



TWIST & SHOUT

FERRIS BUELLERS

GUIDE TO ABUSE

DOMAIN PERMUTATIONS

Presented by Rob Ragan & Kelly Albrink

BISHOPFOX



WHAT IS THIS TALK ABOUT

Types of abuse domain permutations

Why domain abuse happens

Monitoring & Defense techniques

COMMON ATTACK TARGETS
WHO IS BEING
TARGETED



YAHOO!



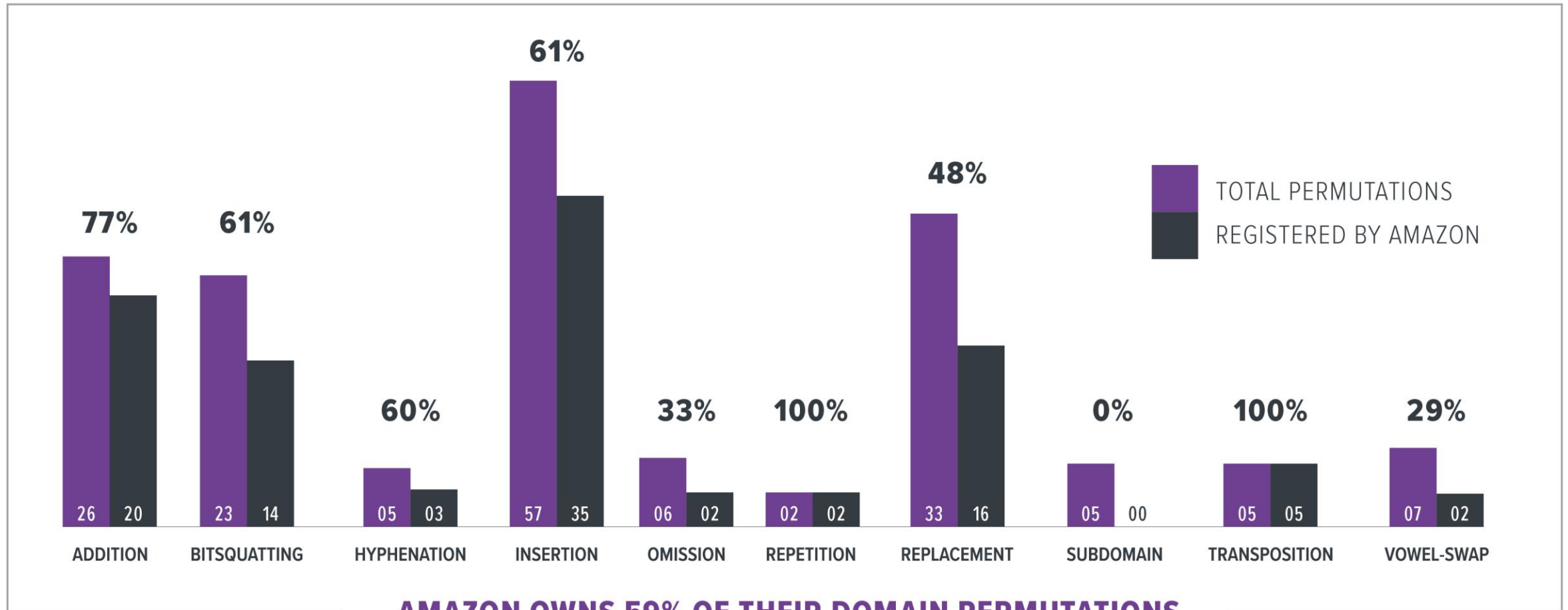
COMCAST



```
https://institutions-api.lix.com
https://oaypal.com
http://aboutus.le.com
https://aboutus.le.com
http://mx.payral.com
https://xn--fcebok-z0c.com
https://pwl-steve.art.com
http://chuang.le.com
http://facebpok.com
https://chuang.le.com
http://ffacebook.com
http://eaextranet.itt.com
https://eaextranet.itt.com
http://dev.cpq.adt.com
http://www.aamazon.com
https://dev.cpq.adt.com
http://pzypal.com
https://sft-ap-2.pgw.st.com
http://paypa1l.com
http://paypaal.com
http://ypal.com
http://pa-ypal.com
http://maypal.com
http://facedbook.com
http://cirs.ahu.edu.cn.q0ogle.com
https://facxebook.com
http://xn--yaho-tqa.com
http://yaghoo.com
http://2019.azon.com
:[]
```

↵

OWNED PERCENTAGE OF DOMAIN PERMUTATIONS



AMAZON OWNS 59% OF THEIR DOMAIN PERMUTATIONS



01



TYPES OF DOMAIN ABUSE



TYPES OF ABUSE

DOMAIN **PERMUTATIONS**

TYPO SQUATTING

HOMOGLYPHS

BIT SQUATTING

ADDITIONS, INSERTIONS, DELETIONS

(TLD) VARIATIONS

SUBDOMAIN PERMUTATIONS



DOMAIN PERMUTATION TYPOSQUATTING

DEFINITION

Registering a version of the targeted domain that is likely to be mistyped

AKA URL Hijacking

EXAMPLE

www.facebook.com
www.facebpok.com
www.facenook.com



DOMAIN PERMUTATION TYPOSQUATTING

DEFINITION

Registering a version of the targeted domain that is likely to be mistyped

AKA URL Hijacking

EXAMPLE

~	!	@	#	\$	%	^	&	*	()	-	+	←	
	1	2	3	4	5	6	7	8	9	0	=		Backspace	
Tab	Q	W	E	R	T	Y	U	I	O	P	}			
Caps Lock	A	S	D	F	G	H	J	K	L	;	'	*	Enter	
Shift		Z	X	C	V	B	N	M	<	>	?	/	Shift	
Ctrl	Win Key	Alt									Alt	Win Key	Menu	Ctrl

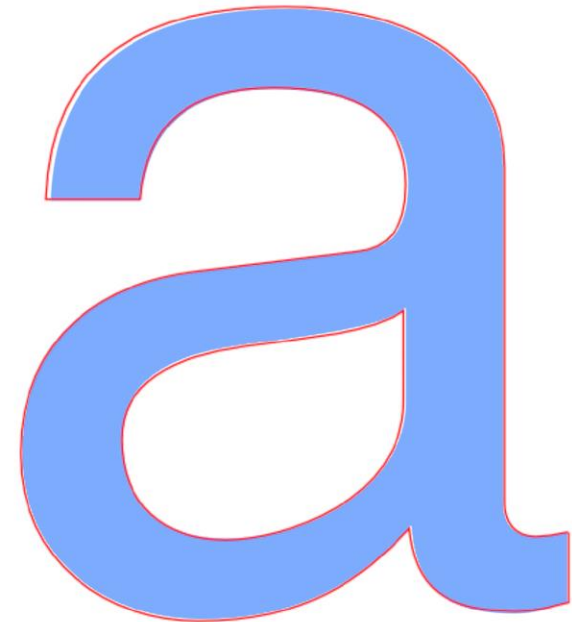
DOMAIN PERMUTATION HOMOGLYPHS

Characters that appear the same
or similar to other characters

EXAMPLES

<http://facebook.com/login.html>

a LATIN SMALL LETTER A	ɑ LATIN SMALL LETTER ALPHA	α GREEK SMALL LETTER ALPHA	а CYRILLIC SMALL LETTER A	ⱥ APL FUNCTIONAL SYMBOL ALPHA	Ⓐ MATHEMATICAL BOLD SMALL A	Ⓐ MATHEMATICAL ITALIC SMALL A	Ⓐ MATHEMATICAL BOLD ITALIC SMALL A
b LATIN SMALL LETTER B	Ḃ LATIN CAPITAL LETTER TONE SIX SIX	Б CYRILLIC CAPITAL LETTER SOFT SIGN	ᄢ CHEROKEE LETTER SI	ᑲ CANADIAN SYLLABICS AIVILIK B	Ⓑ MATHEMATICAL BOLD SMALL B	Ⓑ MATHEMATICAL ITALIC SMALL B	Ⓑ MATHEMATICAL BOLD ITALIC SMALL B
С LATIN SMALL LETTER C	Ϛ GREEK LUNATE SIGMA SYMBOL	С CYRILLIC SMALL LETTER ES	С LATIN LETTER SMALL CAPITAL C	С SMALL ROMAN NUMERAL ONE HUNDRED	Ⓒ DESERET SMALL LETTER CHEE	Ⓒ MATHEMATICAL BOLD SMALL C	Ⓒ MATHEMATICAL ITALIC SMALL C



■ U+0061 LATIN SMALL LETTER A

□ U+0430 CYRILLIC SMALL LETTER A

Both glyphs are set in Helvetica LT Std Roman at identical weight, size, & baseline.

DOMAIN PERMUTATION BIT SQUATTING

The binary representation of the character is changed due to a change of a 0 to a 1 or a 1 to a 0 typically due to hardware failure

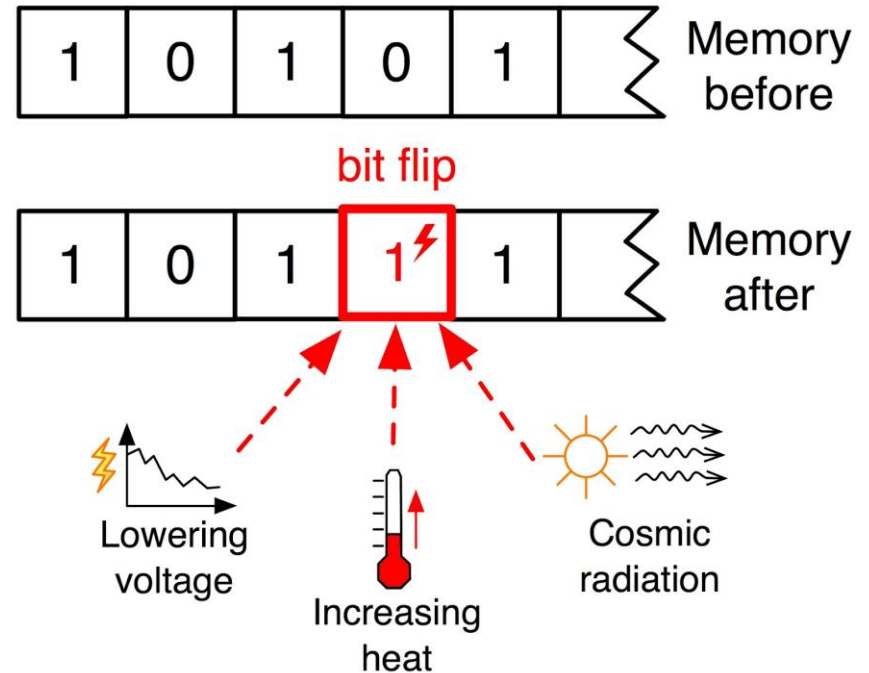
MACHINE ATTACK

Not likely to be mistyped

Not meant to target human error

Memory or storage failure

01100011	01101110	01101110	01011110	01100011	01101111	01101101
c	n	n	.	c	o	m
01100011	01101111	01101110	01011110	01100011	01101111	01101101
c	o	n	.	c	o	m



