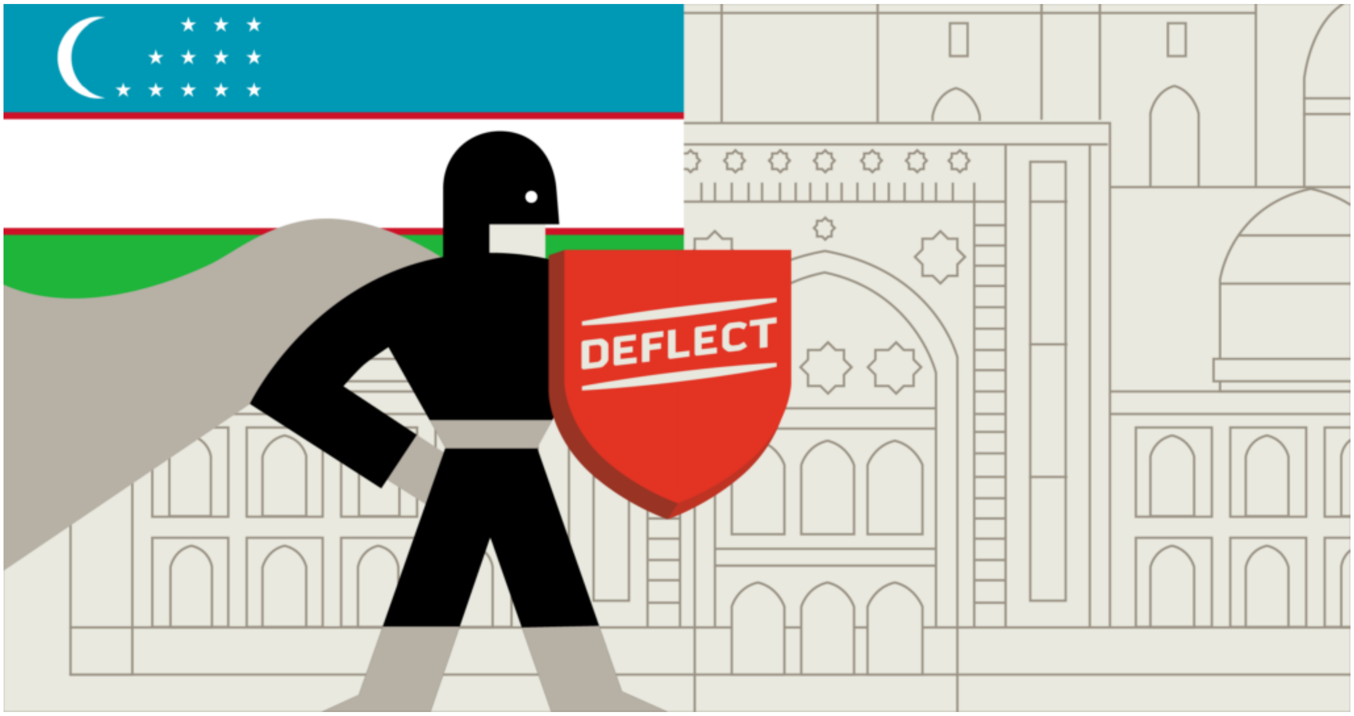
# Deflect Labs Report #6: Phishing and Web Attacks Targeting Uzbek Human Right Activists and Independent Media

equalit.ie/deflect-labs-report-6/

By Etienne

IGF MONTREAL
2024



## Key Findings

- We've discovered infrastructure used to launch and coordinate attacks targeting independent media and human rights activists from Uzbekistan
- The campaign has been active since early 2016, using web and phishing attacks to suppress and exploit their targets
- We have no evidence of who is behind this campaign but the target list points to a new threat actor targeting Uzbek activists and media

## Introduction

The Deflect project was created to protect civil society websites from web attacks, following the publication of "Distributed Denial of Service Attacks Against Independent Media and Human Rights Sites report by the Berkman Center for Internet & Society. During that time we've investigated many DDoS attacks leading to the publication of several reports.

The attacks leading to the publication of this report quickly stood out from the daily onslaught of malicious traffic on Deflect, at first because they were using professional vulnerability scanning tools like Acunetix. The moment we discovered that the origin server of these scans was also hosting fake gmail domains, it became evident that something bigger was going on here.

In this report, we describe all the pieces put together about this campaign, with the hope to contribute to public knowledge about the methods and impact of such attacks against civil society.

