

Unveiling The Cloak

A behind-the-scenes look at what happens when you click that link



**ZERO
NIGHTS
2018**

AN ANNUAL EVENT OF THE
FUTURE

Who we are



Ilya Nesterov

Threat research scientist

facebook.

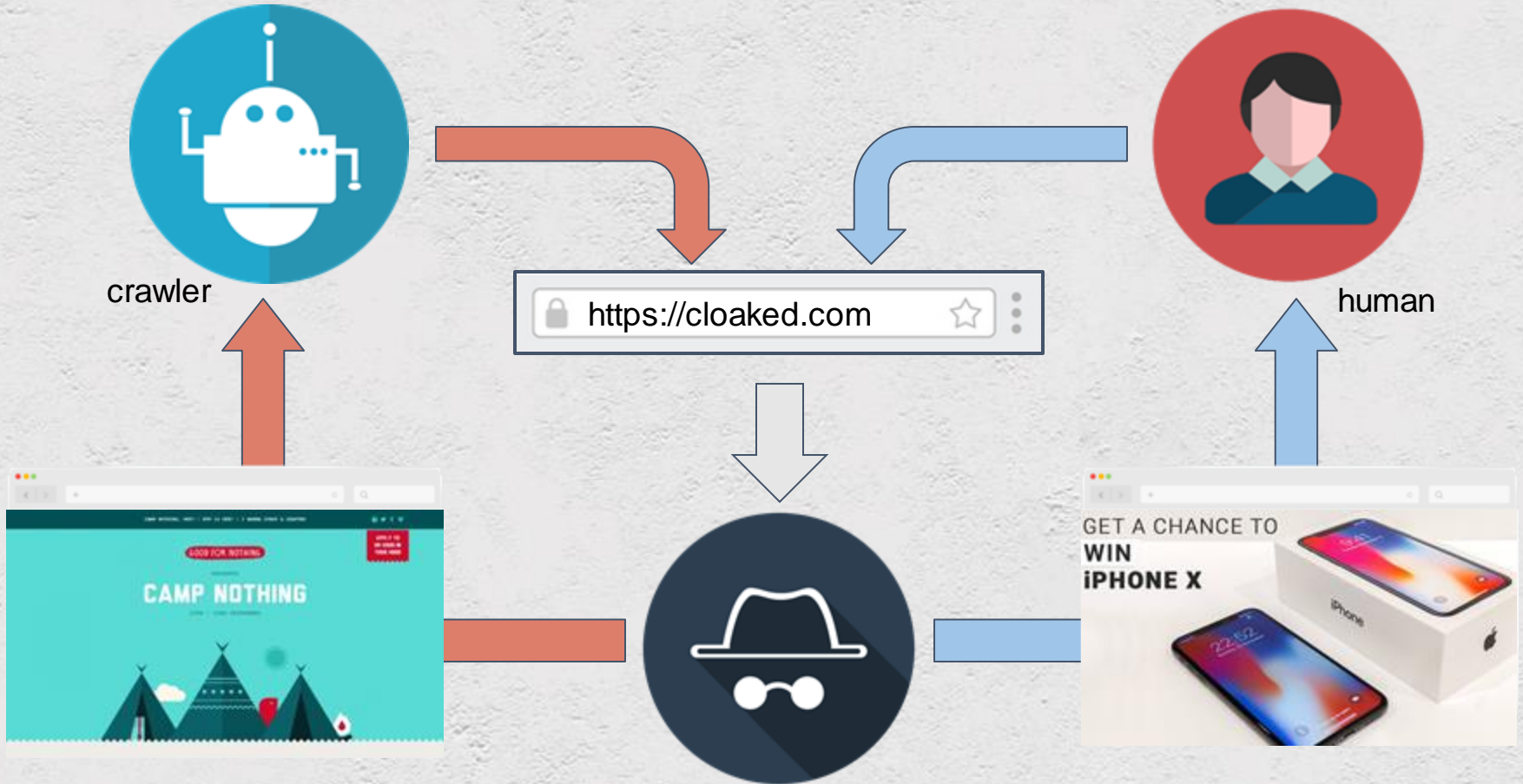


Sergey Shekyan

Software engineer

SH=PE

What is cloaking



Who use it and why

Pharmacy

Black SEO

Malware

Loans

Gamble

Phishing

Affiliate marketing

Crypto

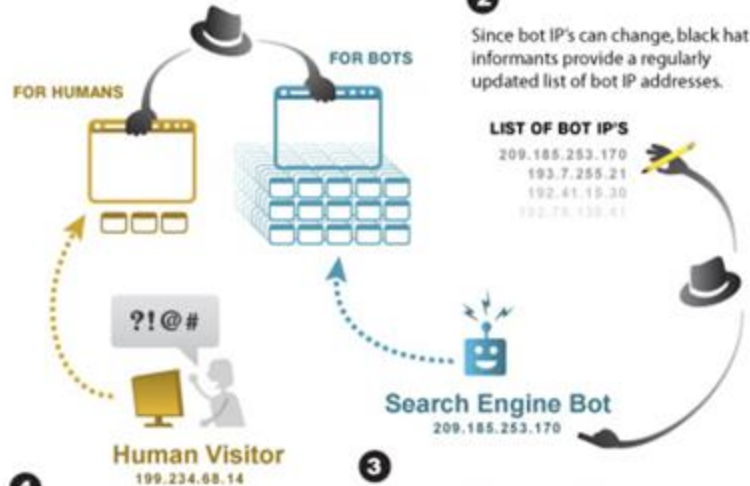
Illegal Services

Pay Per Click

Black Hat Cloaking Explained

1

Sites engaged in black hat SEO prepare two sets of content, one targeted for bots and the other targeted for human visitors. Bots are identified by their IP address.



2

Since bot IP's can change, black hat informants provide a regularly updated list of bot IP addresses.

LIST OF BOT IP'S

209.185.253.170
193.7.255.21
192.41.19.30
192.78.139.41

4

Human visitors often won't find the best information despite the site's high rankings.

3

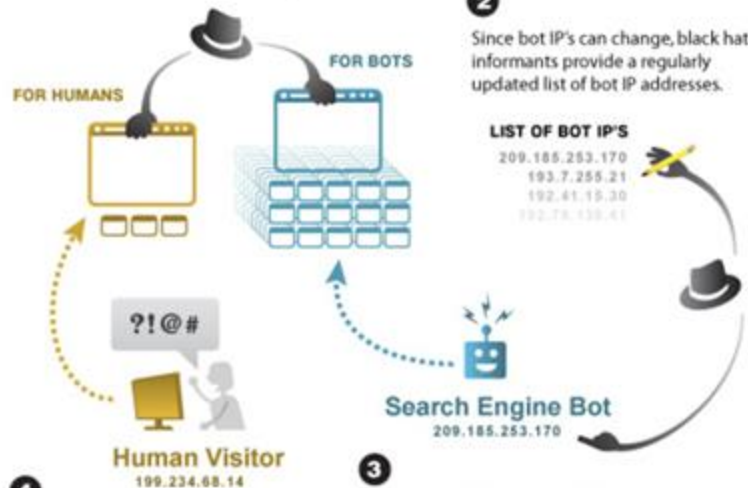
Bots are served abundant fabricated content packed with targeted keywords. This false information boosts rankings.

