ZEROFOX® // Alpha Team

Threat Intelligence Bulletin: 06/11/2021 - 06/17/2021

weekly bulletin

all industries

global

Breach Disclosure: Fotolog

Around December 2018, a social network for photographers experienced a data breach impacting around 16 million accounts. This data was lumped together with a large breach of 16 various sites, totalling around 617 million accounts being sold on the dark web.

Standing Intelligence Requirements

PII & Fraud

For the most up to date list of ZeroFOX Threat Research's Intelligence Requirements, please visit:

https://cloud.zerofox.com/alpha_team/advisories/14956

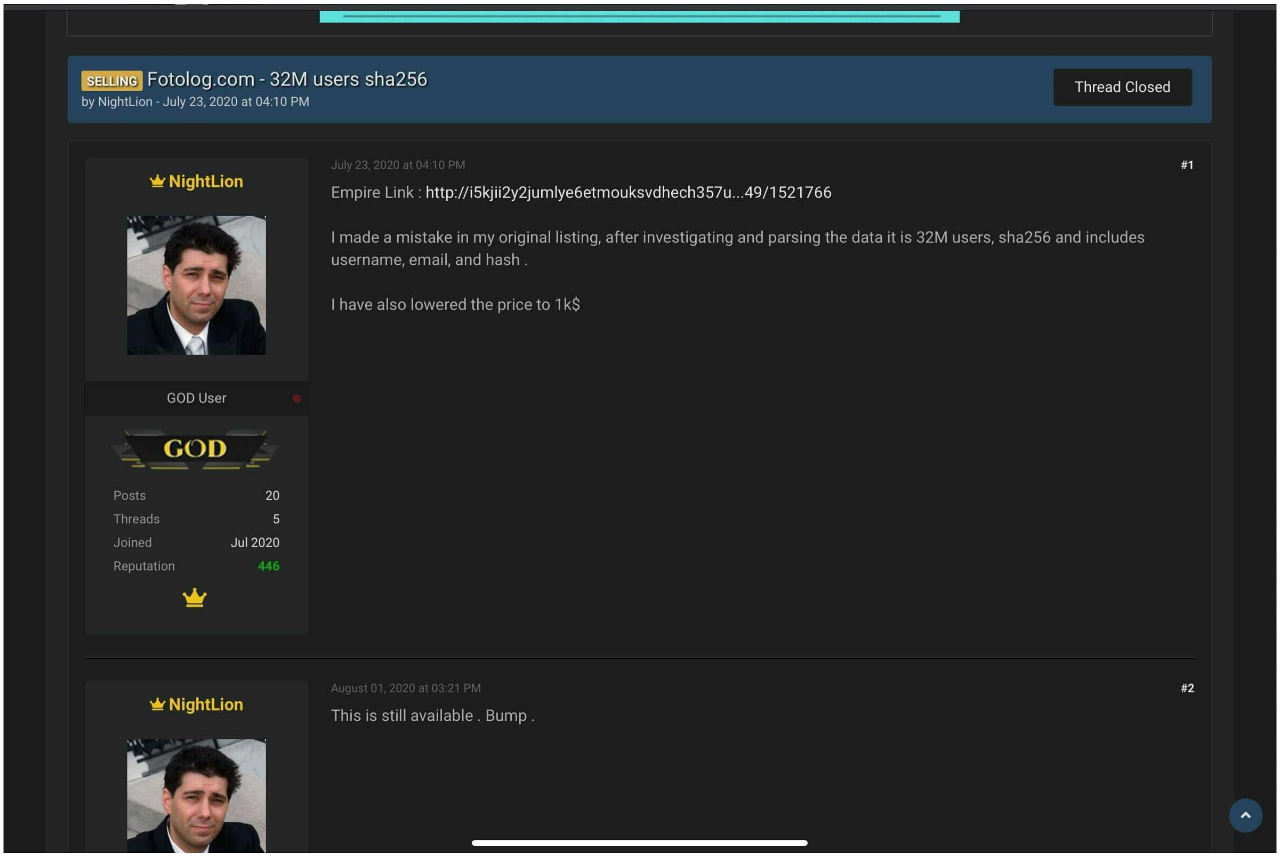
Recommendations

- If not already enabled, turn on the compromised credentials rule for all relevant entities and ensure relevant emails are entered for those entities, or reach out to ask@zerofox.com for assistance
- If one of your entities receives an alert, ZeroFOX recommends immediate password changes for the affected account
- Enable 2-factor authentication for all of your organizational accounts to help mitigate phishing and credential stuffing attacks

Details

A variety of sites data, including Fotolog, MyFitnessPal, MyHeritage, Dubsmash, 500px, Armor Games, and many others were being sold on the dark web. Just recently, the Fotolog data has been making its rounds on the dark web being sold and released.