## Context : Human Rights and Surveillance in Uzbekistan

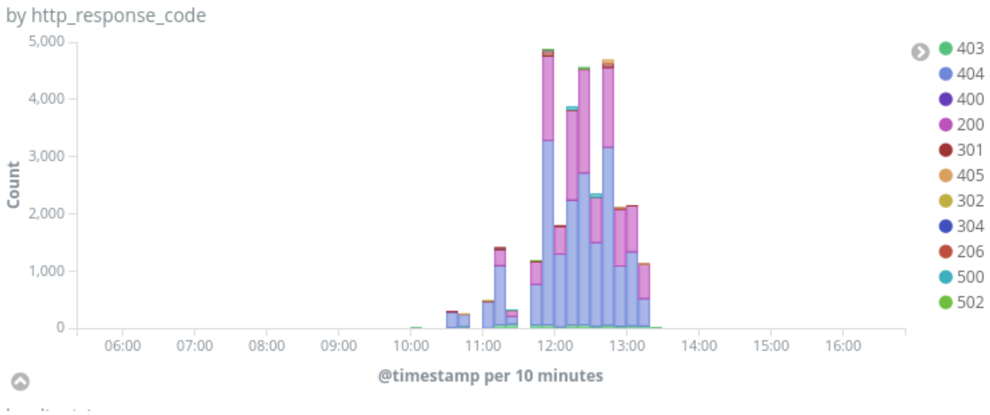
Uzbekistan is defined by many human-rights organizations as an authoritarian state, that has known strong repression of civil society. Since the collapse of the Soviet Union, two presidents have presided over a system that institutionalized  torture and repressed freedom of expression, as documented over the years by Human Rights Watch, Amnesty International and Front Line Defenders, among many others. Repression extended to media and human rights activists in particular, many of whom had to leave the country and continue their work in diaspora.

Emblem of Uzbekistan (wikipedia)

Uzbekistan was one of the first to establish a pervasive Internet censorship infrastructure, blocking access to media and human rights websites. Hacking Team servers in Uzbekistan were identified as early as 2014 by the Citizen Lab. It was later confirmed that Uzbek National Security Service (SNB) were among the customers of Hacking Team solutions from leaked Hacking Team emails. A Privacy International report from 2015 describes the installation in Uzbekistan of several monitoring centers with mass surveillance capabilities provided by the Israeli branch of the US-based company Verint Systems and by the Israel-based company NICE Systems. A 2007 Amnesty International report entitled 'We will find you anywhere' gives more context on the utilisation of these capabilities, describing digital surveillance and targeted attacks against Uzbek journalists and human-right activists. Among other cases, it describes the unfortunate events behind the closure of uznews.net – an independent media website established by Galima Bukharbaeva in 2005 following the Andijan massacre. In 2014, she discovered that her email account had been hacked and information about the organization, including names and personal details journalists in Uzbekistan was published online. Galima is now the editor of Centre1, a Deflect client and one of the targets of this investigation.

## A New Phishing and Web Attack Campaign

On the 16th of November 2018, we identified a large attack against several websites protected by Deflect. This attack used several professional security audit tools like NetSparker and WPScan to scan the websites eltuz.com and centre1.com.



Peak of traffic during the attack (16th of November 2018)

This attack was coming from the IP address 51.15.94.245 (AS12876 – Online AS but an IP range dedicated to Scaleway servers). By looking at older traffic from this same IP address, we found several cases of attacks on other Deflect protected websites, but we also found domains mimicking google and gmail domains hosted on this IP address, like `auth.login.google.email-service[.]host` or `auth.login.googlemail.com.mail-auth[.]top`. We looked into passive DNS databases (using the PassiveTotal Community Edition and other tools like RobTex) and crossed that information with attacks seen on Deflect protected websites with logging enabled. **We uncovered a large campaign combining web and phishing attacks against media and activists**. We found the first evidence of activity from this group in February 2016, and the first evidence of attacks in December 2017.

The list of Deflect protected websites chosen by this campaign, may give some context to the motivation behind them. Four websites were targeted:

- **Fergana News** is a leading independent Russian & Uzbek language news website covering Central Asian countries
- **Eltuz** is an independent Uzbek online media
- **Centre1** is an independent media organization covering news in Central Asia

- **Palestine Chronicle** is a non-profit organization working on human-rights issues in Palestine

Three of these targets are prominent media focusing on Uzbekistan. We have been in contact with their editors and several other Uzbek activists to see if they had received phishing emails as part of this campaign. Some of them were able to confirm receiving such messages and forwarded them to us. Reaching out further afield we were able to get confirmations of phishing attacks from other prominent Uzbek activists who were not linked websites protected by Deflect.

Palestine Chronicle seems to be an outlier in this group of media websites focusing on Uzbekistan. We don’t have a clear hypothesis about why this website was targeted.

## A year of web attacks against civil society

Through passive DNS, we identified three IPs used by the attackers in this operation :

- 46.45.137.74 was used in 2016 and 2017 (timeline is not clear, Istanbul DC, AS197328)
- 139.60.163.29 was used between October 2017 and August 2018 (HostKey, AS395839)
- 51.15.94.245 was used between September 2018 and February 2019 (Scaleway, AS12876)

