June 27, 2021

Privacy & Security Excerpts

Webinars/Events

6/29/2021 2:00 pm EST	ITProToday/Veeam - Teams Data Protection: 8 Facts You NEED to Know!
6/30/2021 11:00 am EST	Veriato - Ransomware Has Evolved, And So Should Your Company
6/30/2021 9:00 am PST	Managed Security Services Forum Los Angeles County
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, collaboration, and resources.
7/22/2021 7:00 am MST	Lexology/Didomi - Privacy Made Positive™ – privacy transparency is an opportunity, not a burden

Latest Tech News

Mozilla launches Rally, a Firefox plugin to let users provide browsing data for research	That means Rally gives users the tools to understand what data is being seen, provides the rules under which it is being collected, encrypts it end-to-end, anonymizes it so that it cannot be tracked back to them
Intermedia Combats Rise of Advanced Cyberattacks With Launch of AI Guardian Email Defense	Acting like a security expert sitting beside users, AI Guardian goes to work by using artificial intelligence to analyze and automatically flag suspicious email from different advanced attack types and, through real-time actions, enables an organization to automatically quarantine and/or delete threats – threats that are designed to evade traditional detection.
Eftpos sends connectID digital identity solution live	ConnectID acts as a broker between identity service providers and merchants or government agencies that require identity verification, such as proof of age, address details, or bank account information.
Musk-Themed '$SpaceX' Cryptoscam Invades YouTube Advertising	YouTube fans have been swindled out of almost $1 million (and counting) thanks to an extremely convincing fake SpaceX crypto-coin campaign that uses a popular decentralized finance protocol called
Crackonosh malware abuses Windows Safe mode to quietly mine for cryptocurrency	The infection chain begins with the drop of an installer and a script that modifies the Windows registry to allow the main malware executable to run in Safe mode.
Microsoft Defender for Endpoint finally gets this important feature	With the new capability, Defender for Endpoint will be able to sniff out unmanaged workstations, servers, and mobile endpoints (Windows, Linux, macOS, iOS, and Android) that haven't yet been onboarded and then secure them.

Analysis, Reports, Trends

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
ZDNet - Average time to fix critical cybersecurity vulnerabilities is 205 days: report	WhiteHat Security researchers said the top five vulnerability classes seen over the last three months include information leakage, insufficient session expiration, cross site scripting, insufficient
SiliconANGLE - Research finds container infrastructure can be exploited in under one hour	The use of botnets continues to rise and they were found to be swiftly finding and infecting new hosts as they become vulnerable. Notably, 50% of new misconfigured Docker container application programming interfaces are attacked by botnets within 56 minutes of being set up.
VentureBeat - Remote onboarding to drive digital identity verification spend	Businesses will be spending $16.7 billion globally on digital identity verification technology by 2026, according to Juniper Research, representing a 77% growth on the anticipated $9.4 billion spend
ZDNet - Ransomware: Too many firms are still willing to pay up if attacked	However, a quarter of respondents fear that their current security procedures might not offer full protection against ransomware threats, describing them as 'somewhat' or 'very' insufficient.