KELA

REPORT

Inside the Black Basta Leak: How Ransomware Operators Gain Access

February 26, 2025

Table of contents

Executive Summary

The BlackBasta leak exposed the inner workings of one of the most active ransomware groups, providing rare insight into their tactics. KELA analyzed the leaked data, focusing on sensitive patterns commonly exploited by ransomware operators to gain unauthorized access to corporate networks and move laterally within them. The analysis reveals the **top 5 most-used initial access points by BlackBasta, tied to credentials sourced from infostealer malware logs, vulnerabilities exploitation and social engineering campaigns.**

To illustrate how these tactics play out in real attacks, KELA examined BlackBasta's attack on a Brazil-based company from the manufacturing & industrial products sector, showing how compromised credentials led to full network access and eventual data exposure. **Initial access was gained through vulnerable RDweb services, likely through valid credentials sourced from infostealer malware logs leaked on cybercrime platforms 6 months prior to the attack.**

This report breaks down the findings, helping organizations understand how attackers operate and how to strengthen their defenses.

BlackBasta Chats Leak

Background

On February 11, 2025, the cybersecurity community was shaken by an unexpected revelation. An administrator of a newly created Telegram group, "Шепот Басты" (*Whisper of Basta*), claimed to have leaked the internal chats of the Black Basta ransomware group. The admin stated that the motivation behind the leak was Black Basta's decision to "cross the line" by attacking Russian banks, a move deemed unacceptable by the leaker. The group was created to "research" Black Basta's activities and shed light on their internal operations.

Interestingly, while the admin's messages were posted in Russian, the language strongly suggested the use of automatic translation, rather than being written by a native speaker. The admin also predominantly referred to herself using the feminine gender.

The admin released the 47.5MB JSON file containing the internal chats and promised more releases in the near future. The leaked data covered a time span from September 18, 2023, to September 28, 2024, offering a look into Black Basta's operations.

What's Inside the Leak?

The leak exposed a vast array of sensitive information, offering a glimpse into the internal workings of the Black Basta ransomware group. The contents included:

- Compromised Credentials — A trove of usernames, passwords, and authentication data for various services, mostly associated with potential BlackBasta victims.
- IP Addresses and Domains — Used for command-and-control (C2) operations and remote access.
- Internal Operational Discussions — Revealing tactics, strategies, and technical procedures.
- Victim Data and Legal Documents — Including data exfiltrated from compromised organizations.
- Payment Information and Cryptocurrency Addresses — Allowing to trace potential financial transactions.
- Technical Infrastructure Details — Such as file servers, proxies and botnets used, etc.

This level of exposure provided invaluable intelligence to cybersecurity researchers and organizations aiming to strengthen their defenses.

KELA's In-Depth Research: Analyzing Initial Access Vectors

KELA focused on identifying sensitive patterns frequently exploited by ransomware operators to gain unauthorized access to corporate networks and perform lateral movement. In the chats, BlackBasta members frequently share valid credentials they use for initial access. Based on their conversations, at least some of these credentials appear to be sourced from infostealer logs:

```
    timestamp: 2023-10-19 09:42:48,
    chat_id: !BOpqkyiMnBRfCPXwod:matrix.bestflowers247.online,
    sender_alias: @usernamegg:matrix.bestflowers247.online,
    message: ```
/Citrix/External/
workspace.
virtualworkspace
/Citrix/XenApp/
/vpn/index.html
/vpn/tmindex.html
/remote/login
/Remote/logon.aspx
/+CSCOE+/
/dana/
/dana-na/
SSLVPN
/RDWeb/Pages/
https://webvpn.
https://screenconnect.
https://cloudvpn.
/global-protect/login.esp
XenApp1/auth/login.aspx
/auth/login.aspx
auth/silentDetection.aspx
https://ctx.
/LogonPoint/
http://workspace.
/Citrix/
:8040
:8100
/console/do/login
webvpn.
:943/admin
screenconnect
hostedrmm
connectwise
```

```
/Citrix/RHWeb/
https://account.meraki.com
/vsapres/
/wcc2/
bomgar
kaseya.net
/owa/auth/logon.aspx
/webclient/
esxvm-vcenter1
https://virtual.
/my.policy
https://tm.login.trendmicro.com
/spog/welcome
/sslvpn_logon.shtml
/authenticationendpoint
```
}
{
    timestamp: 2023-10-19 09:42:58,
    chat_id: !BOpqkyiMnBRfCPXwod:matrix.bestflowers247.online,
    sender_alias: @usernamegg:matrix.bestflowers247.online,
    message: вот по этим запросам еще собрали с других логов
```

*A BlackBasta member sends the list of patterns related to sensitive corporate credentials and claims: "We gathered [information] from logs according to these requests"*

KELA has cross-referenced some of the shared credentials with its data lake of infostealing malware logs, which proved that these credentials originated from the logs (see the use case below). In addition, KELA has seen the actors sourcing credentials using vulnerabilities and phishing/spam campaigns, as well as using compromised email credentials and then looking for remote access credentials in the email conversations. Then, these credentials were either used as initial access vector or in lateral movement phase.

Based on around 3000 unique credentials to sensitive resources, shared in BlackBasta chats, top 10 initial access and lateral movement vectors that Black Basta operators used the most:

1. **Microsoft Remote Desktop Web Access (RD Web)**, associated with the pattern `/rdweb/`
2. **Custom VPN and Security Policies Portals**, associated with `/my.policy`
3. **General Remote Login Portals**, associated with `/remote/login`
4. **GlobalProtect by Palo Alto Networks**, associated with `/global-protect/`
5. **Cisco's VPN (WebVPN, AnyConnect)**, associated with `/+CSCOE+/`

These access points—ranging from Remote Desktop Protocol (RDP) portals to VPN endpoints—are prime targets for cybercriminals seeking initial access. Once compromised,
```