We have identified 15 attacks from the IPs 139.60.163.29 and 51.15.94.245 since December 2017 on Deflect protected websites:

| Date | IP | Target | Tools used |
|---|---|---|---|
| 2017/12/17 | `139.60.163.29` | eltuz.com | WPScan |
| 2018/04/12 | `139.60.163.29` | eltuz.com | Acunetix |
| 2018/09/15 | `51.15.94.245` | www.palestinechronicle.com eltuz.com www.fergana.info and uzbek.fergananews.com | Acunetix and WebCruiser |
| 2018/09/16 | `51.15.94.245` | www.fergana.info | Acunetix |
| 2018/09/17 | `51.15.94.245` | www.fergana.info | Acunetix |
| 2018/09/18 | `51.15.94.245` | www.fergana.info | NetSparker and Acunetix |
| 2018/09/19 | `51.15.94.245` | eltuz.com | NetSparker |
| 2018/09/20 | `51.15.94.245` | www.fergana.info | Acunetix |
| 2018/09/21 | `51.15.94.245` | www.fergana.info | Acunetix |
| 2018/10/08 | `51.15.94.245` | eltuz.com, www.fergananews.com and news.fergananews.com | Unknown |
| 2018/11/16 | `51.15.94.245` | eltuz.com, centre1.com and en.eltuz.com | NetSparker and WPScan |
| 2019/01/18 | `51.15.94.245` | eltuz.com | WPScan |
| 2019/01/19 | `51.15.94.245` | fergana.info www.fergana.info and fergana.agency | Unknown |
| 2019/01/30 | `51.15.94.245` | eltuz.com and en.eltuz.com | Unknown |
| 2019/02/05 | `51.15.94.245` | fergana.info | Acunetix |

Besides classic open-source tools like WPScan, these attacks show the utilization of a wide range of commercial security audit tools, like NetSparker or Acunetix. Acunetix offers a trial version that may have been used here, NetSparker does not, showing that the operators may have a consistent budget (standard offer is $4995 / year, a cracked version may have been used).

It is also surprising to see so many different tools coming from a single server, as many of them require a Graphical User Interface. When we scanned the IP 51.15.94.245, we discovered that it hosted a Squid proxy on port 3128, we think that this proxy was used to relay traffic from the origin operator computer.

Extract of nmap scan of 51.15.94.245 in December 2018 :

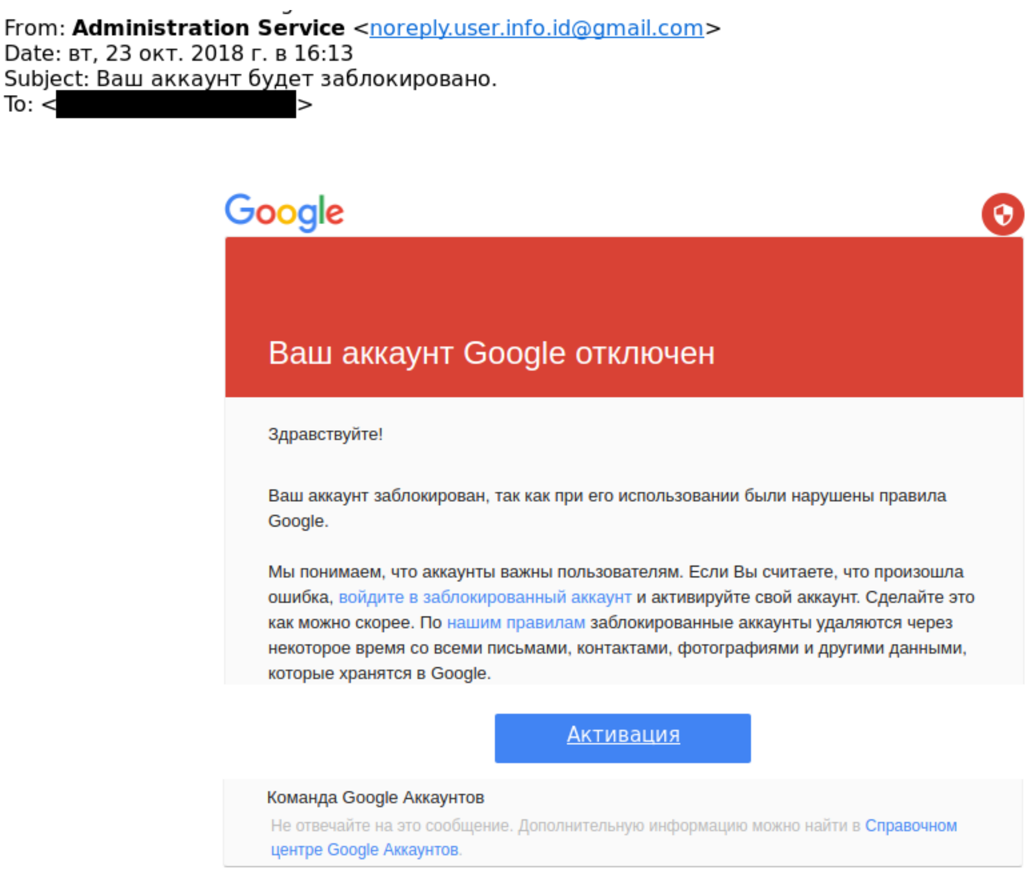
```
3128/tcp  open     http-proxy Squid http proxy 3.5.23
|_http-server-header: squid/3.5.23
|_http-title: ERROR: The requested URL could not be retrieved
```

