# ONE OF THESE THINGS IS NOT LIKE THE OTHER —

# A REPORT ON FAKE DOMAIN ATTACKS

## GLOBAL CIVIL SOCIETY AT RISK

**REPORT ONE OF A SERIES DETAILING SOME OF THE MAJOR DIGITAL THREATS FACING CIVIL SOCIETY ORGANIZATIONS AND HUMAN RIGHTS DEFENDERS**

access

# OVERVIEW OF REPORTS ON GLOBAL CIVIL SOCIETY AT RISK

Civil society organizations and human rights defenders have some of the most sophisticated, relentless, and well-resourced adversaries attempting to surveil and hinder their work. The threat of these adversaries to the operations of civil society groups is compounded by the low capacity of such groups to focus on and mitigate such threats.

The situation is even more dire when compared to the growing corporate understanding of digital threats. In the corporate world, many companies periodically report and analyze digital threats to businesses -- McAfee, PandaLabs, Secunia, Symantec, Verizon, to name only a few. But just as the number and sophistication of attacks targeting corporations have increased over time, so too have the threats faced by civil society organizations to their operations.

With our reports we hope to narrow this gap, and inform civil society groups of some of the digital threats that predominantly target them -- from DDoS and website defacement to fake domain attacks and account compromise. These are attacks we have seen in the operation of our digital security helpline and partner organizations have experienced in the course of their operations. By analyzing the specific threats to civil society organizations and human rights defenders, we aim to provide a higher-level understanding of the technical, socio-political, and legal ways they are perpetrated and mitigated.

This report, "One of These Things is Not Like the Other: An Investigation of Fake Domain Attacks," is the first report in the "Global Civil Society at Risk" series that will be released in the coming months. These reports expand on the general multi-issue report we released in 2012 titled, "Global Civil Society At Risk: An Overview of Some of the Major Cyber Threats Facing Civil Society."[1] In this follow-up report, we trying to delve into more detail on the specific attacks civil society actors face. We see this work as complementary to the tremendous efforts of other organizations in our space such as Citizen Lab in finding and analyzing digital attacks such as targeted malware on civil society organizations.

Through this awareness building and information sharing, we aim to improve the ability of users and organizations to defend themselves against these digital security threats.

1 https://www.accessnow.org/page/-/docs/Access Tech/Global Civil Society at Risk.pdf

# AUTHORS AND ACKNOWLEDGEMENT

This report was written and managed by Michael Carbone. Data analysis and visualization was provided by Béchir Nemlaghi and Dillon Reisman. Peter Micek, Drew Mitnick, and Wes Paisley contributed policy and legal analysis. Mira Rojanasakul designed the report. Many thanks to the following individuals and organizations for their invaluable input into the fake domains chapter of the report: Gustaf Björksten, Brett Solomon, Jochai Ben-Avie, Patrick Ball (Human Rights Data Analysis Group), James Turnbull, Kayne Naughton (Asymmetric Security), Amin Sabeti, the engine room and May First/People Link.

*Access is an international human rights organization*
*that defends and extends the digital rights of users at risk around the world.*

*By combining innovative policy, user engagement, and direct technical support,*
*we fight for open and secure communications for all.*

If you know of any fake domains attacks not covered in this report, please contact us at reports@accessnow.org.

access

# TABLE OF CONTENTS

# I. INTRODUCTION

Civil society organizations and human rights defenders are the targets of a variety of sophisticated attacks to surveil their human and computer networks, impede their work, and dilute or confuse their message. Fake domains have emerged as a unique method employed by the adversaries of civil society organizations towards these goals.

Fake domain attacks are defined as attacks in which an adversary creates a similar-looking website or social media profile to the targeted website. This may be done with the intent to draw readership from the original website and display alternative content, create confusion amongst a targeted community, or serve malware to compromise the target audience of the original website.

In the past, fake domain attacks were used mainly by spammers and online criminals to trick individuals into sharing their private information (often banking credentials) through a fake look-alike or website. That website would often be promulgated through a "phishing" email purported to come from the original website.[2]

The attacks analyzed in this report represent an evolution of these attacks, targeting the online presences and user trust of civil society organizations and media organizations for socio-political rather than economic goals. In addition, the perpetrators of these attack are predominantly state-aligned actors, and in some cases leveraged the privileged position of state-owned Internet Service Providers to propagate the attacks.

**A.**

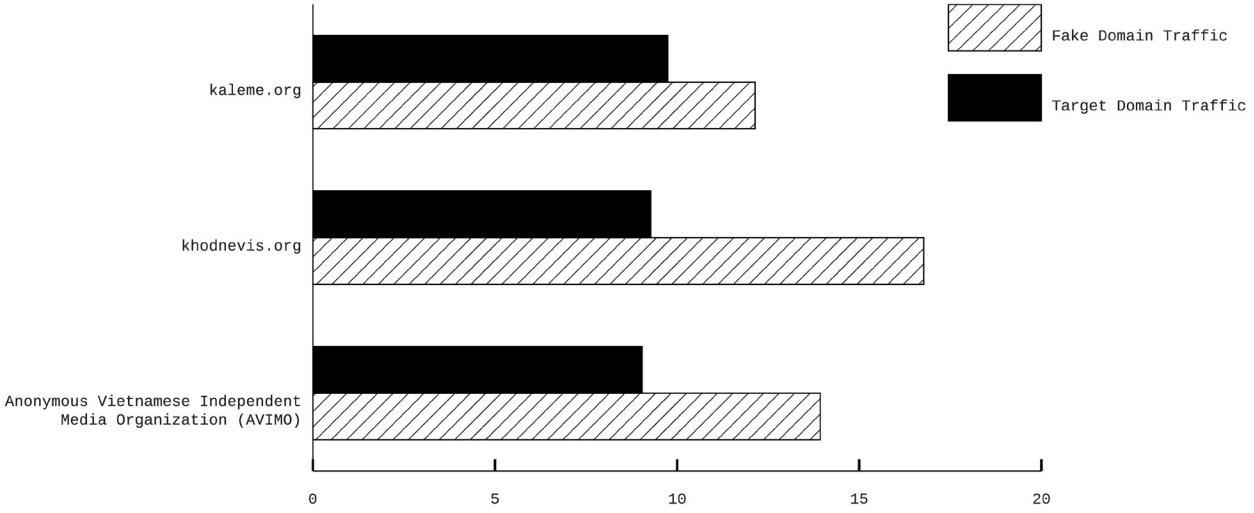

**B.**


**Figures (A) and (B) are screenshots of two nearly-identical news sites (images taken July 3rd, 2013).**

These fake domains range are often very faithful imitations of the target domain. Figures (A) and (B) are screen-shots of two nearly-identical websites from July 3rd, 2013. Only one of them is the legitimate BBC Persian news site (officially bbcpersian.com or bbc.co.uk/persian), while the other is a fake domain (persianbbc.ir) serving alternative content under the same logo, design, and layout. The fake website (B) substitutes pro-government content for the original news content on the targeted BBC website (A). The effect of such imitation can be extremely harmful to consumers of media and the supporters of civil society organizations; in the past, they have successfully drawn a significant amount of both domestic and international traffic away from victimized domains. In certain instances fake domains have even garnered better Alexa traffic rankings than their targets.

