Targeted Surveillance Attacks in Uzbekistan: An Old Threat with New Techniques

amnesty.org/en/latest/research/2020/03/targeted-surveillance-attacks-in-uzbekistan-an-old-threat-with-new-techniques/

March 12, 2020

Research March 12, 2020

Introduction

A new Amnesty International investigation has identified a campaign of phishing and spyware attacks targeting Human Rights Defenders (HRDs) from Uzbekistan.

In May 2019, the Canadian non-profit organisation eQualitie released a report describing an attack campaign using web and phishing attacks against journalists and activists working on Uzbekistan. Based on this report, we began tracking the group that was behind these attacks. We identified a broader infrastructure along with new Windows and Android spyware used by the attackers.

During the investigation, we identified a partial list of targets that confirmed that activists and journalists were targeted by this campaign. This report documents a worrying evolution in the surveillance threat facing HRDs in Uzbekistan, which now appear more sophisticated than previously documented, and able to bypass some security tools HRDs use to protect themselves against surveillance.

Human Rights and Surveillance in Uzbekistan

Amnesty International has documented serious human rights violations, including pervasive torture by security forces and arbitrary detention, in Uzbekistan. Impunity for past abuses continues to prevail despite recent reforms of the criminal justice system and the closure of detention centers notorious for torture. While more independent media outlets have now been able to operate inside Uzbekistan, the rights to freedom of expression, association and peaceful assembly continue to be tightly regulated, and civil society activists face reprisals for their peaceful activities.

The threat of torture, its actual use and sexual violence, have forced many HRDs, government critics and independent journalists to leave Uzbekistan. The few who remain in the country, including activists and journalists released from prison since 2017, and their families, have continued to be under surveillance and have faced intimidation, threats and arbitrary detention by the police and the State Security Service (SGB).

This physical surveillance and repression of Human Rights Defenders and journalists have been supported by a well developed surveillance system. A Privacy International report from 2014 described the technical capabilities deployed within the country to monitor internet and phone communications. An Amnesty International report from 2017 titled, 'We will find you, anywhere' described the threat of surveillance for HRDs including several cases of email hacking using phishing attacks. In 2018, Amnesty International published concerns about the detention and interrogation of a number users of the social media platform Facebook in Uzbekistan, based on administrative charges after they posted comments on their Facebook accounts or 'liked' and shared posts of other social media users. More recently in October 2019, Kaspersky presented the cyber-attack framework of a group called Sandcat that they attribute to the Uzbekistani State-Security Services during a conference.

Phishing using Evolving Techniques

What is phishing?

Credentials phishing (or "Password-Stealing Phishing") consists in the creation of a website that imitates the login prompt of a given online service, such as Gmail or Facebook, with the objective of luring a victim into visiting the malicious page and entering their username and passwords, thereby transmitting these credentials to the attackers.

Based on the threat report published by eQualitie, we have investigated and tracked the evolution of the fake websites and internet infrastructure used by these attackers. The group was very active between May and September 2019, when several dozens of domains were created. Many of these domains mimicked Google domains, such as acccountsgoog1e[.]com or auth-google[.]site, or generic email domains like auth-mail[.]email (Please note: the domains have been purposefully modified by Amnesty International with the marking *[.]* in order to prevent accidental clicks and visits).

Amnesty International
Screenshot of mail-auth[.]online (May 2019)

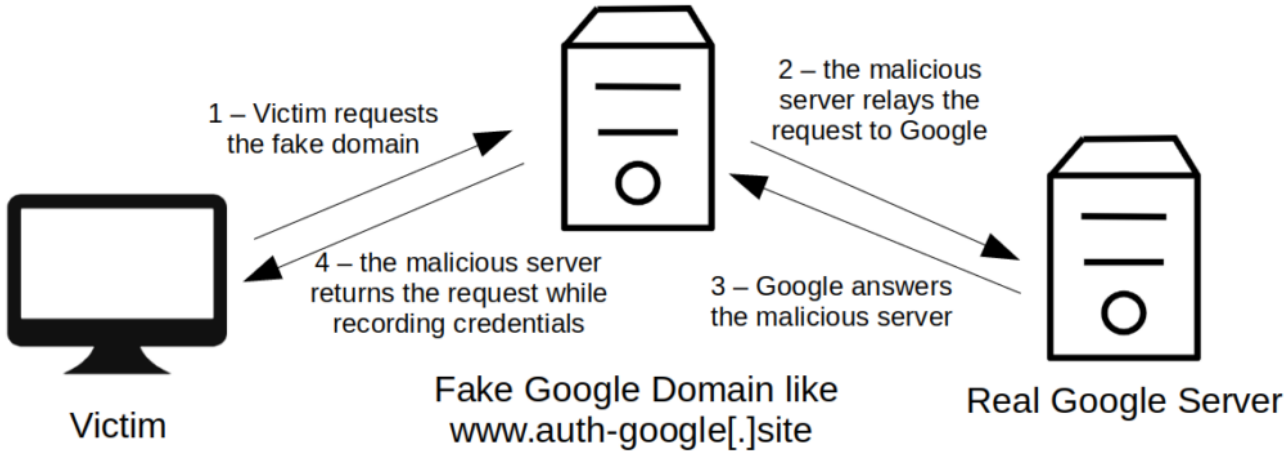
Originally the attackers used cloned pages of, for example, Google login prompts in order to lure targets and steal credentials. This is the most traditional and typical phishing technique, but it is rather simplistic. From June 2019 we observed an evolution in the phishing tactics adopted. Our research reveals that the group started to use a new phishing framework that acts as a relay between the phishing site and the real affected website, in order to bypass most forms of Two-Factor Authentication. In technical language, this technique is often referred to as "*session hijacking"* and the framework used as a *"reverse proxy"*.

