Security Newsletter

27 Sep 2021

Subscribe to this newsletter

FBI held back ransomware decryption key from businesses to run operation targeting hackers

The FBI refrained for almost three weeks from helping to unlock the computers of hundreds of businesses and institutions hobbled by a major ransomware attack this summer, even though the bureau had secretly obtained the digital key needed to do so, according to several current and former U.S. officials.

The key was obtained through access to the servers of the Russia-based criminal gang behind the July attack. Deploying it immediately could have helped the victims, including schools and hospitals, avoid what analysts estimate was millions of dollars in recovery costs.

But the FBI held on to the key, with the agreement of other agencies, in part because it was planning to carry out an operation to disrupt the hackers, a group known as REvil, and the bureau did not want to tip them off. The previously unreported episode highlights the trade-offs law enforcement officials face between trying to damage cyber criminal networks and promptly helping the victims of ransomware — malware that encrypts data on computers, rendering them unusable.

Read More on Washington Post

Even More on Gizmodo

More #News

- Researcher Publishes Source Code for Three Unpatched iPhone Exploits
- The NSA and CIA Use Ad Blockers Because Online Advertising Is So Dangerous

- Police Announce Huge Bust of Mafia's Cyber Crime Operations
- Microsoft rushes to register Autodiscover domains leaking credentials
- EU officially blames Russia for 'Ghostwriter' hacking activities
- REvil ransomware devs added a backdoor to cheat affiliates
- Apple will disable insecure TLS in future iOS, macOS releases
- Microsoft Exchange Autodiscover bugs leak 100K Windows credentials
- Europol links Italian Mafia to million-dollar phishing scheme
- A New APT Hacker Group Spying On Hotels and Governments Worldwide
- Apple's New iCloud Private Relay Service Leaks Users' Real IP Addresses
- Breach reporting required for health apps and devices, FTC says

#Breach Log

- Bitcoin.org hackers steal $17,000 in 'double your cash' scam
- United Health Centers ransomware attack claimed by Vice Society
- Second farming cooperative shut down by ransomware this week
- US farmer cooperative hit by $5.9M BlackMatter ransomware attack
- Colombian Real Estate Agency Leak Exposes Records of Over 100,000 Buyers
- Major European call center provider goes down in ransomware attack

#Patch Time!

- Hackers exploiting critical VMware vCenter CVE-2021-22005 bug
- Emergency Google Chrome update fixes zero-day exploited in the wild
- Cisco fixes highly critical vulnerabilities in IOS XE Software
- SonicWall fixes critical bug allowing SMA 100 device takeover
- Apple patches new zero-day bug used to hack iPhones and Macs
- New macOS zero-day bug lets attackers run commands remotely
- VMware warns of critical bug in default vCenter Server installs
- Netgear fixes dangerous code execution bug in multiple routers
- New Nagios Software Bugs Could Let Hackers Take Over IT Infrastructures

#Tech and #Tools

- Defeating macOS Malware Anti-Analysis Tricks with Radare2
- Detecting and Hunting for the PetitPotam NTLM Relay Attack
- Let's Encrypt's Root Certificate is expiring!
- A guide to combatting human-operated ransomware: Part 1
- 3 New Frameworks For Securing The Software Supply Chain
- Catching the big fish: Analyzing a large-scale phishing-as-a-service operation
- Financially motivated actor breaks certificate parsing to avoid detection
- Hacking LG WebOS Smart TVs Using A Phone

- IAM Vulnerable - Assessing the AWS Assessment Tools
- Apache Dubbo: All roads lead to RCE
- Cring ransomware group exploits ancient ColdFusion server

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

Kindred Group in brief

Kindred Group is one of the world's leading online gambling operators with business across Europe, US and Australia, offering 30 million customers across 9 brands a great form of entertainment in a safe, fair and sustainable environment. The company, which employs about 1,600 people, is listed on Nasdaq Stockholm Large Cap and is a member of the European Gaming and Betting Association (EGBA) and founding member of IBIA (Sports Betting Integrity Association). Kindred Group is audited and certified by eCOGRA for compliance with the 2014 EU Recommendation on Consumer Protection and Responsible Gambling (2014/478/EU). Read more on www.kindredgroup.com.

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