kindred

Security Newsletter

2 September 2019

Subscribe to this newsletter

Google Uncovers How Just Visiting Some Sites Were Secretly Hacking iPhones For Years

Your iPhone can be hacked just by visiting an innocent-looking website, confirms a terrifying report Google researchers released earlier today. The story goes back to a widespread iPhone hacking campaign that cybersecurity researchers from Google's Project Zero discovered earlier this year in the wild, involving at least five unique iPhone exploit chains capable of remotely jailbreaking an iPhone and implanting spyware on it.

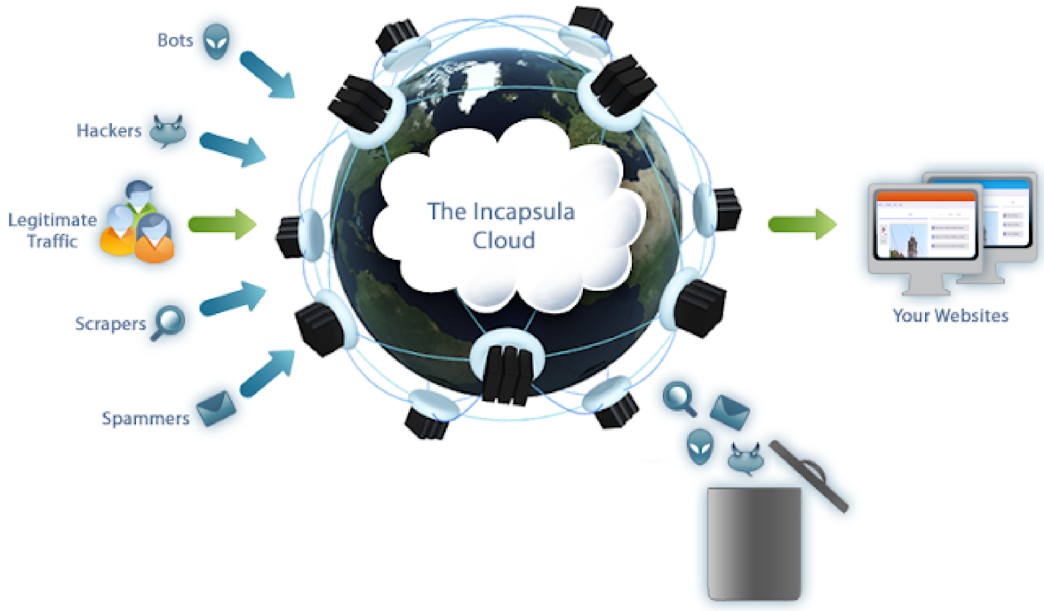
Those iOS exploit chains were found exploiting a total of 14 separate vulnerabilities in Apple's iOS mobile operating system—of which 7 flaws resided in Safari web browser, 5 in the iOS kernel and 2 separate sandbox escape issues—targeting devices with almost every version in that time-frame from iOS 10 through to the latest version of iOS 12.

Now, as Google researcher explained, the attack was being carried out through a small collection of hacked websites with thousands of visitors per week, targeting every iOS user landing on those websites without discrimination. The iPhone exploits were used to deploy an implant primarily designed to steal files like iMessages, photos, and live GPS location data of users, and upload them to an external server every 60 seconds. Takeaway: Since Apple already patched the majority of vulnerabilities exploited by the uncovered iPhone exploits, users are always recommended to keep their devices up-to-date to avoid becoming victims of such attack chains.

Read More on TheHackerNews

Even More on NakedSecurity

Cybersecurity Firm Imperva Discloses Breach



Imperva, a leading provider of Internet firewall services that help Web sites block malicious cyberattacks, alerted customers on Tuesday that a recent data breach exposed email addresses, scrambled passwords, API keys and SSL certificates for a subset of its firewall users.