What is Two-Factor Authentication (2FA)?

Two-factor authentication (often called 2FA) is the utilization of a second mean of authentication beside a password. Common second factors include a temporary code delivered by SMS, a temporary code given by a Smartphone Application (such as FreeOTP or Google Authenticator) and a code generated by a Hardware Security Key (like Yubikey or Solo Key).

Attacks bypassing some forms of second factors are not new. We published a report in December 2018 warning HRDs about them in the context of a phishing campaign with targets in the Middle-East and North-Africa. Latest attacks by this group in Uzbekistan represent the first time Amnesty International observed *session hijacking* used in attacks against HRDs, but several open-source tools published in 2018 and 2019, such as Modlishka or Muraena, have already made this capability publicly available to the information security community.

In practice, a *reverse proxy* used for phishing will intercept all credentials and any two-factor authentication code (typically retrieved via SMS or an authenticator app) and deliver them to the legitimate service, such as; in this case, Google. The service will verify the credentials and, if correct, successfully authorize the victims to their accounts. However, because the *reverse proxy* is monitoring the connection between the victim and the legitimate service, the attackers are then able to steal any token generated to establish an authenticated session and reuse it to access the compromised account.



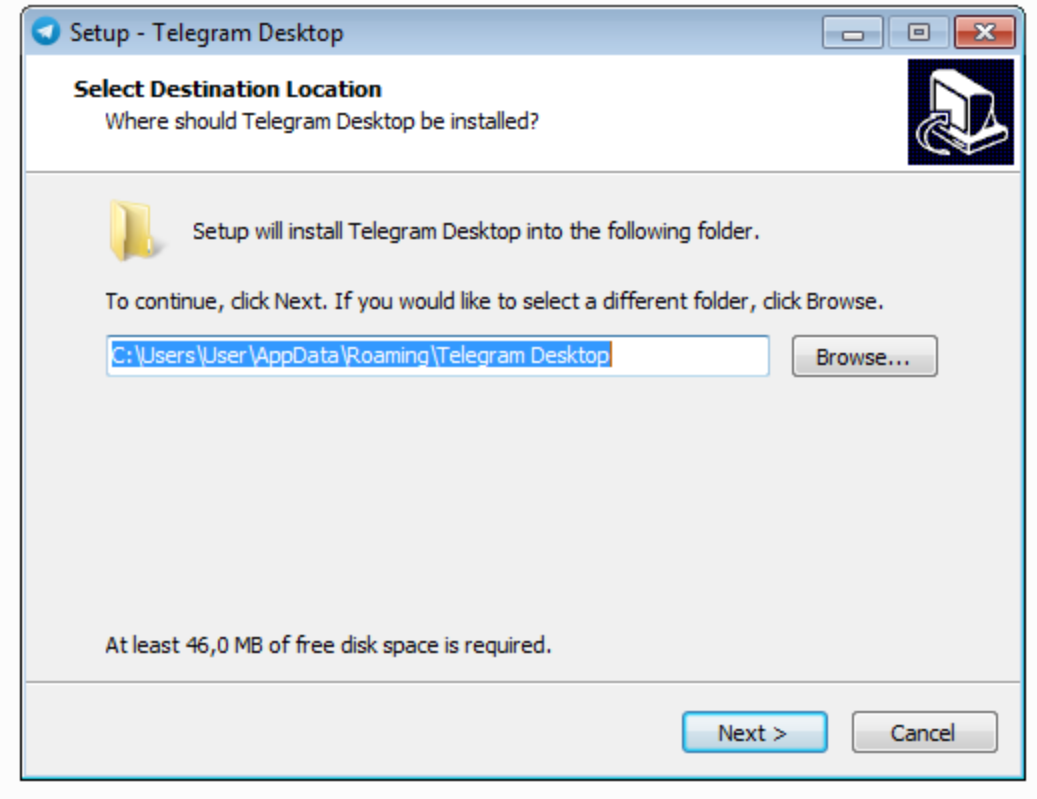
Amnesty International
Reverse-Proxy phishing attack done to bypass 2FA protection
With this technique attackers can bypass most forms of second factor authentication, except Security Keys, such as Yubikeys or SoloKeys, because these hardware tokens programmatically enter a temporary code for a preregistered website only for the verified legitimate domain. If a target is equipped with a Security Key, the phishing attack will fail because the key will refuse to authenticate on the malicious domain the attackers lured the target to.

Amnesty International

Two different hardware tokens : SoloKeys and Yubikeys

Windows Spyware

In additional to the phishing attacks, in May 2019 we also identified two malicious Windows installers hosted on the domain msoffice365[.]win, which appears linked to the previously described phishing campaign. Amnesty International identified an infected Adobe Flash Player installer and an infected Telegram Desktop installer, both deploying variants of the same spyware along with the legitimate software.



Amnesty International
Screenshot of the installer of the Telegram Desktop installer modified to install the spyware
Once infected, the spyware toolkit used by the attackers will be capable of:

- Logging all key strokes;
- Taking screenshots of the desktop every few seconds;
- Stealing password and cookies;

All the harvested data would then be sent to an attackers-operated server located at hpphhpph[.]com

The toolkit is composed of a variety of scripts seemingly developed by the attackers, and a Trojan software derived from a well-known tool known as Quasar Rat.

Android Spyware

During the investigation, we identified an Android spyware communicating with the domain garant-help[.]com, a Command and Control server we found linked to this campaign. This sample is an extended version of Droid-Watcher, an open-source Android spyware that was

discontinued by its main developer in 2016. This sample seems largely based on the original Droid-Watcher code with some additional features and updates.