## A large phishing campaign

After discovering a long list of domains made to resemble popular email providers, we suspected that the operators were also involved in a phishing campaign. We contacted owners of targeted websites, along with several Uzbek human right activists and gathered 14 different phishing emails targeting two activists between March 2018 and February 2019 :

| **Date** | **Sender** | **Subject** | Link |
|---|---|---|---|
| 12th of March 2018 | g.corp.sender[@]gmail.com | У Вас 2 недоставленное сообщение (You have 2 undelivered message) | `http://mail.gmal.con.my-id[.]top/` |
| 13th of June 2018 | service.deamon2018[@]gmail.com | Прекращение предоставления доступа к сервису (Termination of access to the service) | `http://e.mail.gmall.con.my-id[.]top/` |
| 18th of June 2018 | id.warning.users[@]gmail.com | Ваш новый адрес в Gmail: alexis.usa@gmail.com (Your new email address in Gmail: alexis.usa@gmail.com) | `http://e.mail.users.emall.com[.]my-id.top/` |
| 10th of July 2018 | id.warning.daemons[@]gmail.com | Прекращение предоставления доступа к сервису (Termination of access to the service) | `hxxp://gmallls.con-537d7.my-id[.]top/` |
| 10th of July 2018 | id.warning.daemons[@]gmail.com | Прекращение предоставления доступа к сервису (Termination of access to the service) | `http://gmallls.con-4f137.my-id[.]top/` |
| 18th of July 2018 | service.deamon2018[@]gmail.com | [Ticket#2011031810000512] – 3 undelivered messages | `http://login-auth-goglemail-com-7c94e3a1597325b849e26a0b45f0f068.my-id[.]top/` |
| 2nd of August 2018 | id.warning.daemon.service[@]gmail.com | [Important Reminder] Review your data retention settings | None |
| 16th of October 2018 | lolapup.75[@]gmail.com | Экс-хоким Ташкента (Ex-hokim of Tashkent) | `http://office-online-sessions-3959c138e8b8078e683849795e156f98.email-service[.]` |
| 23rd of October 2018 | noreply.user.info.id[@]gmail.com | Ваш аккаунт будет заблокировано (Your account will be blocked.) | `http://gmail-accounts-cb66d53c8c9c1b7c622d915322804cdf.email-service[.]` |
| 25th of October 2018 | warning.service.suspended[@]gmail.com | Ваш аккаунт будет заблокировано. (Your account will be blocked.) | `http://gmail-accounts-bb6f2dfcec87551e99f9cf331c990617.email-service[.]` |
| 18th of February 2019 | service.users.blocked[@]gmail.com | Важное оповещение системы безопасности (Important Security Alert) | `http://id-accounts-blocked-ac5a75e4c0a77cc16fe90cddc01c2499.myconnection[.]w` |
| 18th of February 2019 | mail.suspend.service[@]gmail.com | Оповещения системы безопасности (Security Alerts) | `http://id-accounts-blocked-326e88561ded6371be008af61bf9594d.myconnection[.]w` |
| 21st of February 2019 | service.users.blocked[@]gmail.com | Ваш аккаунт будет заблокирован. (Your account will be blocked.) | `http://id-accounts-blocked-ffb67f7dd7427b9e4fc4e5571247e812.myconnection[.]w` |
| 22nd of February 2019 | service.users.blocked[@]gmail.com | Прекращение предоставления доступа к сервису (Termination of access to the service) | `http://id-accounts-blocked-c23102b28e1ae0f24c9614024628e650.myconnection[.]w` |

Almost all these emails were mimicking Gmail alerts to entice the user to click on the link. For instance this email received on the 23rd of October 2018 pretends that the account will be closed soon, using images of the text hosted on imgur to bypass Gmail detection :



From: **Administration Service** <noreply.user.info.id@gmail.com>
Date: вт, 23 окт. 2018 г. в 16:13
Subject: Ваш аккаунт будет заблокировано.
To: <[redacted]>

Ваш аккаунт Google отключен

Здравствуйте!

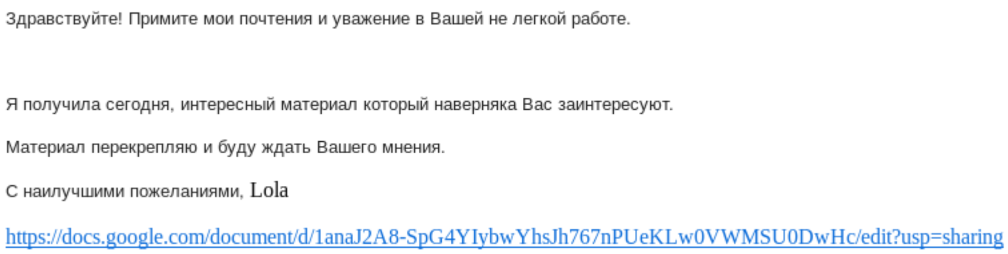
Ваш аккаунт заблокирован, так как при его использовании были нарушены правила Google.

Мы понимаем, что аккаунты важны пользователям. Если Вы считаете, что произошла ошибка, войдите в заблокированный аккаунт и активируйте свой аккаунт. Сделайте это как можно скорее. По нашим правилам заблокированные аккаунты удаляются через некоторое время со всеми письмами, контактами, фотографиями и другими данными, которые хранятся в Google.

