RSAConference2016
San Francisco | February 29 – March 4 | Moscone Center

Connect to Protect

SESSION ID: ASD-T11

Nothing Lasts Forever

A Talk About Expired Security

Matthew Bryant
Application Security Engineer
Uber Technologies Inc.
@IAmMandatory

#RSAC

Matthew Bryant (mandatory)

- Application Security Engineer at Uber Technologies Inc.
- Maintainer of The Hacker Blog: https://thehackerblog.com
- @IAmMandatory
- https://github.com/mandatoryprogrammer

- Signal Fingerprint

05 d4 6b db 51 31 9b 43 b6 6b c6 96 91 fb 3c 1e 60 3c 93 6b 4e 1f 55 8e 54 9a 93 e0 a4 c3 ad 99 34

UBER

EVERYONE'S PRIVATE DRIVER™

What're we talking about here?

- This talk explores the intersection of trust and ephemeral assets.
- Trust is given to things that expire all the time (domains, cloud instances, etc.).
- What happens when an attacker reacquires these things?

Agenda

- Extensions of Trust
- Nothing Lasts Forever, Broken Links and Dangling Trust
- From Expired to Attack-Acquired
- Solving the Problem

UBER

EVERYONE'S PRIVATE DRIVER™

RSAConference2016
San Francisco | February 29 – March 4 | Moscone Center

Connect to Protect

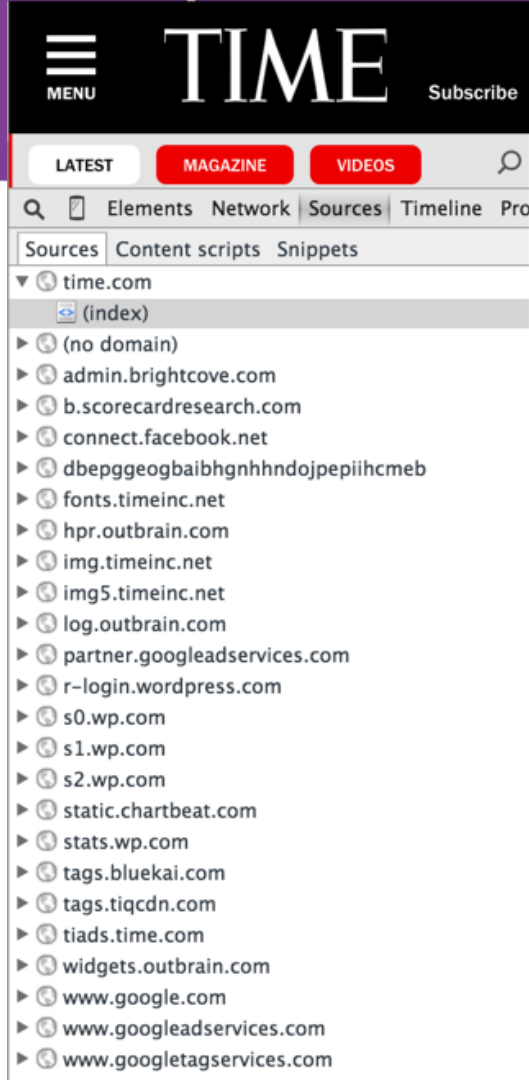
SESSION ID:

Extensions of Trust

Trust Me, I'm Ephemeral

The interconnected web

- The web is tangled.
- External resources happen on every page load.
- These domains are all trusted implicitly.



Third-party Services

- Web applications are all connected via APIs and Software as a Service (SaaS).
- Ephemeral cloud instances are incredibly popular: EC2, Linode, Digital Ocean instances.
- Applications that don’t make use of any external services are now the outliers.

Content Delivery Networks

- Even web libraries are often not self-hosted.
- CDNs are common to handle large amounts of traffic and to prevent denial of service (DDoS) attacks.
- Many sites trusting one service to host JavaScript, CSS, and images for other sites.

Extreme Trust – crossdomain.xml

- One notable instance is with crossdomain.xml policies.
- A crossdomain.xml file specifies which site's are trusted to perform authenticated requests for a domain.
- So example.com could allow http://thirdparty.com to perform actions as logged in users by specifying it in their crossdomain.xml policy.

UBER

EVERYONE'S PRIVATE DRIVER™

RSAConference2016
San Francisco | February 29 – March 4 | Moscone Center

Connect to Protect

SESSION ID:

Nothing Lasts Forever

Broken Links and Dangling Trust

Domains Expire

- Domains don’t last forever – they must be renewed yearly.

Service Plans Expire, Companies Go Out of Business

- Companies and providers go out of business.
- What happens to their clients who've integrated with them?

Dynamic Instances

- With cloud instances you spin up a host until its purpose has been fulfilled — then you terminate it.

- When you kill an instance, are you also removing everything that was pointing to it?

Records Expire But Trust Remains

- When a domain expires, or an instance is terminated, is it still trusted?
- Are DNS records left dangling?
- Are these resources embedded in your pages?
- Do people still trust these instances?

RSAConference2016
San Francisco | February 29 – March 4 | Moscone Center

Connect to Protect

SESSION ID:

From Expired To Attacker-Aquired

Attacking Forgotten Trust

RSAConference2016
San Francisco | February 29 – March 4 | Moscone Center

Connect to Protect

SESSION ID:

Diving Into the Elastic IP Pool

Cloud Nine

The Cloud

- One good example of ephemeral resources are cloud instances.

- EC2, Linode, App Engine, Rack Space, etc.

The Cloud

- These instances are ephemeral by design.
- You pay for what you use, then you spin down the instance.
- These resources are part of a pool that people draw from and release back into.

amazon web services™

UBER

EVERYONE'S PRIVATE DRIVER™

Example Scenario

- Company ExampleCo has a promotional offer site that they want to run for only two weeks.
- They spin up an Amazon EC2 instance and point promotion.exampleco.com to it.
- After the promotion ends, the development team terminates the instance.

Example Scenario

- What went wrong?

Example Scenario

- They didn’t delete the DNS entry pointing to promotion.exampleco.com.

- That IP address was thrown back into the AWS pool to be reused by other users.

Attack Scenario

- These IP addresses could potentially be reallocated by attackers as well.
- However, in the case of AWS you cannot allocate a specific IP.
- In order to gain control of a domain we have to go fishing.
- In an attempt to exploit this we created a program called poolplayer.

Attack Scenario

The program works as follows:

- Allocating an IP address
- Checking multiple DNS databases for the allocated IP (DNS Dumpster, Domain Tools, ViewDNS)
- If the IP has domains or subdomains pointing to it — keep it. If not, throw it back into the pool.

- What I thought it’d be like…


PENN

- In reality it’s more like a lot of this…


VOLCOM

- With the occasional…


PENN

The Results

- The domains are mostly random.
- We allocated everything from government subdomains to Japanese VPN provider endpoints.
- Unpredictable but overtime yielding interesting results.

- sso.dev.siam.education.govt.nz

WELCOME TO EDUCATION.govt.nz

Helping you find what you need to know about education in New Zealand.