Cloaking in 2007

Black Hat Cloaking Explained

1

Sites engaged in black hat SEO prepare two sets of content, one targeted for bots and the other targeted for human visitors. Bots are identified by their IP address.



2

Since bot IP's can change, black hat informants provide a regularly updated list of bot IP addresses.

LIST OF BOT IP'S

209.185.253.170
193.7.255.21
192.41.15.30
192.79.136.41

3

Bots are served abundant fabricated content packed with targeted keywords. This false information boosts rankings.

4

Human visitors often won't find the best information despite the site's high rankings.

2

Since bot IP's can change, black hat informants provide a regularly updated list of bot IP addresses.

LIST OF BOT IP'S

209.185.253.170
193.7.255.21
192.41.15.30
192.79.136.41



Cloaking in 2007

Is it cloaking or fraud detection system?

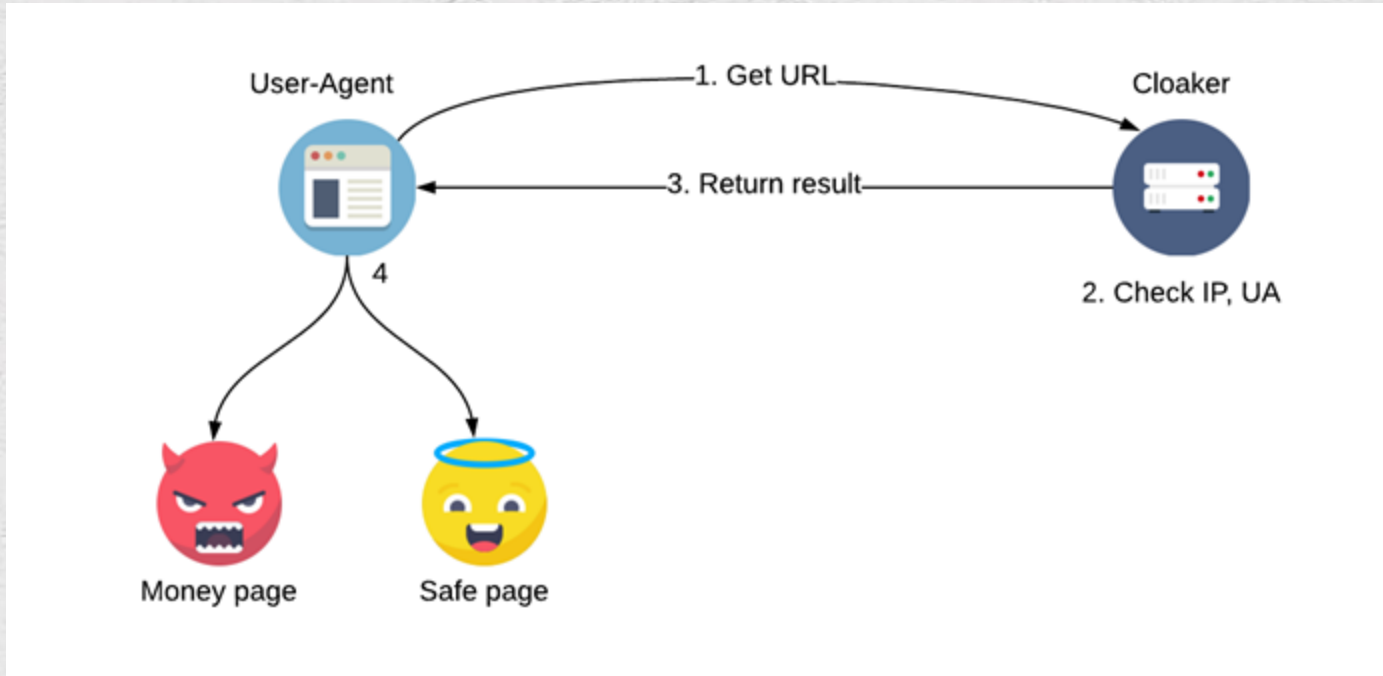
List of Features:

- ✔ Unlimited campaigns
- ✔ Detailed Click Log
- ✔ JavaScript CDN integration
- ✔ PHP integration
- ✔ WordPress plugin
- ✔ API access
- ✔ City level GEO Filter
- ✔ Fast IPv4/IPv6 Filter
- ✔ Weighted URL rotation for split testing
- ✔ Tracker integration
- ✔ URL query parameter filtering
- ✔ CSV exports
- ✔ Real-time stats with hourly granularity
- ✔ IP type filter - corporate, datacenter, residential etc.
- ✔ HTTP referrer filter and logs
- ✔ Device filter
- ✔ OS filter
- ✔ Browser filter
- ✔ ISP/ORG/Carrier filter
- ✔ User-Agent filter
- ✔ PageSentry - Protects landing page
- ✔ VisitorCap - Landing Page Frequency Capper
- ✔ CloakMatic - Smart Campaign Activator
- ✔ Custom Filters
- ✔ WebRTC-based IP Leak Detection
- ✔ IPv6 support
- ✔ Chat support

