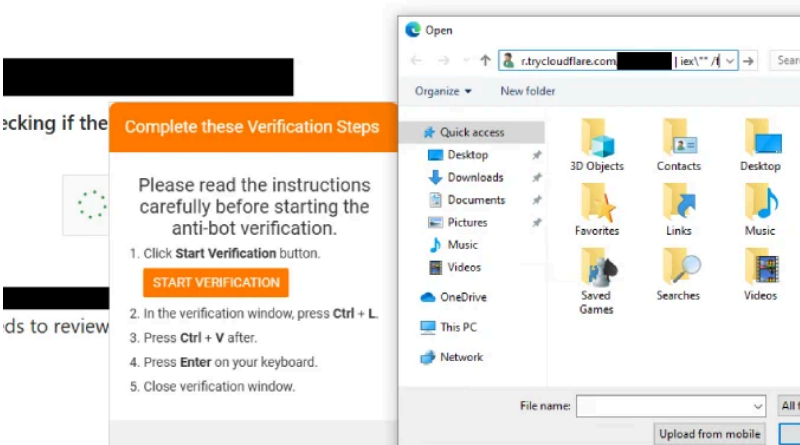


Week of July 14, 2025

Cybersecurity Headlines

Digital Threat Landscape

Cybercrimes, Scams, Threats, Vulnerabilities and Incidents



New PHP-Based Interlock RAT Variant Uses FileFix Delivery Mechanism to Target Multiple Industries

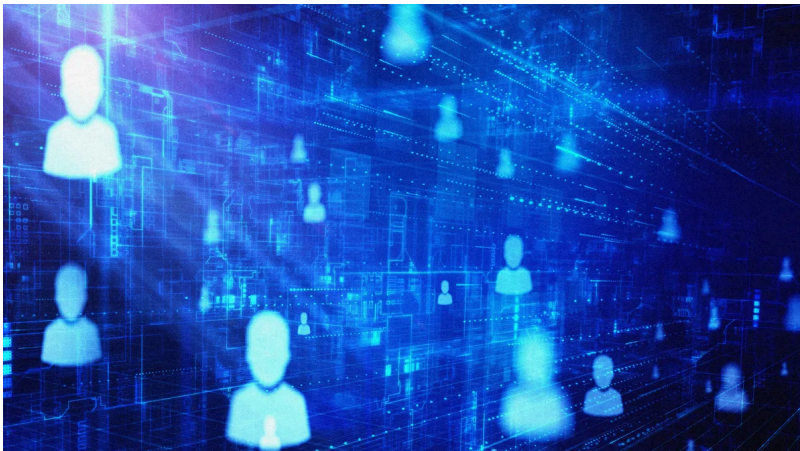
thehackernews.com

Threat actors behind the Interlock ransomware group have unleashed a new PHP variant of its bespoke remote access trojan (RAT) as part of a widespread campaign using a variant of ClickFix called FileFix.

DOGE Denizen Marko Elez Leaked API Key for xAI

krebsonsecurity.com

Marko Elez, a 25-year-old employee at Elon Musk's Department of Government Efficiency (DOGE), has been granted access to sensitive databases at the U.S. Social Security Administration, the Treasury and Justice departments, and the Department of Homeland Security. So it should fill all Americans with a deep sense of confidence to learn that Mr. Elez over the weekend inadvertently published a...



Adoption Agency Data Exposure Revealed Information About Children and Parents

www.wired.com

A trove of 1.1 million records left accessible on the open web shows how much sensitive information can be created—and made vulnerable—during the adoption process.

Securing Core Cloud Identity Infrastructure: Addressing Advanced Threats through Public-Private Collaboration - CISA

www.cisa.gov

In recent years, the cloud landscape has faced increasingly sophisticated threat activity targeting identity and authentication systems. As cloud infrastructure has become more ubiquitous—underpinning key government and critical infrastructure data—s...

Industry Updates

Legislation, Business, Privacy, Updates, Related Technologies



NSA: Volt Typhoon was 'not successful' at persisting in critical infrastructure

therecord.media

Senior cybersecurity officials at the National Security Agency and FBI said the agencies have been successful in addressing some of the Chinese cyber campaigns targeting critical infrastructure in the U.S.

Cybercrime Industry News Technology Get more insights with the Recorded Future Intelligence Cloud. Learn mor

therecord.media

Late last year, Google announced an AI agent called Big Sleep — a project that evolved out of work on vulnerability research assisted by large language models done by Google Project Zero and Google DeepMind. The tool actively searches and finds unknown security vulnerabilities in software.

Senate panel passes Intelligence Authorization Act that takes aim at telecom hacks

therecord.media

The Senate Intelligence Committee on Tuesday approved an annual intelligence authorization bill that aims to augment defenses against digital espionage campaigns like the recent China-linked attack that penetrated multiple U.S. telecommunications networks.















⚡ Weekly Recap: Scattered Spider Arrests, Car Exploits, macOS Malware, Fortinet RCE and More - The Hacker News

thehackernews.com

Call of Duty Makers Takes Game Offline After Reports of RCE Exploit — The makers of Call of Duty: World War 2 announced that the PC version of the game has been taken offline following "reports of an issue." The issue appears to be a security problem...

Please be advised that the following resources and materials are for informational purposes only. The opinions and views expressed in these materials are the opinions of the designated authors and do not reflect the opinions or views of the Commonwealth of Massachusetts, the Executive Office of Technology Services and Security, and/or the Enterprise Risk Management Office, (the Commonwealth). The information posted on this website includes hypertext links or pointers to information created and maintained by other public and/or private organizations. These links and pointers are provided solely for the information and convenience of the user. By selecting a link to an outside website, the user is subject to the privacy, copyright, security, and information quality policies of that website. The Commonwealth is not responsible for transmissions users receive from linked websites.

External Quick links

-  AIScoop
-  BleepingComputer
-  Cisco Talos Intelligence Group
-  CSO Online
-  CyberScoop
-  Cybersecurity Dive
-  Cyware
-  CyberWire
-  FedScoop
-  Government Executive
-  Government Technology
-  ISACA
-  ISSA International
-  Krebs on Security
-  MITRE ATT&CK®
-  NASCIO
-  Schneier on Security
-  SC Media
-  StateScoop
-  The Hacker News
-  The Record