SCHOOL TERMS AND HOLIDAYS

For 2015:
Term 2 ended: Friday 3 July
Term 3 begins: Monday 20 July
Term 3 ends: Friday 25 September

Find term dates

FIND AN EDUCATION SERVICE

Tools to find a school or an early childhood education (ECE) service.

Find a school

Find an ECE service

PARENTS

We've developed a website to give you easy to understand and practical information about education.

Parents website

NEWS | VACANCIES

Why PAI?
23 July 2015

Early Learning funding reminders – July 2015
20 July 2015

Changes to the Ministry of Education websites and email addresses
20 July 2015

Managing child illness in ECE services and kōhanga reo
20 July 2015

01 July 2015
Over 1800 schools on the managed network

22 April 2015
Investing in Educational Success

- area1fte.edu.br

ÁREA1 | DeVry Brasil

Vestibular 25/JUL - Clique e Inscreva-se

Transferência 2015.2 - Clique e Inscreva-se

Like 41k

Pesquisar

já sou ÁREA1

INSTITUCIONAL

DEVRY BRASIL

BENEFÍCIOS INTERNACIONAIS

CURSOS

PROUNI COM QUALIDADE INTERNACIONAL.

+ 4.700 BOLSAS DEVRY BRASIL

ESCOLHA A ÁREA1

Inscreva-se até **20/JULHO**

1 2 3 4 5 6 7 8

ESTUDE NA ÁREA1

Escolha a melhor maneira de ingressar no seu curso: **Vestibular**, **Transferência**, **Portador de diploma**, **ENEM**, **PROUNI** e **Pós-Graduação**.

>> Saiba Mais

QUALIDADE ACADÊMICA

Confira as notas e avaliações dos cursos, de acordo com o MEC e ENADE, que reforçam a visão DeVry de educação de qualidade internacional.

>> Saiba Mais

FIES 2015

A ÁREA1 | DeVry ajuda você a se inscrever no FIES. Ligue para 4020-4900 e receba instruções sobre sua inscrição.

>> Saiba Mais

CENTRAL DE ATENDIMENTO

Entre em contato com a gente! Estamos disponíveis para atendê-lo via: **Chat Online**, Ouvidoria e Contact Center.

>> Saiba Mais

- cert.safetypay.com

Countries United States

SAFETY PAY™

WHO WE ARE WHAT WE DO WHERE WE ARE

How We Work For You

- vpn825798936.softether.net
  sdrservers.softether.net
  cyberdeftech.softether.net
  vpn825798936.softether.net
  vpn719195286.softether.net
  vpn426316912.softether.net
  vpn658514917.softether.net
  vpn286892270.softether.net
  vpn658514917.softether.net
  vpn426316912.softether.net
  vpn658514917.softether.net
  vpn818446566.softether.net vpn163936725.softether.net
  vpn426316912.softether.net
  vpn658514917.softether.net
  vpn765121359.softether.net
  vpn462247143.softether.net vpn797794763.softether.net
  vpn462247143.softether.net
  vpn643885422.softether.net vpn299584053.softether.net
  vpn462247143.softether.net
  willionmax02.softether.net
  vpn462670062.softether.net

ソフトイーサ Web サイト
製品・サービス
無償ソフト・学術実験サービス
導入事例
購入方法
ダウンロード
サポート
報道発表資料
ソフトイーサ 企業情報
お問い合わせ

目次
ソフトイーサの VPN ソフトウェア製品・通信サービス
キャラミん♪
ソフトイーサのその他の技術および無償ソフト

ソフトイーサ Web サイト

ソフトイーサ株式会社 は PacketiX VPN や Desktop VPN をはじめとする高品質な VPN ソフトウェアや通信サービスを開発し、日本国内の 10,000 社を超えるお客様に提供することにより、日本企業の ICT インフラを支えています。

HardEther 1Gbps イーサネット専用線サービス、Desktop VPN Business シンクライアントシステム および QUMA 3D 技術 などのその他の製品・サービスのほか、オープンソース版 SoftEther VPN や遠隔操作型ウイルスの犯人を追跡するための パケット警察 などの強力な通信・セキュリティソフトウェアをフリーソフトとして提供するなど、日本国内における ICT のさらなる発展に貢献いたします。

ソフトイーサの VPN ソフトウェア製品・通信サービス

PacketiX VPN は企業内、クラウドおよびスマートフォン環境のための VPN 構築に利用可能な、複数 VPN プロトコルに対応した VPN ソフトウェアです。強力な機能を有していますが、企業内のシステム管理者や一般 PC ユーザーの方でも容易に導入いただくことができます。PacketiX VPN 4.0 では新たに iPhone や Android からの接続や Cisco ルータ、Microsoft VPN プロトコルとの互換性機能も搭載されました。

- qa.oms.origin.com

Origin

BROWSE GAMES

FREE GAMES

DEALS

Search...

The SIMS 4

SPA DAY

Stressful Week?

Yoga, massages, and more!
Visit the spa or build your own.

Check It Out

DRAGON AGE INQUISITI

Get Armor and

Buy Spoils of the
protect your hero

- uat.ebolaexplained.co.uk

EBOLA

Information from the Institute of Global Health Innovation at Imperial College London

What is Ebola?

What it is, where it's from and how it

Have I got Ebola?

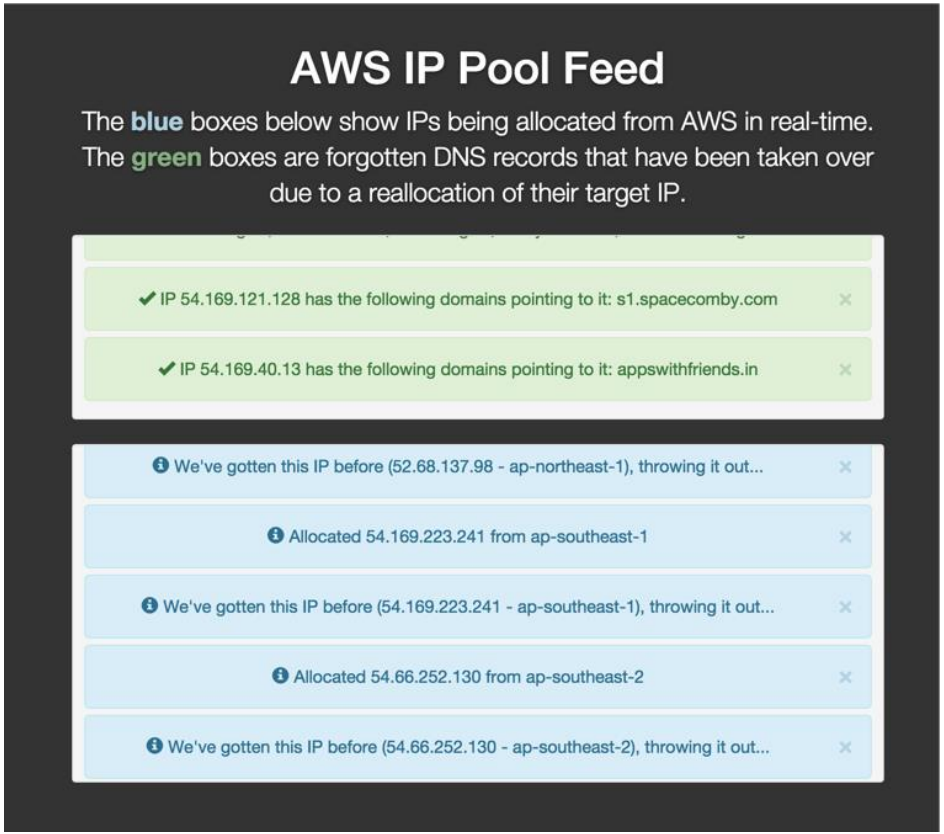
Use this simple symptom checker to

How do you kill Ebola?

