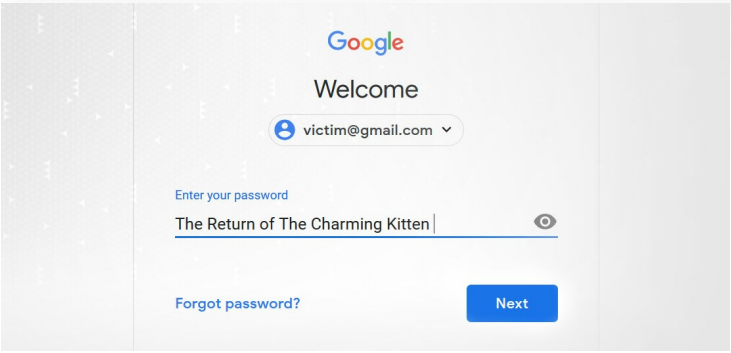
The Return of The Charming Kitten

A review of the latest wave of organized phishing attacks by Iranian state-backed hackers

Certfa Lab · 2018.12.13



Abstract

Phishing attacks are the most common form of infiltration used by Iranian state-backed hackers to gain access into accounts. Certfa reviews the latest campaign of phishing attacks that has been carried out and dubbed as "The Return of The Charming Kitten".

In this campaign, hackers have targeted individuals who are involved in economic and military sanctions against the Islamic Republic of Iran as well as politicians, civil and human rights activists and journalists around the world.

Our review in Certfa demonstrates that the hackers - knowing that their victims use two-step verification - target verification codes and also their email accounts such as Yahoo! and Gmail. As a result, Certfa believes the safest existing way to confront these attacks is using Security Keys such as YubiKey.

Introduction

In early October 2018, MD0ugh, a Twitter user[1], revealed phishing attacks of a group of Iranian hackers against US financial institution infrastructure. According to this user, these attacks could possibly be a reaction to new sanctions against Iran.

The account mentioned a domain with the address accounts[-]support[.]services for the first time. This domain is linked to a group of hackers who are supported by the Iranian government, and that we believe have close ties with the Islamic Revolutionary Guard Corps (IRGC). ClearSky[2] has previously published detailed reports on their activities.

A month after these attacks, the administrators of accounts-support[.]services expanded their activities and started targeting civil and human rights activists, political figures and also Iranian and Western journalists.

Methods of Attacks

Our investigation illustrates that the attackers are utilising different methods to carry out their attacks. These methods can be put into two categories:

1. Phishing attacks through unknown email or social media and messaging accounts
2. Phishing attacks through email or social media and messaging accounts of public figures, which have been hacked by the attackers

We have also found that the hackers have collected information on their targets prior to the phishing attack. The hackers design specific plans for each target based on the level of targets' cyber knowledge, their contacts, activities, working time, and their geographic situation.

We also noticed that, unlike in previous phishing campaigns, in some cases the hackers did not change the password of their victims' accounts in these latest attacks. This allows them to remain undetected and monitor a victim's communications via their email in real time.

Fake alerts of unauthorised access

According to the samples of phishing attacks, the main trick used by these hackers to deceive their targets is that of sending fake alerts through email addresses such as notifications.mailservices@gmail[.]com, noreply.customermails@gmail[.]com, customer]email-delivery[.]info etc. stating that unauthorised individuals have tried to access their accounts.

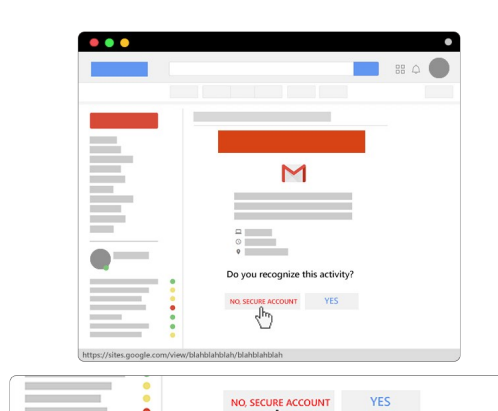


Figure 1. Illustration of safe and secure looking fake links

By using this method, attackers pretend that the email provider has sent security alerts to the targets and they should immediately review and restrict suspicious accesses. More details are available in the "Destination Link" section.

Fake file sharing on Google Drive

Sending links with titles such as share files from Google Drive has been one of the most common tricks that hackers have used in recent years. A unique point of these attacks in comparison with the previous ones is that they use Google Site[3], which allows the hackers to show a fake download page of Google Drive, which tricks the users into thinking it's a real Google Drive page.

