Recent Malware Incidents – Attack Methods and Mitigation

Prepared by: Shifna N

Date: August 2025

■ Introduction

Malware is harmful software that hackers use to steal information, damage systems, or demand money. These attacks can affect anyone — from regular people to big companies. In this report, we will look at three recent malware cases: JSCEAL, Lumma Stealer, and Medusa Ransomware. We will explain how each malware worked and what was done to stop it.

■ JSCEAL – Malicious Ads Targeting Crypto Users

●Attack Method:
In July 2025, a new malware called JSCEAL started targeting people who use cryptocurrency apps. Hackers put fake ads on Facebook and other websites. These ads led people to download fake crypto trading apps. When installed, the apps secretly ran malware that stole login details and wallet information. It also used tricks to hide from normal antivirus programs.

●Mitigation/Resolution:
Cybersecurity experts told people to avoid downloading apps from ads. Security software companies updated their tools so they could detect JSCEAL. They also suggested using security programs that watch for unusual activity, not just known viruses.

■ Lumma Stealer – Global Data Theft Operation

What is Lumma Stealer? The malware that infected over 394,000 Windows PCs worldwide

ET Online • Last Updated: May 21, 2025, 10:32:00 PM IST

FOLLOW US SHARE FONT SIZE SAVE PRINT COMMENT

Synopsis

Microsoft, in collaboration with international law enforcement, dismantled Lumma Stealer, a potent malware that compromised over 394,000 Windows computers. The operation seized 1,300 malicious domains and disrupted the malware's command structure. Lumma Stealer, sold on underground forums, was favored for its ease of use and data theft capabilities, posing a significant threat to global digital infrastructure.

Agencies

Representative image

Microsoft has announced a major takedown operation targeting Lumma Stealer, a powerful piece of malware that infected over 394,000 Windows computers globally between March 16 and May 16, 2025.

Lumma Stealer is an information-stealing malware used by cybercriminals to harvest sensitive data such as passwords, credit card details, bank account information, and cryptocurrency wallet credentials. It has also been linked to ransomware attacks, school system breaches, and theft from

96 YEARS FOUNDERS' DAY

Videos

'He has his reason..':

'It's those lips..': Trump's

●Attack Method:
Between March and May 2025, Lumma Stealer infected over 394,000 Windows computers. It was designed to steal passwords, credit card details, bank info, and cryptocurrency wallet data. It worked through more than 1,300 bad websites controlled by hackers.

●Mitigation/Resolution:
Microsoft worked with the FBI, Europol, and other groups to shut down the bad websites and servers. Security updates were sent out, and people were told to change their passwords, turn on two-factor authentication, and check their devices for malware.

FBI and Europol Disrupt Lumma Stealer Malware Network Linked to 10 Million Infections

May 22, 2025 Ravie Lakshmanan Malware / Cybercrime

A sprawling operation undertaken by global law enforcement agencies and a consortium of private sector firms has disrupted the online infrastructure associated with a commodity information stealer known as Lumma (aka LummaC or LummaC2), seizing 2,300 domains that acted as the command-and-control (C2) backbone to commandeer infected Windows systems.

XM Cyber Webinar On-demand

Are You Reporting on Meaningful Risk or Vanity Metrics?

corelight NDR

Cybersecurity helping defend $10T+ IN MANAGED ASSETS $1B IN DAILY TRADES

ELITE NETWORK DEFENSE STARTS HERE

■ Medusa Ransomware – NASCAR Data Breach

Pro > Security

NASCAR confirms user data breach following Medusa ransomware attack

News By Sead Fadilpašić published 28 July 2025

Months after incident, NASCAR confirms losing data to hackers

Comments (0)

When you purchase through links on our site, we may earn an affiliate commission. Here's how it works.

ADVERTISEMENT

College Admissi Requirements f Master's

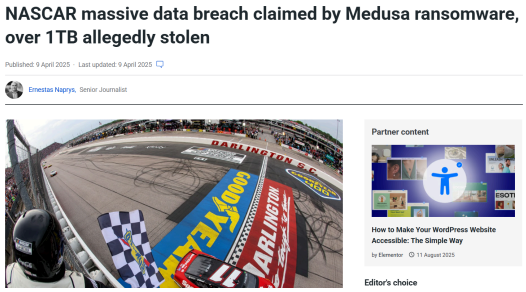
See Search Results For Co Admission Requirements for M

Search Now ›

Get Smart Plan

●Attack Method:
In April 2025, the Medusa ransomware group hacked NASCAR's systems. They claimed to have taken over 1 terabyte of data, including personal information about fans and staff. The hackers locked important files and warned they would publish the stolen data if NASCAR didn't pay them.

●Mitigation/Resolution:
NASCAR worked with cybersecurity experts and law enforcement to secure its systems. They gave free credit monitoring to people whose data was exposed. NASCAR did not say if they paid the ransom, but they managed to restore their systems.



NASCAR massive data breach claimed by Medusa ransomware, over 1TB allegedly stolen

Published: 9 April 2025 · Last updated: 9 April 2025

Ernestas Naprys, Senior Journalist

DARLINGTON S.C.

Partner content

How to Make Your WordPress Website Accessible: The Simple Way

by Elementor 11 August 2025

Editor's choice

■ Conclusion

These three cases show that malware attacks can happen in many ways — fake ads, data-stealing programs, and ransomware. The best way to stay safe is to keep security software updated, avoid suspicious downloads, use strong passwords, turn on two-factor authentication, and act quickly if there is a security problem.

■ References

1. Mandvi. (July 30, 2025). New JSCEAL Attack Targets Crypto App Users to Steal Credentials and Wallets. thecyberexpress.com
2. Lakshmanan, R. (July 30, 2025). Hackers Use Facebook Ads to Spread JSCEAL Malware via Fake Cryptocurrency Trading Apps. thehackernews.com
3. Lakshmanan, R. (May 22, 2025). FBI and Europol Disrupt Lumma Stealer Malware Network Linked to 10 Million Infections. thehackernews.com
4. ET Online. (May 21, 2025). What is Lumma Stealer? The malware that infected over 394,000 Windows PCs worldwide. economictimes.indiatimes.com
5. Naprys, E. (April 9, 2025). NASCAR massive data breach claimed by Medusa ransomware, over 1TB allegedly stolen. cybernews.com
6. Fadilpašić, S. (July 28, 2025). NASCAR confirms user data breach following Medusa ransomware attack. techradar.com