DOMAIN PERMUTATION BIT SQUATTING

The binary representation of the character is changed due to a change of a 0 to a 1 or a 1 to a 0 typically due to hardware failure

MACHINE ATTACK

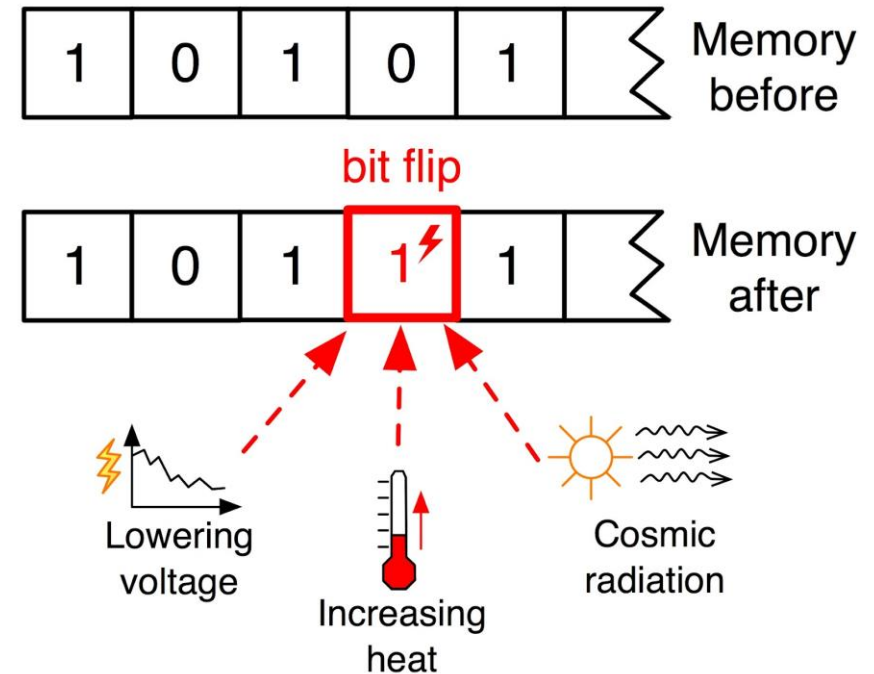
Not likely to be mistyped

Not meant to target human error

Memory or storage failure

INTERCEPT SENSITIVE TRAFFIC

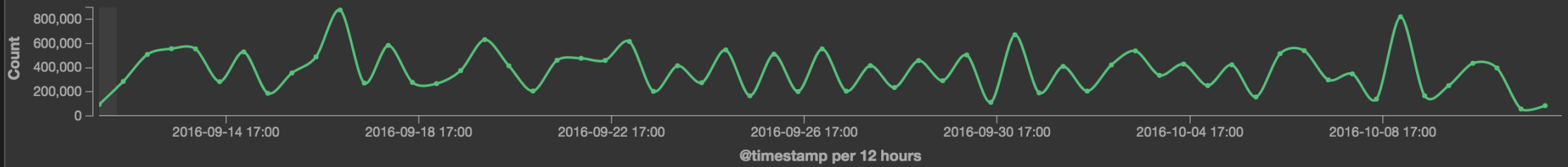
Free SSL certificates make it easier for an attacker to receive sensitive data intended for the original domain