Активация

Команда Google Аккаунтов
Не отвечайте на это сообщение. Дополнительную информацию можно найти в Справочном центре Google Аккаунтов.

The only exception was an email received on the 16th of October 2018 pretending to give confidential information on the former Hokim (governor) of Tashkent :



Здравствуйте! Примите мои почтения и уважение в Вашей не легкой работе.

Я получила сегодня, интересный материал который наверняка Вас заинтересуют.

Материал перекрепляю и буду ждать Вашего мнения.

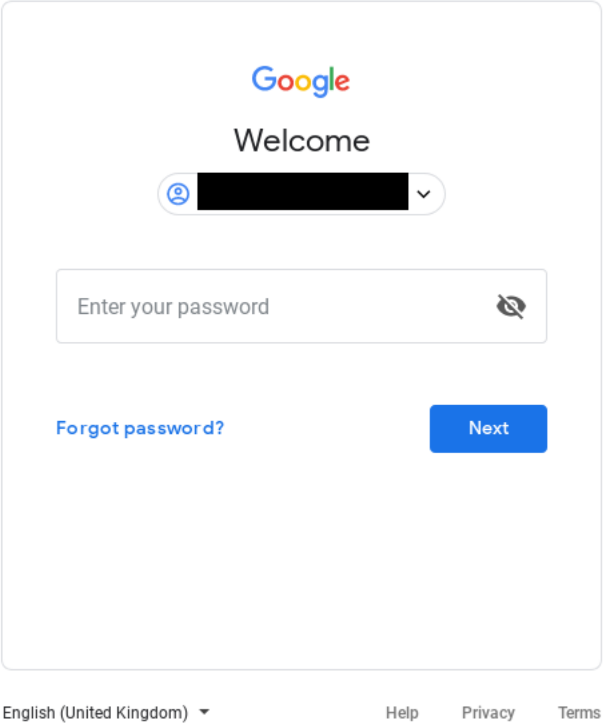
С наилучшими пожеланиями, Lola

https://docs.google.com/document/d/1anaJ2A8-SpG4YIybwYhsJh767nPUeKLw0VWMSU0DwHc/edit?usp=sharing

Emails were using simple tricks to bypass detection, at times drw.sh url shortener (this tool belongs to a Russian security company Doctor Web) or by using open re-directions offered in several Google tools.

Every email we have seen used a different sub-domain, including emails from the same Gmail account and with the same subject line. For instance, two different emails entitled “Прекращение предоставления доступа к сервису” and sent from the same address used `hxxp://gmallls.con-537d7.my-id[.]top/` and `http://gmallls.con-4f137.my-id[.]top/` as phishing domains. We think that the operators used a different sub-domain for every email sent in order to bypass Gmail list of known malicious domains. This would explain the large number of sub-domains identified through passive DNS. We have identified 74 sub-domains for 26 second-level domains used in this campaign (see the appendix below for  full list of discovered domains).

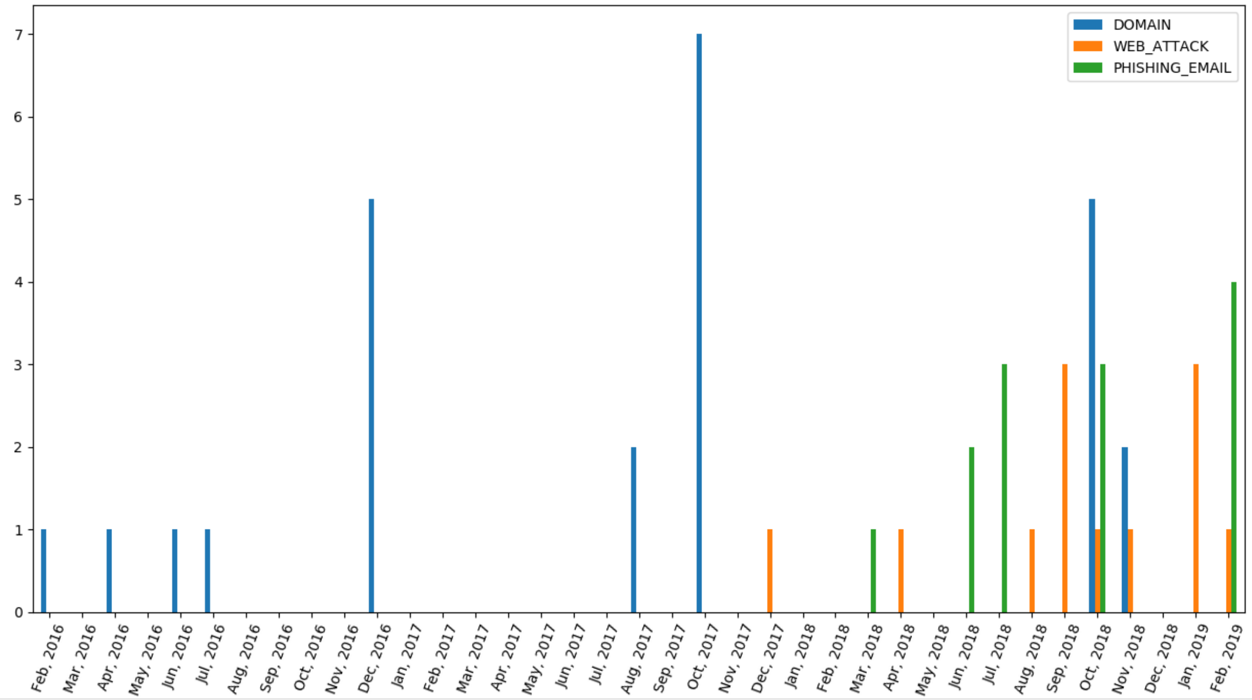
We think that the phishing page stayed online only for a short time after having sent the email in order to avoid detection. We got access to the phishing page of a few emails. We could confirm that the phishing toolkit checked if the password is correct or not (against the actual gmail account) and suspect that they implemented 2 Factor authentication for text messages and 2FA applications, but could not confirm this.



