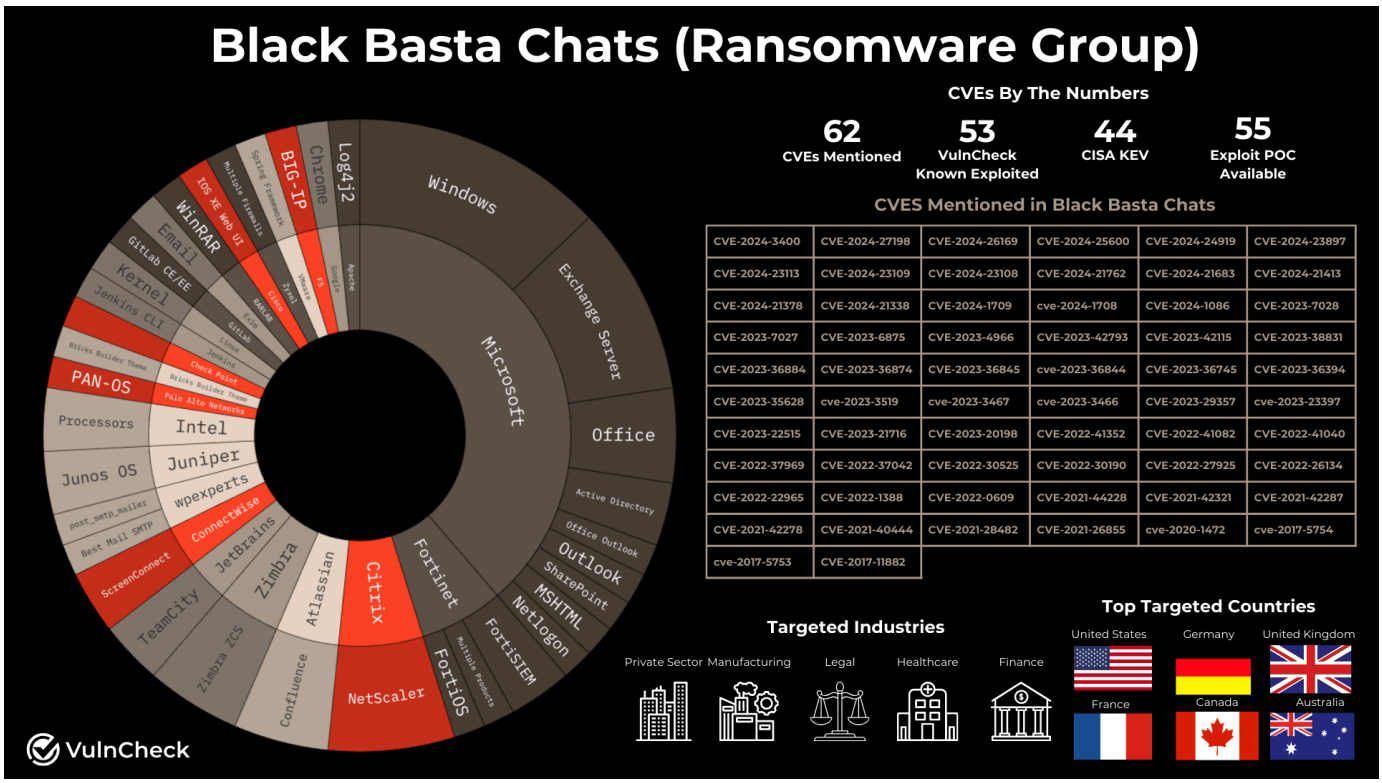
Go back

February 23, 2025

Exposing CVEs from Black Bastas' Chats

Patrick Garrity
in/patrickmgarrity/

vuln-intel cve kev



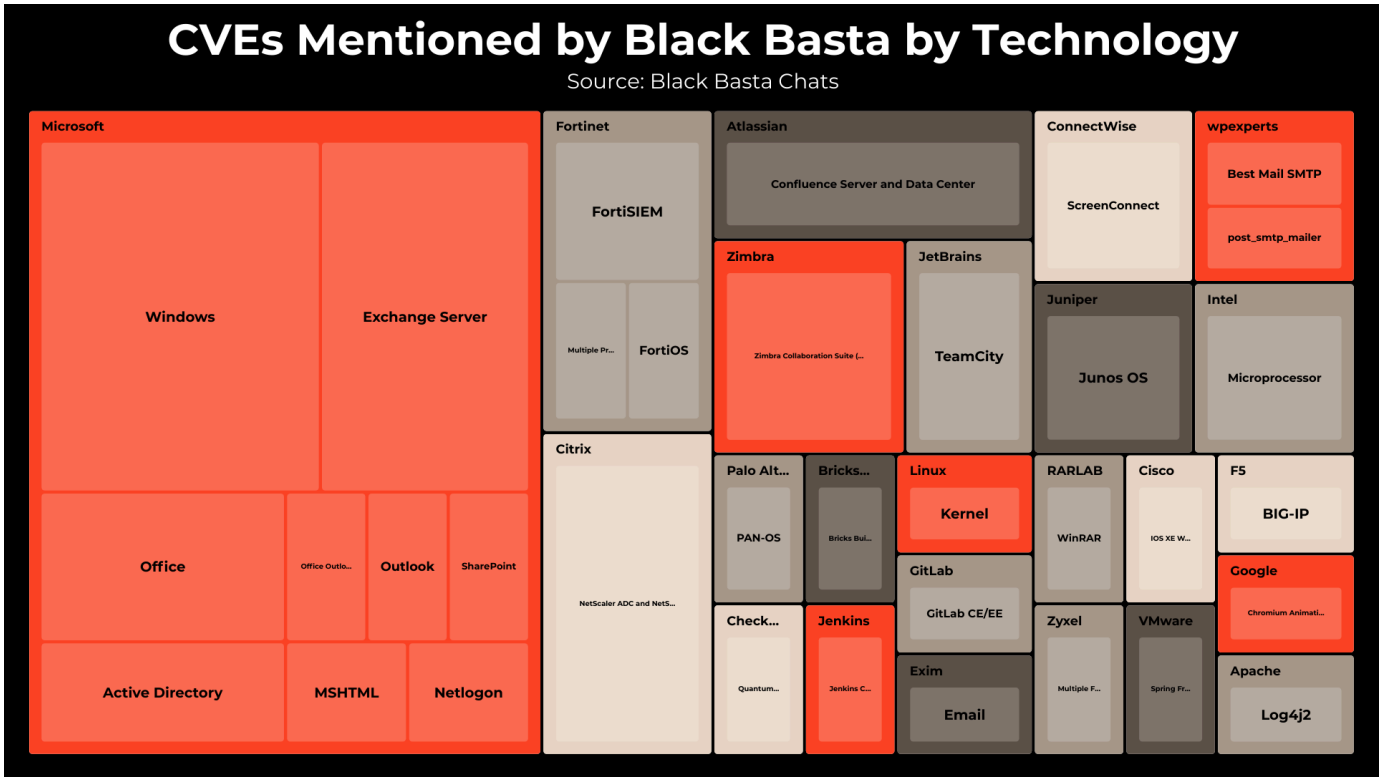
Key Takeaways

- 62 unique CVEs were mentioned in the Black Basta chat logs.
- 53 of the 62 CVEs (85.5%) are known to be exploited and are listed in VulnCheck KEV.
- 44 of the CVEs (70.9%) appear in the CISA KEV catalog.
- Black Basta shows a clear preference for targets with known weaknesses, focusing on vulnerabilities that already have available exploits.
- The group seems to favor widely adopted enterprise technologies, including products like Citrix NetScaler, Confluence Atlassian, Fortinet, Cisco, Palo Alto, CheckPoint, and Microsoft Windows.

Late last week, chat logs from Black Basta became available, offering rare insight into the operations of one of the most infamous ransomware groups. This research focuses on the vulnerabilities and CVEs mentioned in these logs, with the goal of providing defenders with actionable intelligence on the tactics of Black Basta.

The initial phase involved collecting all CVEs referenced in the chats. Although there were discussions about discovering new vulnerabilities, it became evident that Black Basta generally prioritizes known weaknesses, often leveraging available tools and proof-of-concept exploits. It is important to note that a mention of a CVE in the chat does not necessarily mean that it was used in an attack.