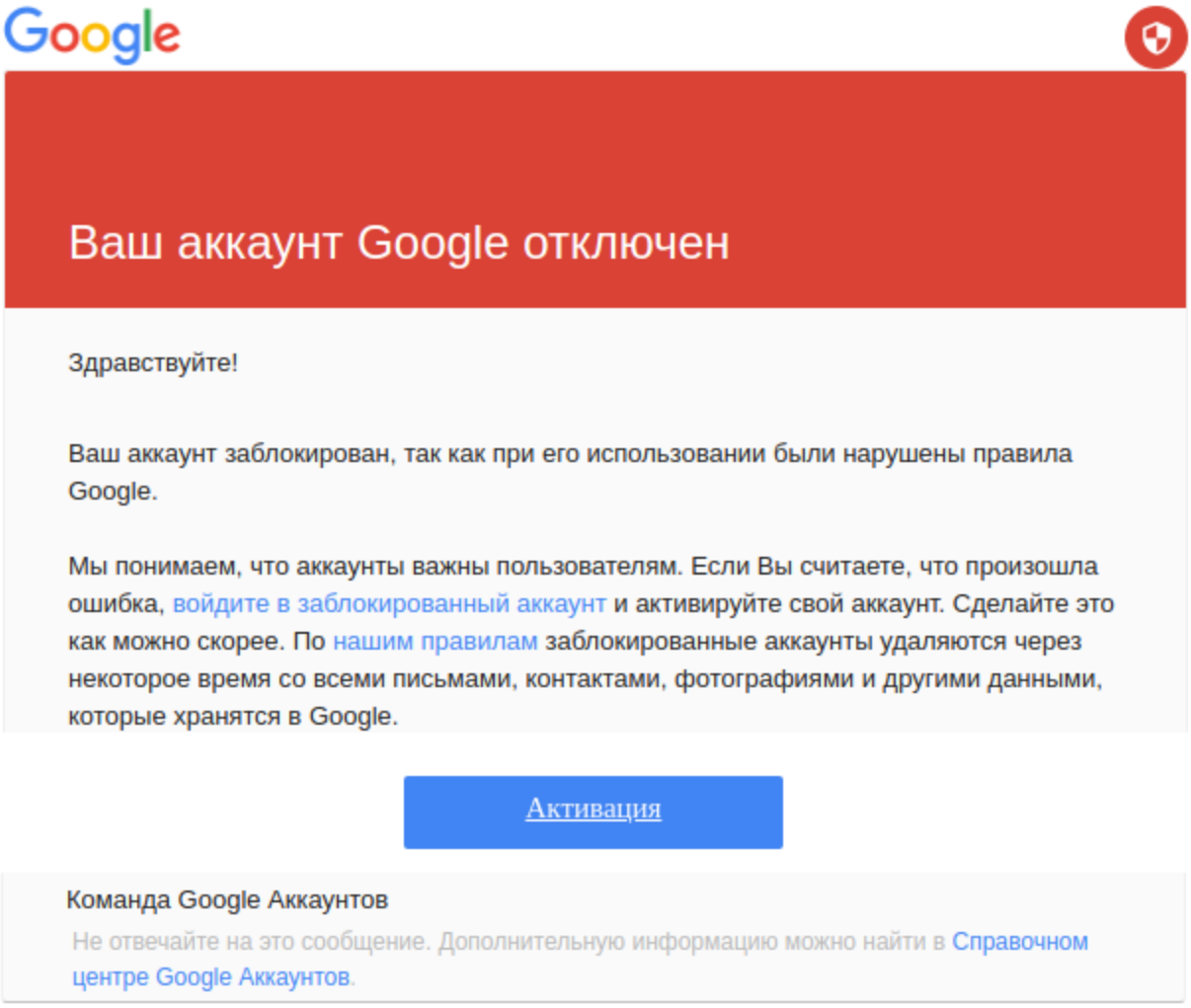
This spyware has the following features:

- Extract device information (configuration, IMEI, phone number, history of Wi-Fi networks, etc.);
- Monitor chat applications, including VKontakte, WhatsApp, Viber, Facebook, IMO, TamTam, Telegram;
- Monitor phone calls and text messages;
- Record phone calls;
- Record audio and video from the embedded microphone and cameras;
- Take screenshots;
- Monitor the clipboard;
- Monitor the geographical location of the device;
- Extract the browser history;
- Receive commands by text messages.

