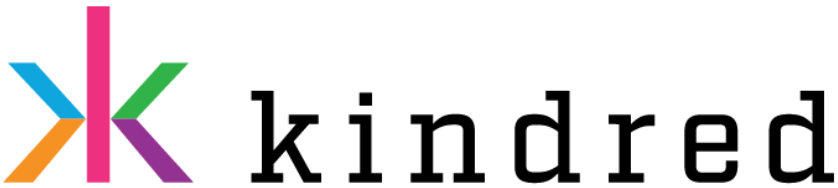
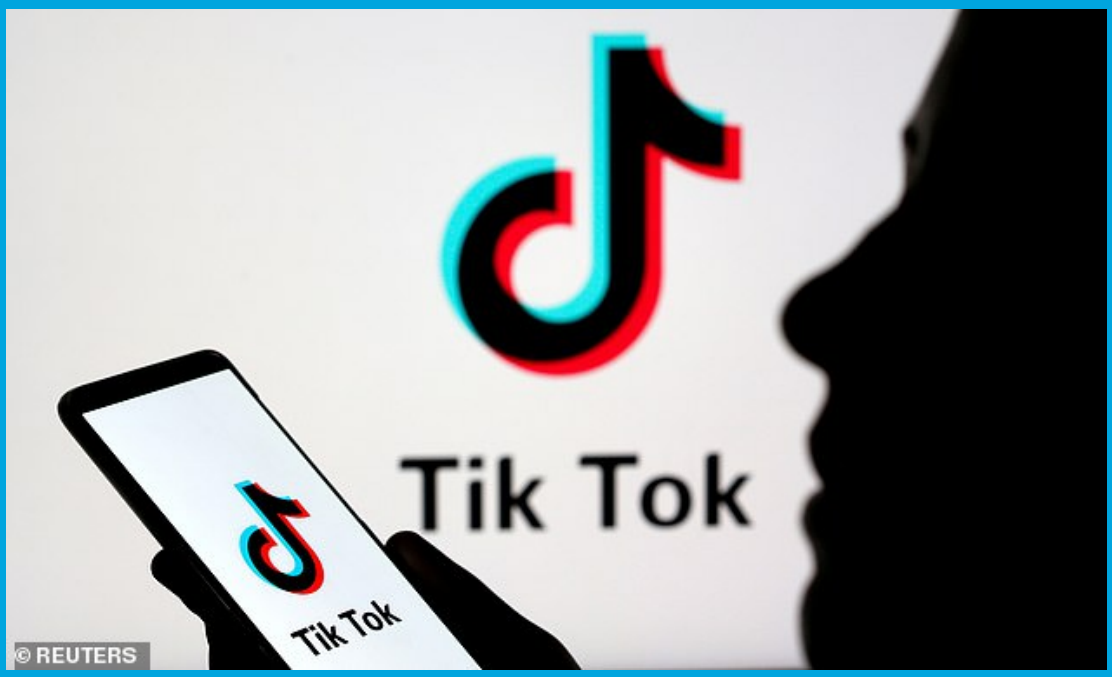


Security Newsletter

6 July 2020

Subscribe to this newsletter

iOS 14 flags TikTok, 53 other apps spying on iPhone clipboards



Sexy selfies? Passwords copied from your password manager? Bank account information? Bitcoin addresses? Yes, yes, scary yes, yes. Anything you've copied recently, they'll paste it into themselves. Such data is typically used for advertising and tracking purposes.

The covert content copying is possible not only for a device's local data, but also on nearby devices, as long as the devices share the same Apple ID and are within about 10 feet of each other. That's enabled by Apple's universal clipboard: a clipboard that enables content to be copied on one device and then pasted into an app running on a separate device.

The iOS 14 developer beta release – which you can download and install now to get an eyeful of this behavior – comes with a feature that's custom-tailored to spotlight this kind of thing: namely, a banner warning that pops up every time an app reads clipboard contents. How many apps snoop on clipboards, and how often? A whole lot, and quite frequently, as was discovered by many of the people who began testing the beta release. A video, posted on 23 June, had been viewed by over 118,000 people as of Tuesday, 30th June and demonstrates apps getting flagged by iOS 14 as they read content.

