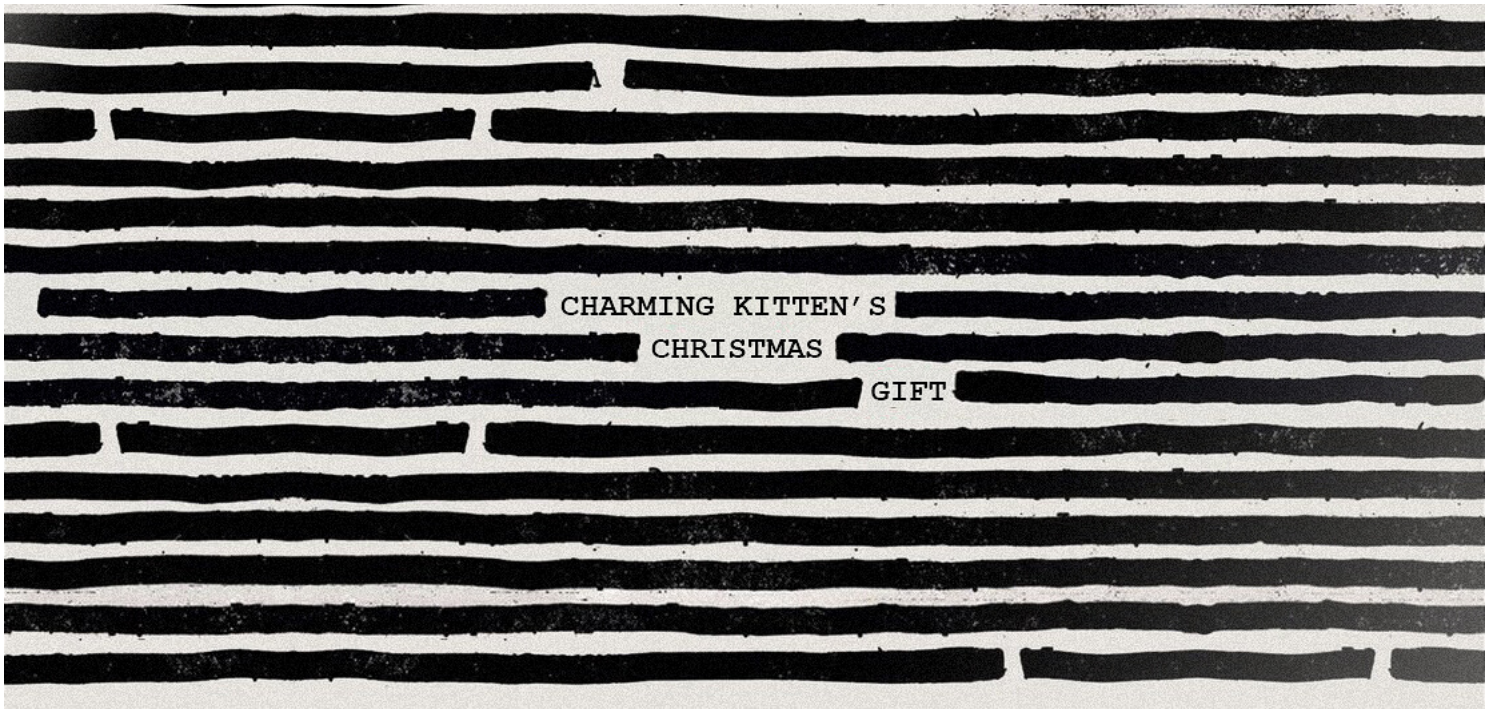
Charming Kitten’s Christmas Gift

blog.certfa.com/posts/charming-kitten-christmas-gift

A review of the latest Charming Kitten phishing campaign

Certfa Lab · 2021.1.8



During the Christmas holidays and the beginning of the new year, the Charming Kitten group, the Iranian state-backed hackers, have begun a targeted phishing campaign of espionage against different individuals to collect information.

Charming Kitten, also known as APT35 and Phosphorus, is one of the hacker groups backed by the Islamic Republic of Iran. The group started the new round of attacks at a time when most companies, offices, organizations, etc. were either closed or half-closed during Christmas holidays and, as a result, their technical support and IT departments were not able to immediately review, identify, and neutralize these cyber incidents. Charming Kitten has taken full advantage of this timing to execute its new campaign to maximum effect.

A review of samples of this phishing campaign shows that the attackers concentrated their attacks on individuals’ online accounts, especially personal emails (Gmail, Yahoo! and Outlook) and business emails (organization and university emails). After accessing the credential details of the accounts, they steal sensitive data from their victims.

Additionally, based on the collected evidence, it is clear that Charming Kitten specifically chose their targets from members of think tanks, political research centers, university professors, journalists, and environmental activists in the countries around the Persian Gulf, Europe, and the US. Our observations show this phishing campaign is a

continuation of other Charming Kitten campaigns that were started in the third and fourth quarters of 2020.

Details Of The Attacks

Our examination of the acquired samples shows hackers generally use two main methods of “Sending Fake SMS” and “Sending Fake Emails” to execute their attacks. It is also important to note that whilst using these two methods, the attackers try not to leave any trace of themselves and, even

after gaining access to their victims’ accounts, they do not block the victims’ access to their own accounts.

Method #1: Fake SMS

Like many other phishing attacks, in this phishing campaign, Charming Kitten uses a fake SMS (Figure 1) to trick their victims. They send confirmation messages stating ‘Google Account Recovery’ to their targets; they claim these messages are sent by Google and the user must follow the link in the SMS to confirm the identity.

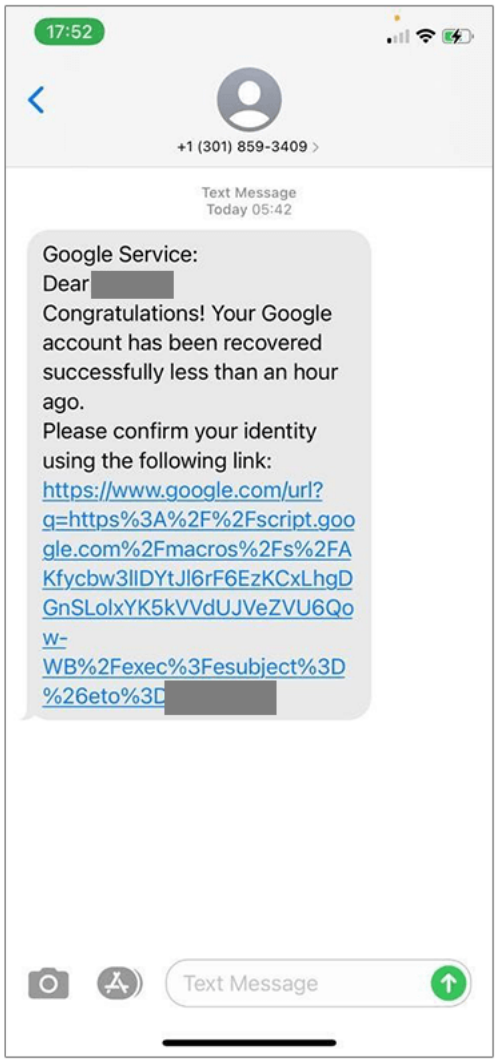


Figure 1. A sample of the fake SMS

The most important point in this method is the structure of the link in the SMS that seems legitimate: hxxps://www.google[.]com/url?q=https://script.google.com/xxxx.