2 These types of phishing attacks have also perpetrated in political contexts -- most recently in the lead-up to the 2013 Iranian presidential election, Iranian users received such attacks in an attempt to steal their Google account credentials, likely for intelligence and surveillance purposes. See: http://googleonlinesecurity.blogspot.com/2013/06/iranian-phishing-on-rise-as-elections.html

**AGGREGATE INTERNATIONAL/DOMESTIC TRAFFIC SCORE (100/LN(ALEXA RANK)) OF TARGET DOMAIN VS. FAKE DOMAIN**




As news organizations and citizen media increasingly rely on digital means to present their work, state-level adversaries are relying on novel ways of diminishing their impact and targeting their readers. Our data provides a window into the methods and effectiveness of these attacks and the type of government environment that gives rise to them.

# II. METHODOLOGY

For each fake domain incident shared with us or encountered during the course of our digital security helpline work, we have sought to distill the most important data points to aid in comparison and analysis. Some of the different aspects we looked at are the domain name and registrar, web host, and attack type for the targeted and fake domains.

In addition to similar domain incidents shared with us or encountered during the course of our digital security helpline work, we also endeavored to find additional fake domains we were not aware of. Two strategies in particular proved fruitful: analyzing other websites hosted on the same IP address as fake domains, and building an automated tool that searched for fake domains from a list of websites likely targeted.

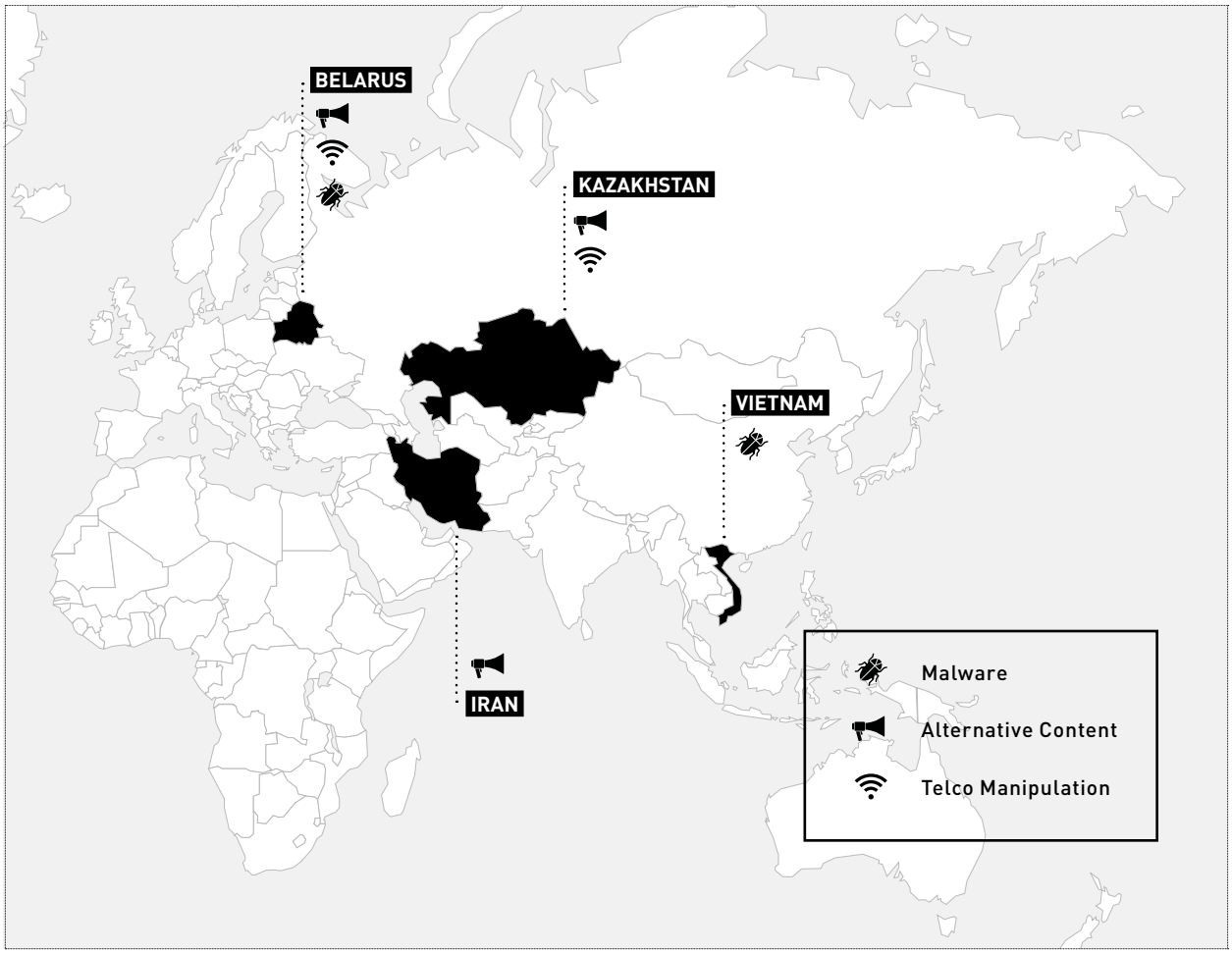
One difficulty in acquiring usable data on these attacks is that the fake domains may only be accessible online for a short period of time, such as around a presidential election. Because of this, we must rely on contemporaneous accounts of these attacks to provide context for the attack, and in malware attacks may be unable to recover the malware itself. With this report, we hope to provide the framing and tools for individuals and organizations to proactively report fake domain attacks, and allow for the more timely collection of data on these attacks.

**Individuals and organizations can use our online tool at fakedomains.accessnow.org to search for possible fake domains of their website.**

While it cannot catch all fake domains, it does look for the most common ways fake domains are generated through modified related urls, and we will continue to improve this tool over time to include other mechanisms for detection.

# III. FAKE DOMAIN ATTACKS

The incidents of fake domain attacks on civil society and media organizations reveal widely divergent methods, uses, and geographies of fake domains. Attacks predominantly occurred in Iran, Belarus, and Vietnam, with rare instances of attacks in Kazakhstan.




The attacks fell into two broad categories: those serving malware (Vietnam and Belarus), and those serving alternative content (Iran, Belarus, and Kazakhstan). In addition, the means of getting to the fake domain were either by going directly to the fake website via an altered URL, through obfuscated URL sharing (such as on social media), or through DNS redirection of the target URL by state-owned telecommunication companies (telcos).

