Teckedin.com®

October 17, 2021

Privacy & Security

Webinars/Events

10/19/2021 10:00 am PST	Gigamon/Ordr - Lunch & Learn: Exposing Ransomware-as-a-Service
10/20/2021 3:00 pm EST	DevOps.com - How to Scale Governance, Compliance and Security through GitHub Actions
10/21/2021	SecurityMetrics Summit 2021
10/26/2021 - 10/27/2021	Cybersecurity Symposium for Smart Cities 2021
11/4/2021	Tessian - Human Layer Security Summit

Latest Tech News

Whole Foods customer records among 82M exposed due to vulnerable database	Overall, the size of the leaked data is approximately 9.57GB. The total number of records when first discovered (between April 25 and July 11) was 28,035,225. After the notice was sent (between April 25 and July 30), the total number of records rose to 82,099,847.
CryptoRom Scam Rakes in $1.4M by Exploiting Apple Enterprise Features	“They strike up a friendship, using the dating game as a ruse, but then quickly move to money, this time in the guise of them doing you a big favor by offering you a chance to join an ‘unbeatable’ investment opportunity,”
MagicCube raises $15M to replace cybersecurity chips with software	It’s estimated that retailers and banks spend billions of dollars a year on in-store payment systems. MagicCube says that i-Accept enables companies to accept payments using a smartphone app instead of specialized hardware, which lowers equipment expenses.
Verizon’s Visible Wireless Carrier Confirms Credential-Stuffing Attack	On Wednesday, Verizon’s Visible – an all-digital, uber-cheap wireless carrier – confirmed what customers have been complaining about on Reddit and Twitter all week: They lost control of their accounts; had their passwords and shipping addresses changed; and some got stuck with bills for pricey new iPhones.
OpenSea ‘Free Gift’ NFTs Drain Cryptowallet Balances	Users of OpenSea, the world’s largest digital-collectible marketplace, have found their cryptocurrency wallets ripped off thanks to cyberattackers weaponizing security bugs that allowed them to highjack user accounts.
Facebook is researching AI systems that see, hear, and remember everything you do	It imagines AI systems that are constantly analyzing peoples’ lives using first-person video; recording what they see, do, and hear in order to help them with everyday tasks.
Deepfence open-sources ThreatMapper to find and rank software vulnerabilities	While Deepfence has always offered an enterprise edition and a community incarnation known as ThreatMapper, the latter of these is now being released under an open source license from tomorrow, October 14.
30 Mins or Less: Rapid Attacks Extort Orgs Without Ransomware	In less time than it takes to get a stuffed crust pizza delivered, a new group called SnapMC can breach an organization’s systems, steal their sensitive data, and demand payment to keep it from being published, according to a new report from NCC Group’s threat intelligence team — no ransomware required.

Analysis, Reports, Trends

Gizmodo - Ransomware Hackers Reportedly Targeted 3 Different U.S. Water Facilities This Year Alone	A joint advisory, published Thursday by the Cybersecurity and Infrastructure Security Agency, the FBI, the NSA, and the Environmental Protection Agency, reveals three previously unknown incidents involving malware attacks on water systems throughout the country
VentureBeat - Cybersecurity report reveals critical business vulnerabilities	According to data from a new Randori report, titled “The Attack Surface Report,” 1 in 15 organizations are running vulnerable versions of SolarWinds. Some of these versions contain exploits that can provide attackers with unauthenticated remote code execution, granting the hackers access to full control of a system.
ZDNet - Critical infrastructure security dubbed 'abysmal' by researchers	On Friday, CloudSEK published a new report exploring ICSs and their security posture in light of recent cyberattacks against industrial, utility, and manufacturing targets. The research focuses on ICSs available through the internet.
VentureBeat - Why enterprises are massively subcontracting cybersecurity work	"A surprisingly large percentage — 56% — of organizations are addressing the hiring crunch by subcontracting at least some portion of their cybersecurity teams, most often to managed service providers.”
VentureBeat - Report: 24% of companies have paid millions in audit fees	Twenty-four percent of companies have paid millions in audit true-up fees over the past three years to companies such as Microsoft, Oracle, and IBM, according to a new report from Flexera.
VentureBeat - Cyberattack response time averages 2 days, report finds	Respondents cited a lack of threat prevention specific to never-before-seen malware as one of their top concerns, followed by a shortage of qualified staffers and hidden persistence tactics.
AiThority - Cybersecurity Tool Sprawl Drives Plans to Outsource Detection and Response	The global independent research uncovered serious challenges facing SOC teams tasked with detecting and responding to emerging cyber threats. Those defending organizations with more than 10,000 employees have an average of almost 46 monitoring tools in place.