GHOST IN THE BROWSER

BROAD-SCALE ESPIONAGE WITH BITSQUATTING

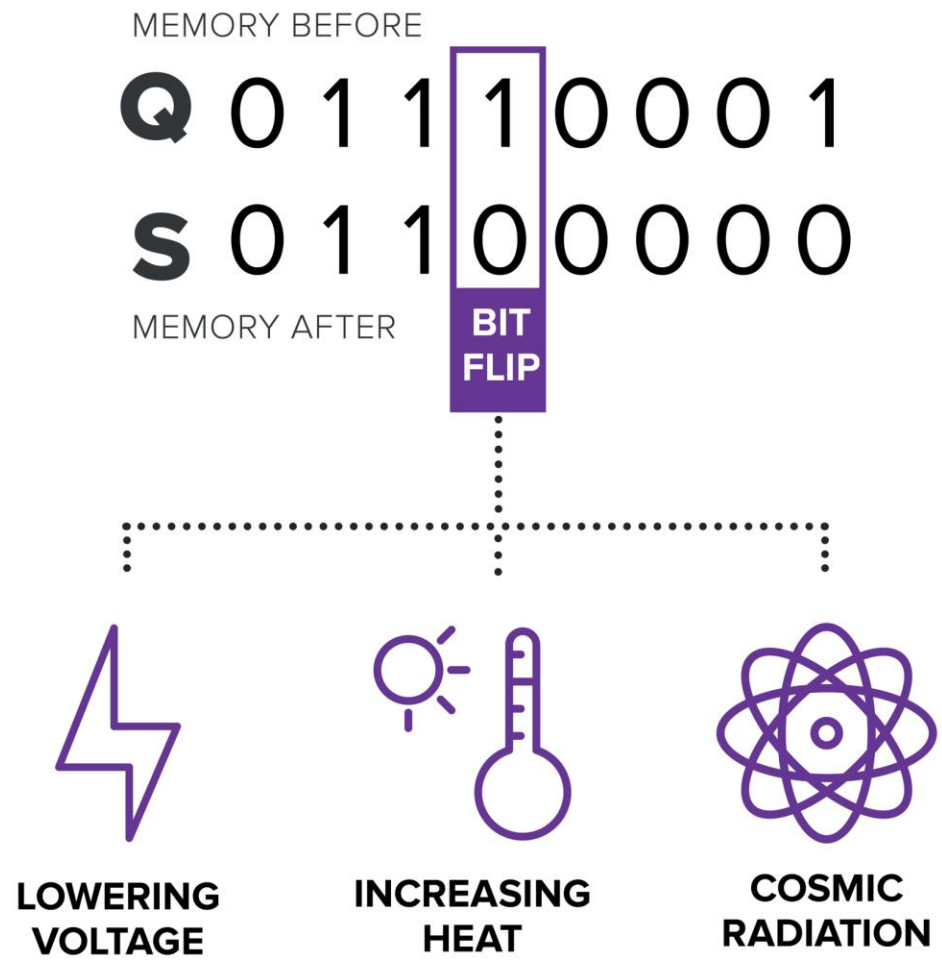
OSCAR SALAZAR | ROB RAGAN OF BISHOP FOX

WHAT IS A **BIT FLIP?**

When a 1 changes to a 0 or a 0 changes to a 1.

These 1's and 0's are used to represent the letters in the text we read.

This attack vector works by exploiting an opportunistic condition when these hardware failures occur.

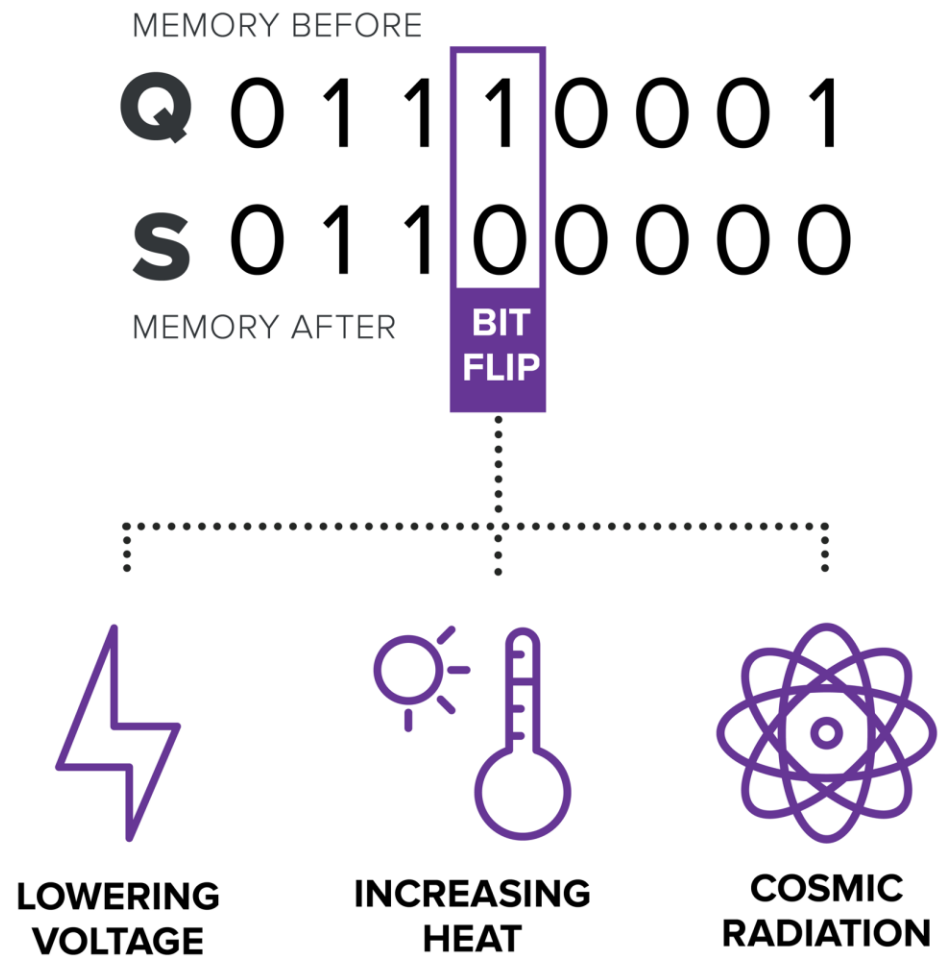


WHAT IS BIT SQUATTING?

Bitsquatting is the act of registering bit flipped variations on a target domain.

Example bitsquat domains of abc.com:

cbc.com
ebc.com
ibc.com
qbc.com
acc.com



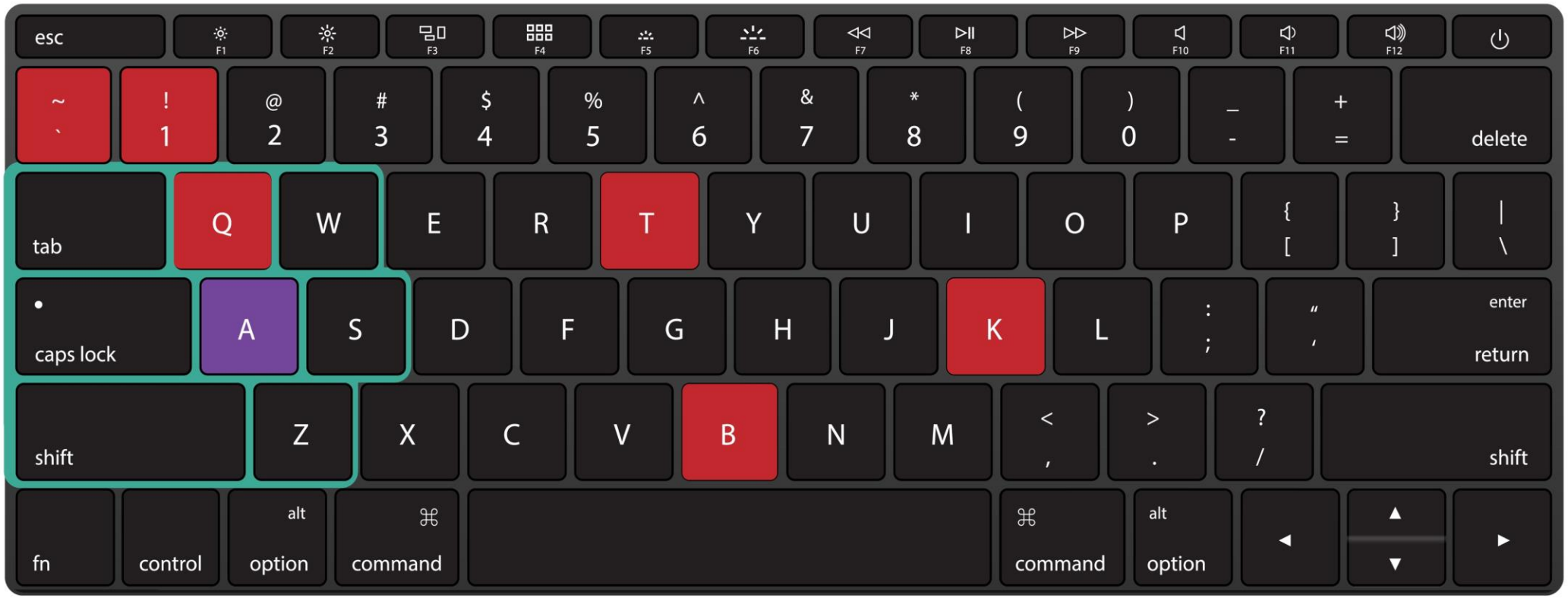
BITSQUAT VS. **TYPOSQUAT**

TARGET KEY

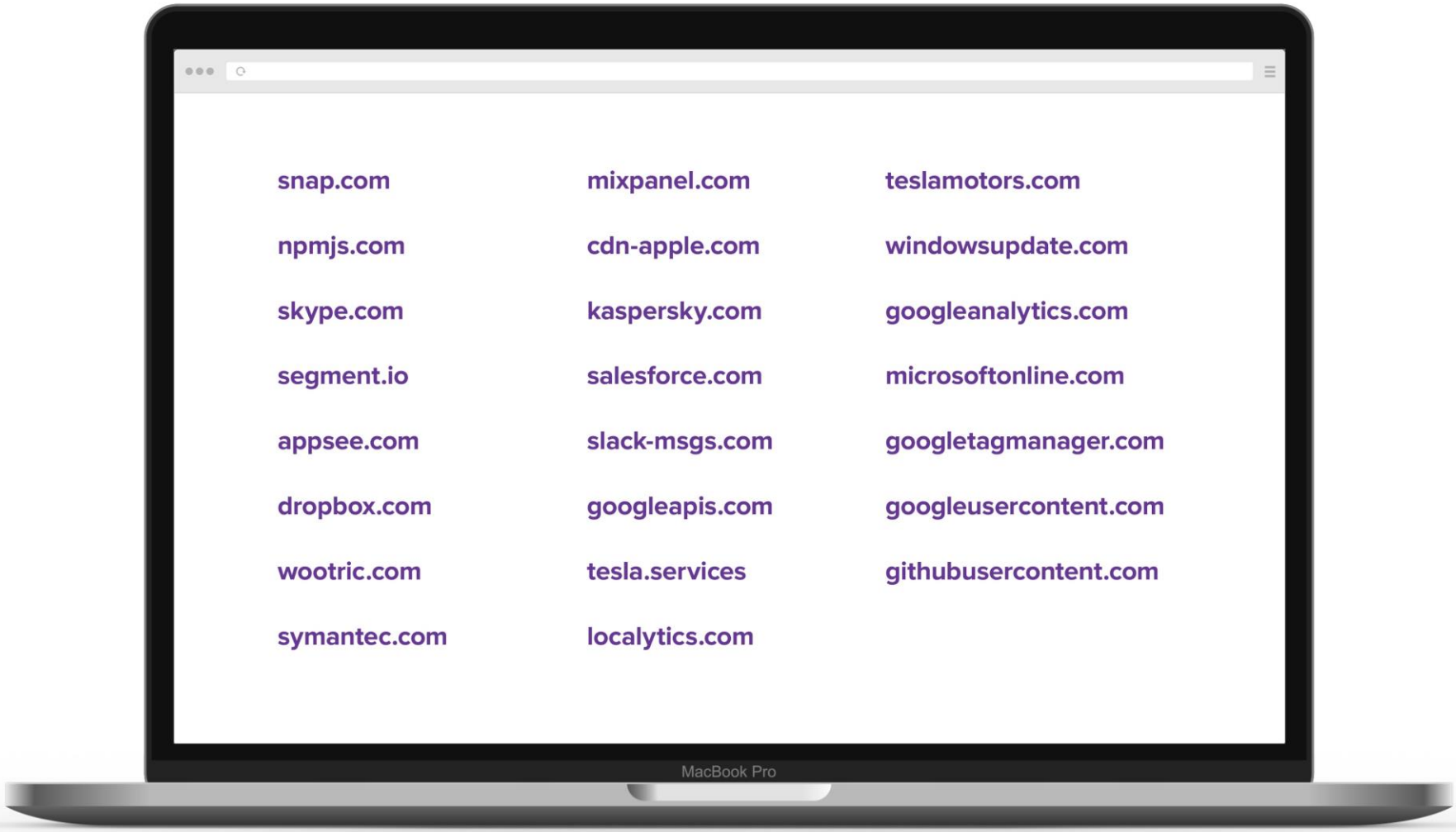
KEY AFTER FLIP OCCURS

Typesquat vs. Bitsquat

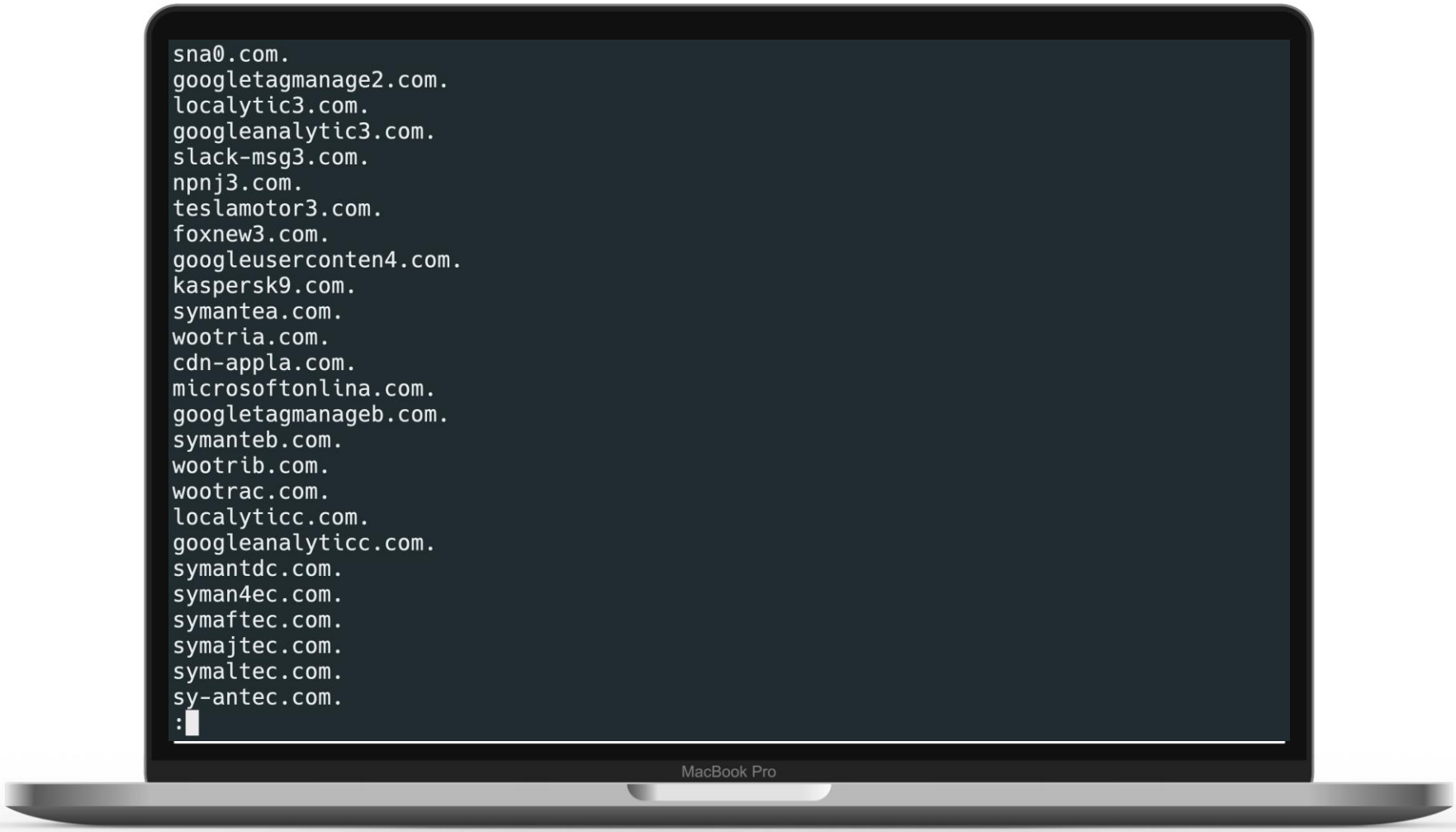
FAT FINGER ZONE



REGISTERED 840 BITFLIPS OF **THESE DOMAINS**



REGISTERED 840 BITFLIPS OF **THESE DOMAINS**



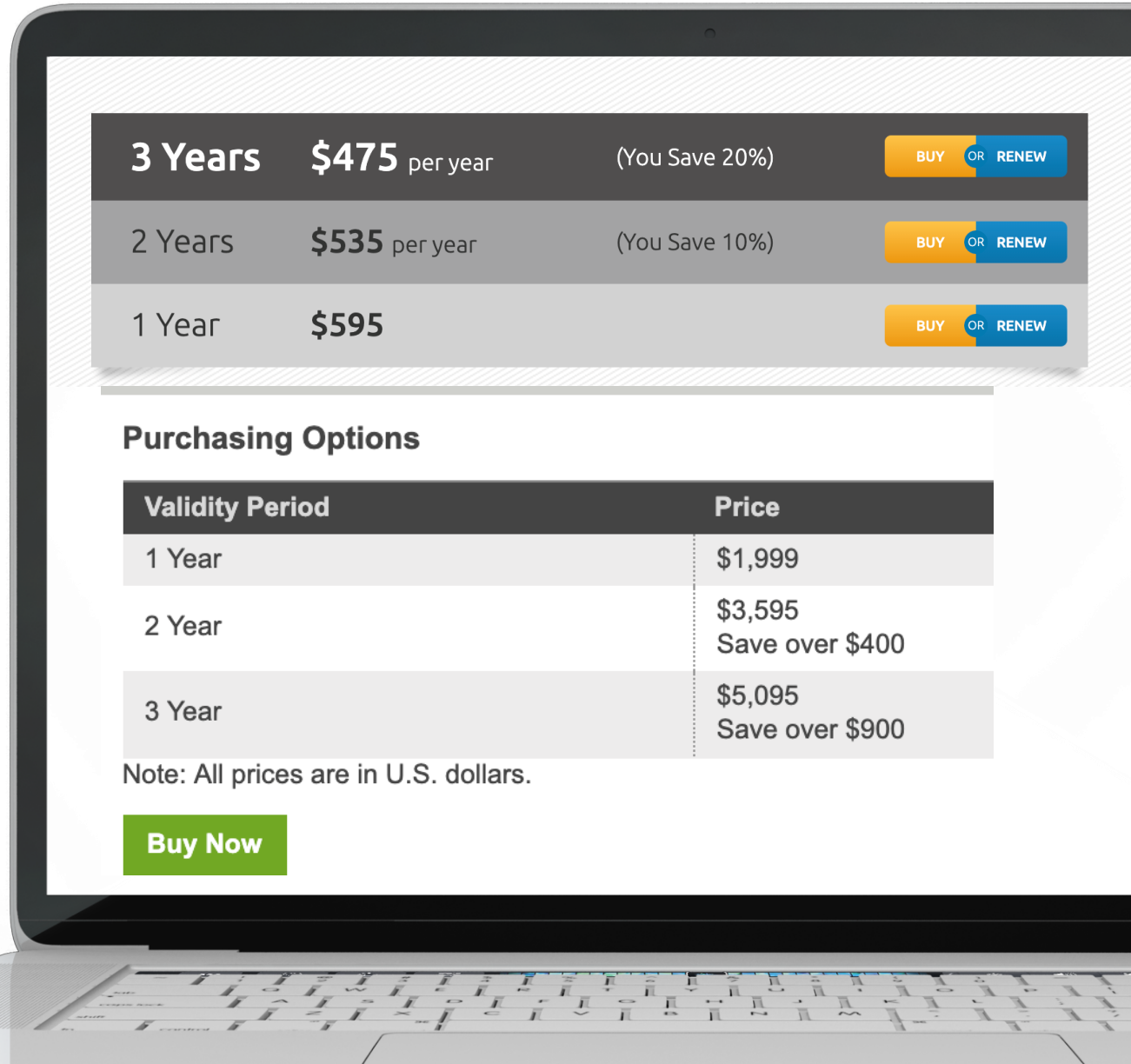
CERTIFICATES

ENCRYPTION IN TRANSIT

Cost Prohibitive (< 2015)

Encrypting data used to be expensive

Costing between $300-$2000 USD for wildcard certificates



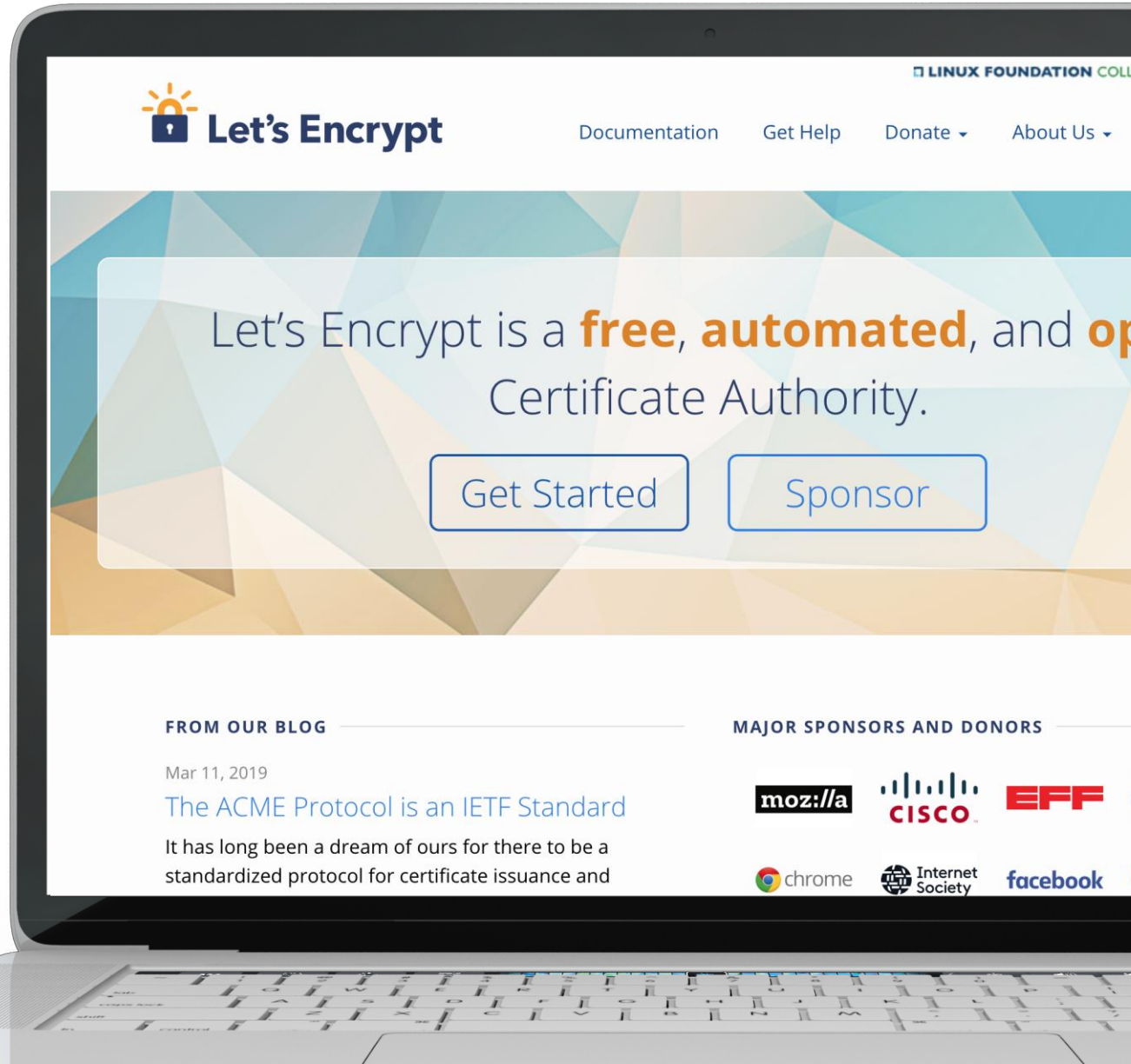
CERTIFICATES FOR ALL

ENCRYPTION IN TRANSIT BECOMES FREE

LetsEncrypt (April 2016)

Certificates become free for all (including threat actors)

