

COVID-19 RELATED CYBER NEWS

Week 14: Saturday 27th June to Friday 3rd July
Compiled by Barry Gooch

COVID-19 RELATED ARTICLES

MAIN SOURCES	
Bleeping Computer	https://www.bleepingcomputer.com
Bloomberg	https://www.bloomberg.com/europe
BBC i-player technology news	https://www.bbc.co.uk/news/technology
Business Insider	https://www.businessinsider.com/international?r=US&IR=T
CNET	https://www.cnet.com/news/
Cyware	https://cyware.com/cyber-security-news-articles
Dark Reading	https://www.darkreading.com
Fireeye	https://www.fireeye.com
Fraud Watch International	https://fraudwatchinternational.com
The Guardian	https://www.theguardian.com/uk
Hackmageddon	https://www.hackmageddon.com
Help Net Security	https://www.helpnetsecurity.com
Info Security Magazine	https://www.infosecurity-magazine.com
Malwarebytes	https://blog.malwarebytes.com/category/malwarebytes-news/
Naked Security (Sophos)	https://nakedsecurity.sophos.com
Reuters technology news	https://uk.reuters.com/news/technology
Risk IQ	https://www.riskiq.com/blog/analyst/covid19-cybercrime-update/?utm_source=homepage&utm_medium=carousel-covid19-cybercrime-blog
Security Boulevard	https://securityboulevard.com
SC Magazine UK	https://www.scmagazineuk.com
SC Magazine US	https://www.scmagazine.com
Sky News	https://news.sky.com/uk
Threatpost	https://threatpost.com
Wall Street Journal	https://www.wsj.com/news/technology
We Live Security	https://www.welivesecurity.com
ZDnet	https://www.zdnet.com/2/

SATURDAY 27th June 2020

- **New Zealand vulnerable to cyber attacks, Key says**
<https://www.stuff.co.nz/business/300043661/new-zealand-vulnerable-to-cyber-attacks-key-says>
- **US, allies prep for cyber attacks in time of COVID-19 with virtual war games**
<https://www.wraltechwire.com/2020/06/27/us-allies-prep-for-cyber-attacks-in-time-of-covid-19-with-virtual-war-games/>
- **Homeland Security Warns That Weak Passwords Can Lead to Ransomware Attacks**
<https://www.cyclonis.com/homeland-security-warns-weak-passwords-can-lead-to-ransomware-attacks/>
- **Russian hackers attack remote US workers with ransomware**
<https://www.indiatvnews.com/technology/news-russian-hackers-attack-remote-us-workers-with-ransomware-629700>
- **COVID-19 scammers unwittingly email cyber security expert**
<https://www.9news.com.au/national/scammers-using-veil-of-covid19-pandemic-unwittingly-email-cyber-security-expert/6be8dc56-0815-4217-bd87-9b72a83577bf>
- **Australia: 20% Increase in Financial fraud During Pandemic**
<https://bitnewstoday.com/news/australia-20-increase-in-financial-fraud-during-pandemic/>
- **Gift card fraud: 1 lakh PAN cards misused**
<https://www.tribuneindia.com/news/haryana/gift-card-fraud-1-lakh-pan-cards-misused-105044>
- **Bank ALERT: Cyber criminals to target customers promising free COVID-19 tests**
<https://www.indiatvnews.com/fyi/bank-alert-cyber-criminals-target-customers-for-free-covid19-tests-cyber-fraud-629624>
- **Global Security in a Flux – The COVID-19 Effect**
<http://diplomatist.com/2020/06/27/global-security-in-a-flux-the-covid-19-effect/>
- **J&K PDD suffers ‘Cyber Attack’: CE**
<http://www.thenorthlines.com/jk-pdd-suffers-cyber-attack-ce/>
- **Why Data Management Needs to be a Priority as Cybercrime Explodes**
<https://www.itnewsafrika.com/2020/06/why-data-management-needs-to-be-a-priority-as-cybercrime-explodes/>
- **Operation In(ter)ception: How a LinkedIn Message can Result in Espionage**
<https://www.itnewsafrika.com/2020/06/operation-interception-how-a-linkedin-message-can-result-in-espionage/>
- **Analyzing The World’s Top 3 Cybercrime Countries**
<https://www.emergingpayments.org/article/analyzing-the-worlds-top-3-cybercrime-countries/>
- **Security Risks of Contactless Payments**
https://securityintelligence.com/articles/the-security-risks-of-contactless-payment/?&web_view=true

- **US Local Government Services Targeted by New Magecart Credit Card Skimming Attack**
https://blog.trendmicro.com/trendlabs-security-intelligence/us-local-government-services-targeted-by-new-magecart-credit-card-skimming-attack/?&web_view=true
- **The Case Against EU Cyber Sanctions for the Bundestag Hack**
https://www.lawfareblog.com/case-against-eu-cyber-sanctions-bundestag-hack/?&web_view=true
- **GeoVision access control devices let hackers steal fingerprints**
<https://www.bleepingcomputer.com/news/security/geovision-access-control-devices-let-hackers-steal-fingerprints/>
- **The scammers promising poison on Facebook**
https://www.bbc.co.uk/news/blogs-trending-53078118?intlink_from_url=https://www.bbc.co.uk/news/technology&link_location=live-reporting-story

SUNDAY 28th June 2020

- **What is a cyber attack, what are the targets and who is behind them? Inside the hacking attacks bombarding Australia**
<https://www.abc.net.au/news/2020-06-29/hacking-cyber-attacks-espionage-china/12398802>
- **Australia invests in Cyber Threat Intelligence platform to shield itself from Cyber Attacks**
<https://www.cybersecurity-insiders.com/australia-invests-in-cyber-threat-intelligence-platform-to-shield-itself-from-cyber-attacks/>
- **Chinese malware used in attacks against Australian orgs**
<https://www.bleepingcomputer.com/news/security/chinese-malware-used-in-attacks-against-australian-orgs/>
- **Swiss Re calls for transparency from companies over cyber attack risks**
<https://www.ft.com/content/13bed6c2-dd89-4c22-a86a-d9a584dd2b06>
- **Cyber crime in India mostly targets business email, says police official**
<https://www.deccanchronicle.com/technology/in-other-news/280620/cyber-crime-in-india-mostly-targets-business-email-says-police-offici.html>
- **Security Incidents in Healthcare Infrastructure during COVID-19 Crisis**
<https://www.safecare-project.eu/?p=588>
- **Organised crimes witness a hike amidst coronavirus pandemic**
<https://www.newdelhitimes.com/organised-crimes-witness-a-hike-amidst-coronavirus-pandemic/>
- **FEATURE: Cybercrime is on the increase during lockdown**
<https://www.sabcnews.com/sabcnews/feature-cybercrime-on-the-increase-during-lockdown/>
- **Cybersecurity, data security and privacy: Seven questions E&P company boards need to ask**
<https://www.worldoil.com/magazine/2020/july-2020/features/cybersecurity-data-security-and-privacy-seven-questions-ep-company-boards-need-to-ask>
- **COVID-19 Impact on Fraud Management in Banking**
<https://www.idc.com/getdoc.jsp?containerId=US46633120>
- **Why Trump's administration is going after Europe's privacy rules**
<https://www.politico.eu/article/donald-trump-administration-gdpr/>
- **The Great Hotel Hack: Adventures in Attacking the Hospitality Industry by Etizaz Mohsin**
<https://www.hospitalitynet.org/video/69000550.html>
- **An Embattled Group of Leakers Picks Up the WikiLeaks Mantle**
https://www.wired.com/story/ddosecrets-blueleaks-wikileaks/?&web_view=true
- **Russian Cybercrime Boss Burkov Gets 9 Years — Krebs on Security**
https://krebsonsecurity.com/2020/06/russian-cybercrime-boss-burkov-gets-9-years/?&web_view=true
- **Why certain characters "glitch" Gmail, YouTube, and Twitter**
<https://www.bleepingcomputer.com/news/technology/why-certain-characters-glitch-gmail-youtube-and-twitter/>

