Security Newsletter

15 Nov 2021

Subscribe to this newsletter

Google Caught Hackers Using a Mac Zero-Day Against Hong Kong Users

Google researchers caught hackers targeting users in Hong Kong exploiting what were at the time unknown vulnerabilities in Apple's Mac operating system. According to the researchers, the attacks have the hallmarks of government-backed hackers.

On Thursday, Google's Threat Analysis Group (TAG), the company's elite team of hacker hunters, published a report detailing the hacking campaign. The researchers didn't go as far as pointing the finger at a specific hacking group or country, but they said it was "a well resourced group, likely state backed."

"We do not have enough technical evidence to provide attribution and we do not speculate about attribution," the head of TAG Shane Huntley told Motherboard in an email. "However, the nature of the activity and targeting is consistent with a government backed actor."

Read More on Vice

Even More on Google blog

Hoax Email Blast Abused Poor Coding in FBI Website

The Federal Bureau of Investigation (FBI) confirmed that its fbi.gov domain name and Internet address were used to blast out thousands of fake emails about a cybercrime investigation. According to an interview with the person who claimed responsibility for the hoax, the spam messages were sent by abusing insecure code in an FBI online portal designed to share information with state and local law enforcement authorities.

Late in the evening on Nov. 12 ET, tens of thousands of emails began flooding out from the FBI address eims@ic.fbi.gov, warning about fake cyberattacks. Around that time, KrebsOnSecurity received a message from the same email address.

“Hi its pompompurin,” read the missive. “Check headers of this email it’s actually coming from FBI server. I am contacting you today because we located a botnet being hosted on your forehead, please take immediate action thanks.” A review of the email’s message headers indicated it had indeed been sent by the FBI, and from the agency’s own Internet address. The domain in the “from:” portion of the email I received — eims@ic.fbi.gov — corresponds to the FBI’s Criminal Justice Information Services division (CJIS).

Read More on Krebs on Security

More #News

- FTC shares ransomware defense tips for small US businesses
- Surveillance firm pays $1 million fine after 'spy van' scandal
- Hacking the Sony Playstation 5

- Microsoft warns of surge in HTML smuggling phishing attacks
- Russian 'King of Fraud' sentenced to 10 years for Methbot scheme
- New bill sets ransomware attack response rules for US financial orgs
- Gmail accounts are used in 91% of all baiting email attacks
- Researchers show that Apple's CSAM scanning can be fooled easily
- Lazarus hackers target researchers with trojanized IDA Pro
- New Android malware targets Netflix, Instagram, and Twitter users
- NUCLEUS:13 TCP security bugs impact critical healthcare devices
- China's cyber watchdog unveils new draft data management regulations
- Cyber-mercenary group Void Balaur has been hacking companies for years
- CERT-PL employees rally around politically-dismissed chief
- Transavia airline fined for weak security practices that led to data breach
- China says a foreign spy agency hacked its airlines, stole passenger records
- The hunt for NOBELIUM, the most sophisticated nation-state attack in history

#Breach Log

- Costco discloses data breach after finding credit card skimmer
- Hackers undetected on Queensland water supplier server for 9 months
- HPE says hackers breached Aruba Central using stolen access key
- Medical software firm urges password resets after ransomware attack

#Patch Time!

- Microsoft Patch Tuesday, November 2021 Edition
- Zero-day bug in all Windows versions gets free unofficial patch
- AMD fixes dozens of Windows 10 graphics driver security bugs
- Ironic twist: WP Reset PRO bug lets hackers wipe WordPress sites
- Microsoft patches Excel zero-day used in attacks, asks Mac users to wait
- Microsoft urges Exchange admins to patch bug exploited in the wild
- Palo Alto Warns of Zero-Day Bug in Firewalls Using GlobalProtect Portal VPN
- 14 New Security Flaws Found in BusyBox Linux Utility for Embedded Devices

#Tech and #Tools

- Secure software supply chain: why every link matters
- Exchange Exploit Leads to Domain Wide Ransomware
- Exploiting CSP in Webkit to Break Authentication & Authorization
- Scanning Millions of Publicly Exposed Docker Containers – Thousands of Secrets Leaked
- The Kerberos Key List Attack: The return of the Read Only Domain Controllers
- Practical HTTP Header Smuggling: Sneaking Past Reverse Proxies to Attack AWS and

Beyond

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