All these apps copying clipboard content have been doing so surreptitiously. They've been tough to spot. The issue underscores what an important update the new warning in iOS 14 is, and Apple plans to credit the researchers for being the impetus for the new notification. The scenario is worse on Android than it is on iOS, given that Android APIs are far more lenient. For example, Android allowed apps running in the background to read the clipboard up until Version 10, as opposed to iOS apps, which can do so only when they're active, as in, running in the foreground.

Read More on NakedSecurity

Hacker ransoms 23k MongoDB databases and threatens to contact GDPR authorities

A hacker has uploaded ransom notes on 22,900 MongoDB databases left exposed online without a password, a number that accounts for roughly 47% of all MongoDB databases accessible online. The hacker is using an automated script to scan for misconfigured MongoDB databases, wiping their content, and leaving a ransom note behind asking for a 0.015 bitcoin (~$140) payment. The attacker is giving companies two days to pay, and threatens to leak their data and then contact the victim's local General Data Protection Regulation (GDPR) enforcement authority to report their data leak.

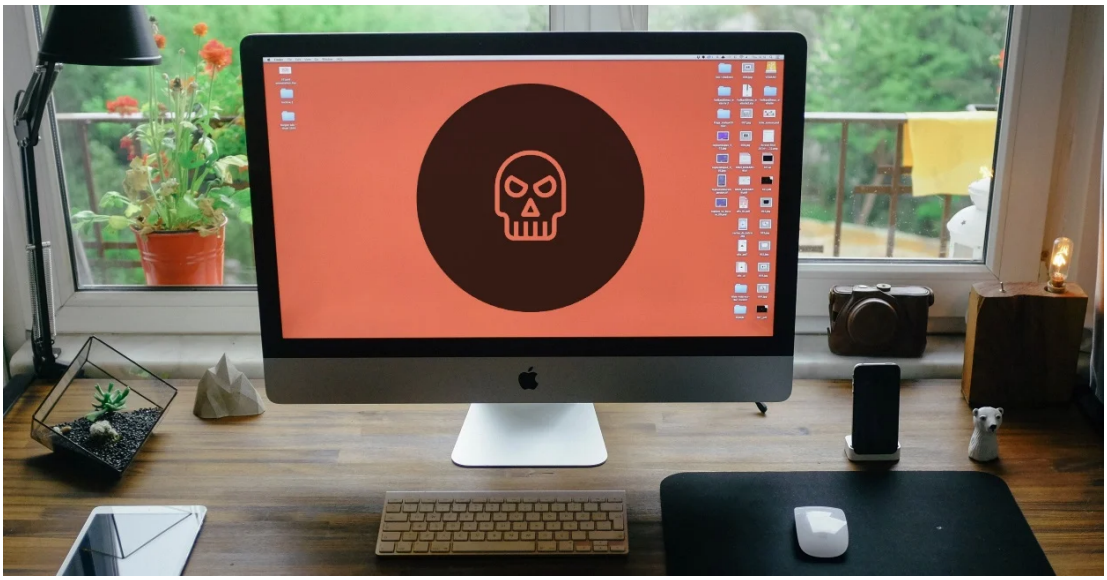
These "MongoDB wiping & ransom" attacks aren't new, per-se. The attacks Gevers spotted today are just the latest phase of a series of attacks that started back in December 2016, when hackers realized they could make serious money by wiping MongoDB servers and leaving a ransom demand behind, tricking server owners desperate to get their files back. More than 28,000 servers were ransomed in a series of attacks in January 2017, another 26,000 in September 2017, and then another 3,000 in February 2019.

The default MongoDB database setup today comes with secure defaults out of the box, but despite this, we still have tens of thousands of servers that get exposed online on a daily basis for one reason or another. For server admins looking to secure their MongoDB servers the proper way, the MongoDB Security page is the best place to start for getting the right advice.

Read More on ZDNet

Even More on WeLiveSecurity

EvilQuest: Ransomware Targets Mac Users



A ransomware strain targeting Mac users is spreading via a fake installer for Little Snitch - a host-based application firewall for macOS. So far, only those who download Mac apps via Torrent are at risk, Reed says, but he suspects there are other points of distribution.

In addition to installing Little Snitch, the fake installer also installs an executable named "patch." A postinstall shell script is downloaded and executes after installation is complete. Having such a postinstall script is normal for this type of app, but in this case it is used to load the malware, according to the report.

