# RANSOMHUB RANSOMWARE DEPLOYED AFTER SIX-DAY ATTACK VIA RDP EXPLOITATION

## Vairav Security News Report

**Date: June 30, 2025**

**Vairav Cyber Threat Intelligence Team**

**Vairav Technology Security Pvt. Ltd.**

Thirbam Sadak 148
Baluwatar, Kathmandu

Phone: +977 4541540
Mobile: +977-9820105900
Email: sales@vairavtech.com

## EXECUTIVE SUMMARY

A recent intrusion detailed by *The DFIR Report* highlights a **highly coordinated six-day attack** where a threat actor compromised an enterprise via exposed **Remote Desktop Protocol (RDP)** and deployed **RansomHub ransomware**. The adversary used **no zero-days**, instead leveraging misconfigurations, password spraying, and legitimate remote management tools to move stealthily and persistently.

## ATTACK TIMELINE & TECHNICAL HIGHLIGHTS

- **Initial Access:**

  – In November 2024, a threat actor conducted password spraying on internet-facing RDP.

  – Success achieved via elevated domain account.

  – Activity traced to 185.190.24.54 and 185.190.24.33 (same ISP).

- **Discovery & Lateral Movement:**

  – Used net, ipconfig, Advanced IP Scanner, and SoftPerfect NetScan.

  – Atera and Splashtop RMM were deployed for persistent access.

  – Extracted credentials via Mimikatz and CredentialsFileView.

- **Exfiltration:**

  – It began on Day 3 using Rclone and cloaked under a nocmd.vbs script.

  – Filtered specific file types (docs, spreadsheets, emails, images).

  – 2.03 GB of data exfiltrated over SFTP on port 443.