MONDAY 29th June 2020

- **'Offensive capability': \$1.3b for new cyber spies to go after hackers**
<https://www.smh.com.au/politics/federal/offensive-capability-1-3b-for-new-cyber-spies-to-go-after-hackers-20200629-p557bk.html>
- **UCSF pays \$1.14 million to decrypt files after ransomware attack**
<https://www.healthcareitnews.com/news/ucsf-pays-114-million-decrypt-files-after-ransomware-attack>
- **Evil Corp's latest ransomware project spreading fast**
<https://www.computerweekly.com/news/252485331/Evil-Corps-latest-ransomware-project-spreading-fast>
- **E-learning data exposure. Ransomware attacks (at least one is successful).**
<https://thecyberwire.com/newsletters/privacy-briefing/2/125>
- **KnowBe4 Research Finds Data Breaches and Insider Threats Keep Australian Organisations Up At Night**
<https://www.knowbe4.com/press/knowbe4-research-finds-data-breaches-and-insider-threats-keep-australian-organisations-up-at-night>
- **Nefilim Gang Leveraged Citrix Gateway Exploit**
<https://cyware.com/news/nefilim-gang-leveraged-citrix-gateway-exploit-6da5fa37>

- **Industrial Cybersecurity Market : Facts, Figures**
<https://jewishlifeneews.com/uncategorized/industrial-cybersecurity-market-facts-figures/>
- **The Highest Case of Indonesian Malware in the Asia Pacific**
<https://www.archyde.com/the-highest-case-of-indonesian-malware-in-the-asia-pacific/>
- **ATO shifts focus on COVID-19 fraud**
<https://www.charteredaccountantsanz.com/member-services/technical/tax/tax-in-focus/ato-shifts-focus-on-covid19-fraud>
- **India chargesheets 12 people in ponzi scam that duped 118,288 investors**
<https://indianewengland.com/2020/06/india-chargesheets-12-people-in-ponzi-scam-that-duped-118288-investors/>
- **French Ex-Prime Minister Found Guilty of Fraud**
<https://www.voanews.com/europe/french-ex-prime-minister-found-guilty-fraud>
- **Lookers uncovers £19m shortfall in fraud investigation**
<https://www.ft.com/content/ace71bf2-baff-4b97-8cf9-64e25647968f>
- **3 ways governments can address cybersecurity in the post-pandemic world**
<https://www.weforum.org/agenda/2020/06/3-ways-governments-can-address-cyber-threats-cyberattacks-cybersecurity-crime-post-pandemic-covid-19-world/>
- **Click and despair: remote workers come under cyber-attack**
<https://pressportal.co.za/it-new-media-and-software/story/20193/click-and-despair-remote-workers-come-under-cyber-attack.html>
- **HOW STATES COULD RESPOND TO NON-STATE CYBER-ATTACKERS**
<https://www.clingendael.org/publication/how-states-could-respond-non-state-cyber-attackers>
- **10 Charged in \$1 Billion Medical Insurance Fraud**
<https://www.voanews.com/economy-business/10-charged-1-billion-medical-insurance-fraud>
- **Kosovo Has Undertaken Critical Steps in Cybersecurity, Says New Cybersecurity Capacity Maturity Model Assessment**
<https://www.worldbank.org/en/news/press-release/2020/06/29/kosovo-has-undertaken-critical-steps-in-cybersecurity>
- **Hackers set return-to-work traps**
<https://uktechnews.co.uk/2020/06/29/hackers-set-return-to-work-traps/>
- **Gang uses DoppelPaymer ransomware to attack Mitsubishi Paper site in Germany**
<https://www.itwire.com/security/gang-uses-doppelpaymer-ransomware-to-attack-mitsubishi-paper-site-in-germany.html>
- **Effective Cybersecurity in Hospitals During #COVID19 and Beyond**
<https://www.infosecurity-magazine.com/news-features/effective-cybersecurity-hospitals/>
- **Attackers Targeted Dozens of U.S. Companies with WastedLocker**
<https://www.tripwire.com/state-of-security/security-data-protection/attackers-targeted-dozens-of-u-s-companies-with-wastedlocker>
- **What Will The Insurance Industry Look Like Post COVID-19**
<https://www.finance-monthly.com/2020/06/what-will-the-insurance-industry-look-like-post-covid-19/>
- **Car Crime Soared During COVID19 Pandemic**
<https://digitpol.com/car-crime-soared-at-covid-pandemic/>
- **CLOP Ransomware Shows Its Presence Again, Targets Indian Conglomerate**
<https://cyware.com/news/clop-ransomware-shows-its-presence-again-targets-indian-conglomerate-fbecf72a>
- **Twitter Apologized on Yet Another Data Breach of Business Accounts**
<https://cyware.com/news/twitter-apologized-on-yet-another-data-breach-of-business-accounts-d0583c84>
- **Hakbit + GuLoader + Microsoft Excel. What's Going On?**
<https://cyware.com/news/hakbit-guloader-microsoft-excel-whats-going-on-914f4415>
- **Multi-Stage Attack Campaigns; This Time Ryuk Delivers the Final Blow**
<https://cyware.com/news/multi-stage-attack-campaigns-this-time-ryuk-delivers-the-final-blow-9078b332>
- **CryptoCore Hacker Group Made the Big Bucks**
<https://cyware.com/news/cryptocore-hacker-group-made-the-big-bucks-462ad27f>
- **Docker Servers Infected With DDoS Malware - XORDDoS, Kaiji Variants**
<https://cyware.com/news/docker-servers-infected-with-ddos-malware-xorddos-kaiji-variants-38730f4f>
- **Golang Worm Broadens its Horizons**
<https://cyware.com/news/golang-worm-broadens-its-horizons-8c500fe8>
- **Evil Corp is Back With New TTPs, Deploys New WastedLocker Ransomware**
<https://cyware.com/news/evil-corp-is-back-with-new-ttps-deploys-new-wastedlocker-ransomware-fbd9d001>
- **Hackers Mining Monero Through Cryptojacking Docker Images**
<https://cyware.com/news/hackers-mining-monero-through-cryptojacking-docker-images-c36270e9>
- **Lucifer Malware Leverages Windows Vulnerabilities for Cryptomining, DDoS Attacks**
<https://cyware.com/news/lucifer-malware-leverages-windows-vulnerabilities-for-cryptomining-ddos-attacks-fde67601>
- **Ransomware is now your biggest online security nightmare. And it's about to get worse**
https://www.zdnet.com/article/ransomware-is-now-your-biggest-online-security-nightmare-and-its-about-to-get-worse/?&web_view=true
- **Massive complexity endangers enterprise endpoint environments**
https://www.helpnetsecurity.com/2020/06/29/enterprise-endpoint-environments/?&web_view=true