In total, there were five SQL databases containing email addresses, SHA256-hashed passwords, security questions and answers, full names, locations, interests, and other profile information. Given the sensitivity of the type of data included, there is an increased possibility of this data being misused or to further exploit victims of this breach.



SELLING Fotolog.com - 32M users sha256

by NightLion - July 23, 2020 at 04:10 PM

Thread Closed

NightLion

GOD User

Posts	20
Threads	5
Joined	Jul 2020
Reputation	446

July 23, 2020 at 04:10 PM #1

Empire Link : http://i5kjii2y2jumlye6etmouksvdhech357u...49/1521766

I made a mistake in my original listing, after investigating and parsing the data it is 32M users, sha256 and includes username, email, and hash .

I have also lowered the price to 1k$

NightLion

August 01, 2020 at 03:21 PM #2

This is still available . Bump .

Figure 1: Example Dark web market posting of Fotolog breach data being sold

Breaking News: 2021-06-11 - 2021-06-17

Baby Clothes Giant Carter’s Leaks 410K Customer Records

Baby clothes retailer Carter’s inadvertently exposed the personal data of hundreds of thousands of its customers, dating back years, according to a new disclosure. The issue started when Linc, a vendor the company used to automate purchases online, started delivering customers shortened URLs with Carter’s purchase and shipping details without basic security protections. The links contained everything from purchase details to tracking information and more. Furthermore, by modifying the Linc URLs, it was possible to access backend JSON data, which revealed even more personal information about customers that wasn’t exposed by the confirmation pages.

See the full report here: https://threatpost.com/baby-clothes-carters-leaks-customer-records/166866/

REvil Hits US Nuclear Weapons Contractor: Report

Sol Oriens, a subcontractor for the U.S. Department of Energy (DOE) that works on nuclear weapons with the National Nuclear Security Administration (NNSA), last month was hit by a cyberattack that experts say came from the REvil ransomware gang. The company has confirmed the breach and is currently investigating the issue.

See the full report here: https://threatpost.com/revil-hits-us-nuclear-weapons-contractor-sol-oriens/166858/

McDonald's Data Breach Exposed Business & Customer Data

McDonald's has been hit with a data breach in which attackers stole some information from company systems in regions such as the United States, South Korea, and Taiwan. Experts found the breach exposed some business contact data for US employees and franchisees, along with some restaurant-specific information like seating capacity and the square footage of play areas. Attackers also stole emails, phone numbers, and addresses belonging to delivery customers in South Korea and Taiwan.

See the full report here:
https://www.darkreading.com/attacks-breaches/mcdonalds-data-breach-exposed-business-and-customer-data/d/d-id/1341282

Emerging Ransomware Targets Dozens of Businesses Worldwide

The Prometheus ransomware claims to have breached 30 organizations in just four months since February 2021. The affected entities involved all sectors in the U.S., U.K., and some in Asia, Europe, the Middle East, and South America, according to new research published by Palo Alto. The modus operandi involves terminating backup and security software-related processes on the system to lock the files behind encryption barriers.

See the full report here: https://thehackernews.com/2021/06/emerging-ransomware-targets-dozens-of.html

7-Year-Old Polkit Flaw Lets Unprivileged Linux Users Gain Root Access

A Privilege escalation vulnerability, tracked as CVE-2021-3560 (CVSS score: 7.8), discovered in the polkit system service could be exploited by a malicious unprivileged local attacker to bypass authorization and escalate permissions to the root user. The flaw is a very old vulnerability that affects polkit versions between 0.113 and 0.118 including Debian-based distributions, based on polkit 0.105, which are also vulnerable. Users are encouraged to update their Linux installations.

