Report on

Phishing Attack Against Iranian Activists

December 2016 - May 2017

IranSec
» A Shield for Defenders

July 2017

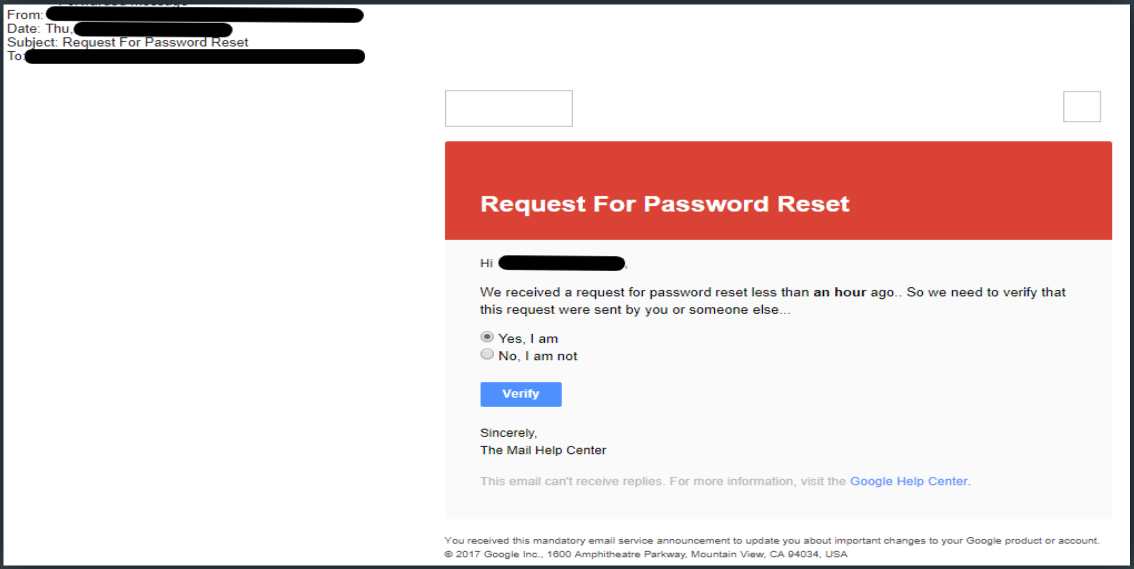
Facts & Figures

- First and second phishing attacks stole information from 300 victims, while third attack succeeded in 200 cases.
- Almost half of the victims seem to be non-Iranians including politicians in North America, Europe, Israel and the Persian Gulf region.
- Iranian victims of the last three attacks were mainly activists living in the U.S.
- The attacks are more advanced and complicated versions of "Charming Kitten" attacks of 2016.

Since early 2017, IranSec received several attack reports regarding suspicious emails received by Iranian journalists and human right activists, demanding the users to change their Gmail passwords.

Previously, teams such as "Flying Kitten", "Charming Kitten" and "Rocket Kitten" had carried out organized and persistent phishing attacks in 2010 targeting civil activists and politicians. Based on research by security experts, the attackers have been trying to collect their victims' personal information using phishing emails and fake web pages. According to published reports, these attacks are primarily targeting Iranian users living abroad, and also foreign politicians, corporations, and economic and military organizations.

IranSec Lab has analyzed samples of emails sent to IranSec. The present report describes three latest versions of these phishing attacks and concludes with a short guide for users to avoid such attacks in future.



From: [redacted]
Date: Thu, [redacted]
Subject: Request For Password Reset
To: [redacted]

Request For Password Reset

Hi [redacted],

We received a request for password reset less than **an hour** ago.. So we need to verify that this request were sent by you or someone else...

● Yes, I am
○ No, I am not

Verify

Sincerely,
The Mail Help Center

This email can't receive replies. For more information, visit the Google Help Center.

You received this mandatory email service announcement to update you about important changes to your Google product or account.
© 2017 Google Inc., 1600 Amphitheatre Parkway, Mountain View, CA 94034, USA

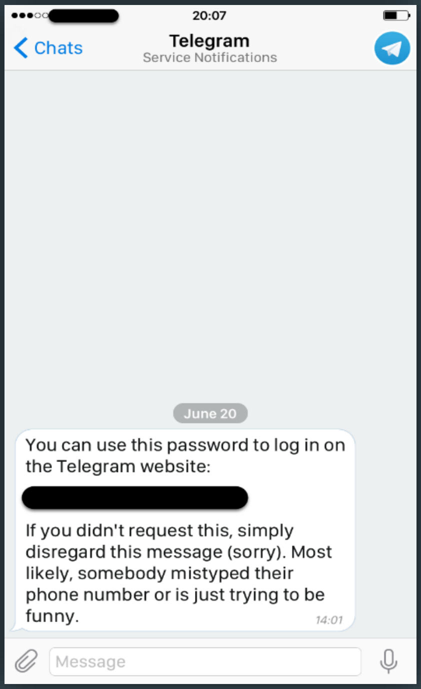
Figure 1: Fake Email Demanding Password Reset

At first glance, it seems that this is a phishing attack. Phishing Attacks aim to gain certain private information (like passwords) of the victim through impersonation of a certain website, email address, or content. They are meant to deceive potential victims by disguising themselves as another person, company or organization.