# A. CATEGORIES OF ATTACKS

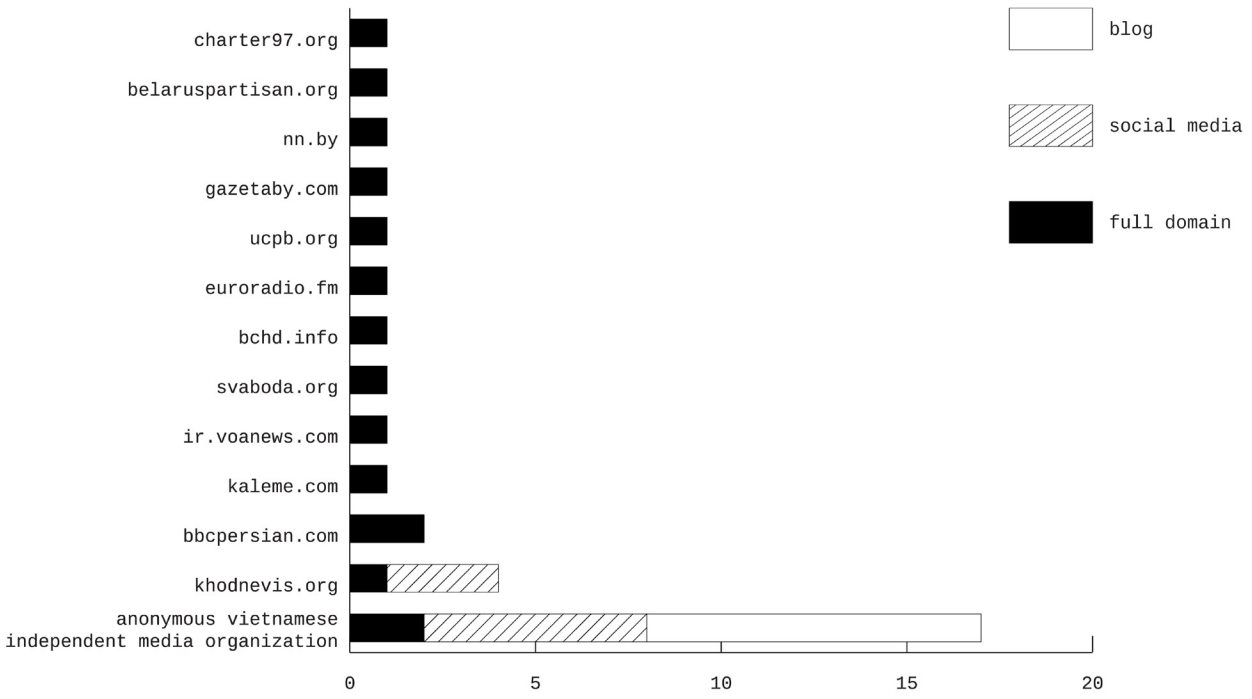
## 1. MALWARE

In these attacks, the fake domains copy the existing content from the targeted website and serve injected malware to visitors of the fake website. These fake domain attacks involve the creation of blogs and social media profiles with similar URL addresses to independent and opposition media groups to serve malware to the users and readers of these independent organizations.

The users of the Belarus news site Charter97.org were the victims of malware served by the fake domain "Charter97.in" in 2011, which leveraged users' trust of their internet service providers (ISPs) to redirect them to the fake website.

In Vietnam, an anonymous Vietnam independent media organization (hereafter "AVIMO") was one targeted organization, with at least nine Blogspot, four Facebook, one Twitter, and one Google+ accounts used to spread malware to the sites' visitors.[3]

**NUMBER OF FAKE DOMAINS/ACCOUNTS PER TARGET**

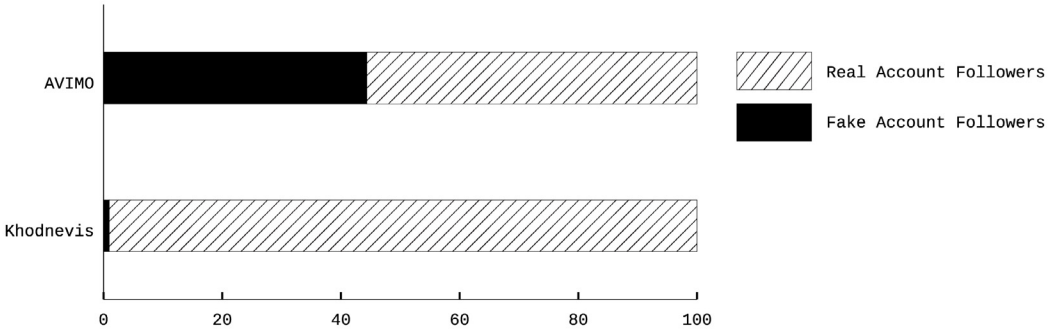



Only one other fake domain attack, the imitation domain made against Iranian site Khodnevis.org, made use of fake social media accounts. The other observed attacks only involved threats made against the full domain.

3 Due to ongoing security concerns, the identity of organization has been anonymized in this report to "AVIMO."

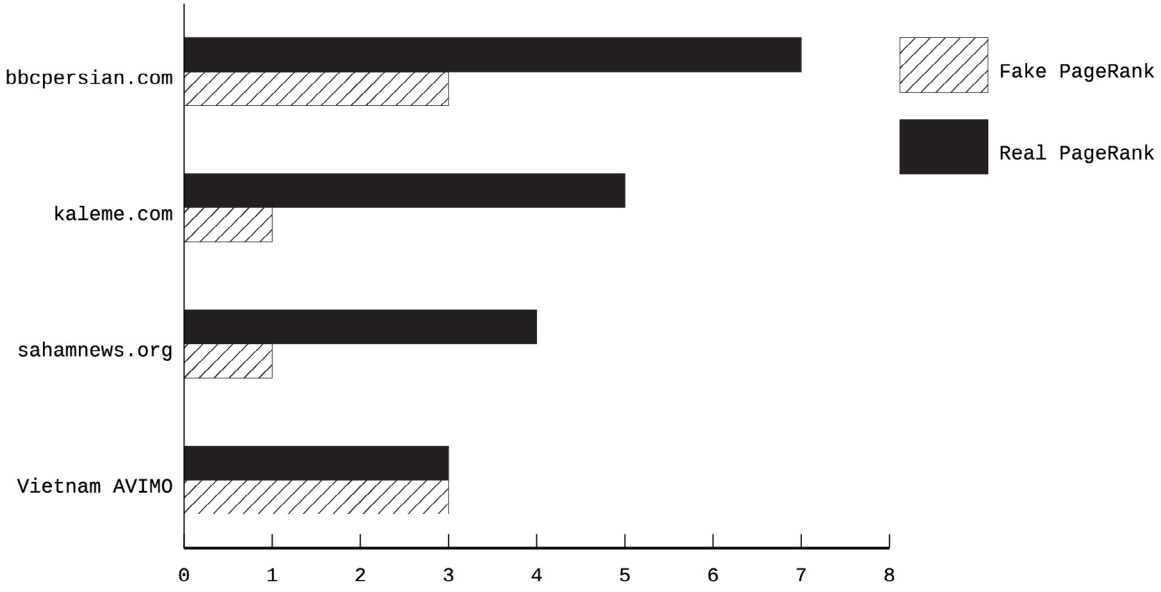
There was a sizable difference in the impact of the presence of fake social media accounts in Vietnam versus that of the fake Khodnevis.org accounts. The use of a wide variety of social media platforms succeeded in misleading nearly a third of interested Vietnamese users into following the fake accounts (thus making them susceptible to the fake domain's malware), whereas the fake Khodnevis website's social media presence did not succeed in drawing away the legitimate Khodnevis' followers.

**FAKE ACCOUNTS' SHARE OF SOCIAL MEDIA FOLLOWERS BY ORGANIZATION**




Google PageRank also provides a valuable measure of a website's relative exposure to the Internet at large. The equal PageRank between the legitimate AVIMO's website and the fake website suggests that both have a similar position in internet search engine results. In the three Iranian cases with complete PageRank data we see that the lack of a major social media presence may have hurt the overall exposure of the fake domains. Ultimately, possible victims of fake domain attacks should be particularly aware of the vulnerabilities posed by the use of fake social media in addition to full domains.