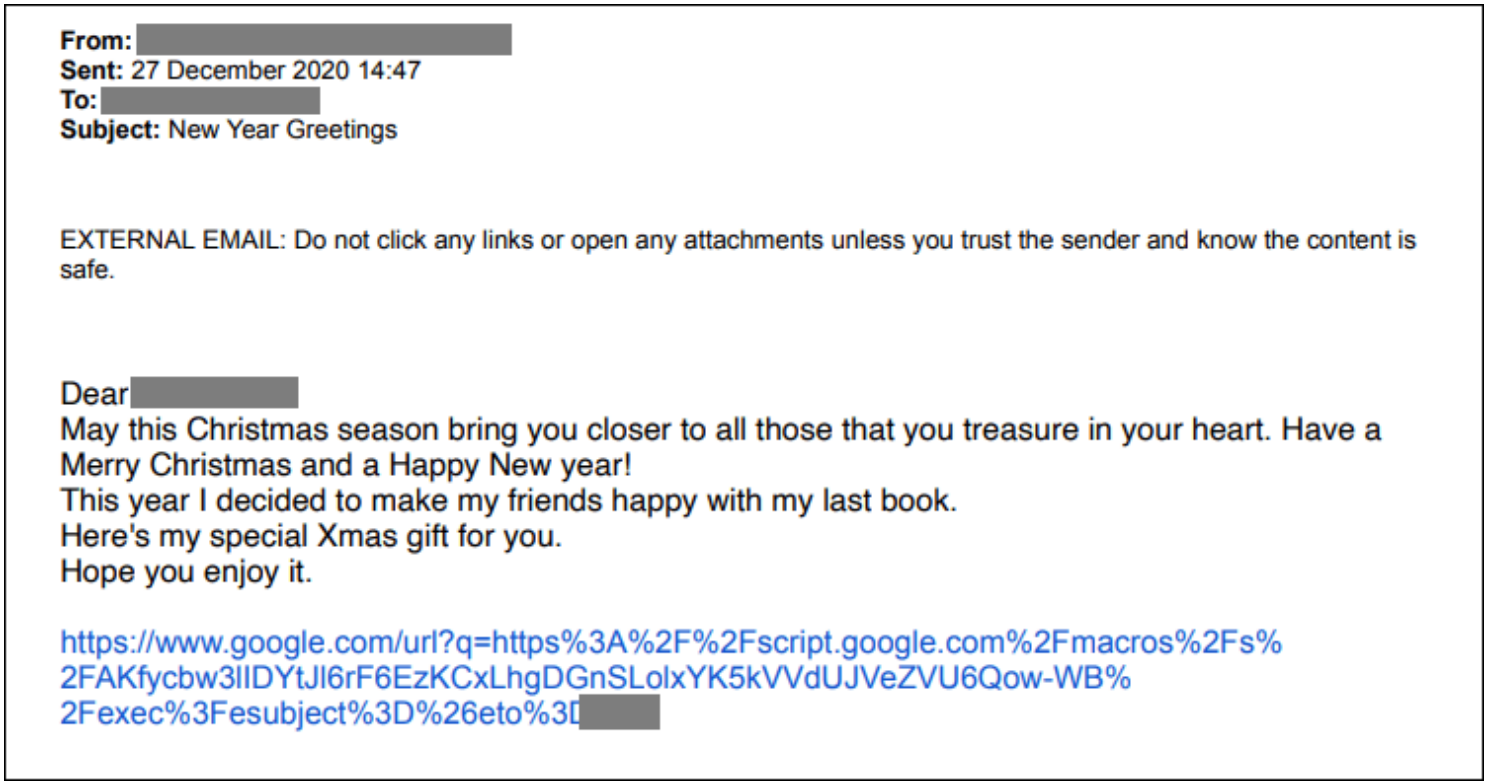
At first glance, these links generally cause less suspicion for the targets. After opening the links and several redirections, the victims are led to final phishing domains such as “mobile[.]recover-session-service[.]site” etc. More detail about this technique is available in the Redirect Chain section.

Method #2: Fake Email

Another method used in this phishing campaign is sending fake emails with deceptive titles like “Merry Christmas, and sending note/book/photo and others”, which are usually sent by previously hacked emails.

Figure 2 shows one of these phishing emails where the attackers cordially invite the target to open the link in the email’s body. In order to achieve this, Charming Kitten used the subject “New Years Greetings” with convincing sentences such as “This year I decided to make my friends happy with my last book. Here’s my special Xmas gift for you.” in

the body of email. By comparing Figure 2 to Figure 1, it is clear that the structure of the link is similar to the links used in the fake SMS.


From: [redacted]
Sent: 27 December 2020 14:47
To: [redacted]
Subject: New Year Greetings

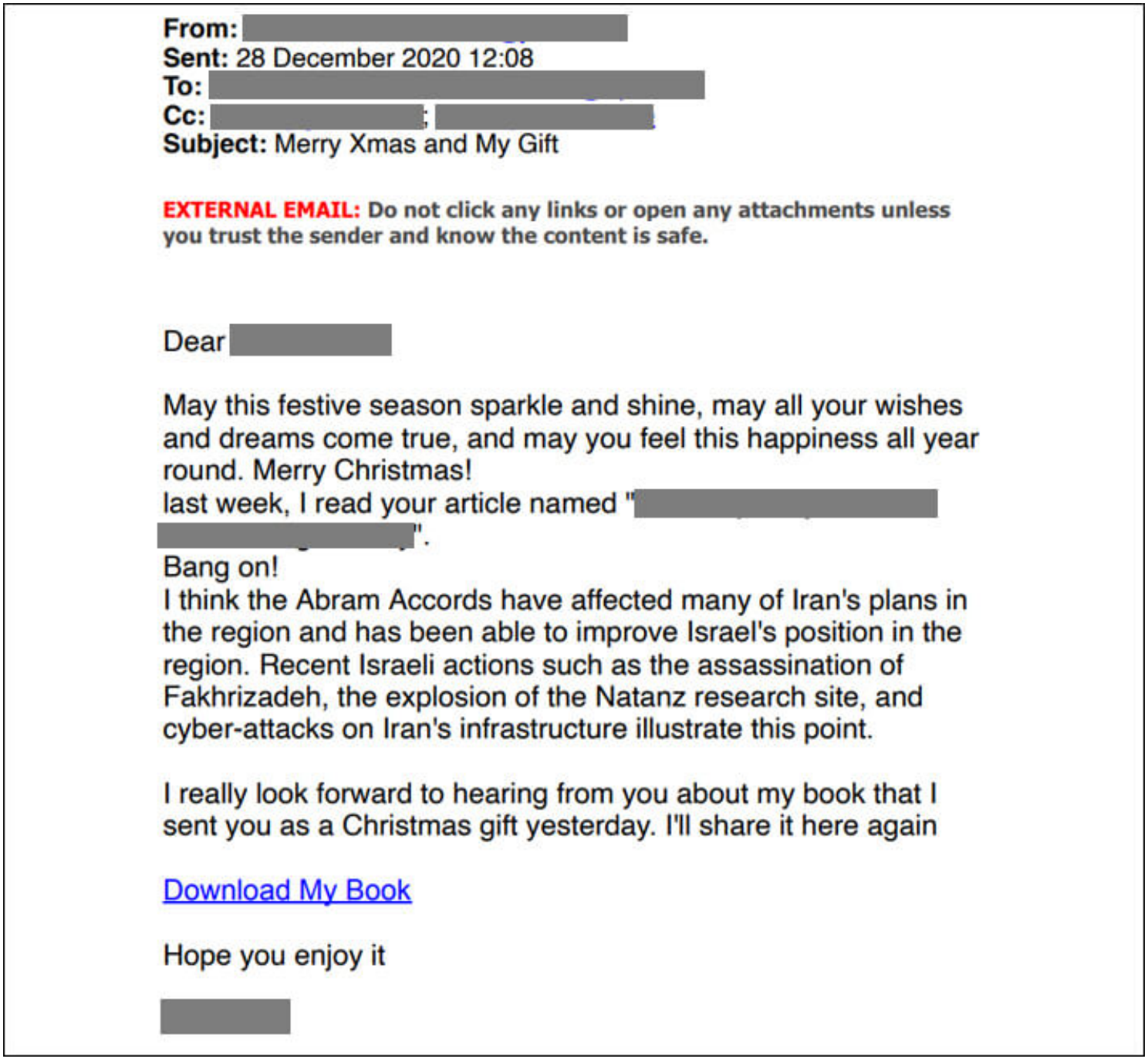
EXTERNAL EMAIL: Do not click any links or open any attachments unless you trust the sender and know the content is safe.