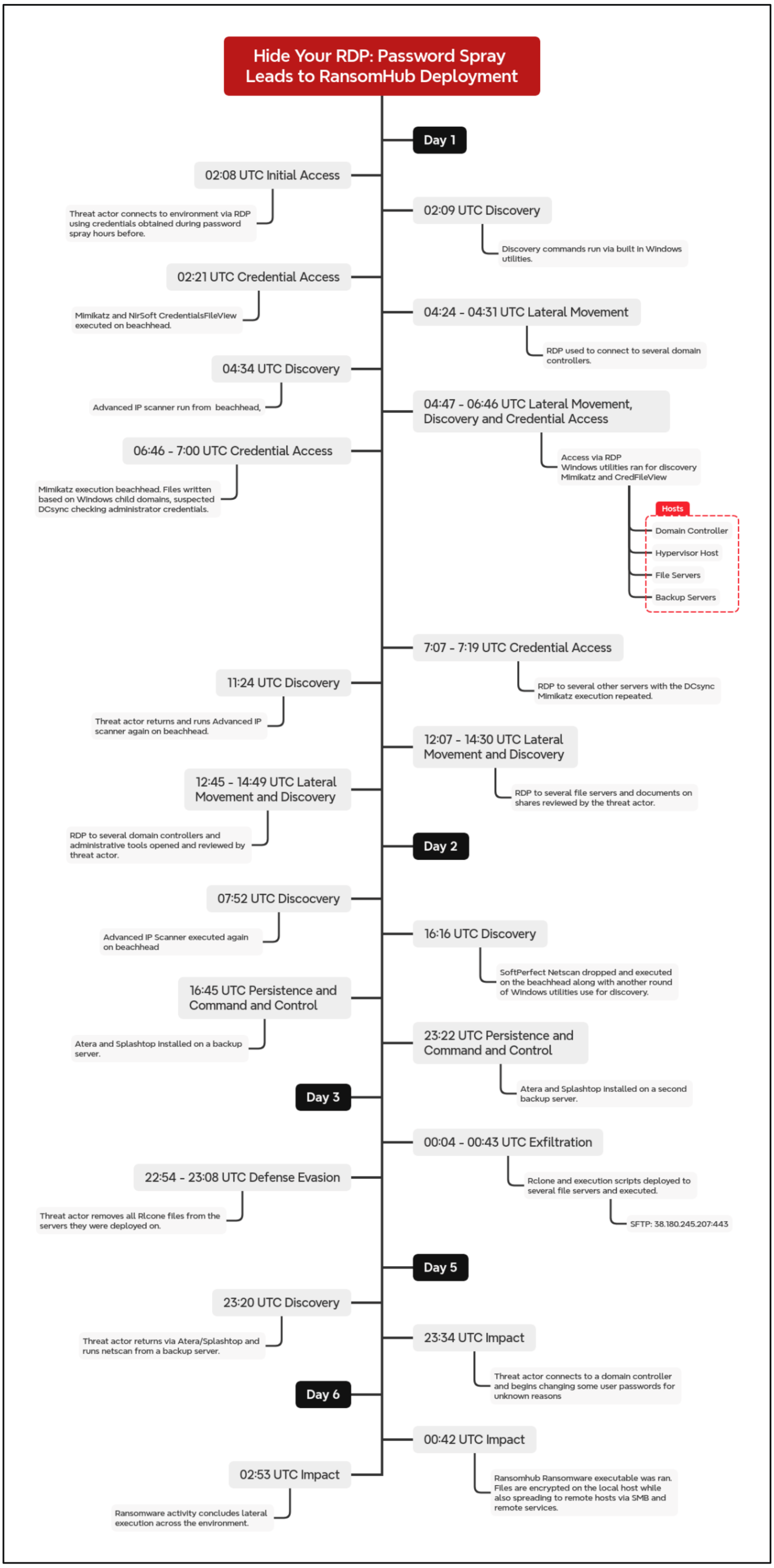
- **Ransomware Deployment (Day 6):**

  – RansomHub binary (amd64.exe) launched via SMB and remote service creation.

  – Executed:

    - vssadmin to delete shadow copies
    - wevtutil to clear logs
    - Symlink abuse and VM termination attempts

  – Encrypted systems left with the RansomHub ransom note.



Hide Your RDP: Password Spray Leads to RansomHub Deployment

Day 1

02:08 UTC Initial Access

Threat actor connects to environment via RDP using credentials obtained during password spray hours before.

02:09 UTC Discovery

Discovery commands run via built in Windows utilities.

02:21 UTC Credential Access

Mimikatz and NirSoft CredentialsFileView executed on beachhead.

04:24 - 04:31 UTC Lateral Movement

RDP used to connect to several domain controllers.

04:34 UTC Discovery

Advanced IP scanner run from beachhead,

04:47 - 06:46 UTC Lateral Movement, Discovery and Credential Access

Access via RDP
Windows utilities ran for discovery
Mimikatz and CredFileView

06:46 - 7:00 UTC Credential Access

Mimikatz execution beachhead. Files written based on Windows child domains, suspected DCsync checking administrator credentials.

7:07 - 7:19 UTC Credential Access

RDP to several other servers with the DCsync Mimikatz execution repeated.

11:24 UTC Discovery

Threat actor returns and runs Advanced IP scanner again on beachhead.

12:07 - 14:30 UTC Lateral Movement and Discovery

RDP to several file servers and documents on shares reviewed by the threat actor.

12:45 - 14:49 UTC Lateral Movement and Discovery

RDP to several domain controllers and administrative tools opened and reviewed by threat actor.

Day 2

07:52 UTC Discocvery

Advanced IP Scanner executed again on beachhead

16:16 UTC Discovery

SoftPerfect Netscan dropped and executed on the beachhead along with another round of Windows utilities use for discovery.

16:45 UTC Persistence and Command and Control

Atera and Splashtop installed on a backup server.

23:22 UTC Persistence and Command and Control

Atera and Splashtop installed on a second backup server.

Day 3

00:04 - 00:43 UTC Exfiltration

Rclone and execution scripts deployed to several file servers and executed.

22:54 - 23:08 UTC Defense Evasion

Threat actor removes all Rlcone files from the servers they were deployed on.

SFTP: 38.180.245.207:443

Day 5

23:20 UTC Discovery

Threat actor returns via Atera/Splashtop and runs netscan from a backup server.

23:34 UTC Impact

Threat actor connects to a domain controller and begins changing some user passwords for unknown reasons