See the full report here: https://thehackernews.com/2021/06/7-year-old-polkit-flaw-lets.html

Unpatched Bugs Found Lurking in Provisioning Platform Used with Cisco UC

Security researchers stated that the Akkadian Provisioning Manager, which is used as a third-party provisioning tool within Cisco Unified Communications environments, has three high-severity security vulnerabilities that can be chained together to enable remote code execution (RCE) with elevated privileges. The vulnerabilities are tracked as CVE-2021-31579, CVE-2021-31580, and CVE-2021-31581 and are all present in version 4.50.18 of the Akkadian platform.

See the full report here: https://threatpost.com/unpatched-bugs-provisioning-cisco-uc/166882/

Audi, Volkswagen data breach affects 3.3 million customers - BleepingComputer

Audi and Volkswagen have suffered a data breach affecting 3.3 million customers after a vendor exposed unsecured data on the Internet. Volkswagen Group of America, Inc. (VWGoA) is the North American subsidiary of the German Volkswagen Group. It is responsible for US and Canadian operations for Volkswagen, Audi, Bentley, Bugatti, Lamborghini, and VW Credit, Inc. According to data breach notifications filed with the California and Maine Attorney General's office, VWGoA disclosed that a vendor left unsecured data exposed on the Internet between August 2019 and May 2021.

See the full report here: https://www.bleepingcomputer.com/news/security/audi-volkswagen-data-breach-affects-33-million-customers/

Microsoft pushes Windows 10 KB4023057 again to fix update issues - BleepingComputer

Microsoft is rolling out the KB4023057 update again to all versions of Windows 10 to ensure that devices can successfully install new updates as they are released. KB4023057 is being released to offer reliability improvements to Windows Update Service components in Windows 10 1507, 1511, 1607, 1703, 1709, 1803, 1909, 2004, 20H2, and 21H1.

See the full report here:
https://www.bleepingcomputer.com/news/microsoft/mic
pushes-windows-10-kb4023057-again-to-fix-update-issues/

Intuit notifies customers of hacked TurboTax accounts - BleepingComputer

Financial software company Intuit has notified TurboTax customers that some of their personal and financial information was accessed by attackers following what looks like a series of account takeover attacks. In account takeover attacks, cybercriminals gain access to their victims' accounts using credentials stolen from other online services following past data breaches. This type of attack works incredibly well against targets who use the same login credentials for multiple sites or services.

See the full report here:
https://www.bleepingcomputer.com/news/security/intuit
notifies-customers-of-hacked-turbotax-accounts/

Codecov ditches Bash Uploader for a NodeJS executable - BleepingComputer

Software testing and code coverage company, Codecov has now introduced a cross-platform uploader meant to replace its former Bash Uploader. This new uploader is available as a static binary executable currently supporting the Windows, Linux, and macOS operating systems. The announcement follows the recent Codecov supply-chain incident that lasted two months, in which attackers had altered the Codecov Bash Uploader to collect sensitive credentials from customer CI/CD environments.

See the full report here:

https://www.bleepingcomputer.com/news/security/code
ditches-bash-uploader-for-a-nodejs-executable/

Avaddon ransomware group closes shop and sends all 2,934 decryption keys to Bleeping Computer - Texasnewstoday.com

In 2021, one of the most prolific ransomware groups, the Avaddon ransomware group, announced that it would shut down operations and provide thousands of victims with free decryption tools. Avaddon ransomware group shared a file containing the decryption keys for 2,934 Avaddon ransomware victims. The unusual number is another example of the number of organizations that have never disclosed an attack. So far, some reports have attributed 88 attacks to Avaddon.

See the full report here: https://texasnewstoday.com/avaddon-ransomware-group-closes-shop-and-sends-all-2934-decryption-keys-to-bleeping-computer/310746/

McDonald's hit by data breach - CNN

McDonald's Corp, the world's largest burger chain, stated that they fell victim of a data breach in South Korea and Taiwan which exposed some customer and employee information. The attackers accessed e-mails, phone numbers and delivery addresses, but the breach did not include customer payment information. The company said its day-to-day operations were not affected and that a ransom was not involved.