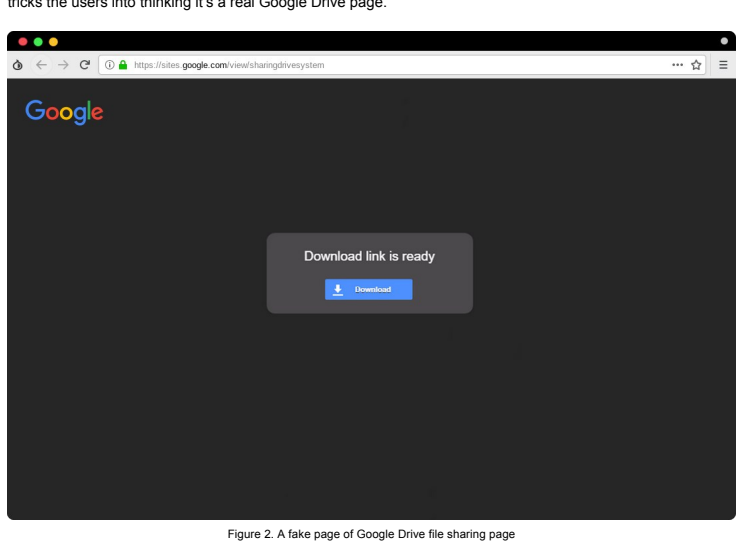


Figure 2. A fake page of Google Drive file sharing page

For example, the hacker had used hxxps://sites.google[.]com/view/sharingdrivesystem to deceive the users and convince them the page is the authentic Google Drive as users can see google.com in the address bar of their browsers. Certfa has reported this link and similar links to Google and Google has now terminated them.

> *By creating websites with the same design and look of Google Drive file sharing page, hackers pretend to be sharing a file with the user, which they should download and run it on their devices. They use hacked Twitter, Facebook and Telegram accounts to send these links and target new users. The truth is there is not any file and the hackers use this page to direct their targets to the fake Google login page, which the users enter their credential details including 2 factor authentication.*

The Attack Structure

Most of these attacks are currently occurring through phishing emails. As a result, it would be useful to take a look the original content in recent phishing campaigns.

Figure 3. An example of codes of phishing email sent to the user

1. Destination link

1.1. Trusted Stage: Internet users around the world consider Google's main domain (google.com) to be a safe and secure address. The attackers misuse this fact and create fake pages on sites.google.com (which is a subdomain of Google) to deceive their targets. Google's Site service gives its users an ability to show various contents on it. The attackers use this ability to send fake alerts and redirect their targets to insecure websites or embedded phishing pages as a iframe on those pages.

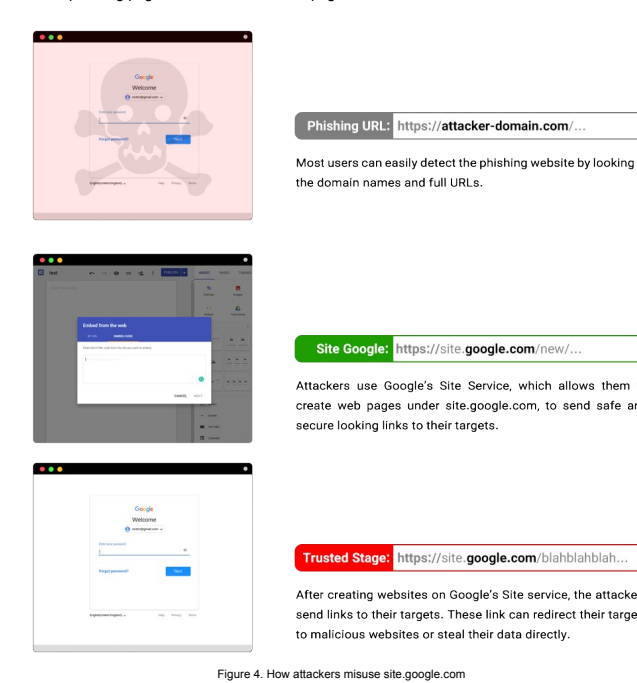


Figure 4. How attackers misuse site.google.com

1.2. Untrusted Stage: Since Google can quickly recognise and eliminate suspicious and malicious links on sites.google.com, the hackers use their own website. The links of phishing websites have similar patterns to a previous phishing campaign which was launched in the past years. For example, attackers use words such as "management", "customize", "service", "identification", "session", "confirm" etc. in the domains name and phishing URLs to deceive users who want to verify their website addresses.

