August 2021

Hacker Daily News

ISSA Information Systems Security Association Barbados Chapter

A review of the past month's vulnerabilities, hacks, cracks and cyber attacks.

This report defines a Ransomware Profile, which identifies security objectives from the **NIST Cybersecurity Framework** that support preventing, responding to, and recovering from ransomware events.

Source: https://csrc.nist.gov/publications/detail/nistir/8374/draft

Europol, the European police coordinating agency, said that police in Europe, the United States and Canada had seized the domains and servers of "**DoubleVPN**", a network used by **criminals to hide their identity during cyber attacks**.

Source: https://www.reuters.com/technology/doublevpn-service-used-by-hackers-seized-shut-down-2021-06-30/

Security researchers in China have accidentally disclosed a critical Windows zero-day bug nicknamed "**PrintNightmare**."

The proof-of-concept discovered by Shenzhen-based Sang for Technologies was released after confusion over another Print Spooler vulnerability status.

Source: https://www.infosecurity-magazine.com/news/printnightmare-zero-day/

Forbes

Subscribe Sign In

EDITORS' PICK | Jul 1, 2021, 11:00am EDT | 3,649 views

NSA And FBI Blame Russia For Massive 'Brute Force' Attacks On Microsoft 365

Thomas Brewster Forbes Staff

Cybersecurity

Associate editor at Forbes, covering cybercrime, privacy, security and surveillance.

Listen to this article now

-03:36

Powered by Trinity Audio

American intelligence and law enforcement agencies have pointed the finger at a Kremlin-backed hacking crew for a **two-year campaign** to break into **Microsoft Office 365 accounts**.

The agencies claimed **Fancy Bear** was really the **85th Main Special Service Center** (**GTsSS**), a unit within the Russian General Staff Main Intelligence Directorate (GRU) and that it had been carrying out its brute force attempts on multiple sectors including government

Source: https://www-forbes-com.cdn.ampproject.org/c/s/www.forbes.com/sites/thomasbrewster/2021/07/01/nsa-and-fbi-blame-russia-for-massive-brute-force-attacks-on-microsoft-365/amp/

Google removes popular Android apps that stole Facebook passwords

Jon Fingas

July 4, 2021, 3:27 pm

Google is still racing to pull Android apps that commit major privacy violations.

Google has removed nine apps from the Play Store after Dr. Web analysts discovered they were **trojans stealing Facebook login details**. These weren't obscure titles — the malware had **over 5.8 million combined** downloads and posed as easy-to-find titles like "Horoscope Daily" and "Rubbish Cleaner."

Source: https://www-engadget-com.cdn.ampproject.org/c/s/www.engadget.com/amp/google-removes-android-apps-stealing-facebook-passwords-192721252.html

REvil ransomware has set a price for decrypting all systems locked during the **Kaseya supply-chain attack**. The gang wants **$70 million** in Bitcoin for the tool that allows all affected businesses to recover their files.

Source: https://www-bleepingcomputer-com.cdn.ampproject.org/c/s/www.bleepingcomputer.com/news/security/revil-ransomware-asks-70-million-to-decrypt-all-kaseya-attack-victims/amp/

THE CRIME REPORT
YOUR CRIMINAL JUSTICE NETWORK

Donate

Nation's First Cyberattack Defense Center Opens in NYC

By **TCR Staff** | July 9, 2021

New York has opened the first **real-time cyber-attack defense center** in a major metropolitan area, reports the Wall Street Journal. The center is in a lower Manhattan skyscraper and has **282 partners** all **sharing intelligence on cyber threats**.

Its 282 members range from Amazon.com Inc. to the New York Police Department and more.

Source: https://thecrimereport.org/2021/07/09/nations-first-cyberattack-defense-center-opens-in-nyc/

A district council in eastern Germany has declared a disaster after its computer systems were paralysed by a hacker attack in what the federal cybersecurity watchdog confirmed was the country's first-ever "**cyber-catastrophe**".

Hackers knocked out the IT operations of the municipality of Anhalt-Bitterfeld, in the state of Saxony-Anhalt, on Tuesday (Jul 6), a spokesperson confirmed to Reuters on Saturday.