Possible Black Basta Targets Mentioned: Vendors & Products



Black Basta appears to be targeting a mix of 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

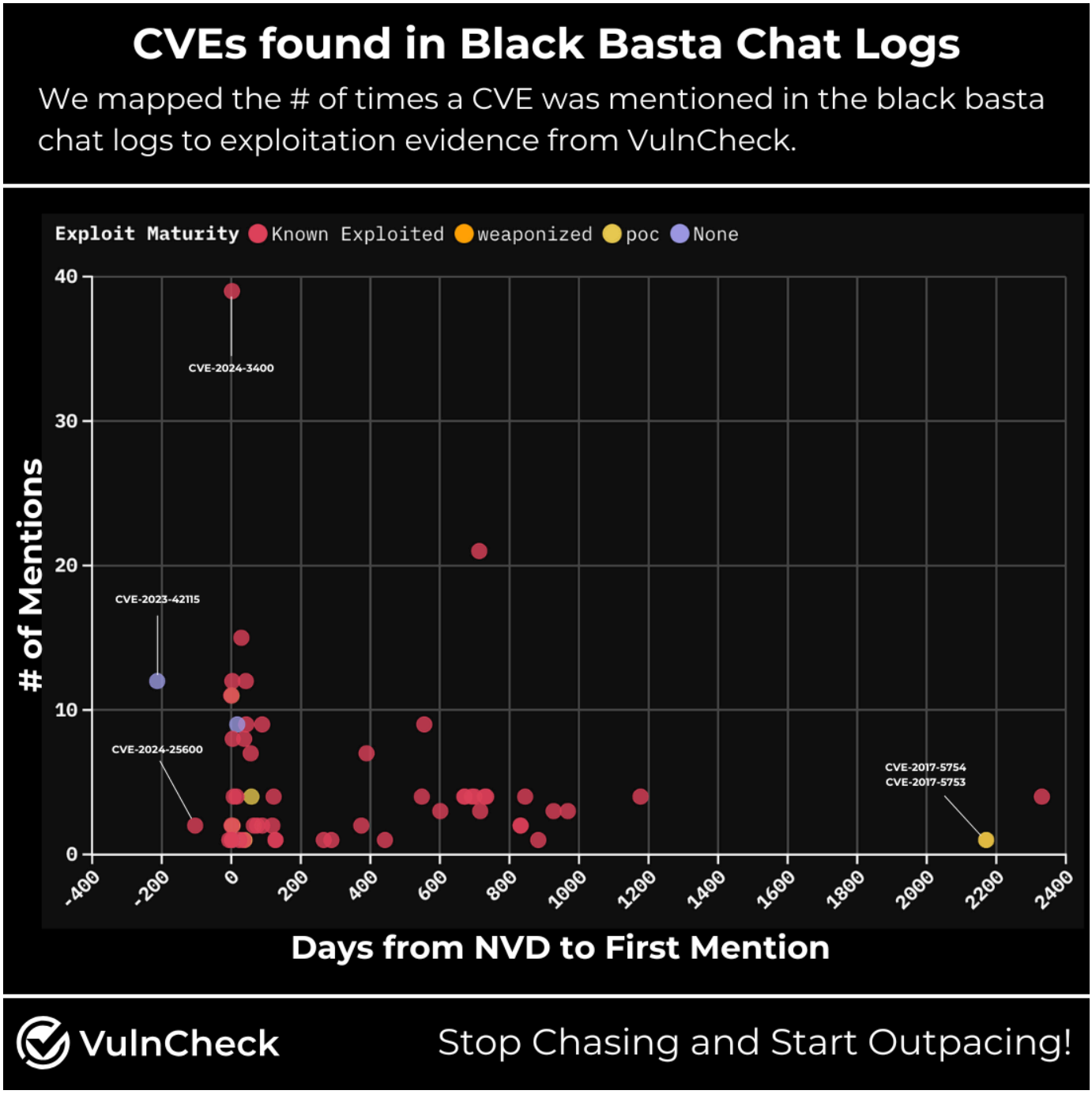
Black Basta appears to also target email and communication services including:

- **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

These email services offer relatively safe vectors for phishing campaigns and can provide initial access into organizations networks.

How Quickly and at what frequency are CVEs being discussed by Black Basta?



