# NetSupport RAT ClickFix Distribution: Surge in Attacks Detected

## Vairav Cyber Security News Report

**Date: February 10, 2025**

**Vairav Cyber Threat Intelligence Team**


## Vairav Technology Security Pvt. Ltd.

Thirbam Sadak 148

Baluwatar, Kathmandu

Phone: +977 4541540

Mobile: +977-9820105900

Email: mail@vairavtech.com

## EXECUTIVE SUMMARY

Security researchers at eSentire have reported a significant rise in attacks involving the NetSupport Remote Access Trojan (RAT), a powerful tool that grants attackers full control over compromised systems. The latest wave of attacks leverages the **ClickFix Initial Access Vector (IAV)**, where victims are tricked into executing malicious PowerShell commands, enabling cybercriminals to establish persistence and steal sensitive data. Organizations across IT operations and cybersecurity sectors are urged to enhance defenses against this evolving threat.

## DETAILS OF THE INCIDENT

The recent campaign distributing NetSupport RAT has been attributed to the ClickFix Initial Access Vector (IAV), where victims are socially engineered into executing malicious PowerShell commands. Once installed, NetSupport RAT grants attackers full remote access to compromised systems, allowing them to execute arbitrary commands, monitor user activities, and exfiltrate sensitive data. The attack relies on phishing emails and deceptive links, tricking users into running malicious scripts.

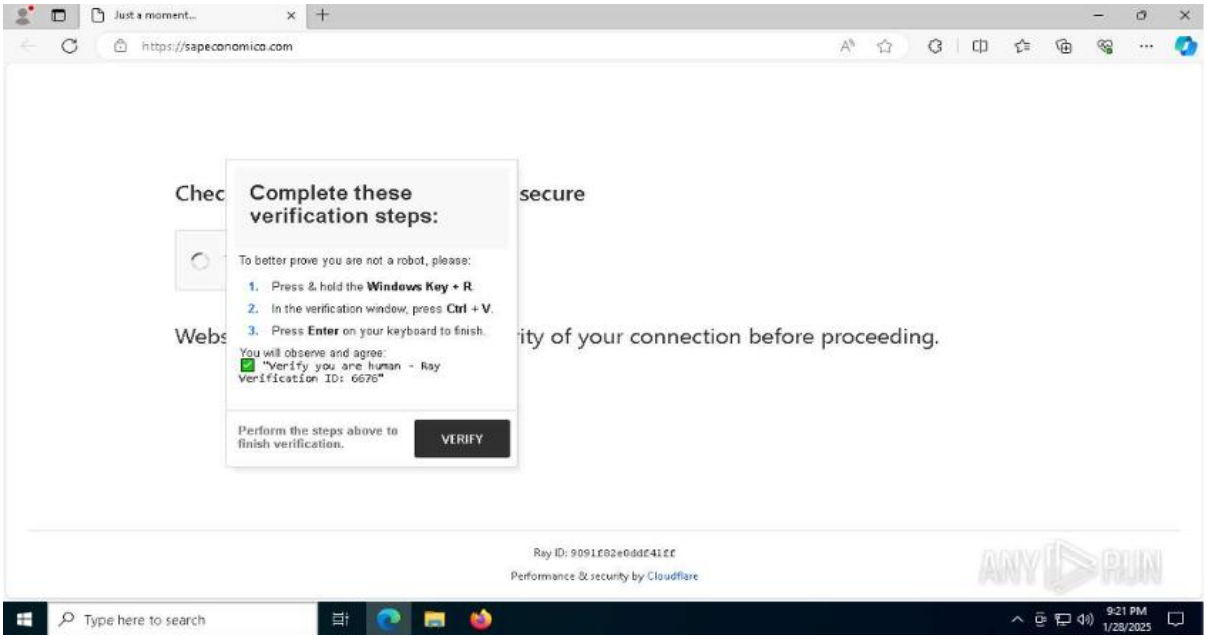


*Figure 1: Phishing page*

The attack was identified through Managed Detection and Response (MDR) investigations, with threat hunts actively being conducted across customer environments. The attacks have primarily targeted organizations in IT operations and cybersecurity sectors.

**Potential Impact**

- Data theft and unauthorized access can lead to fraud, ransom demands, or financial exploitation.
- Remote control capabilities could be used for disruptive activities, sabotage, or deploying additional malware payloads.
- Attackers can extract credentials, corporate documents, and other sensitive files from compromised systems.
- Businesses may face compliance violations and loss of customer trust if customer or company data is compromised.

**Exploitation Methods**

- Users are lured into clicking links that initiate malicious PowerShell execution.
- Attackers use PowerShell-based malware loaders to deliver and execute NetSupport RAT.
- The attack chain starts with targeted phishing messages containing deceptive links.
- NetSupport RAT uses encrypted command-and-control (C2) traffic to avoid detection.
- The infection relies on victims executing malicious scripts unknowingly.

## RECOMMENDED ACTIONS

1. Enhance Email Security – Implement email filtering solutions to detect and block phishing attempts delivering malicious PowerShell commands.
2. Disable Unnecessary PowerShell Features – Restrict PowerShell execution policies and disable untrusted scripts via Group Policy Objects (GPOs) to prevent unauthorized script execution.
3. Monitor and Block Malicious IOCs – Regularly update blocklists with IP addresses, domains, and hashes associated with NetSupport RAT infections.
4. Limit User Permissions – Apply least privilege access controls (LPA) to prevent users from executing unauthorized scripts or installing unauthorized software.
5. Network Segmentation – Restrict RAT communication by segmenting networks and monitoring for unusual outbound traffic.
6. Threat Hunting and Behavioral Analysis – Continuously monitor network and endpoint activity for suspicious behaviors linked to NetSupport RAT.

7. Endpoint Protection and EDR Deployment – Use Endpoint Detection and Response (EDR) solutions to identify and remediate RAT infections in real-time.
8. Regular Software and OS Updates – Patch vulnerable applications and operating systems to prevent exploitation of client-side vulnerabilities.
9. User Awareness Training – Educate employees on social engineering tactics and phishing techniques used in ClickFix-based attacks.
10. Incident Response Readiness – Develop and test incident response playbooks for RAT infections to contain and remediate breaches quickly.

## ADDITIONAL RESOURCES AND OFFICIAL STATEMENTS

https://www.esentire.com/security-advisories/netsupport-rat-clickfix-distribution

https://www.hendryadrian.com/netsupport-rat-clickfix-distribution/

## CONTACT US

**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: mail@vairavtech.com

Website: https://vairavtech.com