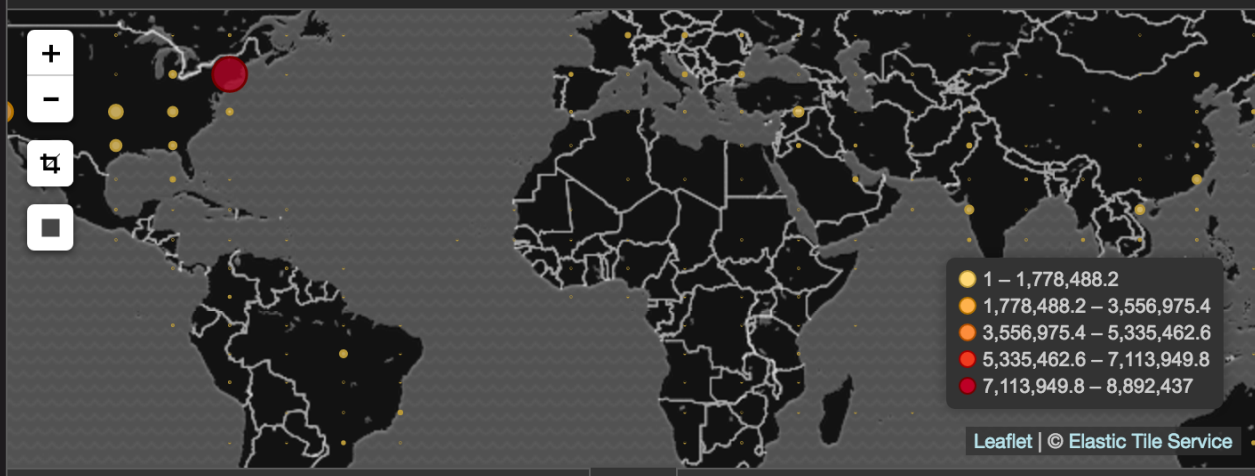
DNS Queries

🔍 📄 📁 🔗 ⊕ ⚙️

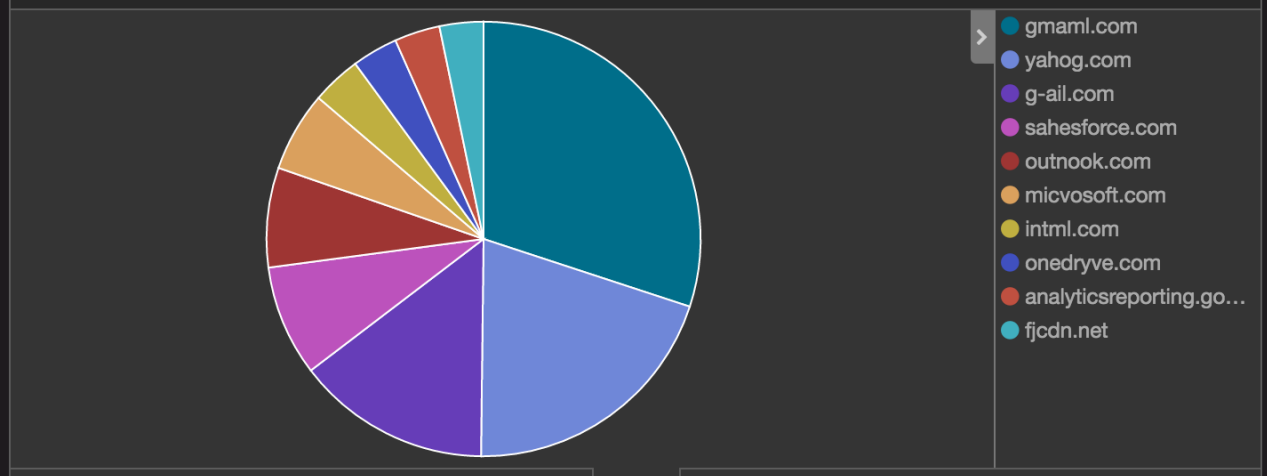
DNS Queries over Time



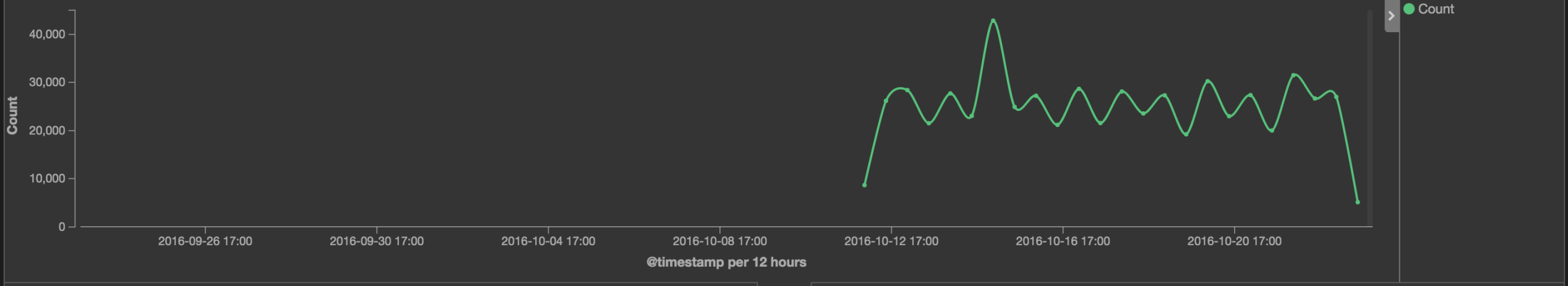
DNS Queries over Location



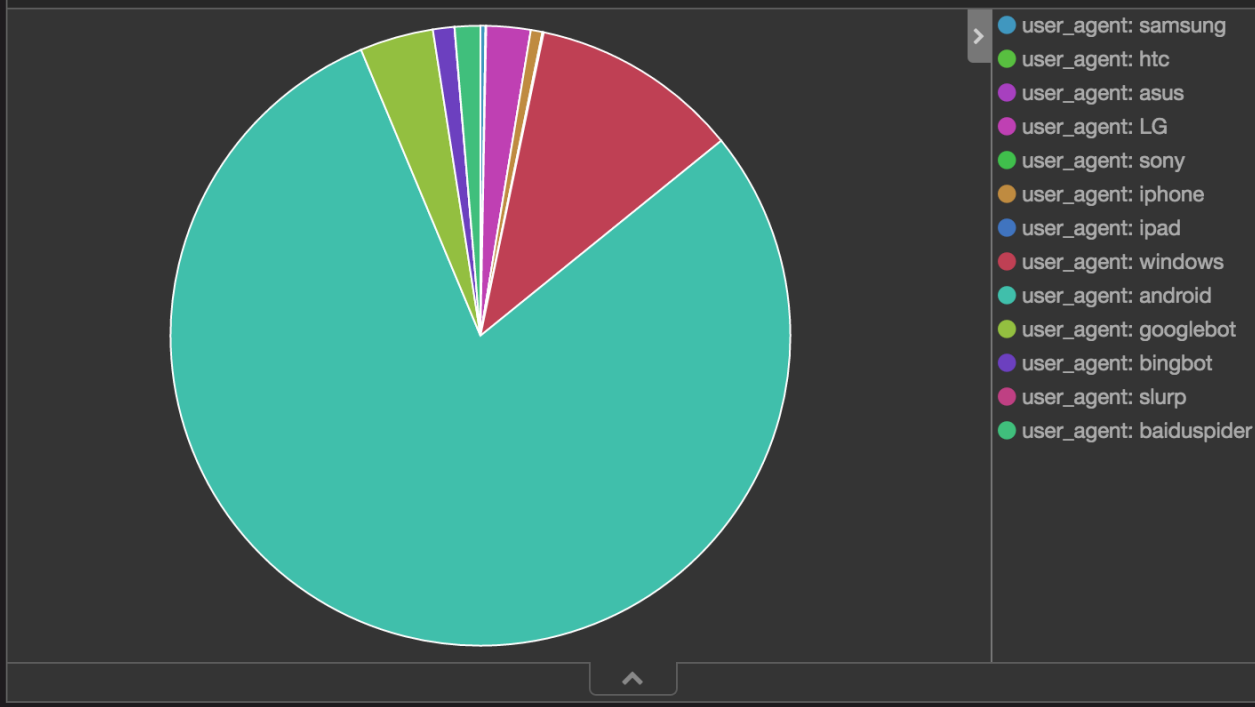
DNS Queries Top Domains



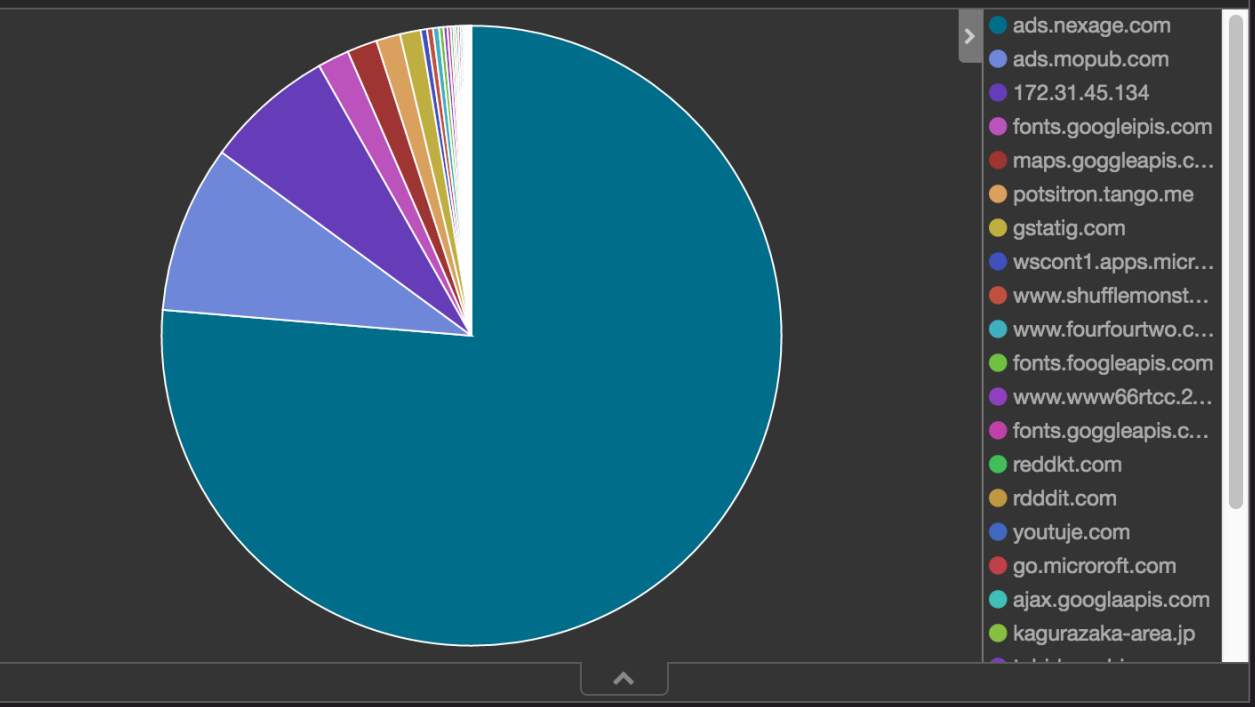
HTTP Over Time



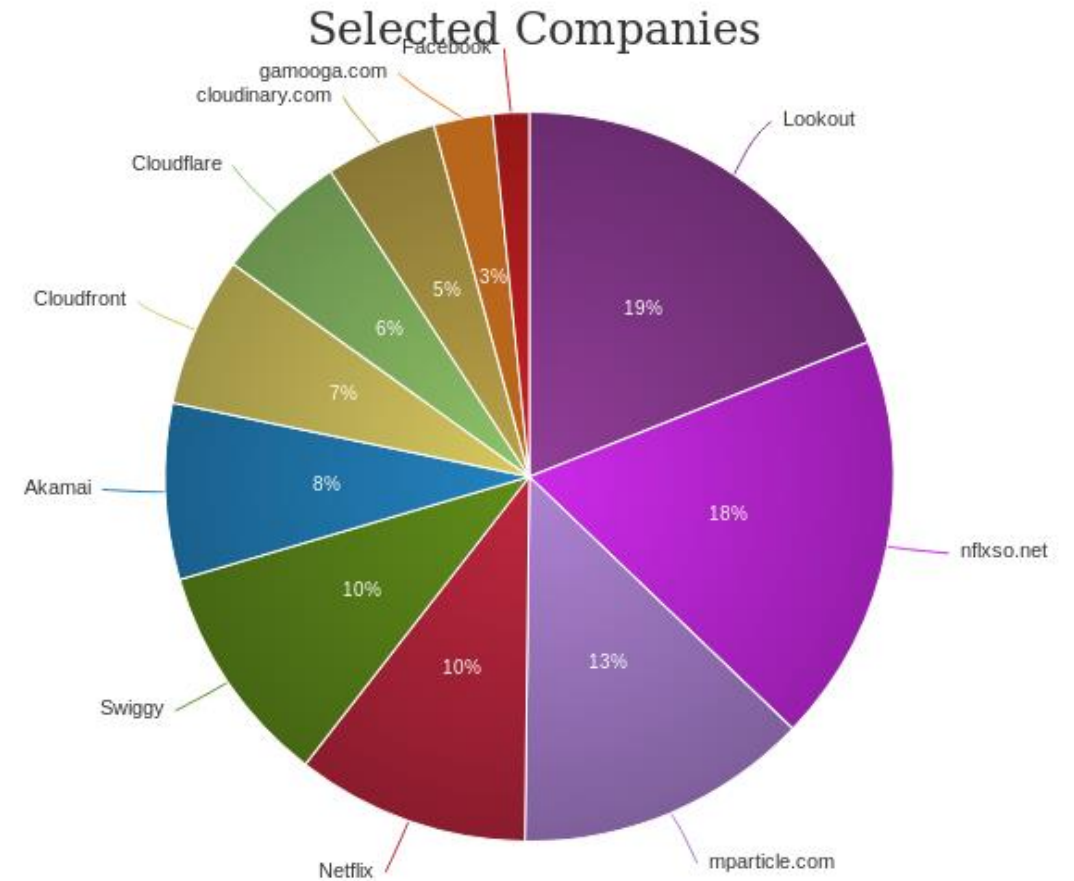
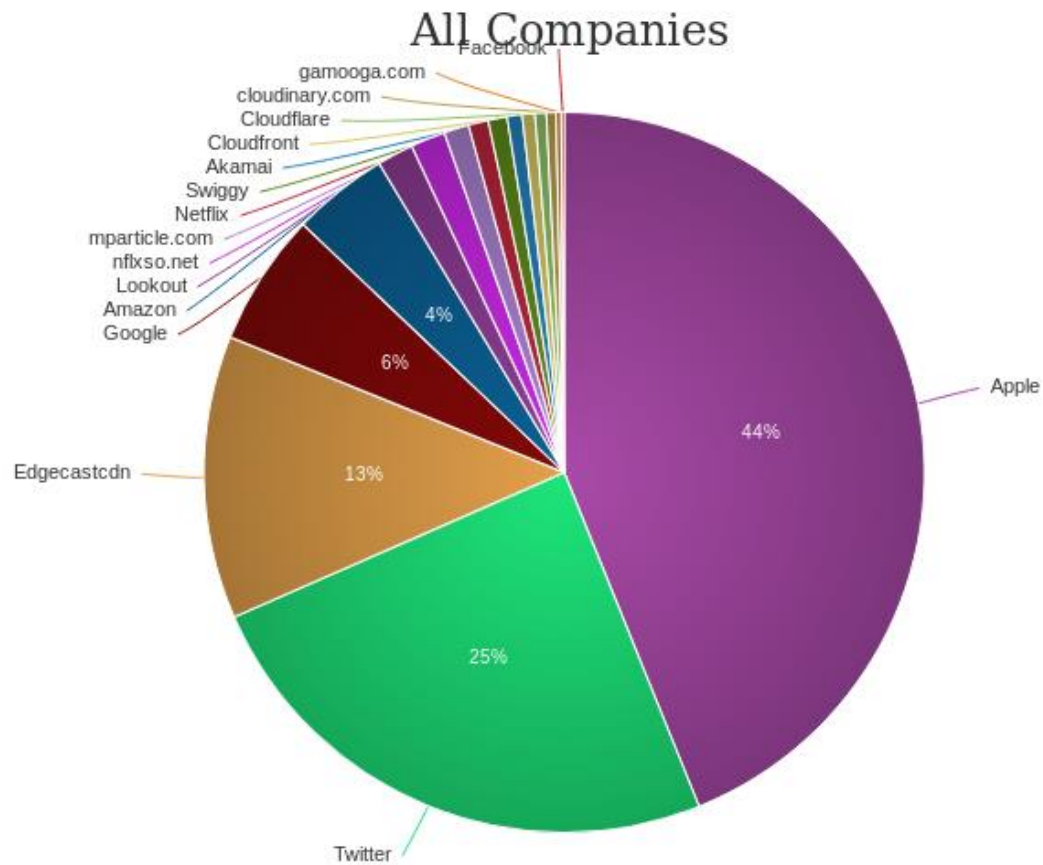
User Agents Breakdown



HTTP Queries Top Hosts



DOMAIN PERMUTATION BIT SQUATTING



DOMAIN ABUSE

TLD VARIATIONS

DEFINITION

Registering a domain with the same domain name as a targeted site, but with a different top level domain (TLD)