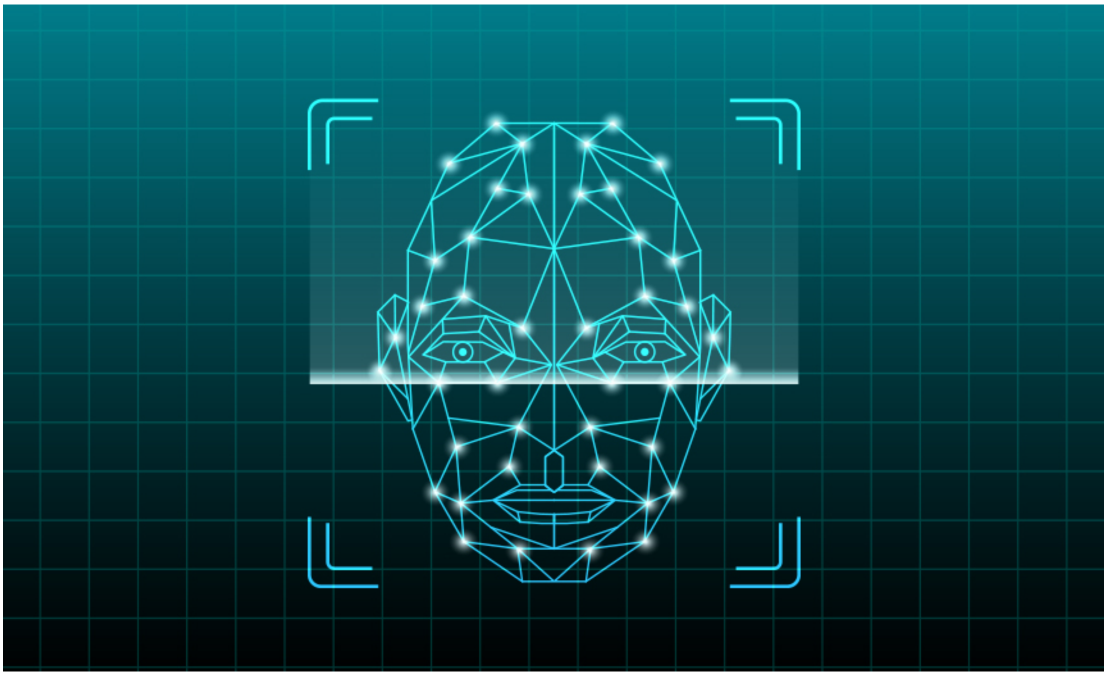
Redwood Shores, Calif.-based Imperva sells technology and services designed to detect and block various types of malicious Web traffic, from denial-of-service attacks to digital probes aimed at undermining the security of Web-based software applications.

“On August 20, 2019, we learned from a third party of a data exposure that impacts a subset of customers of our Cloud WAF product who had accounts through September 15, 2017,” wrote Heli Erickson, director of analyst relations at Imperva. We want to be very clear that this data exposure is limited to our Cloud WAF product. “The moral of the story here is that people need to be asking tough questions of software-as-a-service firms they rely upon, because those vendors are being trusted with the keys to the kingdom,” Knight said. “Even if the vendor in question is a cybersecurity company, it doesn't necessarily mean they're eating their own dog food.””

Read More on KrebsOnSecurity

Even More on ZDNet

Facial Recognition Use in Swedish School Triggers GDPR Fine



Sweden's Data Protection Authority has issued its first fine for violations of the European Union's General Data Protection regulation after a school launched a facial recognition pilot program to track students' attendance without proper consent.

The country's privacy authority issued a fine of 200,000 Swedish Krona ($20,700) to the municipality where the unnamed school is located for violating several of the privacy and biometrics provisions of GDPR, according to the European Data Protection Board. The municipality could have faced a €1 million ($1.1 million) penalty under GDPR, according to the privacy board.

