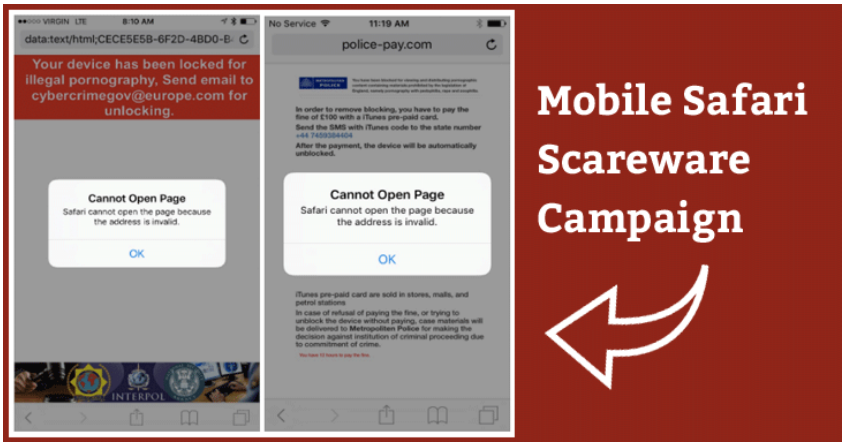
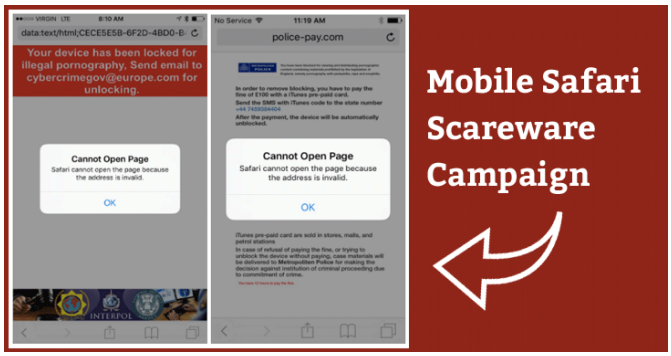
Apple iOS 10.3 Fixes Safari Flaw Used in JavaScript-based Ransomware Campaign



Apple iOS 10.3 Fixes Safari Flaw Used in JavaScript-based Ransomware Campaign

If you own an iPhone or iPad, it's possible you could see popup windows in a sort of endless cycle on your Safari browser, revealing your browser has been locked and asking you to pay a fee to unlock it. Just do not pay any ransom.



A new ransomware campaign has been found exploiting a flaw in Apple's iOS Safari browser in order to extort money from users who view pornography content on their phones or attempt to illegally download pirated music or other sensitive content.

However, the good news is that Apple patched the web browser vulnerability on Monday with the release of iOS version 10.3.

The vulnerability resides in the way Safari displayed JavaScript pop-up windows, which allowed ransomware scammers to display an endless loop of pop-up windows, preventing victims to use the browser, researchers from mobile security provider Lookout said in a blog post published on Monday.

The victims eventually would end up on an attacker website that masquerades itself as a legitimate law enforcement site informing victims that they have to pay a fine for viewing illegal content in order to regain access to their browser.

Lookout researchers called the exploit « scareware, » as the attack doesn't actually encrypt any data and hold it ransom. Rather the attack just scares victims into paying the ransom fee to unlock the browser.

« The scammers abused the handling of pop-up dialogs in Mobile Safari in such a way that it would lock out a victim from using the browser, » Lookout explains.

« The attack would block the use of the Safari browser on iOS until the victim pays the attacker money in the form of an iTunes Gift Card. During the lockout, the attackers displayed threatening messaging in an attempt to scare and coerce victims into paying. »

The scammers effectively used fear as a factor to get victims pay the fee before they realized that there was no real risk to their data and it's very easy to overcome this issue.

While overcoming the threat for users is as simple as clearing their browsing history and cache, iOS 10.3 users are no longer at risk of getting trapped in the endless cycle of JavaScript popups.

Lookout researchers shared the cause of this iOS exploit with Apple last month, and the company has promptly patched the issue with the release of iOS 10.3. Now, pop-up windows only take over a tab, instead of the entire app.

Those iOS 10.2 users who are already hit by this ransomware campaign can clear their browsing cache by navigating to Settings → Safari → Clear History and Website Data.

Swati Khandelwal

***Notre métier** : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus…) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.*

Par des actions d'expertises, d'audits, de formations et de sensibilisation dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement..

(Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)

Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en protection des « Données à Caractère Personnel ».

- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle...) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ; (Autorisation de la DRTEF n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE Cybersécurité & Conformité

Contactez-nous

Réagissez à cet article

Source : *Apple iOS 10.3 Fixes Safari Flaw Used in JavaScript-based Ransomware Campaign*