Day 6

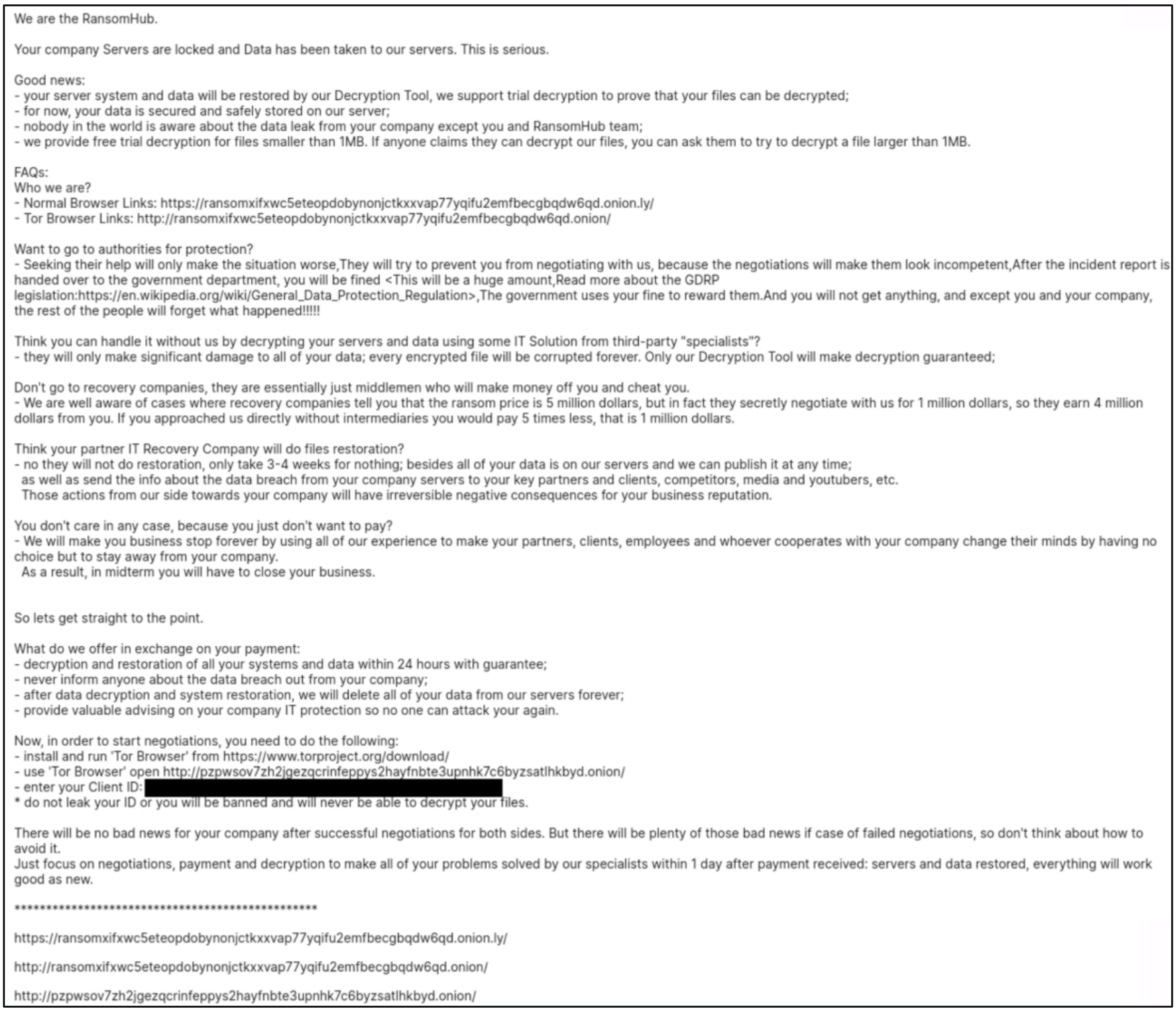
00:42 UTC Impact

02:53 UTC Impact

Ransomhub Ransomware executable was ran. Files are encrypted on the local host while also spreading to remote hosts via SMB and remote services.

Ransomware activity concludes lateral execution across the environment.

*Figure 1: Attack Timeline*



We are the RansomHub.

Your company Servers are locked and Data has been taken to our servers. This is serious.

Good news:
- your server system and data will be restored by our Decryption Tool, we support trial decryption to prove that your files can be decrypted;
- for now, your data is secured and safely stored on our server;
- nobody in the world is aware about the data leak from your company except you and RansomHub team;
- we provide free trial decryption for files smaller than 1MB. If anyone claims they can decrypt our files, you can ask them to try to decrypt a file larger than 1MB.

FAQs:
Who we are?
- Normal Browser Links: https://ransomxifxwc5eteopdobynonjctkxxvap77yqifu2emfbecgbqdw6qd.onion.ly/
- Tor Browser Links: http://ransomxifxwc5eteopdobynonjctkxxvap77yqifu2emfbecgbqdw6qd.onion/

Want to go to authorities for protection?
- Seeking their help will only make the situation worse,They will try to prevent you from negotiating with us, because the negotiations will make them look incompetent,After the incident report is handed over to the government department, you will be fined <This will be a huge amount,Read more about the GDRP legislation:https://en.wikipedia.org/wiki/General_Data_Protection_Regulation>,The government uses your fine to reward them.And you will not get anything, and except you and your company, the rest of the people will forget what happened!!!!!