How to destroy the virus and stop it

Conclusions

- This problem appears to be systemic and not widely explored.
- Over time, finding IP addresses with domains pointing to them will become easier and easier due to IPv4 being limited.
- We may end up with a very crowded pool.



UBER

EVERYONE'S PRIVATE DRIVER™

View This Panel

- http://thehackerblog.com/awsfishing/

https://web.archive.org/web/20150718220435/http://qa.oms.origin.com/

INTERNET ARCHIVE
WayBackMachine

http://qa.oms.origin.com/ Go

JUN JUL AUG
2014 18 2016
2015

1 captures
18 Jul 15 - 18 Jul 15

Mandatory was here

Proof

- https://web.archive.org/http://qa.oms.origin.com/

RSAConference2016
San Francisco | February 29 – March 4 | Moscone Center

Connect to Protect

SESSION ID:

Cross-domain Sniping

Getting Flashy

#RSAC

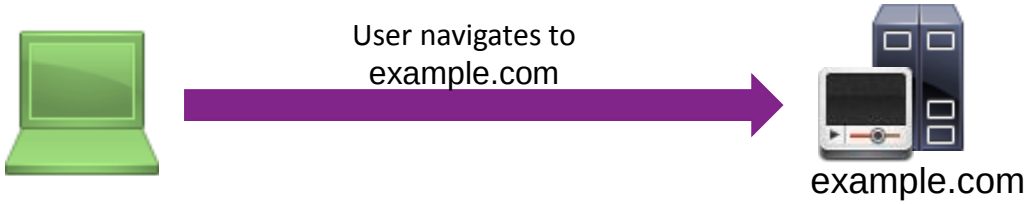
What is crossdomain.xml?

- A crossdomain.xml file specifies which sites can send requests and read response data from your site.

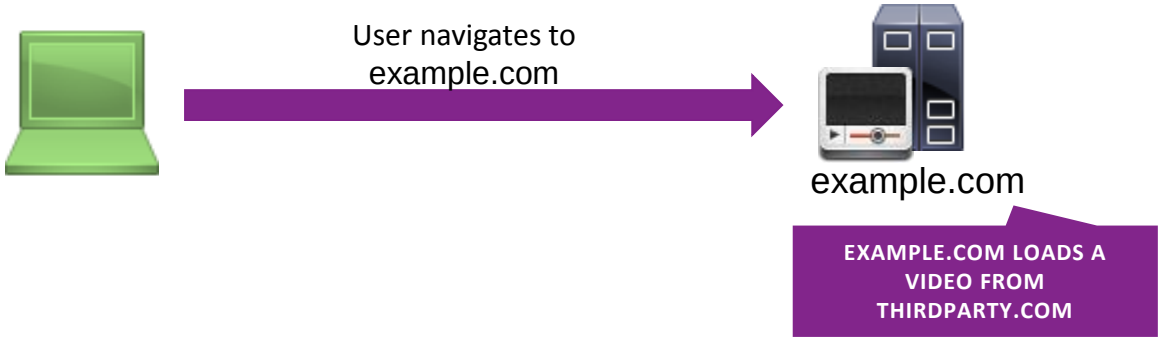
- If a site is listed in a crossdomain.xml file of a site then it can perform actions as logged in users via Flash.