Source: https://www.channelnewsasia.com/business/district-council-declares-germanys-first-ever-cyber-catastrophe-2027566

Microsoft says Chinese hackers used a SolarWinds exploit to conduct attacks

The group was targeting US defense and software organizations.

S. Shah
07.14.21

SolarWinds vulnerabilities continue to be **targeted by overseas hackers** months after the US information technology company suffered a widespread cyberattack.

Microsoft said that a group operating out of China was using **a zero-day remote code execution to attack** SolarWinds software. If successfully exploited, the flaw in the IT company's Serv-U software allows hackers to perform actions like **install and run malicious payloads** or **view and change data**, Microsoft noted in a blog post.

Source: https://www.engadget.com/microsoft-solarwinds-exploit-china-hack-092547713.html

Kaseya was warned of security flaws years before attack

By Kirsten Doyle
14 Jul 2021

Five former employees at IT management software provider Kaseya, say company leaders were **warned of critical security flaws** in its software that enabled a devastating ransomware attack on July 2nd which affected up to 1,500 companies.

The employees said they **flagged several cyber security concerns** to executives between **2017 and 2020**, which weren't fully addressed.

Source: https://www-itweb-co-za.cdn.ampproject.org/c/s/www.itweb.co.za/amp/content/mYZRX79akZ37OgA8

Australian organisations are quietly paying hackers millions in a 'tsunami of cyber crime'

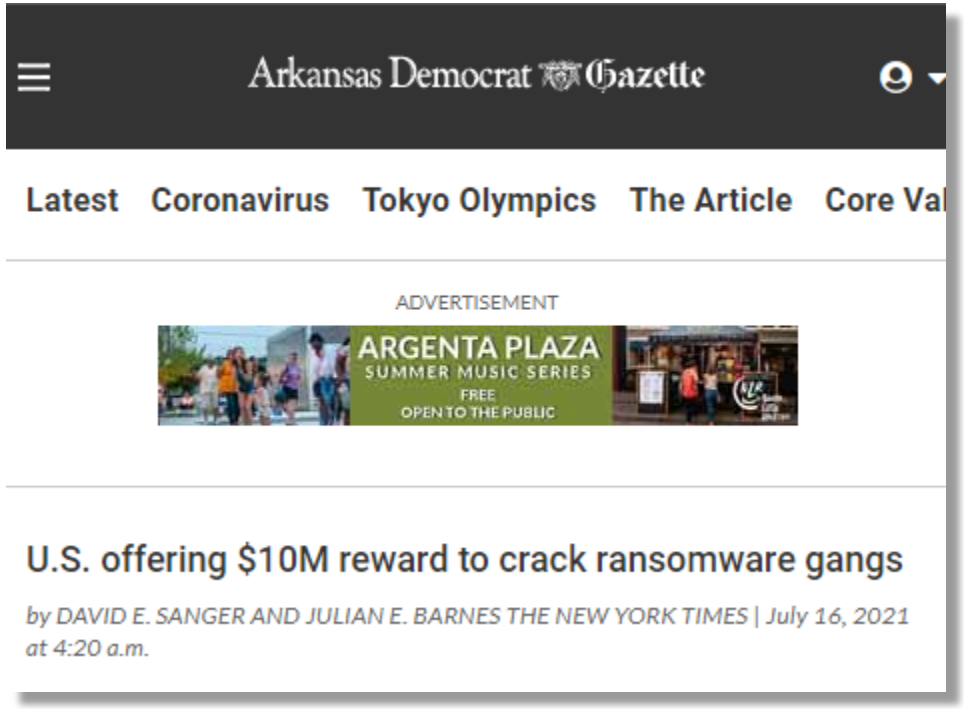
ABC Science / By technology reporter James Purtill

Posted Thu 15 Jul 2021 at 4:00pm, updated Thu 15 Jul 2021 at 4:15pm

For years, Australian organisations have been quietly paying millions in ransoms to hackers who have stolen or encrypted their data.

This money has gone to criminal organisations and encouraged further attacks, creating a **vicious cycle**.