Figure 1 depicts how the phishing email is designed in a way to resemble an email from Google. From the start, three suspicious points can be noted here: First, user had not asked for a password reset; second, the email was sent from an unofficial address of google services (Google sends emails from its google.com domain, rather than its gmail.com domain). And third, awkward grammatical mistakes in the text.

Another method uses social engineering methods to put the victim under pressure. The attackers send several emails with different contents putting the victim under pressure and harassing them to increase chances of committing a mistake. Similar phishing attacks have even included attackers texting their victims' cellphone numbers with password reset requests (disguising as Gmail or Telegram) to frighten the victim and increase chances of such mistakes.

The hackers designing these attacks sent a second email to the victims after a short interval. This email contained a text claiming "Another person has accessed your account from an unknown location" together with fake information including IP address, name of operating system and geographical location of another system accessing their account. There has been reports of up to 6 such warning emails received in only 5 minutes. Figure 3 illustrates one such warning email.

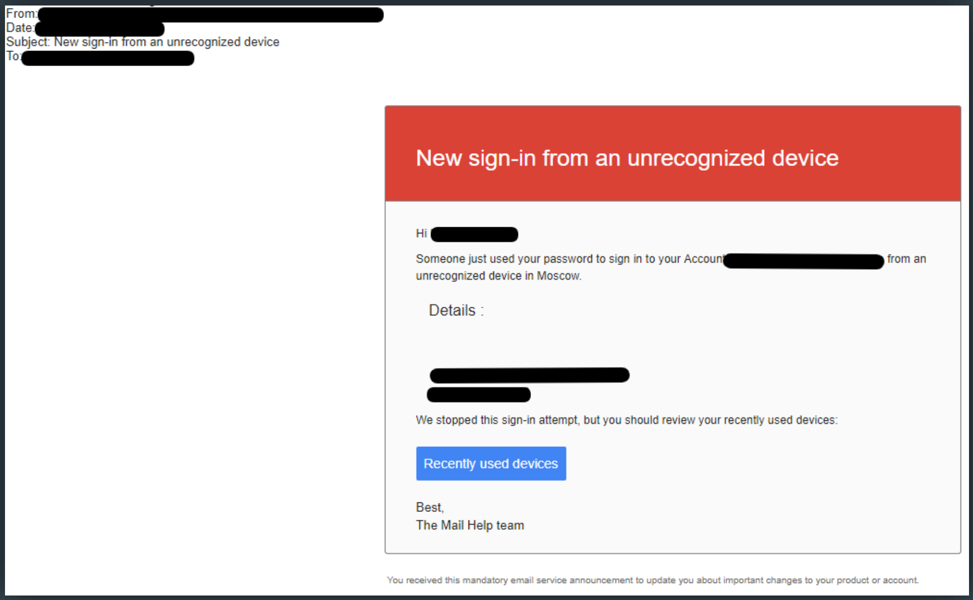


You can use this password to log in on the Telegram website:

[redacted]

If you didn't request this, simply disregard this message (sorry). Most likely, somebody mistyped their phone number or is just trying to be funny. 14:01

Figure 2: Attacking Telegram Accounts



From: [redacted]
Date: [redacted]
Subject: New sign-in from an unrecognized device
To: [redacted]

New sign-in from an unrecognized device

Hi [redacted]

Someone just used your password to sign in to your Account [redacted] from an unrecognized device in Moscow.

Details :

[redacted]

We stopped this sign-in attempt, but you should review your recently used devices:

Best,
The Mail Help team

You received this mandatory email service announcement to update you about important changes to your product or account.

Figure 3: Fake Warning Email

In all three attacks, victims were redirected to a page with an address very similar to addresses used by Google with content resembling a Google login page. Each page was specifically designed for each victim complete with their own avatar and name (Figure 3). In some cases, duration between creation of the fraudulent domain and its use in the phishing scam was very short, apparently in an attempt to decrease risk of detection by Google or third party security experts.

In some cases, shortly after the first phishing email, another fake email was sent as confirmation of a password change in order to increase pressure on the victim and distract them from properly checking the phishing email. Figure 5 shows how after pressing the "Verify" button, the victim is redirected to another page not part of Google domains. This page finally redirects the victim to the fake login page (Figure 4) before redirecting to Google homepage.