EXAMPLES

quickencustomersupport.us

www.amazon.co.jp.amazono-jp.ga

amazon.it

amazon.us

goo.gl





DOMAIN ABUSE SUBDOMAIN PERMUTATIONS

DEFINITION

Appending a target company name as a subdomain to an attack domain

EXAMPLES

*.ealthcare.com

facebook.verification.info

secure.runescape.com-try.top



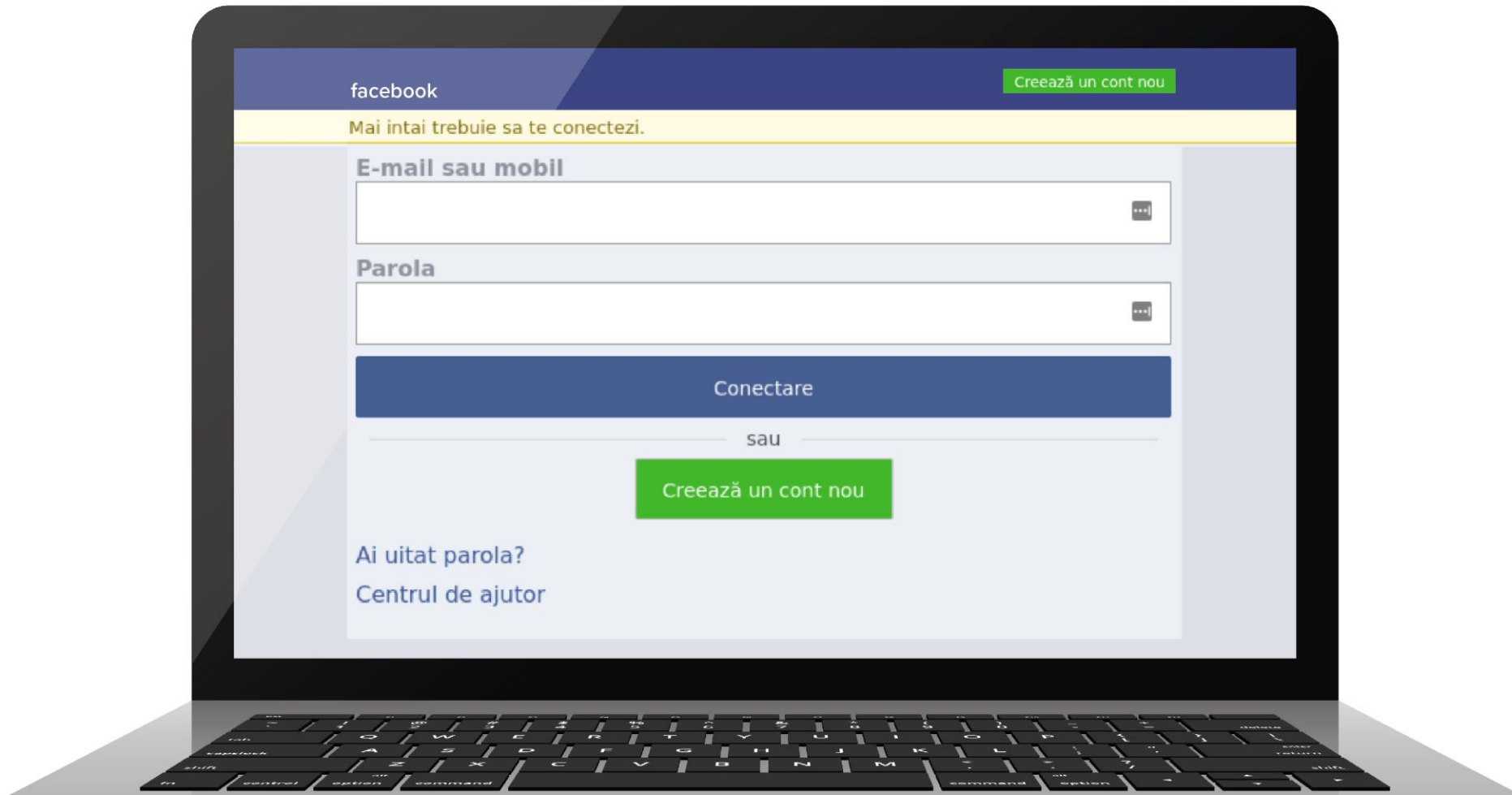
02



TYPES OF **ATTACKS**

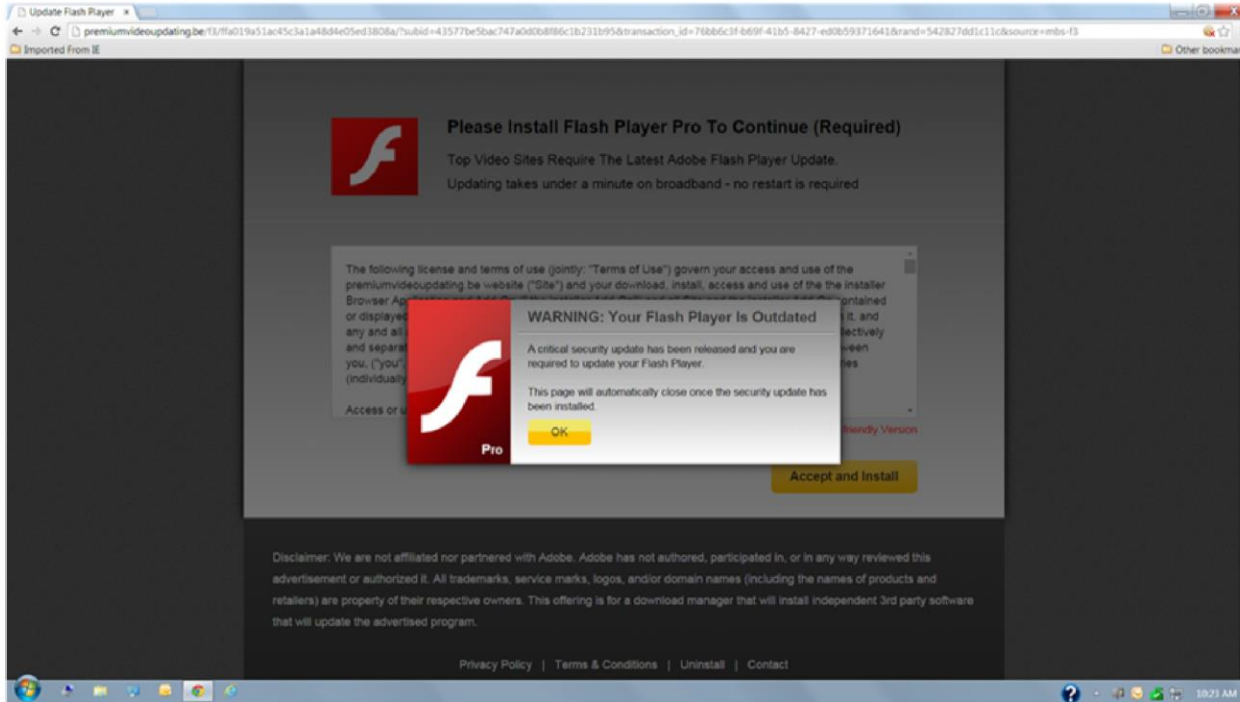
TYPE OF ATTACK PHISHING

<http://facebook.com/login.html>



TYPE OF ATTACK

MALWARE



ADOBE ACROBAT



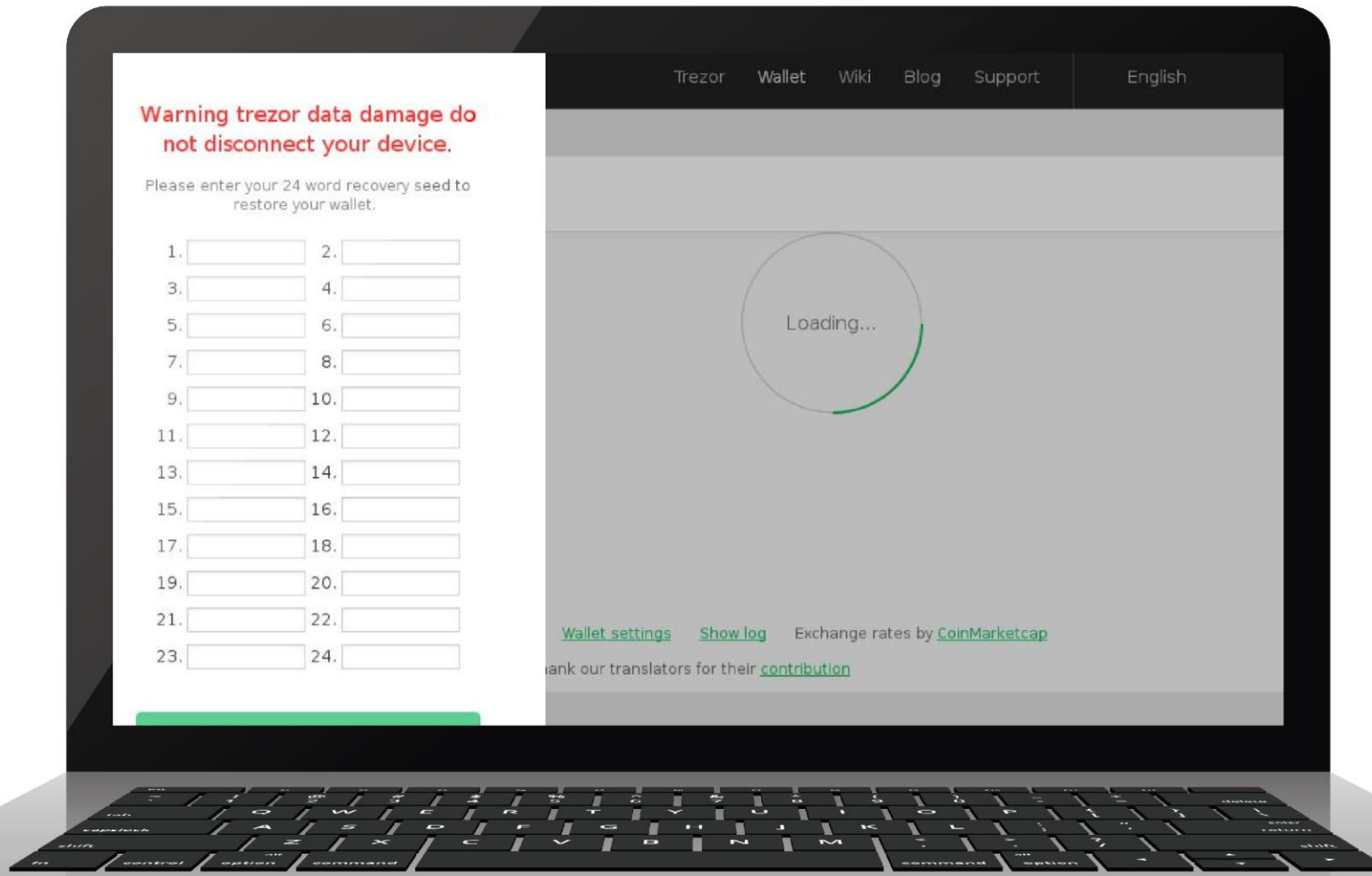
CHROME EXTENSIONS

TYPE OF ATTACK

FRAUD



Trezor.io vs. wallets-trezor.org



REAL VS MALICIOUS FOX WHITE SUPREMACY



Foxnews.com vs. Foxnews.cc



The screenshot shows the Fox News website homepage. At the top, there is a navigation bar with categories like U.S., World, Opinion, Politics, Entertainment, Business, Lifestyle, TV, Fox Nation, Radio, and More. Below this, there are links for 'Hot Topics' (Gun law uproar, Us-North Korea Summit, 'The View' erupts) and 'Markets' (SP500, I:COMP, I:DJII, More). The main content area features a large video player with a 'NOW' indicator and the title 'The Story with Martha MacCallum'. Below this, there are 'Exclusive Clips' with thumbnails for 'SPECIAL REPORT Three Republicans signal they'll join with Dems opposing national emergency' and 'SPECIAL REPORT Drumpf and Kim Jong Un to hold high-stakes talks in Vietnam'. The central headline reads 'BORDER FIGHT Dem-led House rejects emergency declaration, setting up potential veto showdown'. Below the headline, there are two sub-headlines: 'Crowd of 4 holds pro-Drumpf, pro-wall 'rally' in San Francisco' and 'New York, California, 14 other states sue Drumpf in 9th Circuit over emergency declaration'. To the right, there is a promotional box for 'THE MICHAEL COHEN HEARING TOMORROW 10AM ET'. At the bottom right, there is a 'FOX NATION Join Now' button.

Waiting for ads.yahoo.com...

The screenshot shows the Foxnews.cc website. At the top, there is a red banner with the text 'WHITETRASH.COM'. Below this, there is a video player showing a person holding a camera. Below the video, there is text that reads: 'coming real soon, we are out shooting...maybe even you we are still flag working on the site...some of you saw it in it's infancy, don't fret...it's close i want to remind you, we will need female models once our gear is ready...interested?? contact below'. At the bottom, there is a red banner with the text 'CONTACT'.

EXAMPLE