Source: https://www.abc.net.au/news/science/2021-07-16/australian-organisations-paying-millions-ransomware-hackers/100291542



The Biden administration is making a new push to disrupt ransomware attacks on American companies, offering a **$10 million reward** for information that leads to the arrest of the gangs behind the extortion schemes and attempting to make it easier to trace and block cryptocurrency payments.

Source: https://www.arkansasonline.com/news/2021/jul/16/us-offering-10m-reward-to-crack-ransomware-gangs/

ZDNet SECURITY DATA MANAGEMENT

MUST READ QUANTUM COMPUTING: HOW BMW IS GETTING READY FOR THE NEXT TECHNOLOGY REVOLUTION

Phishing continues to be one of the easiest paths for ransomware

A Cloudian survey found that 65% of victims that reported phishing as the entry point had conducted anti-phishing training for employees.

By Jonathan Greig | July 15, 2021 -- 12:00 GMT (05:00 PDT) | Topic: Security

Ransomware gangs are still using phishing as one of the main ways to attack an organization, according to a new survey from Cloudian featuring the insights of 200 IT decision-makers who experienced a ransomware attack over the last two years.

Nearly 25% of all survey respondents said their ransomware attacks started through phishing. For enterprises with **fewer than 500 employees**, **41%** said their attacks started with phishing.

Source: https://www-zdnet-com.cdn.ampproject.org/c/s/www.zdnet.com/google-amp/article/phishing-continues-to-be-one-of-the-easiest-paths-for-ransomware-report/

Hacking

Israeli spyware firm linked to fake Black Lives Matter and Amnesty websites – report

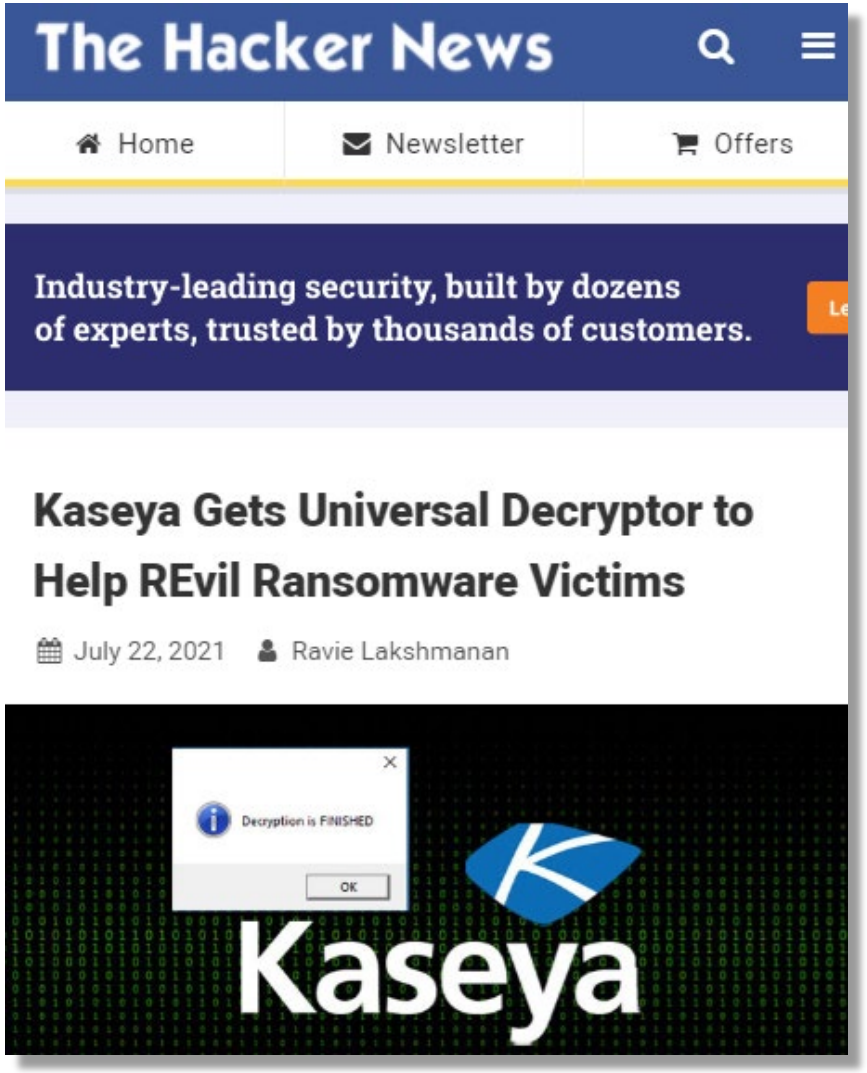
An Israeli company that sells spyware to governments is linked to fake Black Lives Matter and Amnesty International websites that are **used to hack targets**, according to a new report.