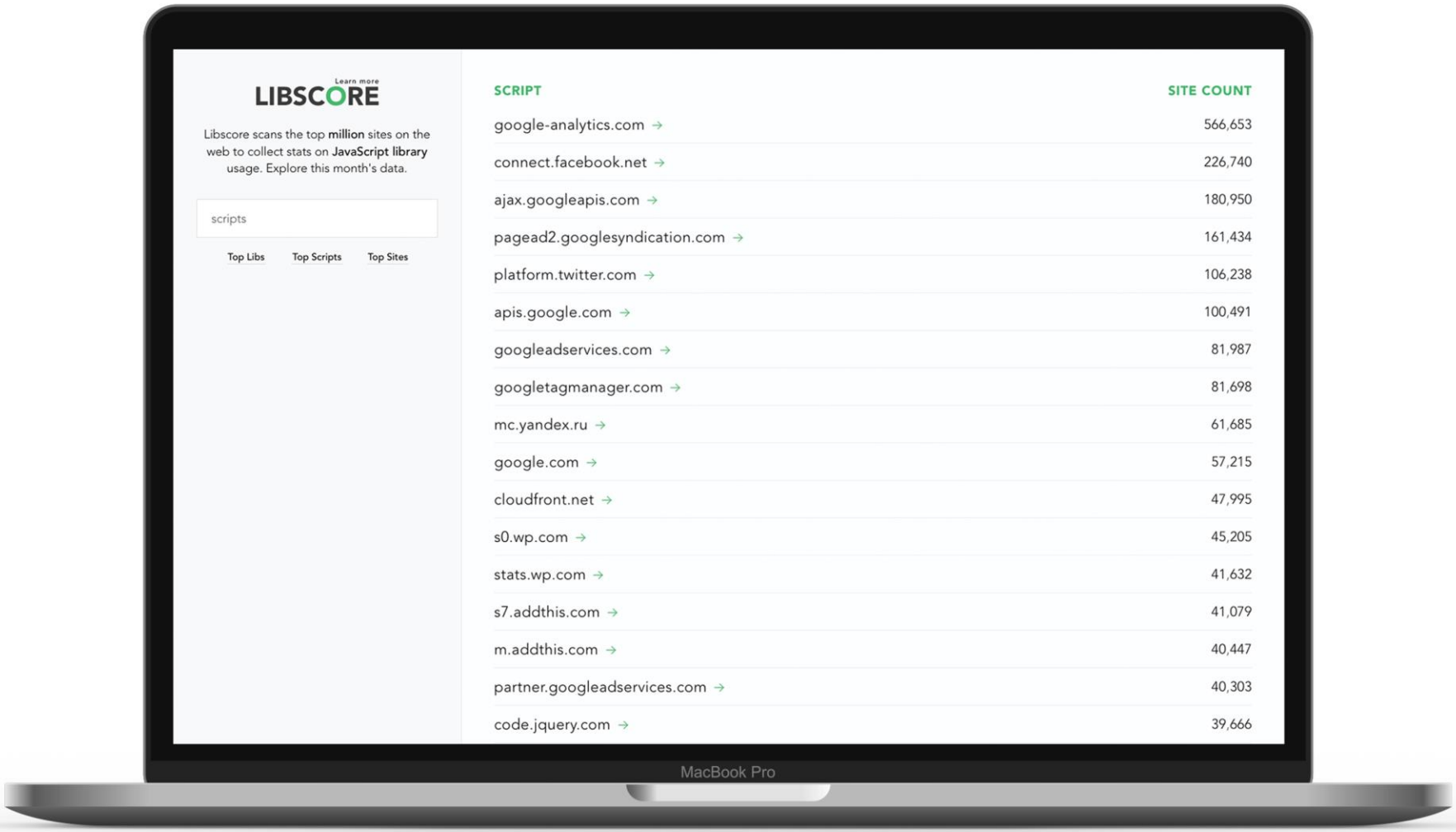
All major cloud providers all provide free certificates



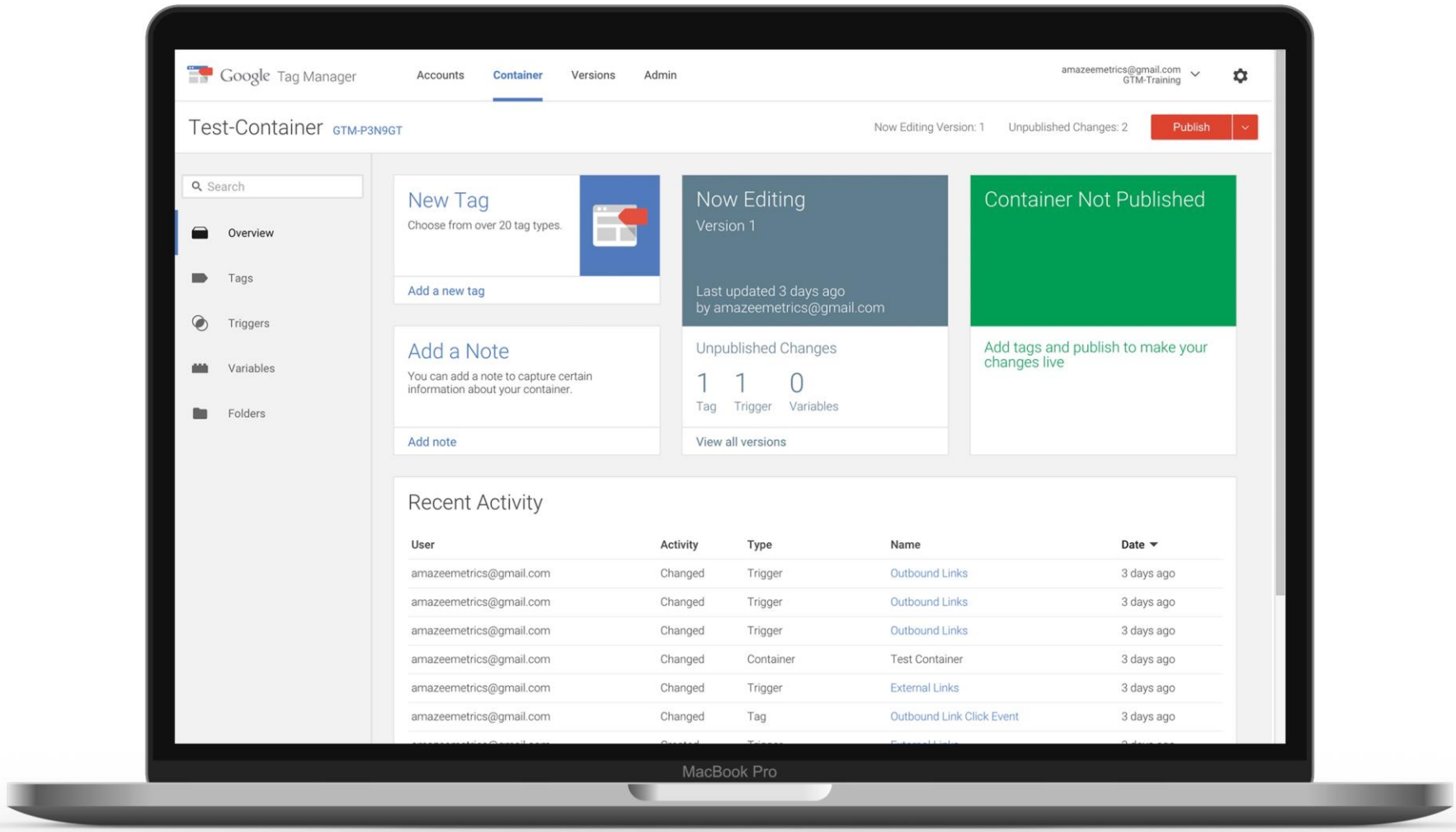
HOW TO SPY ON
USER ACTIVITY

- Register bit squat domains that serve common JavaScript frameworks, libraries, or analytics
- Upon request for .js files or requests with Accept headers expecting JavaScript, response with malicious JS
- Inject script that captures DOM, cookies, screenshots what the user is looking at, and gets cached

MOST POPULAR **JAVASCRIPT LIBRARIES**



MALICIOUS JAVASCRIPT – **GOOGLE TAG MANAGER**



Victim User Agent

```
Mozilla/5.0 (Linux; U; Android 7.0; zh-cn; Mi-4c Build/NRD90M) AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0 Chrome/53.0.2785.146 Mobile Safari/537.36 XiaoMi/MiuiBrowser/9.4.11
```

Cookies

```
JSESSIONID=56FD691E02F536D9F2A16D8B6E38F2B7; _ga=GA1.4.862001398.1550519046; _gid=GA1.4.1232071979.1554341626
```

DOM

```
1. <html><head><!-- Gomgle Tag Manager --><script async="" src="https://www.gomgletagmanager.com/gtm.js?id=GTM-5MWDNS6"></script><script>(function(w,d,s,l,i){
   w[l].push({'gtm.start':new Date().getTime(),event:'gtm.js'});var f=d.getElementsByTagName(s)[0],j=d.createElement(s),dl=l!='dataLayer'?'&l='+l:'';j.async=t
   ps://www.gomgletagmanager.com/gtm.js?id='+i+dl;f.parentNode.insertBefore(j,f);})(window,document,'script','dataLayer','GTM-5MWDNS6');</script><!-- End Gomg
   --><meta charset="utf-8"><meta name="viewport" content="width=device-width,user-scalable=no,initial-scale=1,maximum-scale=1,minimum-scale=1"><title>Subscri
   title><link href="./static/css/failed_default.4f492e7167bd7ae4a66658be22aecf22.css" rel="stylesheet"><style type="text/css"></style></head> <body style="di
   ><!-- Gomgle Tag Manager (noscript) --><noscript><iframe src="https://www.gomgletagmanager.com/ns.html?id=GTM-5MWDNS6"height="0" width="0" style="display:n
   :hidden"></iframe></noscript><!-- End Gomgle Tag Manager (noscript) --><header><img src="./static/img/en_banner_0.4262001305543611.jpg" class="banner" id="
   img id="backArowImg" src="
   S54bXAAAAAAADw/eHBhY2tldCBiZWdpbj0i77u/IiBpZD0iVzVNME1wQ2VoaUh6cmVTek5UY3prYzlkIj8+IDx4OnhtcG1ldGEgeG1sbnM6eD0iYWRvYmU6bnM6bWV0YS8iIHg6eG1wdGs9IkFkb2JlIFhN
   1jMDE0IDc5LjE1MTQ4MSwgMjAxMy8wMy8xMy0xMjowOToxNSAgICAgICAgIj4gPHJkZjpSREYgeG1sbnM6cmRmPSJodHRwOi8vd3d3LnczLm9yZy8xOTk5LzAyLzIyLXJkZi1zeW50YXgtbnMjIj4gPHJkZ
   vbiByZGY6YWJvdXQ9IiIgeG1sbnM6eG1wTU09Imh0dHA6Ly9ucy5hZG9iZS5jb20veGFwLzEuMC9tbS8iIHhtbG5zOnN0UmVmPSJodHRwOi8vbnMuYWRvYmUuY29tL3hhcC8xLjAvc1R5cGUvUmVzb3VyY2
   czp4bXA9Imh0dHA6Ly9ucy5hZG9iZS5jb20veGFwLzEuMC8iIHhtcE1NOk9yaWdpbmFsRG9jdW1lbnRJRD0ieG1wLmRpZDpkZDYzYWY5My02ZDI1LWVjNGEtYjhlNC1lZmNiZWU0MjU5NTkiIHhtcE1NOkR
   nhtcC5kaWQ6OTNDMDYzNzU0RkRCMTFFNkExRTY5N0Q4MDZGMzlBQ0YiIHhtcE1NOkluc3RhbmNlSUQ9InhtcC5paWQ6OTNDMDYzNzQ0RkRCMTFFNkExRTY5N0Q4MDZGMzlBQ0YiIHhtcDpDcmVhdG9yVG9v
   hvdG9zaG9wIENDIChXaW5kb3dzKSI+IDx4bXBNTTpEZXJpdmVkRnJvbSBzdFJlZjppbnN0YW5jZUlEPSJ4bXAuaWlkOmVkOTkwOGE0LTcyMGMtYTk0Yy04NmYyLWJkODI3NTJhMTUwOCIgc3RSZWY6ZG9jO
   wLmRpZDpkZDYzYWY5My02ZDI1LWVjNGEtYjhlNC1lZmNiZWU0MjU5NTkiLz4gPC9yZGY6RGVzY3JpcHRpb24+IDwvcmRmOlJERj4gPC94OnhtcG1ldGE+IDw/eHBhY2tldCBlbmQ9InIiPz4Mf851AAABfE
   MRCGd7e20NfzqDcV+hoWRKSUVoqUUrqKiBa1xfcoePUtFPTiRYkTSWRZN/mTyXTgh6Wz0y+dJjOTTCmVCahDGpM+SO+kkfns1y8FeFL/7VgKogFr1Wwv9r0i41ubdEfadfg//56Yv2CH9Kj8dpiSrhbpAQD
   YBbADhtio0B3ADAmSs+FHANAAPfd4QArgBgiBbqcxakSwAYhaTb5chJJQCMQzeNC7AAgHPzHguiA+cAMIkB1CE6cAYAF7GAKkQHTgFgygFYSG5W6LMZF2AhBwCwSAFYyMYDKFMBtmkpT2PKjdKMSD2QrlI
   JA85QtXAVtZSs3lRXxQ+kqkKLlxVfqxQqlzylW8tEqRJpXSE6T23DMSMQeKGKHO9ZoxBlTo4c87sAdNa5yK6sGLQHoSOKmhSb8Z4mb1jdpn7Ry+Lv2oUjseV+kPdK6wbdMvc7V1Tbn5I30anZYy/p/BBgAM
   ASUVORK5CYII=" class="back-arow"><img src="./static/img/en_logo_0.5875431059614712.png" class="logo" id="logo"></div><p id="bannertext" class="header-txt">
```

MALICIOUS JAVASCRIPT – **GOOGLE TAG MANAGER**

Vulnerable Page URL

http://mgame.robi.com.bd/LPBase/lqy934/

Execution Origin

`http://mgame.robi.com.bd`

User IP Address

202.134.9.132

Location For IP: 202.134.9.132

Continent:	Asia (AS)
Country:	Bangladesh (BD)
Capital:	Dhaka
State:	Dhaka
City Location:	**Dhaka**
Postal:	1204
ISP:	AXIATA Bangladesh (Robi)
Organization:	TM International Bangladesh
AS Number:	AS24432 TM International Bangladesh Ltd.