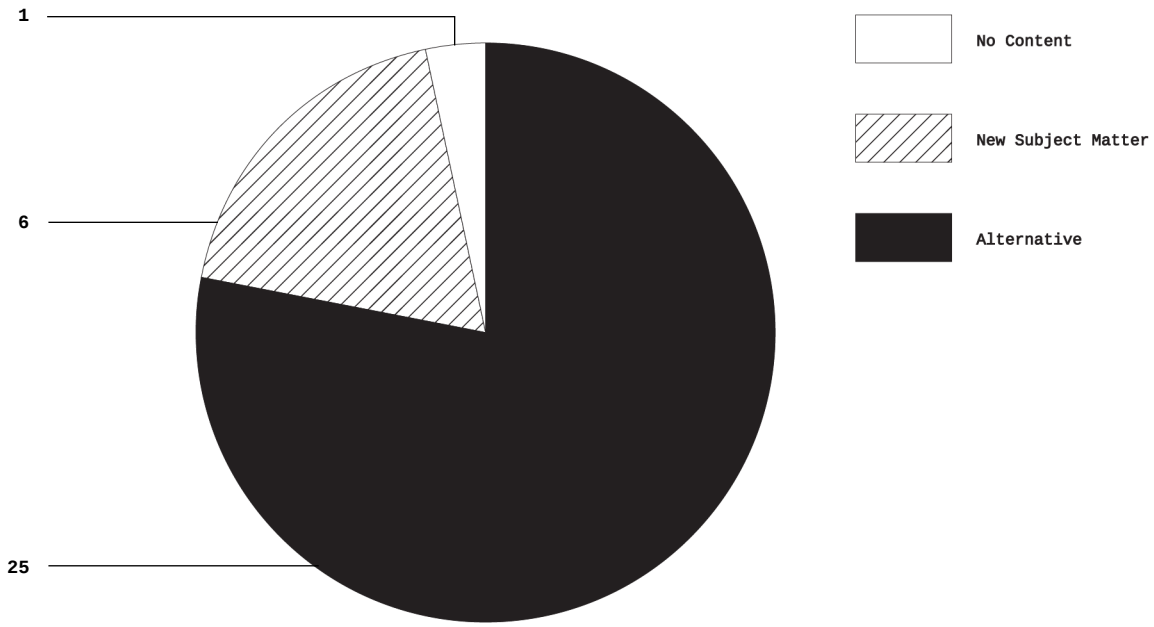
**GOOGLE PAGERANK, REAL VS. FAKE DOMAIN**



## 2. ALTERNATIVE CONTENT

In these attacks, the fake websites copied the existing style and layout of the targeted website-- often including logo and header image -- and served changed content to visitors of the fake website. These fake websites of alternative media sites and fake social profiles of journalists and organizations can then be used to attack the credibility of these actors whose media influence is outside of state control.[4] This is often done by either serving on the imitation website content on the same subject matter as the original website or presenting content on a completely different subject, undermining the original website's goals.

**CONTENT TYPES FOUND ON "CHANGED CONTENT" FAKE DOMAINS**




Not all fake domains in this category aim to alter public opinion over a long period of time. In another fake domain incidence in Belarus, the fake domain attacks occurred surrounding the 2010 presidential election on December 19th. Unlike the targeted websites, the fake domains did not update throughout the day, preventing the promulgation of new information about election events from these established sources. In addition, one of the fake domains -- of Radio Free Europe / Radio Liberty -- changed the location of a planned protest of the election.[5]

In addition to these two main categories, we found some related methods of attacks that augment fake domain attacks or have similarities to them.

4 http://www.guardian.co.uk/world/2013/jan/24/iran-fake-blog-smear-campaign-journalist-bbc

5 http://www.rferl.org/content/belarus_oppositon_websites_hijacked/2253038.html

**USE OF FAKE DOMAINS BY CIVIL SOCIETY AND MEDIA ORGANIZATIONS**

**State-aligned adversaries are not the only groups who utilize fake domains for social and political purposes. Civil society advocacy groups have used the tactic for satirical purposes to raise awareness to causes they feel are underreported by the media. For instance, socio-political activists such as The Yes Men have a long history of creating satirical fake websites of corporations and media organizations as part of their advocacy.[6] Such satire is protected speech in the United States and many other jurisdictions.**

# B. METHODS OF ATTACK

## URL SIMILARITY

Fake domain attacks may exploit user error by placing fake websites on URLs similar to the victim domain but with typos. For example, an attack in Iran was made against the domain www.sahamnews.org, with the perpetrators creating a fake website with the URL www.sahamnew.org, a copy of the original domain with the second 's' missing. If the typo is not too obvious, someone who follows a link to the fake site (or has a typo will typing it into a browser's address bar) may not see the error in the URL.

## URL OBFUSCATION

Adversaries can hide the true destination of a URL from users to mislead them about the website they are trying to access. This could be done, for instance, via "URL shortening," a legitimate service many social media services provide to facilitate sharing links. Shortened URLs often do not look like the actual URLs they represent (for instance, "www.facebook.com/CivilSocietyOrganization" could become "www.tinyurl.com/866bn"). In the attack scenario a shortened URL could purport to represent a legitimate website, when it actually directs users to a fake domain.

## DNS MANIPULATION BY STATE-OWNED TELCOS

In both categories of attack, we found rare cases of state-owned telecommunications companies using DNS manipulation (or "DNS hijacking") to point users in countries toward a fake domain. Belarus and Kazakhstan have briefly redirected domestic visitors of certain independent media websites -- often supported by the political opposition -- to fake versions of those sites. DNS redirection takes advantage of the fact that a computer connected to an internet service provider (ISP) by default relies on the ISP's domain name service (DNS) to convert domain names (like "www.google.com") into computer-understandable IP addresses (like "74.125.131.103"). In these cases, a state-run ISP or telco has redirected DNS requests to the targeted domain names to the wrong IP address, serving the fake website instead.

6 http://theyesmen.org

### TARGETING DURING HIGH-PROFILE POLITICAL EVENTS

A number of the fake domain attacks happen during or surrounding high-profile political events such as presidential elections that are likely to be contentious. Such events tend to draw a large number of users towards the websites for the latest news, providing a strong incentive to block or divert this traffic towards more favorable or friendly media. In the Belarus 2010 presidential election, we saw a number of independent news websites targeted with fake domain attacks on election day, preventing readers from getting updated information on the election or even pointing them to false protest locations. In Iran, news websites like KhabarOnline.ir (the third most-visited Iranian news site[7]) were attacked on the day before election day, with the fake domain KhabareOnline.ir redirecting to Mehr.ir, the official state-approved YouTube alternative for instance.[8]

### CENSORSHIP

One way states improve the reach of fake domains is by blocking domestic access of the targeted websites. Through a number of censorship methods that are increasingly available and accessible to acquire and implement -- IP blocking, DNS filtering, URL keyword blocking, deep packet inspection (DPI) -- governments can ensure that only the most dedicated users will be able to circumvent blocks to access restricted material. Websites serving Iranian audiences that were targeted for fake domains -- BBC News Persian, VOA Farsi, Saham News, Khodnevis were all blocked in Iran, with the exception of Kaleme.

