THREAT BULLETINS

Inside Black Basta: Chat Logs Expose Ransomware Operations

TLP:WHITE

Feb 26, 2025

Summary:

On February 26, 2025, Health-ISAC received information related to insights gathered from leaked chat logs of Black Basta threat actors. These insights include specific vulnerabilities, vendors, products, tools, and targeting approaches for planning attacks. Black Basta is a ransomware-as-a-service (RaaS) operator that emerged in April 2022. Since then, the group has targeted a wide variety of critical infrastructure sectors, including the global health sector.

Leaked Black Basta chat logs spanning a year unveiled the ransomware group's inner workings, offering insights into cybercriminal tactics. Researchers found detailed strategies for attacking victims, including exploiting known vulnerabilities in enterprise technologies like Citrix and Fortinet, and using tools like ZoomInfo and Cobalt Strike.

The group prioritized high-revenue targets with known weaknesses, focusing on finance, health, and legal sectors. They favored readily available exploits and rapidly responded to new security advisories. Internal conflicts led to the leak, revealing candid communication and named targets like Fisker and Cerner. Analysis, aided by AI tools like BlackBastaGPT, exposed their methods, target selection, and exploited vulnerabilities.

This intelligence provides a blueprint for improved cyber defense. Health-ISAC would like to thank Max Morris at Ally for sharing the information contained within this alert.

Analysis:

Beyond the CVEs identified in the chats, there was evidence that Black Basta employed a broader arsenal of exploits while targeting vulnerabilities, using:

- **Opportunistic Exploitation** appears to favor existing vulnerabilities and readily available PoC exploits for initial access, particularly targeting email services. This reinforces the importance of promptly fixing vulnerabilities that are known to be weaponized in any exploit framework or security tool.
- **Tooling and Techniques** discussion frequently referenced tools and platforms such as ZoomInfo, ChatGPT, GitHub, Shodan, Fofa, Metasploit, Core Impact, Cobalt Strike, and Nuclei, a mix of offensive and defensive security tools that underscored the group's flexible, opportunistic approach.
- **Exploit Development & Acquisition** discussion showed evidence that in addition to using known exploits Black Basta likely also has the resources to develop new exploits and considered purchasing exploits from external groups with hesitancy.

An analysis found that Black Basta selected its targets based on several key factors:
Financial Viability and Ransom Payment Potential: The group tends to prioritize high-revenue companies over a large number of random targets. Discussions suggest that fewer high-profile targets generate more revenue than mass-targeting lower-value entities, and there was a clear emphasis on targeting organizations that are more likely to pay ransoms.
Vulnerability-Based Targeting: The group discussed specific exploits for initial access and email services, indicating a preference for targets with known weaknesses, with pre-attack reconnaissance that included checking domain and infrastructure vulnerabilities.
Industry-Specific Selection: Sectors such as legal, financial, health, and industrial companies, typically handling sensitive data, are frequently targeted due to their higher likelihood of paying to protect client confidentiality.
Access to Initial Compromise: Decisions often hinge on whether initial access is available, including leveraging exposed RDP, Citrix, VPN, or email credentials, with some attacks beginning with methods like credential stuffing or brute-force attempts.

Geographical Considerations: Although Black Basta claims to be apolitical, discussions imply that they may selectively target companies in regions with specific financial or regulatory environments.
Use of Stolen Data for Secondary Extortion: In certain cases, the group discussed selling stolen data to competitors or foreign entities, highlighting the attractiveness of targets with valuable intellectual property or business secrets.

Possible Targets Mentioned: Vendors & Products
Initial access devices and Microsoft technologies

- Fortinet: CVE-2024-23109, CVE-2024-23108, CVE-2024-21762, CVE-2024-23113
- Citrix Netscaler: CVE-2023-3519, CVE-2023-3467, CVE-2023-3466, CVE-2023-4966
- Palo Alto Networks Pan-OS: CVE-2024-3400
- Checkpoint: CVE-2024-24919
- F5 Big-IP: CVE-2022-1388
- Juniper OS: CVE-2023-36845, CVE-2023-36844
- Connectwise: CVE-2024-1709, CVE-2024-1708
- Microsoft Windows: CVE-2020-1472, CVE-2021-40444, CVE-2021-42287, CVE-2021-42278, CVE-2022-30190, CVE-2022-37969, CVE-2023-36874, CVE-2023-36884, CVE-2024-21338, CVE-2024-26169, CVE-2023-36394, CVE-2023-35628
- Zyxel: CVE-2022-30525
- Atlassian Confluence CVE-2021-44228, CVE-2024-21683, CVE-2023-22515, CVE-2022-26134
- Brick Builders Wordpress Theme CVE-2024-25600
- Cisco: CVE-2023-20198
- Gitlab: CVE-2023-7028
- Google Chrome: CVE-2022-0609
- Intel: cve-2017-5754, cve-2017-5753
- JetBrains CVE-2024-27198
- Jenkins CVE-2024-23897
- Linux CVE-2024-1086
- JetBrains CVE-2023-42793
- RARLAB CVE-2023-38831
- VMware Spring CVE-2022-22965
- Microsoft SharePoint CVE-2023-29357
- Microsoft Office CVE-2023-23397, CVE-2023-21716, CVE-2017-11882

Email and communication services (offering a vector for phishing campaigns and providing initial access to networks)

- Microsoft Exchange: CVE-2021-26855, CVE-2021-28482, CVE-2021-42321, CVE-2022-41040, CVE-2022-41082, CVE-2023-36745
- Microsoft Outlook: CVE-2024-21378, CVE-2024-21413

- Exim: CVE-2023-42115
- Zimbra: CVE-2022-27925, CVE-2022-37042, CVE-2022-41352
- WordPress SMTP plugins: CVE-2023-6875, CVE-2023-7027

Recommendations:

Health-ISAC provides this information to prevent the successful exploitation and disruption of your security apparatus. For more information, see Health Industry Cybersecurity Practices (HICP): Managing Threats and Protecting Patients.

https://techcrunch.com/2025/02/21/a-huge-trove-of-leaked-black-basta-chat-logs-expose-the-ransomware-gangs-key-members-and-victims/
https://cyberscoop.com/black-basta-internal-chat-leak/
https://www.bleepingcomputer.com/news/security/black-basta-ransomware-gang-s-internal-chat-logs-leak-online/
https://cybernews.com/security/black-basta-ransomware-dissected/
https://vulncheck.com/blog/black-basta-chats
http://www.hudsonrock.com/blackbastagpt

Reference(s)	, Tech Crunch, , Bleeping Computer, Cyberscoop, Cyber News

Sources
https://techcrunch.com/2025/02/21/a-huge-trove-of-leaked-black-basta-chat-logs-expose-the-ransomware-gangs-key-members-and-victims/
https://cyberscoop.com/black-basta-internal-chat-leak/
https://www.bleepingcomputer.com/news/security/black-basta-ransomware-gang-s-internal-chat-logs-leak-online/
https://cybernews.com/security/black-basta-ransomware-dissected/
https://vulncheck.com/blog/black-basta-chats
http://www.hudsonrock.com/blackbastagpt

Incident Date
Feb 27, 2025 (UTC)

Alert ID 7bcf6640

View Alert

Share Feedback

was this helpful? |

Tags Leaked Chat, Black Basta Ransomware

TLP:WHITE Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

For Questions or Comments
Please email us at toc@h-isac.org

Download Health-ISAC's Information Sharing App.

For more updates and alerts, visit: **https://health-isac.cyware.com/webapp/**