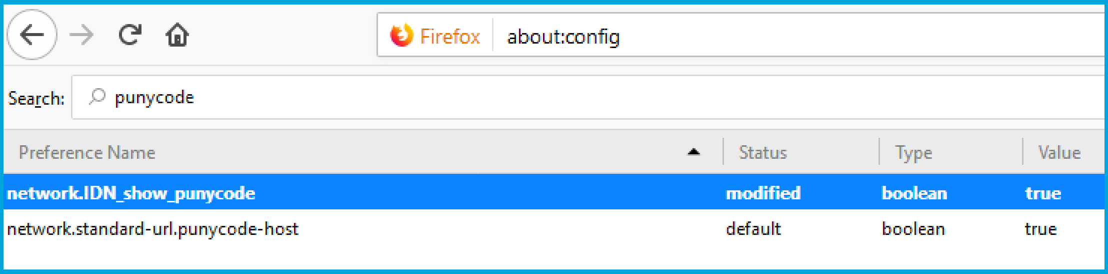
kindred

Security Newsletter

3 December 2018

Subscribe to this newsletter

Half of all Phishing Sites Now Have the Padlock



Firefox about:config

Search: punycode

Preference Name	Status	Type	Value
network.IDN_show_punycode	**modified**	**boolean**	**true**
network.standard-url.punycode-host	default	boolean	true

Maybe you were once advised to “look for the padlock” as a means of telling legitimate e-commerce sites from phishing or malware traps. Unfortunately, this has never been more useless advice. New research indicates that half of all phishing scams are now hosted on Web sites whose Internet address includes the padlock and begins with “https://”.

This alarming shift is notable because a majority of Internet users have taken the age-old “look for the lock” advice to heart, and still associate the lock icon with legitimate sites. A PhishLabs survey conducted last year found more than 80% of respondents believed the green lock indicated a website was either legitimate and/or safe.

In reality, the https:// part of the address (also called “Secure Sockets Layer” or SSL) merely signifies the data being transmitted back and forth between your browser and the site is encrypted and can't be read by third parties. The presence of the padlock does not mean the site is legitimate, nor is it any proof the site has been security-hardened against intrusion from hackers.

Read More on KrebsOnSecurity

Uber fined $1.1 million by UK and Dutch regulators over 2016 data breach

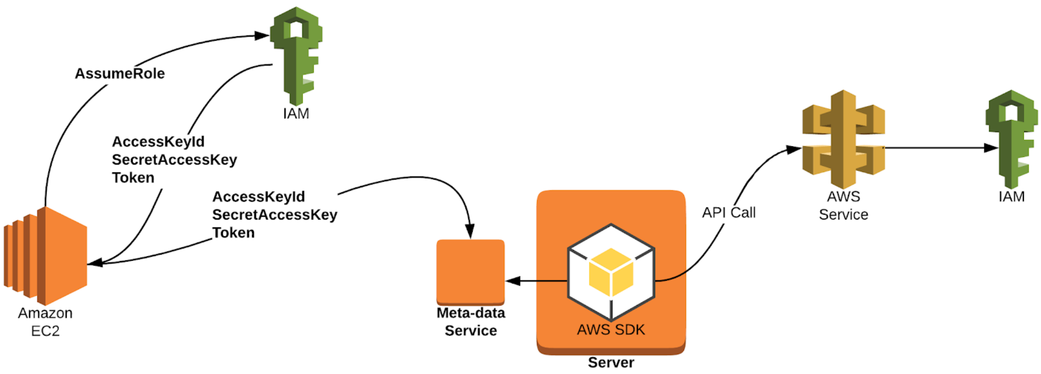
British and Dutch data protection regulators Tuesday hit the ride-sharing company Uber with a total fine of $1,170,892 (~ 1.1 million) for failing to protect its customers' personal information during a 2016 cyber attack involving millions of users.

Late last year, Uber unveiled that the company had suffered a massive data breach in October 2016, exposing names, email addresses and phone numbers of 57 million Uber riders and drivers along with driving license numbers of around 600,000 drivers.

Today Britain's Information Commissioner's Office (ICO) fined Uber 385,000 pounds ($491,102), while the Dutch Data Protection Authority (Dutch DPA) levied a 600,000 euro ($679,790) penalty on Uber for failing to protect the personal information of its 3 million British and 174,000 Dutch citizens, respectively. Since the data breach happened before the EU's General Data Protection Regulation (GDPR) took effect in May 2018, the fine of £385,000 imposed under the UK's old Data Protection Act 1998 is still lesser.

Read More on TheHackerNews

Preventing Credential Compromise in AWS



Previously we wrote about a method for detecting credential compromise in your AWS environment. The methodology focused on a continuous learning model and first use principle. This solution still is reactive in nature — we only detect credential compromise after it has already happened.. Even with detection capabilities, there is a risk that exposed credentials can provide access to sensitive data and/or the ability to cause damage in our environment.

Today, we would like to share two additional layers of security: API enforcement and metadata protection. These layers can be used to help prevent credential compromise in your environment.

Read More on Netflix Technology Blog

More #News

- Cisco pushes fix for failed Webex vulnerability patch
- Atrium Health data breach exposed 2.65 million patient records
- AWS Security Hub Aggregates Alerts From Third-Party Tools
- ElasticSearch server exposed the personal data of over 57 million US citizens
- MITRE Changes the Game in Security Product Testing
- How secure is serverless computing?
- Sennheiser Headset Software Could Allow Man-in-the-Middle SSL Attacks
- After Microsoft complaints, Indian police arrest tech support scammers at 26 call centers
- Google's “deceitful” location tracking is against the law, say 7 EU groups
- Dell Resets All Customers' Passwords After Potential Security Breach
- New industrial espionage campaign leverages AutoCAD-based malware

#Tech and #Tools

- Security baseline (FINAL) for Windows 10 v1809 and Windows Server 2019
- Golem Malware - The Malware Hiding in Your Windows Fonts Folder
- Broken Link Hijacking: Example with AWS Slurp Github Takeover
- GreyNoise Visualizer: Monitor internet mass-scans
- HTCAP: Single Page Application crawler
- XSShell: XSS "reverse shell" framework
- tyton: Kernel-mode rootkit hunter
- Quarantyne: new look at web application firewalling
- Cloud Metadata Dictionary useful for SSRF Testing
- Hunting with ꓘamerka 2.0 aka FIST (Flickr, Instagram, Shodan, Twitter)
- Hiding Through a Maze of IoT Devices abusing UPnP
- Hunting in Active Directory: Unconstrained Delegation & Forests Trusts
- Mapping the ASD Essential 8 to the Mitre ATT&CK™ framework

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