# IV. MITIGATION STRATEGIES

Given these two categories of fake domain attacks and the related use of DNS redirection by state-owned telcos, we will analyze some of the impacts of and mitigation strategies for these attacks. We will first explore existing and prospective technical mitigation techniques for protecting users and websites from these attacks, and then survey some of the policy and legal methods available to mitigate the sources of such attacks.

## A. TECHNICAL MITIGATIONS

### 1. PROTECTING THE USER

**Addressing fake URLs**

The different fake domain attacks require a variety of mitigation strategies. Outside of the DNS redirection cases, users need to navigate to the fake domains in order to interact with them, either through typing the address in the address bar of their browser or by being directed to them through shared URLs on a webpage or in an email. By using services that expand shortened URLs before clicking on them -- such as longurl.org -- one can verify that a link goes to the expected destination address before clicking on it.

In the longer term, we have begun development on a browser plugin to help protect against fake domain attacks. Such a plugin would check the requested URL against a known list of fake domains, as well as have a reporting mechanism for users to report additional fake domains to be protected against. If you are interested in exploring and further developing this project, you can find it on https://github.com/accessnow.

7 https://www.facebook.com/pages/Khabar-Online-EN/104245319728458

8 http://thenextweb.com/insider/2012/12/09/irans-youtube-competitor-has-launched-to-take-on-google-despite-rampant-vpn-usage-in-the-country/

### Fake Domains with Malware

In cases that involve the distribution of malware by the fake domain, there are two mechanisms for such propagation: (1) drive-by malware downloads that exploit browser or plug-in vulnerabilities, or (2) the hosting of compromised software the user downloads herself. These malware vectors are not particular to fake domains, and have been injected into legitimate websites as well.[9]

To protect against drive-by downloads and malware injections, good digital security hygiene is required in keeping software up-to-date and countering common malware vectors like Java and Flash plug-ins. Using web browser security plugins like NoScript, manually making such plug-ins click-to-play, or disabling them in your web browser's settings are other effective ways of mitigating these common paths for the introduction of malware on your computer. Protecting against the possibility of compromised software on fake websites necessitates raising awareness within the targeted population of likely visitors of some of the common paths that can lead to compromise by malware.

### Alternative DNS

In the cases where the fake domains were served to users through DNS redirection by state-run telcos, a user can change the default DNS server their computer relies on (usually the ISP's DNS server) to an alternative DNS server. Some of the more popular alternative DNS servers include OpenDNS and Google Public DNS.

In addition, emerging standards can better secure the DNS system. DNSSEC ensures the authenticity of root server DNS information sent to a recursive resolver such as an ISP's DNS server, but does not protect the user from being served manipulated DNS information by the ISP itself. A complementary proposed specification called DNSCurve seeks to secure and encrypt DNS requests to prevent these types of attacks. DNSCurve has not yet been accepted as an Internet Engineering Task Force standard, but has already been implemented by OpenDNS as DNSCrypt.

For website owners, it is important to ensure the security of the email accounts responsible for administering the domain name registration of a potentially targeted website. Through the compromise of such an account, the DNS records for the address could be changed to point to another website.

## 2. PROTECTING THE WEBSITE

Because fake domains are separate websites from the original targeted website, there are few technical ways to protect the website from such an attack.

In cases where DNS manipulation was used to serve fake domains to users, a site could have an SSL certificate and enable HTTP Strict Transport Security (HSTS) to force https connections to the website. Because the real website has an SSL certificate and its audience knows to expect one, a fake website would likely be unable to produce a valid substitute certificate and the user may be alerted of the discrepancy between the two websites. This assumes a high level of awareness of the role of certificates on the part of the user, and there have been known instances of certificate authorities signing fake certificates.[10]

9 For example, see https://threatpost.com/stolen-winnti-certificates-used-watering-hole-attack-against-tibet-orphans-site-041213/ and https://threatpost.com/researchers-see-uptick-attacks-against-uyghur-users-021413/.

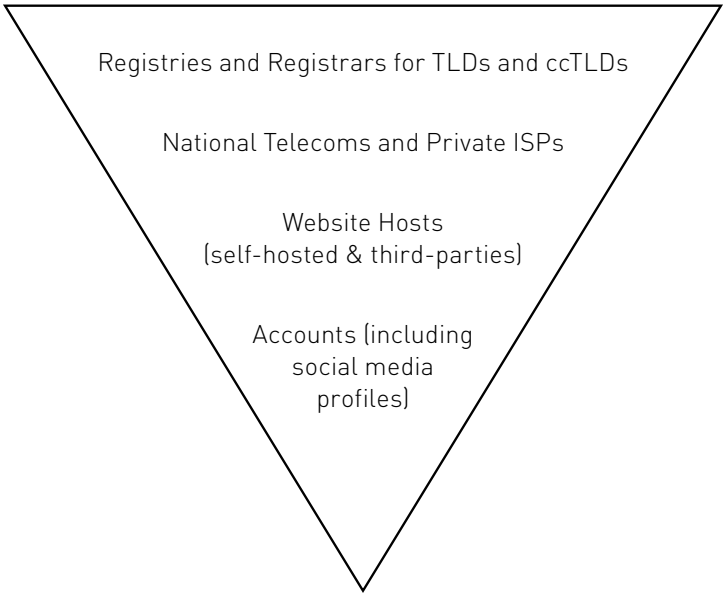
10 For example, see https://threatpost.com/phony-ssl-certificates-issued-google-yahoo-skype-others-032311/, https://threatpost.com/attackers-obtain-valid-cert-google-domains-mozilla-moves-revoke-it-082911/.

In conjunction with the release of this report we have made available an online service at fakedomains.accessnow.org where users and website owners can see if there is a similarly-named domain to a domain they are interested in, such as their own website. Proactive knowledge of such fake domains would allow them to pursue some of the legal strategies covered below.

# B. POLICY/LEGAL MITIGATION: TARGETING THE STACK

Web presences are not created in a vacuum -- the services of a number of providers, companies, and organizations are required to create and maintain such a website, including the TLD registry, domain name registrars, hosting companies, and third-party hosts like social media and blogging platforms. Each of these providers has terms of use policies and agreements with the creators of the domain that can potentially be used to take down the website, whether it is a fake domain or a targeted domain. In addition, these different services exist within the jurisdiction of different countries and broader international institutions, providing additional methods towards these same ends.

**THE "STACK" OF PROVIDERS OF A FAKE DOMAIN**




Because of this, there are numerous avenues with which to pursue an existing fake domain. At the same time, likely targets of fake domain attacks need to be aware that adversaries can focus on these different components for potential technical or legal compromise, especially if the website registrar or web hosting provider is located within the jurisdiction of the potential state adversary.

In attempting to mitigate against fake domains, we will briefly explore this "stack" of laws and business agreements from the international level of domain registries and registrars to national ISPs, web hosts, and social media companies.

## LEVEL 1: DOMAIN REGISTRIES AND REGISTRARS

Domain registries are the organizational and business entities responsible for managing the allocation of domain names. These include top-level domain names (TLDs) such as .com, .net, and .org -- mainly managed by businesses and nonprofits -- and country-code top-level domain names (ccTLDs) such as .us, .ru, .cn and .fr, which are managed by national registries. In order to dispute a fake domain name, there are two levels of dispute mechanisms -- international and national.

