kindred

Security Newsletter

27 January 2020

Subscribe to this newsletter

Saudi Prince Allegedly Hacked World's Richest Man Jeff Bezos Using WhatsApp

The iPhone of Amazon founder Jeff Bezos, CEO of Amazon, was reportedly hacked in May 2018 after receiving a WhatsApp message from the personal account of Saudi crown prince Mohammed bin Salman, the Guardian newspaper revealed today. Citing unnamed sources familiar with digital forensic analysis of the breach, the newspaper claimed that a massive amount of data was exfiltrated from Bezos's phone within hours after he received a malicious video file from the Saudi prince.

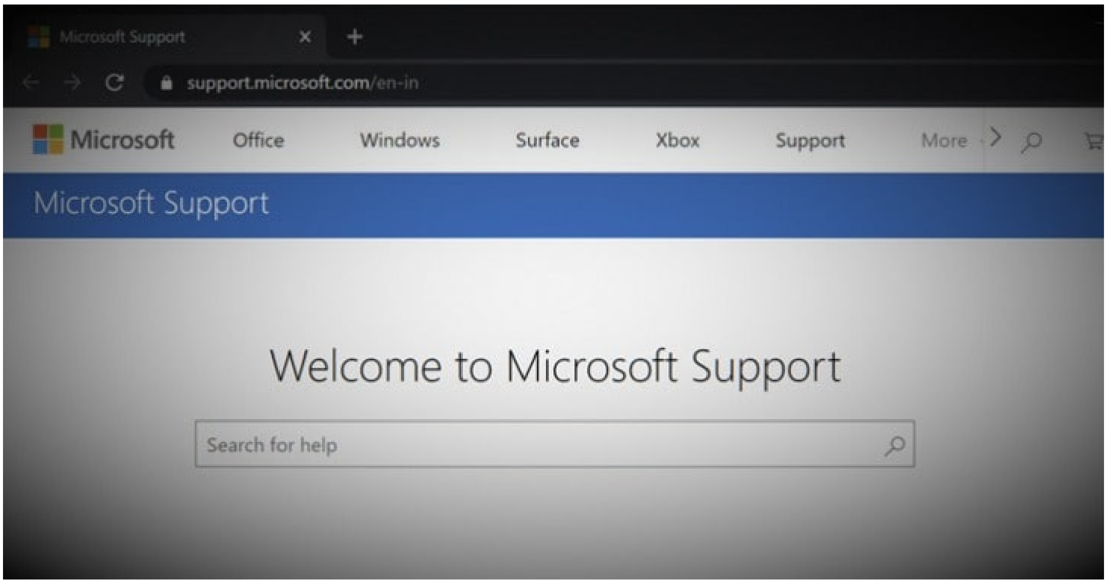
The mysterious file was sent when crown prince Salman and Bezos were having a friendly WhatsApp conversation, and it's 'highly probable' that it exploited an undisclosed zero-day vulnerability of WhatsApp messenger to install malware on Bezos's iPhone. The Guardian said it didn't know what data was extracted from the phone, but the hack happened almost 9 months before an American tabloid newspaper published intimate photos and messages sent by Bezos, disclosing his extramarital affair that leads to a divorce from his wife of 25 years.

At that time, Jeff Bezos pointed out the business relationship between the tabloid newspaper and Saudi Arabia and also hinted that how furious the Saudis were with him for the Washington Post's coverage of the murder of its journalist Jamal Khashoggi, a strong critic of the Kingdom's rulers. Since Bezos also owns the Washington Post and the CIA claimed that Salman ordered Khashoggi's assassination, the relationship between the Amazon chief executive and the Saudi government soured immediately after that. The Saudi Arabia's U.S. Embassy, in a tweet, dismissed the Guardian report by calling it "absurd" and asked for an investigation.