2. Clickable image in emails

The hackers use an image, instead of texts, in the body of their emails, to bypass Google's security and anti-phishing system. For this purpose, attackers have also used third party services such as Firefox Screenshot[4] to host their email images.

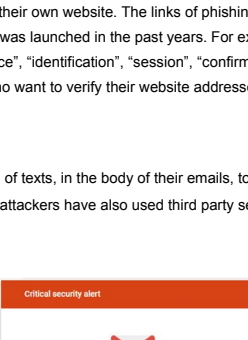


Figure 5. An example of a planted image of fake alarm in a phishing email

3. Hidden tracking image on emails

The attackers use a separate hidden image in the body of the email to notify them when their targets open the email. This trick helps the hackers to act immediately after the target opens the email and clicks on the phishing link.

Phishing Pages

Apart from the content structure of the emails and phishing links, we are sure that attackers use a customized platform to create and store users' credential details. We have also noticed that they have designed the phishing pages for both desktop and mobile versions of Google and Yahoo! mail services and they might use other services in the future.

An interesting technique they have used in recent attacks was once their target enters their username and password, attackers check those credentials on-the-fly and if that information was given correctly, they then ask for 2-step verification code.

In other words, they check victims' usernames and passwords in realtime on their own servers, and even if 2 factor authentication such as text message, authenticator app or one-tap login are enabled they can trick targets and steal that information too.

Figures 6 to 9 demonstrate some examples of the phishing pages, which have been sent to the targets by the Iranian hackers.