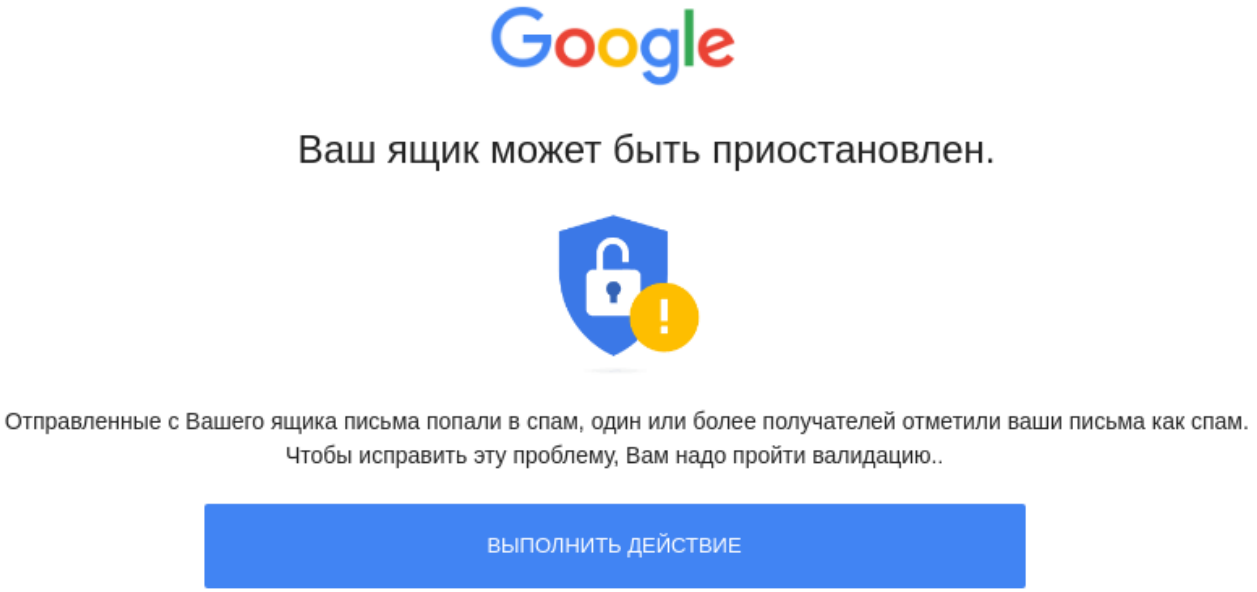
Identification of Targets

While investigating the attackers' infrastructure, we identified an open directory on one of the servers used to host phishing websites. This directory publicly exposed a collection of email templates, most likely used by the attackers to design and deliver the phishing emails to the respective targets. Most of these files came pre-compiled with the email addresses of targeted individuals.

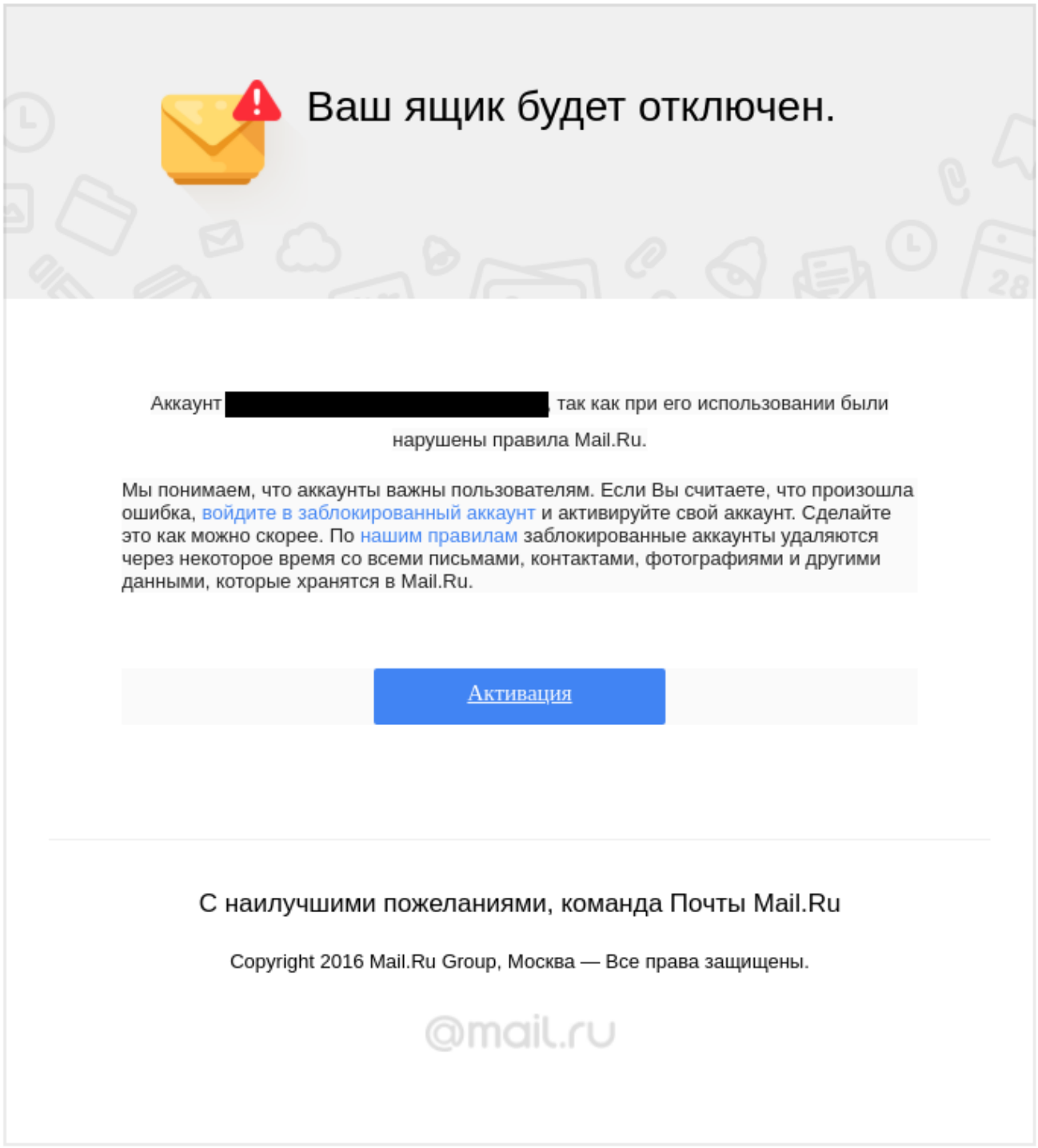
Most of these emails were disguised as email alerts from services such as Google or Mail.ru.



Amnesty International



Amnesty International



Amnesty International

From these exposed templates we identified 170 targeted accounts. Although we suspect them to represent only a subset of the complete list of individuals targeted in this campaign. Most targets we identified are part of universities or governmental organisations of countries neighbouring Uzbekistan, along with several HRDs from Uzbekistan, who Amnesty International took steps to contact, notify and support.