I-CLOUD ACCOUNT

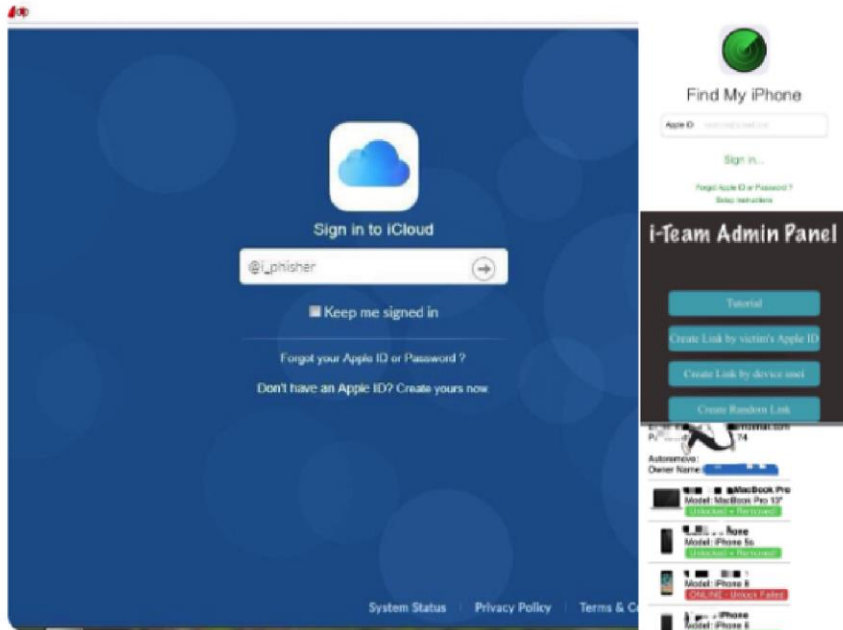


i-Team
@i_phisher

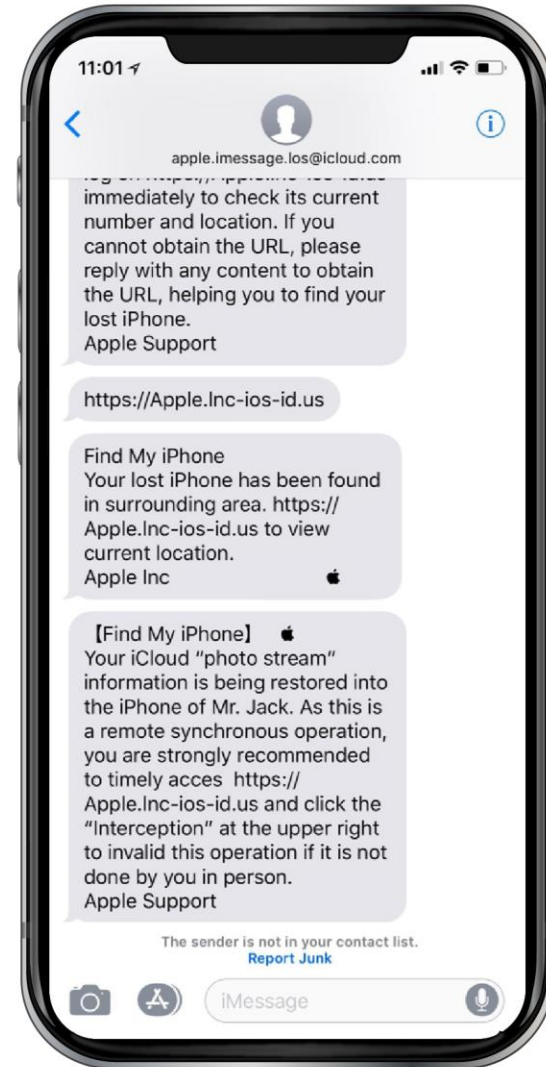
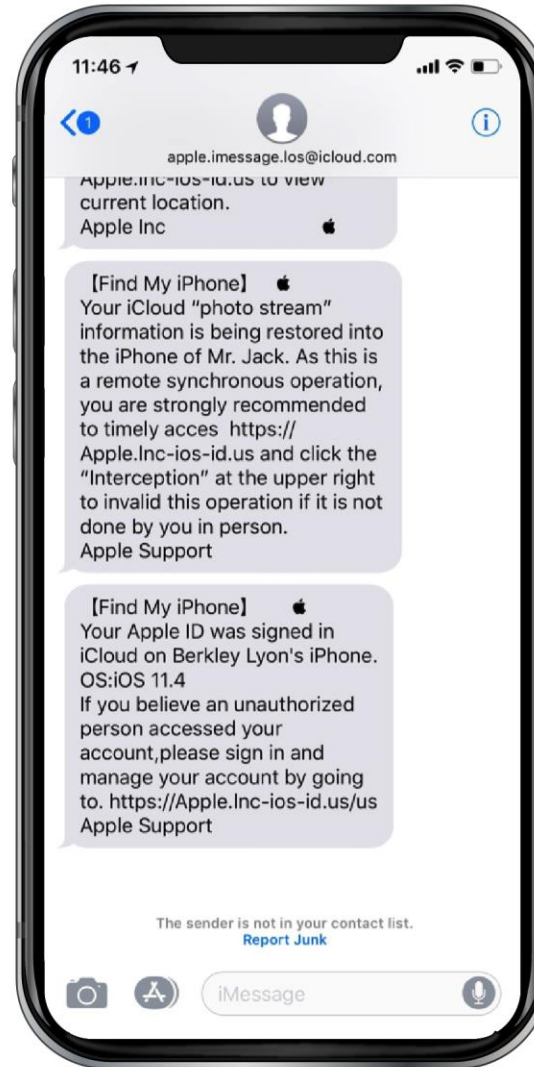
Follow

3 Best Ready to use servers for Fresh devices are available today.

If domain suspends within 3 month, you will always get new instant



12:09 AM - 30 May 2018



EXAMPLE
FUNNY OUTCOME

http://vveilsfargo.com

I love LBL!

**This website is not affiliated with Wellsfargo.com and
and is only for those idiots that have mistakenly typed
the website or have some how come across this link
that was incorrectly spelled!**

03



MONITORING & DEFENSES



MONITORING

STEP 01

GENERATE COMPREHENSIVE LISTS OF

POSSIBLE DOMAINS

dnstwist

by Marcin Ulikowski (elceef)

```
dnstwist 1.02b by <marcin@ulikowski.pl>
```

```
usage: ./dnstwist.py [OPTION]... DOMAIN
```

```
Find similar-looking domain names that adversaries can use to attack,
detect typosquatters, phishing attacks, fraud and corporate espionage
as an additional source of targeted threat intelligence.
```

```
positional arguments:
```

```
domain                domain name or URL to check
```

```
optional arguments:
```

```
-h, --help            show this help message and exit
-c, --csv             print output in CSV format
-j, --json           print output in JSON format
-r, --registered     show only registered domain names
-w, --whois          perform lookup for WHOIS creation/update time
-g, --geoip          perform lookup for GeoIP location
-b, --banners        determine HTTP and SMTP service banners
-s, --ssdeep         fetch web pages and compare their fuzzy hashes
                    evaluate similarity
-m, --mxcheck        check if MX host can be used to intercept email
-d FILE, --dictionary FILE
                    generate additional domains using dictionary
-t NUMBER, --threads NUMBER
                    start specified NUMBER of threads (default: 1)
elceef@osiris:~/dnstwist$
```

```
root@1s:~/tools/dnstwist# python dnstwist.py square.com
```

A close-up, high-angle shot of a young man with dark hair and a light beard, lying on his back on a bed. He is wearing a white t-shirt and white shorts. His eyes are wide open, and his mouth is slightly agape, giving him a surprised or concerned expression. The background is a plain, light-colored wall. The text "STEP 02" is overlaid on the right side of the image in a white, serif font.

STEP 02

Sign in

Phish Finder

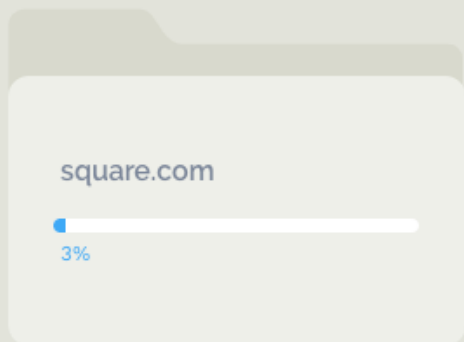
Find phishing
campaigns **before**
they find you!

