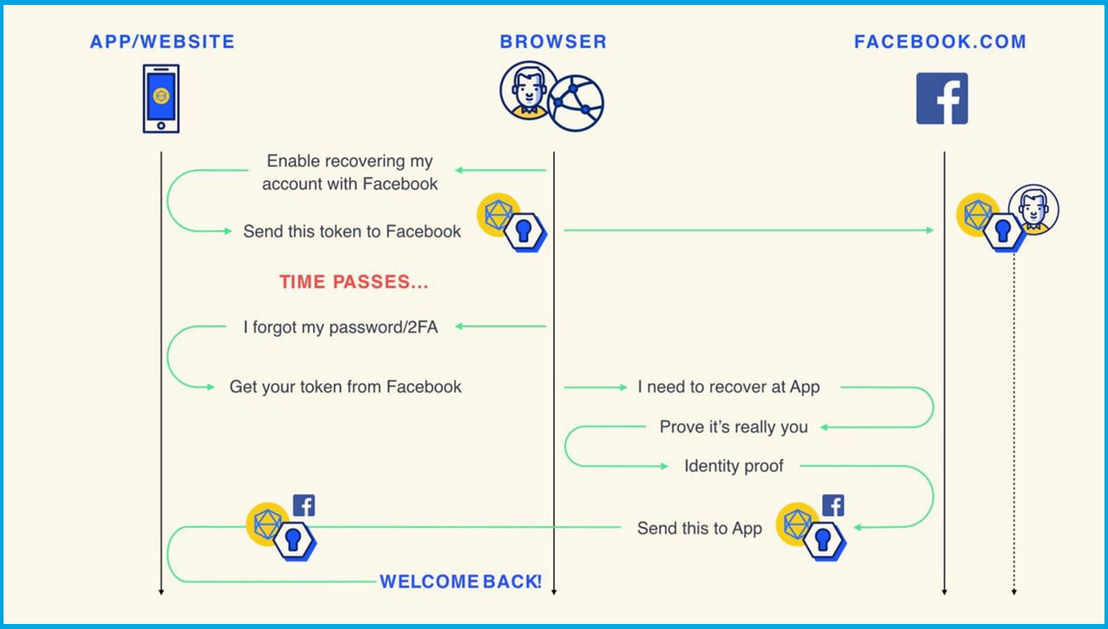
kindred

Security Newsletter

24 April 2017

Delegated Account Recovery with Facebook



A recent study by Gigya in the US and UK revealed that 55 percent of people will abandon a log in page because they forget their password or answer a security question incorrectly. And the trouble doesn't end there: the 45 percent who don't abandon the page are more likely to create a new account than to work through the established account recovery process, making a mess of your data and confusing your CRM systems.

In January, Facebook presented a new approach: Delegated Account Recovery. Instead of requesting user data at the outset, your business creates a recovery token linked to your identifier for the customer, and sends it to Facebook. Facebook keeps it safe and private until that person needs it. When the need to recover access arises, Facebook will take the person through a re-authentication flow and then send the original token back to the service that created it, with a new cryptographic signature from Facebook.

Facebook says that delegated account recovery will be a more secure account recovery vehicle than what's typically used, which is email. The good news: judging by what GitHub and Facebook have described, we don't have to trust Facebook, because it isn't actually handling our personal information, or our app accounts.

Facebook has been working with GitHub to build and test the service, and following a successful trial period, they're giving the developer community access to the protocol as part of a closed beta program and publishing SDKs, documentation, and example applications for both Java and NodeJS server platforms. You can learn more, read the specification, download example code, and apply to participate in Facebook's early access program at https://fb.me/recovery.

Read More

Facebook statement

Hajime, Brickerbot, vigilantes (or competitors?) are attacking Mirai botnet

Authorities have been talking about IoT security standards for years, but in the meantime, some of the same vendors participating in those discussions have continued to ship out insecure devices with the same ol' default passwords. Some crooks have used those blatant vulnerabilities to assemble big IoT botnets, Mirai being the most popular example. But other botnets are currently fighting on Mirai's territory, and we're not sure if they are grey hat acting for our own good, or competitors hiding behind a fake, vigilante posture.

