Teckedin.com®

May 1, 2022

Privacy & Security

Webinars/Events

5/5/2022 1:00 pm CST	ARMA & Zasiio - Poking Holes in Big Buckets – The Impacts of Data Privacy

Latest Tech News

Google says people can now more easily have more personal information removed from search results	In an effort to stop identity theft, Google also said it may remove government IDs, Social Security numbers, tax information, credit card numbers, handwritten signatures, any images of certain IDs, login details, medical records and any other form of identifying official records.
This phishing campaign delivers malware that steals your passwords and chat logs	Detailed by cybersecurity researchers at Bitdefender, RedLine Stealer is offered to in a malware-as-a-service scheme, providing even low-level cyber criminals with the ability to steal many different forms of sensitive personal data – for as little as $150.
Smallstep increases focus on zero-trust and automated certificates, secures $26M	Smallstep aims to enable organizations to take control of their production identity, allowing them to secure their infrastructure by identifying everything and everyone, issuing credentials, encrypting data and communications, and enforcing a robust security policy.
CrowdStrike unveils tools to fight threats to cloud-native applications	This platform employs real-time attack indicators, threat intelligence, developing adversary trade craft and enriched telemetry from across the enterprise, to enable hyper-accurate detections, automated protection and remediation, elite threat hunting and prioritized visibility of vulnerabilities.
Armo raises $30M to bring open-source security to Kubernetes	Kubescape works by scanning configuration files such as YAML and Helm, clusters and worker nodes for misconfigurations and known vulnerabilities from MITRE ATT&CK and other DevOps frameworks and vulnerability databases.
Bug bounty platform Intigriti raises $23M to empower ethical hackers	Intigriti's platform connects companies with ethical hackers so they can provide an incentive for them to test the security of their websites and applications. A company will offer a bounty to any hacker that's able to breach the security of a specific website or application.
Trend Micro launches new attack surface management platform	The technology can automatically discover and secure internal and external facing assets with attack surface discovery, cyber risk analysis, threat mitigation and response.
Washington state universities get funding to create cybersecurity programs as industry demand grows	At the federal level, the Biden administration's FY 2023 budget includes an 11% increase for cybersecurity spending, Cybersecurity Dive reported.
Obsidian Security raises $90M to secure companies' software-as-a-service applications	Inactive accounts in a SaaS application can become a cybersecurity issue if their login credentials are compromised. Hackers could use stolen login credentials to access the data that a company stores in cloud services. Obsidian's platform can spot inactive accounts, as well as cases where sensitive business data is accessible to more users than is strictly necessary, a scenario that also presents cybersecurity risks.

Analysis, Reports, Trends

VentureBeat - Report: 95% of IT leaders say Log4shell was 'major wake-up call' for cloud security	The research found that 87% feel less confident about their cloud security now than they did prior to the incident. The research also found that even 3 months after the incident, 77% of IT leaders are still dealing with Log4J patching with 83% stating that Log4Shell has impacted their ability to address business needs.
TMCNet - Research: Log4Shell a Wake Up Call For Cloud Security With Patching Efforts and Business Impacts Continuing Into 2022	The research also found that even 3 months after the incident, 77% of IT leaders are still dealing with Log4J patching with 83% stating that Log4Shell has impacted their ability to address business needs.
Infosecurity - Five Eyes Agencies List Top 15 Most Exploited Bugs of 2021	In addition to the top 15 list, the security agencies provided an extra list of bugs to patch, including noteworthy systems such as the Accellion File Transfer Appliance (FTA) which was targeted en masse by a cybercrime group with links to FIN11 and Clop ransomware.
VentureBeat - The super malicious insider and the rise of insider threats	Forty-two percent of actionable incidents were related to IP and data theft, including the theft of trade secrets, source code and active collusion with a foreign nexus.
ZDNet - Inside a ransomware incident: How a single mistake left a door open for attackers	While BlackCat has a reputation for running a sophisticated ransomware operation, it was a simple technique that allowed malicious cyber criminals to gain initial access to the network – exploiting an SQL injection vulnerability in an internet-exposed SonicWall SRA 4600 firewall.
VentureBeat - Report: Orgs spend 3,850 hours annually cleaning up email-based cyberattacks	The study confirms that, despite investments in secure email gateways and user security awareness training, bad actors continue to use social engineering emails to breach organizations' defenses. The resulting attack remediation requires 175 hours to resolve each breach, and the most common breach type is compromised Office 365 login credentials (account takeover).

Blogs

Check out our curated blogs. We separate by category. Privacy and Security is one of our popular sections.

https://docs.teckedin.info/docs/curated-blogs-privacy-and-security

Investing In Secular Trends: Hacking And Cybersecurity

Apr 29, 2022 Seeking Alpha

The exponential growth of data creates an attractive, and growing, target for hackers seeking financial gain. Click here to read more.

President Biden Urges Increased Cybersecurity for Business Owners

Apr 29, 2022 digitaljournal.com/

President Biden Urges Increased CybersecurityIn a statement released March 21, 2022, President Joe Biden addressed concerns regarding the nation's

Security leaders relying more heavily on MSPs amid talent crunch

Apr 29, 2022 helpnetsecurity.c...

The cyber skills gap is driving a significant increase in reliance on external managed service providers, according to Neustar.