

Cybersecurity Headlines

Official Security Bulletins

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

CISA Releases Playbook for Infrastructure Resilience Planning

www.cisa.gov

WASHINGTON – Today, the Cybersecurity and Infrastructure Security Agency (CISA) released a companion guide to the Infrastructure Resilience Planning Framework (IRPF), which provides guidance on how local governments and the private sector can work together to plan for the security and resilience of critical infrastructure services in the face of threats. Dubbed the IRPF Playbook, this supplemental

CIS Benchmarks July 2024 Update

www.cisecurity.org

Here is an overview of the CIS Benchmarks that the Center for Internet Security updated or released for July 2024.

Oracle Quarterly Critical Patches Issued July 16, 2024

www.cisecurity.org

Multiple vulnerabilities have been discovered in Oracle products, the most severe of which could allow for remote code execution.

Multiple Vulnerabilities in Google Chrome Could Allow for Arbitrary Code Execution

www.cisecurity.org

Multiple vulnerabilities have been discovered in Google Chrome, the most severe of which could allow for arbitrary code execution. Successful exploitation of the most severe of these vulnerabilities could allow for arbitrary code execution in the ...



Ransomware Attacks Are Noisy. Learn How to Listen for Them.

www.isaca.org

During the initial intrusion stage of a ransomware incident, the attacker has the advantage.



Why So Many Organizations Underestimate Insider Threats

www.isaca.org

Insider threats remain overlooked by many organizations even though they are potentially more devastating than many incidents coming from external attackers.

Cybercrimes, Scams & Incidents

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



Industry News

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



'Unprecedented': Global IT outage grounds planes and takes broadcasters off air

www.cnbc.com

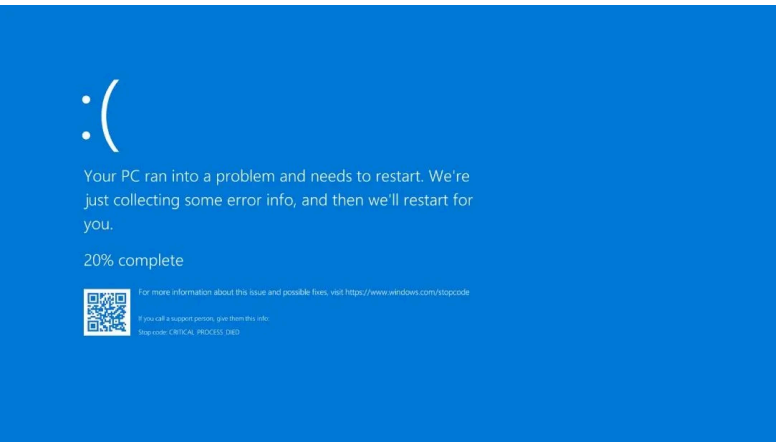
A major IT outage has grounded planes and sent broadcasters off air.



CrowdStrike issue causes major outage affecting businesses around the world

www.cnbc.com

An update by cybersecurity firm CrowdStrike led to a major IT outage on Friday, impacting businesses around the world.



therecord.media

CrowdStrike, one of the world’s leading cybersecurity companies, has said a “defect” rather than a security incident or cyberattack was behind a fault in one of its products that has crashed a large number of Windows workstations globally.

Global Microsoft Meltdown Tied to Bad Crowdstrike Update

krebsonsecurity.com

A faulty software update from cybersecurity vendor Crowdstrike crippled countless Microsoft Windows computers across the globe today, disrupting everything from airline travel and financial institutions to hospitals and businesses online. Crowdstrike said a fix has been deployed, but experts say the recovery from this outage could take some time, as Crowdstrike’s solution needs to be applied manua



BlackCloak | Blog | Why Cybercriminals Target Home Networks

blackcloak.io

This blog explains why cybercriminals target home networks of executives and high-access employees. Learn how to protect your home network.

Judge tosses out most of SEC cybersecurity case against SolarWinds

therecord.media

A U.S. District Court judge has dismissed most of a landmark case against software company SolarWinds, throwing cold water on attempts by the federal government to punish the firm after it was hit by Russia’s Sunburst hacking campaign.



Boston publishes new standard for collecting disability data | StateScoop

statescoop.com

Boston published a new standard that outlines language city departments should use when collecting data about disabilities.



Google eyes security startup Wiz for \$23B in its largest-ever acquisition

www.csoonline.com

The deal could face a lot of regulatory hurdles, according to analysts.



New AI task force convenes state and local officials | StateScoop

statescoop.com

The NewDeal Forum announced a new AI task force convening state and local government officials to explore AI’s potential to improve government services.



