Security Newsletter

23 April 2018

Subscribe to this newsletter

NSA reveals how it beats 0-days

In the ongoing cat-and-mouse game between nation states and attackers, anyone with something to protect has less time than ever to shore up their defenses.

At this week's RSA conference in San Francisco, Dave Hogue, technical director of the US National Security Agency (NSA), reviewed the organization's best practices for defense – one of which is to "harden to best practices," as the NSA often sees attacks against their systems within 24 hours of a new vulnerability being disclosed or discovered in the wild.

Read More

Over 20 Million Users Installed Malicious Ad Blockers From Chrome Store

If you have installed any of the below-mentioned Ad blocker extension in your Chrome browser, you could have been hacked.

A security researcher has spotted five malicious ad blockers extension in the Google Chrome Store that had already been installed by at least 20 million users.

Unfortunately, malicious browser extensions are nothing new. They often have access to everything you do online and could allow its creators to steal any information victims enter into any website they visit, including passwords, web browsing history and credit card details.

Read More

iOS Trustjacking – A Dangerous New iOS Vulnerability

An iPhone user's worst nightmare is to have someone gain persistent control over his/her device, including the ability to record and control all activity without even needing to be in the same room. In this blog post, we present a new vulnerability called "Trustjacking", which allows an attacker to do exactly that.

This vulnerability exploits an iOS feature called iTunes Wi-Fi sync, which allows a user to manage their iOS device without physically connecting it to their computer. A single tap by the iOS device owner when the two are connected to the same network allows an attacker to gain permanent control over the device. In addition, we will walk through past related vulnerabilities and show the changes that Apple has made in order to mitigate them, and why these are not enough to prevent similar attacks.

Read More

Cutting room floor

- Another Critical Flaw Found In Drupal Core—Patch Your Sites Immediately
- Piercing the Veil: Server Side Request Forgery to NIPRNet access
- AMD gaming evolved raptr plays tv remote file execution
- WordPress hacked site – forensics report
- JSON Web Token (JWT) Security Cheat Sheet PDF

#Tech and #Tools

- A fully automated WPA PSK handshake capture script aimed at penetration testing.
- Official python API for Phish.AI public and private API to detect zero-day phishing websites.

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 15 million customers across 100 markets. We offer pre-game and live Sports betting, Poker, Casino and Games through 13 subsidiaries and 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.