Conclusion

This report documents that targeted surveillance remains a threat to HRDs in Uzbekistan. The UN Special Rapporteur on the right to Freedom of Expression, David Kaye, has called on states to impose an immediate moratorium on the export, sale, transfer, use or servicing of privately developed surveillance tools until rigorous human rights safeguards are put in place to regulate such practices. Amnesty International supports this call. As the Special Rapporteur has noted, *"It is insufficient to say that a comprehensive system for control and use of targeted surveillance technologies is broken. It hardly exists."*

This call is especially urgent in the context of Uzbekistan where the legal framework for secret surveillance provides insufficient safeguards against abuse and where direct state access to data is facilitated by the SORM system (a system allowing state authorities to directly access communication and associated data). It is well-established that, *"even the mere possibility of communications information being captured creates an interference with privacy, with a potential chilling effect on rights, including those to free expression and association."* Where – as in Uzbekistan – states fail to put in place adequate safeguards, these chilling effects will lead to an environment in which HRDs cannot realize their rights and struggle to do their job effectively and in safety.

If you believe you have been targeted with attacks similar to the ones described here, or if you are a Human Rights Defender working on Uzbekistan and you think you may be targeted by a similar operation, please contact us at:

share@amnesty.tech

Recommendations

To the Government of Uzbekistan:

> Reform laws to bring the legal regime and related surveillance practices in line with international human rights law and standards

To Other Governments:

> Impose an immediate moratorium on the export, sale, transfer, use or servicing of privately developed surveillance tools until a human rights compliant safeguards regime is in place

To Companies:

> Put in place robust safeguards to ensure that any use of their products or services is compliant with human rights standards.

To Users:

> As we have been reporting since December 2018, techniques to bypass common forms of two-factor authentication are becoming increasingly popular among attackers. Targeted individuals at risk should consider equipping themselves with hardware Security Keys, also known as U2F keys, and enable them wherever possible. With online services, which do not support Security Keys yet, we nevertheless recommend enabling any other less resilient form of two-factor authentication available. For example, secondary verification using codes delivered via SMS or an authenticator app still provide better security than none at all, and can help thwart casual phishing or password re-use.

If you want to read more about phishing and its countermeasures, please refer to Security Without Borders' Guide to Phishing.

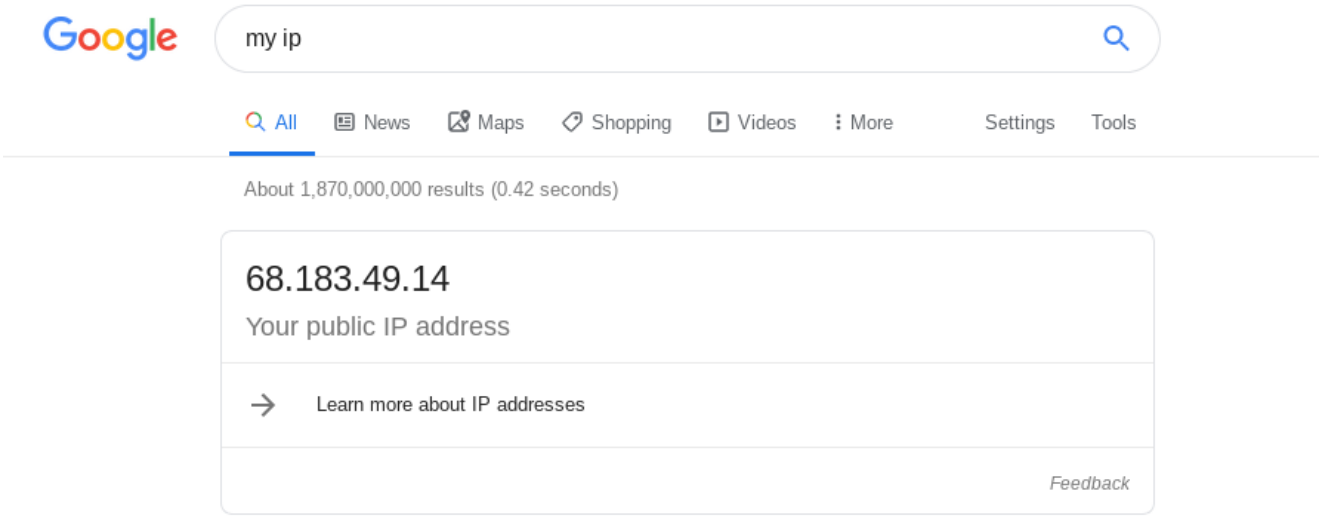
Appendix : Technical Details on the Investigation

Phishing Using Reverse Proxies

This group is largely relying on phishing attacks: we have identified 71 domains hosting phishing websites between May and September 2019.