- **Cybercriminals Carried Out Phishing Attacks By Spoofing Accounting Software Like QuickBooks**
<https://cyware.com/news/cybercriminals-carried-out-phishing-attacks-by-spoofing-accounting-software-like-quickbooks-d21a9a74>
- **Threat Assessment: EKANS Ransomware**
https://unit42.paloaltonetworks.com/threat-assessment-ekans-ransomware/?&web_view=true
- **Apple declined to implement 16 Web APIs in Safari due to privacy concerns**
https://www.zdnet.com/article/apple-declined-to-implement-16-web-apis-in-safari-due-to-privacy-concerns/?&web_view=true
- **US police using Chinese drones are 'at risk' of data breach, DHS warns**
https://nypost.com/2020/06/25/us-police-using-chinese-drones-at-risk-of-data-breach-dhs/?&web_view=true
- **Data breach a concern in edtech startups, warn experts**
https://ciso.economictimes.indiatimes.com/news/data-breach-a-concern-in-edtech-startups-warn-experts/76681913?&web_view=true
- **Brazilian federal police investigates presidential data leak**
https://www.zdnet.com/article/brazilian-federal-police-investigates-presidential-data-leak/?&web_view=true
- **SEC warns off investment in iBSmartify Nigeria cryptocurrencies**
https://www.zdnet.com/article/sec-warns-off-would-be-traders-of-ibsmartify-nigeria-cryptocurrencies/?&web_view=true
- **Office 365 users that are returning to the workplace targeted with Coronavirus training resources**
https://securityaffairs.co/wordpress/105308/cyber-crime/office-365-coronavirus-lures.html?&web_view=true
- **Over 100,000 daily brute-force attacks on RDP in pandemic lockdown**
https://www.bleepingcomputer.com/news/security/over-100k-daily-brute-force-attacks-on-rdp-in-pandemic-lockdown/?&web_view=true
- **Security Breach Impacts State Police Database**
https://www.securityweek.com/security-breach-impacts-state-police-database?&web_view=true
- **France Télévisions group hit by a cyberattack, its antennas were not impacted**
https://securityaffairs.co/wordpress/105269/hacking/france-televisions-group-cyber-attack.html?&web_view=true
- **'Cardplanet' Operator Sentenced to 9 Years for Selling Stolen Credit Cards**
https://threatpost.com/cardplanet-operator-sentenced-stolen-credit-cards/156956/?&web_view=true
- **Thousands of Roblox accounts hacked in support of Trump reelection**
<https://www.bleepingcomputer.com/news/security/thousands-of-roblox-accounts-hacked-in-support-of-trump-reelection/>
- **Singapore hands out coronavirus tracing devices**
https://www.bbc.co.uk/news/business-53216450?intlink_from_url=https://www.bbc.co.uk/news/technology&link_location=live-reporting-story
- **Government department fined over data breach**
https://www.bbc.co.uk/news/world-europe-isle-of-man-53222663?intlink_from_url=https://www.bbc.co.uk/news/technology&link_location=live-reporting-story
- **Lords slam 'unacceptable' delay to Online Harms law**
https://www.bbc.co.uk/news/technology-53222665?intlink_from_url=https://www.bbc.co.uk/news/technology&link_location=live-reporting-story
- **80% of consumers trust a review platform more if it displays fake reviews**
<https://www.helpnetsecurity.com/2020/06/29/fake-reviews/>
- **New vulnerabilities in open source packages down 20% compared to last year**
<https://www.helpnetsecurity.com/2020/06/29/vulnerabilities-open-source-packages/>
- **Does analyzing employee emails run afoul of the GDPR?**
<https://www.helpnetsecurity.com/2020/06/29/analyzing-employee-emails-gdpr/>

TUESDAY 30th June 2020

- **Australia Spending Nearly \$1 Billion on Cyberdefense as China Tensions Rise**
<https://www.nytimes.com/2020/06/30/world/australia/cyber-defense-china-hacking.html>
- **Defence minister announces \$15b boost to tackle cyber attacks on Australia, in wake of "China" hacking**
<https://www.9news.com.au/national/cyber-attack-australia-security-funding-boost-defence/cbf0de21-0b30-4ed2-9bbf-d1668ea115de>
- **Height of Covid-19 in NZ may have brought cyber attacks**
<https://www.rnz.co.nz/national/programmes/first-up/audio/2018752804/height-of-covid-19-in-nz-may-have-brought-cyber-attacks>
- **Ransomware Rampage**
<https://www.sss.co.nz/news-and-updates/ransomware-rampage/>
- **Ransomware Attacks Delivered Via Phishing Campaigns on the Rise**
<https://healthitsecurity.com/news/ransomware-attacks-delivered-via-phishing-campaigns-on-the-rise>
- **From Finland To Afghanistan: Cybercrime Exposure Down To Strategy**
<https://data-economy.com/from-finland-to-afghanistan-cybercrime-exposure-down-to-strategy/>

- **Chinese hackers aggressive since Galwan clash, stealing sensitive info from India: Cyber research expert**
<https://www.indiatoday.in/india/story/chinese-hackers-stealing-sensitive-info-data-from-india-cyfirma-expert-1695342-2020-06-30>
- **Recent cyber attack spree in Australia traced back to Chinese hacking groups**
<https://micky.com.au/recent-cyber-attack-spreed-in-australia-traced-back-to-chinese-hacking-groups/>
- **Gallagher Australia on cybercriminals' tempting target**
<https://www.insurancebusinessmag.com.au/news/cyber/gallagher-australia-on-cybercriminals-tempting-target-226447.aspx>
- **Connected Car Standards - Thank Goodness!**
https://blog.trendmicro.com/connected-car-standards-thank-goodness/?_ga=2.133567886.1892269956.1593702179-1149697676.1585940327
- **Is your ICS being targeted? How to identify whether your organization is being lined-up for a Snake ransomware attack**
<https://www.continuitycentral.com/index.php/news/technology/5270-is-your-ics-being-targeted-how-to-identify-whether-your-organization-is-being-lined-up-for-a-snake-ransomware-attack>
- **Ransomware attack on Indian Highways Authority Email Server**
<https://www.cybersecurity-insiders.com/ransomware-attack-on-indian-highways-authority-server/>
- **MARITIME CYBER ATTACKS QUADRUPLE**
<https://shipip.com/maritime-cyber-attacks-quadruple/>
- **WA public servant accused of \$1m scam flies to South Africa**
<https://www.9news.com.au/national/fremantle-port-authority-jack-merolla-accused-of-million-dollar-scam-flies-to-south-africa/fecc1b6a-a831-489b-b902-cc08db65ae4b>
- **Multi-million dollar corruption scandal hits Fremantle Port as arrest warrants issued for Giacomo 'Jack' Merolla and wife Daniela**
<https://www.perthnow.com.au/news/crime/multi-million-dollar-corruption-scandal-hits-fremantle-port-as-arrest-warrants-issued-for-giacomo-jack-merolla-and-wife-daniela-ng-b881594147z>
- **Bank of China BEC Fraud Investigation**
<https://digitpol.com/bank-of-china-bec-fraud-investigation/>
- **SEON exposes the cybercrime problem the UK is currently facing**
<https://thepayers.com/digital-identity-security-online-fraud/seon-exposes-the-cybercrime-problem-the-uk-is-currently-facing--1243257>
- **HMRC-branded covid-19 scam targets passport details of self-employed**
<https://www.internationalinvestment.net/news/4017130/hmrc-branded-covid-19-scam-targets-passport-details-self-employed>
- **Coronavirus: Bogus contact tracers target the vulnerable**
<https://www.bbc.co.uk/news/uk-wales-53227725>
- **Cyberwarfare Report, Vol. 5, No. 2: Intrusions Intensify During The COVID-19 Pandemic**
<https://cybersecurityventures.com/cyberwarfare-report-q3-2020-intrusions-intensify-during-the-covid-19-pandemic/>
- **The Indian energy market post-COVID-19: driving technological change**
<https://www.osborneclarke.com/insights/indian-energy-market-post-covid-19-driving-technological-change/>
- **Covid-19: Unlocking business after lockdown**
<https://www.pinsentmasons.com/out-law/guides/covid-19---unlocking-business-after-lockdown>
- **Cyber threats to the mining and waste water industries**
<https://dredgewire.com/article/13883/cyber-threats-to-the-mining-and-waste-water-industries/1/company-people>
- **South African Organisations Lag Behind Global Average of Cybersecurity Resilience**
<https://www.itnewsafrika.com/2020/06/south-african-organisations-lag-behind-global-average-of-cybersecurity-resilience/>
- **Google: Here is how phishing and malware attacks are evolving**
<https://www.thesouthafrican.com/technology/google-phishing-and-malware-attacks/>
- **Businesses Lack a Workable Ransomware Recovery Strategy**
<https://www.infosecurity-magazine.com/news/workable-ransomware-recovery/>
- **PonyFinal: The New Data-Stealing Ransomware**
<http://www.itnewsonline.com/news/PonyFinal-The-New-Data-Stealing-Ransomware/1484/9/3>
- **The Psychology of COVID Fraud**
<https://www.psychologytoday.com/za/blog/the-fraud-crisis/202006/the-psychology-covid-fraud>
- **LifeLabs Failed to Protect Canadians' Personal Information, Commissioners Find**
<https://ca.topclassactions.com/privacy/lifelabs-failed-to-protect-canadians-personal-information-commissioners-find/>
- **Will the EU use cyber sanctions against the Kremlin because of attacks on Ukraine?**
<https://www.promoteukraine.org/will-the-eu-use-cyber-sanctions-against-the-kremlin-because-of-attacks-on-ukraine/>
- **Renewable energy firms face growing cyber risk**
https://www.strategic-risk-europe.com/home/renewable-energy-firms-face-growing-cyber-risk/1433741_article
- **A hacker gang is wiping Lenovo NAS devices and asking for ransoms**
https://www.zdnet.com/article/a-hacker-gang-is-wiping-lenovo-nas-devices-and-asking-for-ransoms/?&web_view=true