 [Sign Up Now](#)



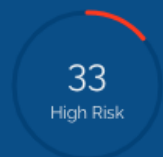
We're scanning your domain

Grab some coffee and take a load off while we scan your domain



Suspicious Domains

239 SUSPICIOUS DOMAINS DISCOVERED












BREAKDOWN OF SUSPICIOUS DOMAINS



- 22% - Hosts a website
- 78% - Can send/recieve emails
- 63% - Registered
- 0% - Known malicious

Domain	Score ▾	Can Send/Receive Emails	Hosts Website	Known Malicious	Registered
square.no	<u>100</u>	ⓘ	ⓘ		
squarerecovery.com	<u>100</u>	ⓘ			2 months ago
squarepayments.com	<u>100</u>				2 years ago
squarehr.com	<u>100</u>	ⓘ	ⓘ		5 years ago
square-online.com	<u>100</u>	ⓘ			19 years ago
squaresecurity.com	<u>100</u>	ⓘ			5 years ago
squareservices.com	<u>100</u>	ⓘ			15 years ago
square-register.com	<u>100</u>	ⓘ	ⓘ		8 years ago
squareaccess.com	<u>100</u>	ⓘ			9 years ago
squarepayment.com	<u>100</u>	ⓘ			4 years ago

Domain	Score 	Can Send/Receive Emails	Hosts Website	Known Malicious	Registered
square.com	<u>100</u>				14 years ago
squareservice.com	<u>100</u>				14 years ago
squaresecure.com	<u>100</u>				4 years ago
squareaccount.com	<u>100</u>				9 years ago
squareauth.com	<u>94</u>				4 months ago
squarecredit.com	<u>90</u>	<div data-bbox="751 656 1274 806" style="border: 1px solid black; padding: 5px; width: fit-content;"> mailstore1.secureserver.net smtp.secureserver.net </div>			9 years ago
loginsquare.com	<u>75</u>				2 years ago
hr-square.com	<u>75</u>				7 months ago
squaresafe.com	<u>75</u>				2 years ago
squareregister.com	<u>75</u>				8 years ago
squaredownload.com	<u>75</u>				3 years ago

TECHNIQUE TWO SPLUNK

Enterprise Security Content Update (ESCU)

Category: Malware

Version: 1

Created: 6/01/2017

Modified: 11/09/2017

Brand Monitoring

Run Story

Description:

Adversaries will often attempt to abuse your brand by using a fully qualified domain name (FQDN) that looks very similar to the real one in an attempt to fool your employees or customers into interacting with malicious infrastructure. This Analytic Story allows you to specify the FQDNs that you care about and will generate alternate permutations from that domain and monitor your infrastructure for indication of DNS activity to those fake domains.

Narrative:

Once configured, the Enterprise Security Content Update app (ESCU) can leverage our adaptation of DNStwist to generate possible permutations of specified brands and/or faux domains. Splunk will continually scan email-sender addresses, web traffic, and DNS requests to provide you with notable events. A drilldown gives you more actionable information, including IP addresses, URLs, and user data. The configuration and enablement processes involve entering your brand into the ES lookup and/or creating a .csv file containing external names you'd like to monitor. Next, you enable the three searches (email, web, and DNS) and set the time interval for scanning. Splunk will create and send you notable events when it identifies a suspicious brand permutation. You'll get the URL, source, IP address with likely geographic information, contextual searches to help you scope the problem, and investigative searches to help kick off your investigation.

Att&ck:

Kill Chain Phases: Delivery Actions on Objective

CIS 20: CIS 7

Data Model: Application_State Authentication Email
Network_Resolution Risk Web

Technologies: Bluecoat Bro Carbon Black Response
CrowdStrike Falcon Linux
Microsoft Exchange Microsoft Windows
Palo Alto Firewall Splunk Enterprise
Splunk Enterprise Security Splunk Stream
Sysmon Tanium Ziften macOS

References: <https://blog.domaintools.com/tag/brand-monitor/>
<https://securingtomorrow.mcafee.com/consumer/fa-safety/what-is-typosquatting/>
<https://blog.malwarebytes.com/cybercrime/2016/06/typosquatting/>

Configure in ES

Description

This search creates permutations of your existing domains and stores them in a specified lookup file so they can be checked for in the associated detection searches.

Search

```
| dnstwist domainlist=domains.csv | eval domain_abuse="true" | table  
domain, domain_abuse | outputlookup brandMonitoring_lookup
```

All time



A young man with dark hair and a wide-eyed, intense expression is shown from the chest up. He is wearing a dark green t-shirt with a yellow graphic. He is holding a white corded telephone receiver in his right hand. The background is a room with yellow walls and white trim. A large, white, semi-transparent rectangular box is overlaid on the image, containing the word "DEFENSES" in a bold, white, sans-serif font.

DEFENSES

DEFENSES

USING DNS TO PROTECT EMPLOYEES

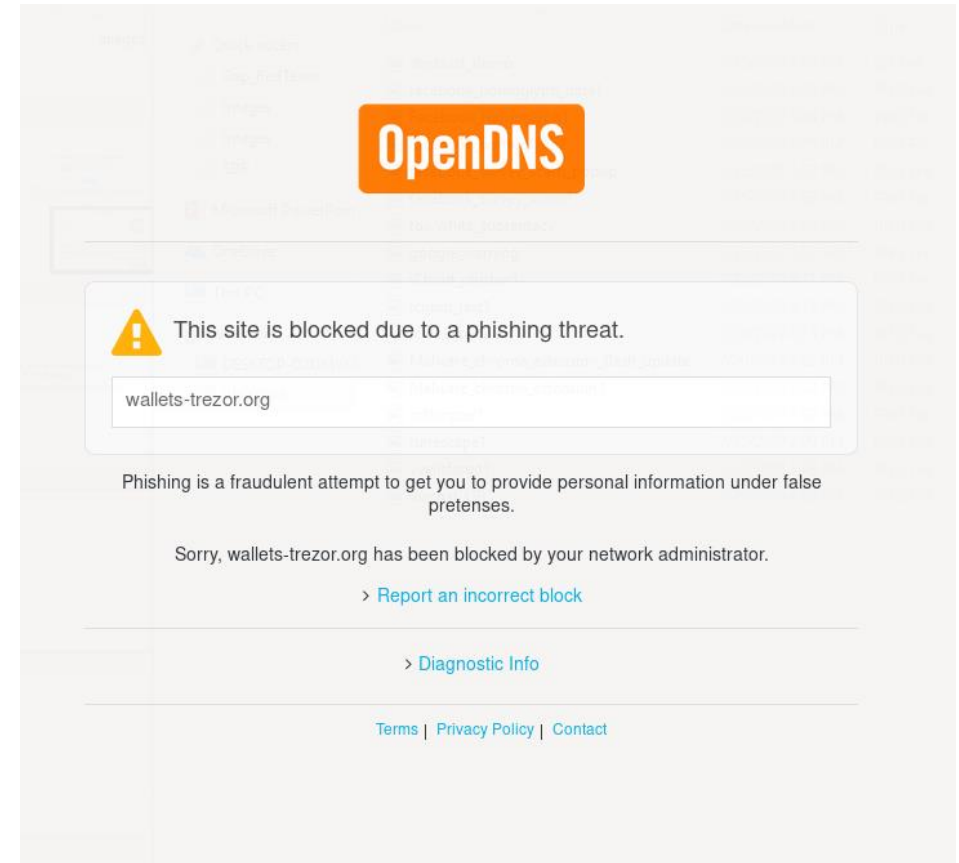
USE DNS TO SINK HOLLING DOMAINS

GOAL

Redirect users from blacklisted domains to a warning page/log server

VIA INTERNAL DNS SERVERS

- Response Policy Zones (RPZ) rules
- Script changes to /etc/hosts file of users
- Jason Fossen released a Windows Sinkhole DNS powershell script as part of SANS SEC505 class
(*Update-HostsFile.ps1* and *Sinkhole-DNS.ps1*)



SINKHOLE DOMAINS

PREVENT USERS FROM VISITING MALICIOUS CONTENT

Response Policy Zones (RPZ)

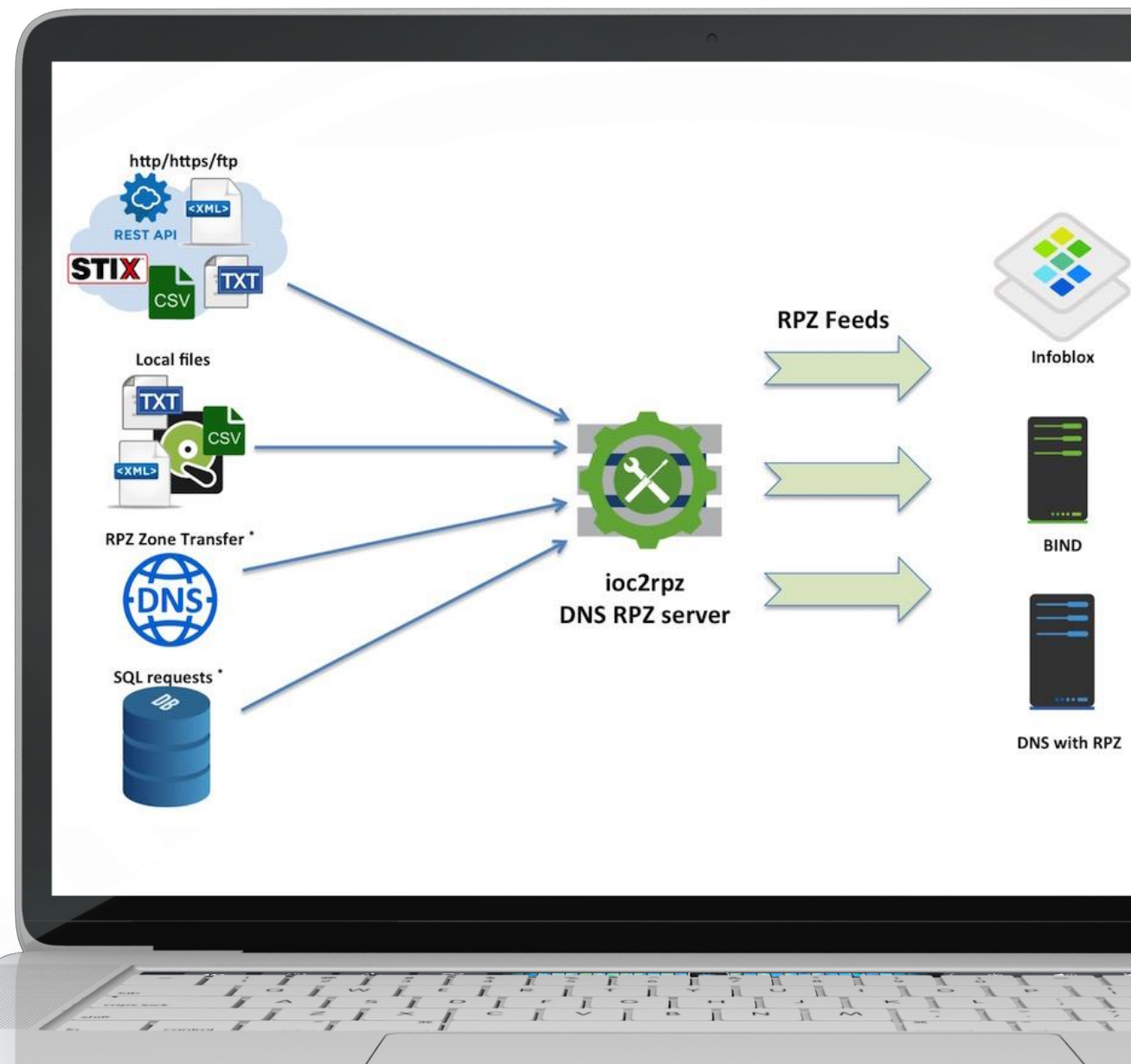
Override global DNS to provide alternate responses to queries

