Black Basta’s blunder: exploiting the gang’s leaked chats

cloudflare.com/threat-intelligence/research/report/black-bastas-blunder-exploiting-the-gangs-leaked-chats/

Threat brief - March 17, 2025

Table of contents

Overview

Black Basta, a notorious ransomware group linked to the Ryuk and Conti criminal enterprises, found itself exposed when a leak of its Matrix chat server surfaced on a Telegram channel. The chat server, hosted on the domain bestflowers247[.]online, was leaked by a user going by the handle ExploitWhispers. The leaked files contained JSON documents detailing timestamps, sender and recipient information, thread IDs, and message content. This data provides actionable insights into the group's operations, helping to identify key accounts and domains used by its members.

The leaked chat data not only offers insight into Black Basta's inner workings but also sheds light on the broader ransomware ecosystem. Understanding how the group navigates this ecosystem provides valuable perspective on its scale and capabilities, with various methods available to assess its effectiveness and impact. One approach is to analyze the cryptocurrency transactions attributed to the criminal enterprise. Kaitlin Martin of the blockchain intelligence firm Chainalysis highlighted this very point in reference to the Black Basta leak:

"On- and off-chain data within the Black Basta leaked chats show how the group relies upon various web services, third-party services, and dark web forums for their operations. Payments to these services by not only Black Basta, but also other ransomware groups, demonstrate the extent to which these services are part of the critical infrastructure of the ransomware ecosystem."

By examining financial transactions and operational dependencies, researchers can better understand the ecosystem in which these groups operate and sustain themselves.

One key aspect of this ecosystem is how ransomware gangs select their victims. While it is certainly true that some industries and regions of the world are disproportionately affected, it seems to be the case that ransomware gangs are not selecting specific victims as much as they are selecting the victims from within a pool of already compromised machines. Ransomware gangs coordinate with criminal teams that infect thousands of machines daily, then review the list of compromised systems to identify those belonging to well-funded enterprises.

In many cases, ransomware gangs purchase initial access to victim hosts from brokers who scour through huge collections of credentials traded and sold in criminal markets and forums. These credentials, harvested by information stealers like LummaC2, often belong to accounts of remote access systems like RDWeb, Citrix, and browser-based VPNs. Understanding this selection process highlights the importance of robust credential security, network segmentation, and proactive threat monitoring to disrupt ransomware operations before they escalate into full-scale attacks.

Prior to the leak, Black Basta ran highly effective ransomware operations, breaching numerous enterprises and inflicting millions of dollars in damages and ransom payments. The leaked chat data provides intelligence on the group's tactics, techniques, and procedures (TTPs), offering visibility into their operations. Using this data, Cloudflare tracked Black Basta activity and uncovered unique insights into their infrastructure and attack methods. Organizations can leverage this information to strengthen their understanding of ransomware gangs like Black Basta to improve their defenses and proactively anticipate their next moves, reducing the risk of falling victim to future attacks.

Cloudforce One dissects Black Basta TTPs

When Cloudforce One obtained the bestflowers.json file, we first enumerated any infrastructure referenced in the chats, focusing on those where we had unique visibility. During this process, we identified techniques employed by Black Basta to facilitate data exfiltration and obscure their remote infrastructure. We conducted a thorough analysis of this infrastructure to assess its potential impact. Our investigation confirmed that many of the domains mentioned in the chats were not used, suggesting they were preemptively created for operational tasks that never materialized.

Black Basta followed a consistent process to set up accounts with infrastructure providers. Group members regularly shared account creation details in the chat, including names, postal addresses, and sign-in credentials. They used corporate-looking domains for email addresses rather than leveraging free email services. When managing their infrastructure, they connected from a variety of networks and inconsistently relied on anonymity services. While their passwords were reasonably complex, they frequently reused the same ones across multiple accounts.