Dear [redacted]
May this Christmas season bring you closer to all those that you treasure in your heart. Have a Merry Christmas and a Happy New year!
This year I decided to make my friends happy with my last book.
Here's my special Xmas gift for you.
Hope you enjoy it.

https://www.google.com/url?q=https%3A%2F%2Fscript.google.com%2Fmacros%2Fs%2FAKfycbw3lIDYtJl6rF6EzKCxLhgDGnSLolxYK5kVVdUJVeZVU6Qow-WB%2Fexec%3Fesubject%3D%26eto%3D[redacted]

Figure 2. A sample of the fake email

We believe that Charming Kitten continuously try different styles of email to trap their victims as quickly as possible. For example, Figure 3 shows another fake email that was sent to the same victim a day after the initial email (Figure 2).



From: [redacted]
Sent: 28 December 2020 12:08
To: [redacted]
Cc: [redacted]; [redacted]
Subject: Merry Xmas and My Gift

EXTERNAL EMAIL: Do not click any links or open any attachments unless you trust the sender and know the content is safe.

Dear [redacted]

May this festive season sparkle and shine, may all your wishes and dreams come true, and may you feel this happiness all year round. Merry Christmas!
last week, I read your article named "[redacted]".
Bang on!
I think the Abram Accords have affected many of Iran's plans in the region and has been able to improve Israel's position in the region. Recent Israeli actions such as the assassination of Fakhrizadeh, the explosion of the Natanz research site, and cyber-attacks on Iran's infrastructure illustrate this point.

I really look forward to hearing from you about my book that I sent you as a Christmas gift yesterday. I'll share it here again

Download My Book

Hope you enjoy it

[redacted]

Figure 3. A sample of fake email after sending the initial email to the target

Redirect Chain

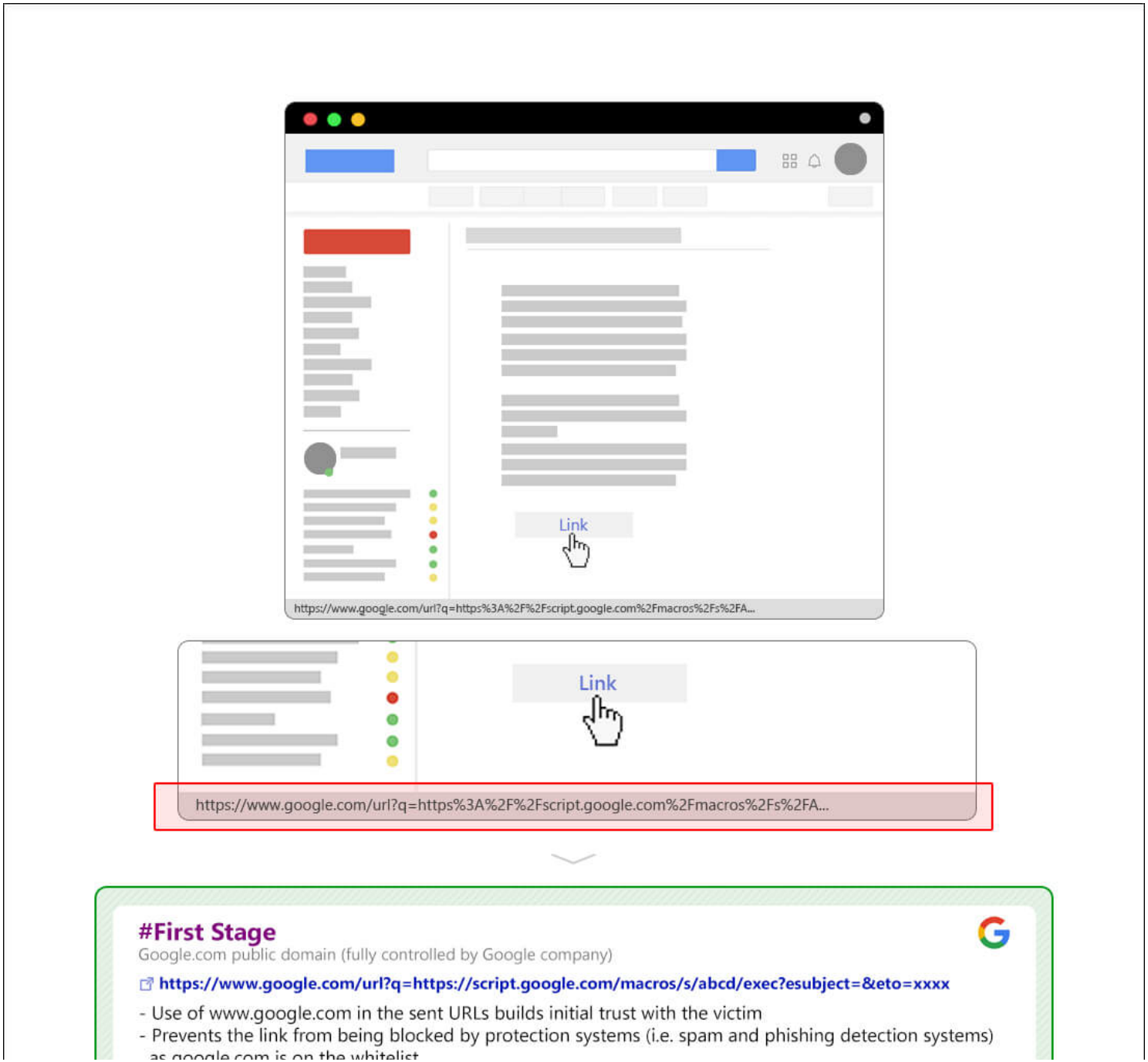
Utilizing and weaponizing legal and credible services to hide destructive intent is one of the techniques used by hackers in some phishing campaigns.

This technique has become significant in the recent campaign by Charming Kitten. Our latest investigations show that this Iranian hacking group has focused on this method over the past two years.

For example, Charming Kitten weaponized “site.google.com”[1] in 2019 and “script.google.com” in this campaign.

