Security Newsletter

17 Jan 2022

Subscribe to this newsletter

Russia Says It Arrested Members of Notorious 'REvil' Ransomware Gang

Russia's Federal Security Service said on Friday that it arrested 14 alleged members of the ransomware gang responsible for the several major attacks in the last year.

In a press release, the FSB announced that it has mapped out the whole criminal organization behind REvil, a ransomware group known for hitting JBS, a large meat manufacturer, and the business software provider Kaseya. Security researchers believe REvil is connected to another group called DarkSide, which the FBI blamed for the hack on Colonial Pipeline hack the operator of the largest gas pipeline in the United States.

The authorities searched 25 residences of the 14 members, seizing 426 million Rubles (some in cryptocurrency), $600,000, and 500,000 euros, as well as computers, crypto wallets and 20 "premium cars," according to the press release.

Read More on Vice

Even More on Reuters

How a Hacker Controlled Dozens of Teslas Using a Flaw in Third-Party App

A 19-year-old hacker and security researcher said he was able to control some features of dozens of Tesla cars all over the world thanks to a vulnerability in a third-party app that allows car owners to track their car's movements, remotely unlock doors, open windows, start keyless driving, honk, and flash lights.

David Colombo, the researcher who found the issue, asked Motherboard not to reveal all the details about his findings—such as the name of the third-party app—given that some of the vulnerabilities he discovered are yet to be fixed. Colombo allowed Motherboard to review his upcoming blog post, which contained the details.

Crucially, he said he cannot control the most important functions of the cars remotely, such as steering, accelerating, and braking. But he could still wreak some havoc.

Read More on Vice

More #News

- Hotel chain switches to Chrome OS to recover from ransomware attack
- BRIEF EA blames support staff for recent hacks of high-profile FIFA accounts
- Russia charges 8 suspected REvil ransomware gang members
- Former DHS official charged with stealing govt employees' PII
- White House reminds tech giants open source is a national security issue
- Android users can now disable 2G to block Stingray attacks
- FCC wants new data breach reporting rules for telecom carriers

- Ukranian police arrests ransomware gang that hit over 50 firms
- UK jails man for spying on teenagers, stealing photos using RATs
- CISA alerts federal agencies of ancient bugs still being exploited
- Extortion DDoS attacks grow stronger and more common
- Europol ordered to erase data on those not linked to crime
- An Examination of the Bug Bounty Marketplace
- At Request of U.S., Russia Rounds Up 14 REvil Ransomware Affiliates

#Breach Log

- Goodwill discloses data breach on its ShopGoodwill platform
- Defense contractor Hensoldt confirms Lorenz ransomware attack
- Multiple Ukrainian government websites hacked and defaced

#Patch Time!

- Windows 'RemotePotato0' zero-day gets an unofficial patch
- Apple fixes doorLock bug that can disable iPhones and iPads
- 'Wormable' Flaw Leads January 2022 Patch Tuesday
- High-Severity Vulnerability in 3 WordPress Plugins

#Tech and #Tools

- Microsoft Defender weakness lets hackers bypass malware detection
- Patchwork APT caught in its own web
- Persistence without "Persistence": Meet The Ultimate Persistence Bug – "NoReboot"
- Apple's Private Relay Is Being Blocked
- APT35 exploits Log4j vulnerability to distribute new modular PowerShell toolkit
- Wading Through Muddy Waters | Recent Activity of an Iranian State-Sponsored Threat Actor
- CVE-2021-45608 | NetUSB RCE Flaw in Millions of End User Routers
- 10 real-world stories of how we've compromised CI/CD pipelines
- Creating an Exploit: SolarWinds Vulnerability CVE-2021-35211
- New Unpatched Apple Safari Browser Bug Allows Cross-Site User Tracking

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