Security Newsletter

9 December 2019

Subscribe to this newsletter

Unpatched Strandhogg Android Vulnerability Actively Exploited in the Wild

Cybersecurity researchers have discovered a new unpatched vulnerability in the Android operating system that dozens of malicious mobile apps are already exploiting in the wild to steal users' banking and other login credentials and spy on their activities. Dubbed Strandhogg, the vulnerability resides in the multitasking feature of Android that can be exploited by a malicious app installed on a device to masquerade as any other app on it, including any privileged system app.

In other words, when a user taps the icon of a legitimate app, the malware exploiting the Strandhogg vulnerability can intercept and hijack this task to display a fake interface to the user instead of launching the legitimate application. By tricking users into thinking they are using a legitimate app, the vulnerability makes it possible for malicious apps to conveniently steal users' credentials using fake login screens.

Promon reported the Strandhogg vulnerability to the Google security team this summer and disclosed details today when the tech giant failed to patch the issue even after a 90-day disclosure timeline.

Read More on TheHacker News

Even More on ZDNet

Iranian hackers deploy new ZeroCleare data-wiping malware

Security researchers from IBM said today they identified a new strain of destructive data-wiping malware that was developed by Iranian state-sponsored hackers and deployed in cyber-attacks against energy companies active in the Middle East. IBM did not name the companies that have been targeted and had data wiped in recent attacks. Instead, IBM's X-Force security team focused on analyzing the malware itself, which they named ZeroCleare.

Unlike many cyber-security firms, IBM's X-Force team did not shy away from attributing the malware and the attacks to a specific country -- in this case, Iran. But unlike many previous cyber-attacks, which are usually carried out by one single group, IBM said this malware and the attacks behind appear to be the efforts of a collaboration between two of Iran's top-tier government-backed hacking units.

As for the malware itself, ZeroCleare is your classic "wiper," a strain of malware designed to delete as much data as possible from an infected host. Wiper malware is usually used in two scenarios. It's either used to mask intrusions by deleting crucial forensic evidence or it's used to damage a victim's ability to carry out its normal business activity -- as was the case of attacks like Shamoon, NotPetya, or Bad Rabbit. IBM said that none of the ZeroCleare attacks were opportunistic and appeared to be targeted against very specific organizations. Past Shamoon attacks targeted companies in the energy sector that were active in the Middle East region, companies that were either Saudi-based or known partners for Saudi-based oil & gas enterprises.

Read More on ZDNet

Even More on BleepingComputer

More #News

- SMS company exposes millions of text messages, credentials online
- FBI Puts $5 Million Bounty On Russian Hackers Behind Dridex Banking Malware
- 61% of malicious ads target Windows users
- Privacy and Security Issues Found in Popular Shopping Apps
- Apple Explains Mysterious iPhone 11 Location Requests
- Spear phishing campaigns—they're sharper than you think
- Over 30,500 Online Piracy Sites Shut Down in Global Operation
- Convicted murderer wins 'right to be forgotten' case
- Fake Steam Skin Giveaway Site Steals your Login Credentials
- Data of 21 million Mixcloud users put up for sale on the dark web
- Facebook Sued Hong Kong Firm for Hacking Users and Ad Fraud Scheme
- Microsoft Warns of Persistent Windows Hello for Business Orphaned Keys
- Salesforce's Heroku Used to Host Magecart Skimmers, Stolen Cards
- Malicious Python Package Available in PyPI Repo for a Year
- Google: 80% of Android Apps Encrypt Traffic by Default
- Avast and AVG Browser Extensions Spying On Chrome and Firefox Users
- ENISA proposes Best Practices and Techniques for Pseudonymisation
- 44 million Microsoft users reused passwords in the first three months of 2019
- Here, have my biometric data, I don´t care.

#Patch Time!

- New Linux Vulnerability Lets Attackers Hijack VPN Connections
- Microsoft Patches Vulnerability Leading to Azure Account Takeover
- Vulnerabilities Disclosed in Kaspersky, Trend Micro Products
- Vulnerability Allows Hackers to Take Control of ABB Substation Protection Devices
- OpenBSD patches authentication bypass, privilege escalation vulnerabilities
- Google Patches Critical DoS Flaw in Android 10
- Critical Flaw in GoAhead Web Server Could Affect Wide Range of IoT Devices
- EFF CertBot 1.0 is live (Let's Encrypt)
- BlackDirect: Microsoft Azure Account Takeover

#Tech and #Tools

- PAF Credentials Checker: Proactively fight against Credential Stuffing
- Researcher Unveils CrackQ, a New Password Cracking Manager (HashCat GUI)
- Introducing Mussels, an application dependency build automation tool
- Two malicious Python libraries caught stealing SSH and GPG keys
- Creating a Rootkit to Learn C
- Software Libraries Are Terrifying - Package typosquatting
- Inferring and hijacking VPN-tunneled TCP connections.
- NTLMRecon: A fast NTLM reconnaissance and information gathering tool without external dependencies.
- First Contact: New Vulnerabilities in Contactless Payment

- A collection of public security audits.
- Empire Beta 3.0
- Email authentication: SPF, DKIM and DMARC out in the wild
- Java security calendar 2019
- CertGraph: visualizing the distribution of trusted CA's
- Prepare, Hunt, and Respond concept model
- Insights from one year of tracking a polymorphic threat
- Cobalt Strike 4.0 – Bring Your Own Weaponization
- Framework-Specific Security Guidelines

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