Although municipal officials argued that the pilot program at the school was started with the students' consent, a spokesperson for the Swedish Data Protection Authority tells Information Security Media Group that the consent was not legally valid because "there is a clear imbalance between the data subject (the pupil) and the controller (the municipality)." The spokesperson added that it's waiting to hear if the municipality will appeal the fine.

Read More on BankInfoSecurity

More #News

- Google adds all Android apps with +100m installs to its bug bounty program
- Three Strategies to Avoid Becoming the Next Capital One
- What Is Social Engineering: The Tactics Used to Manipulate You
- Web clickjacking fraud makes a comeback thanks to JavaScript tricks
- Magecart Hackers Compromise 80 More eCommerce Sites to Steal Credit Cards
- French Police Remotely Removed RETADUP Malware from 850,000 Infected PCs

- Microsoft: Using multi-factor authentication blocks 99.9% of account hacks
- More than half of login attempts on social media accounts are fraudulent
- The Myth of Consumer-Grade Security
- Android 10 coming soon, with important privacy upgrades
- GitHub joins WebAuthn club
- Hostinger Suffers Data Breach – Resets Password For 14 Million Users
- Starbucks Abandons Azure Site, Exposed Subdomain to Hijacking
- Binance Confirms Hacker Obtained Its Users' KYC Data from 3rd-Party Vendor
- Windows 7 Still Used in Almost 50% of Surveyed Businesses
- WARNING — Malware Found in CamScanner Android App With 100+ Million Users
- Company behind Foxit PDF Reader announces security breach
- Ransomware Hits Dental Data Backup Service Offering Ransomware Protection
- Russian police take down malware gang that infected 800,000+ Android smartphones
- Why a Business-Focused Approach to Security Assurance Should Be an Ongoing Investment
- Kaspersky Incident Response report 2018

#Patch Time!

- Code Execution Flaw in QEMU Mostly Impacts Development, Test VMs
- Apple Releases iOS 12.4.1 Emergency Update to Patch 'Jailbreak' Flaw
- Cisco UCS Vulnerabilities Allow Complete Takeover of Affected Systems
- Cisco Fixes Critical Bug in Virtual Service Container for IOS XE
- DLL Hijacking Flaw Patched in Check Point Endpoint Security
- Over 14,500 pulse secure vpn endpoints vulnerable to cve-2019-11510

#Tech and #Tools

- How to use Harbor to scan Docker images for vulnerabilities
- Nine AWS Security Hub best practices
- zeek-httpattacks: detects HTTP requests that are non RFC compliant and used for smuggling
- Avira optimizer local privilege escalation
- Detecting attacks and improving response through the use of real-time security features
- Exploiting AWS ECR and ECS with the Cloud Container Attack Tool (CCAT)
- Open Redirect: A Small But Very Common Vulnerability
- osctrl: A fast and efficient osquery management solution
- A Study of Chinese Passwords
- Th3 L@s7 0f u$ - Analysis of Survival Password Genetics
- Non-root containers, Kubernetes CVE-2019-11245 and why you should care
- Whitelisting LD_PRELOAD libraries using LD_AUDIT
- The World's First Cyber Crime: The Morris Worm [KERNEL PANIC]
- Phishing with SAML and SSO Providers
- How I Hacked Instagram Again
- Yar: Plundering organizations, users and/or repositories.
- Chrome-Password-Dumper

- Chrome-Password-Dumper
- Setup up your Out-of-Band DNS Server
- DFIR Summit & Training 2019 (July 2019)

Kingred Group is growing, so does the Group Security team! We're looking for new talented professionals to come join us:

- You like to break things, then explain how to fix it? Be part of our Cyber Security team
- You prefer the blue team side? Check out our Security analyst position
- Interested in Governance, Risk and Compliance? Apply for our Information Security Specialist role

Kindred is one of the largest online gambling companies in the world with over 24 million customers across 100 markets. 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 over 24 million customers across 100 markets. 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 as an innovation driven company that builds on trust.

You can access the previous newsletters at https://news.infosecgur.us