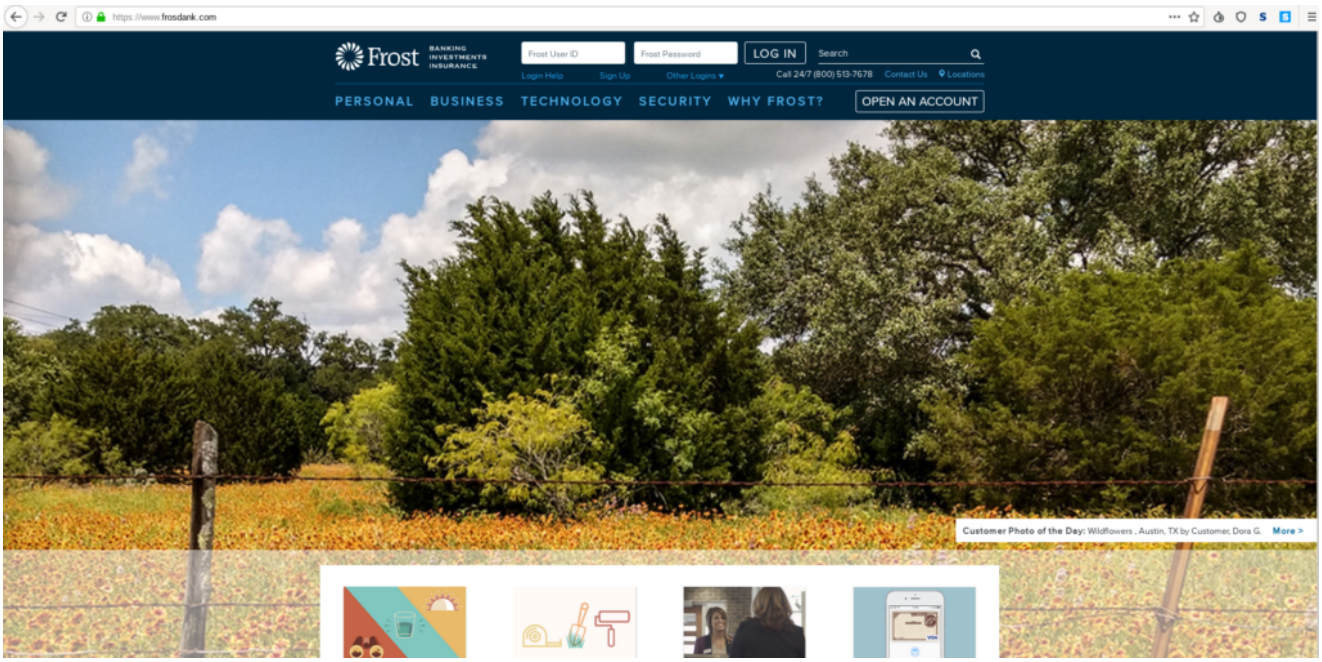
Originally, this group used HTML copies of login pages for phishing. In June 2019, we observed the utilisation of a new tool that acted as a reverse proxy between the domains and the actual platforms in order to hijack sessions. We believe that the attackers relied on a custom-made JavaScript phishing tool.

One proof that these phishing domains were using reverse proxy technique is that we could fully interact with the Google platform through the fake domain. For instance we could use the query "what is my IP?" to get the IP address of the reverse proxy server from the Google search engine:



Amnesty International

At the same time we saw this change in the phishing toolkit, we started to see more and more domains mimicking and proxying traffic to bank and cryptocurrency websites. The phishing domains and websites observed by eQualit.ie since 2016 and by us from May 2019 almost only copied large email providers (mostly Gmail, but also Yandex or Yahoo). From May 2019 to July 2019, we started to see the attackers register and use domains imitating bank and cryptocurrency websites. We could attribute these domains to the same attacker network because they were hosted on the same servers that hosted other phishing domains. For instance the OVH server 51.83.97[.]40 hosted at the same time fake gmail domains like gmail-warning[.]top and fake bank domains like mynavyfedral[.]org in July 2019. This suggests that the attackers might also be involved in online economic crime.



Amnesty International

Phishing website for FrostBank on frosdank[.]com (July 2019)

Here is the list of such domains registered between May and July 2019:

Registration Date	Malicious Domain	Proxying Traffic or Mimicking
2019-05-02	navyfedera1[.]org	https://www.navyfederal.org/
2019-05-20	frostdank[.]com	https://www.frostbank.com/
2019-05-27	comericac[.]com	https://www.comerica.com/
2019-07-03	lamatrest[.]xyz	https://www.bmo.com
2019-07-16	mynavyfedral[.]org	https//www.navyfederal.org/
2019-07-17	desktest5[.]xyz	https://www.scotiabank.com/
2019-07-19	testdhome4[.]xyz	https://www.blockchain.com/
2019-07-29	xn--blckchain-17c[.]com	https://www.blockchain.com/
2019-08-07	xn--navyfderal-36a[.]com	https://www.navyfederal.org/
2019-08-07	xn--navyfedera-j0b[.]org	https://www.navyfederal.org/
2019-08-07	xn--bckchain-v3a30f[.]com	https://www.blockchain.com/
2019-08-15	xn--avfedera-yubm[.]org	https://www.navyfederal.org/
2018-09-22	rc-room[.]com	https://www.coinbase.com/
Unknown	nitroqensports[.]eu	https://nitrogensports.eu/

Windows Malware

In May 2019, we identified two backdoored Windows installers hosted on the domain msoffice365[.]win, one Adobe Flash Player installer and one Telegram Desktop installer, both installing variants of the same malicious toolkit along with the legitimate software.

Both of these malicious samples rely on a set of vbs scripts and DLL to gather information on the system and send it to the domain hpphhpph[.]com