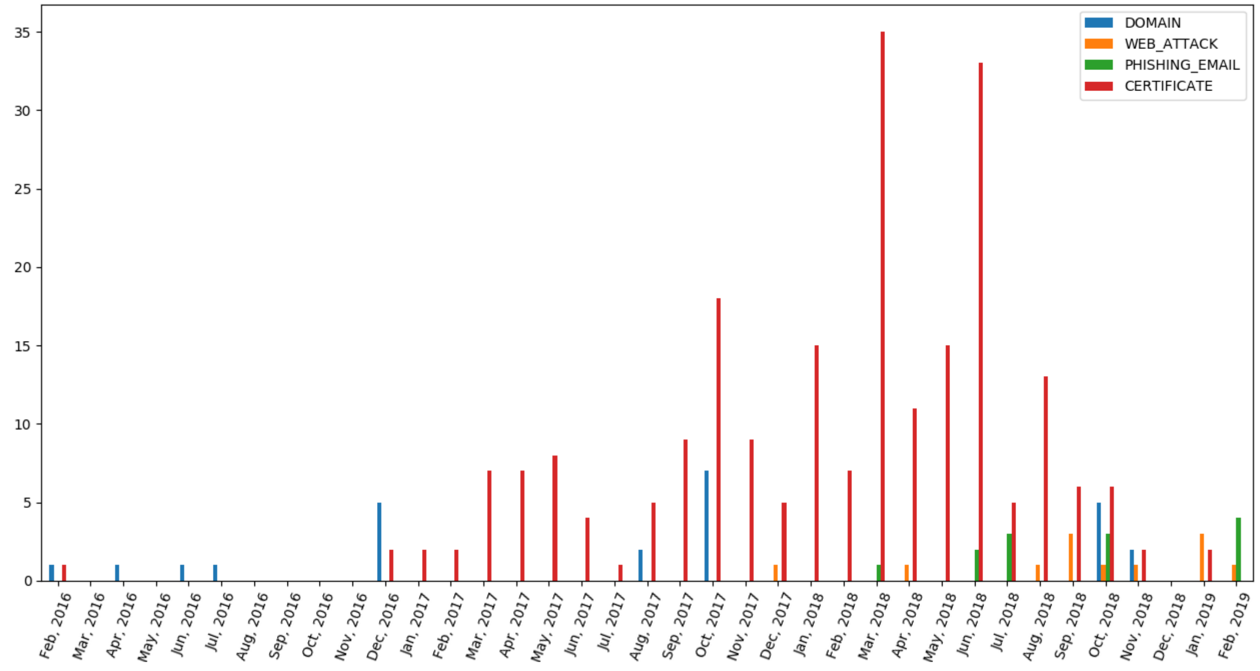
## Timeline for the campaign

We found the first evidence of activity in this operation with the registration of domain `auth-login[.]com` on the 21st of February 2016. Because we discovered the campaign recently, we have little information on attacks during 2016 and 2017, but the domain registration date shows some activity in July and December 2016, and then again in August and October 2017. It is very likely that the campaign started in 2016 and continued in 2017 without any public reporting about it.

Here is a first timeline we obtained based on domain registration dates and dates of web attacks and phishing emails :



To confirm that this group had some activity during 2016 and 2017, we gathered encryption (TLS) certificates for these domains and sub-domains from the crt.sh Certificate Transparency Database. We identified 230 certificates generated for these domains, most of them created by Cloudfare. Here is a new timeline integrating the creation of TLS certificates :