Our examination shows the hackers have used a mix of services such as ‘script.google.com’ and ‘iplogger.org’ in this campaign in order to create a chain of redirection to obfusticate their hacking operations. Redirection links initially help bypass the security layers in email services, and then provide the attackers more control to redirect the target to the final URL.

Figure 4 shows an experimental example of the function of each link in the redirect chain technique.


Link
https://www.google.com/url?q=https%3A%2F%2Fscript.google.com%2Fmacros%2Fs%2FA...
Link
https://www.google.com/url?q=https%3A%2F%2Fscript.google.com%2Fmacros%2Fs%2FA...
#First Stage
Google.com public domain (fully controlled by Google company)
https://www.google.com/url?q=https://script.google.com/macros/s/abcd/exec?esubject=&eto=xxxx
- Use of www.google.com in the sent URLs builds initial trust with the victim
- Prevents the link from being blocked by protection systems (i.e. spam and phishing detection systems)
as google.com is on the whitelist

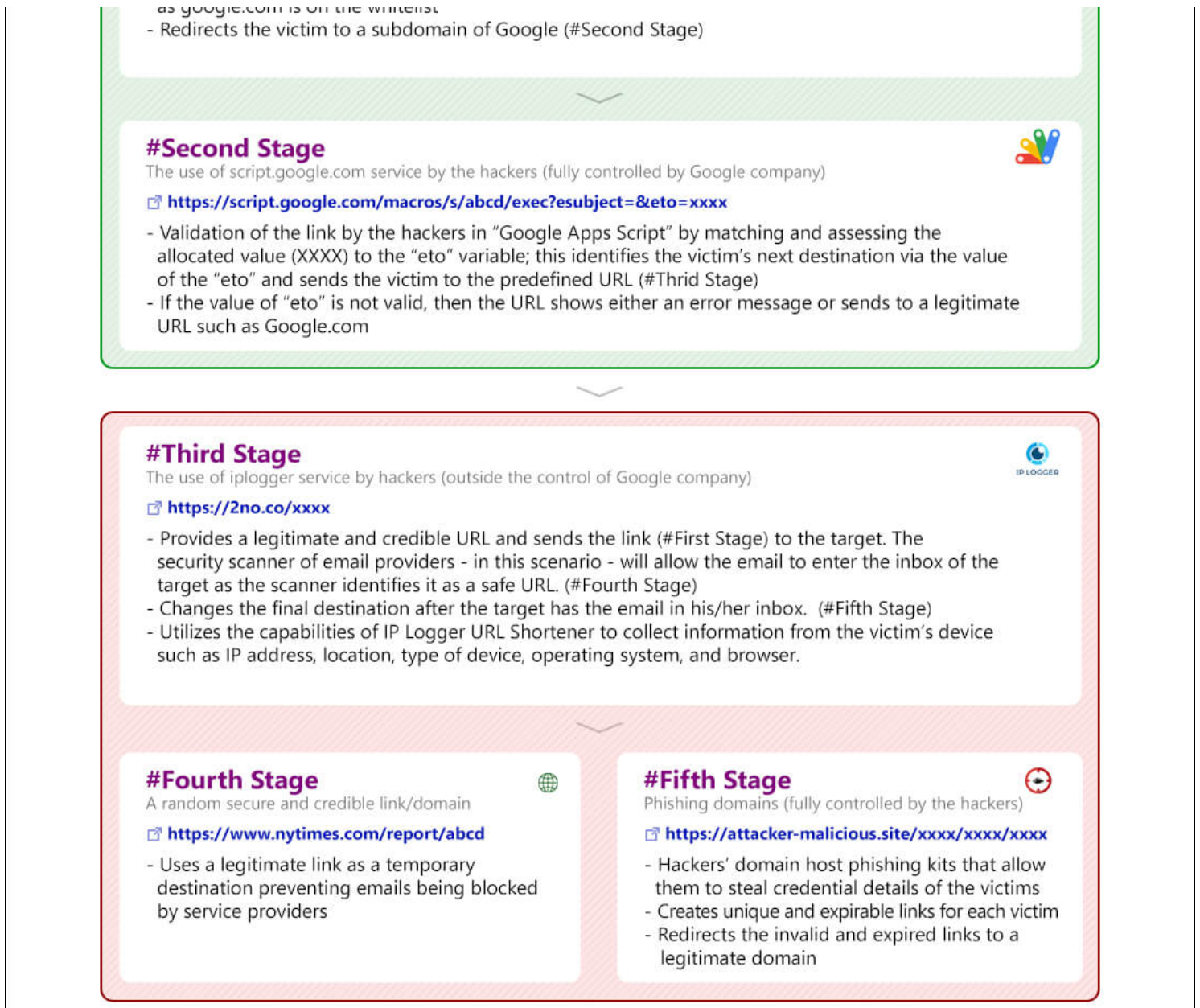

as google.com is on the whitelist
- Redirects the victim to a subdomain of Google (#Second Stage)
#Second Stage
The use of script.google.com service by the hackers (fully controlled by Google company)
https://script.google.com/macros/s/abcd/exec?esubject=&eto=xxxx
- Validation of the link by the hackers in "Google Apps Script" by matching and assessing the allocated value (XXXX) to the "eto" variable; this identifies the victim's next destination via the value of the "eto" and sends the victim to the predefined URL (#Thrid Stage)
- If the value of "eto" is not valid, then the URL shows either an error message or sends to a legitimate URL such as Google.com
#Third Stage
The use of iplogger service by hackers (outside the control of Google company)
IP LOGGER
https://2no.co/xxxx
- Provides a legitimate and credible URL and sends the link (#First Stage) to the target. The security scanner of email providers - in this scenario - will allow the email to enter the inbox of the target as the scanner identifies it as a safe URL. (#Fourth Stage)
- Changes the final destination after the target has the email in his/her inbox. (#Fifth Stage)
- Utilizes the capabilities of IP Logger URL Shortener to collect information from the victim's device such as IP address, location, type of device, operating system, and browser.
#Fourth Stage
A random secure and credible link/domain
https://www.nytimes.com/report/abcd
- Uses a legitimate link as a temporary destination preventing emails being blocked by service providers
#Fifth Stage
Phishing domains (fully controlled by the hackers)
https://attacker-malicious.site/xxxx/xxxx/xxxx
- Hackers' domain host phishing kits that allow them to steal credential details of the victims
- Creates unique and expirable links for each victim
- Redirects the invalid and expired links to a legitimate domain

Figure 4. Experimental example for redirect chain

Infinite different types of phishing attacks

Our investigation shows Charming Kitten has targeted different people and organisations in relatively different fields. For example, based on our initial findings, the hackers use domain names such as mail-newyorker[.]com, news12[.]com[.]recover-session-service[.]site with the intention of targeting “The New Yorker” online magazine readers and “News 12 Networks” TV channel staff and their audience.

Charming Kitten had previously used the same method using names such as Wall Street Journal[1], CNN[2], Deutsche Welle[3], etc.