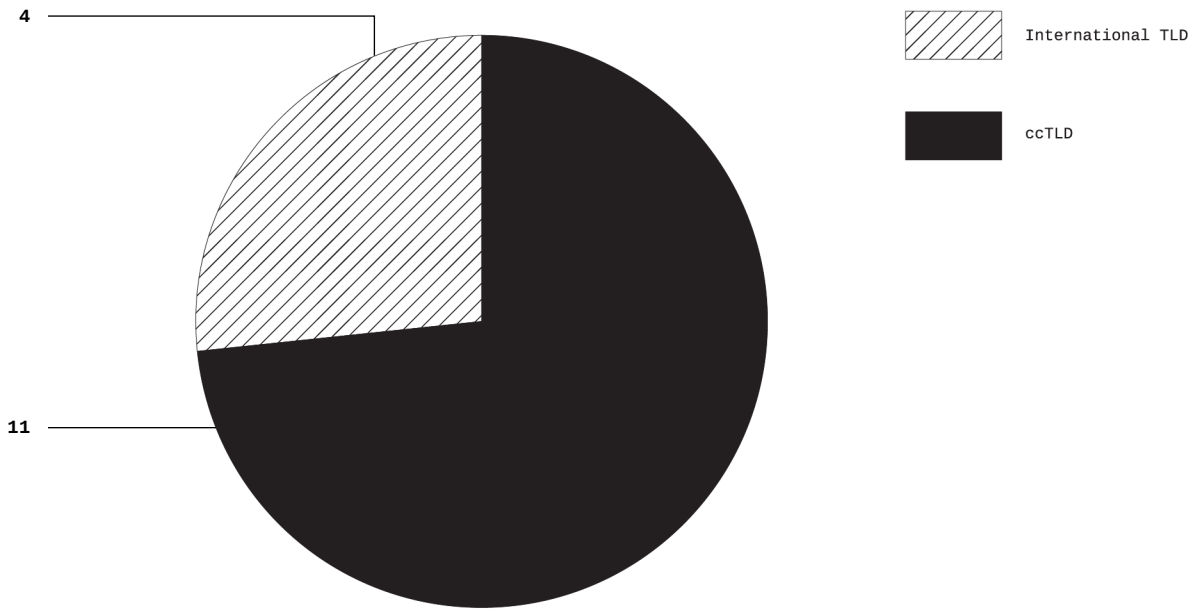
All TLDs are covered by ICANN's Uniform Domain-Name Dispute-Resolution Policy (UDRP) as a potential means of a targeted website to pursue legal action against fake domains. The UDRP process is begun when the complaint alleges an abusive registration of a domain, in our case a fake domain targeting an existing website.

Such a complaint requires (in part) that the "domain name is identical or confusingly similar to a trademark or service mark in which the complainant has rights," probably not a difficult threshold for the fake domains with mirrored layouts, logo, designs, or content.[11]

However, submission to the UDRP dispute process is only voluntary for ccTLDs.[12] Because of this, some ccTLDs (including .uk, .de, .us, .cn, .in, and .ru) lie outside the UDRP and require disputes to be pursued through their own dispute resolution services or national civil courts.[13] In data we received, many fake domains were registered under national registries as opposed to international registries.

Situations where the dispute arbitrator is a national body related to the perpetrator of the fake domain attack could result in a difficult appeals process. Even so, we have seen examples of attacks where the fake domain was registered with an unrelated country's ccTLD. Many of the Belarusian fake domains we saw were registered not .by (Belarus' national registry) but on .in, the ccTLD for India. Though the Indian registry uses its own dispute resolution process outside of the UDRP, a Belarusian target may still be able to work with the registry to take down the fake domains.

**CCTLD VS INTERNATIONAL TLDS USED BY FAKE DOMAINS**




Some national laws, such as the U.S. Anticybersquatting Consumer Protection Act (ACPA) of 1999, provide similar guidance as the UDRP towards mitigating fake domain attacks at the domain registrar level. Complaints

11 UDRP 4(a)(i). https://www.icann.org/en/help/dndr/udrp/policy

12 http://www.icann.org/registrar-reports/accredited-list.html

13 http://www.wipo.int/amc/en/domains/cctld/

can include "an Internet domain name or other identifier of an online location that is (i) the trademark of a person or entity other than the person or entity registering or using the identifier; or (ii) sufficiently similar to a trademark of a person or entity other than the person or entity registering or using the identifier as to be likely to (I) cause confusion or mistake; (II) deceive."[14]

This describes many fake domain attacks, whether the use of trademarks of other entities (such as using the BBC News logo on the fake BBC Persia website) or the confusion due to similar URLs. Regarding the similar web addresses of the fake domains to the targeted domains, US courts have ruled that "the intentional registration of domain names that are misspellings of distinctive or famous names, causing an Internet user who makes a slight spelling or typing error to reach an unintended site . . . is a classic example of a specific practice the ACPA was designed to prohibit."[15]

In addition, the "trademarks" that the ACPA seeks to protect includes both registered trademarks and unregistered common-law marks, providing additional flexibility for targeted organizations and websites that may have not formally registered a trademark.[16]

These mitigation strategies take a long period of time to adjudicate either internationally or nationally. Directing efforts towards other services in the "stack" may be a stronger strategy in the short-term, though for some large organizations with time like the BBC approaching the registrar may be a viable method. However, the national control of ccTLDs presents unique difficulties for the many fake domains that use ccTLDs, especially if those ccTLDs are not voluntarily part of the UDRP process. This includes all of the fake Belarus domains, which utilized .in and would require interaction with the Indian domain registry.

The Iranian fake domains present an interesting case, as all of them fall under that UDRP process -- .co and .ir. Given that one can go through the UDRP process without exhausting the option of going through the national dispute process (and vice versa), how such a dispute would ultimately be handled is unclear. At minimum, such an activity would likely raise awareness and create public pressure on the specific fake domain and the national registry that may protect it.

**KEEPING SIGHT OF YOUR DOMAIN NAME**

**While a civil society organization's website can be the target of a variety of attacks, maintaining ownership over the domain name itself is one of the most important ways to prevent the hijacking of an organization's identity and users. This point was emphasized by the experience of the Information-Analytic Center Eurasia, a research center sponsored in part by the main opposition party in Kazakhstan, the Republican People's Party of Kazakhstan. In mid-2012 the ownership of their original domain name (eurasia.org.ru) was transferred away from the original owners and they were unable to reclaim it. The new owners immediately removed all political analysis and content from the website, leaving the old owners to rebuild their website at neweurasia.info. To better protect a domain name against malicious ownership transfers, lock the transfer of your domain name and choose a domain registry and registrar that would not be politically influenced.**

14 See ACPA Section 4:2(i-ii), http://thomas.loc.gov/cgi-bin/query/z?c106:S.1255.IS:=

15 Shields v. Zuccarini, 254 F3d 476 (3d Cir. 2001), ¶32 and ¶35. See: http://openjurist.org/254/f3d/476/joseph-shields-the-joe-cartoon-company-v-john-zuccarini-cupcake-city.

16 Martin Samson, "The Anticybersquatting Consumer Protection Act: Key Information", New York Law Journal, Sept 9, 2005: http://www.internetlibrary.com/publications/anticybsquattSamson9-05_art.cfm.