- **Knoxville police regain access to computer system following ransomware attack**
<https://eu.knoxnews.com/story/news/local/2020/06/30/knoxville-police-regain-computer-system-access-after-ransomware-attack/5350331002/>
- **Corporate cyber attacks in East Africa on the rise in the last three months**
<https://anticorruptiondigest.com/2020/06/30/corporate-cyber-attacks-in-east-africa-on-the-rise-in-the-last-three-months/#ixzz6R9ua61gh>
- **Senators move to boost state and local cybersecurity as part of annual defense bill**
https://thehill.com/policy/cybersecurity/505108-senators-move-to-boost-state-and-local-cybersecurity-as-part-of-annual?&web_view=true
- **Researchers create tool for protecting children's online privacy**
https://www.helpnetsecurity.com/2020/06/30/protecting-childrens-online-privacy/?&web_view=true
- **The Rise of Cyber-Terrorism, and the Future of its Detection**
https://www.infosecurity-magazine.com/next-gen-infosec/cyber-terrorism-detection/?&web_view=true
- **Malware Incidents Fall Despite Overall Rise in Security Events Last Year**
https://www.infosecurity-magazine.com/news/malware-overall-rise-security/?&web_view=true
- **PROMETHIUM extends global reach with StrongPity3 APT**
https://blog.talosintelligence.com/2020/06/promethium-extends-with-strongpity3.html?&web_view=true
- **REvil Ransomware Gang Adds Auction Feature for Stolen Data**
https://threatpost.com/revil-ransomware-gang-auction-stolen-data/157006/?&web_view=true
- **Eight cities using Click2Gov targeted in Magecart skimming attacks**
https://www.scmagazine.com/home/security-news/eight-cities-using-click2gov-targeted-in-magecart-skimming-attacks/?&web_view=true
- **Hacking Timeline: Fxmsp's Rise and Apparent Fall**
https://www.govinfosecurity.com/hacking-timeline-fxmssps-rise-apparent-fall-a-14519?&web_view=true
- **US Cyber Command says foreign hackers will most likely exploit new PAN-OS security bug**
https://www.zdnet.com/article/us-cyber-command-says-foreign-hackers-will-most-likely-exploit-new-pan-os-security-bug/?&web_view=true
- **Hacker Drains \$500K From DeFi Liquidity Provider Balancer**
https://www.coindesk.com/hacker-drains-defi-liquidity-balancer?&web_view=true
- **New South Wales to implement sector-wide cybersecurity strategy**
https://www.zdnet.com/article/new-south-wales-to-implement-sector-wide-cyber-strategy/?&web_view=true
- **Files Stolen from 945 Websites Discovered on Dark Web**
https://www.darkreading.com/vulnerabilities---threats/files-stolen-from-945-websites-discovered-on-dark-web/d/d-id/1338192?&web_view=true
- **Half of Internet Users Fall Victim to Cyber Attacks**
https://hotforsecurity.bitdefender.com/blog/half-of-internet-users-fall-victim-to-cyber-attacks-23613.html?&web_view=true
- **The Senate has questions about DISA's network security system**
https://www.defensenews.com/cyber/2020/06/29/the-senate-has-questions-about-disas-network-security-system/?&web_view=true
- **Campaigners Call for Computer Misuse Act Revision on 30th Anniversary**
https://www.infosecurity-magazine.com/news/campaigners-misuse-revisionn-30/?&web_view=true
- **Google removes 25 Android apps caught stealing Facebook credentials**
https://www.zdnet.com/article/google-removes-25-android-apps-caught-stealing-facebook-credentials/?&web_view=true
- **Fake "DNS Update" emails targeting site owners and admins**
https://www.helpnetsecurity.com/2020/06/30/fake-dns-update/?&web_view=true
- **Researchers Find New Calendar-Based Phishing Campaign**
https://www.infosecurity-magazine.com/news/calendar-phishing-campaign/?&web_view=true
- **Driver Vulnerabilities Facilitate Attacks on ATMs, PoS Systems**
https://www.securityweek.com/driver-vulnerabilities-facilitate-attacks-atms-pos-systems?&web_view=true
- **The more cybersecurity tools an enterprise deploys, the less effective their defense is**
https://www.zdnet.com/article/the-more-cybersecurity-tools-an-enterprise-deploys-the-less-effective-their-defense-is/?&web_view=true
- **How public safety systems can be abused by nation state actors**
https://www.bleepingcomputer.com/news/security/how-public-safety-systems-can-be-abused-by-nation-state-actors/?&web_view=true
- **FBI Warns Consumers About COVID-19 Antibody Testing Scams**
https://hotforsecurity.bitdefender.com/blog/fbi-warns-consumers-about-covid-19-antibody-testing-scams-23617.html?&web_view=true
- **Chinese hackers employed malware to steal and encrypt data of Indian organizations**
https://ciso.economicstimes.indiatimes.com/news/china-based-hackers-employed-malware-to-obtain-data-encrypt-them-for-ransom/76708222?&web_view=true
- **U.S. FCC issues final orders declaring Huawei, ZTE national security threats**
https://www.reuters.com/article/us-usa-china-telecom/u-s-fcc-issues-final-orders-declaring-huawei-zte-national-security-threats-idUSKBN24130A?&web_view=true

- **Devious Bitcoin scam uses targeted texts and celeb endorsements**
<https://www.bleepingcomputer.com/news/security/devious-bitcoin-scam-uses-targeted-texts-and-celeb-endorsements/>
- **How much does your boss need to know about you?**
https://www.bbc.co.uk/news/business-53109207?intlink_from_url=https://www.bbc.co.uk/news/technology&link_location=live-reporting-story
- **Facebook defends push against 'false news'**
<https://www.bbc.co.uk/news/blogs-trending-53228343>
- **3 Ways to Flatten the Health Data Hacking Curve**
<https://www.darkreading.com/vulnerabilities---threats/3-ways-to-flatten-the-health-data-hacking-curve/a/d-id/1338164>
- **Remote employees encounter 59 risky URLs per week**
<https://www.helpnetsecurity.com/2020/06/30/remote-employees-secure/>
- **200% increase in invoice and payment fraud BEC attacks**
<https://www.helpnetsecurity.com/2020/06/30/payment-fraud-bec-attacks/>
- **New privacy-preserving SSO algorithm hides user info from third parties**
<https://www.helpnetsecurity.com/2020/06/30/privacy-preserving-ss0-algorithm/>
- **InFraud Cybercrime Gang Member Pleads Guilty to Charges**
<https://www.infosecurity-magazine.com/news/infraud-gang-member-pleads-guilty/>