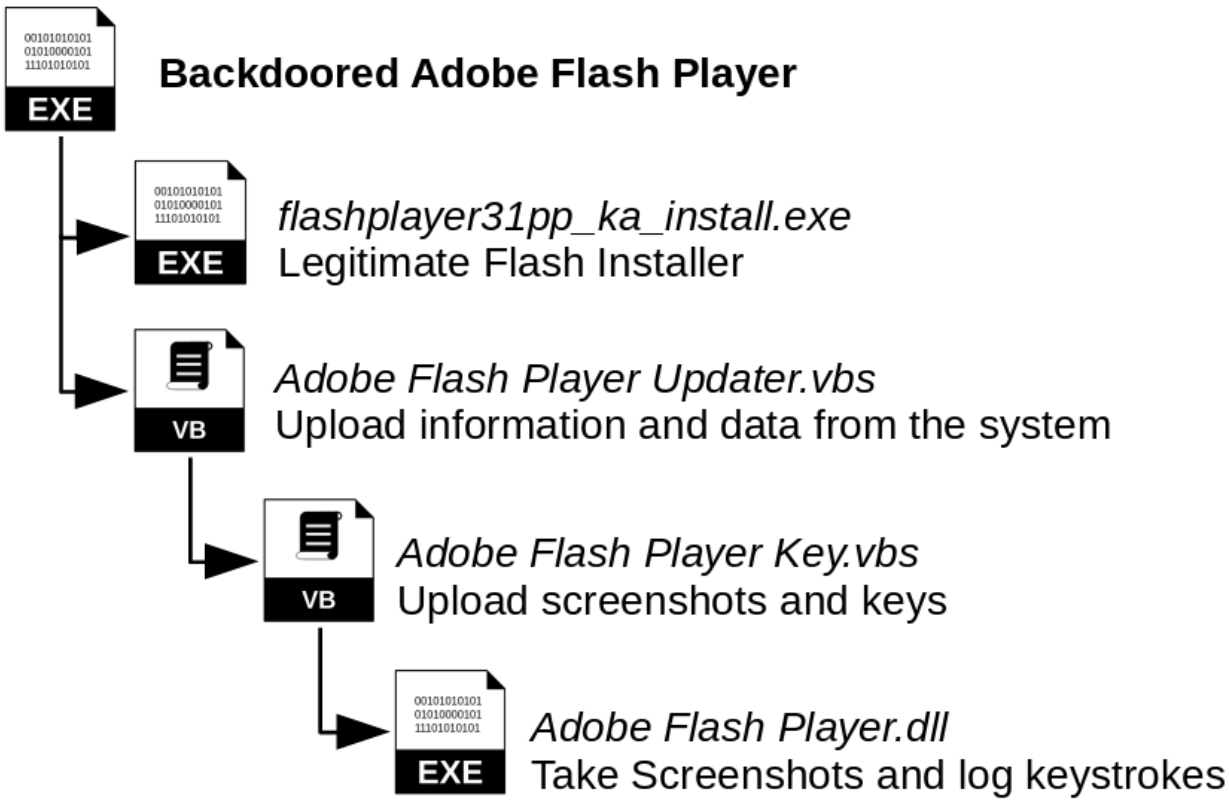
The Fake Adobe Flash Player installs the following files :

- In C:\Program Files (x86)\Adobe Company\Adobe Flash Player
  - Adobe Flash Player Updater.vbs
  - flashplayer31pp_ka_install.exe (Legitimate Flash Player installer)
  - Uninstall.exe (Legitimate Uninstaller)
  - Uninstall.ini (Legitimate Uninstaller info file)

- In C:\Users\User\AppData\Roaming\Microsoft\Adobe Flash Player
  - Adobe Flash Player.dll
  - Adobe Flash Player Key.vbs

During the installation, the malicious script Adobe Flash Player Updater.vbs is launched along with the legitimate installer flashplayer31pp_ka_install.exe. Adobe Flash Player Updater.vbs is a VBS script in charge of registering a new compromised device to the Command & Control server, gather information on the host (information on the device, list of applications, logs of Telegram chats, Firefox, The Bat email client and Total Commander FTP credentials, Chrome, Firefox and Opera history) and schedule tasks to have Adobe Flash Player Updater.vbs and Adobe Flash Player Key.vbs launched every minutes.

Adobe Flash Player Key.vbs is VBS script that launches Adobe Flash Player.dll, a tool that takes a screenshot of the screen every seconds and run a KeyLogger, and then send the images and keystrokes taken to the C&C server.