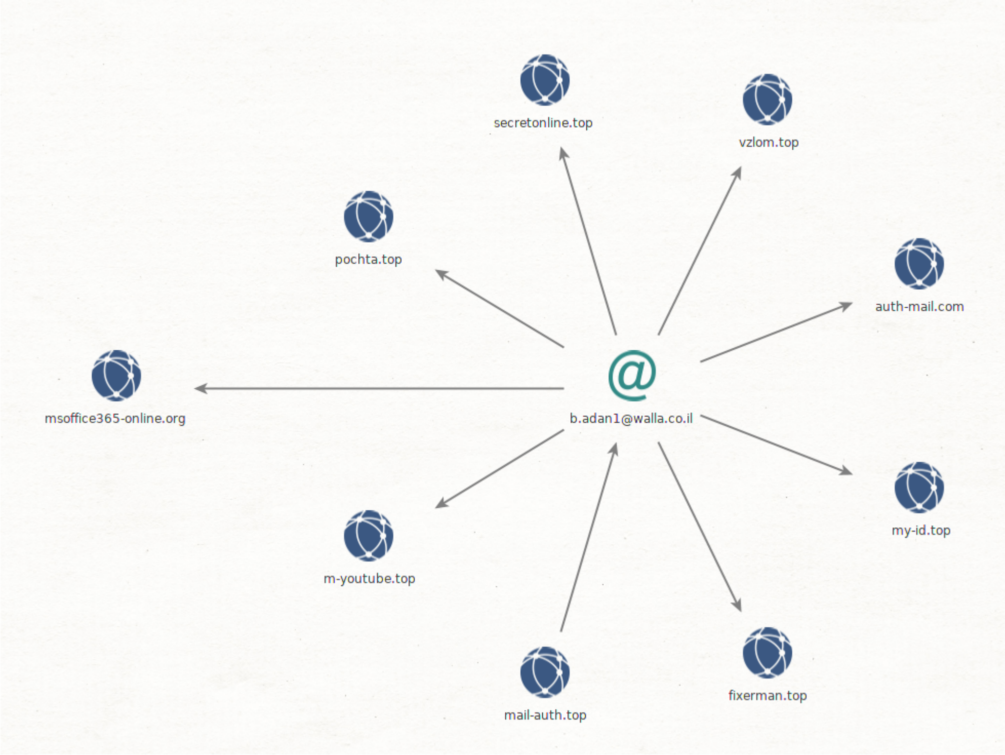


We see here many certificates created since December 2016 and continuing over 2017, which shows that this group had some activity during that time. The large number of certificates over 2017 and 2018 comes from campaign operators using Cloudflare for several domains. Cloudflare creates several short-lived certificates at the same time when protecting a website.

It is also interesting to note that the campaign started in February 2016, with some activity in the summer of 2016, which happens to when the former Uzbek president Islam Karimov died, news first reported by Fergana News, one of the targets of this attack campaign.

## Infrastructure Analysis

We identified domains and subdomains of this campaign through analysis of passive DNS information, using mostly the Community access of PassiveTotal. Many domains in 2016/2017 reused the same registrant email address, `b.adan1@walla.co.il` , which helped us identify other domains related to this campaign :



Based on this list, we identified subdomains and IP addresses associated with them, and discovered three IP addresses used in the operation. We used Shodan historical data and dates of passive DNS data to estimate the timeline of the utilisation of the different servers :

- 46.45.137.74 was used in 2016 and 2017
- 139.60.163.29 was used between October 2017 and August 2018
- 51.15.94.245 was used between September and February 2019

We have identified 74 sub-domains for 26 second-level domains used in this campaign (see the appendix for a full list of IOCs). Most of these domains are mimicking Gmail, but there are also domains mimicking Yandex ( `auth.yandex.ru.my-id[.]top` ), mail.ru ( `mail.ru.my-id[.]top` ) qip.ru ( `account.qip.ru.mail-help-support[.]info` ), yahoo ( `auth.yahoo.com.mail-help-support[.]info` ), Live ( `login.live.com.mail-help-support[.]info` ) or rambler.ru ( `mail.rambler.ru.mail-help-support[.]info` ). Most of these domains are sub-domains of a few generic second-level domains (like `auth-mail.com` ), but there are a few specific second-level domains that are interesting :

- `bit-ly[.]host` mimicking bit.ly
- `m-youtube[.]top` and `m-youtube[.]org` for Youtube
- `ecoit[.]email` which could mimick https://www.ecoi.net
- `pochta[.]top` likely mimick https://www.pochta.ru/, the Russian Post website
- We have not found any information on `vzlom[.]top` and `fixerman[.]top` . Vzlom means “break into” in Russian, so it could have hosted or mimicked a security website

## A weird Cyber-criminality Nexus

It is quite unusual to see connections between targeted attacks and cyber-criminal enterprises, however during this investigation we encountered two such links.

The first one is with the domain `msoffice365[.]win` which was registered by `b.adan1@walla.co.il` (as well as many other domains from this campaign) on the 7th of December 2016. This domain was identified as a C2 server for a cryptocurrency theft tool called Quant, as described in this Forcepoint report released in December 2017. Virus Total confirms that this domain hosted several samples of this malware in November 2017 (it was registered for a year). We have not seen any malicious activity from this domain related to our campaign, but as explained earlier, we have marginal access to the group’s activity in 2017.

