Over 600 organizations subjected to global EncryptHub attacks

By SC Staff

Published: 2025-02-27 · Archived: 2026-04-05 19:09:00 UTC

Threat Intelligence, Phishing, Malware

(Adobe Stock)

At least 618 organizations around the world had their networks compromised by the EncryptHub threat actor, also known as Larva-208, in a social engineering and spear-phishing attack campaign that has been ongoing since June, according to BleepingComputer.

After leveraging SMS and voice phishing, as well as fraudulent login pages for Microsoft 365, Cisco AnyConnect, and other corporate VPN offerings to facilitate initial access, EncryptHub lured targets into installing AnyDesk, TeamViewer, and other remote monitoring and management software for lateral movement before utilizing PowerShell scripts that deliver the Rhadamanthys, Stealc, and Fickle Stealer infomation-stealing payloads, a report from PRODAFT revealed.

Aside from exfiltrating cryptocurrency wallet and VPN client configuration data, EncryptHub also sought to compromise password manager data and files with certain file extensions and keywords before deploying a custom PowerShell-based data encryptor.

Further analysis showed the presence of the Larva-148 subgroup, from which EncryptHub may be obtaining its domains and phishing kits.

SC Staff

Related

Stryker back online after cyberattack

SC StaffApril 3, 2026

BleepingComputer reports that major U.S. medical device firm Stryker has confirmed resuming full operations three weeks after a cyberattack by Iran-linked hacktivist operation Handala, which led to the wiping of several of its systems.

Get daily email updates

SC Media's daily must-read of the most current and pressing daily news