Goal

Protect users by blocking all domain permutations from being reached

Block known malicious domains

<https://github.com/Homas/ioc2rpz>



Demo

AWS t2.micro running:

- ioc2rpz
- ioc2rpz.gui

Feeds:

- <https://malwaredomains.com>
- <https://github.com/notracking/hosts-blocklists>

IOCs - 145374

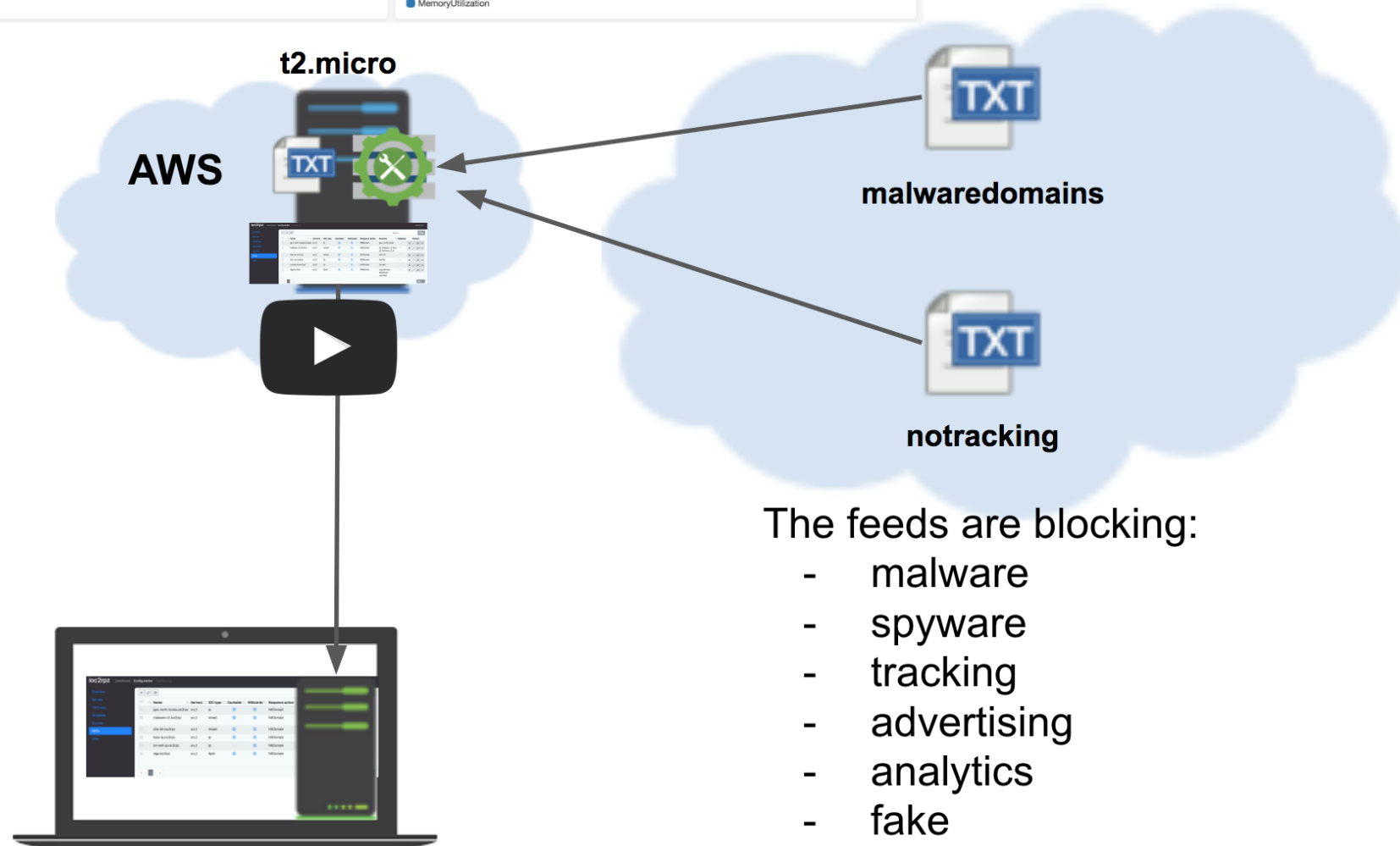
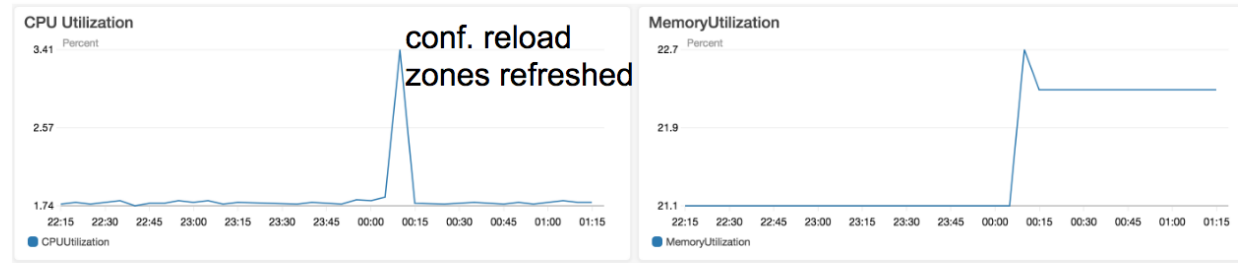
RPZ Rules - 290748

Whitelist:

- Local whitelist

Macbook with VirtualBox:

- Linux server running ISC bind



The feeds are blocking:

- malware
- spyware
- tracking
- advertising
- analytics
- fake
- webminers

UPCOMING BROWSER PROTECTIONS

WARNINGS FOR LOOKALIKE URLS

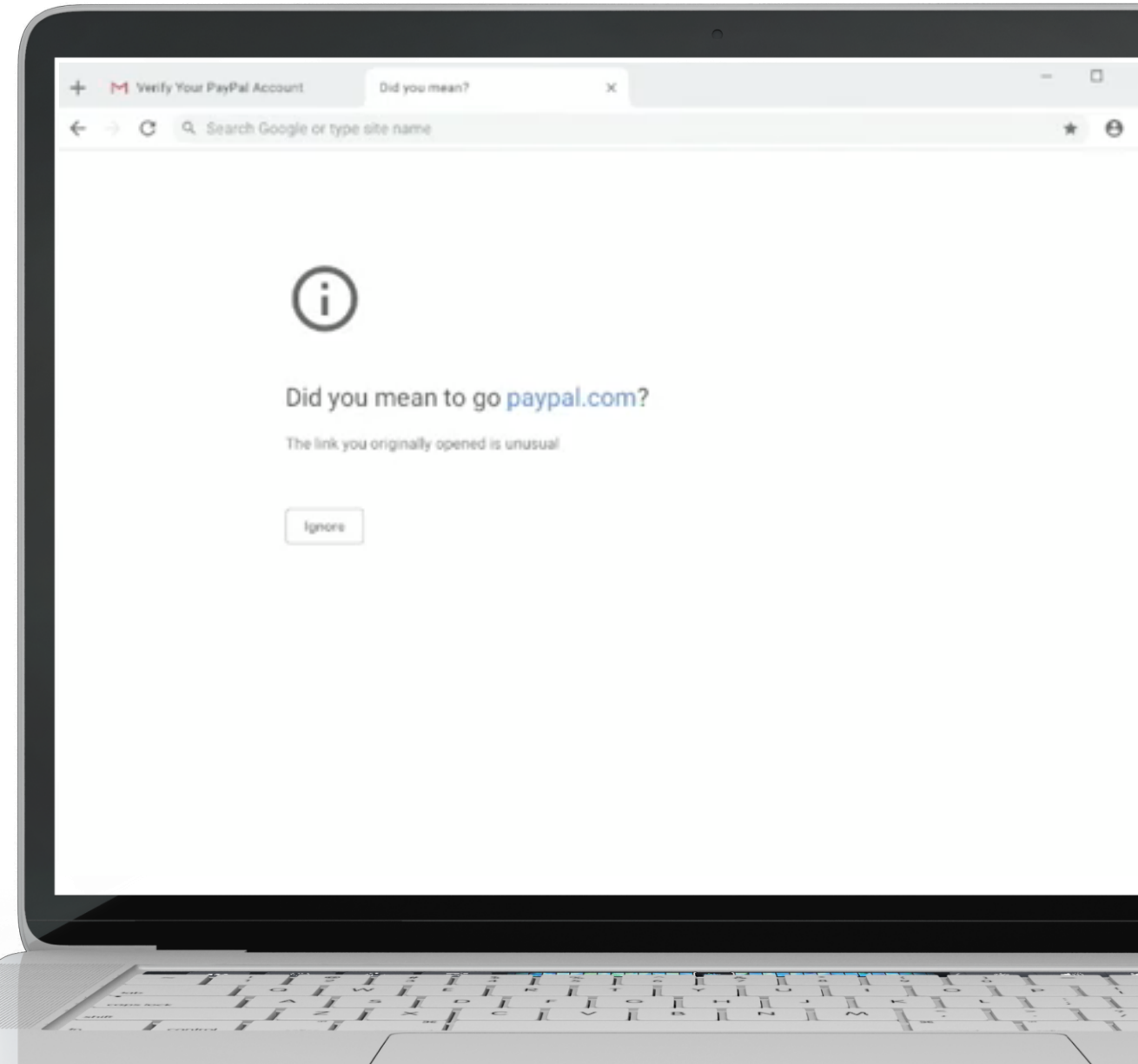
Chrome Warnings

Based domain permutations of sites with a high PageRank
Prompt user to confirm

Goal

Deter attacks by interpreting likely malicious domain requests and prompting user to confirm

https://chromium.googlesource.com/chromium/src/+master/docs/security/url_display_guidelines/url_display_guidelines.md