The second link we have found is between the domain `auth-login[.]com` and the groups behind the Bedep trojan and the Angler exploit kit. `auth-login[.]com` was linked to this operation through the subdomain `login.yandex.ru.auth-login[.]com` that fit the pattern of long subdomains mimicking Yandex from this campaign and it was hosted on the same IP address 46.45.137.74 in March and April 2016 according to RiskIQ. This domain was registered in February 2016 by `yingw90@yahoo.com` (David Bowers from Grovetown, GA in the US according to whois information). This email address was also used to register hundreds of domains used in a Bedep campaign as described by Talos in February 2016 (and confirmed by several other reports). Angler exploit kit is one of the most notorious exploit kit, that was commonly used by cyber-criminals between 2013 and 2016. Bedep is a generic backdoor that was identified in 2015, and used almost exclusively with the Angler exploit kit. It should be noted that Trustwave documented the utilization of Bedep in 2015 to increase the number of views of pro-Russian propaganda videos.

Even if we have not seen any utilisation of these two domains in this campaign, these two links seem too strong to be considered cirmcumstantial. These links could show a collaboration between cyber-criminal groups and state-sponsored groups or services. It is interesting to remember the potential involvement of Russian hacking groups in attacks on Uznews.net editor in 2014, as described by Amnesty international.

## Taking Down Servers is Hard

When the attack was discovered, we decided to investigate without sending any abuse requests, until a clearer picture of the campaign emerged. In January, we decided that we had enough knowledge of the campaign and started to send abuse requests – for fake Gmail addresses to Google and for the URL shorteners to Doctor Web. We did not receive any answer but noticed that the Doctor Web URLs were taken down a few days after.

Regarding the Scaleway server, we entered into an unexpected loop with their abuse process.  Scaleway operates by sending the abuse request directly to the customer and then asks them for confirmation that the issue has been resolved. This process works fine in the case of a compromised server, but does not work when the server was rented intentionally for malicious activities. We did not want to send an abuse request because it would have involved giving away information to the operators. We contacted Scaleway directly and it took some time to find the right person on the security team. They acknowledged the difficulty of having an efficient Abuse Process, and after we sent them an anonymized version of this report along with proof that phishing websites were hosted on the server, they took down the server around the 25th of January 2019.

Being an infrastructure provider, we understand the difficulty of dealing with abuse requests. For a lot of hosting providers, the number of requests is what makes a case urgent or not. We encourage hosting providers to better engage with organisations working to protect Civil Society and establish trust relationships that help quickly mitigate the effects of malicious campaigns.

## Conclusion

In this report, we have documented a prolonged phishing and web attack campaign focusing on media covering Uzbekistan and Uzbek human right activists. It shows that once again, digital attacks are a threat for human-right activists and independent media. There are several threat actors known to use both phishing and web attacks combined (like the Vietnam-related group Ocean Lotus), but this campaign shows a dual strategy targeting civil society websites and their editors at the same time.

We have no evidence of government involvement in this operation, but these attacks are clearly targeted on prominent voices of Uzbek civil society. They also share strong similarities with the hack of Uznews.net in 2014, where the editor's mailbox was compromised through a phishing email that appeared as a notice from Google warning her that the account had been involved in distributing illegal pornography.

Over the past 10 years, several organisations like the Citizen Lab or Amnesty International have dedicated lots of time and effort to document digital surveillance and targeted attacks against Civil Society. We hope that this report will contribute to these efforts, and show that today, more than ever, we need to continue supporting civil society against digital surveillance and intrusion.

### Counter-Measures Against such Attacks

If you think you are targeted by similar campaigns, here is a list of recommendations to protect yourself.

Against phishing attacks, it is important to learn to recognize classic phishing emails. We give some examples in this report, but you can read other similar reports by the Citizen Lab. You can also read this nice explanation by NetAlert and practice with this Google Jigsaw quizz. The second important point is to make sure that you have configured 2-Factor Authentication on your email and social media accounts. Two-Factor Authentication means using a second way to authenticate when you log-in besides your password. Common second factors include text messages, temporary password apps or hardware tokens. We recommend using either temporary password apps (like Google Authenticator; FreeOTP) or Hardware Keys (like YubiKeys). Hardware keys are known to be more secure and strongly recommended if you are an at-risk activist or journalist.

Against web attacks, if you are using a CMS like WordPress or Drupal, it is very important to update both the CMS and its plugins very regularly, and avoid using un-maintained plugins (it is very common to have websites compromised because of outdated plugins). Civil society websites are welcome to apply to Deflect for free website protection.

## Appendix

## Acknowledgement

We would like to thank Front Line Defenders and Scaleway for their help. We would also like to thank ipinfo.io and RiskIQ for their tools that helped us in the investigation.

## Indicators of Compromise

Top level domains :

```
email-service.host
email-session.host
support-email.site
support-email.host
email-support.host
myconnection.website
ecoit.email
my-cabinet.com
my-id.top
msoffice365-online.org
secretonline.top
m-youtube.top
auth-mail.com
mail-help-support.info
mail-support.info
auth-mail.me
auth-login.com
email-x.com
auth-mail.ru
mail-auth.top
msoffice365.win
bit-ly.host
m-youtube.org
vzlom.top
pochta.top
fixerman.top
```

You can find a full list of indicators on github : https://github.com/equalitie/deflect_labs_6_indicators