## LEVEL 2: NATIONAL TELCOS AND PRIVATE ISPS

The fake domain attacks in Belarus and Kazakhstan highlight the important (and potentially dangerous) role telecommunications companies play between the user and the greater internet. In both cases, a state-run telco which services the vast majority of the population of the country redirected requests made to an opposition media website over to a fake domain of that organization. Presumably, a telco would carry out this action at the behest of the state government or ruling party.[17]

The nexus between governments and corporations has received increasing attention in international human rights forums. The UN Guiding Principles on Business and Human Rights define the responsibilities of states and business enterprises to protect and respect human rights. To mitigate governmental attacks on human rights committed through telcos, there are strategies affected users and organizations can use to work with governments and telecommunication companies to help address any grievances.

### Obligations on governments

Governments have the duty to protect against human rights abuses, even those committed by third parties like corporations.[18] When state-owned or -controlled corporations are found to contribute to abuses, their activities may violate the state's own international legal obligations.[19]

Where a government instigates or fails to stop fake domain attacks carried out by ISPs or partly state-owned telcos, it is contributing to violations of the human rights of access to information and privacy, and the freedoms of expression and association. The state must cease the abuse, take steps to ensure non-repetition, and provide access to effective remedy for those adversely affected. Legal recourse by affected users should leverage a these obligations in attempts to alleviate human rights abuses.

### Telcos and ISPs

Distilling international norms, Access has produced pragmatic guides to help telcos, ISPs and other information and communication technology (ICT) companies better prepare for, mitigate, and remedy their human rights impacts. The Access Telco Action Plan[20] recommends that, when faced with requests to restrict user rights or otherwise contribute to human rights abuses, telcos should:

1. Scrutinize the request to ensure that it is compliant with all relevant legal or regulatory requirements. Requests should be submitted in writing, signed by the proper official, and state the legal basis for the request.

2. Evaluate the potential to avoid or limit responses to government requests through unilateral or multi-stakeholder advocacy.

17 While the more common abuses involve government access to user data or disruption of networks, telcos have been enlisted in political propaganda and misinformation campaigns. In early 2011, after pressuring its major telcos to shutdown the internet, Egypt requested the companies send pro-regime text messages to all subscribers. They complied with the first request, but one telco pushed back by refusing to send a second, and the government relented.

18 UN Guiding Principles on Business and Human Rights, http://www.business-humanrights.org/media/documents/ruggie/ruggie-guiding-principles-21-mar-2011.pdf. States may breach their international human rights law obligations where abuse by private businesses "can be attributed to them, or where they fail to take appropriate steps" to curtail and redress the abuse. Guiding Principle 1.

19 Id. Per Guiding Principle 4, the state's duties increase depending on the context: "[t]he closer a business enterprise is to the State, or the more it relies on statutory authority or taxpayer support, the stronger the State's policy rationale becomes for ensuring that the enterprise respects human rights."

20 https://www.accessnow.org/page/-/docs/Telco_Action_Plan.pdf

3. Narrowly interpret and enforce the request in the least restrictive means and shortest duration possible so as to maximize the protection of users' access, freedom of expression, and privacy. For unclear or vague requests, seek clarification from government authorities, or legally challenge the request. Reject any request inconsistent with local law, regulatory requirements, or contractual provisions.

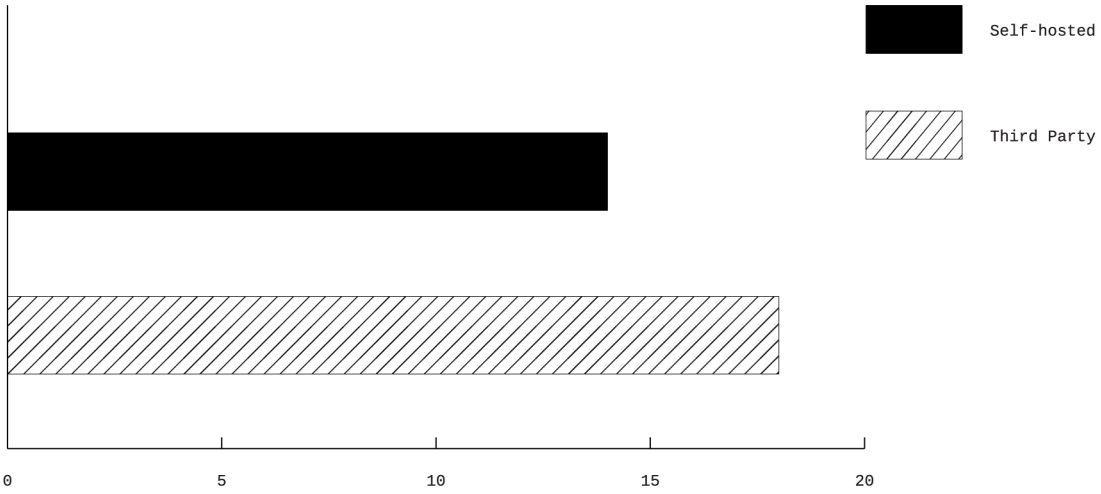
**Remedy**

If they have contributed to violations, telcos should immediately cease the harmful activities and "provide for or cooperate in their remediation through legitimate processes."[21] In addition to shutting down the fake domains, this means telcos should offer and advertise channels for those affected to communicate grievances and find adequate redress. Clear, responsive, and effective grievance mechanisms are explored in the Access Telco Remedy Plan,[22] and include user notification measures, appeals provisions, and transparent multistakeholder engagement.

## LEVEL 3: WEB HOSTS (SELF-HOSTED AND THIRD-PARTIES)

Long-term fake domain attacks to shape public opinion may be the most difficult form of fake domain attack to mitigate. For self-hosted fake domains, the domain registrar and hosting provider of the fake website ought to be engaged. There are cases, however, where this might be difficult. The fake Farsi Voice of America website, for example, was registered on .ir and was hosted in Iran. And while the Belarusian '.in' domains had Indian registries, they too were hosted on IP addresses from the national Belarusian telco Belpak. In circumstances like these, where the hosting provider is located in the same state that is likely perpetrating or supporting the fake domain, there may be little legal recourse against the web host.

**OBSERVED FAKE DOMAIN HOSTS, SELF-HOSTED VS. THIRD PARTY**




21 Guiding Principle 22.

22 https://www.accessnow.org/telco-remedy-plan

For fake domains hosted on third-party platforms (e.g. Facebook, Blogspot), successfully taking down the fake domain is dependent on the jurisdiction of the platform, the jurisdiction of the original targeted website, and what existing legal obligations the platform has with the jurisdiction, if any. In addition, having existing relationships with the platform providers may provide a faster and more responsive resolution to these attacks. Through relationship-building between the targeted civil society organization and the service provider, the mitigation strategy for these types of domain attacks could be improved. Third-party hosted domains and social media profiles also provide other avenues for recourse.

## LEVEL 4: ACCOUNTS (INCLUDING SOCIAL MEDIA PROFILES)

Fake profiles and accounts on social media websites are one additional component of third-party hosted content for which recourse exists.

At present, the companies vary in how exactly they address the possibility of a fake account. Twitter does not automatically verify accounts and has a more open parody policy, while Facebook and Google+ require users to give their real names, though these names are not verified.

Nearly all social media companies examined -- Facebook, Twitter, Google+, FriendFeed -- have Terms of Service that feature procedures for challenging the legitimacy of a domain or content hosted on the platform.

