EpsilonRed ransomware group hits one of India's financial software powerhouses

therecord.media/epsilonred-ransomware-group-hits-one-of-indias-financial-software-powerhouses/

June 4, 2021

Nucleus Software Exports, an Indian company that provides lending software to banks and retail stores, has suffered a major ransomware attack that crippled some of its internal networks and encrypted sensitive business information.

The incident took place last Sunday, on May 30, according to a document the company filed on Tuesday with the Indian National Stock Exchange authority.

NUCLEUS SOFTWARE

NUCLEUS SOFTWARE EXPORTS LTD.
CIN : L74899DL1989PLC034594
Corporate Office
A-39, Sector-62, Noida,
Uttar Pradesh, 201307. India.
T.: + 91 . 120 . 4031 . 400
F.: +91 . 120 . 4031 . 672
E.: nsl@nucleussoftware.com
W.: www.nucleussoftware.com

June 1, 2021

The Listing Department **The National Stock Exchange of India Ltd.** **Exchange Plaza, Bandra-Kurla Complex** **Bandra (E)** **Mumbai-400051.** **Fax Nos. 022-26598236/237/238**	**The Listing Department** **Bombay Stock Exchange Limited** **Phiroze Jeejeebhoy Towers,** **25th Floor, Dalal Street** **Mumbai-400001** **Fax No. 022-22722061/41/39**

Dear Sirs,

Sub: Intimation under Regulation 30 of Securities and Exchange Board of India (Listing Obligations and Disclosure Requirements) Regulations, 2015

This is to inform that on 30th May 2021, a breach on our servers was noted and brought to our notice. A ransomware demand was made to us.

We have already initiated steps to take care of the issues. Our cybersecurity team and a specialist team of cyber-specialists is already on the job.

Image: The Record

In a quarterly report filed on Thursday, NSE said it's in the process of containing the damage and recovering and restoring impacted systems.

"So far as sensitive data is concerned, we'd like to assure our customers that there is NO financial data of any customer available/stored with us and therefore the question of any leakage or loss of client data does not arise," the company told Indian financial regulators.

But while an NSE spokesperson has declined to comment on the attack on several occasions, members of the cyber-security community have been able to track down the ransomware strain that was deployed on the company's network.

https://twitter.com/prohack/status/1398968456746127363

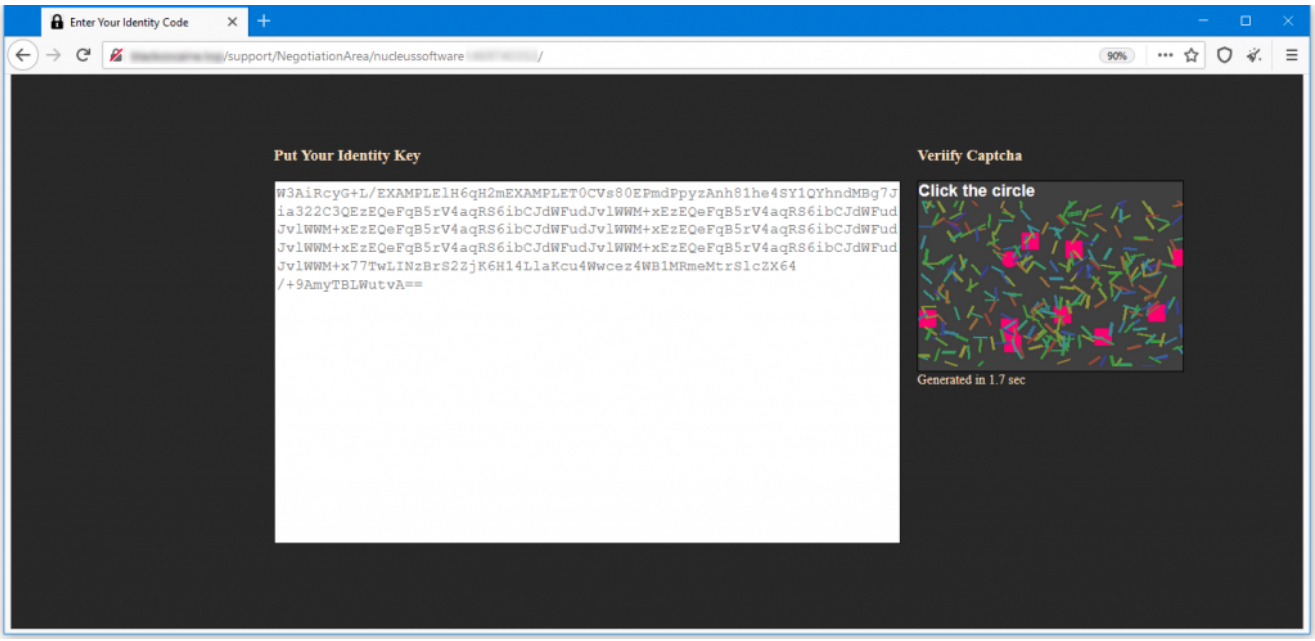

Image: The Record

The ransomware, identified as BlackCocaine, but more commonly known as **EpsilonRed**, is among the most recent ransomware strains discovered.

First spotted last month by UK security firm Sophos, the EpsilonRed gang works by targeting unpatched Microsoft Exchange email servers vulnerable to the ProxyLogon exploit, getting a foothold on the vulnerable system, and then deploying a collection of PowerShell scripts to allow it to move internally inside a victim's network.

In its report, Sophos said the ransomware gang has been successful in at least some of their attacks, discovering payments of $210,000 from previous incidents.

While NSE has not confirmed that the entry point for their breach was an Exchange server nor if it paid the ransom demand, the incident proves that even with tools that Sophos described as "bare-bones," a ransomware gang was capable of infiltrating a major financial software supplier and hold it for ransom with little effort.

But because the ransomware is still new, its code is not yet top-notch. An Emsisoft malware analyst, which took a look at the BlackCocaine/EpsilonRed sample, recommended that companies to reach out in case of an attack, as there might be ways to recover files under certain conditions.

Tags

- BlackCocaine
- EpsilonRed
- Finance
- India
- Ransomware
- security breach

Catalin Cimpanu is a cybersecurity reporter for The Record. He previously worked at ZDNet and Bleeping Computer, where he became a well-known name in the industry for his constant scoops on new vulnerabilities, cyberattacks, and law enforcement actions against hackers.