Ukrainian Institutions Targeted Using HATVIBE and CHERRYSPY Malware

By The Hacker News

Published: 2024-07-23 · Archived: 2026-04-05 15:24:47 UTC

The Computer Emergency Response Team of Ukraine (CERT-UA) has alerted of a spear-phishing campaign that targeted a scientific research institution in the country with malware known as HATVIBE and CHERRYSPY.

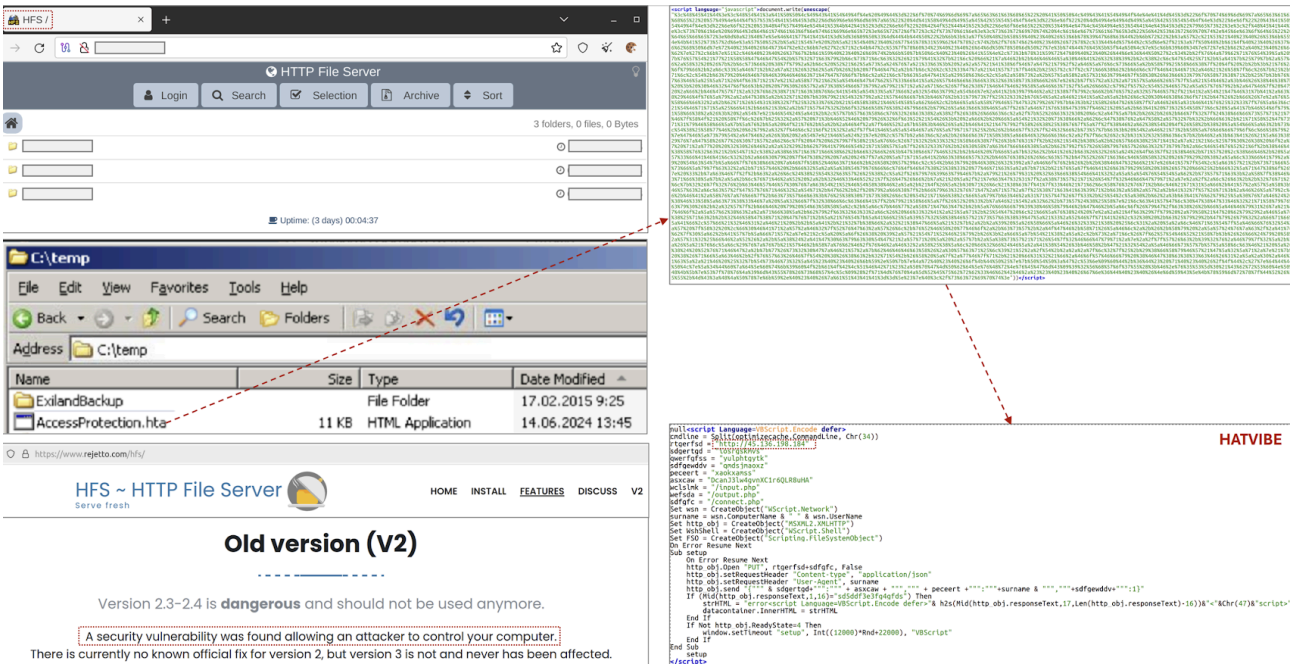
The agency attributed the attack to a threat actor it tracks under the name UAC-0063, which was previously observed targeting various government entities to gather sensitive information using keyloggers and backdoors.

The attack is characterized by the use of a compromised email account belonging to an employee of the organization to send phishing messages to "dozens" of recipients containing a macro-laced Microsoft Word (DOCX) attachment.

Opening the document and enabling macros results in the execution of an encoded HTML Application (HTA) named HATVIBE, which sets up persistence on the host using a scheduled task and paves the way for a Python backdoor codenamed CHERRYSPY, which is capable of running commands issued by a remote server.

CERT-UA said it detected "numerous cases" of HATVIBE infections that exploit a known security flaw in HTTP File Server (CVE-2024-23692, CVSS score: 9.8) for initial access.

UAC-0063 has been associated with a Russia-linked nation-state group dubbed APT28 with moderate confidence. APT28, which is also referred to as BlueDelta, Fancy Bear, Forest Blizzard, FROZENLAKE, Iron Twilight, ITG05, Pawn Storm, Sednit, Sofacy, and TA422, is affiliated with Russia's strategic military intelligence unit, the GRU.



The development comes as CERT-UA detailed another phishing campaign targeting Ukrainian defense enterprises with booby-trapped PDF files embedding a link that, when clicked, downloads an executable (aka GLUEEGG), which is responsible for decrypting and running a Lua-based loader called DROPCLUE.

DROPCLUE is designed to open a decoy document to the victim, while covertly downloading a legitimate Remote Desktop program called Atera Agent using the curl utility. The attack has been linked to a cluster tracked as UAC-0180.

Found this article interesting? Follow us on Google News, Twitter and LinkedIn to read more exclusive content we post.

Source: https://thehackernews.com/2024/07/ukrainian-institutions-targeted-using.html