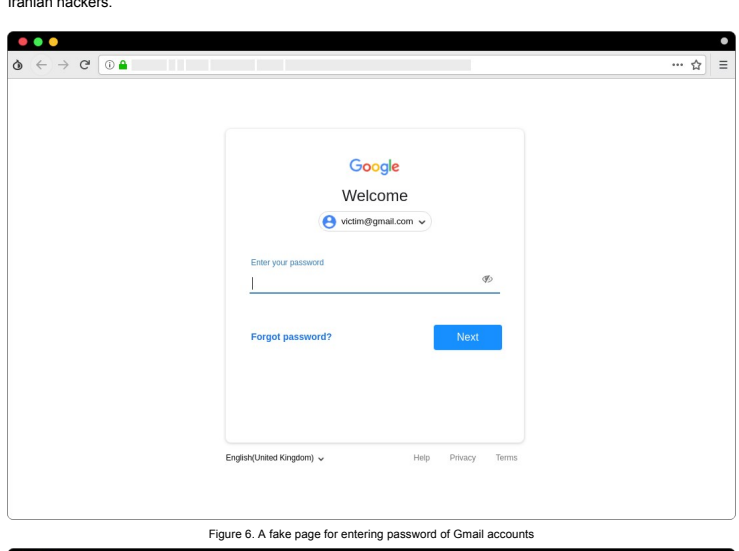


Figure 6. A fake page for entering password of Gmail accounts

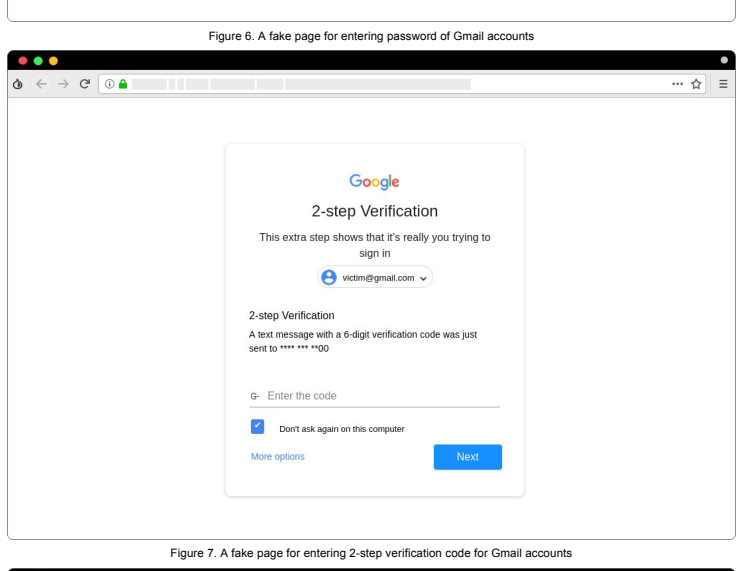


Figure 7. A fake page for entering 2-step verification code for Gmail accounts

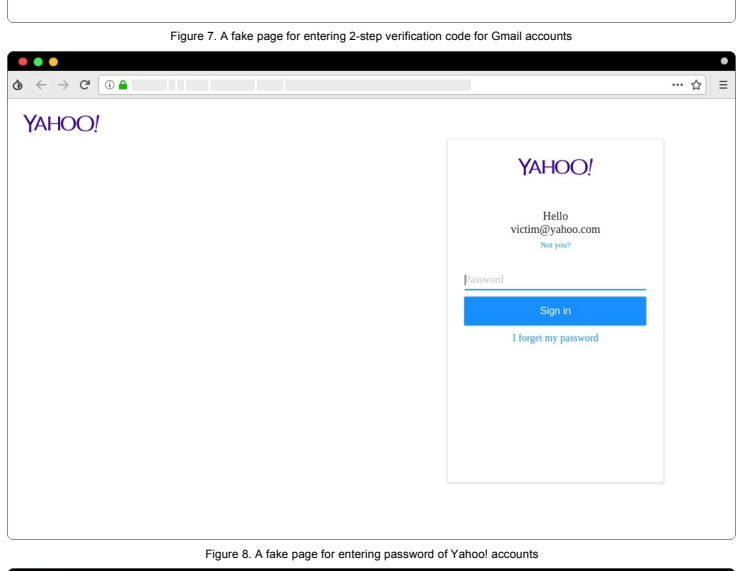


Figure 8. A fake page for entering password of Yahoo! accounts

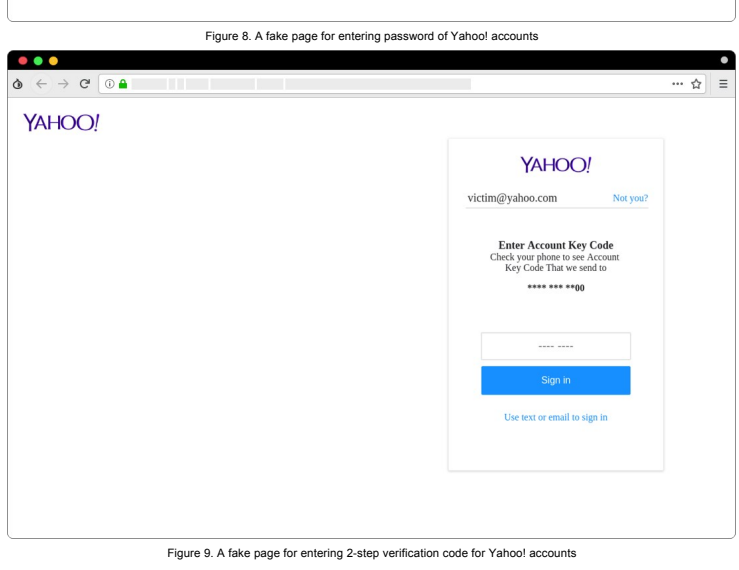


Figure 9. A fake page for entering 2-step verification code for Yahoo! accounts

Hacker's Footprints

Our primary reviews of the phishing websites linked to this campaign show that hackers have set up a remarkable number of domains. Our latest findings show that for this phishing campaign in a relatively short period of time, (September to November 2018), they have used more than 20 domain names. The number of phishing domains has increased at the time of writing this report. Closer investigation of these servers revealed how their network of domain names have been used in recent attacks.