MALICIOUS JAVASCRIPT INJECTION

GOOGLE TAG MANAGER

Referer

```
http://ptldgame.robi.com.bd/0009Fw?tid=015ca55fde007e2ed48&offer_id=130&sub_affid=45
```

Victim User Agent

```
Mozilla/5.0 (Linux; U; Android 7.0; zh-cn; Mi-4c Build/NRD90M) AppleWebKit/537.36 (KHTML, like Gecko) Version/4.0 Chrome XiaoMi/MiuiBrowser/9.4.11
```

Cookies

```
JSESSIONID=56FD691E02F536D9F2A16D8B6E38F2B7; _ga=GA1.4.862001398.1550519046; _gid=GA1.4.1232071979.1554341626
```

MALICIOUS JAVASCRIPT INJECTION

GOOGLE TAG MANAGER

213.186.182.67 https://www.elevay.com/ar/info/uk-tier-1-visa/?ut...

Location For IP: 213.186.182.67	
Continent:	Asia (AS)
Country:	Jordan (JO)
Capital:	Amman
State:	Al Balqa'
City Location:	**Amman**
ISP:	Jordan Data Communications Company LLC
Organization:	Jordan Data Communications Company LLC
AS Number:	AS8376 Jordan Data Communications Company LLC

View Full Report

Resend Email Report

Delete

MALICIOUS JAVASCRIPT INJECTION

GOOGLE TAG MANAGER

https://www.elevay.com/ar/info/uk-tier-1-visa/?utm_source=Adwords&utm_medium=Arabic&utm_campaign=UK&utm_keyword=%D9%85%D8%AA%D8%B7%D9%84%D8%A8%D8%A7%D8%AA%20%2B%D8%A7%D9%84%D9%81%D9%8A%D8%B2%D8%A7%20%2

Execution Origin

`https://www.elevay.com`

User IP Address

213.186.182.67

Referer

`https://www.google.com/`

Victim User Agent

`Mozilla/5.0 (iPhone; CPU iPhone OS 12_1_4 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.0 Mobile/15E148 Safari/604.1`

Victim User Agent

```
Mozilla/5.0 (iPhone; CPU iPhone OS 12_1_4 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/12.0 Mobile/15E148 Safari/604.1
```

Cookies

```
MXCookie=; ORG1188=25b11841-c4f7-4b60-bdf9-d7414b48b4ef; PHPSESSID=baj705gddjdsbd7ksfk2tie4e5
```

DOM

```
<html data-whatinput="touch" data-whatintent="touch" class=" whatinput-types-initial whatinput-types-touch"><head>
        <!-- Google Tag Manager -->
        <script type="text/javascript" async="" src="https://cdn.livechatinc.com/tracking.js"></script><script async="" src="https://www.googletageanager.com/gtm.js?id=GTM-NL6PHNS"></script><script>(function(w,d,s,l,i){w[l]=w[l]||[];w[l].push({'gtm.start':
        new Date().getTime(),event:'gtm.js'});var f=d.getElementsByTagName(s)[0],
        j=d.createElement(s),dl=l!='dataLayer'?'&l='+l:'';j.async=true;j.src=
        'https://www.googletageanager.com/gtm.js?id='+i+dl;f.parentNode.insertBefore(j,f);
        })(window,document,'script','dataLayer','GTM-NL6PHNS');</script>
        <!-- End Google Tag Manager -->
        <meta http-equiv="Content-Type" content="text/html; charset=utf-8">

        <!--
        ==============================================
        Mobile Specific Metas
        ==============================================
        -->
        <meta name="viewport" content="width=device-width, initial-scale=1, maximum-scale=1">


```

MALICIOUS JAVASCRIPT INJECTION

GOOGLE TAG MANAGER

Thumbnail	Victim IP	Vulnerable Page URI	Options
	27.92.54.4	https://swallows-crew.flpjp.com/mypage	View Full Report Resend Email Report Delete
	114.142.249.79	https://pipahdpewavin.blogspot.com/2012/04/war...	View Full Report Resend Email Report Delete

HOW TO STEAL
PASSWORDS

BISHOPFOX

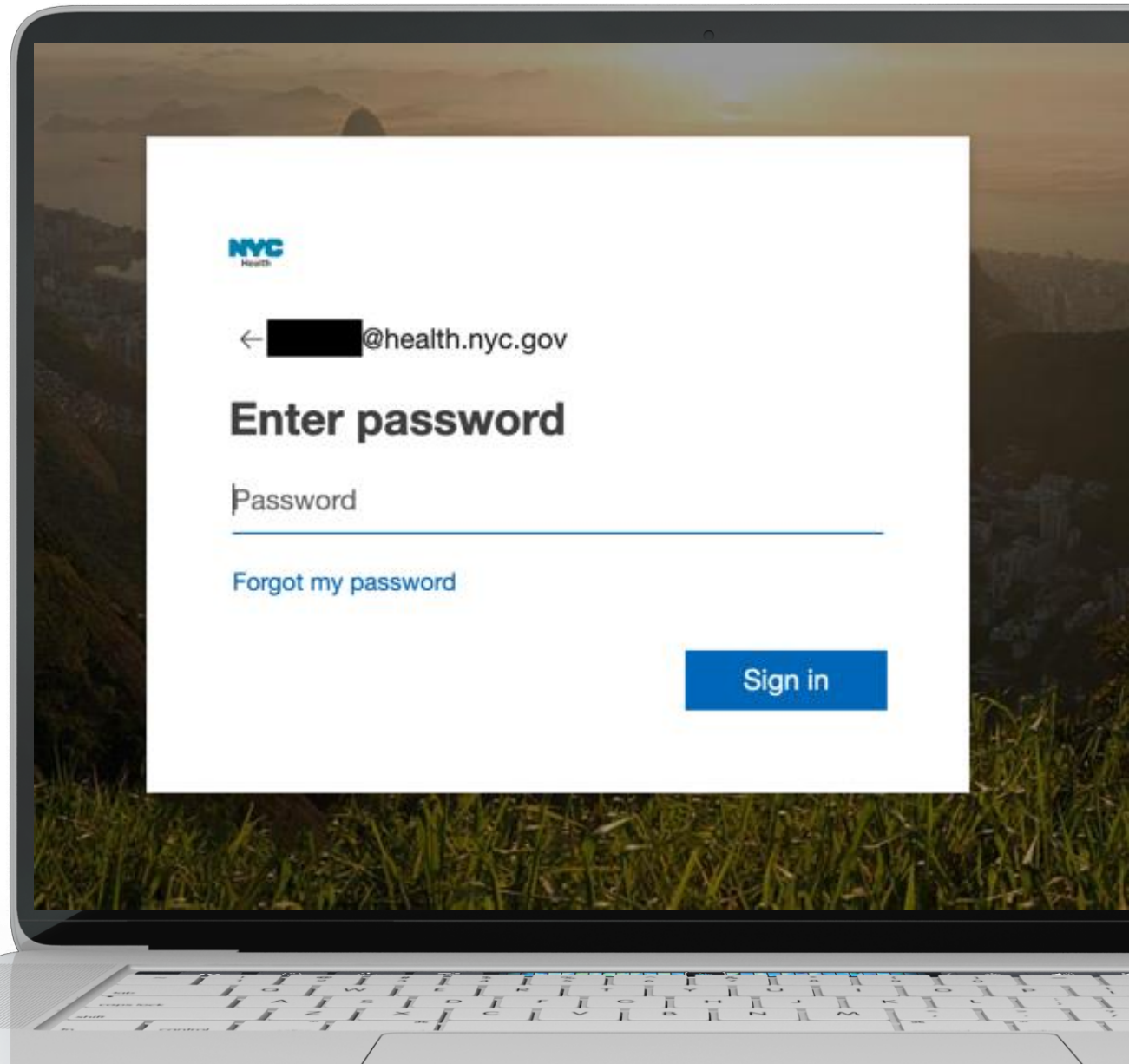
AUTHENTICATION DOMAINS

MICROSOFTONLINE BITFLIPS

Single Sign-On (SSO) Abuse

Intercepted dozens of password resets and login attempts per week

Captured usernames, passwords, and phone numbers used during authentication



Victim: NYC.gov via Microsoft SSO


```
POST / HTTP/1.1
Host: passwordreset.misrosoftonline.com
Accept: */*
Content-Length: 4793
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Cookie: CookiesSupportedCookie=True;
ASP.NET_SessionId=jt40orkjm0ldpjyp43rsuegw; flt=Iris; BannerLogoUrl=;
SessionId=sonjsyvgeosmktykrnwhubqd;
TrackingId=1d9f3b0095ce4f9ba081e1e69af3a0ff;
WorkflowConsistencyCheck=63689285984614677 8; x-ms-gateway-dc=EUS; x-ms-gateway-
env=PROD; x-ms-gateway-su=a
Origin: https://passwordreset.misrosoftonline.com
Referer: https://passwordreset.misrosoftonline.com/
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/73.0.3683.86 Safari/537.36
X-Microsoftajax: Delta=true
X-Requested-With: XMLHttpRequest
```

Victim: NYC.gov via Microsoft SSO


```
ctl00$ScriptManagerMain=ctl00$ContentPlaceholderMainContent$UpdatePanelMain|ctl
00$ContentPlaceholderMainContent$ButtonNext
__LASTFOCUS=
__EVENTTARGET=ctl00$ContentPlaceholderMainContent$ButtonNext
__EVENTARGUMENT=
__VIEWSTATE=...snippet...
__VIEWSTATEGENERATOR=CA0B0334
__VIEWSTATEENCRYPTED=
__EVENTVALIDATION=...snippet...
ctl00$ContentPlaceholderMainContent$TextBoxPassword1=E--REDACTED--!
ctl00$ContentPlaceholderMainContent$TextBoxPassword2=E--REDACTED--!
ctl00$ContentPlaceholderMainContent$CurrentViewName=ViewNewPassword
ctl00$ContentPlaceholderMainContent$LiveCaptchaMode=Image
ctl00$ContentPlaceholderMainContent$WorkflowConsistencyCheck=63689285550306518 2
ctl00$CorrelationID=0c79cd97-4f64-4cb3-858d-df668335eb25
ctl00$OrgIdUserName=REDACTED@health.nyc.gov
ctl00$OrgIdTenantDomain=
ctl00$NameCoexistenceAccount=
__ASYNCPOST=true
```

Victim: Dialog.lk via Microsoft SSO

```
POST / HTTP/1.1
Host: passwordreset.microsoftonlind.com
Content-Length: 1901
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Cookie: flt=Iris; CookiesSupportedCookie=True;
SessionId=v4habso3dvjg0foiadx1nb4i;
TrackingId=77ccd32b142b4243910076d17437613c;
ASP.NET_SessionId=htcwq3sm1u4pelut0iexsb3c; x-ms-gateway-dc=EUS; x-ms-gateway-
env=PROD; x-ms-gateway-su=a;
BannerLogoUrl=https://secure.aadcdn.microsoftonline-p.com/dbd5a2dd-
hdbnknj009h4yrwi9fy38-
8bdidayuif3v916ej4vhk/logintenantbranding/0/bannerlogo?ts=636066981069285032;
WorkflowConsistencyCheck=63689871647045652 3
Origin: https://passwordreset.microsoftonlind.com
Referer: https://passwordreset.microsoftonlind.com/
User-Agent: Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/72.0.3626.121 Safari/537.36
Via: HTTPS/1.1 proxy.dialog.dialoggsm.com AC161E19
X-Microsoftajax: Delta=true
X-Requested-With: XMLHttpRequest
```

Victim: Dialog.lk via Microsoft SSO


```
ctl00$ScriptManagerMain=ctl00$ContentPlaceholderMainContent$UpdatePanelMain|ctl
00$ContentPlaceholderMainContent$ButtonNext
__EVENTTARGET=ctl00$ContentPlaceholderMainContent$ButtonNext
__VIEWSTATE=...snippet...
__VIEWSTATEGENERATOR=CA0B0334
__EVENTVALIDATION=...snippet...
ctl00$ContentPlaceholderMainContent$TextBoxPassword1=S--REDACTED--9
ctl00$ContentPlaceholderMainContent$TextBoxPassword2=S--REDACTED--9
ctl00$ContentPlaceholderMainContent$CurrentViewName=ViewNewPassword
ctl00$ContentPlaceholderMainContent$LiveCaptchaMode=Image
ctl00$ContentPlaceholderMainContent$WorkflowConsistencyCheck=63689871647045652 3
ctl00$CorrelationID=77ccd32b-142b-4243-9100-76d17437613c
ctl00$OrgIdUserName=REDACTED@dialog.lk
ctl00$OrgIdTenantDomain=
ctl00$NameCoexistenceAccount=
__ASYNCPOST=true
```

Victim: SCC via Microsoft SSO


```
POST / HTTP/1.1
Host: passwordreset.microsofponline.com
Content-Length: 2622
Content-Type: application/x-www-form-urlencoded
Cookie: flt=Iris; CookiesSupportedCookie=True;
SessionId=zepksk0joi3epee2ez353h3b;
TrackingId=5a5ce80770814f6bacb465a77c50d4e4;
ASP.NET_SessionId=ondfuinlf5xmeh2f4omzdm5w; x-ms-gateway-dc=EUS; x-ms-gateway-
env=PROD; x-ms-gateway-su=b; BannerLogoUrl=;
WorkflowConsistencyCheck=636903074814782645
Origin: https://passwordreset.microsofponline.com
Referer: https://passwordreset.microsofponline.com/
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 6.1; Win64; x64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/72.0.3626.121 Safari/537.36
```

