kindred

Security Newsletter

7 May 2018

Subscribe to this newsletter

The Mozilla Foundation is testing a new mechanism for securing domain name server traffic that uses the encrypted HTTPS channel. It is an attempt to speed up the internet, reduce the threat of man-in-the-middle attacks and keep prying eyes from monitoring what users do online.

Starting in the next several weeks, Mozilla plans to run tests using a developer version of its Firefox browser with the help of the Mozilla developer community and content management and delivery network firm Cloudflare. Developers will be testing a proposed standard called Trusted Recursive Resolver via DNS over HTTPS, or DoH for short. The standard is winding its way through a draft process and is scheduled to be voted on for ratification by the Internet Engineering Task Force (IETF) later this year.

However, despite potential gains in speed, security and privacy, some have expressed concerns pointing out that centralizing DNS traffic through gatekeepers trades one privacy problem with another.

Read More

TLS 1.3 Is Coming

The much required Transport Layer Security version TLS 1.3 approved finally by IETF after 28 drafts. TLS 1.3 is not a minor redesign, it is a major redesign of TLS 1.2.

Internet Engineering Task Force (IETF) is an open source community of network designers, operators, vendors, and researchers who collaborate to evaluate the standards.

TLS 1.2 was published in August 2008 after a long hold up as of March 21st, 2018, TLS 1.3 has now been concluded, after going into more than four years and 28 drafts.

Read More

IDN Homograph Attack Is Back

Even the most vigilant internet users are susceptible to this IDN homograph attack

A new wave of Unicode Domain Phishing attacks are tricking even the most seasoned of internet veterans thanks to its clever use of homographs.

For those that don't know a homograph is a set of two or more words that are spelled the same but have different meanings and origins. In this case, homograph is an imperfect descriptor, but it's still sufficient. To execute a Unicode Domain Phishing attack, you first need a Unicode domain. Typically, the URLs you type are in ASCII, that stands for American Standard Code for Information Interchange. However, in 2003, a specification was added to allow Unicode characters to be used in domain names. Unicode is an industry standard for encoding text expressed in most of the world's written languages. The idea behind this was to give international internet users the ability to follow links in their own language. But, as with everything on the internet, somebody found a way to exploit this.

- Researcher Xudong Zheng published a proof of concept last year that highlights the issue. In the POC, Zheng uses Unicode to produce a web page that resembles Apple's. To do this, he created a domain with Punycode, which allows for Internationalized Domain Names. He then mixed in Unicode with ASCII to create a website that actually says "Apple.com"

Read More

Cutting room floor

- A Vulnerability in 7-Zip Could Allow for Arbitrary Code Execution
- Faulty Patch for Oracle WebLogic Flaw Opens Updated Servers to Hackers Again
- A glitch caused Twitter passwords to be stored in plain text on an internal log.

#Tech and #Tools

- Security Onion is a free and open source Linux distribution for intrusion detection, enterprise security monitoring, and log management.
- Empire is a PowerShell and Python post-exploitation agent.
- SecLists is the security tester's companion. It is a collection of multiple types of lists used during security assessments
- bettercap is the Swiss army knife for network attacks and monitoring.
- Volatility an advanced memory forensics framework
- EvilURL generate unicode evil domains for IDN Homograph Attack and detect them.
- Infection Monkey - Data center Security Testing Tool

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.