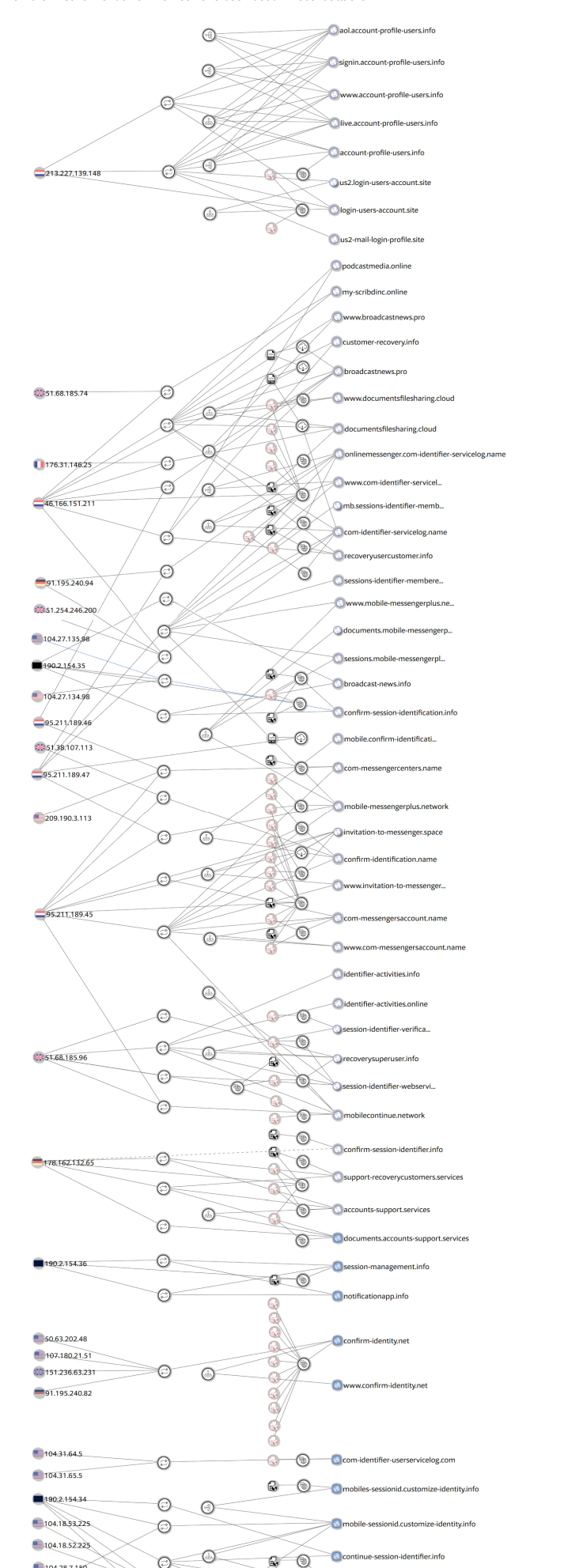


Figure 10. Deep data of the attackers' network in this phishing campaign, which gathered by Certfa[5]

Moreover, our technical reviews reveal that the individuals, who are involved in this campaign used Virtual Private Networks (VPNs) and proxies with Dutch and French IP addresses to hide their original location. In spite of their efforts, we have uncovered enough evidence to prove that the attackers were using their real IP addresses (i.e 89.198.179[.]103 and 31.2.213[.]18 from Iran during the preparation phase of their campaign).

Also, some domain names and servers of this campaign are very similar to the methods, techniques and targets that been used by Charming Kitten, a group of hackers who are linked to the Iranian government. Consequently, we believe Charming Kitten and the Iranian hacker(s) belonging to this group have returned and launched new cyber attacks against various people around the world and with more focus on Israeli and American citizens.

Conclusion

Phishing attacks are the most popular method of stealing data and hacking account amongst Iranian hackers, but the most significant fact about this campaign is its timing. This campaign launched weeks before 4 November 2018 which is when the U.S. imposed new sanctions on Iran. This campaign tries to collect information by infiltrating the accounts of non-Iranian political figures and authorities who work on economic and military sanctions against Iran.

In other words, hackers who are supported by the Iranian government pick their targets according to policies and international interests for the Iranian government and also where Iran wants to have impact indirectly.

A a result, we propose a series of recommendations to tech companies, policymakers, civil society actors and internet users to effectively lessen the threat of this type of attack and even thwart them.

Our recommendations to tech companies and policy makers:

- Stop using 2 factor authentication by text plain message/SMS.
- Start using Security Keys (i.e. YubiKey) for 2 factor authentication for high ranking individuals who have sensitive jobs or activities.
- Do not use one-tap login verification process.

Our recommendations to civil society and the Iranian diaspora media:

- Inform employees and colleagues about any phishing threats and encourage them to use Security Keys such as Yubikey for 2 factor authentication and activate Google's Advanced Protection Program.
- Always use company and institution email accounts instead of personal email for sensitive communications. Change Sender Policy Framework or SPF[6] settings according to the communication policy of the company/organisation such as restricting receiving emails from outside of the working network. For example, G Suite allows admins to block receiving emails from unauthorised address or domains[7].
- Encourage the public to enable 2 factor authentication on their account by mobile apps such as Google Authenticator.

