

Black Basta Ransomware

Impacting 500+ organizations and counting

<https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-131a>
 CVEs: CVE-2024-1709, CVE-2020-1472, CVE-2021-42278, CVE-2021-42287, CVE-2021-34527

A new alert from CISA, the FBI, the Department of Health and Human Services (HHS), and the Multi-State Information Sharing and Analysis Center (MS-ISAC) reveals that Black Basta affiliates have attacked 12 of the 16 critical infrastructure sectors, including healthcare organizations.

Background

Black Basta is a type of ransomware-as-a-service (RaaS) that was first discovered in April 2022. Since then, its affiliates have targeted numerous businesses and critical infrastructure in North America, Europe, and Australia. By May 2024, Black Basta has impacted over 500 organizations worldwide. In this Ransomware-as-a-Service (RaaS) model, the developers offer a service such as ransomware, an infrastructure for payment processing and ransom negotiation, and technical support to its affiliates.

Black Basta has been seen to use techniques such as phishing and exploiting public facing applications to gain initial access. Previously, it was seen to exploit the PrintNightmare (CVE-2021-34527), ZeroLogon (CVE-2020-1472) and Follina (CVE-2022-30190) vulnerabilities for privilege escalation. n't

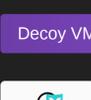
Latest Developments

- February 28, 2024: FortiGuard Labs released an outbreak alert on ConnectWise vulnerability CVE-2024-1709, which has been exploited by Black Basta recently. <https://www.fortiguard.com/outbreak-alert/connectwise-screenconnect-attack>
- June 01, 2023: Fortinet released a detailed blog on Blackbasta Ransomware and how Antivirus Service and FortiEDR detects and blocks the ransomware. <https://www.fortinet.com/blog/threat-research/ransomware-roundup-black-basta>

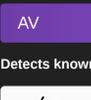
PROTECT

Countermeasures across the security fabric for protecting assets, data and network from cybersecurity events:

Lure



Decoy VM



AV

Detects known malware related to the Outbreak



DB 92.04124



DB 92.04124



DB 92.04124



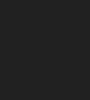
DB 92.04124



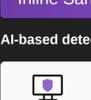
DB 92.04124



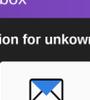
DB 92.04124



DB 92.04124



DB 92.04124



DB 92.04124

Inline Sandbox

AI-based detection for unknown and new variants of Black Basta ransomware



Vulnerability

Find vulnerable systems installed on the network related to Black Basta campaigns



AV (Pre-filter)

Detects known malware related to the Outbreak



DB 92.04124

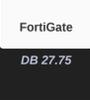


DB 92.04124



DB 92.04124

Behavior Detection



IPS

Detects and blocks attack attempts leveraging the vulnerability



DB 27.75



DB 27.75



DB 27.75



DB 27.75



DB 27.75

Web App Security

Detects and blocks web application vulnerability attack attempts by Black Basta ransomware



Pre-execution



Anti-ransomware



DETECT

Find and correlate important information to identify an outbreak, the following updates are available to raise alert and generate reports:

IOC



Outbreak Detection



DB 2.00046



DB 1.00021



v7.4+

Threat Hunting



Playbook



v7.4+

RESPOND

Develop containment techniques to mitigate impacts of security events:

Automated Response

Services that can automatically respond to this outbreak.



Assisted Response Services

Experts to assist you with analysis, containment and response activities.



RECOVER

Improve security posture and processes by implementing security awareness and training, in preparation for (and recovery from) security incidents:

NOC/SOC Training

Train your network and security professionals and optimize your incident response to stay on top of the cyberattacks.



End-User Training

Raise security awareness to your employees that are continuously being targeted by phishing, drive-by download and other forms of cyberattacks.



IDENTIFY

Identify processes and assets that need protection:

Attack Surface Hardening

Check Security Fabric devices to build actionable configuration recommendations and key indicators.



Attack Surface Monitoring (Inside & Outside)

Security reconnaissance and penetration testing services, covering both internal & external attack vectors, including those introduced internally via software supply chain.



Additional Resources

- Fortinet Blog <https://www.fortinet.com/blog/threat-research/ransomware-roundup-black-basta>
- CISA Advisory <https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-131a>
- CRN <https://www.crn.com/news/security/2024/black-basta-ransomware-attack-brought-down-ascension-it-systems-report>
- ConnectWise Outbreak <https://www.fortiguard.com/outbreak-alert/connectwise-screenconnect-attack>
- American Hospital Association <https://www.aha.org/news/headline/2024-05-10-agencies-warn-accelerating-attacks-health-care-black-basta-ransomware-group>

Learn more about [FortiGuard Outbreak Alerts](#)