See the full report here: https://www.cnn.com/2021/06/11/business/mcdonalds-data-breach/index.html

Interpol shuts down thousands of fake online pharmacies - BleepingComputer

Interpol has taken down thousands of online marketplaces that posed as pharmacies and distributing dangerous fake and illicit drugs and medicine. Many individuals were knowingly buying illicit medicines but thousands of victims were unknowingly putting their health and potentially their lives at risk. The US Federal Trade Commission provides consumers with advice on avoiding getting scammed while looking for health products and services online.

See the full report here:
https://www.bleepingcomputer.com/news/security/interp
shuts-down-thousands-of-fake-online-pharmacies/

NVIDIA is dropping support for Windows 7 and Windows 8 drivers - BleepingComputer

NVIDIA, an American multinational technology company, stated that they will provide new features, bug fixes, or performance enhancements to Game Ready Drivers for Windows 10 only and is dropping support for Windows 7, Windows 8, and Windows 8.1 drivers starting in October. 2021. Windows 7 and Windows 8 have already reached the end of extended support and no longer receive free security fixes, while Windows 8.1 will no longer receive security updates starting on January 1st, 2023.

See the full report here:
https://www.bleepingcomputer.com/news/software/nvid
is-dropping-support-for-windows-7-and-windows-8-drivers/

Mysterious Custom Malware Collects Billions of Stolen Data

Points - Threatpost

Researchers have uncovered a 1.2-terabyte database of stolen data, lifted from 3.2 million Windows-based computers over two years by an unknown, custom malware. The heisted info includes 6.6 million files and 26 million credentials and 2 billion web login cookies, with 400 million of the latter still valid at the time of the database's discovery.

See the full report here: https://threatpost.com/custom-malware-stolen-data/166753/

Watch out - that Minecraft mod could be dangerous malware - TechRadar

Fans of Minecraft have been urged to exercise caution when installing add-ons and mods for their game after warnings from cybersecurity experts. Researchers at Kaspersky have discovered a significant rise in the volume of malware masquerading at Minecraft mods, particularly on the Google Play app store. The malicious files won't add to the Minecraft experience but can make a victim's smartphone or tablet unusable due to a deluge of annoying and intrusive adverts.

See the full report here: https://www.techradar.com/news/watch-out-that-minecraft-mod-could-be-dangerous-malware

FBI Investigating 100 Ransomware Variants - MSSP Alert

Federal law enforcement is investigating 100 different ransomware variants and now considers ransomware attacks as terrorism. Many of the ransomware types the Federal Bureau of Investigation (FBI) is examining can be traced back to Russian hackers, Christopher Wray, the agency's director, told the Wall Street Journal (WSJ) in an interview.

See the full report here: https://www.msspalert.com/cybersecurity-breaches-and-attacks/ransomware/fbi-investigating-100-ransomware-variants/

Fujifilm resumes normal operations after ransomware attack - BleepingComputer

Japanese multinational conglomerate Fujifilm says that it has resumed regular business and customer operations following a ransomware attack that forced it to shut the entire network on June 4. On June 4, Fujifilm asked employees to shut off their computers and all servers on the network after an ongoing network outage blocked access to email, the billing system, and an internal reporting system.

See the full report here: https://www.bleepingcomputer.com/news/security/fujifil
resumes-normal-operations-after-ransomware-attack/

Moobot Milks Tenda Router Bugs for Propagation

A variant of the Mirai botnet called Moobot saw a big spike in activity recently, with researchers picking up widespread scanning in their telemetry for a known vulnerability in Tenda routers. It turns out that it was being pushed out from a new cyber-underground malware domain, known as Cyberium, which has been anchoring a large amount of Mirai variant activity.

See the full report here: https://threatpost.com/moobot-tenda-router-bugs/166902/

Microsoft: SEO poisoning used to backdoor targets with malware - BleepingComputer

Microsoft is tracking a series of attacks that use SEO poisoning to infect targets with a remote access trojan (RAT) capable of stealing the victims' sensitive info and backdooring their systems. The malware delivered in this campaign is SolarMarker (aka Jupyter, Polazert, and Yellow Cockatoo), a .NET RAT that runs in memory and is used by attackers to drop other payloads on infected devices.