First there is Hajime. Once in control of a target, it blocks several ports used by rival IoT-ware, a perfect annoyance for Mirai. Lacking a module that could be used to launch DDoS, it currently sends a signed message stating "Just a white hat securing some systems. Important messages will be signed like this! Hajime Author. Contact CLOSED. Stay sharp!". According to new estimates it has taken over at least “tens of thousands” of devices, especially in Brazil, Iran, Thailand, the Russian Federation and Turkey.

As regards Brickerbot, it is the first threat of its kind that intentionally bricked IoT and networking devices, by rewriting the flash storage space of affected devices with random data. Such actions rendered troves of devices useless, many needing a firmware reinstall, but as many needing to be replaced altogether. BrickerBot allegedly wiped over two million devices.

The message for all owners of IoT devices is to secure your devices, and for vendors of those devices to pull their fingers out and update firmware. In the case of Mirai and Hajime, simply applying a decent password and username is an excellent start.

BrickerBot

Hajime

Did Microsoft delayed February's patch tuesday to fix Shadowbrokers' flaws ?

Microsoft delayed its February security update slate to finish patching critical flaws in Windows that a hacker gang tried to sell, several security experts have argued. MS17-010, one of several security bulletins Microsoft issued in March, was just one of several cited Friday by the Redmond, Wash. developer when it said it had already patched most of the vulnerabilities exploited by just-leaked hacking tools.

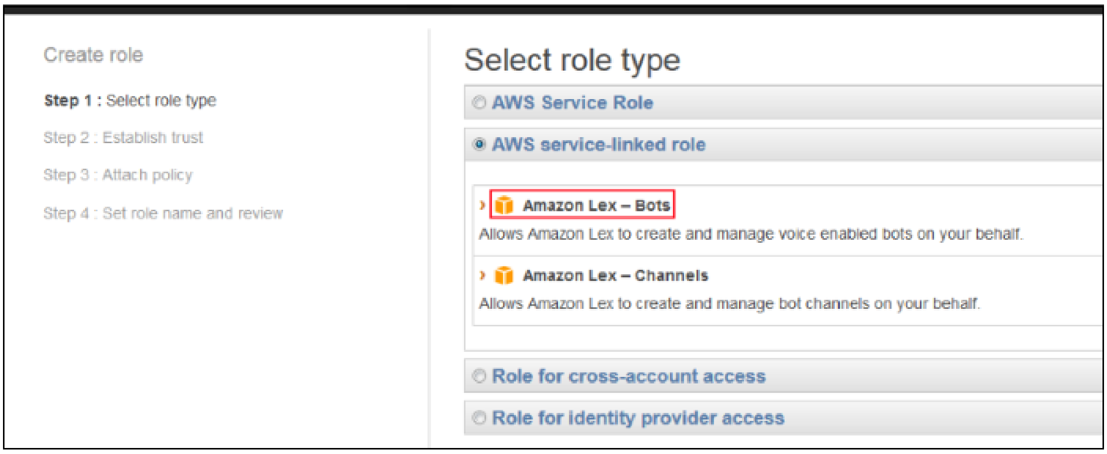
Those tools -- 12 different Windows exploits -- had been included in a large data dump made April 14 by a hacker group dubbed Shadow Brokers, which is believed to have ties to Russia. The exploits, as well as a trove of documents, had been stolen from the National Security Agency (NSA), Shadow Brokers claimed. The timing -- Shadow Brokers' January auction, Microsoft's MS17-010 release in March -- and the unprecedented, and still unexplained, decision by the latter to postpone all of February's security updates, brought several security professionals to the same connect-the-dots conclusions.

Two months ago, Microsoft issued only a vague statement when it cancelled February's patches, saying, "We discovered a last-minute issue that could impact some customers and was not resolved in time for our planned updates." Nor has the company explained how it came to find the vulnerabilities it rushed to patch in MS17-010. Although Microsoft asserted that it had not been alerted by outsiders, it did not respond to questions from journalists, including how it learned of the bugs.