Subject: Qoroq Shipwreck Pics
From: [redacted]
Date: 12/27/2020, 10:28 PM
To: [redacted]

ممنونم از مقاله تون. بسیار عالی بود و ازش لذت بردم. عکسها و مطالب بسیار جذاب بود.تبریک میگم بهتون.
اتفاقا سفری که یکی دو سال پیش با یکی از دوستانم به این منطقه داشتیم عکسهای خوبی از این لوکیشن گرفتیم که به نکات جالبی رسیدیم که توی مقاله شما ندیدم. فکر میکنم عکسها و مطالبم رو ببینید متوجه ش بشید. براتون همینجا شیر میکنم.

https://www.google.com/url?q=https%3A%2F%2Fscript.google.com%2Fmacros%2Fs%2FAKfycbw3lIDYtJl6rF6EzKCxLhgDGnSLolxYK5kVVdUJVeZVU6Qow-WB%2Fexec%3Fesubject%3D%26eto%3[redacted]

--
[redacted]

Figure 5. Another example of the phishing emails from Charming Kitten

> **Translation:**
> Thanks for your article. It was fantastic and I enjoyed it. Photos and contents were very interesting. Congratulations! We actually traveled to this area with my friends a couple of years ago and took some good pictures at this location and found some interesting things that I didn’t see in your article. I think you’ll understand if you see my pictures and contents. I’ll share it for you here.

In reviewing other samples, we have found that Charming Kitten has used many fake domains to target different online accounts in different services. Although accounts such as Gmail, Yahoo! and

Outlook are the main targets of this campaign, there are more samples that show this Iranian hacking group targets other services such as Planet.com and PlanetObserver.com - both are online satellite imagery services for special sectors such as governments, industries, and military defenses - which shows the breadth of their campaign. Figures 6 to 8 are different series of phishing pages that were developed by Charming Kitten.

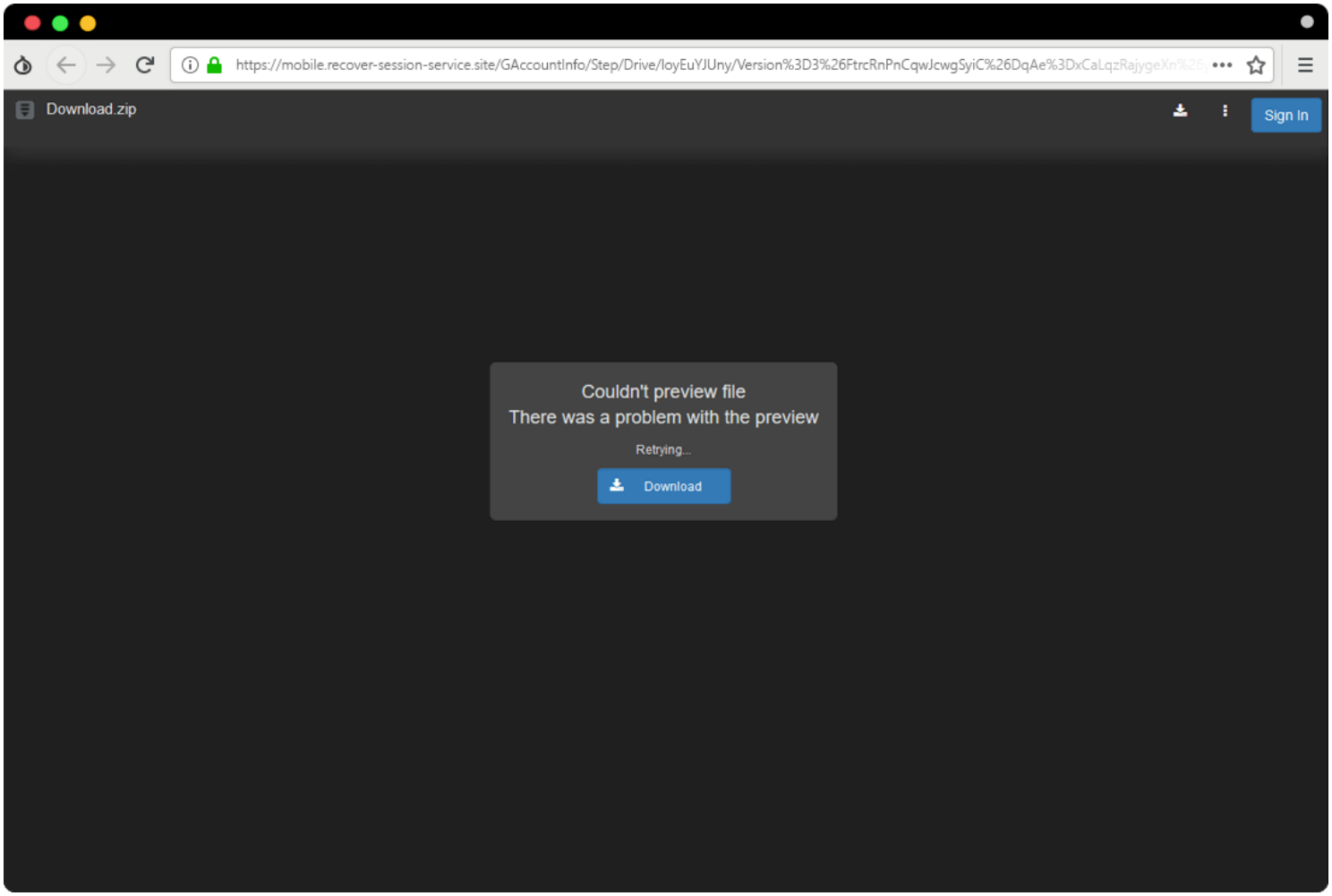


Figure 6. A fake Google Drive page to steal credential details of a Google account.[4]