Cloaking in **2018**

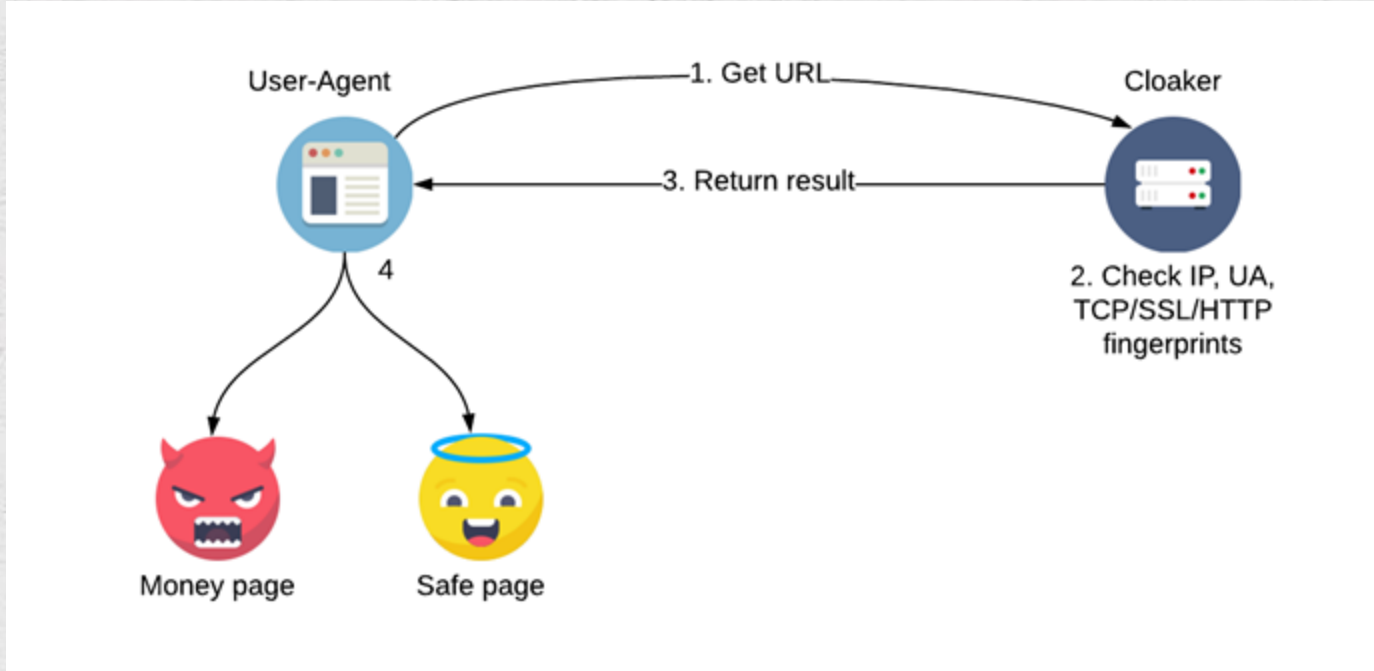
Cloaking systems classification

Detection based on source IP address information and UA



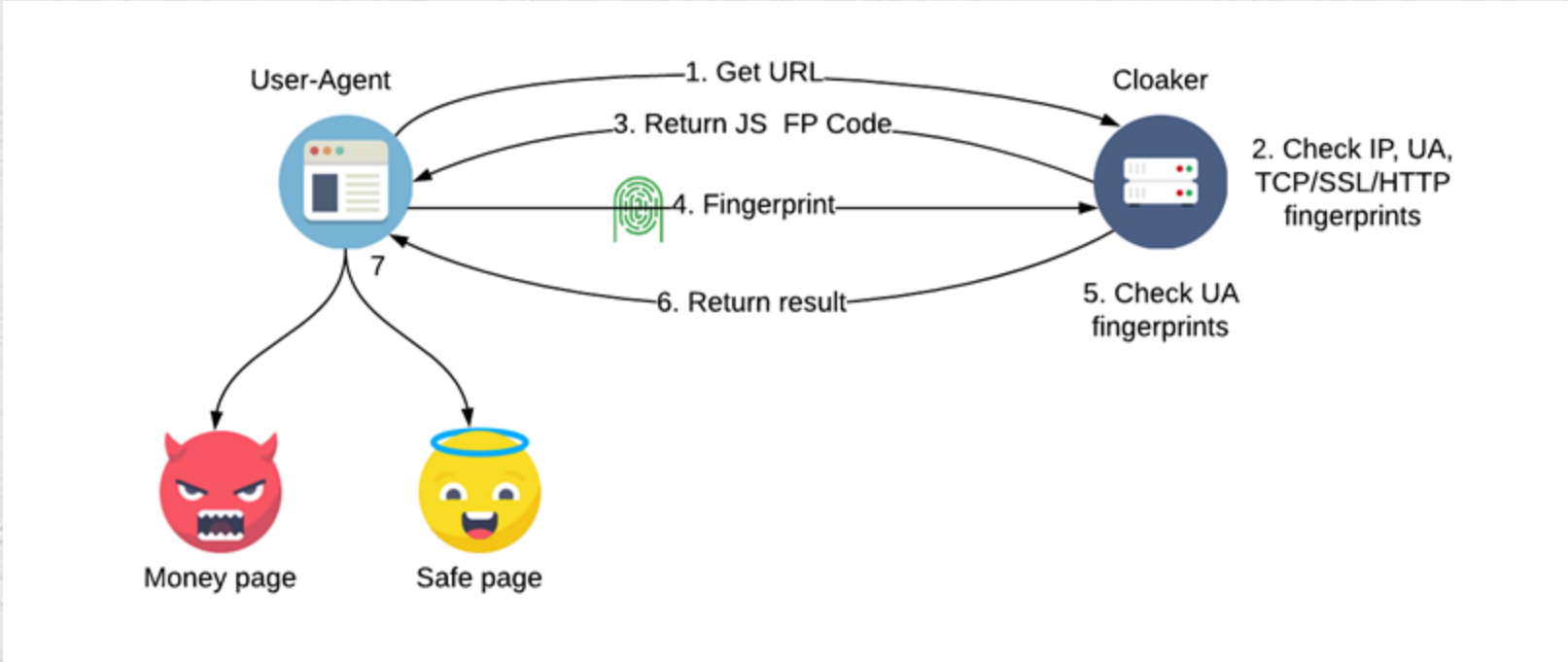
Naive Adversary

Leverage passive network stack fingerprinting: TCP/SSL/HTTP



Intermediate Adversary

Advanced adversary: UA fingerprinting



Advanced Adversary

Naive cloaking system example
linkscloaking.com

Links Cloaking

HOME ABOUT US HOW IT WORKS PRICING TERMS & CONDITIONS CONTACT

BASIC	ADVANCE	PRO
\$80 / Month	\$120 / Month	\$150 / Month
10 Campaigns / day	20 Campaigns / day	Unlimited Campaigns / day
7000 Links hits	15000 Links hits	Unlimited Links hits
Change link status / No	Change link status / yes	Change link status / yes
Detail log / No	Detail log / No	Detail log / yes
Access to all Networks	Access to all Networks	Access to all Networks
Live support 12 hr	Live support 18 hr	Live support 24 hr
Facebook Groups/Pages sharing	Facebook Groups/Pages sharing	Facebook Groups/Pages sharing
ADS Network (Google/Facebook/Bing/Yahoo etc.)	ADS Network (Google/Facebook/Bing/Yahoo etc.)	ADS Network (Google/Facebook/Bing/Yahoo etc.)