Our recommendations to users:

- Do not click on unknown links. For reviewing suspicious activities on your account or change the password, instead of clicking on any link, you can go to your "My Account" settings from your email directly which is more safer.
- Use email encryption such PGP for sensitive emails which prevent hackers reading your emails in the first place.
- Do not store classified and sensitive information as a plain text in your mailbox.
- HTTPS being before a domain names in a URL does not mean that the content of a website is secure or trusted - it's just a secure extension of the HTTP protocol. Do not forget many phishing websites are currently operating under HTTPS protocol too.

IOCs

- 178.162.132[.]65
- 190.2.154[.]34
- 190.2.154[.]35
- 190.2.154[.]36
- 190.2.154[.]38
- 46.166.151[.]211
- 51.38.87[.]64
- 51.38.87[.]65
- 51.68.185[.]96
- 51.38.107[.]113
- 95.211.189[.]45
- 95.211.189[.]46
- 95.211.189[.]47
- 213.227.139[.]148
- 54.37.241[.]221
- 54.38.144[.]250
- 54.38.144[.]251
- 54.38.144[.]252
- 85.17.127[.]172
- 85.17.127[.]173
- 85.17.127[.]174
- 85.17.127[.]175
- 89.198.179[.]103
- 31.2.213[.]18
- accounts-support[.]services
- broadcast-news[.]info
- broadcastnews[.]pro
- com-identifier-servicelog[.]info
- com-identifier-servicelog[.]name
- com-identifier-userservicelog[.]com
- confirm-session-identification[.]info
- confirm-session-identifier[.]info
- confirmation-service[.]info
- customer-recovery[.]info
- customize-identity[.]info
- document-share[.]info
- document.support-recoverycustomers[.]services
- documentofficupdate[.]info
- documents.accounts-support[.]services
- documentsfilesharing[.]cloud
- email-delivery[.]info
- mobile-sessionid.customize-identity[.]info
- mobiles-sessionid.customize-identity[.]info
- my-scribdinc[.]online
- myyahoo.ddns[.]net
- notificationapp[.]info
- onlinemessenger.com-identifier-servicelog[.]name
- podcastmedia[.]online
- recoveryusercustomer[.]info
- session-management[.]info
- support-recoverycustomers[.]services
- continue-session-identifier[.]info
- mobilecontinue[.]network
- session-identifier-webservice.mobilecontinue[.]network
- com-messengersaccount[.]name
- invitation-to-messenger[.]space
- confirm-identification[.]name
- mobilecontinue[.]network
- mobile.confirm-identification[.]name
- services.confirm-identification[.]name
- mobile-messengerplus[.]network
- confirm.mobile-messengerplus[.]network
- com-messengercenters[.]name
- securemail.mobile-messengerplus[.]network
- documents.mobile-messengerplus[.]network
- confirm-identity[.]net
- identifier-sessions-mailactivityid[.]site
- activatecodeoption.ddns[.]net
- broadcastpopuer.ddns[.]net
- books.com-identifier-servicelog[.]name
- mb.sessions-identifier-memberemailid[.]network
- sessions-identifier-memberemailid[.]network
- sessions.mobile-messengerplus[.]network
- confirm-verification-process[.]systems
- accounts.confirm-verification-process[.]systems
- broadcastnews.ddns[.]net
- account-profile-users[.]info
- us2-mail-login-profile[.]site
- us2.login-users-account[.]site
- login-users-account[.]site
- live.account-profile-users[.]info
- signin.account-profile-users[.]info
- aol.account-profile-users[.]info
- users-account[.]site

Footnotes:

1. https://s.certfa.com/q1514c
https://s.certfa.com/eNnnag
https://s.certfa.com/ur93p2 ↩
2. ClearSkye Cyber Security (2018), "Charming Kitten, Iranian cyber espionage against human rights activists, academic researchers and media outlets - and the HBO hacker connection". Accessed November 15, 2018. https://s.certfa.com/1ulIxk ↩
3. Sites. Accessed November 23, 2018. https://sites.google.com/ ↩
4. Firefox Screenshots. Accessed November 15, 2018. https://screenshots.firefox.com/ ↩
5. VirusTotal Graph. Accessed November 25, 2018. https://s.certfa.com/OgQUSC ↩
6. Sender Policy Framework or SPF is an email authentication method to detect forged sender addresses in emails. SPF allows the recipient to check that an email claiming to come from a specific domain comes from an IP address authorized by that domain's administrators. ↩
7. G Suite Administrator Help (2018), "Restrict messages to authorized addresses or domains". Accessed November 29, 2018. https://support.google.com/a/answer/2640542?hl=en ↩

Charming Kitten APT Iran Phishing