Teckedin.com

July 4,, 2021

Privacy & Security Excerpts

Webinars/Events

7/8/2021 12:00 pm MST	IBM & Mid-Market Tech Talks - Effective Cyber Resiliency & Ransomware Protection
7/6/2021 - 7/8/2021	Secure and Private Compute Summit
7/8/2021 11:30 am MST	TAC Security - Risk and Vulnerability Management On a Single Platform
7/12/2021 - 7/15/2021	DFRWS 2021 - Digital Forensics
7/16/2021 - 7/17/2021	The Diana Initiative 2021 is a two-day conference to elevate, inspire, and support women/non-binaries of all races, cultures, and backgrounds through every stage of their information security career with education,
7/22/2021 7:00 am MST	Lexology/Didomi - Privacy Made Positive™ – privacy transparency is an opportunity, not a burden

Latest Tech News

LinkedIn's 1.2B Data-Scrape Victims Already Being Targeted by Attackers	Just days after a yet another data-scraping operation aimed at LinkedIn was discovered, evidence has popped up in a popular hacker forum that the vast amount of lifted data is being collated and re-
Kaseya urges customers to immediately shut down VSA servers after ransomware attack	"We engaged our internal incident response team and leading industry experts in forensic investigations to help us determine the root cause of the issue. We notified law enforcement and government cy-
TrickBot Spruces Up Its Banking Trojan Module	Kryptos Logic researchers explained that the development is notable given that TrickBot has evolved from its banking-trojan days to focus almost exclusively on acting as a first-stage, multipurpose malware
Microsoft warns of Windows 'PrintNightmare' vulnerability that's being actively exploited	While Microsoft hasn't rated the vulnerability, it allows attackers to remotely execute code with system-level privileges, which is as critical and problematic as you can get in Windows.
PayPal phishing attack uses legitimate services to bypass Google Workspace security	The domain of the email sender is securesever dot net, which is hosted by GoDaddy. After clicking "Restore Account Access," victims are taken to a phishing page that resembles the PayPal login portal. The page asks victims for their email or mobile number and PayPal account password.
Google adds new checks to Scorecards, an automated tool that scans open-source software for security	Scorecards works by auto-generating a risk score for any open-source project based on metrics such as its security policy, a code review and continuous test coverage using fuzzing and static code analysis tools

Analysis, Reports, Trends

AiThority - 20 Martech Leaders on What they Think About Google's Decision to Continue Cookie Tracking	"Moving away from third party cookies and toward first-party data puts consumers in control of how their data is used while companies can deliver real-time experiences that are most relevant to
VentureBeat - Aqua Security: 50% of new Docker instances attacked within 56 minutes	The majority of attacks were focused on crypto mining, which may be perceived as "more of a nuisance than a severe threat," Aqua Security noted. However, 40% of attacks also involved backdoors to gain access to the victim's environment and networks.
AiThority - Digital Advertising Trends Disrupted by Increasing Security And Quality Violation	According to the latest report on digital advertising trends, online advertising is no longer safe and secured from malvertising and fraud. One in every 150 impressions is either deemed dangerous
The State of Kubernetes Security	Twice each year for its State of Kubernetes Security report, StackRox examines how companies are adopting Kubernetes, containers and cloud-native technologies while meeting the challeng-
VentureBeat - 7 keys to evaluating zero trust security frameworks	Interest in zero trust grew more than 230% in 2020 over 2019, according to Gartner. Twenty to thirty new vendors claim to have zero trust-native products or services every quarter, with at least a dozen or more entirely new solutions announced at the RSA Conference
ZDNet - IT leaders say cybersecurity funding being wasted on remote work support: survey	Respondents were more split on the top concerns, with 39% referencing software vulnerabilities, 37% expressing concern about reused usernames and passwords and 36% mentioning unsecured networks. Another 29% said device theft was also a concern.
ZDNet - Hackers are trying to attack big companies. Small suppliers are the weakest link	Researchers at cybersecurity company BlueVoyant examined hundreds of SMB defence company subcontractor firms and found that over half of them had severe vulnerabilities within their networks, including unsecured ports and unsupported or unpatched software