGs on existing cybersecurity frameworks and guidance to protect against the most common and impactful threats, tactics, techniques, and procedures. Visit CISA's Cross-Sector Cybersecurity Performance Goals for more information on the CPGs, including additional recommended baseline protections.

- **Install updates for operating systems, software, and firmware as soon as they are released** [CPG 1.E]. Prioritize updating Known Exploited Vulnerabilities (KEV).
- **Require phishing-resistant multi-factor authentication (MFA)** [CPG 2.H] for as many services as possible.
- **Implement recommendations, including training users to recognize and report phishing attempts** [CPG 2.I], from joint Phishing Guidance: Stopping the Attack Cycle at Phase One.
- **Secure remote access software** by applying mitigations from joint Guide to Securing Remote Access Software.
- **Make backups of critical systems and device configurations** [CPG 2.R] to enable devices to be repaired and restored.
- **Apply mitigations from the joint #StopRansomware Guide**.

The authoring organizations also recommend network defenders of HPH Sector and other critical infrastructure organizations to reference CISA's Mitigation Guide: Healthcare and Public Health (HPH) Sector and HHS's HPH Cybersecurity Performance Goals, which provide best practices to combat pervasive cyber threats against organizations. Recommendations include the following:

- **Asset Management and Security**: Cybersecurity professionals should identify and understand all relationships or interdependencies, functionality of each asset, what it exposes, and what software is running to ensure critical data and systems are protected appropriately. HPH Sector organizations should ensure electronic PHI (ePHI) is protected and compliant with the Health Insurance Portability and Accountability Act (HIPAA). Organizations can complete asset inventories using active scans, passive processes, or a combination of both techniques.

- **Email Security and Phishing Prevention**: Organizations should install modern anti-malware software and automatically update signatures where possible. For additional guidance, see CISA's Enhance Email and Web Security Guide.
  - **Check for embedded or spoofed hyperlinks**: Validate the URL of the link matches the text of the link itself. This can be achieved by hovering your cursor over the link to view the URL of the website to be accessed.
- **Access Management**: Phishing-resistant MFA completes the same process but removes 'people' from the equation to help thwart social engineering scams and targeted phishing attacks that may have been successful using traditional MFA. The two main forms of phishing-resistant MFA are FIDO/Web Authentication (WebAuthn) authentication and Public Key Infrastructure (PKI)-based authentication. Prioritize phishing-resistant MFA on accounts with the highest risk, such as privileged administrative accounts on key assets. For additional information on phishing-resistant MFA, see CISA's Implementing Phishing-Resistant MFA Guide.
- **Vulnerability Management and Assessment**: Once vulnerabilities are identified across your environment, evaluate and prioritize to appropriately deal with the posed risks according to your organization's risk strategy. To assist with prioritization, it is essential to:
  - **Map your assets to business-critical functions.** For vulnerability remediation, prioritize assets that are most critical for ongoing operations or which, if affected, could impact your organization's business continuity, sensitive PII (or PHI) security, reputation, or financial position.
  - **Use threat intelligence information.** For remediation, prioritize vulnerabilities actively exploited by threat actors. To assist, leverage CISA's KEV Catalog and other threat intelligence feeds.
  - **Leverage prioritization methodologies, ratings, and scores**. The Common Vulnerability Scoring System (CVSS) assesses the technical severity of vulnerabilities. The Exploit Prediction Scoring System (EPSS) measures the likelihood of exploitation and can help with deciding which vulnerabilities to prioritize. CISA's Stakeholder-Specific Vulnerability Categorization (SSVC) methodology leverages decision trees to prioritize relevant vulnerabilities into four decisions, Track, Track*, Attend, and Act based on exploitation status, technical impact, mission prevalence, and impacts to safety and public-wellbeing.

VALIDATE SECURITY CONTROLS

In addition to applying mitigations, the authoring organizations recommend exercising, testing, and validating your organization's security program against the threat behaviors mapped to the MITRE ATT&CK for Enterprise framework in this advisory. The authoring organizations recommend testing your existing security controls inventory to assess how they perform against the ATT&CK techniques described in this advisory.

To get started:

1. Select an ATT&CK technique described in this advisory (see Tables 2-6).
2. Align your security technologies against the technique.
3. Test your technologies against the technique.
4. Analyze your detection and prevention technologies' performance.
5. Repeat the process for all security technologies to obtain a set of comprehensive performance data.
6. Tune your security program, including people, processes, and technologies, based on the data generated by this process.

The authoring organizations recommend continually testing your security program, at scale, in a production environment to ensure optimal performance against the MITRE ATT&CK techniques identified in this advisory.

REFERENCES

[1] SentinelOne: Black Basta Ransomware | Attacks Deploy Custom EDR Evasion Tools Tied to FIN7 Threat Actor

[2] Trend Micro: Ransomware Spotlight - Black Basta

[3] Kroll: Black Basta - Technical Analysis

[4] Who Is Black Basta? (blackberry.com)

[5] Palo Alto Networks: Threat Assessment - Black Basta Ransomware

REPORTING

Your organization has no obligation to respond or provide information back to FBI in response to this joint CSA. If, after reviewing the information provided, your organization decides to provide information to FBI, reporting must be consistent with applicable state and federal laws.

FBI is interested in any information that can be shared, to include boundary logs showing communication to and from foreign IP addresses, a sample ransom note, communications with threat actors, Bitcoin wallet information, decryptor files, and/or a benign sample of an encrypted file.

Additional details of interest include: a targeted company point of contact, status and scope of infection, estimated loss, operational impact, transaction IDs, date of infection, date detected, initial attack vector, and host- and network-based indicators.

FBI, CISA, and HHS do not encourage paying ransom as payment does not guarantee victim files will be recovered. Furthermore, payment may also embolden adversaries to target additional organizations, encourage other criminal actors to engage in the distribution of ransomware, and/or fund illicit activities. Regardless of whether you or your organization have decided to pay the ransom, FBI and CISA urge you to promptly report ransomware incidents to FBI's Internet Crime Complain Center (IC3), a local FBI Field Office, or CISA via the agency's Incident Reporting System or its 24/7 Operations Center (report@cisa.gov or by calling 1-844-Say-CISA [1-844-729-2472]).

DISCLAIMER

The information in this report is being provided "as is" for informational purposes only. FBI, CISA, HHS, and MS-ISAC do not endorse any commercial entity, product, company, or service, including any entities, products, or services linked within this document. Any reference to specific commercial entities, products, processes, or services by service mark, trademark, manufacturer, or otherwise, does not constitute or imply endorsement, recommendation, or favoring by FBI, CISA, HHS, and MS-ISAC.

VERSION HISTORY

May 10, 2024: Initial version.

November 8, 2024: Updates noted throughout.