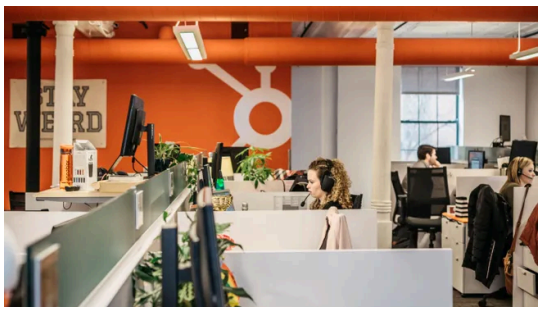
Week of July 1, 2024

Cybersecurity Headlines

Cybercrimes, Scams & Incidents

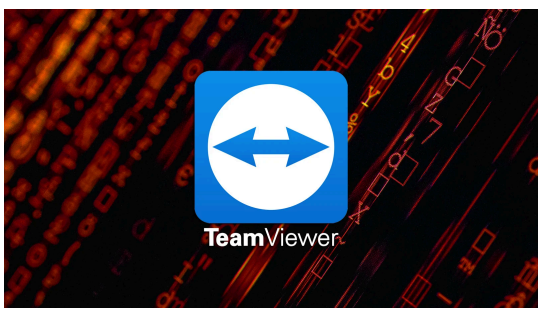
Headlines related to cybercrimes and scams including international cybersecurity news and high-profile incidents like ransomware and malware attacks



HubSpot reports nearly 50 customer accounts compromised

www.cybersecuritydive.com

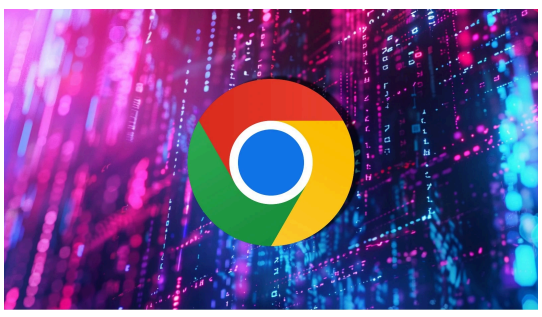
The customer relationship management vendor said it notified all impacted customers, but it has not publicly disclosed how attackers gained unauthorized access.



TeamViewer links corporate cyberattack to Russian state hackers

www.bleepingcomputer.com

RMM software developer TeamViewer says a Russian state-sponsored hacking group known as Midnight Blizzard is believed to be behind a breach of their corporate network this week.



Google Chrome to let Isolated Web App access sensitive USB devices

www.bleepingcomputer.com

Google is working on a new Unrestricted WebUSB feature, which allows trusted isolated web apps to bypass security restrictions in the WebUSB API.

Official Security Bulletins

Headlines from CISA, MS-ISAC, and other official sources

MassDOT Alerts Customers of EZDriveMA Scam

www.mass.gov

BOSTON — The Massachusetts Department of Transportation (MassDOT) is warning EZDriveMA customers of a text message-based scam, also known as smishing. The scammers are claiming to represent the tolling agency and requesting payment for unpaid tolls.

The targeted phone numbers seem to be chosen at random and are not uniquely associated with an account or usage of toll roads.

CISA Releases the Marine Transportation System Resilience Assessment Guide

www.cisa.gov

WASHINGTON – Today, the Cybersecurity and Infrastructure Security Agency (CISA) is releasing an update to the agency's Marine Transportation System Resilience Assessment Guide (MTS Guide) with a new, more accessible web-based tool for stakeholders in the maritime domain. The Resilience Assessment Resource Matrix provides users of the MTS Guide with a curated list of more than 100 off-the-shelf...

Looking Ahead to Better Prepare Today

www.cisa.gov

CISA Releases the Latest Update to the Secure Tomorrow Series Toolkit

Critical infrastructure owners and operators have a lot on their plate. Social, technological, economic, environmental, and political changes contribute to new and evolving risks at seemingly faster rates.

Center for Internet Security (CIS) Releases CIS Controls v8.1 with New Governance Recommendations

www.cisecurity.org

CIS Controls v8.1 represents the latest evolution in cybersecurity standards to improve an enterprise's cybersecurity posture.

CIS Controls v8.1 Mapping to NIST SP 800-171 Rev 2

www.cisecurity.org

This document contains mappings of the CIS Critical Security Controls® (CIS Controls®) v8.1 and CIS Safeguards to NIST SP 800-171 Rev 2.

Why Employee Cybersecurity Awareness Training Is Important

www.cisecurity.org

Not everyone invests in employee cybersecurity awareness training. Here's four experts' thoughts on why you should – and a way to save in the process!

Industry News

Headlines collected from across the cybersecurity industry related to legislation, business, and big tech

Cisco warns of NX-OS zero-day exploited to deploy custom malware

www.bleepingcomputer.com

Cisco has patched an NX-OS zero-day exploited in April attacks to install previously unknown malware as root on vulnerable switches.

Senate leader demands answers from CISA on Ivanti-enabled hack of sensitive systems

therecord.media

Sen. Charles Grassley (R-IA) on Wednesday sent Cybersecurity and Infrastructure Security Agency (CISA) Director Jen Easterly a stern letter seeking documentation and answers relating to a January hack of the agency's Chemical Security Assessment Tool...

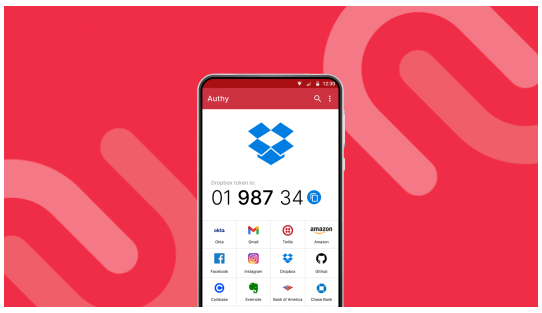
Microsoft warns of elevated risk in Rockwell Automation PanelView Plus CVEs

www.cybersecuritydive.com

Microsoft researchers warn the vulnerabilities can be exploited, potentially resulting in remote code execution and denial of service.