Read More

NSA hacking tools

Introducing an Easier Way to Delegate Permissions to AWS Services: Service-Linked Roles



Create role

Step 1 : Select role type

Step 2 : Establish trust

Step 3 : Attach policy

Step 4 : Set role name and review

Select role type

○ AWS Service Role

● AWS service-linked role

› Amazon Lex – Bots

Allows Amazon Lex to create and manage voice enabled bots on your behalf.

› Amazon Lex – Channels

Allows Amazon Lex to create and manage bot channels on your behalf.

○ Role for cross-account access

○ Role for identity provider access

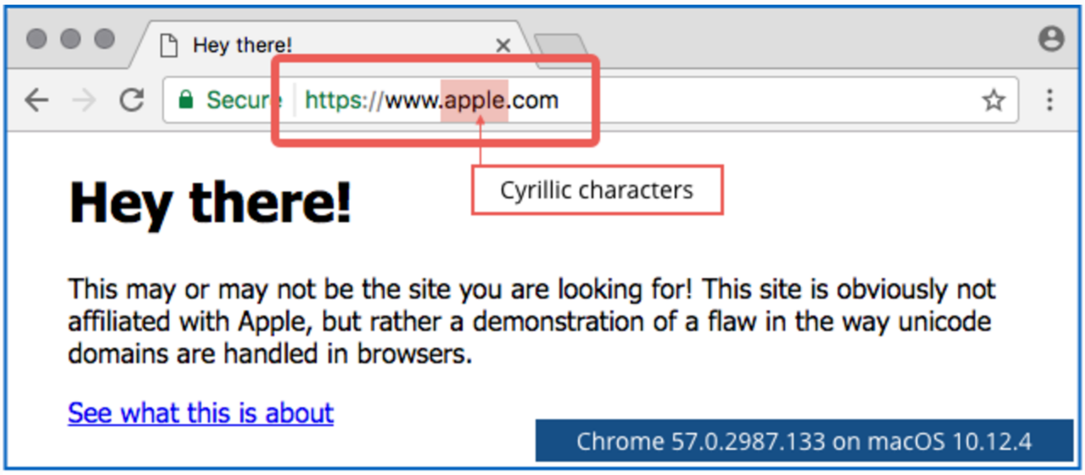
Some AWS services create and manage AWS resources on your behalf. To do this, these services require you to delegate permissions to them by using AWS Identity and Access Management (IAM) roles. Today, AWS IAM introduces service-linked roles, which give you an easier and more secure way to delegate permissions to AWS services.

Each service-linked role links to an AWS service, which is called the linked service. Service-linked roles provide a secure way to delegate permissions to AWS services because only the linked service can assume a service-linked role. This makes it easier for you to manage the permissions you delegate to AWS services.

To start, you can use service-linked roles with Amazon Lex, Over time, more AWS services will use service-linked roles as a way for you to delegate permissions to them to create and manage AWS resources on your behalf.

Read More

Phishing with ‘punycode’ – when foreign letters spell English words



Hey there!

This may or may not be the site you are looking for! This site is obviously not affiliated with Apple, but rather a demonstration of a flaw in the way unicode domains are handled in browsers.

See what this is about

Chrome 57.0.2987.133 on macOS 10.12.4

The curiously-named system known as punycode is a way of converting words that can’t be written in ASCII, such as the Ancient Greek phrase ΓΝΩΘΙΣΕΑΥΤΟΝ (know yourself), into an ASCII encoding, like this: xn--mxadglfwep7amk6b. This makes it possible to encode so-called International Domain Names (IDNs) – ones that include non-ASCII characters – using only the Roman letters A to Z, the digits 0 to 9 and the hyphen (-) character, as required for DNS domains for example.