WEDNESDAY 1st July 2020

- **Cyber attacks keeping business leaders up at night, new research finds**
<https://securitybrief.com.au/story/cyber-attacks-keeping-business-leaders-up-at-night-new-research-finds>
- **India steps up vigil for cyber attacks from China after apps ban**
https://economictimes.indiatimes.com/tech/internet/india-steps-up-vigil-for-cyber-attacks-from-china-after-apps-ban/articleshow/76710580.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst
- **Danish Agro almost back to normal after April ransomware attack**
<https://www.feednavigator.com/Article/2020/07/01/Danish-Agro-almost-back-to-normal-after-April-ransomware-attack>
- **DHS CISA Urges Patch of Critical Palo Alto Pan-OS Vulnerability**
<https://healthitsecurity.com/news/dhs-cisa-urges-patch-of-critical-palo-alto-pan-os-vulnerability>
- **COVID-19 Complicates the US-China Cyber Threat Landscape**
<https://thediplomat.com/2020/07/covid-19-complicates-the-us-china-cyber-threat-landscape/>
- **Did a Chinese Hack Kill Canada's Greatest Tech Company?**
<https://www.bloomberg.com/news/features/2020-07-01/did-china-steal-canada-s-edge-in-5g-from-nortel>
- **Surge in unique clients reporting brute-force attack attempts**
<https://www.helpnetsecurity.com/2020/07/01/brute-force-attack-attempts/>
- **Taiwan hit by ransomware attacks 1.5 times more often than global average**
<https://www.taiwannews.com.tw/en/news/3956985>
- **Over 82,000 Aussies' details leaked in crypto scam**
<https://www.itnews.com.au/news/over-82000-aussies-details-leaked-in-crypto-scam-549929>
- **America's Cup fraud allegations: NZ, Hungarian police investigating alleged scam**
<https://www.stuff.co.nz/sport/americas-cup/121998108/americas-cup-fraud-allegations-nz-hungarian-police-investigating-alleged-scam>
- **Big gold fraud busted in China! Gold market spooked by massive counterfeiting scandal**
<https://www.businesstoday.in/current/world/biggest-gold-fraud-busted-in-china-83-tons-of-fake-gold-bars-used-as-loan-collateral/story/408497.html>
- **Security lapse at South Africa's LogBox exposed user accounts and medical data**
<https://techcrunch.com/2020/07/01/security-lapse-at-south-africas-logbox-exposed-medical-data/>
- **After grinding investigation, Luckin Coffee confirms \$300 million revenue fraud**
<https://techcrunch.com/2020/07/01/after-grinding-investigation-luckin-coffee-confirms-300-million-revenue-fraud/>
- **Research: Why Corporate Fraud Reports are Down**
https://hbr.org/2020/07/research-why-corporate-fraud-reports-are-down?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+harvardbusiness+%28HBR.org%29
- **Aussies set aside £760mn to fight cybercrime**
<https://telecoms.com/505291/aussies-set-aside-760mn-to-fight-cybercrime/>
- **UK PM refers to Huawei as a "hostile state vendor"**
<https://telecoms.com/505283/uk-pm-refers-to-huawei-as-a-hostile-state-vendor/>
- **NEW ZEALAND: SIGNIFICANT CHANGES TO NZ'S PRIVACY ACT – BUT WHERE IS THE BITE?**
<https://blogs.dlapiper.com/privacymatters/new-zealand-significant-changes-to-nzs-privacy-act-but-where-is-the-bite/>
- **How to vaccinate your organization against a cyber pandemic**
<https://www.weforum.org/agenda/2020/07/vaccinate-organization-cyberattack-pandemic/>
- **China's surveillance of Uighurs may have been more extensive than thought. Reactions to Hong Kong-focused national security law.**
<https://thecyberwire.com/newsletters/daily-briefing/9/127>

- **Scam Attempts on Gumtree Have Surged During South Africa's Lockdown**
<https://www.itnewsafrika.com/2020/07/scam-attempts-on-gumtree-have-surged-during-south-africas-lockdown/>
- **New laws proposed for South Africa – including rules around the messages you can send**
<https://businessstech.co.za/news/government/412591/new-laws-proposed-for-south-africa-including-rules-around-the-messages-you-can-send/>
- **South Africa: Cybercrime post COVID-19 - Authorized push payment fraud in the world of investments**
<https://www.lexology.com/library/detail.aspx?q=912d2298-c739-408b-91f3-f55a4601e05b>
- **Qatar hired ex-CIA, US military officials to hack Republican activist Broidy: Reports**
<https://english.alarabiya.net/en/News/gulf/2020/07/01/Qatar-hired-former-CIA-US-military-officials-to-hack-Republican-activist-Reports.html>
- **S. Africa moves closer to legalizing regulation of cybercrimes**
https://www.marketwatch.com/press-release/s-africa-moves-closer-to-legalizing-regulation-of-cybercrimes-2020-07-01?mod=mw_more_headlines&tesla=y
- **Duncannon, Pa., Bolsters Cybersecurity After Ransomware Attack**
<https://anticorruptiondigest.com/2020/07/01/duncannon-pa-bolsters-cybersecurity-after-ransomware-attack/#axzz6R9uYP1x3>
- **Cyber Attack in Telecom Sector Market Detailed Insights on Upcoming Trends 2020-25:Market Growth Insightead**
<http://www.digitaljournal.com/pr/4728252#ixzz6RAV62JJe>
- **Your Car May Be Vulnerable to Cyber attacks**
<https://news-af.feednews.com/news/detail/860ccf87ae4ee38d87b83b476b7cde1b>
- **Coronavirus (Covid-19) Business Impact Automotive Cyber Security Market: Global Competition Outlook By 2025**
<https://www.marketwatch.com/press-release/coronavirus-covid-19-business-impact-automotive-cyber-security-market-global-competition-outlook-by-2025-2020-07-01?tesla=y>
- **Sudden Rise in Email Based Ransomware Attacks**
<https://www.secureworldexpo.com/industry-news/phishing-trending-ransomware-strains>
- **Android virus. Versions provided. The list of infected apps for 2020**
<https://www.2-spyware.com/remove-android-virus.html>
- **Goa Police arrests two persons for online vishing fraud**
<https://www.bignewsnetwork.com/news/265626235/goa-police-arrests-two-persons-for-online-vishing-fraud>
- **Lookers share trading suspended after fraud probe delays 2019 results**
https://www.am-online.com/news/dealer-news/2020/07/01/lookers-requests-share-trading-suspension-after-fraud-probe-delays-2019-results?utm_campaign=01_07_2020_AM_daily_newsletter&utm_medium=email&utm_content=AM%20%20Newsletter%20-%20Daily&utm_source=adestra&utm_term=Lookers%20share%20trading%20suspended%20after%20fraud%20probe%20delays%202019%20results&gclid=200752
- **Demand for stolen credit cards has dropped in the pandemic**
<https://fortune.com/2020/07/01/stolen-credit-cards-marketplaces-cybercrime/>
- **Living on a prayer? Netgear not quite halfway there with patches for 28 out of 79 vulnerable router models**
https://www.theregister.com/2020/06/30/netgear_router_patches_28_of_79_done/?&web_view=true
- **Ripple20 Threatens Increasingly Connected Medical Devices**
https://www.darkreading.com/vulnerabilities---threats/ripple20-threatens-increasingly-connected-medical-devices/d/d-id/1338241?&web_view=true
- **New ThiefQuest ransomware discovered targeting macOS users**
https://www.zdnet.com/article/new-evilquest-ransomware-discovered-targeting-macos-users/?&web_view=true
- **New privacy-preserving SSO algorithm hides user info from third parties**
https://www.helpnetsecurity.com/2020/06/30/privacy-preserving-ssso-algorithm/?&web_view=true
- **Verified Instagram account running copyright infringement phishing scam**
https://www.hackread.com/verified-instagram-account-copyright-infringement-phishing-scam/?&web_view=true
- **New Cybersecurity Standard for IoT Devices Established By ETSI**
https://www.infosecurity-magazine.com/news/cybersecurity-standard-iot-etsi/?&web_view=true
- **Operators of Android hacking kit impersonate postal services in US and Europe**
https://www.cybercoop.com/fakespy-android-cyberreason-postal-service/?&web_view=true
- **DDoS Attacks Jump 542% from Q4 2019 to Q1 2020**
https://www.darkreading.com/threat-intelligence/ddos-attacks-jump-542--from-q4-2019-to-q1-2020/d/d-id/1338208?&web_view=true
- **COVID-19 'Breach Bubble' Waiting to Pop?**
https://krebsonsecurity.com/2020/06/covid-19-breach-bubble-waiting-to-pop/?&web_view=true
- **Realizing cybersecurity risks does not mean sticking to the rules**
https://www.helpnetsecurity.com/2020/07/01/realizing-cybersecurity-risks/?&web_view=true
- **Verizon Media, PayPal, Twitter Top Bug-Bounty Rankings**
https://threatpost.com/verizon-media-paypal-twitter-bug-bounty-rankings/157040/?&web_view=true