Read More BankInfoSecurity

Even More on BleepingComputer

More #News

- GoldenSpy backdoor installed by tax software gets remotely removed
- Employees know the rules but just don't care
- Developer of Mirai, Qbot-based DDoS botnets jailed for 13 months
- Microsoft quietly created a Windows 10 File Recovery tool, how to use
- Apple declined to implement 16 Web APIs in Safari due to privacy concerns
- Apple strong-arms entire CA industry into one-year certificate lifespans
- Russian Hacker Gets 9-Year Jail for Running Online Shop of Stolen Credit Cards
- Magecart Card Skimmer Hidden in Image's EXIF Metadata
- 2020 sees rise in invoice and payment fraud BEC attacks
- UCSF Med School Pays $1.1 Million Ransom
- Hundreds arrested after encrypted messaging network takeover

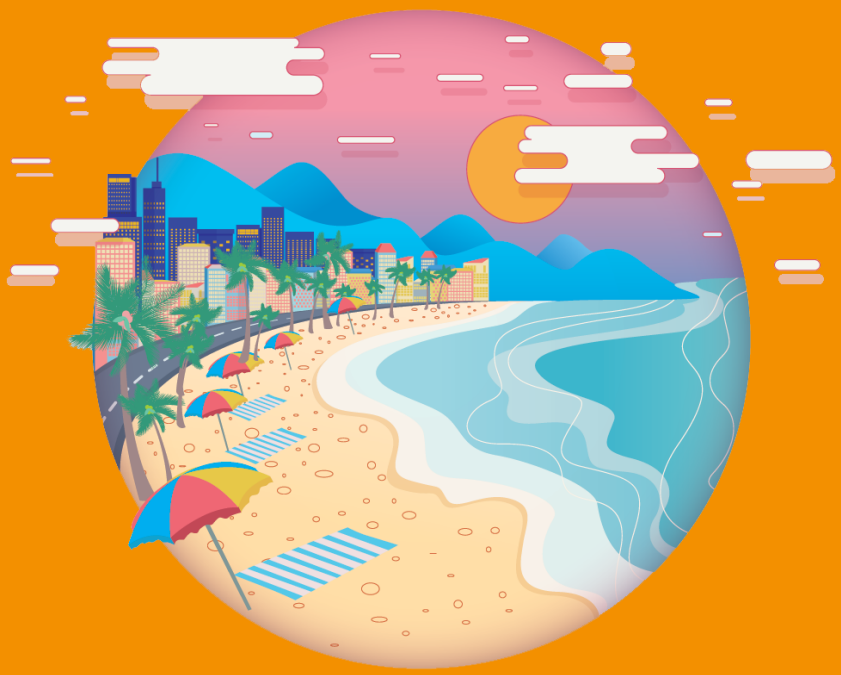
#Patch Time!

- Cisco Discloses Details of Chrome, Firefox Vulnerabilities
- Microsoft releases emergency update to fix two serious Windows flaws
- Mozilla rolls out emergency Firefox update to fix search issues
- Adobe, Mastercard, Visa warn online store owners of Magento 1.x EOL
- Palo Alto Networks patches critical vulnerability in firewall OS

#Tech and #Tools

- Major vulnerability in Telia routers (FDEU-CVE-2019-10222)
- Leonidas: framework for executing attacker actions in the cloud
- Machine to machine authentication on Azure
- Detect lateral movement with Azure Sentinel
- progress-burp: track vulnerability assessment progress in Burp
- SSH Emergency Access
- System hardening in Android 11
- PWDB - New generation of Password Mass-Analysis
- Corporate_Masks: 8-14 character Hashcat masks for corporate accounts
- Elastic Security opens public detection rules repo
- Active Directory Exploitation Cheat Sheet
- Bypassing MFA Implementation in OWA
- Inside Microsoft Threat Protection: Attack modeling for finding and stopping lateral movement

Summer break!



It's time for the Kindred Group Security team to take some holiday. The newsletter will be off for a few weeks but don't worry, we'll be back. See you soon for some awesome infosec news!

This content was created by Kindred Group Security. Please share if you enjoyed!

Kindred Group in brief

Kindred is one of the largest online gambling companies in the world with a diverse team of 1,600 people serving over 26 million customers across Europe, Australia and the US. We offer pre-game and live Sports betting, Poker, Casino and Games through 11 brands across our markets. We are committed to offer our customers the best deal and user experience possible, while ensuring a safe and fair gambling environment. Kindred is a pioneer in the online gambling industry and is an innovation driven company that builds on trust.

You can access the previous newsletters at https://news.infosecgur.us