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
Which companies are most often targeted?

And what percentage of their domain permutations do they own?

**COMMON ATTACK TARGETS**

**WHO IS BEING TARGETED**

- Wells Fargo
- T
- Netflix
- LinkedIn
- Facebook
- Chase
- Dropbox
- Yahoo!
- AT&T
- Gmail
- Amazon
- Microsoft
- PayPal
- Comcast
- Apple
- Bank of America
OWNED PERCENTAGE OF
DOMAIN PERMUTATIONS

AMAZON OWNS 59% OF THEIR DOMAIN PERMUTATIONS
1. Types of Domain Abuse

- Typo squatting
- Homoglyphs
- Bit squatting
- Top Level Domain (TLD) variations

2. Subdomain Permutations
TYPES OF ABUSE

DOMAIN PERMUTATIONS

TYPO SQUATTING
HOMOGlyphS
BIT SQUATTING
ADDITIONS, INSERTIONS, DELETIONS
(TLD) VARIATIONS
SUBDOMAIN PERMUTATIONS
Typosquatting

• Definition: registering a version of the targeted domain that is likely to be mistyped

• AKA URL Hijacking

• Example: facebpok.com
Typosquatting

Definition: registering a version of the targeted domain that is likely to be mistyped

AKA URL Hijacking

Example: facebpok.com
Homoglyphs

Definition: characters that appear the same or similar to other characters

Examples:

http://facẹboọk.com/login.html

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

https://github.com/bishopfox/cervus
DOMIAN PERMUTATION

BIT SQUATTING

All Companies

Selected Companies

https://kushaldas.in/posts/tracking-my-phone-s-silent-connections.html
TLD Variations

Definition: registering a domain with the same domain name as a targeted site, but with a different top level domain (TLD).

Examples:
- 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
TYPES OF ATTACKS
Malware

- Old way: Fake Adobe Acrobat
- New way: Malicious Chrome extensions

Type of Attack: Malware

Adobe Acrobat

Chrome Extensions
Fraud • wallets-trezor.org

Emulates trezor.io to try to steal cryptocurrency wallet seeds.

Type of Attack

FRAUD

Trezor.io vs. wallets-trezor.org

Warning: trezor data damage do not disconnect your device.

Please enter your 24 word recovery seed to restore your wallet.

1. 
2. 
3. 
4. 
5. 
6. 
7. 
8. 
9. 
10. 
11. 
12. 
13. 
14. 
15. 
16. 
17. 
18. 
19. 
20. 
21. 
22. 
23. 
24.
REAL VS MALICIOUS
FOX WHITE SUPREMACY

Foxnews.com vs. Foxnews.cc
I-Cloud Account Example

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

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

http://vvwellsfargo.com

I love LBL!

This website is not affiliated with Wellsfargo.com 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
Part 1: Monitoring
Generating comprehensive lists of possible domains

• dnstwist by Marcin Ulikowski (elceef)

Takes a domain name as a seed and generates permutations.
Perceptual analysis

• If there is open service on web port:
  • Screenshot
  • Fuzzyhashing
  • Compare to target/original

STEP 02
PhishFinder

Find phishing campaigns before they find you!

Email Address

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/receive emails
- **63%** Registered
- **0%** Known malicious