Cybersecurity regulations face 'uphill battle' after Chevron ruling

cyberscoop.com



Hackers abused API to verify millions of Authy MFA phone numbers

www.bleepingcomputer.com

Twilio has confirmed that an unsecured API endpoint allowed threat actors to verify the phone numbers of millions of Authy multi-factor authentication users, potentially making them vulnerable to SMS phishing and SIM swapping attacks.

SneakyChef espionage group targets government agencies with SugarGh0st and more infection techniques

blog.talosintelligence.com

Cisco Talos recently discovered an ongoing campaign from SneakyChef, a newly discovered threat actor using SugarGh0st malware, as early as August 2023.

The Not-So-Secret Network Access Broker x999xx

krebsonsecurity.com

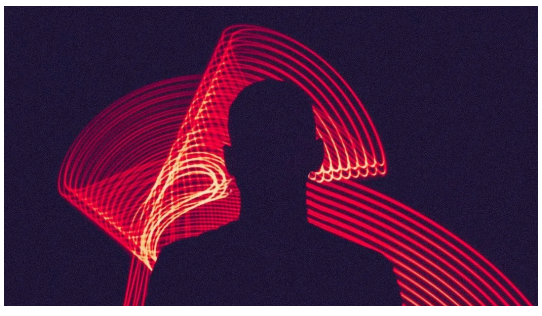
Most accomplished cybercriminals go out of their way to separate their real names from their hacker handles. But among certain old-school Russian hackers it is not uncommon to find major players who have done little to prevent people from figuring out who they are in real life. A case study in this phenomenon is “x999xx,” the nickname chosen by a venerated Russian hacker

New Open SSH Vulnerability

www.schneier.com

It’s a serious one:

The vulnerability, which is a signal handler race condition in OpenSSH’s server (sshd), allows unauthenticated remote code execution (RCE) as root on glibc-based Linux systems; that presents a significant security risk. This race condition affects sshd in its default configuration.



New ransomware group uses phone calls to pressure victims, researchers say

therecord.media

Researchers at cybersecurity company Halcyon say a new ransomware group labeled Volcano Demon does not use a leak site for stolen data, and instead calls victims to pressure them into making an extortion payment.

The Biden administration has looked to regulation to strengthen cybersecurity rules, but a Supreme Court ruling threatens that effort.

Massachusetts names digital accessibility and equity board members | StateScoop

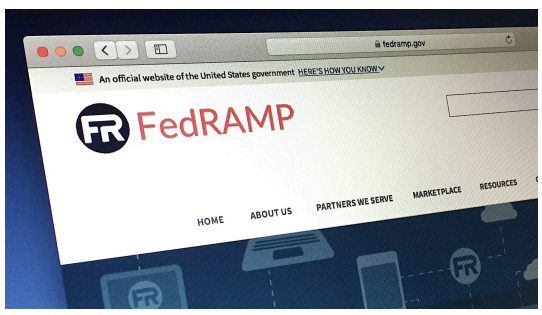
statescoop.com

The Massachusetts Digital Accessibility and Equity Governance Board named three new members, with specializations in accessibility, education, assistive technologies and web accessibility.

‘I don’t see it happening’: CISA chief dismisses ban on ransomware payments

therecord.media

Jen Easterly, the director of the U.S. Cybersecurity and Infrastructure Security Agency, on Thursday poured cold water on suggestions the United States might bring in a ban on ransomware payments.



GSA prioritizes generative AI in FedRAMP authorizations under new framework

fedscoop.com

The framework will initially prioritize chat interfaces, code-generation and debugging tools, and prompt-based image generators, as well as APIs that integrate those capabilities.

Examining the Risks of IT Hero Culture

www.isaca.org

ISACA’s 2024 Annual General Meeting of the Membership will be conducted in person in Schaumburg, Illinois, USA on 24 July at 8 a.m. Central Daylight Time at the ASA Auditorium and virtually.

CDK restores service for small group of car dealers

www.cybersecuritydive.com

The software vendor said it will restore critical services in phases, but warned some integrations with third-party vendors might be delayed.

US businesses struggle to obtain cyber insurance, lawmakers are told

cyberscoop.com

Rising premiums and restrictive policies are creating uncertainty among American businesses about whether insurance policies will cover breaches.

Nearly 4,000 arrested in global police crackdown on online scam networks

therecord.media

International law enforcement said on Thursday that it dismantled online scam networks in several countries, arresting over 3,900 suspects and seizing $257 million in illegally obtained assets.

10 most powerful cybersecurity companies today

www.csoonline.com

With AI and generative AI capabilities on the rise, a shift toward consolidation and platforms over point solutions is redefining the IT security market — as well as its leading vendors.

TeamViewer attributes breach to APT29. LockBit's claim to have breached the US Federal Reserve appears to be false.

www.thecyberwire.com

Microsoft provides updates on Midnight Blizzard email hack. CISA warns chemical facilities of potential breach. Google disrupts Chinese influence operations.

Microsoft warns of 'Skeleton Key' jailbreak affecting many generative AI models

www.csoonline.com

Abusers can trick the model into ignoring responsible AI guardrails and responding with harmful or malicious content.

- Cyware
- CyberWire
- FedScoop
- Government Executive
- Government Technology
- ISACA
- Krebs on Security
- MITRE ATT&CK®
- NASCIO
- NIST
- Schneier on Security
- StateScoop
- The Hacker News
- The Record