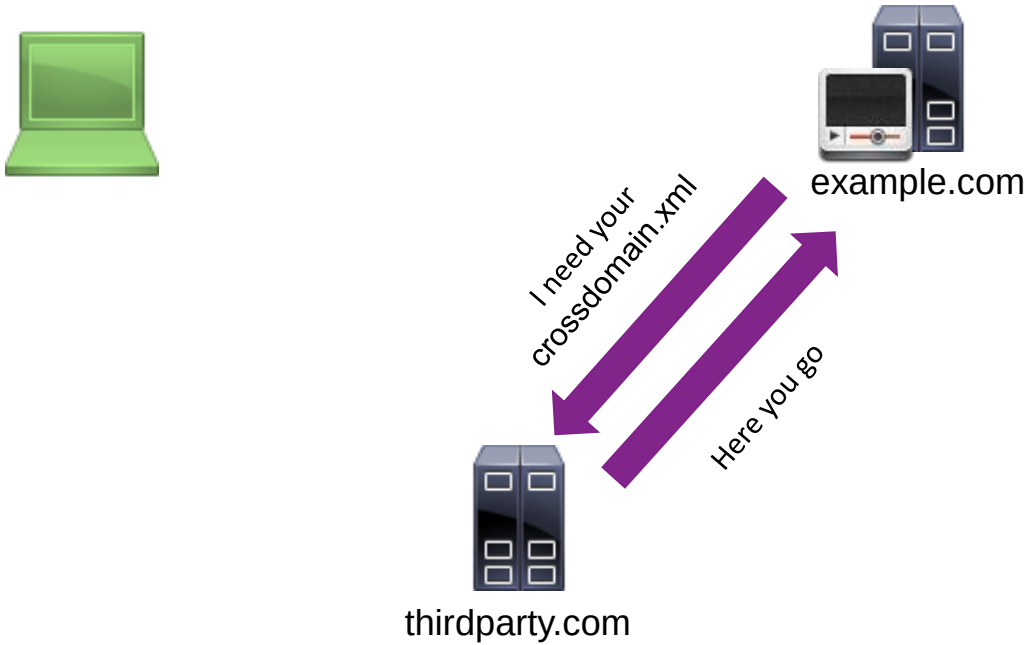
example.com

thirdparty.com


User navigates to
example.com
example.com


thirdparty.com

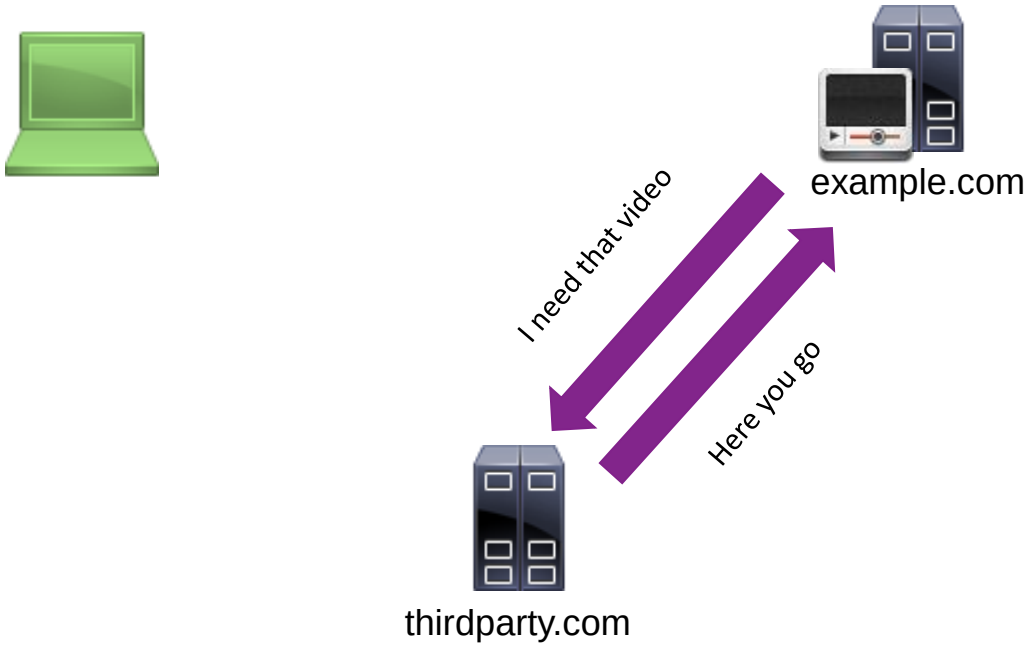

User navigates to
example.com
example.com
EXAMPLE.COM LOADS A VIDEO FROM THIRDPARTY.COM
thirdparty.com


example.com
I need your crossdomain.xml
Here you go
thirdparty.com

example.com

EXAMPLE.COM IS IN THE WHITELIST!

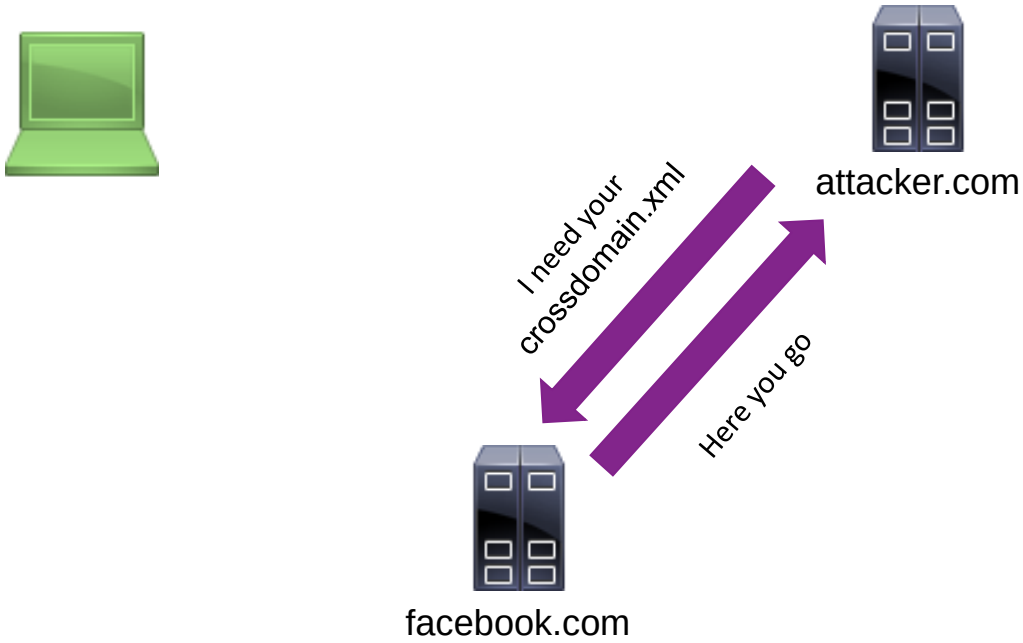
thirdparty.com


example.com
I need that video
Here you go
thirdparty.com

example.com

VIDEO STARTS PLAYING

thirdparty.com



UBER
EVERYONE'S PRIVATE DRIVER™

attacker.com

ATTACKER.COM NOT IN FACEBOOK'S WHITELIST! REQUEST BLOCKED.

facebook.com

Scanning Crossdomain.xml

- crossdomain.xml policies are commonplace.
- They are a perfect example of trusting ephemeral instances.
- If a domain is in your crossdomain.xml file then it is trusted to perform authenticated requests.

<allow-access-from domain="bscapps.cards.go.com" />
<allow-access-from domain="bscapps.disney.go.com" />
<allow-access-from domain="www.disney.go.com" />
<allow-access-from domain="ads.disney.go.com" />
<allow-access-from domain="ad.disney.go.com" />
<allow-access-from domain="Adsatt.Disney.starwave.com" />
<allow-access-from domain="*.starwave.com" />
<allow-access-from domain="*.Disney.starwave.com" />
<allow-access-from domain="*.disney.starwave.com" />
<allow-access-from domain="*.screenplayinc.com" />
<allow-access-from domain="*.totaleclips.com" />
<allow-access-from domain="cablelocator.disney.go.com" />
<allow-access-from domain="quiz.disney.go.com" />
<allow-access-from domain="studio.go.com" />
<allow-access-from domain="studio.disney.go.com" />
<allow-access-from domain="forums.go.com" />
<allow-access-from domain="tokenzone.go.com" />
<allow-access-from domain="tokenzone.disney.go.com" />
<allow-access-from domain="apsc.disney.go.com" />
<allow-access-from domain="a.disney.go.com" />
<allow-access-from domain="tv.disney.go.com" />
<allow-access-from domain="atv.disney.go.com" />
<allow-access-from domain="dcapps.disney.go.com" />
<allow-access-from domain="dcquiz.disney.go.com" />
<allow-access-from domain="scores.disney.go.com" />

Planning Our Attack

- We need to gain control over one of the domains listed in the cross-domain whitelist.

- How can this be done?

photobucket

UBER

EVERYONE'S PRIVATE DRIVER™

Photobucket Security

- Photobucket isn't new to security issues.
- Popular host for both public and private photos.
- Mobile application syncs photos from phone via app to the online service.
- Naturally, due to private photos being stored this is a big target for hackers.

TECH

The Dark Art Of "Fusking"

A hole in Photobucket's privacy has made it so that private albums can be accessed with little work. This hole has remained open for at least 5 years.

posted on Aug. 7, 2012, at 1:23 p.m.

Katie Notopoulos
BuzzFeed News Reporter

logos.wikia.com

Last Friday night, *Wired* writer Mat Honan had his Twitter and email accounts

BuzzFeed NEWS

Here Are The Top Stories

- Republican John Kasich is running for president. He's governor of Ohio, a key swing state in presidential elections.
- Burundi began voting in its disputed presidential election and Pierre Nkurunziza looks set to win a third term as president.
- Penguin Random House has provided BuzzFeed with an exclusive look at some of the original and final interior art for Dr. Seuss's new book.