See the full report here:
https://www.bleepingcomputer.com/news/security/micro
seo-poisoning-used-to-backdoor-targets-with-malware/

Microsoft: Scammers use Office 365 MFA bypass in BEC attacks - BleepingComputer

Microsoft 365 Defender researchers have disrupted the cloud-based infrastructure used by scammers behind a recent large-scale business email compromise (BEC) campaign. The attackers compromised their targets' mailboxes using phishing and exfiltrated sensitive info in emails matching forwarding rules, allowing them to gain access to messages relating to financial transactions.

See the full report here: https://www.bleepingcomputer.com/news/security/micro scammers-bypass-office-365-mfa-in-bec-attacks/

Apple Issues Urgent Patches for 2 Zero-Day Flaws Exploited in the Wild

Apple releases its latest update, iOS 12.5.4, that addresses three security fixes, including a memory corruption issue in the ASN.1 decoder (CVE-2021-30737) and two flaws concerning the WebKit browser engine, tracked CVE-2021-30761 and CVE-2021-30762, that could be abused to achieve remote code execution. Users of Apple devices are recommended to update to the latest versions to mitigate the risk associated with the vulnerabilities.

See the full report here: https://thehackernews.com/2021/06/apple-issues-urgent-patches-for-2-zero.html

NoxPlayer Supply-Chain Attack is Likely the Work of Gelsemium Hackers

Gelsemium, a new cyber-espionage group, has been linked to a supply chain attack targeting the NoxPlayer Android emulator that was disclosed recently. The campaign dubbed "Operation NightScout," and the adversary targeted software's update mechanism to install backdoors such as Gh0st RAT and PoisonIvy RAT which helped them to spy on its victims.

See the full report here: https://thehackernews.com/2021/06/noxplayer-supply-chain-attack-is-likely.html

Ransomware attackers are leveraging old SonicWall SRA flaw (CVE-2019-7481)

Security researchers are warning that a cyber-criminal group is exploiting CVE-2019-7481 – an older SQL injection vulnerability affecting SonicWall Secure Remote Access (SRA) 4600 devices running firmware versions 8.x and 9.x. SonicWall's recommendation is to upgrade any legacy SRA devices to the 10.x versioning recommended in light of the 2021 zero-day disclosure.

See the full report here: https://www.helpnetsecurity.com/2021/06/14/cve-2019-7481/

Utilities 'Concerningly' at Risk from Active Exploits

Cyberattacks targeting critical national infrastructure (CNI) tend to be the work of nation-states advanced persistent threat (APT) groups working with specific goals. Utility companies have had to, in short order, ensure that they are available for business online and they have legacy systems that work in favor of attackers. Security researchers recommend that these companies must have a mitigation plan that enables rapid triage and mitigation.

See the full report here: https://threatpost.com/utilities-risk-active-exploits/166908/

Alibaba suffers billion-item data leak of usernames and mobile numbers

Alibaba’s Chinese shopping operation Taobao has suffered a data breach and over a billion usernames and mobile phone numbers were lifted from the site by a crawler developed by an affiliate marketer. Alibaba notified authorities about the breach and an investigation commenced, and the matter landed in the People's Court of Suiyang District which convicted a developer and his employer of lifting the data.

See the full report here: https://go.theregister.com/feed/www.theregister.com/20

Avaddon ransomware's exit sheds light on victim landscape - BleepingComputer

Recently a new analysis report has disclosed that the Avaddon ransomware operators decided to shut down their operation and anonymously shared their victims' decryption keys with BleepingComputer, a security website. It is not clear why Avaddon shut down its operation, but it is believed that this could be due to the increased pressure exerted by the US government and law enforcement.

See the full report here: https://www.bleepingcomputer.com/news/security/avad
ransomwares-exit-sheds-light-on-victim-landscape/

Windows 10 KB5001391 update causes News & Interests display issues - BleepingComputer

Microsoft has confirmed a known issue causing the text on the "News and Interests" Windows Taskbar to get blurry after installing recent Windows 10 updates. Impacted platforms include only the following client Windows versions: Windows 10, version 21H1; Windows 10, version 20H2; Windows 10, version 2004; Windows 10, version 1909. The resolution to be provided by the company in a future Windows release.