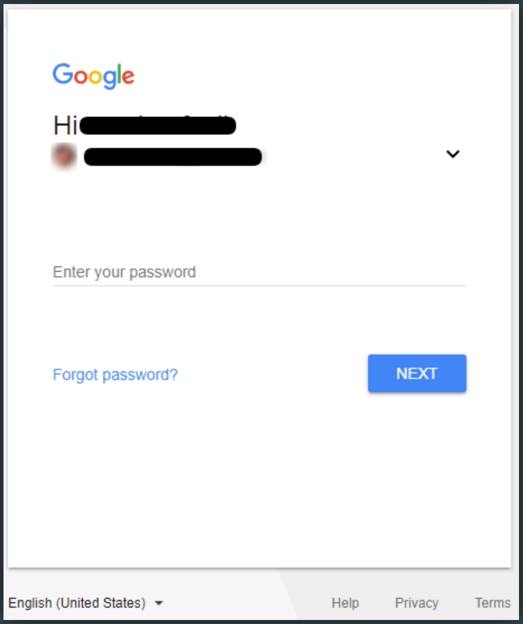
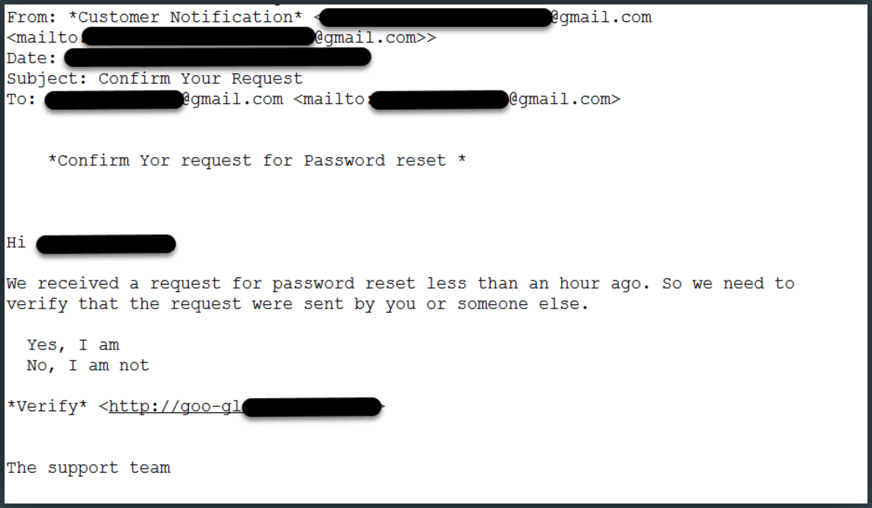


Figure 4: Fake Page for entering the email with the avatars of the victims

In most cases analyzed by IranSec, hackers had sufficient information about their victims and their internet connections. Phishing emails were sent to victims during their peak working hours, or simultaneous messages were sent to multiple accounts of the victim (on various social networks) to create a sense of a comprehensive attack on the victim, in order to decrease their caution. In some cases, fake warnings or confirmation emails were even sent to victim's recovery (backup) email address claiming a password change, a failed login, or a new password. It can be concluded that hackers designing these attacks did not choose their victims randomly, they rather had detailed information about their victims' behaviors and activities.



```
From: *Customer Notification* <[redacted]@gmail.com
<mailto[redacted]@gmail.com>>
Date: [redacted]
Subject: Confirm Your Request
To: [redacted]@gmail.com <mailto[redacted]@gmail.com>


    *Confirm Yor request for Password reset *



Hi [redacted]

We received a request for password reset less than an hour ago. So we need to
verify that the request were sent by you or someone else.

  Yes, I am
  No, I am not

*Verify* <http://goo-gl[redacted]


The support team
```

Figure 5: Text-only version of Figure 1 email redirects the victim to a fake page after pressing "Verify" button

Figure 6: Overview of avatars used in the attacks (images are blurred to protect privacy)

Further research by IranSec reveals about half of the total 500 victims in these serial phishing attacks were Iranian human rights activists and journalists. Unfortunately, no exact number of victims of these phishing attacks is available. Although victims have been identified and warned about the attacks as much as possible, extent of information revealed to the attackers cannot be estimated. Almost half of the victims were non-Iranian politicians, civil activists and businesspersons in Europe, United States or the Middle East.

The phishing attacks were not limited to early 2016 and were repeated in other time periods to target other groups of Iranian activists. The attackers fixed some of their previous mistakes and developed an altered method (by changing their targeting method and using different content, time and type for their fake emails). Despite the alterations, however, there is no doubt that these three attacks are linked to each other.