Get The News App

Connect With BuzzFeed Tech

Like Us On Facebook

GAWKER

Ladies: 8,000 Creeps on Reddit Are Sharing the Nude Photos You Posted to Photobucket

Max Read
Filed to: REDDIT 8/08/12 2:45pm

880,433

EVERYONE'S PRIVATE DRIVER™

Fusker

From Wikipedia, the free encyclopedia

Fusker is a type of website or utility that extracts images from a web page, typically from free hosted galleries. Fusker software allows users to identify a sequence of images with a single pattern, for example:

```
http://www.example.com/images/pic[1-16].jpg
```

This would identify images pic1.jpg, pic2.jpg, through pic16.jpg.

When this pattern is given to a fusker website, the website would produce a page that displays all sixteen images in that range. Patterns can also contain lists of words, such as `http://www.example.com/images/{small,medium,big}.jpg`, which will produce three urls, each with one word from the bracketed list. The web page is then presented to the person who entered the fusker, and can also be saved on the fusker web server so that other people may view it.

The Fix from Photobucket

File Name Scrambling

To protect your privacy, we recommend that you select the options to scramble both future and past upload file names. However, if you intend for your photos to be public or used for business purposes, we recognize that you may not want to scramble.

For Future Uploads

- [x] (Recommended) During upload, scramble file names to make links hard to guess

For All Previous Uploads

Scramble File Names

Scrambling file names changes links.
You will need to re-establish published links once the scramble is complete.

