kindred

Security Newsletter

29 March 2021

Subscribe to this newsletter

Google's top security teams unilaterally shut down a counterterrorism operation

Google's Project Zero team caught an unexpectedly big fish recently: an “expert” hacking group exploiting 11 powerful vulnerabilities to compromise devices running iOS, Android, and Windows.

A pair of recent Google blog posts detail the collection of these zero-day vulnerabilities that were discovered over the course of nine months. They caught the attention of cybersecurity experts thanks to their scale, sophistication, and speed.

It turned out however that the hackers in question were actually Western government operatives actively conducting a counterterrorism operation.

Read More on Technology Review

More #News

- T-Mobile, Verizon, AT&T Stop SMS Hijacks After Motherboard Investigation
- Brazil leads in phishing attacks
- Chrome web browser's new security defaults
- Ransomware gang urges victims’ customers to demand a ransom payment
- TLS 1.0, 1.1 officially deprecated

#Breach Log

- New Advanced Android Malware Posing as “System Update”
- Ransomwared Bank Tells Customers It Lost Their SSNs
- Credit Card Hacking Forum Gets Hacked, Exposing 300,000 Hackers’ Accounts
- High-availability server maker Stratus hit by ransomware
- Insurance giant CNA hit by new Phoenix CryptoLocker ransomware

#Patch Time!

- Apple Issues Urgent Patch Update for Another Zero–Day Under Attack
- OpenSSL Releases Patches for 2 High-Severity Security Vulnerabilities
- Another Critical RCE Flaw Discovered in SolarWinds Orion Platform
- Critical code execution vulnerability fixed in Adobe ColdFusion
- Cisco addresses critical bug in Windows, macOS Jabber clients
- Critical netmask networking bug impacts thousands of applications

#Tech and #Tools

- One day short of a full chain: Real world exploit chains explained
- PoisonApple - a macOS persistence tool
- Why should you care about Content Security Policy?
- H2C Smuggling in the Wild
- The Consumer Authentication Strength Maturity Model (CASMM)
- Buffer overruns, license violations, and bad code: FreeBSD 13’s close call
- OpenSSL fixes two high-severity crypto bugs
- How to bypass CloudFlare bot protection ?

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