FedRAMP 'undeniably' in state of limbo without final OMB modernization guidance, Rep. Connolly says

fedscoop.com



CISA Warns of Actively Exploited RCE Flaw in GeoServer GeoTools Software

thehackernews.com

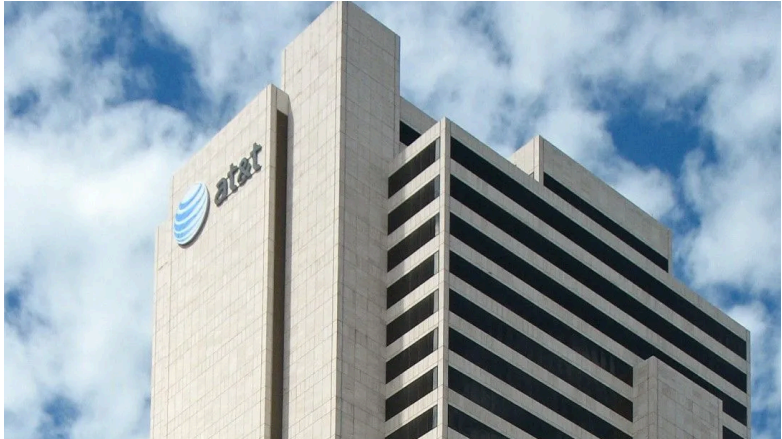
CISA warns of actively exploited vulnerability in GeoServer GeoTools. Critical flaw allows remote code execution. Users urged to patch immediately.



New BugSleep malware implant deployed in MuddyWater attacks

www.bleepingcomputer.com

The Iranian-backed MuddyWater hacking group has partially switched to using a new custom-tailored malware implant to steal files and run commands on compromised systems.



AT&T reportedly paid ransom for deletion of stolen call logs after culprit allegedly detained

therecord.media

The scale of AT&T's data breach continued to widen over the weekend, with reports emerging that AT&T paid a \$370,000 ransom to a hacker who obtained the logs of calls and texts to more than 100 million customers.

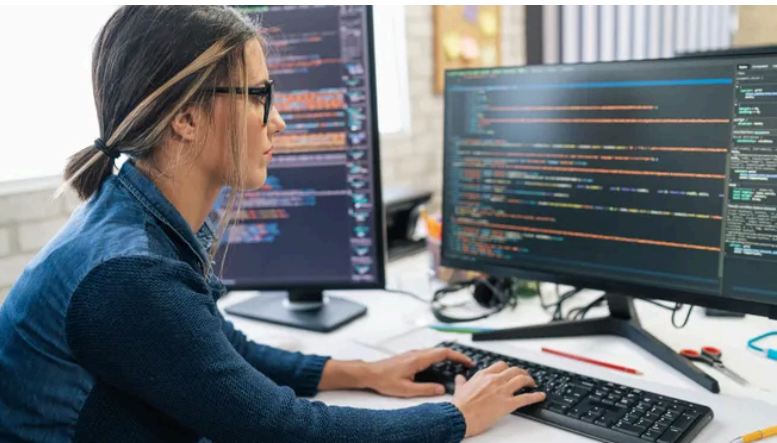
Researchers: Weak Security Defaults Enabled Squarespace Domains Hijacks

krebsonsecurity.com

At least a dozen organizations with domain names at domain registrar Squarespace saw their websites hijacked last week. Squarespace bought all assets of Google Domains a year ago, but many customers still haven't set up their new accounts. Experts say malicious hackers learned they could commandeer any migrated Squarespace accounts that hadn't yet been registered, merely by supplying an email...



However, that “limbo” is an improvement from where the program was not long ago, Connolly admitted.



Nearly 1 in 3 software development professionals unaware of secure practices

www.cybersecuritydive.com

The knowledge gap, identified in a Linux Foundation report, comes as malicious hackers increasingly target critical vulnerabilities.



76% of SaaS companies use 'dark patterns,' analysis finds

www.cybersecuritydive.com

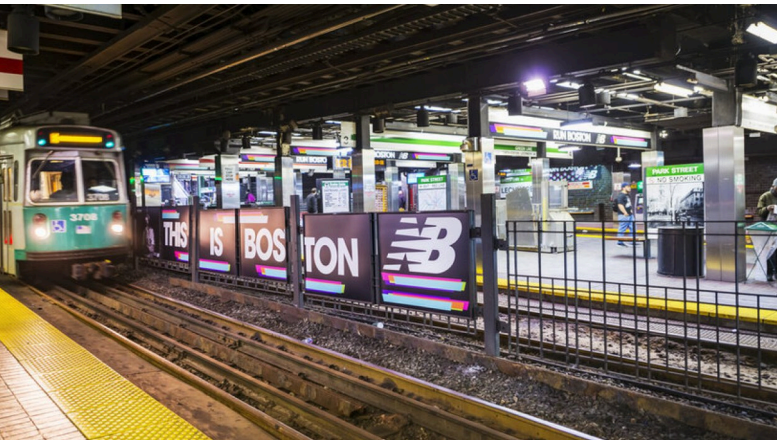
With federal regulators and states clamping down on the practice, companies might take a hard look at how they're presenting information on their websites and in their apps.