UBER

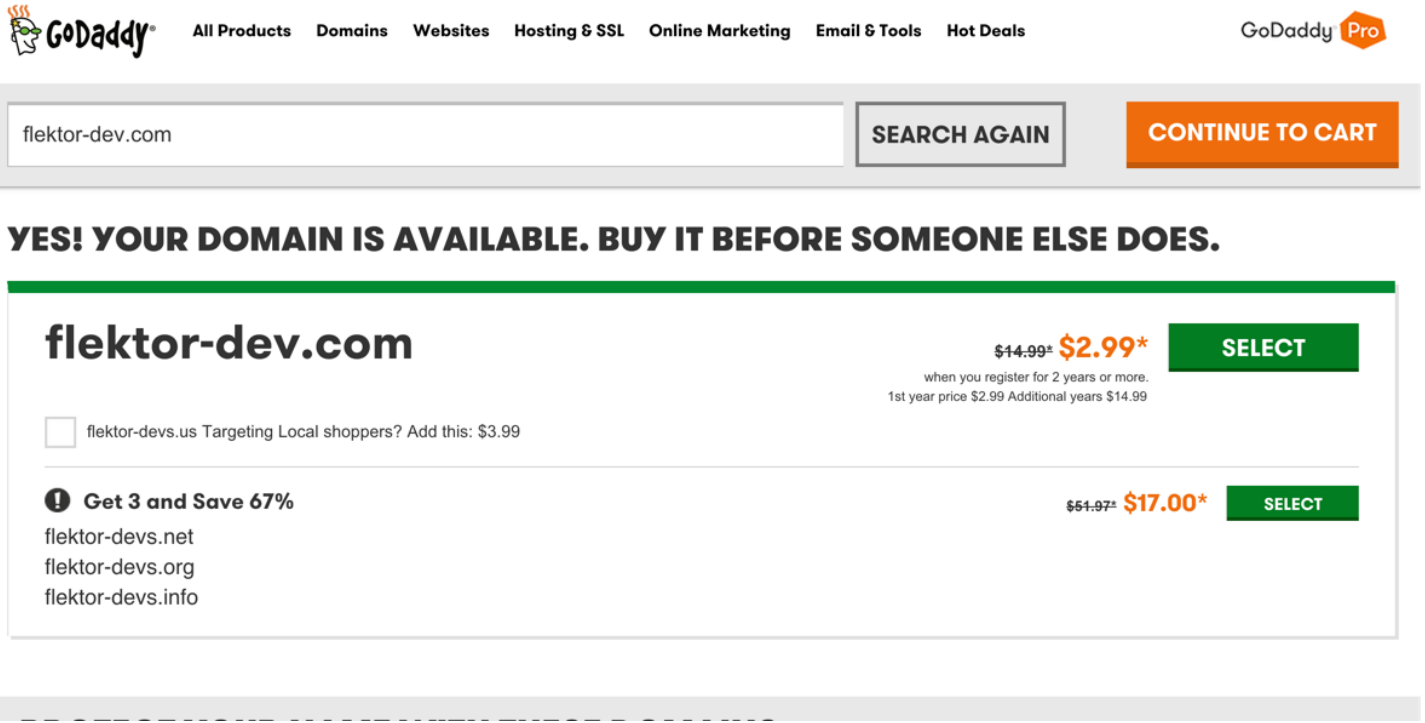
EVERYONE'S PRIVATE DRIVER™

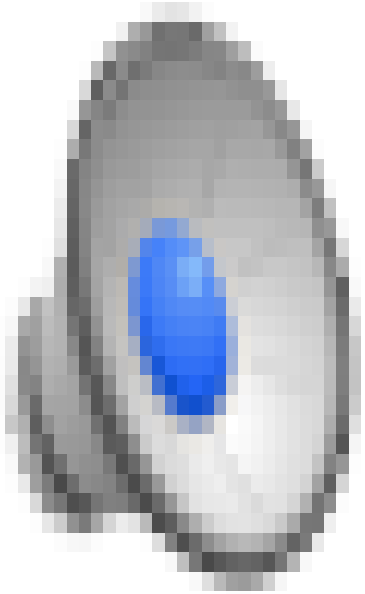
Photobucket Security

- Despite all of this added protection, we're going to bypass all of it.

```
– <cross-domain-policy>
    <site-control permitted-cross-domain-policies="all"/>
    <allow-http-request-headers-from domain="*.photobucket.com" headers="*"/>
    <allow-http-request-headers-from domain="*.pixlr.com" headers="*"/>
    <allow-access-from domain="*.photobucket.com"/>
    <allow-access-from domain="*.tinypic.com"/>
    <allow-access-from domain="*.englaze.com"/>
    <allow-access-from domain="*.englaze.net"/>
    <allow-access-from domain="*.nglaze.com"/>
    <allow-access-from domain="*.nglaze.net"/>
    <allow-access-from domain="*.flektor-dev.com"/>
    <allow-access-from domain="*.flektor-lab.com"/>
    <allow-access-from domain="*.flektor.com"/>
    <allow-access-from domain="*.flip.com"/>
    <allow-access-from domain="*.advancemags.com"/>
    <allow-access-from domain="*.dannypatterson.com"/>
    <allow-access-from domain="*.scrapblog.com"/>
    <allow-access-from domain="*.scrapblog.net"/>
    <allow-access-from domain="*.photoshop.com"/>
    <allow-access-from domain="*.adobe.com"/>
    <allow-access-from domain="*.mego.com"/>
    <allow-access-from domain="*.5glabs.com"/>
    <allow-access-from domain="*.zude.com"/>
    <allow-access-from domain="*.fotoflexer.com"/>
    <allow-access-from domain="photobkt-images.adbureau.net"/>
    <allow-access-from domain="*.pbsrc.com"/>
    <allow-access-from domain="*.pixlr.com"/>
  </cross-domain-policy>
```

```
– <cross-domain-policy>
    <site-control permitted-cross-domain-policies="all"/>
    <allow-http-request-headers-from domain="*.photobucket.com" headers="*"/>
    <allow-http-request-headers-from domain="*.pixlr.com" headers="*"/>
    <allow-access-from domain="*.photobucket.com"/>
    <allow-access-from domain="*.tinypic.com"/>
    <allow-access-from domain="*.englaze.com"/>
    <allow-access-from domain="*.englaze.net"/>
    <allow-access-from domain="*.nglaze.com"/>
    <allow-access-from domain="*.nglaze.net"/>
    <allow-access-from domain="*.flektor-dev.com"/>
    <allow-access-from domain="*.flektor-lab.com"/>
    <allow-access-from domain="*.flektor.com"/>
    <allow-access-from domain="*.flip.com"/>
    <allow-access-from domain="*.advancemags.com"/>
    <allow-access-from domain="*.dannypatterson.com"/>
    <allow-access-from domain="*.scrapblog.com"/>
    <allow-access-from domain="*.scrapblog.net"/>
    <allow-access-from domain="*.photoshop.com"/>
    <allow-access-from domain="*.adobe.com"/>
    <allow-access-from domain="*.mego.com"/>
    <allow-access-from domain="*.5glabs.com"/>
    <allow-access-from domain="*.zude.com"/>
    <allow-access-from domain="*.fotoflexer.com"/>
    <allow-access-from domain="photobkt-images.adbureau.net"/>
    <allow-access-from domain="*.pbsrc.com"/>
    <allow-access-from domain="*.pixlr.com"/>
  </cross-domain-policy>
```


GoDaddy
All Products
Domains
Websites
Hosting & SSL
Online Marketing
Email & Tools
Hot Deals
GoDaddy Pro
flektor-dev.com
SEARCH AGAIN
CONTINUE TO CART
YES! YOUR DOMAIN IS AVAILABLE. BUY IT BEFORE SOMEONE ELSE DOES.
flektor-dev.com
$14.99‡ $2.99*
SELECT
when you register for 2 years or more.
1st year price $2.99 Additional years $14.99
flektor-devs.us Targeting Local shoppers? Add this: $3.99
Get 3 and Save 67%
$51.97‡ $17.00*
SELECT
flektor-devs.net
flektor-devs.org
flektor-devs.info