A Tel Aviv-based firm is marketing "**untraceable**" spyware that can infect and monitor computers and phones.

Source: https://www.theguardian.com/technology/2021/jul/15/spyware-company-impersonates-activist-groups-black-lives-matter

French President **Emmanuel Macron** leads a list of **14 current or former heads of state** who may have been targeted for hacking by clients of the notorious Israeli spyware firm NSO Group.

Source: https://wtop.com/asia/2021/07/macron-among-14-heads-of-states-on-potential-spyware-list/



Nearly three weeks after Florida-based software vendor Kaseya was hit by a widespread supply-chain ransomware attack, the company on Thursday said it obtained a universal decryptor to unlock systems and help customers recover their data.

Source: https://thehackernews.com/2021/07/kaseya-gets-universal-decryptor-to-help.html

Hospital Network Reveals Cause Of 2020 Cyberattack

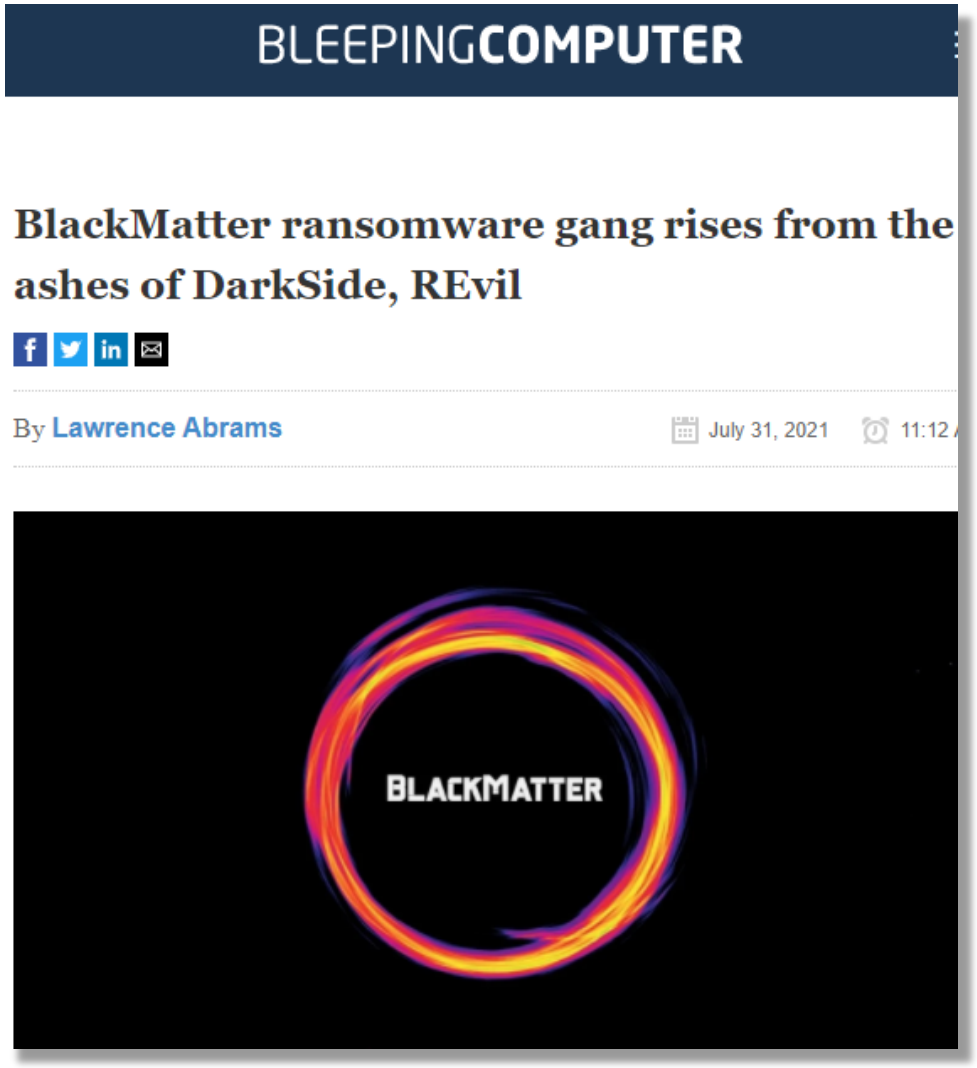
WAMC Northeast Public Radio | By Pat Bradley