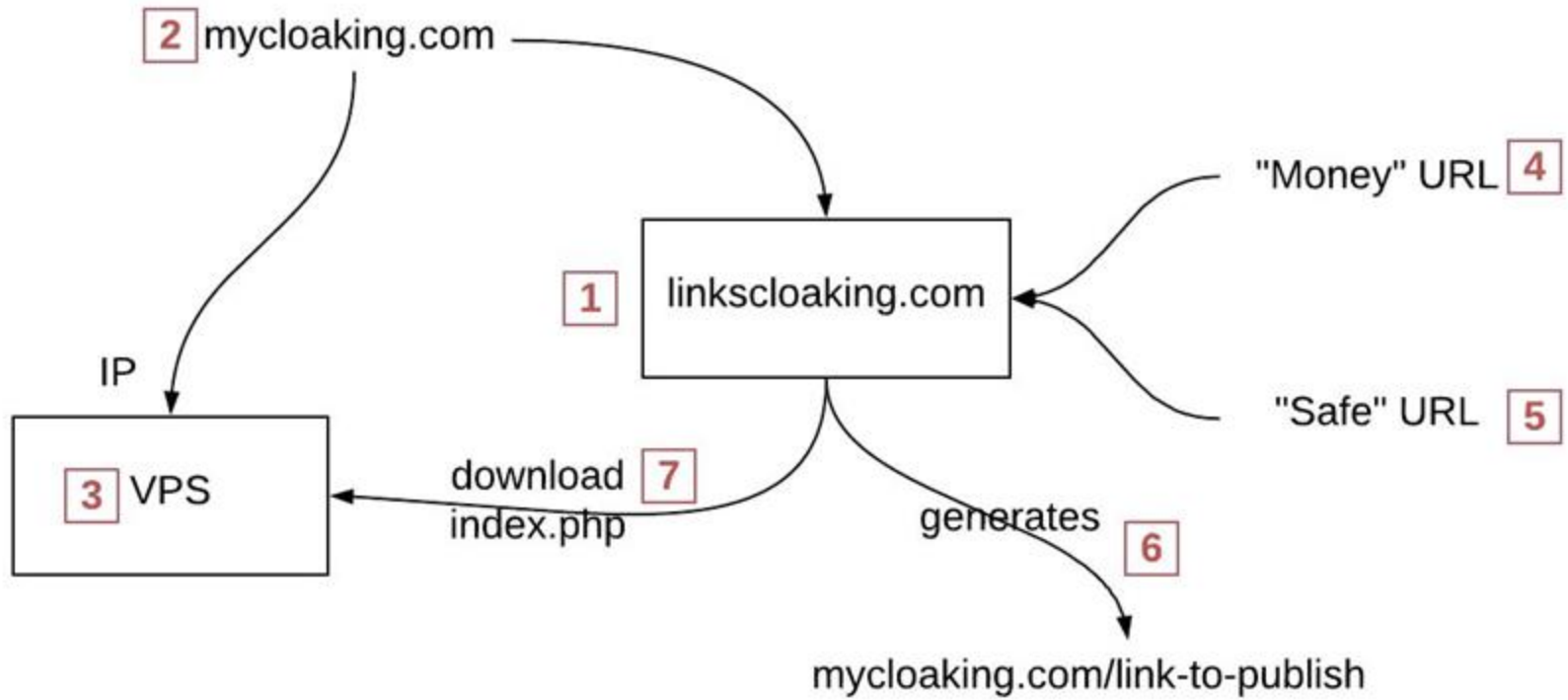
linkscloaking.com plans

ALL LINK LIST

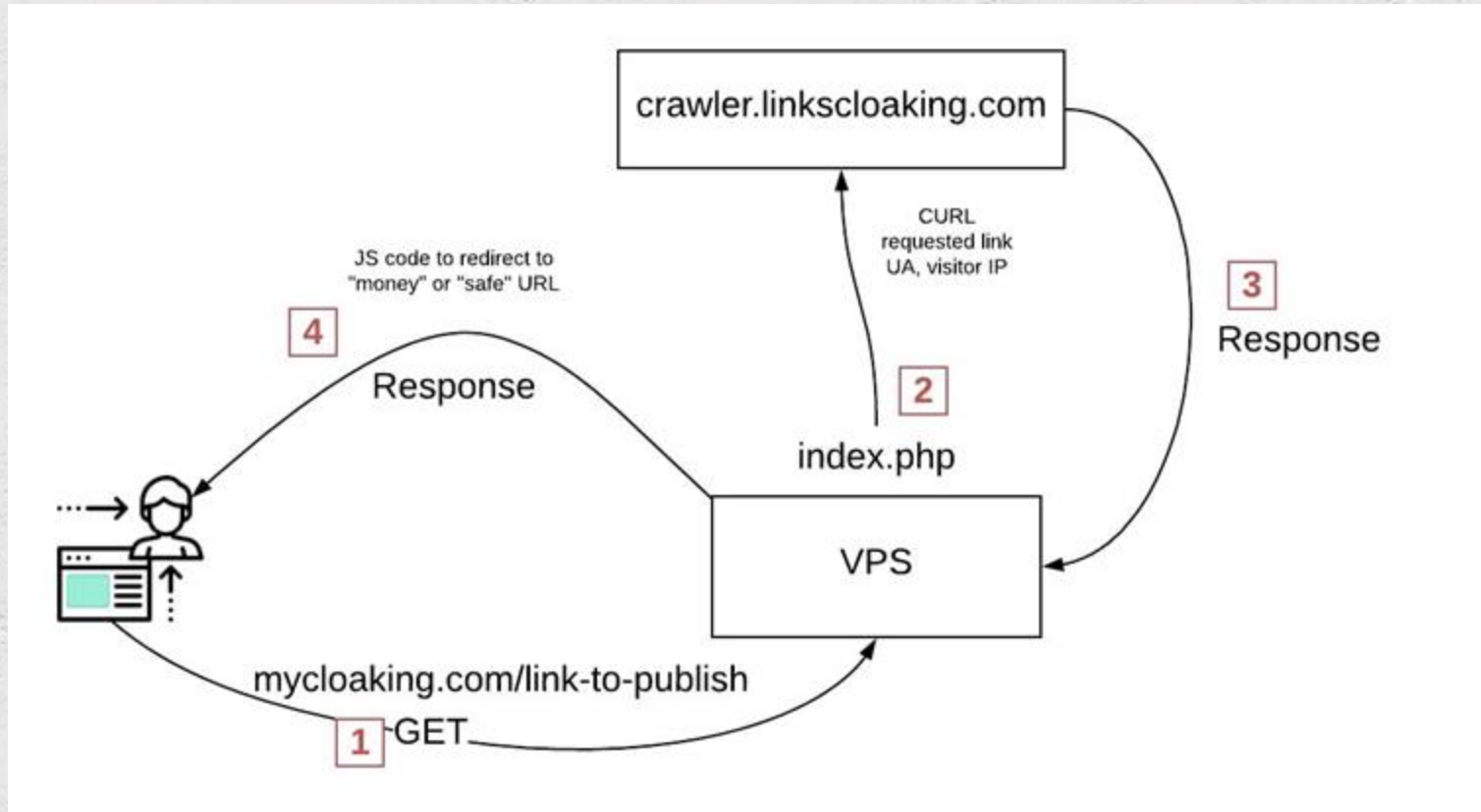
Note: With delete button you see an edit button, by default your link is on means traffic goes to your money page. If you will off any link then traffic moves to masking page that you used during cloak a link

#	Domain	Added Date	Country	Traffic	Type	Link	Money Uri	State	Action
1		2018-05-17 12:20:41	All	54					  

linkscloaking.com admin panel



linkscloaking.com configuration steps



linkscloaking.com how it works?


```
</php
function file_get_contents_curl($url)
{
    $ch = curl_init();
    curl_setopt($ch, CURLOPT_HEADER, 0);
    curl_setopt($ch, CURLOPT_RETURNTRANSFER, 1);
    curl_setopt($ch, CURLOPT_URL, $url);
    curl_setopt($ch, CURLOPT_FOLLOWLOCATION, 1);
    $data = curl_exec($ch);
    curl_close($ch);
    return $data;
}
$rr=base64_encode($_SERVER['HTTP_USER_AGENT']);
$ipp=$_SERVER['REMOTE_ADDR'];
$actual_link = "http://".$_SERVER['HTTP_HOST'].$_SERVER["REQUEST_URI"];
$html = file_get_contents_curl("http://crawler.links cloaking.com/linknew.php?dlink=$actual_link&rbt=$rr&ip=$ipp");
echo $html;
?>
```

links cloaking.com what is under the hood?

```
</php
function file_get_contents_curl($url)
{
    $ch = curl_init();
    curl_setopt($ch, CURLOPT_HEADER, 0);
    curl_setopt($ch, CURLOPT_RETURNTRANSFER, 1);
    curl_setopt($ch, CURLOPT_URL, $url);
    curl_setopt($ch, CURLOPT_FOLLOWLOCATION, 1);
    $data = curl_exec($ch);
    curl_close($ch);
    return $data;
}
$rr=base64_encode($_SERVER['HTTP_USER_AGENT']);
$ipp=$_SERVER['REMOTE_ADDR'];
$actual_link = "http://".$_SERVER['HTTP_HOST'].$_SERVER["REQUEST_URI"];
$html = file_get_contents_curl("http://crawler.links cloaking.com/linknew.php?dlink=$actual_link&rbt=$rr&ip=$ipp");
echo $html;
?>
```

BASIC

\$80 / Month

ADVANCE

\$120 / Month

PRO

\$150 / Month

links cloaking.com what is under the hood?