Victim: SCC via Microsoft SSO


```
ctl00$ContentPlaceholderMainContent$MultigateAuthenticationControl_Instance$Pho
neGateControl_Office$PhoneGateControl_PhoneNumberValidationBox=--REDACTED--2452
...snippet...
ctl00$ContentPlaceholderMainContent$CurrentViewName=ViewMultigateUserControl
ctl00$ContentPlaceholderMainContent$LiveCaptchaMode=Image
ctl00$ContentPlaceholderMainContent$WorkflowConsistencyCheck=636903074814782645
ctl00$CorrelationID=5a5ce807-7081-4f6b-acb4-65a77c50d4e4
ctl00$OrgIdUserName=REDACTED@fr.scc.com
ctl00$OrgIdTenantDomain=
ctl00$NameCoexistenceAccount=
__EVENTTARGET=ctl00$ContentPlaceholderMainContent$MultigateAuthenticationContro
l_Instance$PhoneGateControl_Office$PhoneGateControl_ButtonSend
```

Victim: Shell via Microsoft SSO

```
GET /db1e96a8-a3da-442a-930b-235cac24cd5c/oauth2/authorize?client_id=b8870aea-
69be-41ab-9597-
20ea98f260af&redirect_uri=https%3a%2f%2fhub.shell.com%2f&response_mode=form_pos
t&response_type=code+id_token&scope=openid+profile+email&state=OpenIdConnect.Au
thenticationProperties%3doa7JrwOKyMd7OzDdc7GC6h5WQXQS6oU9UVgoPf8KqDu-
9wXcmXbWGPux_4LegyVzxrcWTwBovONc0emBuC3tMFWCuLgNpjrLGZWUVeUYcsfTp0J5QbFCwKp93ZA
Mb_mWTigJUxlMoJv_-0noaZGNdG7ExFyA2g3Zz7nHfs7GMWe4whMID5Fs2M3o-
lxZEEwmEVKI04zMpkP217sXPCdWBXk5vMOSvZJfj2JCbvWyBsbPET_WZ1_EQNIEkmrjInot&nonce=6
36894866829597824.YzI5MzNhYWQtOTkwOS00Njg1LWIxMzAtZDRlNDc0YjIwYzgwYjY1ZDMxZmMtN
jUyZi00NTdiLTgxZTMtNjBiZmY4YzMzMTI3 HTTP/1.1
Host: login.micrgsoftonline.com
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*
;q=0.8,application/signed-exchange;v=b3
Cookie: _sm_au=aaaaaaaaaaaaaaaaaaaa
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 6.1) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/73.0.3683.86 Safari/537.36
X-Forwarded-For: 134.163.57.49, 165.225.35.5
```

Victim: YouTube via Google APIs

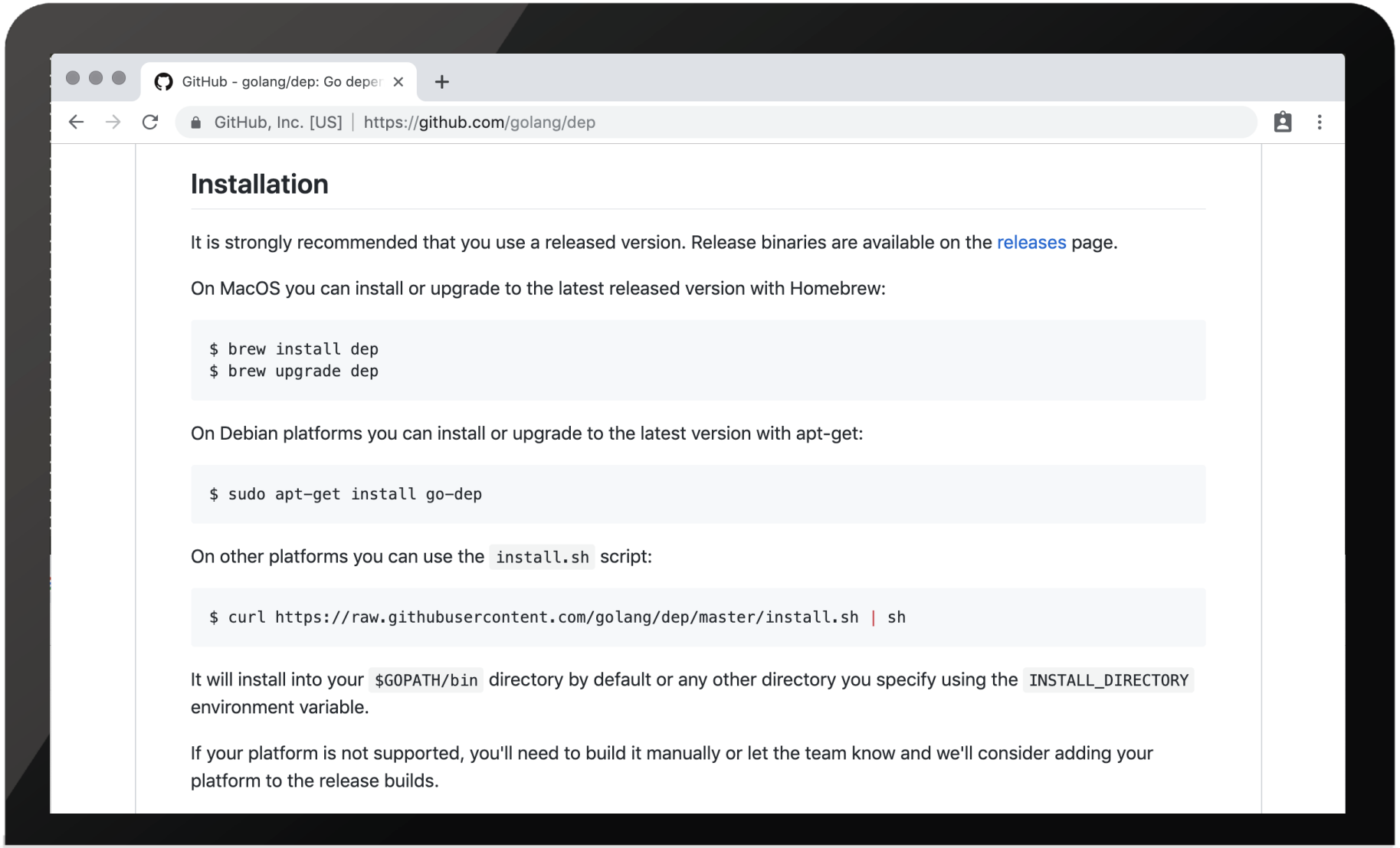
```
POST /youtubei/v1/log_event?key=AIzaSyB-63vPrdThhKuerbB2N_l7Kwwcxj6yUAc
HTTP/1.1
Host: ynutubei.foogleapis.com
Accept-Language: da-dk
Authorization: Bearer ya29.GtUB3AbMdUNuIQyxCqjffE8WleW4WqU—REDACTED—
cvsA0ite3GfoDM
Content-Length: 8308
Content-Type: application/x-protobuf
User-Agent: com.google.ios.youtube/14.11.8 (iPhone7,2; U; CPU iOS 12_1_2 like
Mac OS X; da_DK)
X-Forwarded-For: 85.202.21.158
X-Goog-Api-Format-Version: 2
X-Goog-Device-Auth:
device_id=AEQ63XEPEr4HzUJzF+T9dTx8g++7NidXjZ8FYx15gN8Qv29Lt8psytlG+9aQn/SDGSKRw
iBnzCZEtCypdg1SigmRyh5yfrgwbQUImgkfT388Pe1hOB9T3xQaplUUEUx3iIaMzCZFMLUdEQ,data=
AFjJpFR6R7+n,content=AFjJpFTPjcPtqqqoMiDdxzHJmQm5iT3JMw
X-Goog-Visitor-Id: Cgt5dERMalBhQWpJMCik1vnkBQ%3D%3D
```

HOW TO GET
RCE

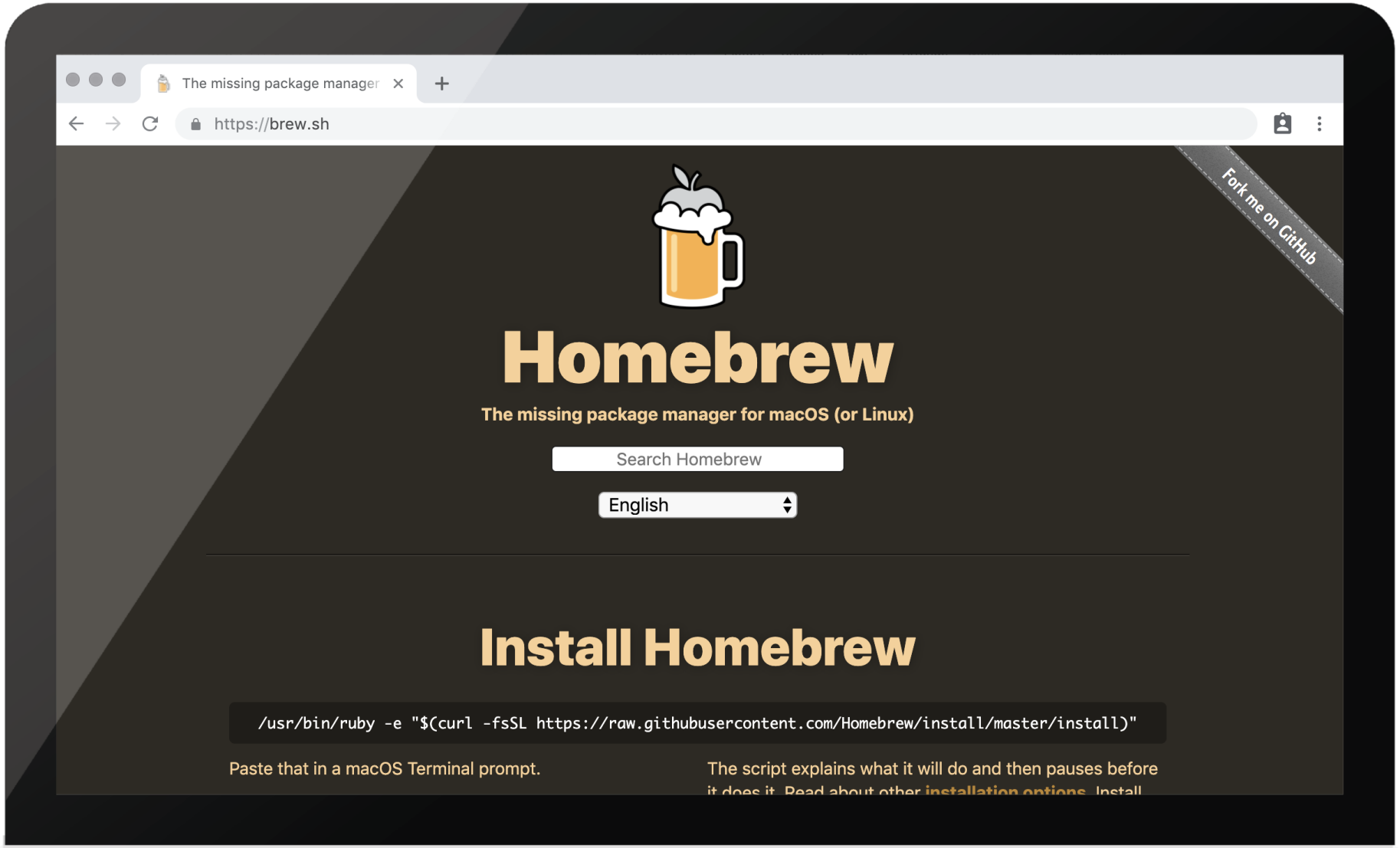
Victim: Install via Github

...
http://raw.githubusercon**v**ent.com/Angristan/OpenVPN-install/master/openvpn-install.sh
https://raw.github**e**sercontent.com/Security-Onion-Solutions/elk-test/master/securityonion_elsa2elk.sh
https://raw.githubuserc**k**ntent.com/kada115/bukan-untuk-umum/master/instatools.sh
https://raw.githubuserconta**n**t.com/alexa/avs-devive-sdk/master/tools/Install/pi.sh
https://raw.githubuserconta**n**t.com/diyhue/diyHue/master/BridgeEmulator/easy_install.sh
https://raw.githubuserconta**n**t.com/docker-32bits/ubuntu/master/buildimage.sh
https://raw.githubuserconta**n**t.com/Hax4us/metasploit_termux/master/metasploit.sh
https://raw.githubuserconta**n**t.com/jeedom/core/master/install.sh
https://raw.githubusercontend**d**.com/MichMich/MagicMirror/master/installers/raspberry.sh
https://raw.githubusercontend**d**.com/Zer0CoolX/guacamole-install-rhel/master/guac-install.sh
https://raw.githubuser**g**ontent.com/creationix/nvm/v0.34.0/install.sh
https://raw.githubuser**s**ontent.com/robbyrussell/oh-my-zsh/master/tools/install.sh
https://r**e**w.githubuserconta**n**t.com/alexa/avs-devi**v**e-sdk/master/tools/Install/setup.sh
https://raw.**f**ithubusercontent.com/Homebrew/install/master/install
https://raw.github**e**sercontent.com/Homebrew/install/master/install
https://raw.githubu**q**ercontent.com/Homebrew/install/master/install