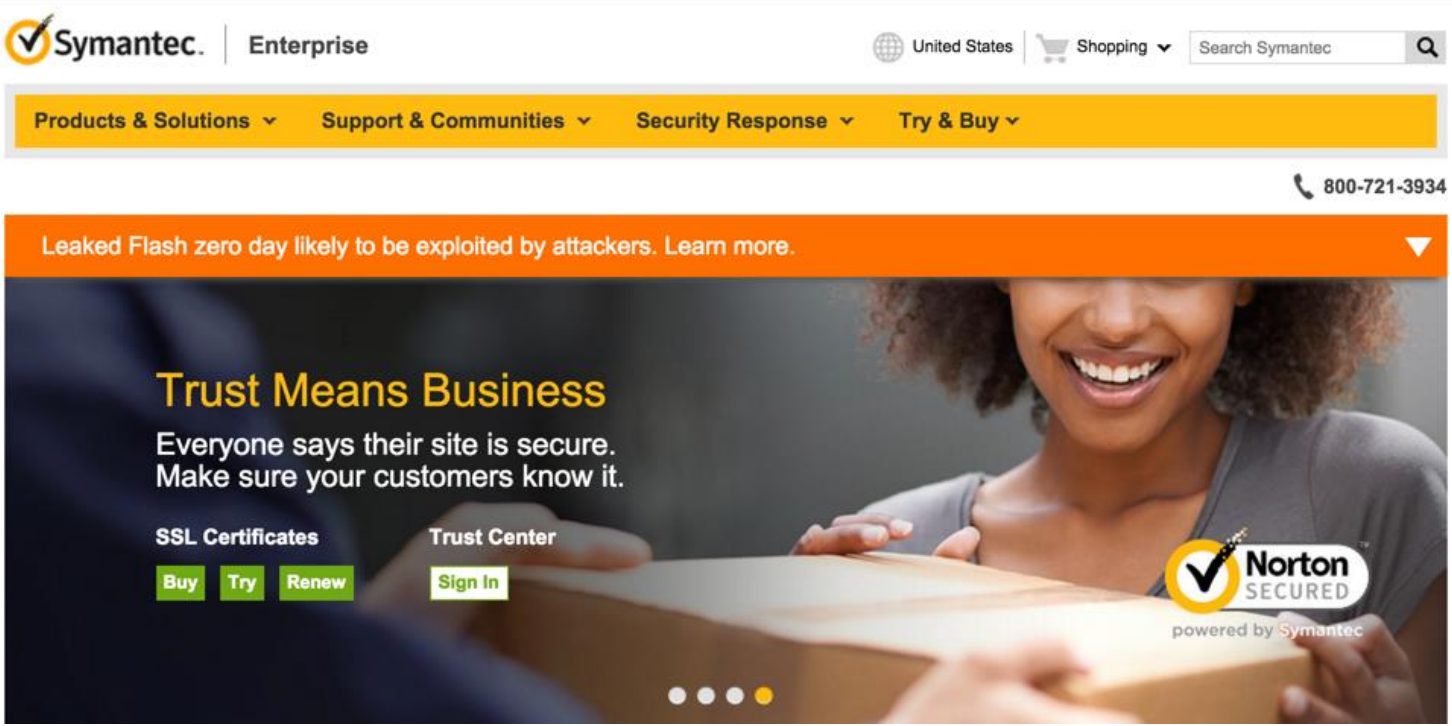


UBER

EVERYONE'S PRIVATE DRIVER™

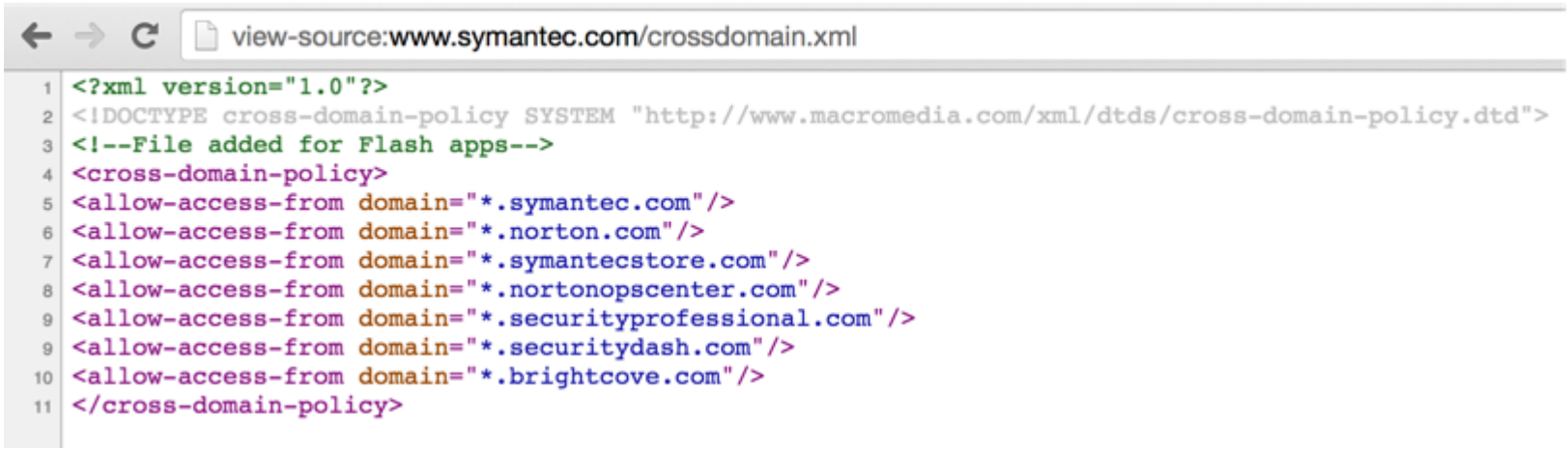
Thinking bigger

- Photobucket isn't an isolated incident.
- We scanned the Alexa top 1,000 domains and found many other instances.
- Even companies that specialize in security made the mistake of having expired domains in their crossdomain.xml.

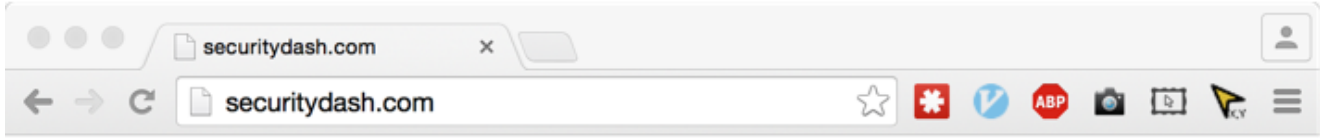


UBER

EVERYONE'S PRIVATE DRIVER™


view-source:www.symantec.com/crossdomain.xml
<?xml version="1.0"?>
<!DOCTYPE cross-domain-policy SYSTEM "http://www.macromedia.com/xml/dtds/cross-domain-policy.dtd">
<!--File added for Flash apps-->
<cross-domain-policy>
<allow-access-from domain="*.symantec.com"/>
<allow-access-from domain="*.norton.com"/>
<allow-access-from domain="*.symantecstore.com"/>
<allow-access-from domain="*.nortonopscenter.com"/>
<allow-access-from domain="*.securityprofessional.com"/>
<allow-access-from domain="*.securitydash.com"/>
<allow-access-from domain="*.brightcove.com"/>
</cross-domain-policy>


view-source:www.symantec.com/crossdomain.xml
<?xml version="1.0"?>
<!DOCTYPE cross-domain-policy SYSTEM "http://www.macromedia.com/xml/dtds/cross-domain-policy.dtd">
<!--File added for Flash apps-->
<cross-domain-policy>
<allow-access-from domain="*.symantec.com"/>
<allow-access-from domain="*.norton.com"/>
<allow-access-from domain="*.symantecstore.com"/>
<allow-access-from domain="*.securityprofessional.com"/>
<allow-access-from domain="*.brightcove.com"/>
</cross-domain-policy>



UBER

EVERYONE'S PRIVATE DRIVER™

RSA Conference 2016
San Francisco | February 29 – March 4 | Moscone Center

Connect to Protect

SESSION ID:

The Front Page of Time

Get With the Times

Third-party Web Resources

- A majority of sites include web resources from third-party domains.
- You have popular sites loading CSS, JavaScript, images, Flash, and other resources from CDNs and third party providers.
- When these domains expire it’s often a silent failure.

Yet Another Scanner

- We built a scanner to check if any external resources included on the front pages of the Alexa Top 10,000 had expired.
- It was meant to be a quick test to prove the idea, only the homepage was checked.
- Future tests would include spidering entire sites to find expired external resources.

UBER

EVERYONE'S PRIVATE DRIVER™

Oops!

- The scanner flagged Time.com as containing an expired domain name in an external resource.

<noscript>

<img height="1" width="1" alt="" style="display:none"
src="https://wwwhpacebook.com/tr?id=345214065653621&
amp;ev=PixelInitialized"/>

</noscript>

Tracking Time Users for 10$

- Domain is free to be registered.
- This image is loaded when the user's browser has JavaScript disabled.
- HTML is on every Time.com news article.

What can we do with this?

- Track users without JavaScript as they navigate the site.
- Spawn 401 basic authentication prompts to phish credentials from users.
- X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*

- We collected **267,377** requests before pointing the domain to **127.0.0.1**.
- **74,083** had the Do Not Track header set.
- Multiple bots tracking the Time's homepage

Going Forward

- While this expired external resource was not active content (an image inside of a noscript tag), it still allowed a variety of abuses.

- Given a script tag or external style sheet, we could deface the page and carry out more complex attacks.

RSA Conference2016
San Francisco | February 29 – March 4 | Moscone Center

Connect to Protect

SESSION ID:

The NoScript Misnomer

Many Eyes Make All Bugs Shallow

- NoScript is a popular Firefox add-on with >2 million users.

- Blocks all JavaScript, Flash, and Java unless the user explicitly allows it.

- Advertised as “The best security you can get in a web browser!”

SECURITY

Why Edward Snowden gave a shoutout to the NoScript add-on for Firefox

JORDAN NOVET, TOM CHERADAR MARCH 10, 2014 12:23 PM

TAGS: EDWARD SNOWDEN, INFORMACTION, MOZILLA CORPORATION, MOZILLA FOUNDATION, NOSCRIPT, SECURITY, TOP-STORIES

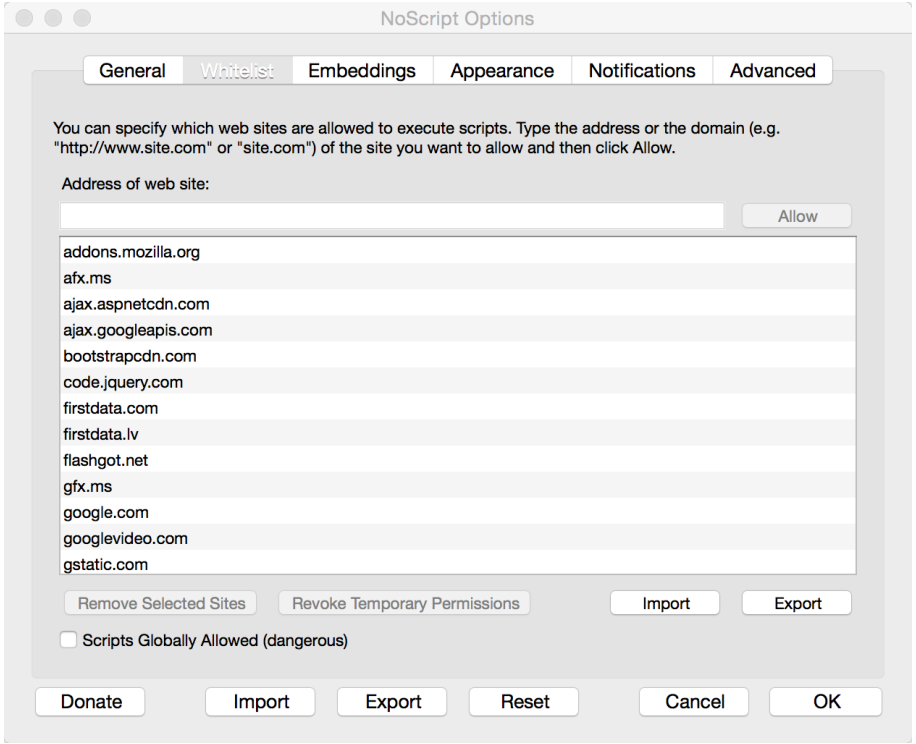
Why is this helpful?