Request to crawler.lincscloaking.com

```
[23/May/2018:18:44:23] - (index) - http://crawler.lincscloaking.com/linknew.php?dlink=http://
.c CLOAKER PROVIDED URL &rbt=TW96aWxsYS81LjAgKG10aG9uZTsgQ1BVIg10aG9uZSBPUyAxMV8yXzYgbGlrZSBNYWNg
T1MgWCkgQXBwbGVXZWJLaXQvNjA0LjUuNiAoS0hUTUwsIGxpa2UgR2Vja28pIE1vYm1sZS8xNUQxMDAgW0ZCQU4vRkJJT1M7RkJBVi8
xNzIuMC4wLjQ2Ljk000ZCQ1YvMTA4NDI1MzU500ZCRFYvaVBob25lNiwx00ZCTUQvaVBob25l00ZCU04vaU9T00ZCU1YvMTEuMi4200
ZCU1MvMjtGQkNSL0FUJlQ7RkJJRC9waG9uZTtGQkxkDL2VuX1VT00ZCT1AvNTtGQlJWJzEwOTQ2NDY0M10=&ip=141.126.1.173
```

```
[23/May/2018:18:44:23] - (index) -
```









```
<script type="text/javascript">
    window.open("http://200.100.100.100/GOOD URL", "_parent");
</script>
```

Response to UA

linkscloaking.com cloaking server response

Advanced cloaking system
leadcloak.com

MONTHLY PLANS

 Unlimited campaigns creation	STARTER 	PROFESSIONAL 	PREMIUM 	ENTERPRISE 
 Unlimited traffic	\$399 / MONTH	\$619 / MONTH	\$1199 / MONTH	\$1999 / MONTH
 Access to all networks	Up to 5 active campaigns at once	Up to 10 active campaigns at once	Up to 20 active campaigns at once	Up to 40 active campaigns at once
 Multi-user support	Sign Up	Sign Up	Sign Up	Sign Up

leadcloak.com plans



Using "iFrame" Cloaked URLs (Power Mode)

Browser security prohibits loading insecure ("http://") elements inside a secure ("https://") page. So, if you are using "iFrame" with a "http://" cloaked URL, do not load your safe URL securely (over "https://"). You can load "https://" elements inside a "http://" page without having any problems, but not the opposite. In order to use a "https://" Safe URL, your Cloaked URL *and all subsequent redirects or pages* must also be loaded over "https://".

If you are already promoting a "https://" Safe URL but are ready to begin using the iFrame method with a "http://" Cloaked URL, simply configure your server to redirect all "https://" Safe URL traffic to the "http://" version (this can also be done via Cloudflare).

NOTE: The offer you are promoting may not be designed to load inside an iFrame. If this is the case, add a **target="_blank"** attribute to the offer links on your landing page so that they open in a tab.

Facebook

Please be aware that Facebook may use its mobile application to track the visitor redirect chain. Therefore, if you are targeting **mobile traffic**(desktop-only campaigns may not be affected), we highly recommend that you use the Power Mode implementation (to perform client-side tests).

Note:

- If your safe URL is loaded securely (over "https://"), all URLs appearing in iFrame redirects must also be loaded securely.
- If you are using a tracking link as your cloaked URL, use the "iFrame" method. No other changes are necessary.

leadcloak.com power mode

Advanced Connection Settings

Block IPv6 Visitors Enable Disable

Check IP PTR records (perform reverse DNS lookup) and apply filters? Enable Disable
Highly recommended when the traffic source is Google or Facebook.

Use advanced User Agent detection filters? Enable Disable

Allowed Connection Types All
 Cable/DSL
 Cellular
 Corporate
 Dialup

Advanced Location Rules Disabled
 Block visitors without a 'City' value
 Block visitors without a 'Region' value
 Block visitors without both 'City' AND 'Region' values
 Block visitors without a 'City' OR 'Region' value

Allow Mobile Proxies? Enable Disable

Block TOR Proxies Enable Disable

Allowed ISP Types Commercial ISPs (Disable this option for extra security in exchange for a higher bleed rate)
 Organizations
 Government & Military
 Universities, Colleges, Schools, and Libraries
 Residential
 Mobile ISP
 Residential & Mobile
 Data Center, and Web Hosting, Content Delivery Networks
 Search Engine Spiders and Bots

Global Built-in Filters Global Fingerprinted Devices/IPs Filter
 Global ORG, ISP, ASN Filter
 Global UA, Referrer Filters

leadcloak.com campaign setup

 **Your code is ready**

Your campaign is set up and you're good to go..! New campaigns are always started in 'Under Review' state.

Please submit your campaign for approval in Under review state! Once approved, please switch the campaign to Active. Unsafe visitors will always see the safe page and real/safe visitors will always see the money page even in the Active state.

Again, please don't forget to change the Campaign Status once your campaign is approved unless you have enabled CloakMatic, which takes of switching the states automatically for you.

Note: It is critical that you always use SSL on the domain where you upload the code.

LeadCloak offers multiple types of integration codes to suit your needs depending upon on what ad network you plan on running your ads on.

There are multiple types of integration codes that supports various modes to perform "client-side" and/or "server-side" tests including a plugin for WordPress.

Simple Javascript Mode Cloaker

Simple PHP Mode Cloaker

Advanced Mode Cloaker (Combo Cloaker - Simple Javascript and Simple PHP)

Power Mode Cloaker (PHP only)

Power Mode Cloaker (with integrated Advanced Mode)