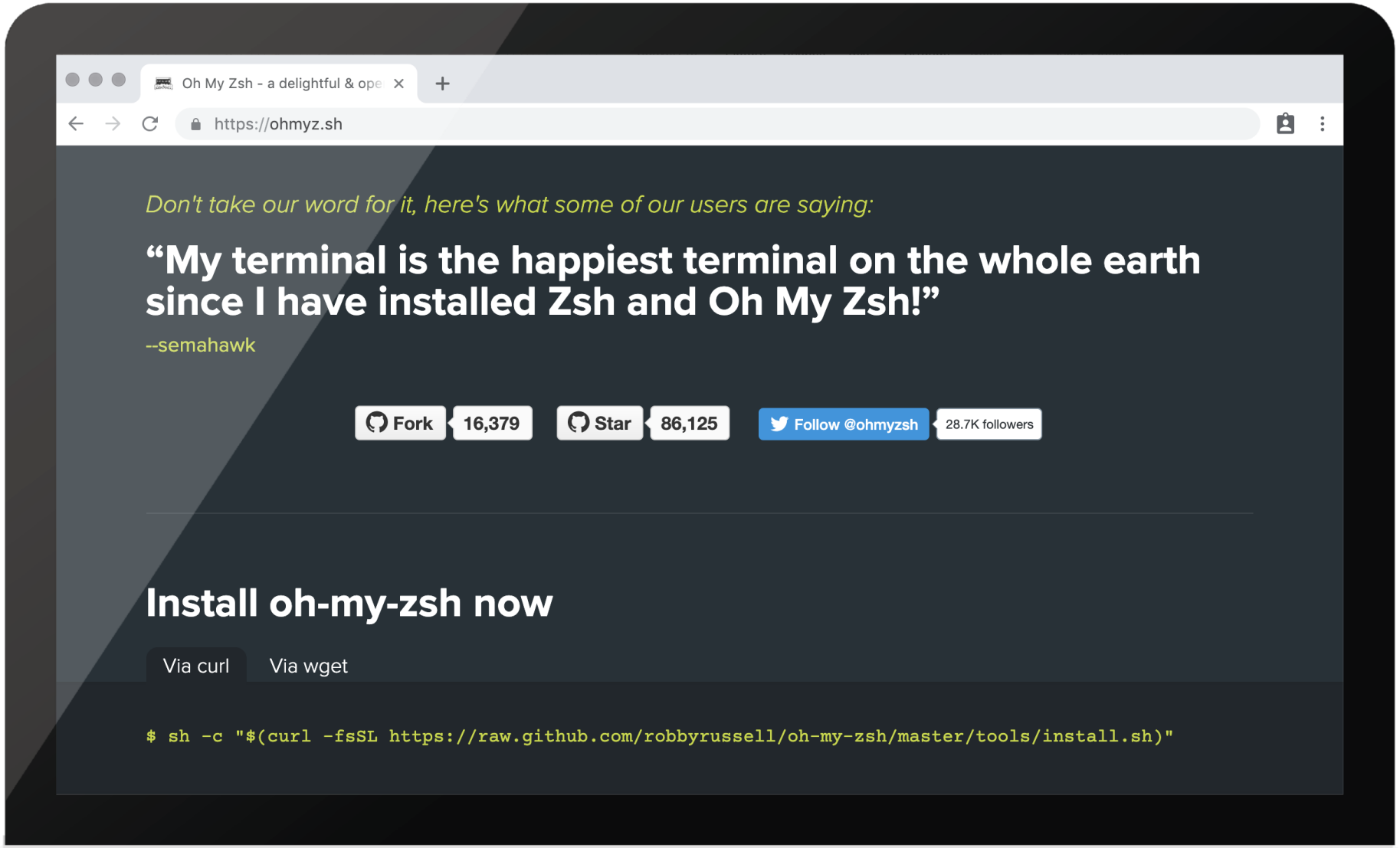
GITHUBUSERCONTENT.COM DIRECTLY TO RCE



GITHUBUSERCONTENT.COM DIRECTLY TO RCE



GITHUBUSERCONTENT.COM DIRECTLY TO RCE

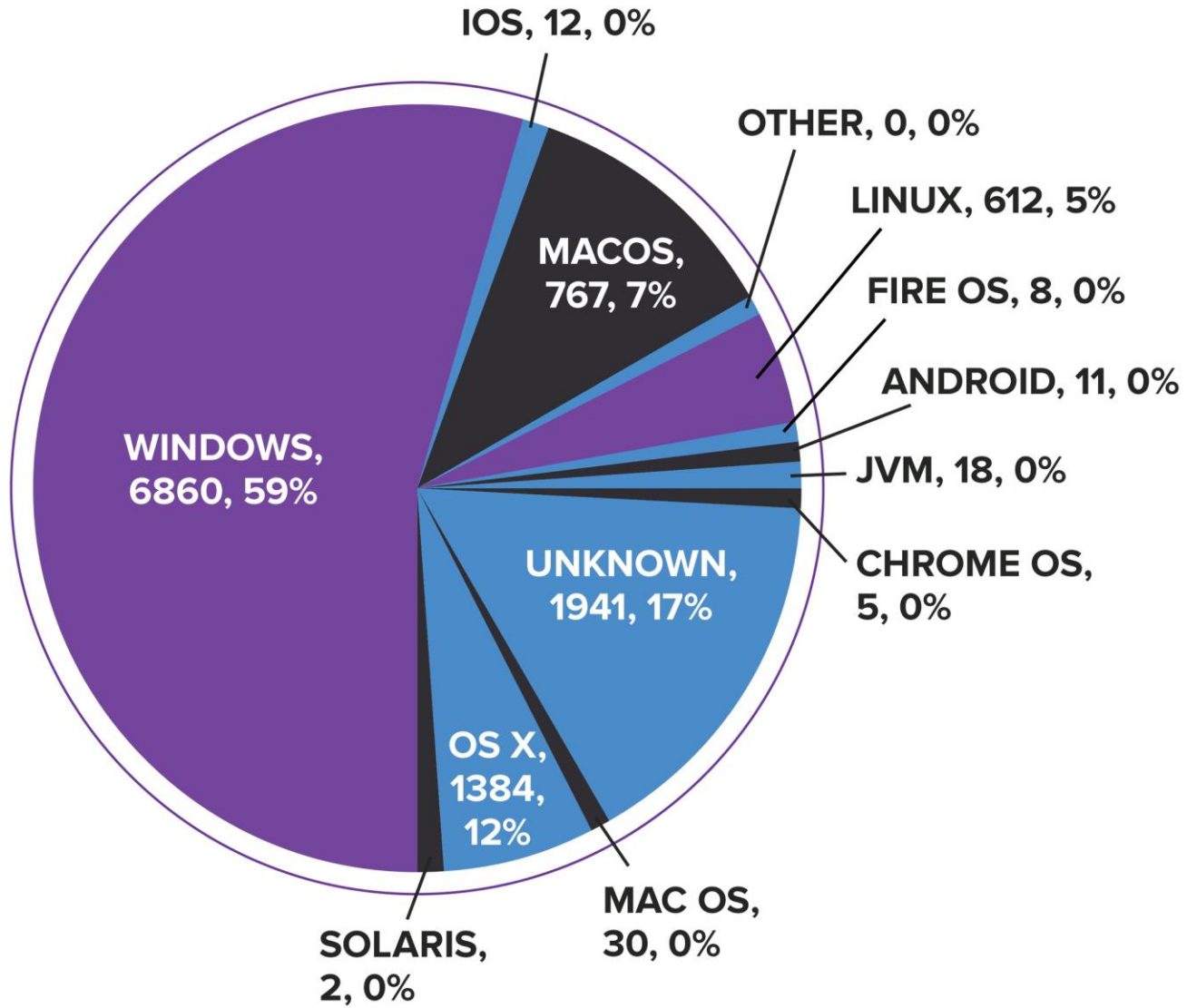


OBSERVATIONS
WHAT DID WE SEE?

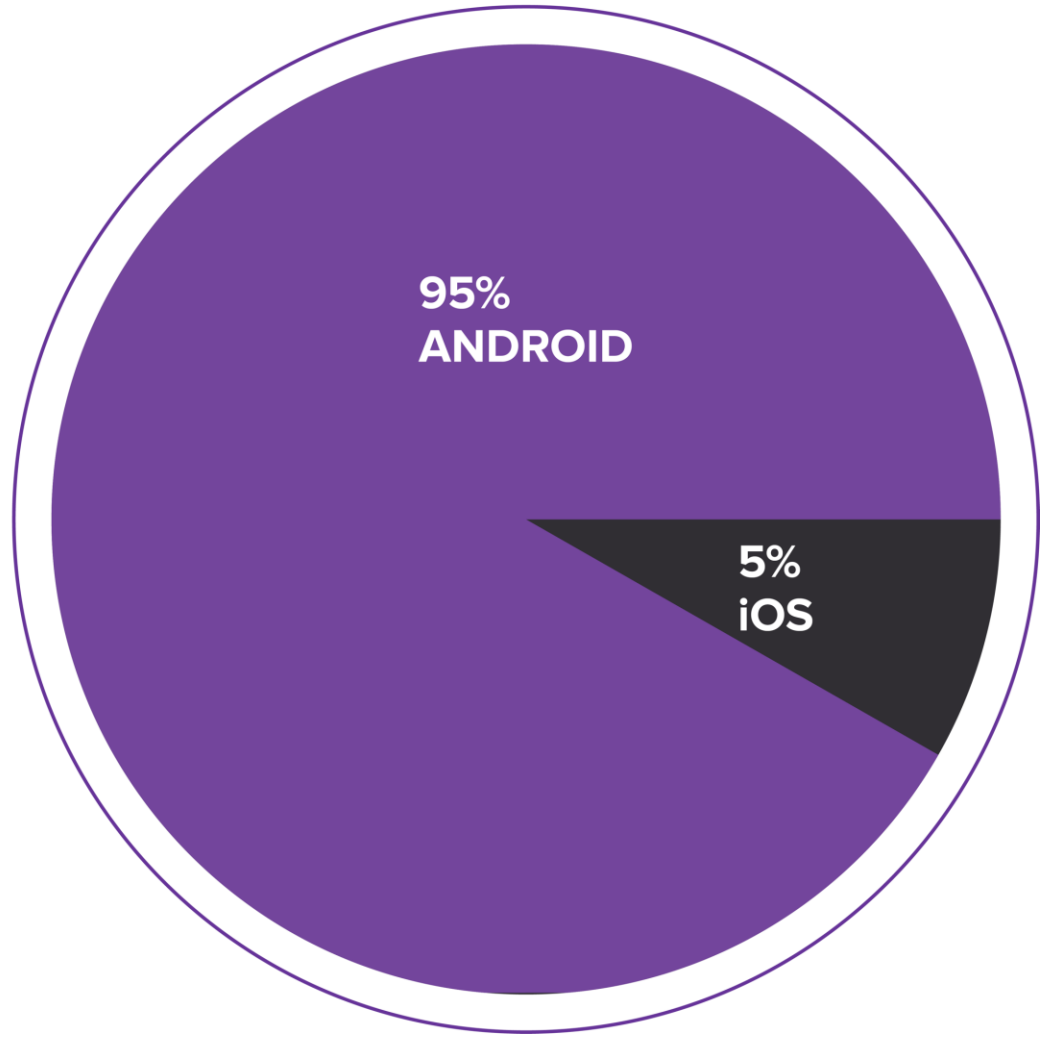
BISHOPFOX

WHERE THIS IS **HAPPENING**

USER-AGENTS
OBSERVED



MOBILE USER-AGENTS OBSERVED



OBSERVATIONS
WHO ELSE IS LISTENING?