See the full report here: https://www.bleepingcomputer.com/news/microsoft/win10-kb5001391-update-causes-news-and-interests-display-issues/

Paradise Ransomware source code released on a hacking forum - BleepingComputer

The complete source code for the Paradise Ransomware has been released on a hacking forum allowing any would-be cybercriminal to develop their customized ransomware operation. The link to the source code is only accessible to active users on the site who have previously replied to or reacted to other posts on the site.

See the full report here:
https://www.bleepingcomputer.com/news/security/parac
ransomware-source-code-released-on-a-hacking-forum/

Menominee Casino Resort in Wisconsin Shuttered by Cyberattack - Casino.Org News

The Menominee Casino Resort in Wisconsin remained closed at the time of publication, has confirmed it was the victim of a devastating cyberattack Friday. General manager Daniel Hanson said on the casino’s Facebook page that Menominee officials were working with cybersecurity and forensic experts from the FBI to investigate and assess the impact.

See the full report here: https://www.casino.org/news/menominee-casino-resort-in-wisconsin-shuttered-by-beyond-significant-cyberattack/

Notorious 'Anonymous' Hacker Nabbed in Mexico, Deported to U.S. - Bloomberg

A group of homeless men and women in California were protesting the city of Santa Cruz's decades-old prohibition against overnight encampments in August 2010 when police officers attempted to disband the rally by detaining the protesters. Among those arrested, a 45-year-old vagabond, according to local press reports. Doyon, who goes by the online moniker "Commander X", also happened to be a member of the hacking group Anonymous and three months after the protest, someone knocked out Santa Cruz County's website, according to a 2011 federal indictment unsealed Monday.

See the full report here: https://www.bloomberg.com/news/articles/2021-06-14/fugitive-hacking-suspect-from-anonymous-group-nabbed-in-mexico

80% of ransomware victims suffer repeat attacks, according to new report - CBS News

As the list of known ransomware targets continues to expand amid the COVID-19 pandemic, victims run the risk of repeat cyber attacks, according to a new report published by a U.S. cybersecurity firm on Wednesday. Boston-based Cybereason found 80% of organizations that previously paid ransom demands confirmed they were exposed to a second attack, according to a commissioned survey of 1,263 cybersecurity professionals in varying industries from the U.S., United Kingdom, Spain, Germany, France, United Arab Emirates, and Singapore.

See the full report here: https://www.cbsnews.com/news/ransomware-victims-suffer-repeat-attacks-new-report/

Experts Shed Light On Distinctive Tactics Used by Hades Ransomware

Cybersecurity researchers on Tuesday disclosed "distinctive" tactics, techniques, and procedures (TTPs) adopted by operators of Hades ransomware that set it apart from the rest of the pack, attributing it to a financially motivated threat group called GOLD WINTER. In many ways, the GOLD WINTER threat group is a typical post-intrusion ransomware threat group that pursues high-value targets to maximize how much money it can extort from its victims, researchers from SecureWorks Counter Threat Unit (CTU) said in an analysis report.

See the full report here:
https://thehackernews.com/2021/06/experts-shed-light-on-distinctive.html

Peloton Bike+ vulnerability allowed complete takeover of devices - BleepingComputer

A vulnerability was discovered in the Peloton Bike+fitness machine that allowed a threat actor to gain complete control over the device, including its video camera and microphone. While Peloton correctly set the device to a locked state, McAfee researchers discovered that they could still load a modified image as a bug was preventing the system from not verifying if the device was unlocked. The company has now fixed the vulnerability.

See the full report here:
https://www.bleepingcomputer.com/news/security/pelot
bike-plus-vulnerability-allowed-complete-takeover-of-devices/

Microsoft Defender ATP now warns of jailbroken iPhones, iPads - BleepingComputer

Microsoft has added support for detecting jailbroken iOS devices to Microsoft Defender for Endpoint, the enterprise version of its Windows 10 Defender antivirus. By jailbreaking iOS devices, users gain complete write and execution access by elevating their permissions to root, thus removing all restrictions imposed by Apple on installing applications and customizing the OS behavior. If it's detected that a device is jailbroken, an alert is surfaced to the security team in Microsoft 365 Defender, which then marks the device as high-risk allow users to block it from accessing corporate resources.