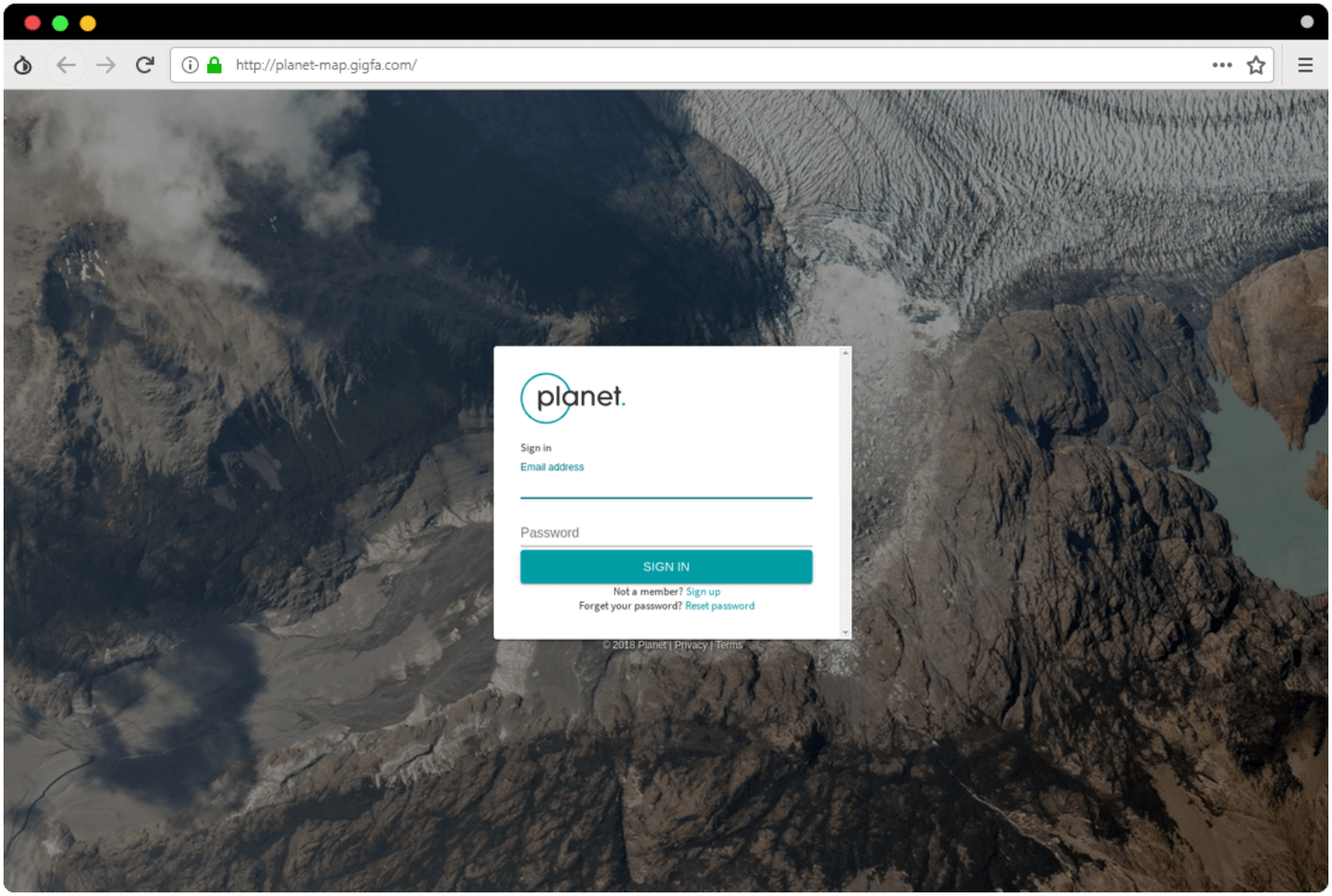


Figure 7. An initial copy of Planet.com on an Iranian free hosting website to create a fake login page and steal the credential details of Planet.com’s users. This page has been recently transferred to hello-planet[.]com.[5]

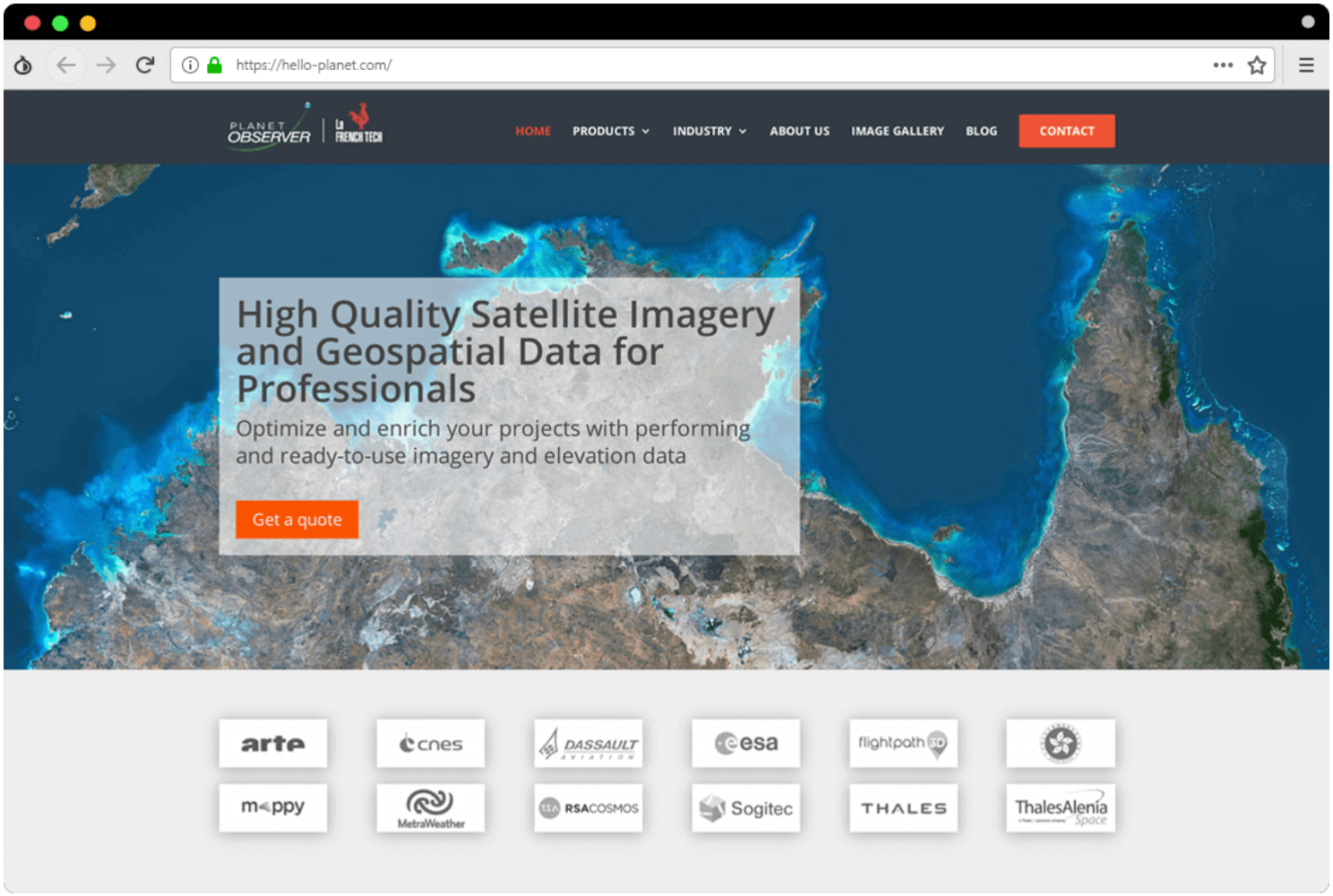


Figure 8. A fake website of PlanetObserver.com[6]

Infrastructure and History

We have reviewed and matched five common indicators to assess and analyze the infrastructure that has been used by Charming Kitten (Figure 9). This infrastructure has been used mostly in the third and fourth quarters of 2020:

- Reverse IP/DNS lookup and matching the history with other common indicators
- Common IP or IP CIDR range match
- Use of unconventional TLD (i.e. .site) and using WHOIS protection
- Use of deceptive words such as session, confirm, recovery, verification, service, etc., in the name of the URLs as well as subdomains

- Parallel use of Dynamic DNS, such as ddns.net, in a short period of time, which has a temporal matching with other indicators

Reviewing these indicators side by side show that Charming Kitten has been constantly active in recent months and has executed other attacks at the time of writing this report.

In reviewing related activity patterns of Charming Kitten and information about the infrastructure used by this hacking group, we believe the extent and scale of this campaign is significant in comparison with previous activity of Charming Kitten.