**For an overview of some of the ways to contact these companies and inform them of fake profiles on their service, please see the appendix "Removing Fake Profiles on Social Media Websites."**

Ideally, those procedures should conform to due process principles to help ensure users are not deprived of their legitimate content. For example, the users should be notified when their domain name is challenged or alleged to be infringing.

**The process should be adversarial--both the challenger and the holder of the domain name should be provided an opportunity to argue their case, and there should be an appeals mechanism to any decision.**

Given the threat to digital freedoms posed by fake domains, disputes should be overseen by specifically trained staff with human rights expertise.

For organizations that are not companies and not individuals, it is more difficult for groups that are victims of fake accounts to prove abuse. In these cases there is a chance the organizations are not officially registered with the government. Without official identification, a third-party social media outlet would have a harder time arbitrating fake account claims. This becomes even more difficult if the group works in a hostile political climate, where the organization wishes to maintain its anonymity or simply cannot receive governmental recognition.

When addressing social networking sites for grievances, it is helpful that you provide all the necessary information the website requests in order to receive a timely response.

# V. CONCLUSION

Fake domain attacks go beyond the phishing attacks for banking information or commercial gain traditionally understood to involve fake domains -- they represent a significant front some state-aligned actors are waging against independent media and civil society organizations.

The attacks analyzed in this report tend to fall within two categories:

- State-aligned actors targeting the websites of popular alternative news organizations to instead promote state-supporting content. This was often done in conjunction with domestic blocking of the original website. This attack was most frequently seen in Iran, and was also seen in Belarus and Kazakhstan.
- State-aligned actors targeting the websites of popular independent organizations with malware to compromise the security of users who frequent these websites. This has been seen most frequently in Vietnam and Belarus.

We have observed these attacks on the eves of elections and other important political events, including during critical social and political periods. Such attacks in Iran and Belarus attempted to minimize the spread of information and disrupt potential civil unrest during political elections and anniversaries.

Other attacks in Belarus and Kazakhstan utilized the privileged position internet service providers (ISPs) have in a user's interaction with websites to redirect them away from targeted websites to the fake websites. In addition, many fake domains took advantage of procuring similarly-named URLs as the targeted website in order to provide a sense of trust to the unwary user.

Since fake domain attacks require the resources of many levels of service providers, from national and international domain registries down to social networks, the targets of fake domains have many potential avenues of recourse against attack.

1. Depending on the registry of the fake domains, owners of targeted domains can potentially appeal the status of a fake domain's registration via ICANN's Uniform Domain-Name Dispute-Resolution Policy or the appropriate national domain arbitration process.
2. Failing a solution at the registry-level, when a national ISP or telecommunications company is involved in perpetrating the attack, as in the case of Belarus and Kazakhstan, there ought to be recourse via the government or company where human rights obligations are at stake. The Access Telco Remedy Plan provides a framework for telcos to address such user grievances.
3. When commercial or 3rd-party web hosts are involved in serving the fake domain, these entities may have paths for affected users to fight against a fake domain attack. Unfortunately in many cases, such as with the fake Farsi Voice of America page, a self-hosted website does not provide such an avenue for appeal. In addition, this is made more difficult if the host of the website is an entity associated with the attacker, which could be in the case in pro-government fake domain attacks.

4. Nearly all social media outlets -- Facebook, Twitter, Blogspot, Google+, and more -- have Terms of Service that allow for challenges against accounts impersonating individuals or organizations. The creation of fake social media accounts has been observed in several of the attacks we looked at in this report -- the attack against the independent Vietnamese media organization in particular used a strong social media presence to direct users to the fake domains. The spread of such attacks can been mitigated through these challenge processes with the relevant company.

Global civil society is at risk -- by providing the technical, legal, and policy frameworks for mitigating these attacks, this report should give human rights defenders the tools and understanding needed to better protect themselves and their work in an increasingly hostile digital world.

# APPENDIX

## DATA TABLE

Below is a table of data points used in this report.

| NAME | ASSOCIATED COUNTRY | TARGET DOMAIN | SUPPORTIVE DOMAINS | FAKE DOMAIN | FAKE SUPPORTIVE DOMAINS |
|---|---|---|---|---|---|
| BBC Persian | Iran | • bbcpersian.com<br>• bbc.co.uk/persian | - | • persianbbc.ir<br>• bbcpersia.ir | - |
| Voice of America Farsi | Iran | • ir.voanews.com | - | • voa-farsi.ir | - |
| Saham News | Iran | • sahamnews.org | - | • sahamnew.org | - |
| Khodnevis | Iran | • khodnevis.org | • facebook.com/khodnevis1<br>• friendfeed.com/khodnevis1<br>• twitter.com/khodnevis_org | • khodnevis.co | • facebook.com/khodnevis2<br>• friendfeed.com/khodnevis2<br>• twitter.com/khodnevis1 |
| Kaleme | Iran | • kaleme.com | - | • kalame.co | - |
| Khabar Online | Iran | • khabaronline.ir | • facebook.com/www.khabaronline.ir | • khabareonline.ir | - |
| Charter 97 | Belarus | • charter97.org | • charter97.eu<br>• charter97.info | • charter97.in | - |
| Belarus Partisan | Belarus | • belaruspartisan.org | 0 | • belaruspartisan.in | - |

| NAME | ASSOCIATED COUNTRY | TARGET DOMAIN | SUPPORTIVE DOMAINS | FAKE DOMAIN | FAKE SUPPORTIVE DOMAINS |
|---|---|---|---|---|---|
| NN | Belarus | • nn.by | - | • nnby.in | - |
| Gazetaby | Belarus | • gazetaby.com | - | • gazetaby.in | - |
| UCPB | Belarus | • ucpb.org | - | • ucpb.in | - |
| EuroRadio | Belarus | • euroradio.fm | - | • euroradio.in | - |
| BCHD | Belarus | • bchd.info | - | • bchdd.in | - |
| Information Analytic Center Eurasia | Kazakhstan | • eurasia.org.ru (formerly, prior to May/June 2012) | neweurasia.tv | • eurasia.org.ru (on and after May/June 2012) | - |
| Anonymous Vietnamese Independent Media Organization (AVIMO) | Vietnam | (1) | (1) | (2) | (14) |

# HOW TO REMOVE FAKE PROFILES ON SOCIAL MEDIA WEBSITES

1. Identify the URLs of all accounts impersonating your group or self.
2. Go to the help section of the social networking site and file a report. You may be required to provide identification to help prove your identity.
    - If it is unsafe to provide such personal information:
        - Contact customer service and ask for alternative methods to prove your identity.
        - Have your followers or other group members file a complaint with the company.
3. Be aware companies have to weigh their policies on free speech and parody against your right to avoid harassment or false information.
    - Relevant help sections on commonly used social media websites:
    - Facebook: https://www.facebook.com/help/174210519303259/, https://www.facebook.com/help/167722253287296, and https://www.facebook.com/help/204039956299586
    - FriendFeed.com : https://friendfeed.com/about/contact/terms
    - Twitter: https://support.twitter.com/forms/impersonation, https://support.twitter.com/groups/56-policies-violations/topics/238-report-a-violation/articles/20170142-reporting-impersonation-accounts
    - Google+: https://support.google.com/plus/troubleshooter/1715140
4. What if there is no response from the company, or an impersonation complaint has been inadequately resolved by a company?
    - Contact an international human rights group that can help address your grievances.

**If you know of any fake domains attacks not covered in this report, please contact us at reports@accessnow.org.**