Scottish Cyber Coordination Centre

Daily threat bulletin

24 June 2024

Vulnerabilities

Facebook PrestaShop module exploited to steal credit cards

BleepingComputer - 23 June 2024 11:08

Hackers are exploiting a flaw in a premium Facebook module for PrestaShop named pkfacebook to deploy a card skimmer on vulnerable e-commerce sites and steal people's payment credit card details. [...]

SolarWinds Serv-U Vulnerability Under Active Attack - Patch Immediately

The Hacker News - 21 June 2024 15:24

A recently patched high-severity flaw impacting SolarWinds Serv-U file transfer software is being actively exploited by malicious actors in the wild.The vulnerability, tracked as CVE-2024-28995 (CVSS score: 8.6), concerns a directory transversal bug that could allow attackers to read sensitive files on the host machine.Affecting all versions of the software prior to and including Serv-U 15.4.2

Phoenix UEFI flaw puts long list of Intel chips in hot seat

The Register - 21 June 2024 17:27

Researchers discuss it in same breath as BlackLotus and MosaicRegressor A new vulnerability in UEFI firmware is threatening the security of a wide range of Intel chip families in a similar fashion to BlackLotus and others like it....

Threat actors and malware

Experts found a bug in the Linux version of RansomHub ransomware

Security Affairs - 22 June 2024 10:45

The RansomHub ransomware operators added a Linux encryptor to their arsenal, the version targets VMware ESXi environments. RansomHub ransomware operation relies on a new Linux version of the encrypted to target VMware ESXi environments. Although RansomHub only emerged in February 2024, it has rapidly grown and has become the fourth most prolific ransomware operator over [...]

Multiple Threat Actors Deploying Open-Source Rafel RAT to Target Android Devices

The Hacker News - 24 June 2024 11:34

Multiple threat actors, including cyber espionage groups, are employing an open-source Android remote administration tool called Rafel RAT to meet their operational objectives by masquerading it as Instagram, WhatsApp, and various e-commerce and antivirus apps."It

provides malicious actors with a powerful toolkit for remote administration and control, enabling a range of malicious activities

ExCobalt Cyber Gang Targets Russian Sectors with New GoRed Backdoor

The Hacker News - 22 June 2024 17:58

Russian organizations have been targeted by a cybercrime gang called ExCobalt using a previously unknown Golang-based backdoor known as GoRed."ExCobalt focuses on cyber espionage and includes several members active since at least 2016 and presumably once part of the notorious Cobalt Gang," Positive Technologies researchers Vladislav Lunin and Alexander Badayev said in a technical report

Chinese Hackers Deploy SpiceRAT and SugarGh0st in Global Espionage Campaign

The Hacker News - 21 June 2024 20:12

A previously undocumented Chinese-speaking threat actor codenamed SneakyChef has been linked to an espionage campaign primarily targeting government entities across Asia and EMEA (Europe, Middle East, and Africa) with SugarGh0st malware since at least August 2023."SneakyChef uses lures that are scanned documents of government agencies, most of which are related to various countries' Ministries

Multifactor Authentication Is Not Enough to Protect Cloud Data

darkreading - 21 June 2024 17:15

Ticketmaster, Santander Bank, and other large firms have suffered data leaks from a large cloud-based service, underscoring that companies need to pay attention to authentication.

UK incidents

Synnovis Attackers Publish NHS Patient Data Online

Infosecurity Magazine - 21 June 2024 10:50

Ransomware group Qilin has reportedly published nearly 400GB of data stolen following the attack on NHS provider Synnovis in early June

First million breached Ticketmaster records released for free

Malwarebytes - 21 June 2024 17:01

A cybercriminals is giving 1 million data records from the Ticketmaster breach away for free, saying that Ticketmaster refused to pay