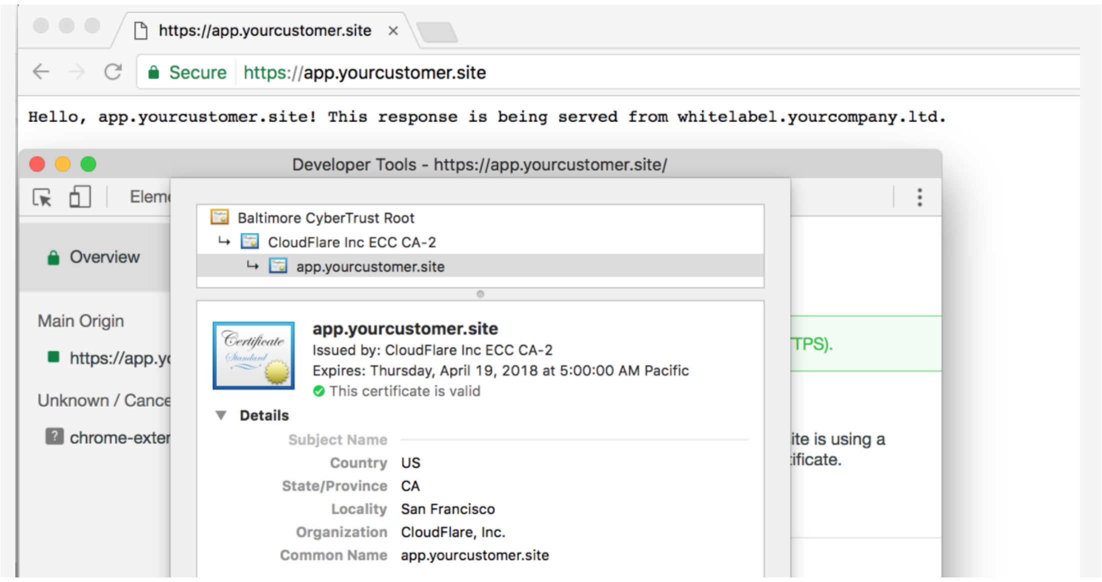
By default, browser makers were supposed to read the Punycode URL and transform it into Unicode characters inside the browser. Nevertheless, browser makers were quick to understand that Punycode could be used to disguise phishing sites as legitimate sites. We call this homograph attacks, and it has been known since 2001. That’s why, some browser makers introduced filters to render URLs as Punycode (instead of Unicode) if the URL contained characters from different languages (eg., Cyrillic + Latin), deeming such URLs as phishing attempts. This meant that only Punycode URLs in one language would be rendered as Unicode...

...and this is exactly what this new attack is doing, the researcher managed to create a domain that looked like apple .com, only using cyrillic characters. Browsers are now into a dilemma, leaving everything in punycode is seen as culturally insensitive, but leaving it like this allow dangerous abuse. In the meantime, using a password manager would protect you from the risk of pasting password in an incorrectly named site. You can also look at the certificate details, which will contain the Common Name it is issued to in...punycode.

Read More

Even more

Introducing SSL for SaaS



https://app.yourcustomer.site

Secure https://app.yourcustomer.site

```
Hello, app.yourcustomer.site! This response is being served from whitelabel.yourcompany.ltd.
```

Developer Tools - https://app.yourcustomer.site/

Baltimore CyberTrust Root
↳ CloudFlare Inc ECC CA-2
↳ app.yourcustomer.site

app.yourcustomer.site
Issued by: CloudFlare Inc ECC CA-2
Expires: Thursday, April 19, 2018 at 5:00:00 AM Pacific
✓ This certificate is valid

▼ **Details**

Subject Name	
Country	US
State/Province	CA
Locality	San Francisco
Organization	CloudFlare, Inc.
Common Name	app.yourcustomer.site

This week, Cloudflare unveiled SSL for SaaS companies, a wholesale SSL solution that will allow SaaS companies to extend Cloudflare benefits to their customers on their own domain without the need for engineering or support work or any extensive customer set-up.

The need for providing SSL to SaaS customers on unique domains is frequently hindered by difficulties in implementation. Cloudflare's SSL for SaaS seeks to address this problem. Customers add the initial CNAME into their domain, after which SaaS companies send a single API call to them. Cloudflare then provisions the hostname for forwarding, acquires SSL certificates to enable HTTPS and HTTP/2, and sits in front of the customer's site to protect against DDoS and layer 7 attacks on customer websites. In addition, customers of SaaS companies using Cloudflare's wholesale SSL will receive the same CDN, WAF, HTTP/2, and load balancing benefits as other Cloudflare customers.

SSL for SaaS is available for any bring-your-own-domain SaaS applications, such as content management solutions, eCommerce platforms, web portals, and PaaS companies that allow apps to be served on customer host names.

Read More

Official statement

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.