they serve as gateways within corporate networks, leading to data exfiltration and eventual ransomware deployment. These credentials are also particularly important at the lateral movement stage, allowing ransomware operators to access and compromise all the network. KELA has noticed that these and other sensitive credentials were discussed both in both contexts. These findings align with other researchers' insights, specifically about vulnerabilities used by BlackBasta to gather initial access.

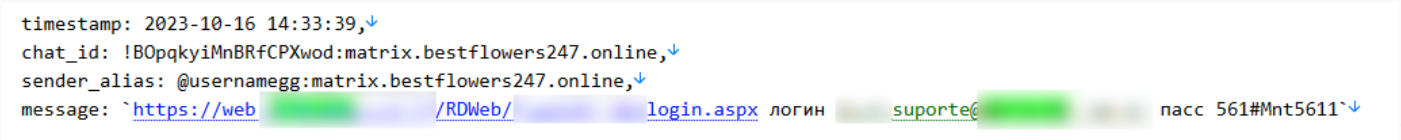
Victim Spotlight: Brazilian company Attacked Through Infostealer Malware Logs

The compromise of a Brazil-based company from the manufacturing & industrial products sector illustrates the group's use of valid credentials for initial access. Here's a detailed look into how the Black Basta group infiltrated and exploited this Brazilian industrial company.

Timeline of the Compromise

October 16, 2023 — Initial Access Through Infostealer Malware Logs

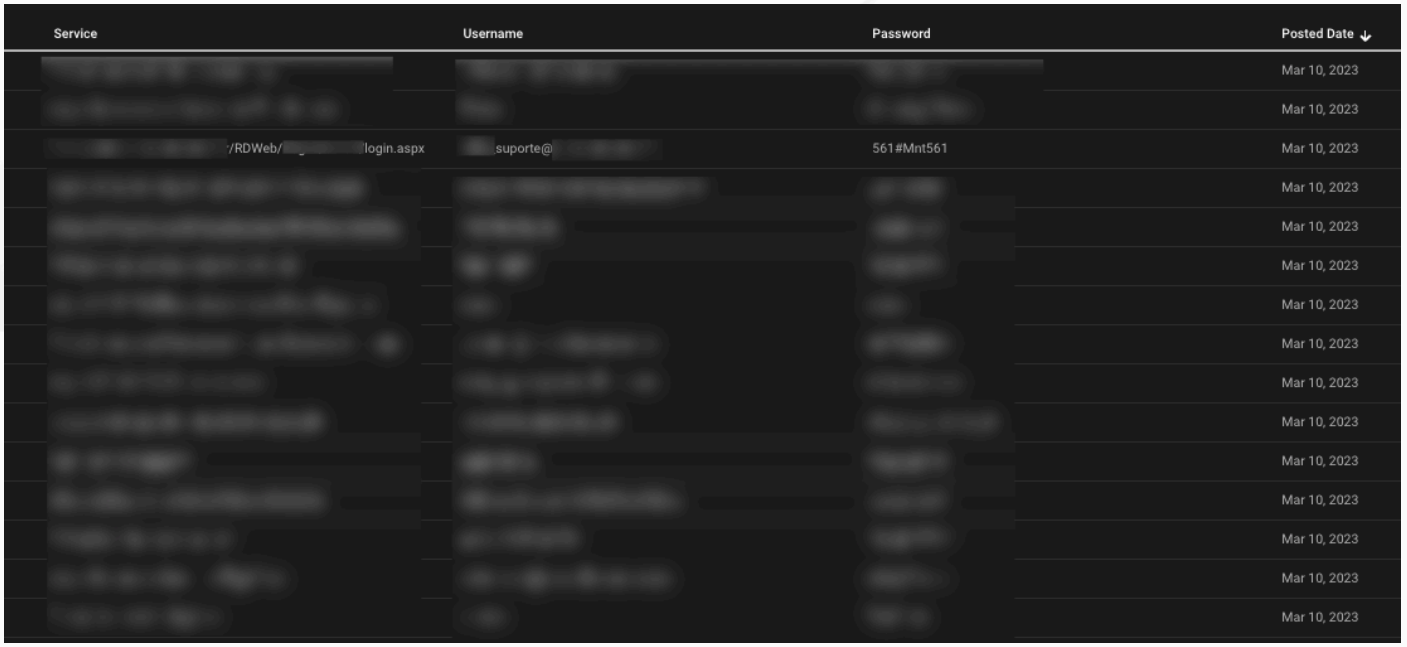
The first indication of the company's breach within Black Basta's internal chats emerged on October 16, 2023. Operators shared an RDweb login portal link, with username and password.