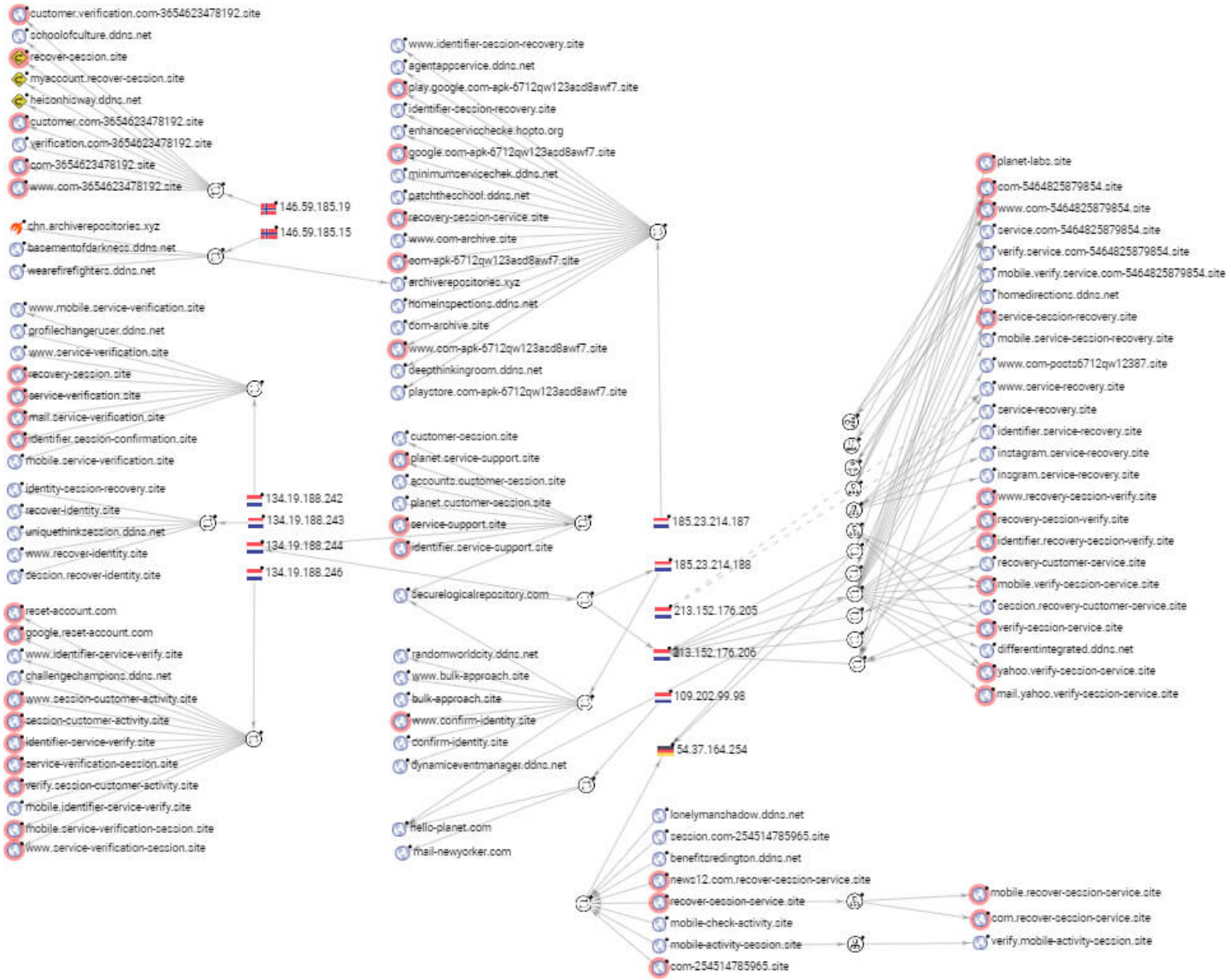

customer.verification.com-3654623478192.site
schoolofculture.ddns.net
recover-session.site
myaccount.recover-session.site
heisonhiway.ddns.net
customer.com-3654623478192.site
verification.com-3654623478192.site
com-3654623478192.site
www.com-3654623478192.site
146.59.185.19
146.59.185.15
chn.archiverepositories.xyz
basementofdarkness.ddns.net
wearefirefighters.ddns.net
www.identifier-session-recovery.site
agentappservice.ddns.net
play.google.com-apk-6712qw123asd8awf7.site
identifier-session-recovery.site
enhanceservicchecke.hopto.org
google.com-apk-6712qw123asd8awf7.site
minimumservicechek.ddns.net
patchtheschool.ddns.net
recovery-session-service.site
www.com-archive.site
com-apk-6712qw123asd8awf7.site
archiverepositories.xyz
homeinspections.ddns.net
dom-archive.site
www.com-apk-6712qw123asd8awf7.site
deepthinkingroom.ddns.net
playstore.com-apk-6712qw123asd8awf7.site
planet-labo.site
com-5464825879854.site
www.com-5464825879854.site
service.com-5464825879854.site
verify.service.com-5464825879854.site
mobile.verify.service.com-5464825879854.site
homedirections.ddns.net
service-session-recovery.site
mobile.service-session-recovery.site
www.com-posts6712qw12387.site
www.service-recovery.site
service-recovery.site
identifier.service-recovery.site
instagram.service-recovery.site
inagram.service-recovery.site
www.recovery-session-verify.site
recovery-session-verify.site
identifier.recovery-session-verify.site
recovery-customer-service.site
mobile.verify-session-service.site
session.recovery-customer-service.site
verify-session-service.site
differentintegrated.ddns.net
yahoo.verify-session-service.site
mail.yahoo.verify-session-service.site
www.mobile.service-verification.site
profilechangeruser.ddns.net
www.service-verification.site
recovery-session.site
service-verification.site
mail.service-verification.site
identifier.session-confirmation.site
mobile.service-verification.site
identity-session-recovery.site
recover-identity.site
uniquethinksession.ddns.net
www.recover-identity.site
session.recover-identity.site
134.19.188.242
134.19.188.243
134.19.188.244
134.19.188.246
customer-session.site
planet.service-support.site
accounts.customer-session.site
planet.customer-session.site
service-support.site
identifier.service-support.site
185.23.214.187
185.23.214.188
213.152.176.205
213.152.176.206
109.202.99.98
54.37.164.254
securelogicalrepository.com
randomworldcity.ddns.net
www.bulk-approach.site
bulk-approach.site
www.confirm-identity.site
confirm-identity.site
dynamiceventmanager.ddns.net
hello-planet.com
mail-newyorker.com
reset-account.com
google.reset-account.com
www.identifier-service-verify.site
challengechampions.ddns.net
www.session-customer-activity.site
session-customer-activity.site
identifier-service-verify.site
service-verification-session.site
verify.session-customer-activity.site
mobile.identifier-service-verify.site
mobile.service-verification-session.site
www.service-verification-session.site
lonelymanshadow.ddns.net
session.com-254514785965.site
benefitsredington.ddns.net
news12.com.recover-session-service.site
recover-session-service.site
mobile-check-activity.site
mobile-activity-session.site
com-254514785965.site
mobile.recover-session-service.site
com.recover-session-service.site
verify.mobile-activity-session.site

Figure 9. Overview of the infrastructure of Charming Kitten's phishing campaign in the second half of 2020[7]

Conclusion And Recommendations

This investigation only relates to one aspect of the Iran-backed hacker group's activities in recent months; the extent and magnitude of this campaign was unforeseeable. We can conclude that Charming Kitten has used complex techniques to gain access to individuals and organizations that Iranian intelligence services are interested in targeting.

In order to protect yourself against these attacks, we strongly recommend using secure and safe authentication methods such as two factor authentication with security keys, such YubiKey[8], for your online accounts.

As usual, we firmly suggest not to click on unknown links, to carefully review any URLs before entering credential information, and not to download and run unknown files on mobile, personal or work computers. These measures can significantly protect people who are the targets of these types of campaigns.

It is important to note that the main cases mentioned in this report relate to the latest Charming Kitten’s phishing campaign and that this campaign has significantly intensified in recent days.