Navigation suggestions for lookalike URLs



Reset all to default

Experiments

74.0.3688.0

Available

Unavailable

● Navigation suggestions for lookalike URLs

Enable navigation suggestions for URLs that are visually similar to popular domains or to domains with a site engagement score. – Mac, Windows, Linux, Chrome OS

[#enable-lookalike-url-navigation-suggestions](#)

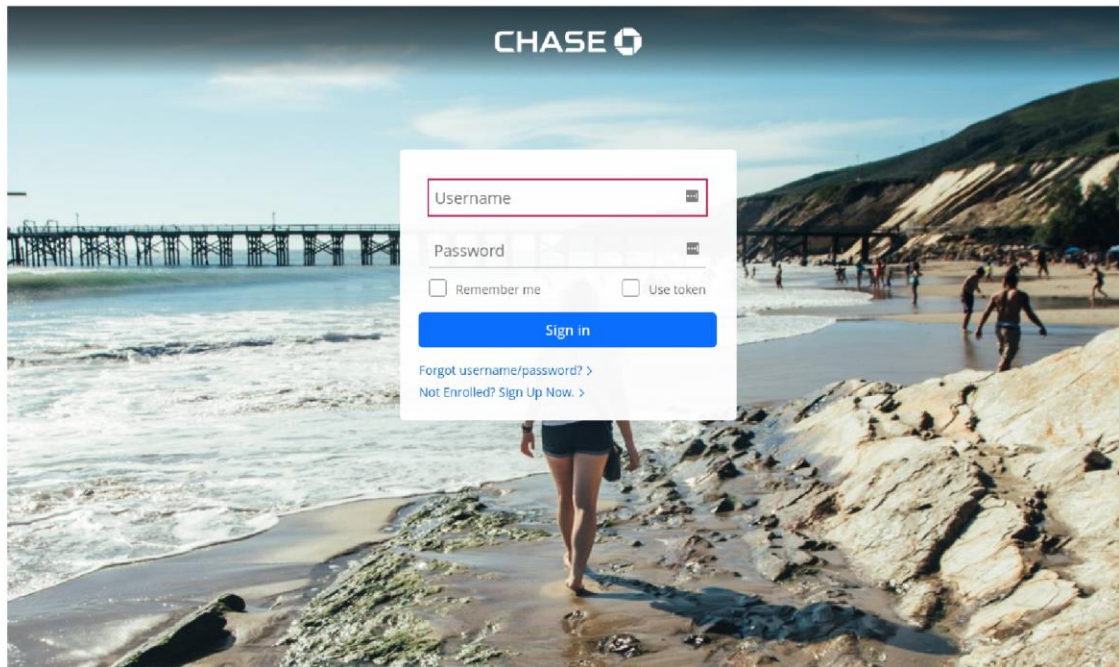
Enabled ▾

A photograph of a red car parked behind a chain-link fence. In the background, three people are standing near a building. The scene is surrounded by green foliage. A large white text box is overlaid on the center of the image.

FIGHT BACK

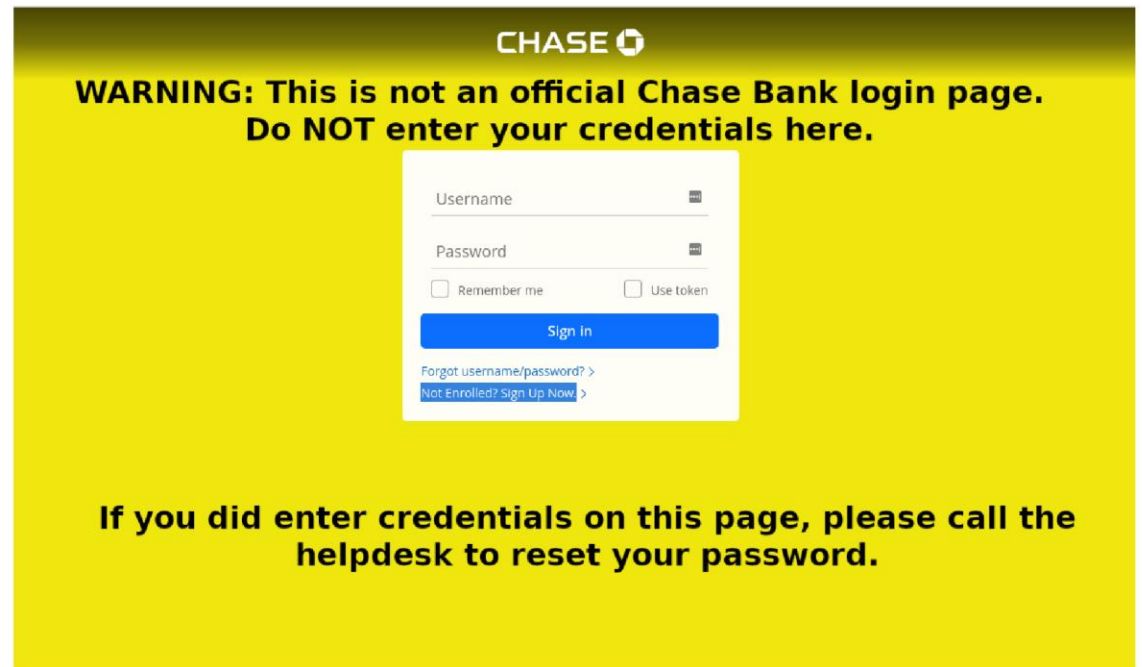
REPLACEMENT WARNINGS FIGHTING BACK

Scammers are lazy and will often link to images hosted on your own servers replace stolen images with warnings



Follow us: [f](#) [i](#) [t](#) [v](#) [i](#)

BEFORE



Follow us: [f](#) [i](#) [t](#) [v](#) [i](#)

AFTER

FIGHT BACK

CALL IN THE **LAWYERS**

ICANN ARBITRATION VIA UNIFORM DOMAIN NAME DISPUTE RESOLUTION POLICY (UDRP)

- Fee: \$1,300 for the first domain name
- If complaint filer wins, domain is transferred to them
- *Typical time frame:* 50-60 domains

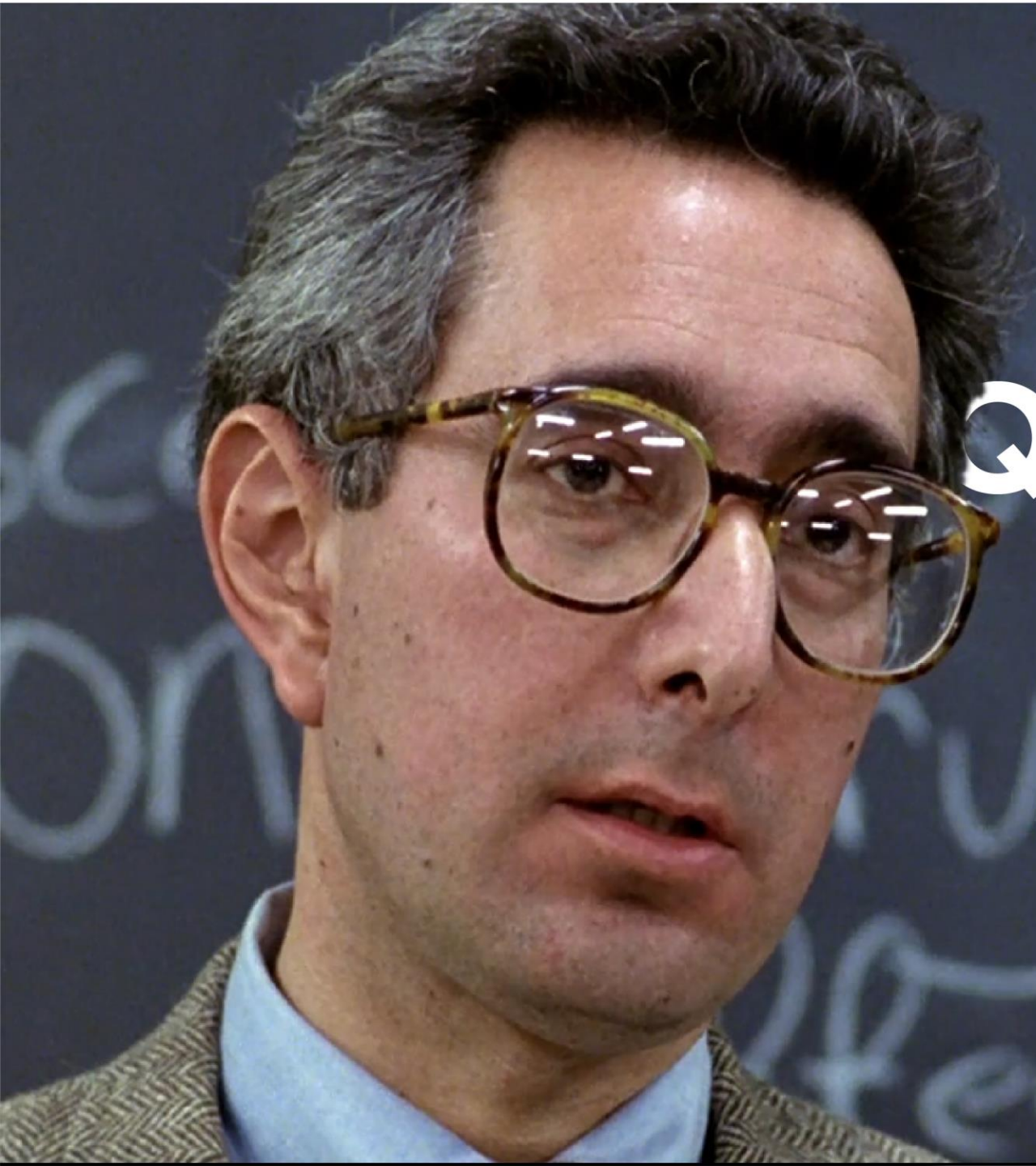
ANTICYBERSQUATTING CONSUMER PROTECTION ACT (ACPA)

- Penalties \$100,000 per domain



A photograph of three young people on a rooftop. On the left, a young man in a tan and black jacket looks forward. In the center, a young woman in a white shirt and grey shorts looks slightly to the right. On the right, a young man in a grey t-shirt and tan pants has his hands on his head, looking upwards. A large, white, semi-transparent rectangular box is overlaid across the middle of the image, containing the text "THE BIG PICTURE" in a bold, white, sans-serif font. The background is a plain, light-colored wall, and some foliage is visible on the left and bottom edges.

THE BIG PICTURE



**QUESTIONS?
ANYONE?
ANYONE?**

sharing it

sharing it

City of Chicago
Harold Washington, Mayor

THANK YOU