- **Personal details of 1.29 million LimeRoad customers up for sale on dark web**
https://ciso.economicstimes.indiatimes.com/news/personal-details-of-1-29-million-limeroad-customers-up-for-sale-on-darkweb-cyble/76715156?&web_view=true
- **Microsoft releases emergency security update to fix two bugs in Windows codecs**
https://www.zdnet.com/article/microsoft-releases-emergency-security-update-to-fix-two-bugs-in-windows-codecs/?&web_view=true
- **Unsecured Chinese companies leak users' sensitive personal and business data**
https://cybernews.com/security/unsecured-chinese-companies-leak-users-sensitive-personal-and-business-data/?&web_view=true
- **CISA Issues Advisory on Home Routers**
https://www.darkreading.com/vulnerabilities---threats/cisa-issues-advisory-on-home-routers/d/d-id/1338204?&web_view=true
- **After six months of stonewalling by Apple, app dev goes public with macOS privacy protection bypass**
https://www.theregister.com/2020/07/01/apple_macos_privacy_bypass/?&web_view=true
- **Attackers Spread Cobalt Strike via IndigoDrop In Government Directed Attacks**
<https://cyware.com/news/attackers-spread-cobalt-strike-via-indigodrop-in-government-directed-attacks-f46795dd>
- **Fxmsp Group Made Millions by Selling Network Access**
<https://cyware.com/news/fxmsp-group-made-millions-by-selling-network-access-abd222b4>
- **New Botnet Breaks the Record of the Biggest PPS DDoS Attack**
<https://cyware.com/news/new-botnet-breaks-the-record-of-the-biggest-pps-ddos-attack-69aaa78d>
- **Ransomware Operators: Having at It and Having It**
<https://cyware.com/news/ransomware-operators-having-at-it-and-having-it-c1818d3d>
- **Unauthorized Data Sharing Puts Companies at Risk**
https://www.infosecurity-magazine.com/news/unauthorized-data-sharing-puts/?&web_view=true
- **How Various Malware Families Steal Your Gaming Data**
<https://cyware.com/news/how-various-malware-families-steal-your-gaming-data-1f491259>
- **NASA Watchdog Reports on Why the Agency Still Struggles with Cybersecurity**
https://www.nextgov.com/cybersecurity/2020/06/nasa-watchdog-reports-why-agency-still-struggles-cybersecurity/166531/?&web_view=true
- **Researchers Show How Hackers Can Target ICS via Barcode Scanners**
https://www.securityweek.com/researchers-show-how-hackers-can-target-ics-barcode-scanners?&web_view=true
- **BBC Publishes Screenshots Allegedly Depicting Ransom Negotiations Between NetWalker and UCSF**
https://hotforsecurity.bitdefender.com/blog/bbc-publishes-screenshots-allegedly-depicting-ransomware-negotiations-between-netwalker-and-ucsf-23626.html?&web_view=true
- **UK court shuts down scam cryptocurrency platform GPay Ltd, £1.5 million in client funds lost**
https://www.zdnet.com/article/uk-court-shuts-down-cryptocurrency-platform-after-losing-1-5-million-in-client-funds/?&web_view=true
- **Google to protect employee privacy on company-owned devices**
https://ciso.economicstimes.indiatimes.com/news/google-to-protect-employee-privacy-on-company-owned-devices/76730471?&web_view=true
- **Windows POS malware uses DNS to smuggle stolen credit cards**
<https://www.bleepingcomputer.com/news/security/windows-pos-malware-uses-dns-to-smuggle-stolen-credit-cards/>
- **Another COVID-19 Side Effect: Rising Nation-State Cyber Activity**
<https://www.darkreading.com/vulnerabilities---threats/another-covid-19-side-effect-rising-nation-state-cyber-activity/a/d-id/1338186>

THURSDAY 2nd July 2020

- **State-Sponsored Cyber Attacks Threaten Australian Critical Infrastructure**
<https://www.cpomagazine.com/cyber-security/state-sponsored-cyber-attacks-threaten-australian-critical-infrastructure/>
- **Attivo Networks raises the stakes against 'Ransomware 2.0'**
<https://securitybrief.com.au/story/attivo-networks-raises-the-stakes-against-ransomware-2-0>
- **Building ransomware resilience: preparing for the golden hour**
<https://www.teiss.co.uk/building-ransomware-resilience-preparing-for-the-golden-hour/>
- **Kerala Cyber Hackers break into Delhi State HM website, Ransomware campaign targets news websites, and more**
<https://cloudsek.com/threatintel/tag/coronavirus/>
- **3 in 4 companies lack an adequate cyber response plan**
<https://www.technologydecisions.com.au/content/information-technology-professionals-association/article/3-in-4-companies-lack-an-adequate-cyber-response-plan-909324814>
- **Security Think Tank: AI cyber attacks will be a step-change for criminals**
<https://www.computerweekly.com/opinion/Security-Think-Tank-AI-cyber-attacks-will-be-a-step-change-for-criminals>
- **Microsoft warns public of Covid-19-related cyberattacks**
<https://www.asiaone.com/digital/microsoft-warns-public-covid-19-related-cyberattacks>

- **Cyber Attacks at Sea: Blinding Warships.**
<https://www.cyberdefensemagazine.com/cyber-attacks-at-sea-blinding-warships/>
- **Inside a ransomware attack: From the first breach to the ransom demand**
<https://www.zdnet.com/article/inside-a-ransomware-attack-from-the-first-breach-to-encrypting-a-network-in-just-two-weeks/>
- **Ransomware and media coverage thereof. A criminal-market-leading information stealer. The formerly autonomous city of Hong Kong.**
<https://thecyberwire.com/newsletters/daily-briefing/9/128>
- **AFP freezes 50 bank accounts over early super access fraud fears**
<https://inqld.com.au/news/2020/07/02/afp-freezes-50-bank-accounts-over-super-early-access-fraud-fears/>
- **China's biggest gold fraud, 4% of its reserves may be fake: Report**
https://economictimes.indiatimes.com/news/international/world-news/chinas-biggest-gold-fraud-4-of-its-reserves-may-be-fake-report/articleshow/76707339.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst
- **Police roll up crime networks in Europe after infiltrating popular encrypted chat app**
<https://techcrunch.com/2020/07/02/police-roll-up-crime-networks-in-europe-after-infiltrating-popular-encrypted-chat-app/>
- **Facebook discovers it shared user data with at least 5,000 app developers after a cutoff date**
<https://techcrunch.com/2020/07/02/facebook-discovers-it-shared-user-data-with-at-least-5000-app-developers-after-a-cutoff-date/>
- **A vulnerability in some bitcoin wallets leads to double spend attacks and inflated balance**
<https://techcrunch.com/2020/07/01/a-vulnerability-in-some-bitcoin-wallets-leads-to-double-spend-attacks-and-inflated-balance/>
- **State-backed COVID-19 disinfo spreads faster and farther than local news outlets in 4 languages**
<https://techcrunch.com/2020/07/01/state-backed-covid-19-disinfo-spreads-faster-and-farther-than-local-news-outlets-in-4-languages/>
- **2 Years After Businessman Leaves India, Banks Allege Rs 350 crore Fraud**
<https://www.ndtv.com/india-news/manjit-singh-makhni-2-years-after-businessman-leaves-india-bank-alleges-rs-350-crore-fraud-2256160>
- **Mumbai Airport scam: GVK Group chairman, son booked by CBI for siphoning off Rs 705 cr**
<https://economictimes.indiatimes.com/news/politics-and-nation/mumbai-airport-scam-gvk-group-chairman-son-booked-by-cbi-for-siphoning-off-rs-705-cr/vedioshow/76743554.cms>
- **YES Bank fraud: Rana Kapoor given interim protection from arrest till July 11**
<https://www.hindustantimes.com/india-news/yes-bank-fraud-rana-kapoor-given-interim-protection-from-arrest-till-july-11/story-G7Sz7RzkXy0WH8BuPWVHdN.html>
- **Disney worker charged with fraud**
https://www.travelmole.com/news_feature.php?news_id=2043348
- **EncroChat hack shows there's no such thing as secure communications**
<https://telecoms.com/505343/encrochat-hack-shows-theres-no-such-thing-as-secure-communications/>
- **Cyber (non)cooperation in the Gulf**
<https://www.cyajax.com/2020/07/02/cyber-noncooperation-in-the-gulf/>
- **Cyber Strike By Foreign Force Caused Iran Explosion: Israeli Experts**
<https://breakingdefense.com/2020/07/cyber-strike-by-foreign-force-causes-iran-explosion-israeli-experts/>
- **Iran to Lock Down Persian Gulf Trade Hub After Virus Surge**
<https://www.bloombergquint.com/politics/iran-to-lock-down-persian-gulf-trade-hub-after-virus-surge>
- **'Leaders need to prioritise cybersecurity'**
<https://www.northweststar.com.au/story/6815538/leaders-need-to-prioritise-cybersecurity/>
- **US, UK Should Partner on 5G as Huawei Concerns Build**
<https://www.industryweek.com/the-economy/competitiveness/article/21135727/us-uk-should-partner-on-5g-as-huawei-concerns-build>
- **Ransomware Gangs Don't Need PR Help — Krebs on Security – Krebs on Security**
<https://www.businessfast.co.uk/ransomware-gangs-dont-need-pr-help-krebs-on-security-krebs-on-security/>
- **Hacker forum flooded with data stolen from 14 companies**
<https://www.cybersafe.news/hacker-forum-flooded-with-data-stolen-from-14-companies/>
- **Fighting Europe's Covid-19 Infodemic: Freedom of Expression Concerns**
<https://www.csis.org/blogs/technology-policy-blog/fighting-europes-covid-19-infodemic-freedom-expression-concerns>
- **NCA and police smash thousands of criminal conspiracies after infiltration of encrypted communication platform in UK's biggest ever law enforcement operation**
<https://www.nationalcrimeagency.gov.uk/news/operation-venetic>
- **Data breach at Canadian insurance firm exposes personal information**
<https://portswigger.net/daily-swig/data-breach-at-canadian-insurance-firm-exposes-personal-information>
- **One out of every 142 passwords is '123456'**
https://www.zdnet.com/article/one-out-of-every-142-passwords-is-123456/?&web_view=true
- **Alina Point-of-Sale Malware Spotted in Ongoing Campaign**
https://threatpost.com/alina-point-sale-malware-ongoing-campaign/157087/?&web_view=true