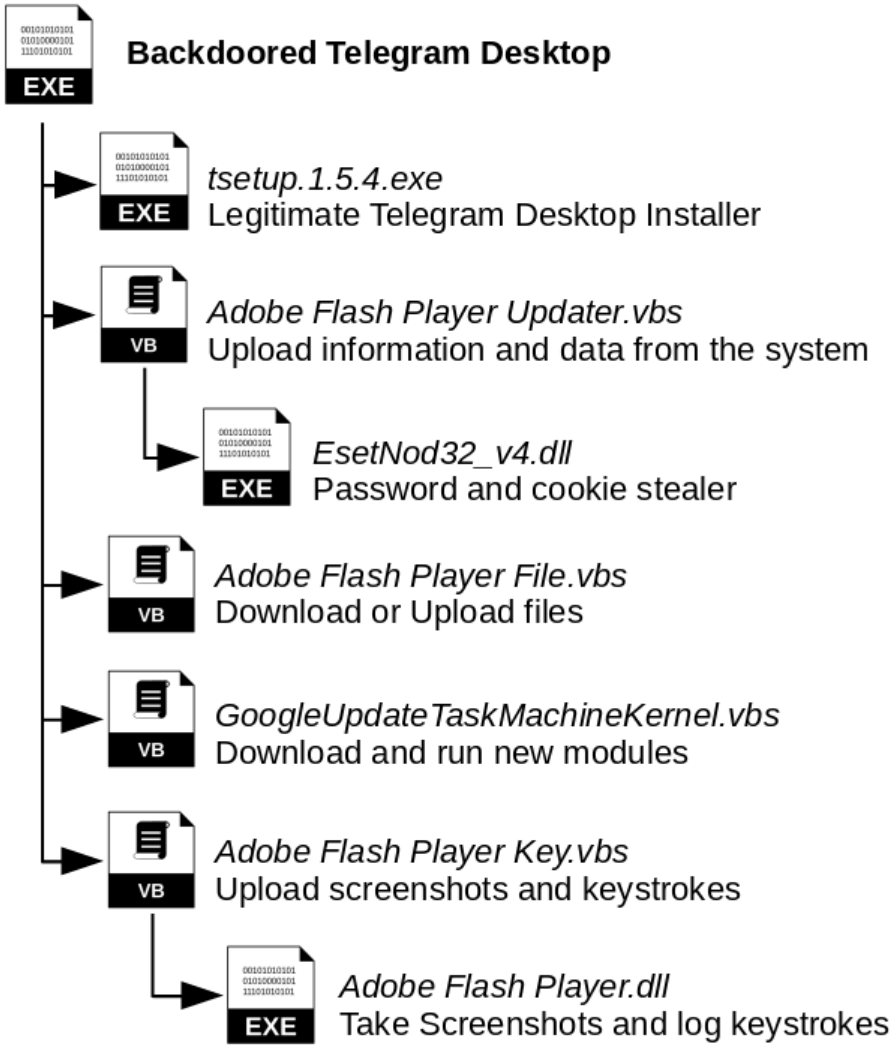


Amnesty International

The Telegram Installer relies on variant of the same scripts with a few additional tools :

- GoogleUpdateTaskMachineKernel.vbs : a script to download additional modules from the C&C server and run them through scheduled tasks

- EsetNod32_v3.5.dll and EsetNod32_v4.dll which are more advanced password and cookie stealers reusing code taken from the Quasar-RAT , an open source Windows malware.



Amnesty International

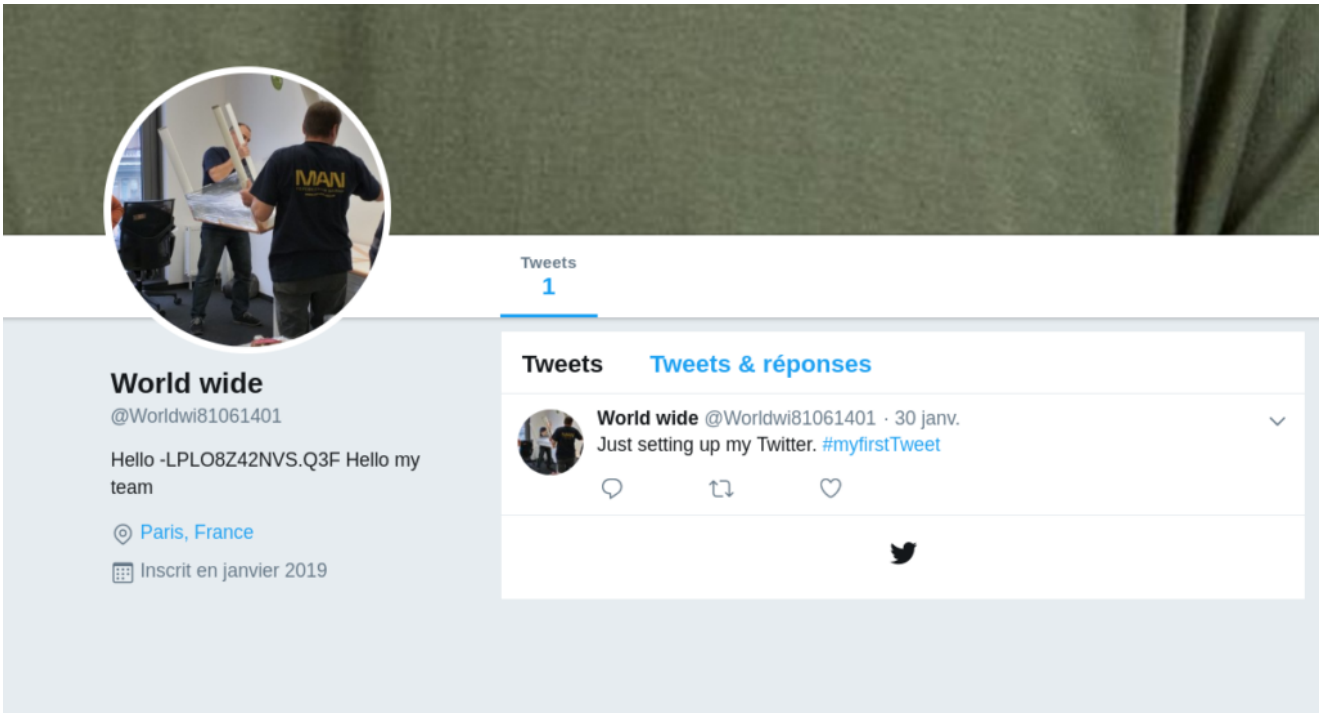
This patchwork of different tools combined with easy to update VBS scripts allow to heavily monitor the activity of a compromised computer by sending every minute, any key stroke done, screenshot, new password and browsing history, thus providing a complete view of the user activity.

Android Malware

During our enumeration of the infrastructure, we identified an Android spyware communicating with one of the domains of this operation (garant-help[.]com) as Command and Control server. This sample is an improved version of Droid-Watcher, an open-source Android malware that was discontinued by its main developer in 2016.

One update from Droid-Watcher is that this malware retrieves the location of the Command and Control server to communicate with, from an encoded string included in the description of a Twitter account registered at @Worldwi81061401 (we have notified Twitter about this

account, which was later suspended):



Amnesty International
Screenshot of the Twitter profile @Worldwi81061401 (July 2019, suspended now)
The encoded string in the profile description (LPLO8Z42NVS.Q3F) once decoded gives the domain garant-help[.]com.

Indicators of Compromise

We are releasing here indicators of compromise for this campaign. If you think you have been targeted by this campaign, or if you have some information on this operation, please contact us at

share@amnesty.tech

You can find a full list of indicators of compromise on this github repository : https://github.com/AmnestyTech/investigations/tree/master/2020-03-12_uzbekistan

Related Content