BISHOPFOX

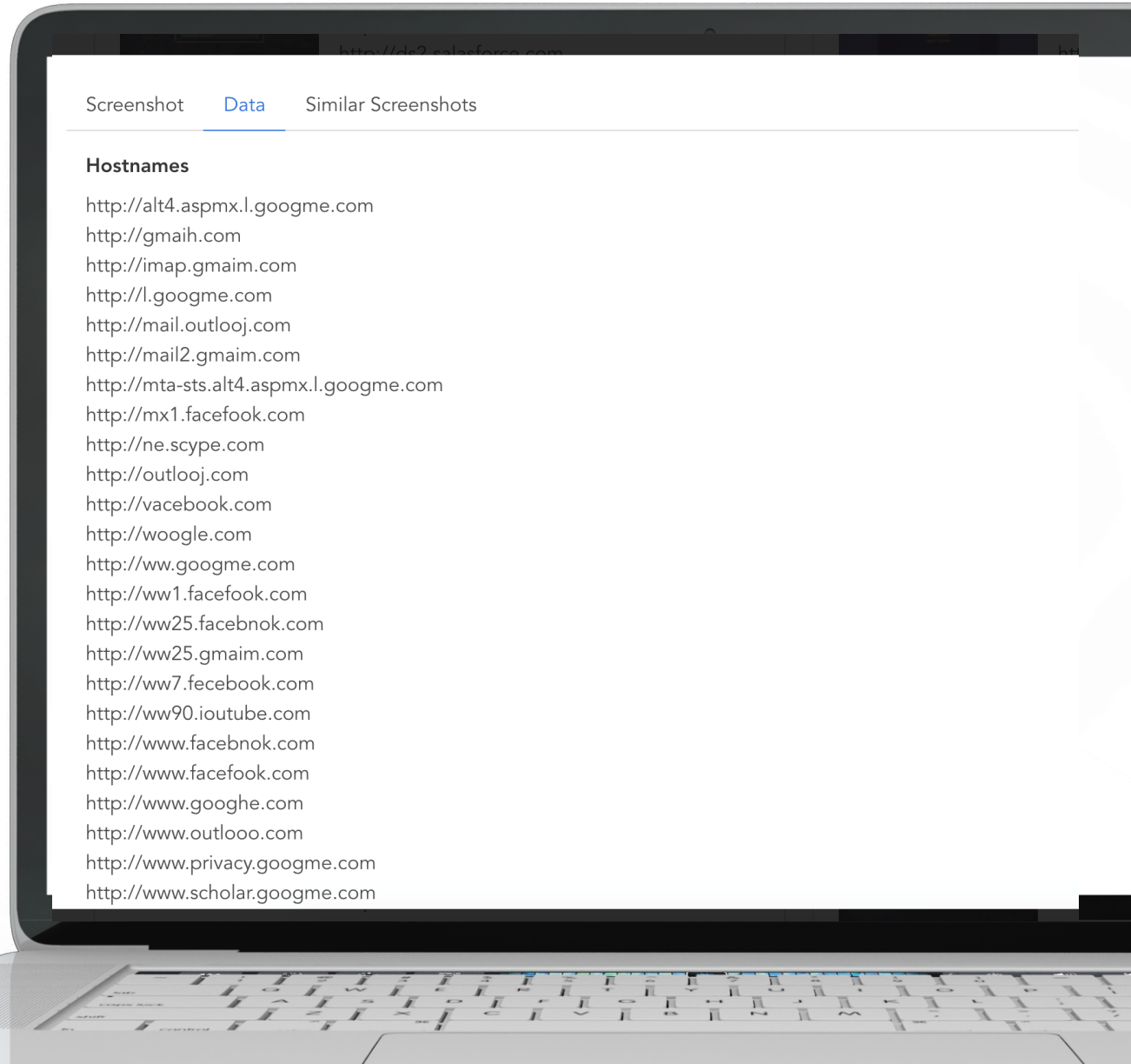
MONITORING BITFLIPS

CONTINOUSLY INSPECT SERVICES

Subdomain discovery

Service discovery (HTTPS, SMTP, DNS)