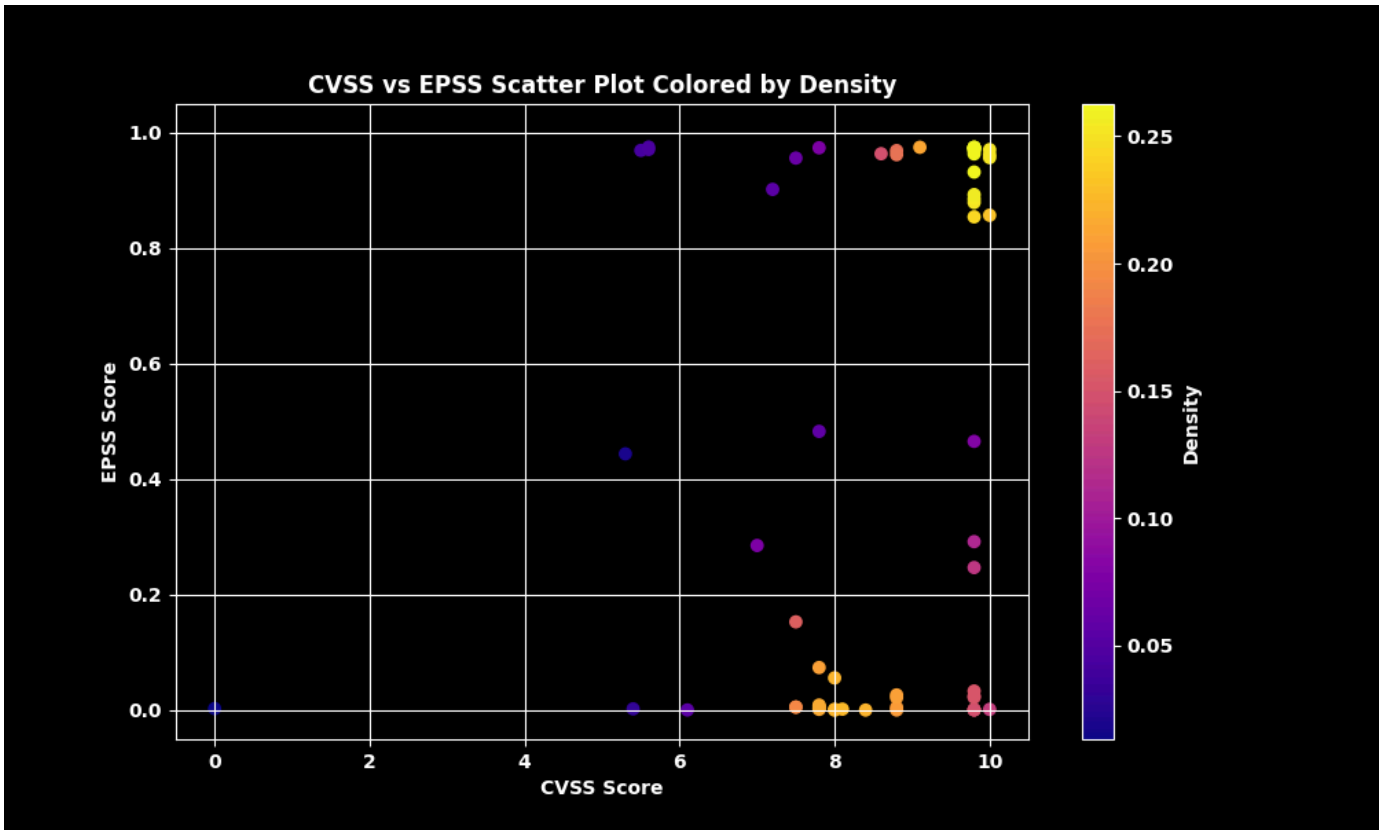
Analyzing the timeline between the publication of CVEs and their first mention in the chats provides insight into Black Basta's targeting speed:

- **Rapid Response:** Within days of new security advisories being issued, members discussed vulnerabilities related to products such as Citrix NetScaler, Check Point Quantum Security Gateways, ConnectWise ScreenConnect, Microsoft Office Outlook, Fortinet FortiSIEM, Palo Alto Networks PAN-OS, Atlassian Confluence Server and Data Center, Cisco IOS XE Web UI, Microsoft Windows, GitLab CE/EE, and Fortinet FortiOS.
- **Pre-Publication Mentions:** Interestingly, three CVEs were discussed before their official publication:
  - Fortinet FortiOS (CVE-2024-23113)
  - Bricks Builder WordPress Theme (CVE-2024-25600)
  - Exim Email (CVE-2023-42115) According to VulnCheck, while these CVE IDs were included in product security advisories, there was a delay in the official publication by the CVE numbering authority.
- **Older Vulnerabilities:** A number of older vulnerabilities also appeared in the chats, often as part of a "Top 10 of 2022" list that highlighted widely exploited issues. One CVE was even described as "Old but not forgotten."

```
ТОП 10 из 2022

1. Follina (CVE-2022-30190)
2. Log4Shell (CVE-2021-44228)
3. Spring4Shell (CVE-2022-22965)
4. F5 BIG-IP (CVE-2022-1388)
5. Google Chrome zero-day (CVE-2022-0609)
6. Old but not forgotten - Microsoft Office bug (CVE-2017-11882)
7. ProxyNotShell (CVE-2022-41082, CVE-2022-41040)
8. Zimbra Collaboration Suite bugs (CVE-2022-27925, CVE-2022-41352)
9. Atlassian Confluence RCE flaw (CVE-2022-26134)
10. Zyxel RCE vulnerability (CVE-2022-30525)
```

How Do EPSS and CVSS Score the Mentioned CVEs?



We mapped CVSS and EPSS to the CVEs discovered in the Black Basta logs using a scatter plot. The distribution highlights both CVSS and EPSS have broad scoring distribution among the CVEs mentioned.

Are All CVEs Discussed Known to be Exploited or Used by Black Basta?

Of the 62 unique CVEs mentioned by Black Basta, VulnCheck KEV tracks 53 of the vulnerabilities as confirmed as being exploited in the wild.

Below are some notable observations on the nine CVEs where there was previously no evidence of exploitation:

CVE-2017-5754 & CVE-2017-5753 (Intel Vulnerabilities):

- Referenced in a Dell advisory.
- CVE-2017-5754 features a weaponized Core Impact exploit and four PoC exploits; CVE-2017-5753 has eight PoC exploits.
- Both have EPSS scores exceeding 0.97, suggesting they should be prioritized with urgency.

CVE-2024-21378 (Microsoft Outlook RCE):

- Black Basta confirmed it works in a production environment. “We've tested the new RCE in Microsoft Outlook (CVE-2024-21378) in a production environment and confirm it works

CVE-2023-7027 (WordPress Plugin Vulnerability):

- Identified as one of two options to compromise SMTP services on Wordpress.
- Three PoC exploits are available, the EPSS score remains low (0.00263).

CVE-2023-36394 (Microsoft Windows):

- Black Basta considered purchasing an exploit for this CVE.
- No known PoC exploits exist that we are aware of, and the EPSS score is elevated at 0.28553.

CVE-2024-23109 & CVE-2024-23108 (FortiSIEM Vulnerabilities):

- Both were highlighted due to their perfect CVSS scores of 10.
- CVE-2024-23108 has three PoC exploits, none have been observed for CVE-2024-23109.
- Both share low EPSS scores (0.00124).

CVE-2023-35628 (Microsoft Windows Vulnerability):

- Comes with three PoC exploits and an EPSS score of 0.00213.
- An MSRC link was provided for further details.

CVE-2023-42115 (Exim Email Server Vulnerability):