Wordpress Plugin

Pixel Codes for Facebook

leadcloak.com campaign setup complete

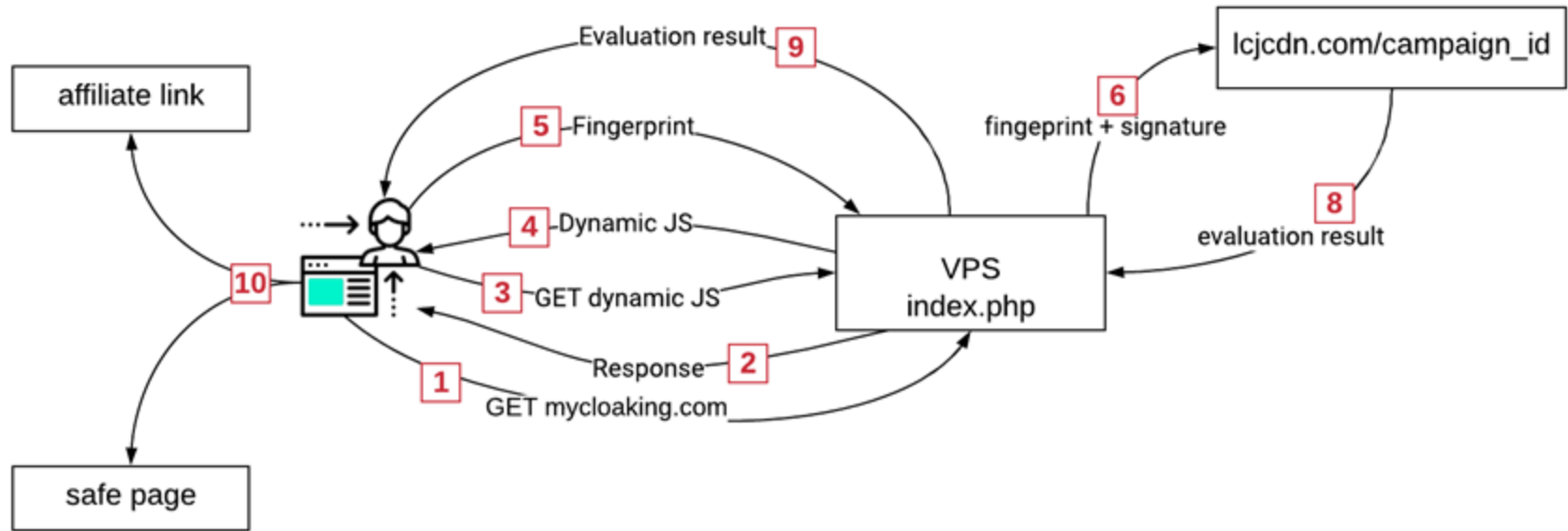
Downloaded file name: abracadabra-power-mode-advanced-cloaker.zip

Inside you find these files:

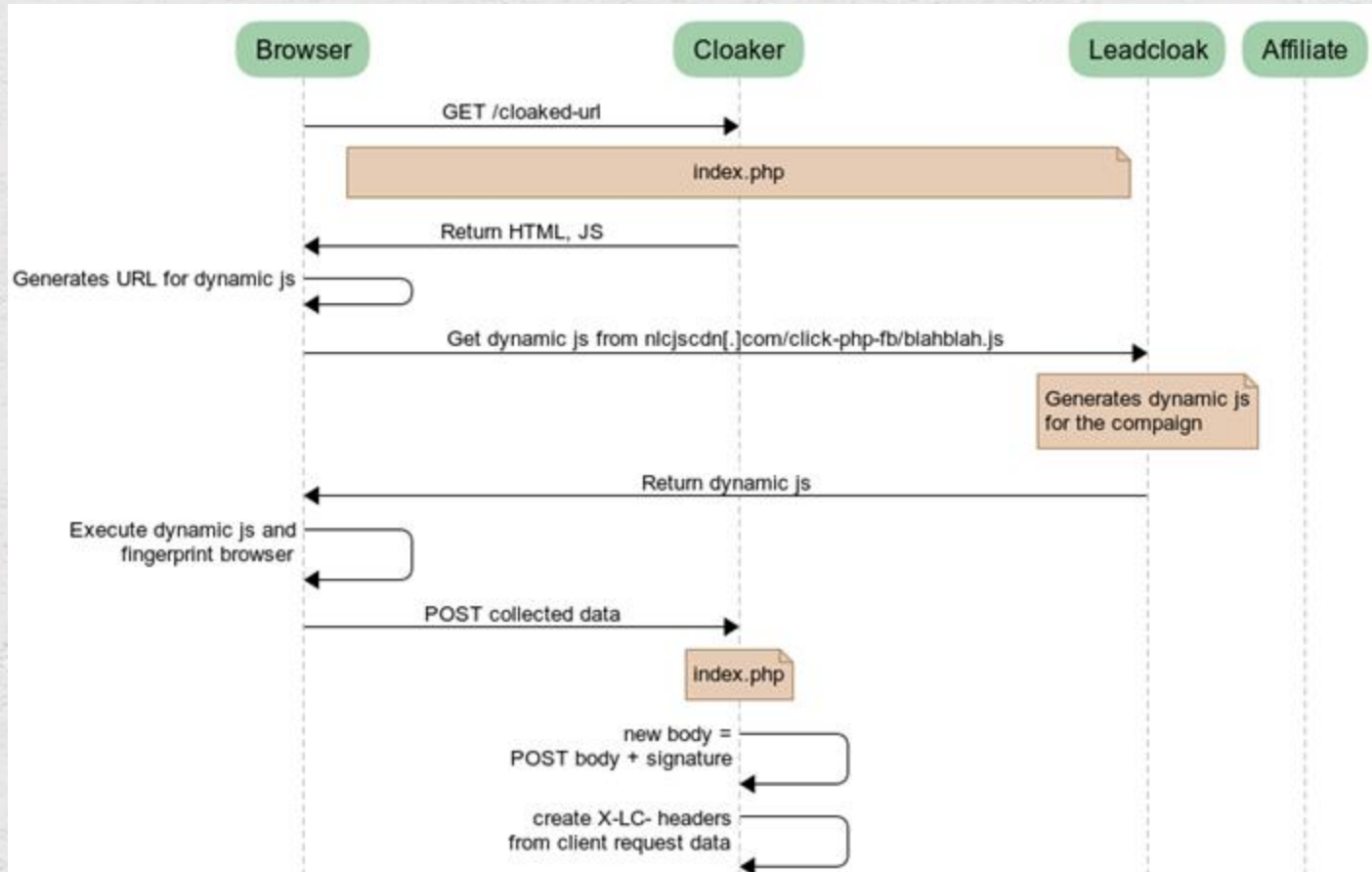
- abracadabra.js
- ajax-loader.gif
- index.php
- leadcloak-abracadabra.php