IOCs

- 54.37.164[.]254
- 109.202.99[.]98
- 134.19.188[.]242
- 134.19.188[.]243
- 134.19.188[.]244
- 134.19.188[.]246

- 185.23.214[.]188
- 213.152.176[.]205
- 213.152.176[.]206
- 146.59.185[.]15
- 146.59.185[.]19
- 185.23.214[.]187
- com-254514785965[.]site
- mobile[.]verification[.]session[.]com-254514785965[.]site
- session[.]com-254514785965[.]site
- verification[.]session[.]com-254514785965[.]site
- www[.]com-254514785965[.]site
- com-546482587985 4[.]site

- mobile[.]verify[.]service[.]com-546482587985 4[.]site
- service[.]com-546482587985 4[.]site
- verify[.]service[.]com-546482587985 4[.]site
- www[.]com-546482587985 4[.]site
- benefitsredington[.]ddns[.]net
- lonelymanshadow[.]ddns[.]net
- mobile-activity-session[.]site
- verify[.]mobile-activity-session[.]site
- www[.]mobile-activity-session[.]site
- mobile-check-activity[.]site
- www[.]mobile-check-activity[.]site
- com[.]recover-session-service[.]site
- mobile[.]recover-session-service[.]site
- news12[.]com[.]recover-session-service[.]site

- recover-session-service[.]site
- www[.]recover-session-service[.]site
- hello-planet[.]com
- mail-newyorker[.]com
- profilechangeruser[.]ddns[.]net
- www[.]service-verification[.]site
- www[.]mobile[.]service-verification[.]site
- service-verification[.]site
- mobile[.]service-verification[.]site
- mail[.]service-verification[.]site
- com[.]service-verification[.]site
- app-e[.]request[.]unlock-service[.]accounts[.]service-verification[.]site
- instagram[.]com[.]service-verification[.]site

- unlock-service[.]accounts[.]service-verification[.]site
- request[.]unlock-service[.]accounts[.]service-verification[.]site
- accounts[.]service-verification[.]site
- identifier[.]recovery-session[.]site
- recovery-session[.]site
- www[.]recovery-session[.]site
- www[.]identifier[.]recovery-session[.]site
- identifier[.]session-confirmation[.]site
- session-confirmation[.]site
- www[.]session-confirmation[.]site
- identity-session-recovery[.]site
- uniquethinksession[.]ddns[.]net
- recover-identity[.]site

- session[.]recover-identity[.]site
- www[.]recover-identity[.]site
- securelogicalrepository[.]com
- service-support[.]site
- customer-session[.]site
- planet[.]customer-session[.]site
- accounts[.]customer-session[.]site
- www[.]customer-session[.]site
- www[.]service-support[.]site
- identifier[.]service-support[.]site
- planet[.]service-support[.]site
- reset-account[.]com
- google[.]reset-account[.]com
- www[.]reset-account[.]com
- session-customer-activity[.]site

- verify[.]session-customer-activity[.]site
- www[.]session-customer-activity[.]site
- www[.]identifier-service-verify[.]site
- identifier-service-verify[.]site
- mobile[.]identifier-service-verify[.]site
- challengechampions[.]ddns[.]net
- service-verification-session[.]site
- mobile[.]service-verification-session[.]site
- www[.]service-verification-session[.]site
- chn[.]archiverepositories[.]xyz
- www[.]archiverepositories[.]xyz
- archiverepositories[.]xyz
- a[.]archiverepositories[.]xyz
- wearefirefighters[.]ddns[.]net
- basementofdarkness[.]ddns[.]net

- heisonhisway[.]ddns[.]net
- recover-session[.]site
- www[.]recover-session[.]site
- myaccount[.]recover-session[.]site
- schoolofculture[.]ddns[.]net
- customer[.]verification[.]com-3654623478192[.]site
- com-3654623478192[.]site
- customer[.]com-3654623478192[.]site
- www[.]com-3654623478192[.]site
- verification[.]com-3654623478192[.]site
- enhanceservicchecke[.]hopto[.]org
- minimumservicechek[.]ddns[.]net
- playstore[.]com-apk-6712qw123asd8awf7[.]site

- www[.]com-apk-6712qw123asd8awf7[.]site
- www[.]identifier-session-recovery[.]site
- google[.]com-apk-6712qw123asd8awf7[.]site
- play[.]google[.]com-apk-6712qw123asd8awf7[.]site
- identifier-session-recovery[.]site
- com-apk-6712qw123asd8awf7[.]site
- agentappservice[.]ddns[.]net
- www[.]com-archive[.]site
- com-archive[.]site
- patchtheschool[.]ddns[.]net
- www[.]recovery-session-service[.]site
- mobile[.]recovery-session-service[.]site
- homeinspections[.]ddns[.]net
- recovery-session-service[.]site

- deepthinkingroom[.]ddns[.]net
- randomworldcity[.]ddns[.]net
- bulk-approach[.]site
- www[.]bulk-approach[.]site
- confirm-identity[.]site
- www[.]confirm-identity[.]site
- dynamiceventmanager[.]ddns[.]net
- service-recovery[.]site
- differentintegrated[.]ddns[.]net
- verify-session-service[.]site
- yahoo[.]verify-session-service[.]site
- mail[.]yahoo[.]verify-session-service[.]site
- www[.]verify-session-service[.]site
- mobile[.]verify-session-service[.]site
- session[.]recovery-customer-service[.]site

- recovery-customer-service[.]site
- www[.]recovery-customer-service[.]site
- homedirections[.]ddns[.]net
- recovery-session-verify[.]site
- www[.]recovery-session-verify[.]site
- identifier[.]recovery-session-verify[.]site
- service-session-recovery[.]site
- mobile[.]service-session-recovery[.]site
- www[.]service-session-recovery[.]site
- planet-labs[.]site
- mail[.]com-posts6712qw12387[.]site
- video[.]instagram[.]service-recovery[.]site
- insgram[.]service-recovery[.]site
- identifier[.]service-recovery[.]site
- instagram[.]service-recovery[.]site

- www[.]planet-labs[.]site
- com-posts6712qw12387[.]site
- www[.]com-posts6712qw12387[.]site
- www[.]service-recovery[.]site
- planet-map[.]gigfa[.]com

Footnotes:

---

1. Certfa.com. “Fake Interview: The New Activity of Charming Kitten”. Accessed January 5, 2021. https://s.certfa.com/Mg5p41 ⇆

2. clearskysec.com. “The Kittens Are Back in Town”. Accessed January 5, 2021. https://s.certfa.com/Q91xTz ⇆
3. clearskysec.com. “The Kittens Are Back in Town 3”. Accessed January 5, 2021. https://s.certfa.com/yIs38b ⇆
4. URLScan.io, “Fake Google Drive to steal google account credential”. Accessed January 5, 2021. https://s.certfa.com/q91bBa ⇆
5. URLScan.io, “Fake planet.com login page for steal user account credential”. Accessed January 5, 2021. https://s.certfa.com/hMvpi1 ⇆

6. URLScan.io, “Fake planetobserver.com website”. Accessed January 5, 2021. https://s.certfa.com/pN9140 ⇆
7. VirusTotal.com, “Overview of the new infrastructure used by Charming Kitten”. Accessed January 5, 2021. https://s.certfa.com/uIoXnm ⇆
8. Wikipedia.org “YubiKey” Accessed January 5, 2021. https://s.certfa.com/o0pXiI ⇆