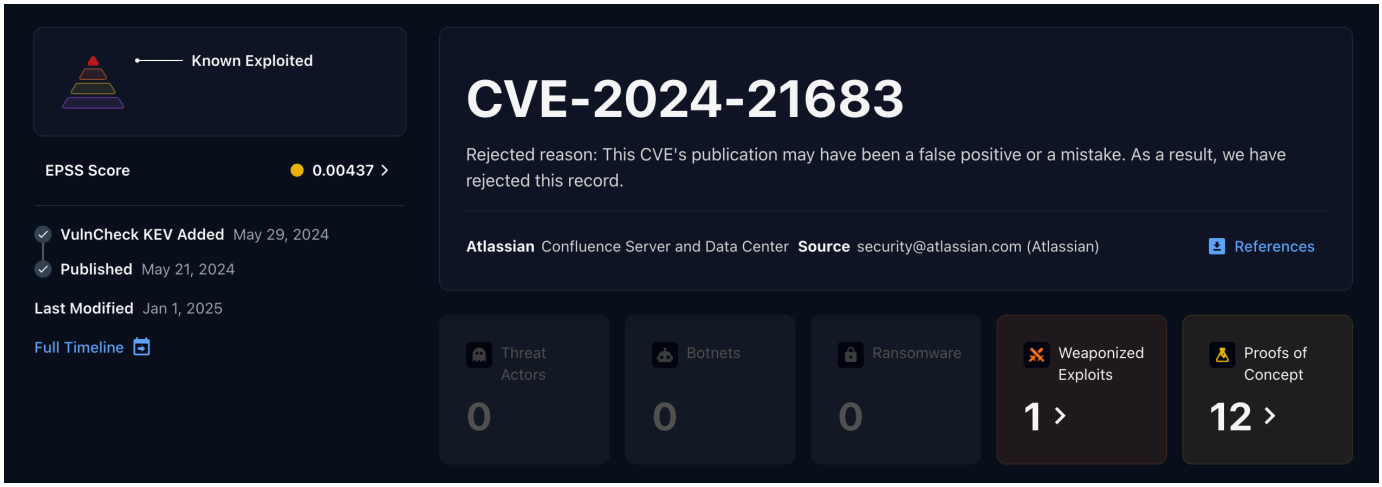
- Reiterated in the chats as a prime target, one comment noted, “SMTP, but I didn’t find a single PoC, I'm collecting all Exim servers.”
- Its EPSS score is 0.00075.

After remediating all vulnerabilities confirmed to be exploited in the wild, those found in VulnCheck KEV, it would then be advisable to treat any of the CVEs mentioned in the Black

Basta chats as if they are being exploited in the wild.

CVE-2024-21683 Rejected by CVE.org

Black Basta also mentions Atlassian Confluence CVE-2024-21683 which is listed by CVE.org as rejected, but there is evidence of exploitation from Shadow Server, available exploits including a MetaSploit module for this CVE, and a Atlassian vendor security advisory.



What other vulnerabilities and tools might be being used by Blackbasta?

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

- **Opportunistic Exploitation:** The group appears to favor existing vulnerabilities and readily available PoC exploits for initial access, particularly targeting email services.
- **Tooling and Techniques:** Discussions frequently reference tools and platforms such as ZoomInfo, ChatGPT, GitHub, Shodan, Fofa, Metasploit, Core Impact, Cobalt Strike, and Nuclei among other tools. A mix of offensive and defensive security tools underscores the group's flexible, opportunistic approach.
- **Exploit Development & Acquisition:** In addition to using known exploits, there is evidence suggesting that Black Basta has the resources to develop new exploits. On several occasions, they also considered purchasing exploits from external groups with hesitancy.

This opportunistic behavior reinforces the importance of promptly fixing vulnerabilities that are known to be weaponized in any exploit framework or security tool.