A BlackBasta member shared RDWeb credentials for a Brazil-based industrial company

The same login credentials were observed by KELA to be leaked as part of information stealer malware logs on March 10, 2023. The credentials are associated with a Brazil-based software company, likely a company providing technical support to the original victim. An infected machine contains 50 compromised credentials, some of which appear to be related to additional clients of this software company. Therefore, **the attack appears to have originated from a technical support employee infected by infostealing malware. These exact credentials were leaked more than 6 months before BlackBasta used them as initial access vector in their attack.**

After the attack, the same credentials were shared more than 20 times in various Telegram channels, allowing additional compromise, if the access was not secured following the incident.



A machine infected with infostealing malware, containing a credentials of Brazil-based software company to the BlackBasta victim's RDWeb

Shortly after sharing initial credentials, BlackBasta attackers have exchanged other credential dumps, including hashed credentials, likely after moving laterally through the network. This indicated that the attackers were attempting to escalate privileges and secure persistent access to the victim's systems.

Finally, the actors have exchanged additional information about the victim, gathered the victim's profile Zoominfo, which usually allows actors to assess the victim's likelihood to pay ransom.

October 18, 2023 — Victim Compromised

It apparently took the actors 2 days to compromise the company, steal the data and deploy ransomware, based on the infection date specified in internal logs later.

November 7, 2023 — Preparing for Extortion

On November 7, 2023, Black Basta operators moved into the extortion phase. Chat logs revealed that the attackers had added the victim to their leak site, possibly in hidden mode, and were finalizing materials for public exposure.

November 10, 2023 — Public Disclosure

By November 10, 2023, the victim was officially published on the blog, with the timer for the full data leak after 9 days.

BlackBasta's TTPs

The breach described above clearly illustrates Black Basta's broader operational patterns:

- **RDweb Exploitation:** Initial access was gained through vulnerable RDweb services, likely through valid credentials (T1078) sourced from infostealer malware logs leaked on cybercrime platforms 6 months prior to the attack.
- **Credential Dumping and Hash Extraction:** The attackers quickly moved to harvest credentials and escalate privileges (T1003, T1555), enabling them to control more critical systems.
- **Data Exfiltration and Ransomware Deployment:** After gaining extensive access, the attackers exfiltrated sensitive data (T1041) before deploying ransomware to encrypt critical files (T1486), effectively locking the victim out of their own systems.
- **Victim Profiling:** References to public business directories like ZoomInfo (T1591) indicated that attackers gathered intelligence on the company to strengthen their negotiation leverage and assess the potential ransom value (T1657).

This structured approach, from initial access to data theft and public extortion, showcases Black Basta's strategic use of compromised credentials, internal reconnaissance, and victim profiling to maximize the impact of their ransomware campaigns.

Key Takeaways for Organizations

The BlackBasta leak offers a clear blueprint for organizations to enhance their cybersecurity posture:

1. **Secure Remote Access:** Disable unnecessary RDP services or secure them using VPNs and multi-factor authentication (MFA).
2. **Monitor External Exposure:** Regularly scan for exposed endpoints and patch vulnerabilities promptly, as well use threat intelligence solutions to track assets compromised by infostealers.
3. **Harden Credential Security:** Enforce strong password policies and employ tools to detect leaked credentials.
4. **Implement Incident Response Plans:** Have predefined protocols for ransomware incidents, including data backups and legal considerations.

As KELA continues to analyze the leaked data, more insights are expected to emerge, potentially helping organizations and law enforcement agencies thwart future ransomware attacks.