Threat Prevention & Detection in SaaS Environments - 101

thehackernews.com

Learn about the growing identity-based threats in SaaS applications and how to mitigate them with ITDR and robust identity security measures



Boston to Roll Out Tap-to-Pay Transit Fare Payment Option

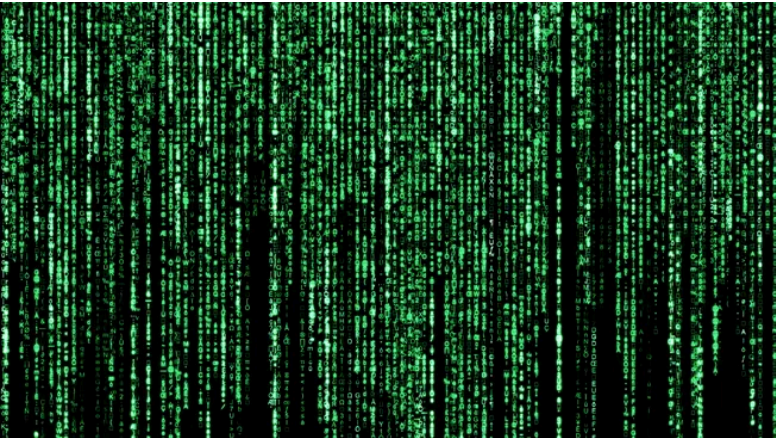
www.govtech.com

The Massachusetts Bay Transportation Authority, in partnership with Cubic Transportation Systems, will introduce new contactless tap-to-ride technology, where riders tap a credit card or digital wallet to pay transit fares.

Wallets tied to CDK ransom group received \$25 million two days after attack

cyberscoop.com

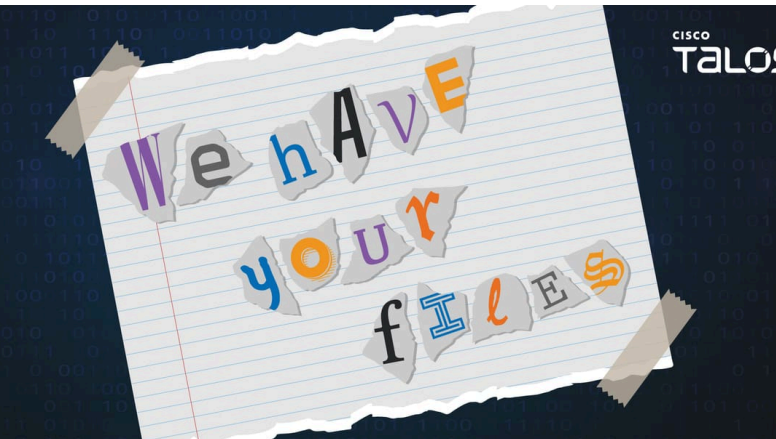
Researchers say the wallets that received the large bitcoin payment are tied to BlackSuit affiliates



Ransomware leak site posts jumped 20% in Q2

www.cybersecuritydive.com

Threat groups claimed attacks on 1,237 organizations during the quarter, marking an increase from Q1. U.S.-based businesses accounted for more than half of all victims, Reliaquest found.



Inside the ransomware playbook: Analyzing attack chains and mapping common TTPs

blog.talosintelligence.com

Based on a comprehensive review of more than a dozen prominent ransomware groups, we identified several commonalities in TTPs, along with several notable differences and outliers.



Impact of data breaches is fueling scam campaigns

blog.talosintelligence.com

Data breaches have become one of the most crucial threats to organizations across the globe, and they've only become more prevalent and serious over time.



Email addresses of 15 million Trello users leaked on hacking forum

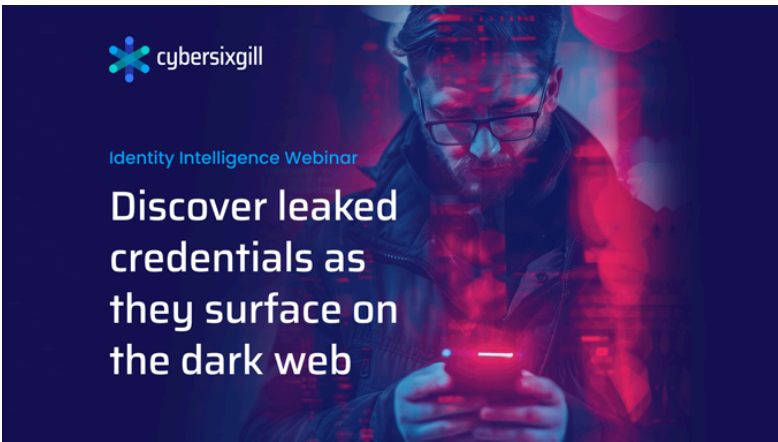
www.bleepingcomputer.com



The current state of MITRE ATT&CK.

www.thecyberwire.com

Rick Howard, The CSO, Chief Analyst, and Senior Fellow at N2K Cyber, discusses the current state of MITRE ATT&CK with CyberWire Hash Table guests Frank Duff, Tidal Cyber's Chief Innovation Officer, Amy Robertson, MITRE Threat Intelligence Engineer an...







Safeguard Personal and Corporate Identities with Identity Intelligence

thehackernews.com

Discover the importance of identity intelligence in mitigating cyber threats and protecting sensitive data. Learn how Cybersixgill can help secure you

A threat actor has released over 15 million email addresses associated with Trello accounts that were collected using an unsecured API in January.

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.

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