See the full report here:
https://www.bleepingcomputer.com/news/security/micro
defender-atp-now-warns-of-jailbroken-iphones-
ipads/

Millions of Connected Cameras Open to Eavesdropping

Millions of connected security and home cameras contain a critical software vulnerability that can allow remote attackers to tap into video feeds, according to a warning from the Cybersecurity and Infrastructure Security Agency (CISA). The bug is tracked as CVE-2021-3293 with a CVSS score of 9.1 out of 10. The flaw has been introduced via a supply-chain component from ThroughTek that is used by several original equipment manufacturers (OEMs) of security cameras, along with makers of IoT devices like baby- and pet-monitoring cameras, and robotic and battery devices. So far, no known public exploits are targeting the bug in the wild yet.

See the full report here: https://threatpost.com/millions-connected-cameras-eavesdropping/166950/

Malicious PDFs Flood the Web, Lead to Password-Snarfing

Microsoft Security Intelligence researchers have discovered that the SolarMarker (also known as Jupyter) makers are looking for new success by using an old technique, Search Engine Optimization (SEO) poisoning. They're stuffing thousands of PDF documents with SEO keywords and links that start a chain of redirects that eventually leads to malware. The SolarMarker backdoor malware steals data and credentials from browsers and sends the stolen data to a command-and-control (C2) server. It manages to persist by creating shortcuts in the Startup folder and by modifying desktop shortcuts.

See the full report here: https://threatpost.com/rotten-pdfs-flood-web-password-snarfing/166932/

Ukraine Police Disrupt Cl0p Ransomware Operation

Law enforcement officials in Ukraine have arrested six members of Cl0p, a ransomware gang that most recently was associated with attacks on Stanford University Medical School and on victims of an earlier breach at enterprise firewall company Accellion. As part of the operation, Ukrainian police conducted searches in 21 homes in the capital city of Kiev and in the general region. The Cyberpolice of Ukraine described the arrests as resulting from an international operation involving law enforcement authorities from Korea, the United States, and Interpol.

See the full report here: https://www.darkreading.com/attacks-breaches/ukraine-police-disrupt-cl0p-ransomware-operation/d/d-id/1341323

Largest US propane distributor discloses '8-second' data

breach - BleepingComputer

America's largest propane provider, AmeriGas, has disclosed a data breach that impacted 123 employees. The breach, however, originated at J. J. Keller, a vendor responsible for providing Department of Transportation (DOT) compliance services to AmeriGas. On May 10th, J. J. Keller detected suspicious activity on their systems associated with a company email account. The threat actor was able to gain access to an internal email with spreadsheet attachments containing 123 AmeriGas employees' information, including Lab IDs, social security numbers, driver's license numbers, and dates of birth.

See the full report here:
https://www.bleepingcomputer.com/news/security/large
us-propane-distributor-discloses-8-second-data-breach/

Scammers mail fake Ledger devices to steal your cryptocurrency - BleepingComputer

Scammers are sending fake replacement devices to Ledger customers exposed in a recent data breach that is used to steal cryptocurrency wallets. In a post on Reddit, a Ledger user shared a devious scam after receiving what looks like a Ledger Nano X device in the mail. The device came in authentic-looking packaging, with a letter explaining that the device was sent to replace their existing one as their customer information was leaked online on the RaidForum hacking forum. The enclosed instructions tell the person to connect the Ledger to their computer and run the enclosed application, which will, in turn, prompt the user with steps to import their wallet to the new device.

See the full report here:
https://www.bleepingcomputer.com/news/cryptocurrenc
mail-fake-ledger-devices-to-steal-your-
cryptocurrency/

Over a billion records belonging to CVS Health exposed online

On Thursday, researchers discovered an online database belonging to CVS Health, which was not password-protection and had no form of authentication in place to prevent unauthorized entry. The database, 204GB in size, contained event and configuration data including production records of visitor IDs, session IDs, device access information, such as whether visitors to the firm's domains used an iPhone or Android handset as well as a blueprint of how the logging system operated from the backend. Search records exposed also included queries for medications, COVID-19 vaccines, and a variety of CVS products, referencing both CVS Health and CVS.com.

See the full report here:
https://www.zdnet.com/article/billions-of-records-belonging-to-cvs-health-exposed-online/