- NoScript protects you from many 0days by blocking active content.

- Forces consent into the browsing process.

The NoScript Misnomer

- NoScript is a misleading title however as the add-on ships with an internal whitelist of domains.
- At the time of this presentation creation, there are currently 111 entries in NoScript's default whitelist.
- All of these sites can bypass the functionality provided by the add-on because they are trusted.


NoScript Options
General
Whitelist
Embeddings
Appearance
Notifications
Advanced
You can specify which web sites are allowed to execute scripts. Type the address or the domain (e.g. "http://www.site.com" or "site.com") of the site you want to allow and then click Allow.
Address of web site:
Allow
addons.mozilla.org
afx.ms
ajax.aspnetcdn.com
ajax.googleapis.com
bootstrapcdn.com
code.jquery.com
firstdata.com
firstdata.lv
flashgot.net
gfx.ms
google.com
googlevideo.com
gstatic.com
Remove Selected Sites
Revoke Temporary Permissions
Import
Export
Scripts Globally Allowed (dangerous)
Donate
Import
Export
Reset
Cancel
OK

Bypassing NoScript

- The original strategy was to find a way to store arbitrary JavaScript on one of the whitelisted sites.
- However, the journey was cut short when one of the domains in the default whitelist returned an NXDOMAIN upon querying its DNS.
- The domain: vjs.zendcdn.net

DNS Enumeration

mandatory> dig NS **zendcdn.net**

; <<>> DiG 9.8.3-P1 <<>> NS zendcdn.net

;; global options: +cmd

;; Got answer:

;; ->>HEADER<<- opcode: QUERY, status: **NXDOMAIN**, id: 21164

;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 0

✓ zendcdn.net

This domain is available!

$10.69/year

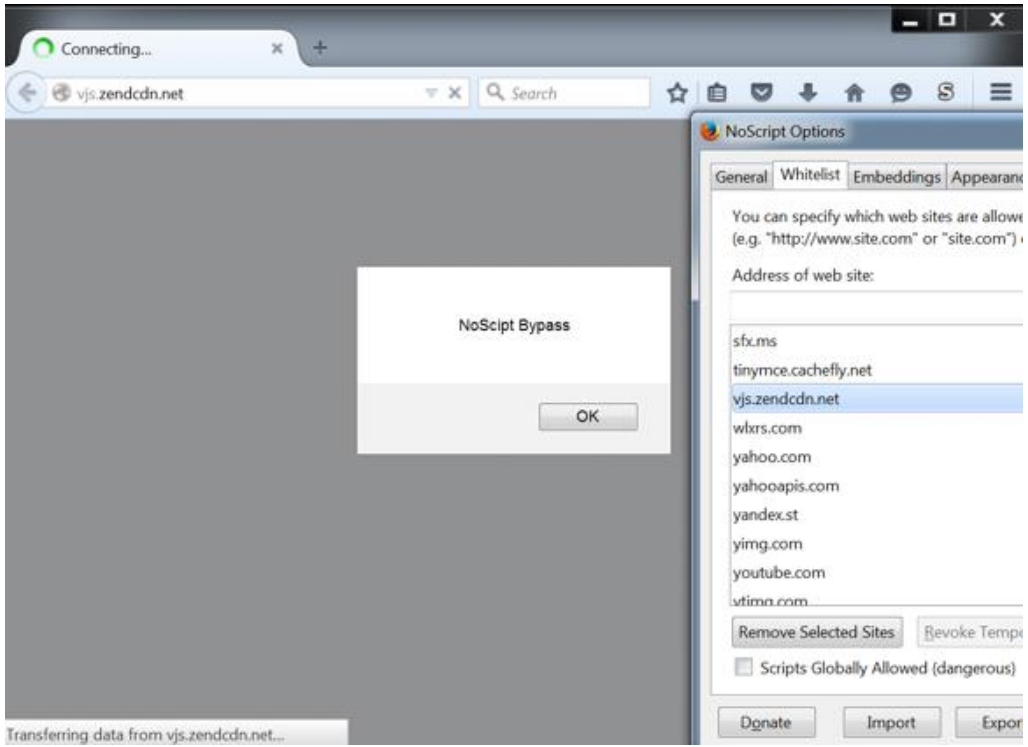
zendcdn.net Bulk Options Search

Search Results

Popular | New | International | Prime | Favorites

Filter extensions

zendcdn.net $10.69/year



UBER
EVERYONE'S PRIVATE DRIVER™

Remediation

- This issue was disclosed to the creator of NoScript and was fixed in hours.
- The update was available two days later.

RSA Conference2016
San Francisco | February 29 – March 4 | Moscone Center

Connect to Protect

SESSION ID:

Solving the Problem

Pain is Temporary, Glory is Eternal

What we do to fix this?

- Change policies to include steps for ensuring the removal of DNS records and other references to dynamic instances.

- Monitor not only your own domain names, but domain names that you trust, as well.
  - Domains in crossdomain.xml
  - Domains in CNAME records
  - Domains in third-party script includes

Tools

- To find these vulnerabilities, we've created a few tools.

- Using the same tools we use to hunt for these vulnerabilities, you can scan for these problems in your own infrastructure.

Tools

- Crossdomain.xml Scanning Tool
  - https://github.com/mandatoryprogrammer/xpire-crossdomain-scanner
- XCNAME
  - https://github.com/mandatoryprogrammer/xcname

Thank you

- Questions?

Sources

- https://commons.wikimedia.org/wiki/File:Robot-icon.png
- https://openclipart.org/detail/18414/weather-symbols
- https://www.microsoft.com/en-us/download/details.aspx?id=35772
- http://www.abc.net.au/news/2014-12-19/an-over-populated-chinese-swimming-pool/5978934
- http://www.havana-live.com/news/2015/02/01/havana-host-ernest-hemingway-marling-fishing-tournament.html
- https://cierralyn.wordpress.com/2010/08/10/italy-part-2-volterra-rome-cinque-terra-deep-sea-fishing-and-a-bit-more-of-florence/for-blog-64/