Think you can handle it without us by decrypting your servers and data using some IT Solution from third-party "specialists"?
- they will only make significant damage to all of your data; every encrypted file will be corrupted forever. Only our Decryption Tool will make decryption guaranteed;

Don't go to recovery companies, they are essentially just middlemen who will make money off you and cheat you.
- We are well aware of cases where recovery companies tell you that the ransom price is 5 million dollars, but in fact they secretly negotiate with us for 1 million dollars, so they earn 4 million dollars from you. If you approached us directly without intermediaries you would pay 5 times less, that is 1 million dollars.

Think your partner IT Recovery Company will do files restoration?
- no they will not do restoration, only take 3-4 weeks for nothing; besides all of your data is on our servers and we can publish it at any time;
 as well as send the info about the data breach from your company servers to your key partners and clients, competitors, media and youtubers, etc.
 Those actions from our side towards your company will have irreversible negative consequences for your business reputation.

You don't care in any case, because you just don't want to pay?
- We will make you business stop forever by using all of our experience to make your partners, clients, employees and whoever cooperates with your company change their minds by having no choice but to stay away from your company.
 As a result, in midterm you will have to close your business.

So lets get straight to the point.

What do we offer in exchange on your payment:
- decryption and restoration of all your systems and data within 24 hours with guarantee;
- never inform anyone about the data breach out from your company;
- after data decryption and system restoration, we will delete all of your data from our servers forever;
- provide valuable advising on your company IT protection so no one can attack your again.

Now, in order to start negotiations, you need to do the following:
- install and run 'Tor Browser' from https://www.torproject.org/download/
- use 'Tor Browser' open http://pzpwsov7zh2jgezqcrinfeppys2hayfnbte3upnhk7c6byzsatlhkbyd.onion/
- enter your Client ID: [redacted]
* do not leak your ID or you will be banned and will never be able to decrypt your files.

There will be no bad news for your company after successful negotiations for both sides. But there will be plenty of those bad news if case of failed negotiations, so don't think about how to avoid it.
Just focus on negotiations, payment and decryption to make all of your problems solved by our specialists within 1 day after payment received: servers and data restored, everything will work good as new.

************************************************

https://ransomxifxwc5eteopdobynonjctkxxvap77yqifu2emfbecgbqdw6qd.onion.ly/

http://ransomxifxwc5eteopdobynonjctkxxvap77yqifu2emfbecgbqdw6qd.onion/

http://pzpwsov7zh2jgezqcrinfeppys2hayfnbte3upnhk7c6byzsatlhkbyd.onion/

*Figure 2: Ransom note of RansomHub*

## INDICATORS OF COMPROMISE (IOCs)

| File Hashes |
|---|
| *ec45ebd938e363e36cacb42e968a960fbe4e21ced511f0ea2c0790b743ff3c67* |
| *25117dcb2d852df15fe44c5757147e7038f289e6156b0f6ab86d02c0e97328cb* |
| *e14ba0fb92e16bb7db3b1efac4b13aee178542c6994543e7535d8efaa589870c* |
| *4775dfb24f85f5d776f538018a98cc6a9853a1840f5c00b7d0c54695f03a11d9* |
| *ffd09a5c27938d1f7424ed66d1474cfeb3df72daabdf10e09f161ed1ffd21271* |

## RECOMMENDATIONS

1. Restrict or disable RDP access from the internet. Require VPN + MFA for remote access.
2. Track Event IDs **4624** (logon), **7045** (new service install), and **Sysmon** logs for script execution or process injection.
3. Memory inspection is used to identify tools like **Mimikatz** or LSASS access patterns.
4. Continuously review software inventory and alert on **Atera**, **Splashtop**, and similar tools.
5. Investigate unusual SFTP data transfers over common web ports.

## REFERENCES

https://thedfirreport.com/2025/06/30/hide-your-rdp-password-spray-leads-to-ransomhub-deployment/

https://securityonline.info/ransomhub-breach-six-day-attack-leveraged-rdp-rmm-tools-mimikatz-for-data-exfiltration-ransomware/

**Vairav Technology Security Pvt. Ltd.**

**Cyber Defender from the land of Gurkha**

Thirbam Sadak 148, Baluwatar
Kathmandu, Nepal
Phone: +977-01-4541540
Mobile: +977-9820105900
Email: sales@vairavtech.com
Website: https://vairavtech.com