After completing the investigation into Black Basta's infrastructure, we closely reviewed the chats to analyze their methods for initial access, post-exploitation tactics, and negotiation strategies. Black Basta actively leveraged precursor malware like Qakbot to infiltrate a vast number of machines worldwide. After gaining access, they identified high-value targets through post exploitation tasks, including well known techniques like installing persistent beacons, enumerating directories, and escalating privileges.

In some cases, they breached systems using other methods that involved credentials harvested by an information stealer. Cloudforce One discovered some of the associated accounts in collections of credentials traded and freely shared in Telegram channels dedicated to information stealer logs. An example Telegram message involving one of these compromised accounts is depicted in the image below.

Black Basta’s reliance on credential theft and malware underscores the interconnected nature of the ransomware ecosystem—an ecosystem that thrives not only on initial access but also on the financial infrastructure that sustains its operations. Ransom payments flow through cryptocurrency, primarily Bitcoin. The leaked chats contain numerous cryptocurrency addresses that may serve as payment destinations, which can be clustered with others addresses to analyze Black Basta’s financial footprint and impact.

The group also references cryptocurrency when arranging payments for infrastructure, with requestors specifying the amount and sometimes offering multiple cryptocurrency payment options. This mirrors practices observed in the Conti chat leaks from 2022, where team members routinely asked managers to make cryptocurrency payments for virtual private servers, domain names, and VPN services.

How to protect yourself

Many journals and blogs offer ransomware mitigation recommendations, but they often fail to address the root causes of incidents. Ransomware groups typically gain initial access through a few key methods:

- Credential theft and resale: Information stealers harvest remote access credentials, which are then sold to initial access brokers. These brokers, in turn, sell them to ransomware gangs.
- Precursor malware deployment: Threat actors distribute malware like Qakbot and IcedID via widespread spam campaigns. They then identify high-value ransomware targets from the infected machines. Attackers often deliver this malware through email attachments with embedded scripts, or links to files containing scripts, that download and execute malicious payloads.
- Exploiting vulnerable edge devices: Ransomware groups frequently exploit unpatched vulnerabilities in firewalls, VPN appliances, and file-sharing services to gain unauthorized access. Many ransomware incidents originate from these weaknesses.

Follow these recommendations to reduce your exposure to ransomware:

- Disable browser-stored passwords: Enterprises that provide an organizational password manager should prevent users from saving credentials in web browsers.
- Secure remote access systems: Require multi-factor authentication (MFA) for RDP, RDWeb, Citrix, VPNs, and other remote access services exposed to the internet.
- Educate users about bootleg software: Illegitimate software is a primary source of information stealers that harvest credentials later sold to initial access brokers.
- Filter email attachments carefully: Block attachments containing active content, such as macros or scripts, to prevent malware delivery.
- Block risky office macros: Prevent the execution of macros in Office documents flagged with the Mark of the Web, which indicates they were downloaded from the internet.

- Report abuse on Cloudflare’s networks: If you identify suspicious activity, report it at Cloudflare’s Trust Hub.

Indicators of Compromise

The following list of domains, extracted from Black Basta’s chat logs, are associated with malware and data exfiltration. While some of these domains were active in the past and are unlikely to appear in future traffic, conducting a retrospective analysis could help identify any historical connections. Detecting past activity associated with these domains may indicate malware communication with a command-and-control server.

The table includes some of the prominent domains and IP addresses found in the leaked chats, but only provides a sampling of the Black Basta indicators tracked by Cloudforce One. For a full list of indicators along with additional actionable context, see the Cloudforce One Threat Events platform.