*abracadabra - random string representing campaign identifier

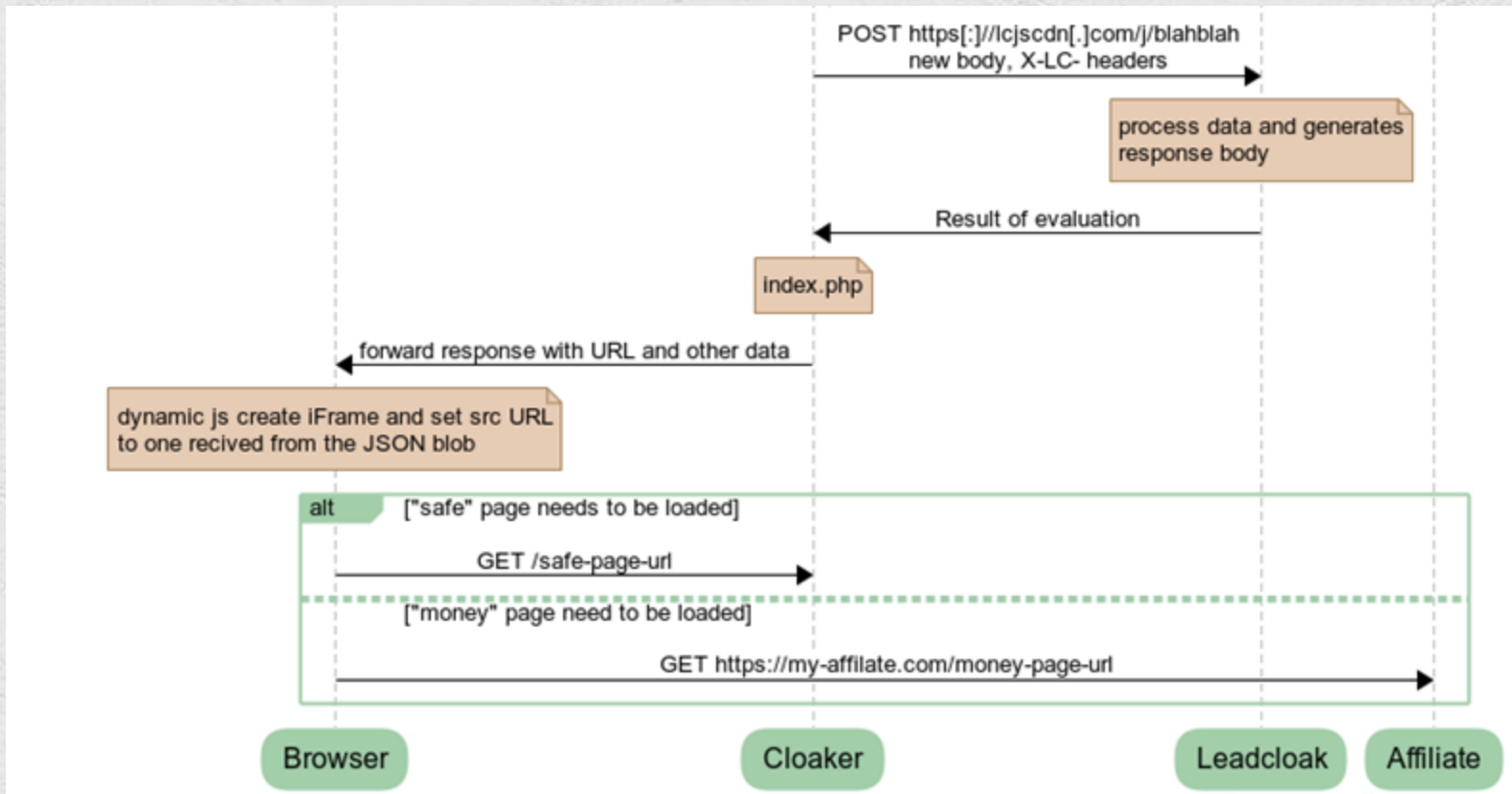
leadcloak.com power mode. What is inside?



leadcloak.com How it works?



leadcloak.com advanced power mode part 1



leadcloak.com advanced power mode part 2

- when LeadCloak response contains "safe" URL

```
["https://[REDACTED]/store/", false, "[REDACTED]", 15336[REDACTED], false]
```

- when LeadCloak response contains "money" URL

```
["https://[REDACTED]/about/?&brand=Apple&model=iPhone&os=iOS&
browser=UCBrowser+for+iPhone&city=San+Jose&country=United+States&
org=Verizon+Wireless&isp=Verizon+Wireless&carrier=Verizon&
model2=iPhone%7CiPhone+3G%7CiPhone+3GS%7CiPhone+4%7CiPhone+4S%7CiPhone+5%7CiPhon
e+5S%7CiPhone+6%7CiPhone+6+Plus%7CiPhone+6s%7CiPhone+6s+Plus%7CiPhone+SE%7CiPhon
e+7%7CiPhone+7+Plus%7CiPhone+8%7CiPhone+8+Plus%7CiPhone+X&
connectiontype=Cellular&countrycode=US&domain=myvzw.com&timestamp=15336[REDACTED]&
ip=[REDACTED].0.225&", true, "[REDACTED]", "", false]
```

leadcloak.com cloaker response result

```
function p(t, z) {
  $.ajax({
    type: "POST",
    dataType: "json",
    cache: false,
    url: location.href,
    data: "q=" + xha(t),
    success: function(xhr) {
      if ((xhr[0] !== "") && (document.URL !== xhr[0])) {
        document.getElementsByTagName('body')[0].innerHTML =
win(xhr[0]);
      }
    }
  });
}

function win(rem) {
  return '<iframe id="isrc" src="' + rem + '" style="visibility:visible
!important; position:absolute; top:0; left:0; bottom:0; right:0; width:100%;
height:100%; border:none; margin:0; padding:0; overflow:hidden; z-index:999;">
</iframe>'
}
```

leadcloak.com iFrames to circumvent detection

Feb 2, 2018



kirey ragin
BANNED

BANNED

How can I hide the destination website of a link from facebook and youtube

Feb 5, 2018



bartosimpsonio
Jr. VIP

Jr. VIP

Premium Member


You're looking for a cloaker. For FB and YT you need a pro cloaker.

What people say in cyber underground




What They Said About Us



 I have improved my leads quality in 3 days thanks to JustCloakit.com cloaking platform. Affiliates, this platform is for you!

★★★★★

STEPHEN JACKOB, CEO

 Fast and secured cloaking platform, I get 100% real targeted traffic - no more bots, crawlers, spy tools and scanners and undesired irrelevant traffic. I truly recommend.

★★★★★

ROY FENDER, ONLINE MARKETING EXPERT

About Us

Just Cloak It is a boutique private service for Cloaking & Fraud Prevention specifically aimed at on-line marketers who are interested in improving their Lead Quality & ROI by protecting their links and reducing fraudulent traffic. We currently monitor millions of visits daily and serve over 3,000 clients worldwide. Our Fraud Prevention & Cloaking platform blocks fraud and undesired visits in real-time thus keeping our clients' websites secured & sealed from undesired traffic.

Just Cloak It, originally designed for filtering "bad" visits and reduce fraud, supports the major networks as well as monitoring organic visits and traffic. By using our advanced platform, you can view your traffic in

Our Skills

Fraud Prevention & Traffic Monitoring

100%

Cloaking Solutions & Traffic Filtering

100%

Locations Targeting & Matching

100%

Links & Websites Protection

100%



THE #1 PREMIUM AFFILIATE MARKETING COMMUNITY

Justcloakits is your gateway to affiliate marketing. Whether you are experienced and need a networking hub, or want to launch your first campaign online, we have something for you.

Join Us Now



Links Protection

Game! Which one is fraud?



Monthly Plans

BASIC PLAN	ADVANCED PLAN	PRO PLAN	ELITE PLAN
\$399 /month	\$619 /month	\$1,199 /month	\$1,999 /month
Up to 5 active campaigns at once	Up to 10 active campaigns at once	Up to 20 active campaigns at once	Up to 40 active campaigns at once
Unlimited campaigns creation	Unlimited Campaigns Creation	Unlimited campaigns creation	Unlimited campaigns creation
Unlimited Traffic	Unlimited Traffic	Unlimited Traffic	Unlimited Traffic
Access to all Networks	Access to all Networks	Access to all networks	Access to all networks
Live support	Live support	Live support	Live support
Contact Us	Contact Us	Contact Us	Contact Us

Just Cloak It is a boutique private service for Cloaking & Fraud Prevention specifically aimed at on-line marketers who are interested in improving their Lead Quality & ROI by protecting their links and reducing fraudulent traffic. We currently monitor millions of visits daily and serve over 3,000 clients worldwide. Our Fraud Prevention & Cloaking platform blocks fraud and undesired visits in real-time thus keeping our clients' websites secured & sealed from undesired traffic.