<table>
<thead>
<tr>
<th>Domain</th>
<th>Score</th>
<th>Can Send/Receive Emails</th>
<th>Hosts Website</th>
<th>Known Malicious</th>
<th>Registered</th>
</tr>
</thead>
<tbody>
<tr>
<td>square.no</td>
<td>100</td>
<td>1</td>
<td></td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>squarerecover.com</td>
<td>100</td>
<td>1</td>
<td></td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>squarepayments.com</td>
<td>100</td>
<td>1</td>
<td></td>
<td>0</td>
<td>2 months ago</td>
</tr>
<tr>
<td>squarehr.com</td>
<td>100</td>
<td>1</td>
<td></td>
<td>0</td>
<td>5 years ago</td>
</tr>
<tr>
<td>square-online.com</td>
<td>100</td>
<td>1</td>
<td></td>
<td>0</td>
<td>19 years ago</td>
</tr>
<tr>
<td>squaresecurity.com</td>
<td>100</td>
<td>1</td>
<td></td>
<td>0</td>
<td>5 years ago</td>
</tr>
<tr>
<td>squareservices.com</td>
<td>100</td>
<td>1</td>
<td></td>
<td>0</td>
<td>15 years ago</td>
</tr>
<tr>
<td>square-register.com</td>
<td>100</td>
<td>1</td>
<td></td>
<td>0</td>
<td>8 years ago</td>
</tr>
<tr>
<td>squareaccess.com</td>
<td>100</td>
<td>1</td>
<td></td>
<td>0</td>
<td>9 years ago</td>
</tr>
<tr>
<td>squarepayment.com</td>
<td>100</td>
<td>1</td>
<td></td>
<td>0</td>
<td>4 years ago</td>
</tr>
<tr>
<td>Domain</td>
<td>Score</td>
<td>Can Send/Receive Emails</td>
<td>Hosts Website</td>
<td>Known Malicious</td>
<td>Registered</td>
</tr>
<tr>
<td>---------------------</td>
<td>-------</td>
<td>-------------------------</td>
<td>---------------</td>
<td>----------------</td>
<td>-----------------</td>
</tr>
<tr>
<td>squareservice.com</td>
<td>100</td>
<td>🔄</td>
<td></td>
<td></td>
<td>14 years ago</td>
</tr>
<tr>
<td>squaresecure.com</td>
<td>100</td>
<td>🔄</td>
<td></td>
<td></td>
<td>4 years ago</td>
</tr>
<tr>
<td>squareaccount.com</td>
<td>100</td>
<td>🔄</td>
<td></td>
<td></td>
<td>9 years ago</td>
</tr>
<tr>
<td>squareauth.com</td>
<td>94</td>
<td>🔄</td>
<td></td>
<td></td>
<td>4 months ago</td>
</tr>
<tr>
<td>squarecredit.com</td>
<td>90</td>
<td>🔄</td>
<td></td>
<td></td>
<td>9 years ago</td>
</tr>
<tr>
<td>loginsquare.com</td>
<td>75</td>
<td>🔄</td>
<td></td>
<td></td>
<td>2 years ago</td>
</tr>
<tr>
<td>hr-square.com</td>
<td>75</td>
<td>🔄</td>
<td></td>
<td></td>
<td>7 months ago</td>
</tr>
<tr>
<td>squaresafe.com</td>
<td>75</td>
<td>🔄</td>
<td></td>
<td></td>
<td>2 years ago</td>
</tr>
<tr>
<td>squareregister.com</td>
<td>75</td>
<td>🔄</td>
<td></td>
<td></td>
<td>8 years ago</td>
</tr>
<tr>
<td>squaredownload.com</td>
<td>75</td>
<td>🔄</td>
<td></td>
<td></td>
<td>3 years ago</td>
</tr>
</tbody>
</table>
**Technique Two**

**SPLUNK**

Enterprise Security Content Update (ESCU)

---

**Brand Monitoring**

**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 DNS twist 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.

---

**Attack:**

- Delivery
- Actions on Objective

**Kill Chain Phases:**

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/fraudsecurity/what-is-typo-squatting/  
https://blog.malwarebytes.com/cybercrime/2016/04/typo-squatting/
DEFENSES
DEFENSES

USING DNS TO PROTECT EMPLOYEES

USE DNS TO SINK HOLING 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)
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
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

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
Part 3: Fighting Back
Fighting Back

Replacement Warnings

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

**BEFORE**

**AFTER**

**WARNING:** This is not an official Chase Bank login page. Do NOT enter your credentials here.

If you did enter credentials on this page, please call the helpdesk to reset your password.
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 days

ANTICYBERSQUATTING CONSUMER PROTECTION ACT (ACPA)

- Penalties $100,000 per domain
The big picture

Something from this scene.
QUESTIONS? ANYONE? ANYONE?
Thank you.