- **Joint operation uncovers complex money laundering scheme in Romania**
https://ec.europa.eu/anti-fraud/media-corner/news/02-07-2020/joint-operation-uncovers-complex-money-laundering-scheme-romania_en
- **Report accuses China of extensive mobile spyware use to track ethnic minority group**
<https://www.scmagazine.com/home/security-news/apts-cyberespionage/report-accuses-china-of-extensive-mobile-spyware-use-to-track-ethnic-minority-group/>
- **Federal Reserve shares tips on mitigating synthetic identity fraud**
https://www.bleepingcomputer.com/news/security/federal-reserve-shares-tips-on-mitigating-synthetic-identity-fraud/?&web_view=true
- **Connection discovered between Chinese hacker group APT15 and defense contractor**
https://www.zdnet.com/article/connection-discovered-between-chinese-hacker-group-apt15-and-defense-contractor/?&web_view=true
- **US Government shares tips on defending against cyberattacks via Tor**
https://www.bleepingcomputer.com/news/security/us-govt-shares-tips-on-defending-against-cyberattacks-via-tor/?&web_view=true
- **Snake ransomware poses unique danger to industrial systems**
https://searchsecurity.techtarget.com/news/252485531/Snake-ransomware-poses-unique-danger-to-industrial-systems?&web_view=true
- **Remote Workers Becoming More Security Conscious Although Bad Habits Persist**
https://www.infosecurity-magazine.com/news/remote-workers-security-conscious/?&web_view=true
- **'GoldenSpy' tax software attackers try to erase evidence of malware**
https://www.scmagazine.com/home/security-news/cybercrime/goldenspy-tax-software-campaign-tries-to-erase-evidence-of-malware/?&web_view=true
- **Netgear Starts Patching Serious Vulnerabilities Affecting Tens of Products**
https://www.securityweek.com/netgear-starts-patching-serious-vulnerabilities-affecting-tens-products?&web_view=true
- **TrickBot malware now checks screen resolution to evade analysis**
https://www.bleepingcomputer.com/news/security/trickbot-malware-now-checks-screen-resolution-to-evade-analysis/?&web_view=true
- **Italian Data Protection Authority Fines UniCredit Bank Nearly \$677,000 for Pre-GDPR Data Breach**
https://www.huntonprivacyblog.com/2020/07/01/italian-garante-fines-bank-600000-euros-for-pre-gdpr-data-breach/?&web_view=true
- **Hacker ransoms 23k MongoDB databases and threatens to contact GDPR authorities**
https://www.zdnet.com/article/hacker-ransoms-23k-mongodb-databases-and-threatens-to-contact-gdpr-authorities/?&web_view=true
- **Valak: More Than Meets the Eye**
https://www.cybereason.com/blog/valak-more-than-meets-the-eye?&web_view=true
- **New information disclosure vulnerability discovered in Mozilla Firefox**
https://blog.talosintelligence.com/2020/07/vuln-spotlight-firefox-information-leak-july-2020.html?&web_view=true
- **Even during the pandemic, healthcare organizations successfully fending off attacks**
https://www.scmagazine.com/home/security-news/even-during-pandemic-healthcare-orgs-successfully-fending-off-attacks/?&web_view=true
- **Cisco Warns of High-Severity Bug in Small Business Switch Lineup**
https://threatpost.com/cisco-warns-high-severity-bug-small-business-switch/157090/?&web_view=true
- **Remote code execution vulnerabilities discovered in LEADTOOLS 20**
https://blog.talosintelligence.com/2020/07/vuln-spotlight-leadtools-rce-july-2020.html?&web_view=true
- **Critical Apache Guacamole Flaws Put Remote Desktops at Risk of Hacking**
https://thehackernews.com/2020/07/apache-guacamole-hacking.html?&web_view=true
- **Inside a ransomware attack: From the first breach to the ransom demand**
https://www.zdnet.com/article/inside-a-ransomware-attack-from-the-first-breach-to-encrypting-a-network-in-just-two-weeks/?&web_view=true
- **Committee hits roadblock in probing Commonwealth cybersecurity performance**
https://www.zdnet.com/article/committee-hits-roadblock-in-probing-commonwealth-cybersecurity-performance/?&web_view=true
- **Data breach at CNY Works career center may have exposed personal information of 56,000 clients**
https://www.syracuse.com/business/2020/07/data-breach-at-cny-works-career-center-may-have-exposed-personal-information-of-56000-clients.html?&web_view=true
- **IBM study says more than half of Indian companies report data breach in last two years**
https://www.thehindubusinessline.com/info-tech/ibm-study-says-more-than-half-of-indian-companies-report-data-breach-in-last-two-years/article31971174.ece?&web_view=true
- **Sodinokibi gang begins dark web celebrity data auctions**
https://www.computerweekly.com/news/252485589/Sodinokibi-gang-begins-dark-web-celebrity-data-auctions?&web_view=true
- **40% of security pros say half of cyberattacks bypass their WAF**
<https://www.helpnetsecurity.com/2020/07/02/cyberattacks-bypass-waf/>

- **DHS Shares Data on Top Cyber Threats to Federal Agencies**
https://www.darkreading.com/vulnerabilities---threats/dhs-shares-data-on-top-cyberthreats-to-federal-agencies/d/d-id/1338261?&web_view=true
- **Malwarebytes AdwCleaner now removes malware from the command line**
<https://www.bleepingcomputer.com/news/security/malwarebytes-adwcleaner-now-removes-malware-from-the-command-line/>
- **Katie Price calls for penalties for online abuse**
https://www.bbc.co.uk/news/uk-politics-53261907?intlink_from_url=https://www.bbc.co.uk/news/technology&link_location=live-reporting-story
- **Lessons from COVID-19 Cyberattacks: Where Do We Go Next?**
<https://www.darkreading.com/endpoint/lessons-from-covid-19-cyberattacks-where-do-we-go-next/a/d-id/1338190>
- **NetWalker ransomware group claims attack on Fort Worth transportation agency**
<https://www.scmagazine.com/home/security-news/ransomware/netwalker-ransomware-group-claims-attack-on-fort-worth-transportation-agency/>
- **Report accuses China of extensive mobile spyware use to track ethnic minority group**
<https://www.scmagazine.com/home/security-news/apts-cyberespionage/report-accuses-china-of-extensive-mobile-spyware-use-to-track-ethnic-minority-group/>