Published July 27, 2021 at 6:12 PM EDT

LISTEN • 0:52

A University of Vermont Health Network official says a cyberattack that crippled its computer systems last fall costing an estimated **$50 million**, mostly in lost revenue, happened after **an employee opened a personal email on a company laptop while on vacation**.

Source: https://www.wamc.org/new-england-news/2021-07-27/hospital-network-reveals-cause-of-2020-cyberattack



BLEEPINGCOMPUTER

BlackMatter ransomware gang rises from the ashes of DarkSide, REvil

By Lawrence Abrams

July 31, 2021 11:12

A new ransomware gang named **BlackMatter** is purchasing access to corporate networks while claiming to include the best features from the notorious and now-defunct **REvil** and **DarkSide** operations.

Source: https://www-bleepingcomputer-com.cdn.ampproject.org/c/s/www.bleepingcomputer.com/news/security/blackmatter-ransomware-gang-rises-from-the-ashes-of-darkside-revil/amp/

HSE spent nearly €700,000 setting up 'war room' after ransomware attack

Details of the spending have emerged following the publication of contract award notices by the health authority

SHARE COMMENTS

By Darragh McDonagh

05:00, 2 AUG 2021

The UK HSE (Health and Safety Executive) **spent almost €700,000 setting up a "war room"** at the Citywest Hotel in Dublin as part of its response to the **cyber attack on its ICT systems in May**.

The outlay on accommodation, computer equipment, furniture and maintenance services for the HSE's situation centre at the hotel was part of more than **€3.6 million in costs incurred in the immediate aftermath of the ransomware hack**.

Source: https://www.irishmirror.ie/news/irish-news/hse-spent-nearly-700000-setting-24664494

Taiwanese motherboard maker Gigabyte has been hit by the **RansomEXX** ransomware gang, who threaten to publish **112GB** of stolen data unless a ransom is paid.

Source: https://www-bleepingcomputer-com.cdn.ampproject.org/c/s/www.bleepingcomputer.com/news/security/computer-hardware-giant-gigabyte-hit-by-ransomexx-ransomware/amp/

Ransomware Attacks: No Longer a Matter of "If," but "When"

Daniel Burrus 1 week ago

There were roughly **65,000** Ransomware attacks that *didn't* make headlines throughout the already tumultuous year of 2020; **an attack every *hour*!**

Source: https://www-business2community-com.cdn.ampproject.org/c/s/www.business2community.com/cybersecurity/ransomware-attacks-no-longer-a-matter-of-if-but-when-02422771/amp

Data Breaches Exposed 18 Billion Records In First Half Of 2021

1,767 reported breaches in six months is a huge number... but it's actually down from previous years.

Adam Rowe

August 6th 2021 | 4:27 am

The business world saw a total of **1,767** publicly reported data breaches across the first six months of 2021, accounting for the exposure of **18.8 billion** records.

Source: https://tech.co/news/data-breaches-exposed-18-billion-records-in-first-half-of-2021

ISSA
Information Systems Security Association
Barbados Chapter

The End

Prepared By:
Dwight Robinson
www.cyberandrisk.com