Read More on TheHackerNews

A timeline of events surrounding the Bezos phone hack

Microsoft Exposed 250M Customer Support Records on Leaky Servers



Microsoft disclosed a security breach caused by a misconfigured internal customer support database that led to the accidental exposure of roughly 250 million customer support and service records, some of them containing personally identifiable information. Microsoft confirmed that due to misconfigured security rules added to the server in question on December 5, 2019, enabled exposure of the data, which remained the same until engineers remediated the configuration on December 31, 2019. Microsoft didn't get into details such as the number of records exposed, the type of database that was left unprotected, or the type of personal information that was left in the open, only that data in the support case analytics database was "redacted using automated tools to remove personal information." While most of the records stored within the heavily-redacted internal customer support database used for support case analytics did not contain personal information, some non-standard PII wasn't anonymized. For instance, email addresses separated with spaces like 'username @ domain.com' instead of 'username@domain.com' were left untouched by Microsoft's automated PII redaction tools.

As a result of the incident, Microsoft says it is taking steps to better lock down its use of cloud-based databases. For example, the company has pledged to improve auditing of its security rules for internal resources as well as to expand the scope of tools it uses to search for any security rule misconfigurations. The company says it will also expand its alerting systems to try and sound red alerts whenever security rule misconfigurations occur.

Read More on BleepingComputer

Even More on BankInfoSecurity

More #News

- Euro Cup and Olympics Ticket Reseller Hit by MageCart

- NIST’s new privacy rules – what you need to know
- Regus spills data of 900 staff on Trello board set to ‘public’
- Maze Ransomware Not Getting Paid, Leaks Data Left and Right
- Phishing Incident at UPS Store Chain Exposes Customer Info
- This Citibank Phishing Scam Could Trick Many People
- Ubisoft sues DDoS-for-hire operators for ruining game play
- Thousands of WordPress Sites Hacked to Fuel Scam Campaign
- Apple Addresses iPhone 11 Location Privacy Concern
- Maze Ransomware Not Getting Paid, Leaks Data Left and Right
- How to use a physical security key to sign into supported websites
- Actively Exploited IE 11 Zero-Day Bug Gets Temporary Patch
- Card-Stealing Scripts Infect Perricone's European Skin Care Sites
- Visa's plan against Magecart attacks: Devalue and disrupt
- Mitsubishi Electric discloses security breach, China is main suspect
- Serious Vulnerabilities Expose Honeywell Surveillance Systems to Attacks

#Patch Time!

- Cisco Patches Critical Vulnerability in Network Security Tool
- Citrix Releases Scanner to Detect Hacked Citrix ADC Appliances
- Unofficial Patch Released for Recently Disclosed Internet Explorer Zero-Day
- German government to pay €800,000 in Windows 7 ESU fees this year
- Multiple Vulnerabilities Found in AMD ATI Radeon Graphics Cards
- Siemens Warns of Security Risks Associated With Use of ActiveX
- Legacy TLS is on the way out: Start deprecating TLSv1.0 and TLSv1.1 now

#Tech and #Tools

- Moving Fast and Securing Things
- Revisiting Remote Desktop Lateral Movement
- HPKP is no more!
- Android Enterprise security whitepaper details defenses
- Azure Security Benchmark—90 security and compliance best practices for your workloads in Azure
- Satellite: A Payload and Proxy Service for Red Team Operations
- Attacker Deploying Mitigation for Citrix NetScaler Vulnerability While Maintaining Backdoor
- Automated Anomaly-Detection in DNS Zones
- ThreatHunter Playbook
- Awesome Forensics tools curated list
- VirusTotal is not an Incident Responder
- THC tips and tricks
- Sec in your DevOps: Adding the OWASP Dependency Check to your Jenkins pipeline
- Adversary Tactics - PowerShell Training
- Analysis of the Evidence of Surveillance of Mr. Bezos’ personal phone - Key Technical Elements -

Kingred Group is growing, so does the Group Security team! We're looking for new talented professionals to come join us. You can find all our open vacancies on our career page.

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