FRIDAY 3rd July 2020

- **NZI notes spike in cyber risks alongside COVID-19**
<https://www.insurancebusinessmag.com/nz/news/cyber/nzi-notes-spike-in-cyber-risks-alongside-covid19-226818.aspx>
- **Xerox files allegedly stolen by Maze ransomware group: reports**
<https://www.crn.com.au/news/xerox-files-allegedly-stolen-by-maze-ransomware-group-reports-550026>
- **Serious Vulnerabilities identified in the OpenClinic GA Integrated Hospital Information Management System**
<https://hipaaclicks.com/category/healthcare-cybersecurity/>
- **NHAI was hit by ransomware attack, suffered loss of data**
http://timesofindia.indiatimes.com/articleshow/76760994.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst
- **India bans 59 Chinese apps including TikTok, Helo, WeChat**
https://economictimes.indiatimes.com/tech/software/india-bans-59-chinese-apps-including-tiktok-helo-wechat/articleshow/76694814.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst
- **Taiwan fended off China's cyber attacks on eve of presidential inauguration**
<https://www.taiwannews.com.tw/en/news/3959608>
- **What SMEs should do to be safe from ransomware attacks**
<https://vietreader.com/business/finance/3721-what-smes-should-do-to-be-safe-from-ransomware-attacks.html>
- **More than 6,500 applications for JobKeeper rejected due to ineligibility or fraud, ATO says**
<https://www.abc.net.au/news/2020-07-03/more-than-6500-applications-for-jobkeeper-rejected-due-to-fraud/12415670>
- **Former City of Perth councillor charged with fraud, forging records**
<https://www.smh.com.au/national/western-australia/former-city-of-perth-councillor-charged-with-fraud-forging-records-20200703-p558vb.html>
- **India Says Drugs Safe after Generics Fraud**
<https://www.industryweek.com/operations/safety/article/21960399/india-says-drugs-safe-after-generics-fraud>
- **Dutch watchdog warns against data sharing to combat COVID-19**
<https://telecoms.com/505348/dutch-watchdog-warns-against-data-sharing-to-combat-covid-19/>
- **Were recent cyberattacks on Australia result of escalating trade tensions?**
<https://www.miragenews.com/were-recent-cyberattacks-on-australia-result-of-escalating-trade-tensions/>
- **Cyber insurance still at a nascent stage in India**
<https://www.financialexpress.com/money/insurance/cyber-insurance-still-at-a-nascent-stage-in-india-email-spoofing-phishing-attacks-icici-lombard-general-insurance-bharti-axa-general-insurance/2011732>
- **Iran Threatens Retaliation After What It Calls Possible Cyber Attack on Nuclear Site**
<https://www.nytimes.com/reuters/2020/07/03/world/middleeast/03reuters-iran-nuclear-natanz.html>
- **Very limited cyber attacks against Iranian facilities: Jalali**
<https://en.mehrnews.com/news/160482/Very-limited-cyber-attacks-against-Iranian-facilities-Jalali>
- **Security Flaw in Health Startup Exposed User Accounts and Medical Information**
<https://www.itnewsafrika.com/2020/07/security-flaw-in-health-startup-exposed-user-accounts-and-medical-information/>
- **3 Steps for Middle East Organizations to Enhance Cybersecurity Amid COVID-19 Spikes**
<https://www.ameinfo.com/industry/technology/3-steps-for-middle-east-organizations-to-enhance-cybersecurity-amid-covid-19-spikes>
- **Tech experts warn new Mac ransomware more sinister than it appears**
<https://www.thesouthafrican.com/technology/tech-experts-warn-new-mac-ransomware-more-sinister-than-it-appears/>
- **Malaysia suspends Pakistan pilots after licence fraud revelation**
<https://www.wionews.com/south-asia/malaysia-suspends-pakistan-pilots-after-licence-fraud-revelation-310573>

- **These are the most common banking scams in South Africa**
<https://anticorruptiondigest.com/2020/06/30/these-are-the-most-common-banking-scams-in-south-africa/#ixzz6RAANOjvN>
 - **European Defense Companies the Target of Cyber Espionage Over LinkedIn**
<https://www.cpomagazine.com/news/european-defense-companies-the-target-of-cyber-espionage-over-linkedin/>
 - **P.E.I. ransomware attack costs taxpayers more than \$900K**
<https://www.cbc.ca/news/canada/prince-edward-island/pei-ransomware-attack-costs-1.5636485>
 - **Ofcom calls on mobile operators to continue supporting the vulnerable**
<https://www.insidetelecom.com/ofcom-calls-on-mobile-operators-to-continue-supporting-the-vulnerable/>
 - **National Security Agency warns that VPNs could be vulnerable to cyberattacks**
https://www.cbsnews.com/news/national-security-agency-warns-that-vpns-could-be-susceptible-to-cyberattacks/?ftag=CNM-00-10aag7e&web_view=true
 - **Researchers find Google Chrome PDFium memory corruption vulnerability**
https://blog.talosintelligence.com/2020/07/vuln-spotlight-chrome-pdfium-corruption-july-2020.html?&web_view=true
 - **NSA releases guidance on securing IPsec Virtual Private Networks**
https://www.bleepingcomputer.com/news/security/nsa-releases-guidance-on-securing-ipsec-virtual-private-networks/?&web_view=true
 - **US Schools and Colleges Have Leaked 24.5 Million Records Since 2005**
https://www.infosecurity-magazine.com/news/us-education-leaked-records-since/?&web_view=true
 - **Windows 10 background image tool can be abused to download malware**
https://www.bleepingcomputer.com/news/security/windows-10-background-image-tool-can-be-abused-to-download-malware/?&web_view=true
 - **Sixteen Facebook apps caught secretly sharing data with third-parties**
https://www.zdnet.com/article/sixteen-facebook-apps-caught-secretly-sharing-data-with-third-parties/?&web_view=true
 - **F5 emits fixes for critical flaws in BIG-IP application delivery controllers**
https://www.theregister.com/2020/07/03/f5_critical_flaws_big_ip/?&web_view=true
 - **Artificial Intelligence Systems Will Need to Have Certification, CISA Official Says**
https://www.nextgov.com/cybersecurity/2020/07/artificial-intelligence-systems-will-need-have-certification-cisa-official-says/166600/?&web_view=true
 - **NetWalker ransomware group claims attack on Trinity Metro**
https://www.scmagazine.com/home/security-news/ransomware/netwalker-ransomware-group-claims-attack-on-fort-worth-transportation-agency/?&web_view=true
 - **V Shred data leak exposes PII, sensitive photos of fitness customers and trainers**
https://www.zdnet.com/article/v-shred-data-leak-exposes-pii-sensitive-photos-of-fitness-customers-and-trainers/?&web_view=true
 - **BMW customer database for sale on dark web**
https://www.scmagazine.com/home/security-news/bmw-customer-database-for-sale-on-dark-web/?&web_view=true
 - **Sodinokibi Ransomware Operators hit electrical energy company Light S.A.**
https://securityaffairs.co/wordpress/105477/cyber-crime/sodinokibi-ransomware-light-s-a.html?&web_view=true
 - **Avaddon ransomware shows that Excel 4.0 macros are still effective**
https://www.cyber_w.bleepingcomputer.com/news/security/avaddon-ransomware-shows-that-excel-40-macros-are-still-effective/
 - **US Cyber Command urges F5 customers to patch critical BIG-IP flaw**
<https://www.bleepingcomputer.com/news/security/us-cyber-command-urges-f5-customers-to-patch-critical-big-ip-flaw/>
 - **Try2Cry ransomware tries to worm its way to other Windows systems**
<https://www.bleepingcomputer.com/news/security/try2cry-ransomware-tries-to-worm-its-way-to-other-windows-systems/>
 - **How can you be sure what you see online is real?**
https://www.bbc.co.uk/news/stories-52996401?intlink_from_url=https://www.bbc.co.uk/news/technology&link_location=live-reporting-map
 - **How does coronavirus contact tracing work?**
https://www.bbc.co.uk/news/explainers-52442754?intlink_from_url=https://www.bbc.co.uk/news/technology&link_location=live-reporting-story
 - **Moose Remain Unaware of Lottery Privacy Breach**
<https://www.infosecurity-magazine.com/news/moose-unaware-lottery-privacy/>
 - **Record Number Enrol in Online NCSC CyberFirst Courses**
<https://www.infosecurity-magazine.com/news/record-ncsc-cyberfirst-courses/>
- [End]

The contents of this report are all taken from 3rd party sources and PROFIT does not endorse or warrant the information as being accurate or correct. The sources referred to are either well known specialist IT industry websites or general press websites however we cannot guarantee the links or websites as being malware free.

PROFIT is the working name of Prevention of Fraud in Travel Ltd a Company registered in England number 08059895. VAT number 29475664

PROFIT