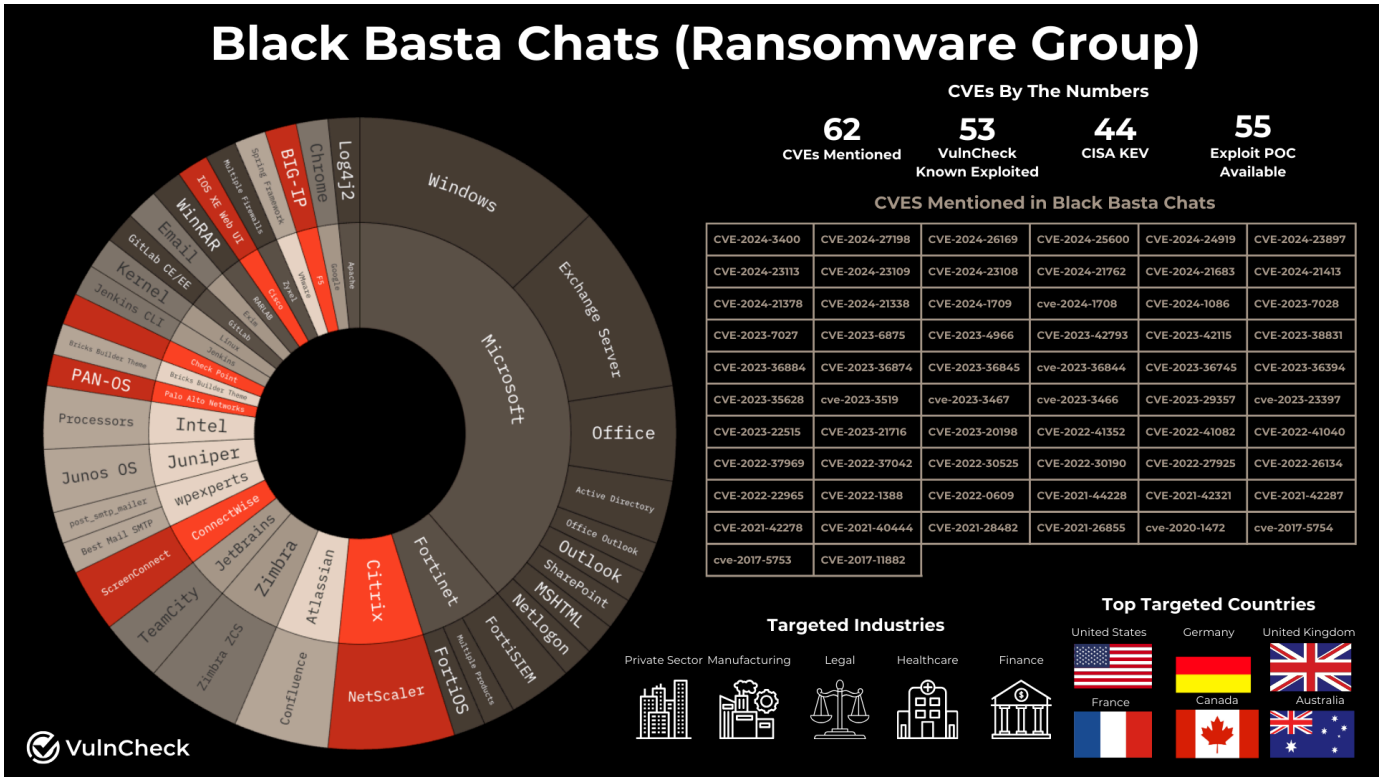
Additional Observations

Black Basta selects 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.
  - There is a clear emphasis on targeting organizations that are more likely to pay ransoms.
- Vulnerability-Based Targeting:
  - They discuss specific exploits for initial access and email services, indicating a preference for targets with known weaknesses.
  - Pre-attack reconnaissance includes checking domain and infrastructure vulnerabilities.
- Industry-Specific Selection:
  - Sectors such as legal, financial, healthcare, 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. This includes leveraging exposed RDP, Citrix, VPN, or email credentials.
  - Some attacks begin 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 discusses selling stolen data to competitors or foreign entities, highlighting the attractiveness of targets with valuable intellectual property or business secrets.

Final Thoughts on the Black Basta Chats



The analysis of Black Basta's chat logs reveals a methodical yet opportunistic approach that focuses on well-known vulnerabilities and high-value targets. While the group leverages established exploit frameworks and readily available tools, their discussions also suggest potential for new exploit development and tactical shifts. For defenders, the key takeaway is to prioritize the remediation of vulnerabilities using an evidence based approach.

About VulnCheck

VulnCheck is helping organizations not just to solve the vulnerability prioritization challenge - we're working to help equip any product manager, security team and threat hunting team to get faster and more accurate intelligence with infinite efficiency using VulnCheck solutions.

We knew that we needed better data, faster across the board, in our industry. So that's what we deliver to the market. We're going to continue to deliver key insights on vulnerability management, exploitation and major trends we can extrapolate from our dataset to continuously support practitioners.

Are you interested in learning more? If so, VulnCheck's Exploit & Vulnerability Intelligence has the broadest coverage.

VulnCheck

VulnCheck helps organizations outpace adversaries with vulnerability intelligence that predicts avenues of attack with speed and accuracy.

Products

- Exploit & Vulnerability Intelligence
- Initial Access Intelligence
- IP Intelligence
- VulnCheck for Government

Resources

- Documentation
- API
- Changelog
- Glossary
- Contact Support

Community

VulnCheck KEV

NVD++

XDB

Knowledge Base

Report a Vulnerability

Open Source

SDK for Go

SDK for Python

CLI

GitHub Action

go-exploit

Company

Blog

News and Awards

Press Releases

Partners

Events

VulnCheck Advisories

Leadership Team

Legal

Privacy Policy

Terms & Conditions

Vulnerability Disclosure Policy