Just Cloak It, originally designed for filtering "bad" visits and reduce fraud, supports the major networks as well as monitoring organic visits and traffic. By using our advanced platform, you can view your traffic in



\$150 /Month
STARTER

10 active campaigns

10,000 Hits

Facebook Pages / Groups (Only)

Geo Tracking / No

ISP Filtering / No

Campaign Log / No

Change Link State / No

Server Response 100%

Live Support

Purchase

\$200 /Month
GOLD

20 active campaigns

20,000 Hits

Facebook and all ADS networks (limited)

Geo Tracking / No

ISP Filtering / No

Campaign Log / Yes

Change Link State / Yes

Server Response 100%

Live Support

Purchase

\$250 /Month
DIAMOND

Unlimited active campaigns

Unlimited Hits

Facebook and all ADS networks (Unlimited)

Geo Tracking / Yes

ISP Filtering / Yes

Campaign Log / Yes

Change Link State / Yes

Server Response 100%

Live Support

Purchase

Game! Which one is fraud?



Attention! Justcloakits.com cloaking scam

Thread

...witnessed a new cloaking website/service which is called: **justcloakits.com** (note the 'S'). They claim to sell cloaking services having cheap...

Thread by: mrblackjack, May 9, 2018, 31 replies, in forum: Cloaking and Content Generators

Fraud around cloaking in cyber underground



Attention! Justcloakits.com cloaking scam

Thread

...witnessed a new cloaking website/service which is called: **justcloakits.com** (note the 'S'). They claim to sell cloaking services having cheap...

Thread by: mrblackjack, May 9, 2018, 31 replies, in forum: Cloaking and Content Generators

in the last few months, you probably witnessed a new cloaking website/service which is called: **justcloakits.com** (note the 'S'). They claim to sell cloaking services having cheap packages, and if you pay attention closely, the text on their website is taken from our veteran brand: <http://justcloakit.com>.

As the owner of the famous veteran brand: <http://justcloakit.com>, I state here that we have no relation to the fake site: **justcloakits.com**. After going through a deep research about this fake site, it seems a phishing service that is meant to:

1. steal <http://justcloakit.com> real users' login details and credentials as well as their campaigns
2. mislead potential / new users into thinking it's the real <http://justcloakit.com> brand.

They offer cheap prices, declaring themselves as the authenticated brand but actually provide you with nothing.

Be Warned!

Fraud around cloaking in cyber underground



Attention! Justcloakits.com cloaking scam

Thread

...witnessed a new cloaking website/service which is called: **justcloakits.com** (note the 'S'). They claim to sell cloaking services having cheap...

Thread by: [mrblackjack](#), May 9, 2018, 31 replies

in the last few months, you probably witnessed a new **justcloakits.com** (note the 'S'). They claim to sell cloaking services. Pay attention closely, the text on their website is taken from

As the owner of the famous veteran brand: <http://justcloak.com> fake site: **justcloakits.com**. After going through a deep analysis, the service that is meant to:

1. steal <http://justcloak.com> real users' login details and
2. mislead potential / new users into thinking it's the real site

They offer cheap prices, declaring themselves as the best. In reality, they are doing nothing.

Be Warned!

The screenshot shows the homepage of justcloakits.com. The navigation bar includes links for Home, About, How it Works, Services, Pricing, Faqs, Contact, and Login. The main content area features three pricing plans:

Plan	Price	Active Campaigns	Hits	Facebook Pages / Groups	Geo Tracking	ISP Filtering	Campaign Log	Change Link State	Server Response	Live Support
Silver	\$150 /Month	10	10,000	Facebook Pages / Groups (Dry)	No	No	No	No	100%	Yes
Gold	\$200 /Month	20	20,000	Facebook and all ADS networks (Limited)	No	No	Yes	Yes	100%	Yes
Diamond	\$250 /Month	Unlimited	Unlimited	Facebook and all ADS networks (Unlimited)	Yes	Yes	Yes	Yes	100%	Yes

Fraud around cloaking in cyber underground

Campaign Survival

Google	- 2 Weeks
Facebook	- 3 months
Pop-Networks	- 3 Weeks
Porn-Networks	- 3 Weeks
Native	- 1 month

Cloaking campaign survival times

How companies detect cloaking

Detect redirect chain

- Compare redirect chain for crawler with emulated user

Why it doesn't work?

- iFrame, content rewrite
- Detect emulated user

Myths about cloaking detection

Landing page content analysis

- Compare landing page for crawler with “real” user

Why it doesn't work?

- False positives
 - Same link = different results based on Geolocation, device types
 - SPA
 - Page for crawler might have different content (no Ads)
- Bust emulated user
 - “Real” user is not a real user
- Privacy
 - Sampling content received by real user is a either a privacy leak or an information loss
 - Ad networks wouldn't share data with each other

Myths about cloaking detection

Table 2: Comparison of cloaking detection methods

Methods	Features	Max F1 Score	IP/SEM	Extraction Time	Data Transmitted	Comparison Time
Najork [17]	W, L, T	low	✓	$O(N_W + N_L + N_T)$	$O(1)$	$O(1)$
Term & Link Diff [27]	W, L	medium	✗	$O(N_W + N_L)$	$O(N_W + N_L)$	$O(N_W + N_L)$
Wu & Davison [26]	W, L	medium	✗	$O(N_W + N_L)$	$O(N_W + N_L)$	$O(N_W + N_L)$
CloakingScore [7]	W	medium	✗	$O(N_W)$	$O(N_W)$	$O(N_W)$
TagDiff [14]	W, T	high	✗	$O(N_W + N_T)$	$O(N_W + N_T)$	$O(N_W + N_T)$
Dagger [23]	W, T	high	✗	$O(N_W + N_T)$	$O(N_T)$	$O(N_T)$
Hybrid Detection [8]	W, L, T	high	✗	$O(N_W + N_L + N_T)$	$O(N_L + N_T)$	$O(N_L + N_T^2)$
Cloaker Catcher	W, L, T	high	✓	$O(N_W + N_T)$	$O(1)$	$O(1)$

W: words, *T*: tags, *L*: links

Cloaking detection methods research

- Replay real user traffic
 - Hard to scale due to variables in requests that needs to be identified, signed components that contain timestamps/UA specific data, etc
- Automate known good User Agent
 - Detectable out of the box (navigator.webdriver, emulated user-events, user timings, system configurations)
- Modify known good User Agent
 - Hardware fingerprints likely leak it (TCP, SSL, WebGL)
 - Hard to maintain
- Mobile device emulators
 - Hard to fake sensor data
 - Replay doesn't make sense
- Proxy through residential IPs
 - That's cool, but fingerprints still bust you

“real” user vs real user emulation

Thank you!

@ilya_online
@sshekyan



**ZERO
NIGHTS
2018**

ALL RIGHTS RESERVED BY THE ORGANIZATION