Domain Name	IP Resolution	Domain Creation Time
securecloudmanage[.]com	170.130.165.132	2024-03-05 13:04:52.236672+00
helpatelier[.]com	91.240.202.138	2024-03-14 09:38:30.173591+00
ultimateparlor[.]com	89.117.2.54	2024-05-24 12:47:08.455469+00
gentillytransfer[.]com	89.117.2.89	2024-05-27 12:05:53.701176+00
onegamesonline[.]com	89.117.2.90	2024-05-28 08:02:53.092536+00
northhollandservices[.]com	38.180.159.239	2024-05-28 08:42:52.569909+00
flowersmound[.]com	89.117.1.52	2024-05-28 08:54:40.571323+00
emezaconsulting[.]com	131.226.2.133	2024-05-28 12:32:26.106612+00
rogersfilms[.]com	204.93.201.244	2024-05-28 11:45:36.083471+00
vatrafreedom[.]com	84.32.45.66	2024-05-28 12:05:08.75151+00
giencoe[.]com	45.128.135.14	2024-05-28 17:56:52.682707+00

Domain Name	IP Resolution	Domain Creation Time
gites-prevert-vosges[.]com	185.208.158.174	2024-05-28 20:01:12.922021+00
palmspringsvrbo[.]com	191.96.53.148	2024-05-28 20:17:47.319948+00
zink-net[.]com	131.226.2.134	2024-05-28 20:36:42.299783+00
venturarp[.]com	193.160.32.11	2024-05-28 22:02:09.107554+00
schlangenbiss[.]com	216.146.25.106	2024-05-28 21:46:54.425764+00
imatec-centre[.]com	91.196.70.165	2024-05-29 14:07:16.853144+00
dragopale[.]com	185.208.158.185	2024-05-29 15:02:03.129715+00
cars-cn[.]com	191.96.53.158	2024-05-29 14:52:48.606726+00
leaguesecure[.]com	131.226.2.136	2024-05-29 15:36:30.074671+00
deviantnode[.]com	193.160.32.41	2024-05-29 16:43:24.092781+00
onlinesayfa[.]com	128.254.207.82	2024-05-29 16:33:46.219601+00
homegrownhoops[.]net	45.128.133.17	2024-05-31 08:00:14.783392+00
nhatrangtour[.]net	181.215.68.28	2024-05-31 09:11:03.912393+00
dwadesigns[.]net	131.226.2.94	2024-05-31 10:24:33.097051+00
dirtydreams[.]net	193.160.32.51	2024-05-31 12:36:39.13195+00
mickiemckittrick[.]net	216.146.25.53	2024-05-31 12:54:13.799473+00
lowellplumbers[.]net	131.226.2.141	2024-05-31 14:03:58.626894+00

Domain Name	IP Resolution	Domain Creation Time
microsoftapp365[.]com	93.127.217.226	2024-06-12 15:44:22.158827+00
microsoftonline365[.]net	155.94.192.112	2024-06-12 15:57:06.390643+00
microsoft-online-365[.]net	38.132.111.19	2024-06-12 16:11:46.039318+00
proline-billiard[.]com	93.127.217.226	2024-06-12 22:11:56.12727+00
das-inter[.]net	155.94.192.112	2024-06-12 22:26:10.301132+00
apd-disc[.]com	38.132.111.19	2024-06-12 22:38:35.725516+00
halagifts[.]com	217.15.175.191	2024-06-18 18:38:39.9041+00

About Cloudforce One

Cloudflare’s mission is to help build a better Internet. And a better Internet can only exist with forces of good that detect, disrupt and degrade threat actors who seek to erode trust and bend the Internet for personal or political gain. Enter Cloudforce One – Cloudflare’s dedicated team of world-renowned threat researchers, tasked with publishing threat intelligence to arm security teams with the necessary context to make fast, confident decisions. We identify and defend against attacks with unique insight that no one else has.

The foundation of our visibility is Cloudflare’s global network – one of the largest in the world – which encompasses about 20% of the Internet. Our services are adopted by millions of users across every corner of the Internet, giving us unparalleled visibility into global events – including the most interesting attacks on the Internet. This vantage point allows Cloudforce One to execute real-time reconnaissance, disrupt attacks from the point of launch, and turn intelligence into tactical success.