Captured screenshot of application



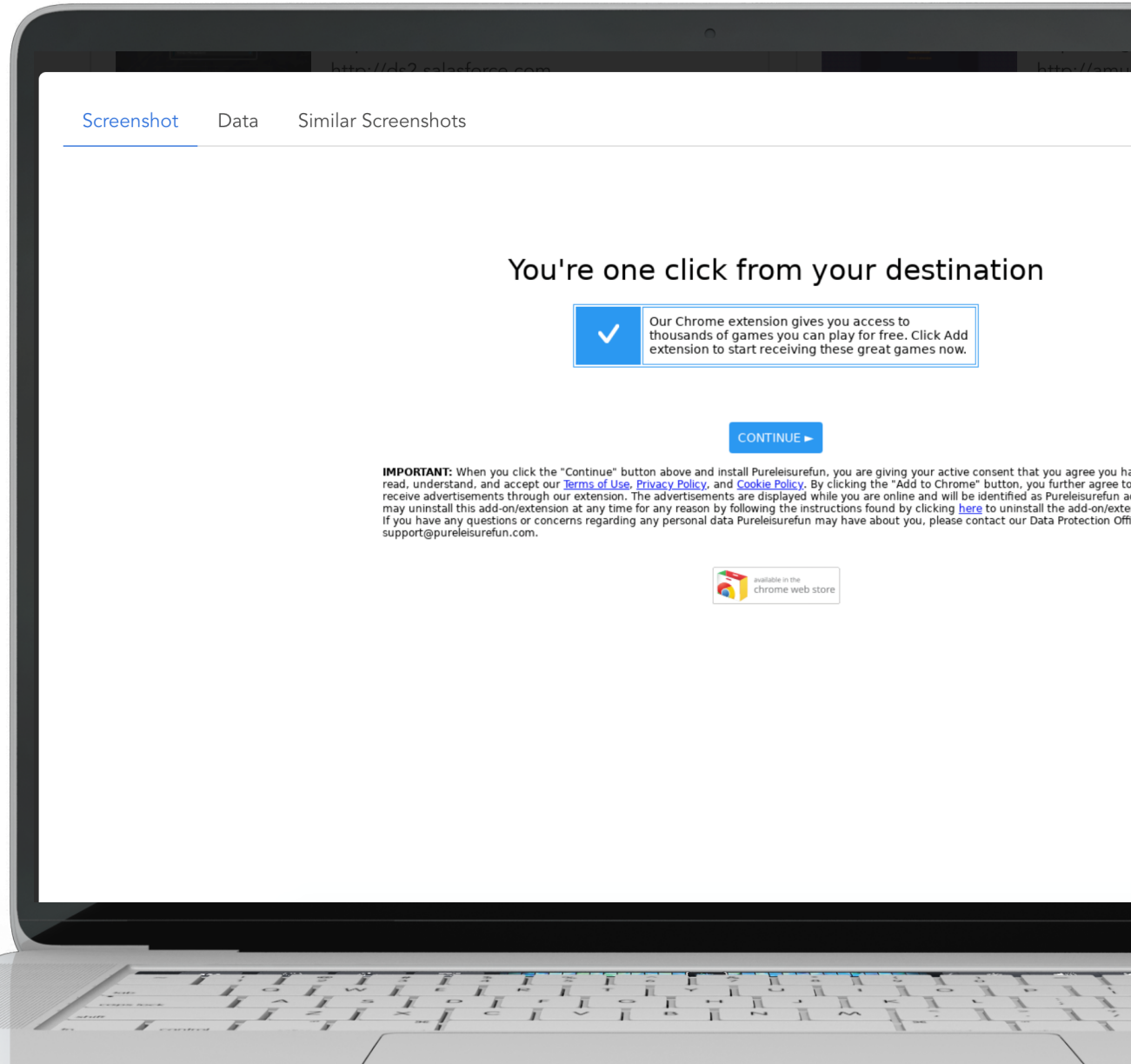
MONITORING BITFLIPS

CONTINOUSLY INSPECT SERVICES

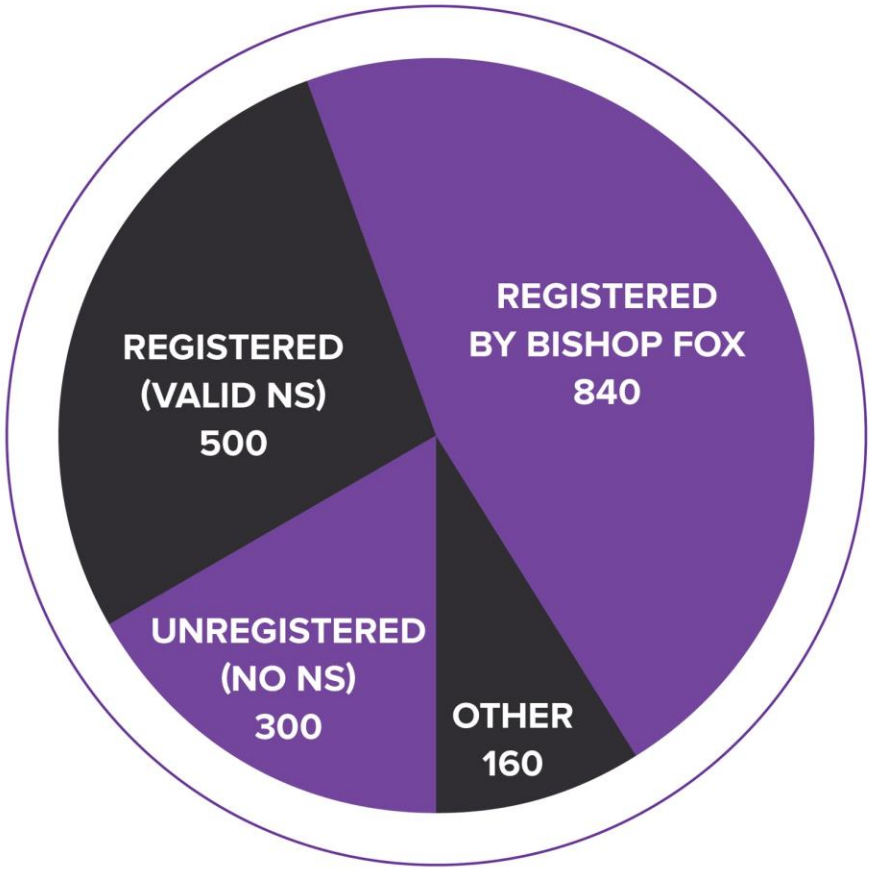
Malicious Chrome Extensions

Requests permission to all sensitive content

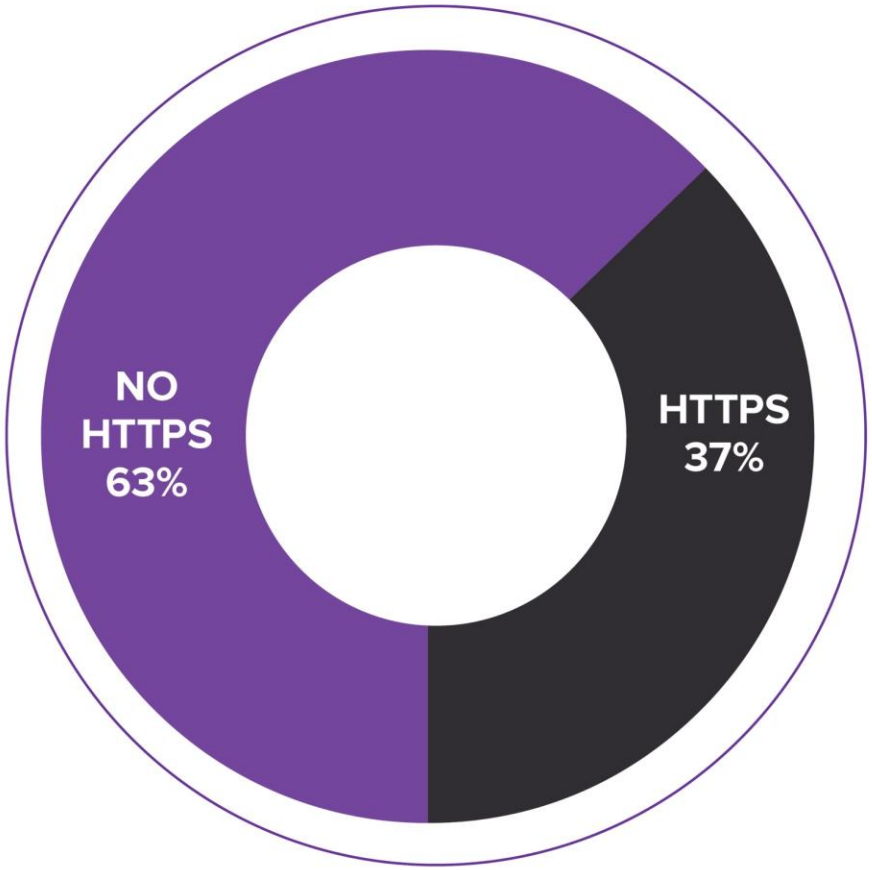
Compromise all of clients traffic



BITFLIP REGISTERED SATURATION



HTTPS ON REGISTERED BITFLIP DOMAINS



RECOMMENDATIONS & MITIGATIONS
DEFENSE TACTICS

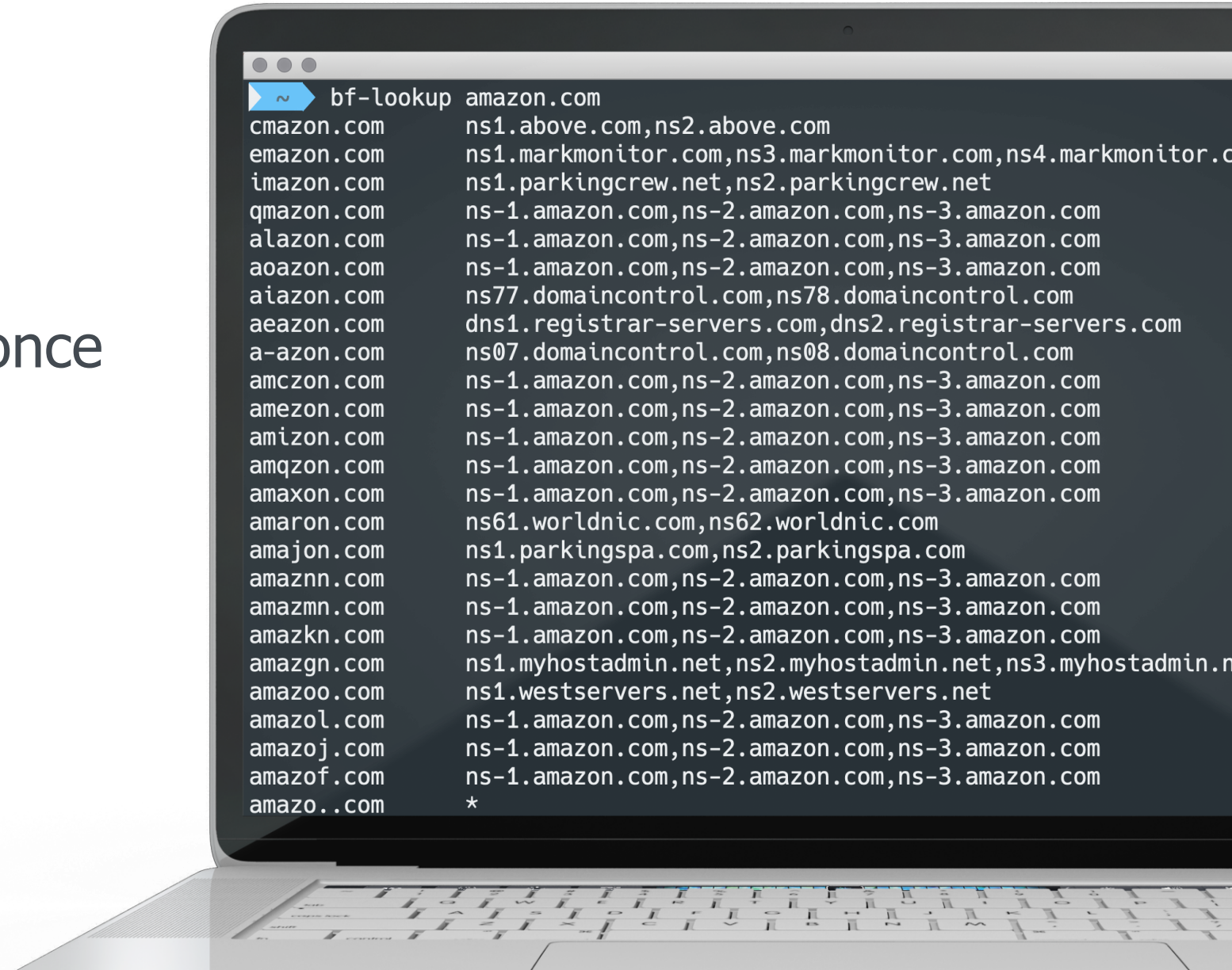
BISHOPFOX

DEFENSIVE DOMAIN REGISTRATION

STOP BIT SQUATTERS

Register All Bitflip Variations

Seize control of domains once others are listening



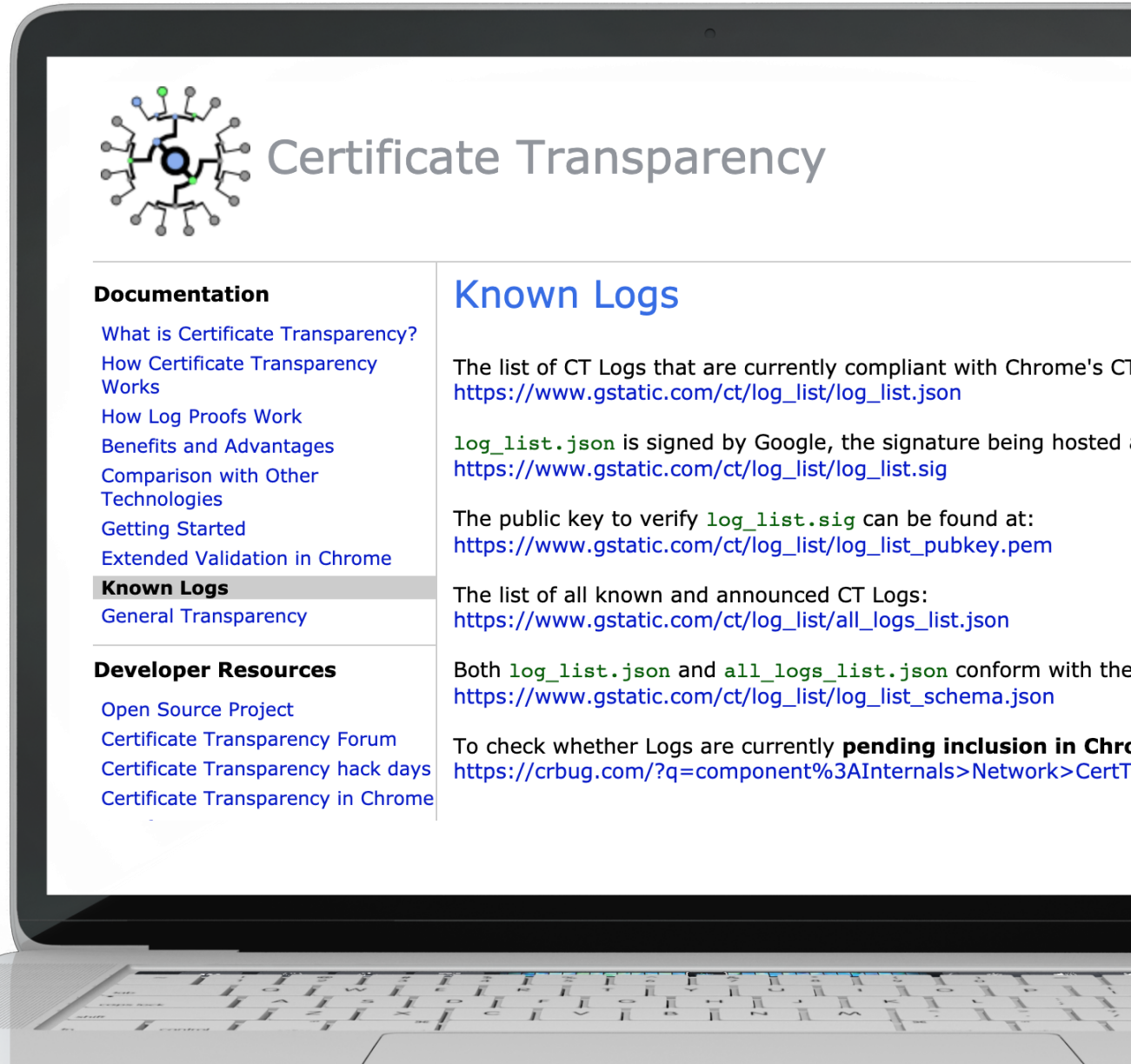
CERTIFICATE TRANSPERENCY

MONITOR CTL FOR WILDCARD CERTIFICATES

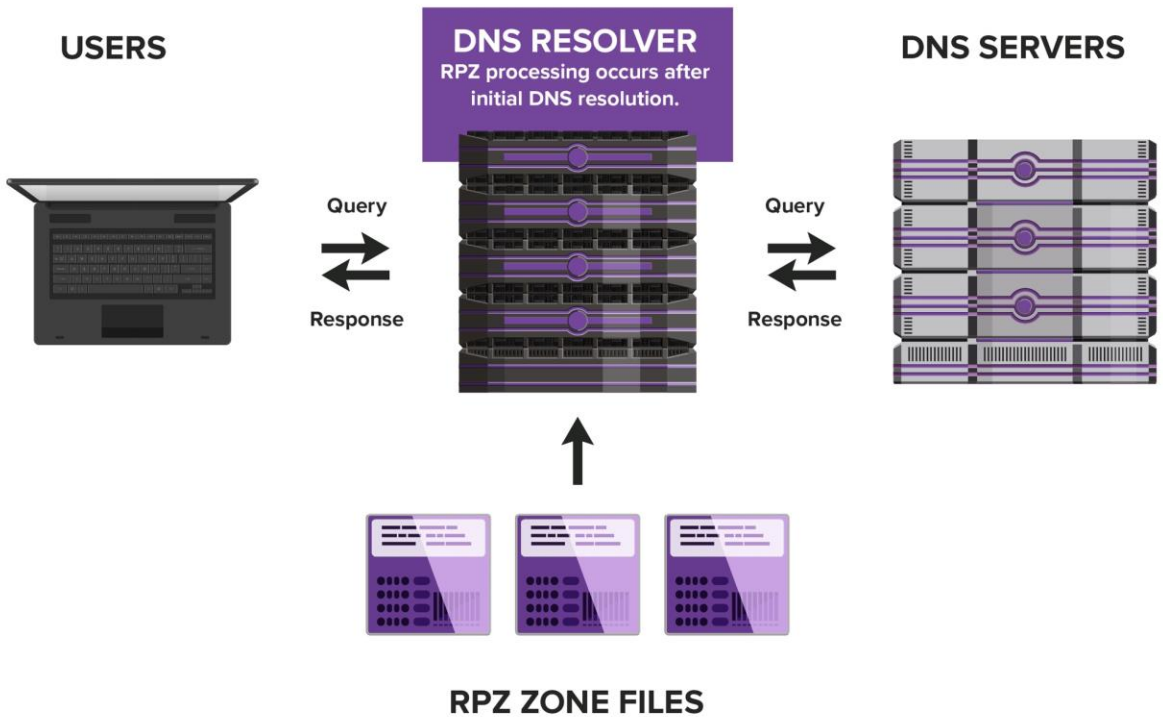
Malicious CTL Activity

Indicates threat is planning to intercept sensitive traffic

Set alerts for domains you rely on for secure communication



RESPONSE POLICY ZONE (RPZ)



CONTROL DNS RESPONSES

- DNS filtering to override global resolutions and control what your systems can access
- Generate a list of bitflips that you want to ensure resolve to the correct site and apply that ruleset to your organizations DNS resolvers
- Rewrite responses to send users to a walled garden

Victim: Every 20 minutes…

```
POST /Microsoft-Server-ActiveSync?jAkHBBA22TTYxUdjsTN/vFqGT1aWBAAAAAACV1A=
HTTP/1.1
Host: apidat.googleusercontend.com
Authorization: RPSToken
t=EwAgA91JBAAUXVHTgKyJm1pMwJWonrGcwEzI3LwAAUPhkqiHOGW7gMuZjvEnv+OjIsmNjNCl7Glgh
oWxYkSkWH3n757kphPuxeERn…snippet…/u36OJ2QCp97zpI6avas6VScgG0i19keW8e38Rb8FF7ej1
nNObcTFMpYILg9DnFqzI5A32N3oXUirXauGRENlm4UC15JA3ZhlnSBEupUtBGUloR8qATi2IXd1IuaI
OXt44MkPohpQbvULEeDsYyMeKC9G5xbI6ejWAssQfr5KgI=&p=
Content-Length: 64
Content-Type: application/vnd.ms-sync
Pragma: no-cache
X-Forwarded-For: 109.42.2.6
X-Ms-Wl: WindowsPhone/8.0
X-Wlas-Tracing: true

jVR2?EFGSIDFGDomainIdFGInternalFolderType
```

Victim: Every 20 minutes…

```
OPTIONS /Microsoft-Server-
ActiveSync?User=lenzthomas161&DeviceId=36D934D8C54763B1337FBC5A864F5696&DeviceT
ype=WP HTTP/1.1
Host: apidat.googleusercontend.com
Authorization: RPSToken
t=EwAgA91JBAAUXVHTgKyJm1pMwJWonrGcwEzI3LwAAUPhkqiHOGW7gMuZjvEnv+OjIsmNjNCl7Glgh
oWxYkSkWH3n757kphPuxeERn…snippet…/u36OJ2QCp97zpI6avas6VScgG0i19keW8e38Rb8FF7ej1
nNObcTFMpYILg9DnFqzI5A32N3oXUirXauGRENlm4UC15JA3ZhlnSBEupUtBGUloR8qATi2IXd1IuaI
OXt44MkPohpQbvULEeDsYyMeKC9G5xbI6ejWAssQfr5KgI=&p=
Cache-Control: no-cache
Ms-Asprotocolversion: 14.0
Pragma: no-cache
User-Agent: MSFT-WP/8.10.14219
X-Forwarded-For: 109.42.2.6
X-Ms-Wl: WindowsPhone/8.0
X-Wlas-Tracing: true
```

Calendar Sync: Every 30 minutes...

```
PROPFIND /caldav/v2/biancabonvivant%40gmail.com/user HTTP/1.1
Host: apidata.goocleusercontent.com
Accept-Encoding: gzip, deflate
Authorization: Bearer ya29.GmXlBuDism5sXX_--REDACTED--
oUy6aLVnaorcW8ZfEcxIRHOLVfrw
Cache-Control: no-cache
Content-Length: 144
Content-Type: text/xml
Depth: 0
Pragma: no-cache
User-Agent: MSFT-WIN-3/10.0.17134 (gzip)
X-Forwarded-For: 173.174.51.65
X-Forwarded-Port: 443
X-Forwarded-Proto: https

<?xml version="1.0" encoding="UTF-8"?><propfind xmlns="DAV:"><prop><calendar-
home-set xmlns="urn:ietf:params:xml:ns:caldav" /></prop></propfind>
```

PREVIOUS BIT FLIP RESEARCH

ADDITIONAL RESOURCES

DEF CON 23 - Luke Young - Investigating the Practicality and Cost of Abusing Memory Errors

https://www.youtube.com/watch?v=4b5disac9g4

Defcon 21 - Jaeson Schultz - Examining the Bitsquatting Attack Surface

https://www.youtube.com/watch?v=IhwE1S4x36s

DEFCON 19 – Artem Dinnaberg - Bit-squatting: DNS Hijacking Without Exploitation

https://www.youtube.com/watch?v=aT7mnSstKGs

Michael Brooks – Starnoise Research Project - rewirethe.net

QUESTIONS

BISHOPFOX