Given the range of these attacks, use of multiple servers and domains, change of hacking methods, and targeting those sociopolitical activists and journalists critical of the Iranian government, it is highly probable that these attacks were supported by the Iranian government. Additionally, traces of "Charming Kitten" hacking group was detected, the same group involved in distributing a malware called "MacDownloader". The malware was uploaded to a web page visually similar to an American aerospace company (selling jet turbines and other industrial equipment). Security experts believe the malware is targeting Iranian opposition and other activists. It infects victim's system through a fake Flash installation downloader and transfers user information to hackers' servers upon entering of iCloud Keychain password.

The malware structure is based on the fact that Safari browser and other Mac OS services automatically save passwords in the Keychain for future logins. This malware was created in late 2016 by amateur developers and uses code from other previous malwares[1].

Several domains and servers of this group have since been identified and takedown requests have been placed. Figure below illustrates connections between attacking servers and fake domains, outlining software and hardware infrastructure used for previous (and possible future) attacks. Please note that domain names, IP addresses and server information has been removed from the figure.

The figure depicts 50 fake domains, 7 emails, 19 IP addresses and other details regarding the latest three phishing identified so far. Distribution of dots in the diagram shows the connection between them. Hackers changed email addresses, domains, servers and other details at different times to remove any remaining traces. Upon further analysis, our specialists could recover some of those information and establish connections between these domains and emails.

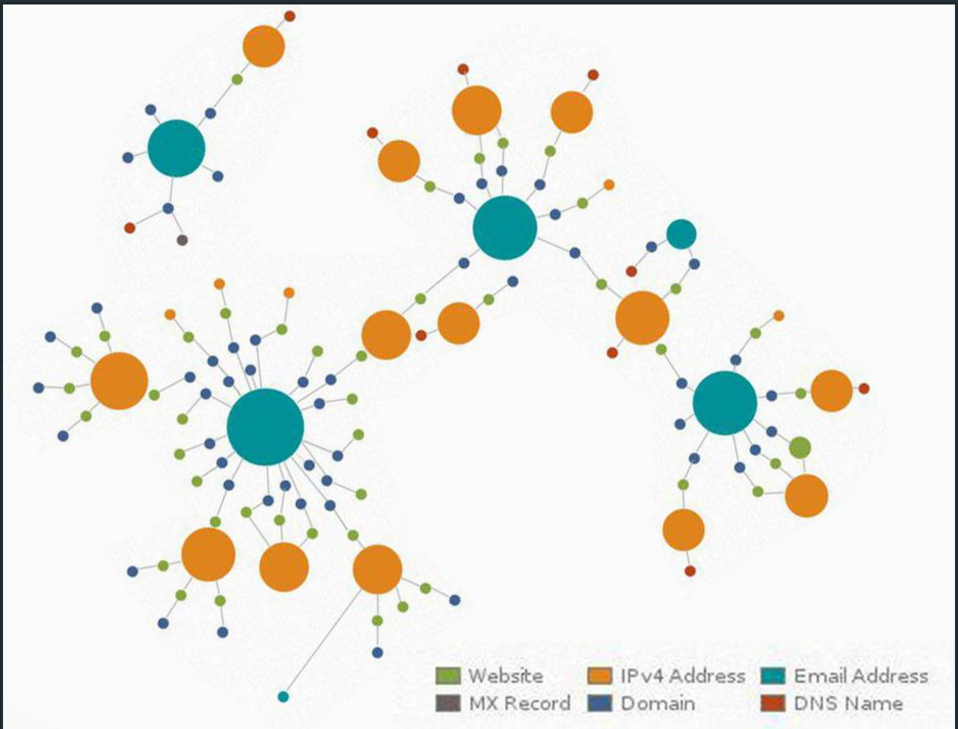


Figure 7: Distribution of Websites, IPs, Emails, DNS Servers, MX Servers and Domains

[1] https://iranthreats.github.io/resources/macdownloader-macos-malware

Iransec Recommendations to Avoid Phishing Attempts

- Use "Google Authentication" Application to confirm ID login
- Use Password Management Applications with browser extension an option for link identification and direct password entry to links
- Disable the image preview option in email links

In case of receiving password change email or suspicion of an attack, keep calm! This email might be a trap. Before any further action analyze the following:

- Check the sender's address. Is it a valid address?
- Read the email text carefully. Has anything suspicious happened that you are receiving such an email (e.g. password change)?
- Check links and addresses of pages requesting your account information and/or passwords. Are you being redirected to the same page as you expected? Check the address on the bar at the top of your browser window

If you happen to enter your personal information in a phishing page, keep calm and:

- Enter your account and change your password.
- Make sure no one else is connected to your ID. If so, terminate their access. For instance, in Gmail, click on the "Last Account Activity" button to see users connected now.
- Consult a security expert to be totally safe.

IranSec; a Shield for Defenders

IranSec

Summer 2017
IranSec Security Lab

Be in Touch
support@iransec.org