The Kittens Are Back in Town 2

Charming Kitten Campaign Keeps Going on, Using New Impersonation Methods

October 2019

TLP:WHITE

Table of Content

Introduction

On the 15th of September 2019, we have published a report[1] about a sharp increase in Charming Kitten attacks against researchers from the US, Middle East, and France, focusing on Iranian academic researchers, Iranian dissidents in the US. In our last report, we exposed a new cyber espionage campaign that was conducted in July 2019. Since then, we observed another wave of these attacks, leveraging new impersonating vectors and IOCs.

Until these days, Iran was not known as a country who tends to interfere in elections around the world. From a historical perspective, this type of cyber activities had been attributed mainly to the Russian APT groups such as APT28 (known as Fancy Bear). The group is infamous for hacking American Democratic National Committee emails and targeting German and French campaign members, in an attempt to circumvent the elections in the US, Germany and France. Microsoft's October announcement exposes, for first time, that **Charming Kitten, an Iranian APT group, plays a role in the domain of cyber-attacks for the purpose of interfering with democratic procedures.**

On 4th of October 2019[2], Microsoft has announced that Phosphorus (known as Charming Kitten) attempted to attack email accounts that are associated with the following targets: U.S. presidential campaign, current and former U.S. government officials, journalists covering global politics, and prominent Iranians living outside Iran. These spear-phishing attacks were conducted by Charming Kitten in August and September. **We evaluate in a medium-high level of confidence, that Microsoft's discovery and our findings in our previous and existing reports is a congruent operation, based on the following issues:**

1. **Same victim profiles** – In both cases, the victims were individuals of interest to Iran in the fields of academic research, human rights, opposition to the Islamic Republic of Iran's regime (such as NIAC) and journalists. Although the congruent is not exactly similar, our sample is mainly based on Israeli victims.
2. **Time overlapping** – In our latest report, we mentioned that we have observed an escalation of the attacks in July-August 2019. In their announcement, Microsoft mentioned that the attacks occurred on 'In a 30-day period between August and September'.
3. **Similar attack vectors** – In both cases, Charming Kitten used similar attack vectors which are:
    a. Password recovery impersonation of the secondary email belonging to the victims in both cases.
    b. Both attack vectors used spear-phishing emails in order to target Microsoft, Google and Yahoo services.
    c. In our research, we identified a spear-phishing attack via SMS messages, indicating that Charming Kitten gathers phone numbers of the relevant victim. Microsoft found that Charming Kitten gathers phone numbers for password recovery and two-factor authentications of the relevant victims to gain control to their email accounts.

In this report, we uncovered four new spear-phishing methods used by this group, alongside with new indicators of this operation.

[1] https://www.clearskysec.com/the-kittens-are-back-in-town/
[2] https://blogs.microsoft.com/on-the-issues/2019/10/04/recent-cyberattacks-require-us-all-to-be-vigilant/

About Charming Kitten

Charming Kitten, also known as APT35 or Ajax or Phosphorus, is an Iranian cyber-espionage group active since 2014[3].This APT is associated with the Ministry of Intelligence of Iran. In our previous report, we made an attack timeline. Below is a key event timeline:

2015

- *ClearSky* discovered the first wave of phishing attacks, named "Thamar reservoir".

2017

- *ClearSky* exposed a vast espinage operation against Iranian experts working in the academy, human rights activists and media personnel.

2018

- Charming Kitten attempted to attack *ClearSky* and our customers directly via a fraudulent website impersonating the ClearSky portal.
- *ClearSky* identified new wave of attacks against researchers in the Middle East, using fake emails and look-alike websites.

2019

- **March** - *Microsoft* filed an official complaint against the group for "establishing an internet-based cyber theft operation referred to as 'Phosphorus'."
- **September** - *ClearSky* published a report about a sharp increase in Charming Kitten attacks. It appears that group has initiated a new cyber espionage campaign comprised of two stages.
- **October** - *Microsoft* announced that 'the group is making attempts to identify consumer email accounts belonging to specific Microsoft customers, including a **US Presidential Candidate** . *ClearSky* exposed new impersonation vectors.

See corresponding footnote for relevant references[4].

[3] https://attack.mitre.org/groups/G0058/

[4] 2015 - https://www.clearskysec.com/thamar-reservoir/
2017 - https://www.clearskysec.com/charmingkitten/
2018 - https://www.bleepingcomputer.com/news/security/iranian-apt-poses-as-israeli-cyber-security-firm-that-exposed-its-operations/
March 2019 - https://noticeofpleadings.com/phosphorus/files/Complaint.pdf
September 2019 – https://www.clearskysec.com/the-kittens-are-back-in-town/
October 2019 - https://blogs.microsoft.com/on-the-issues/2019/10/04/recent-cyberattacks-require-us-all-to-be-vigilant/

Attack Vector

Charming Kitten keep trying to attack their victims with spear-phishing methods. We observed an escalation in the volume of phishing attempts. It can be divided into three attack platforms -

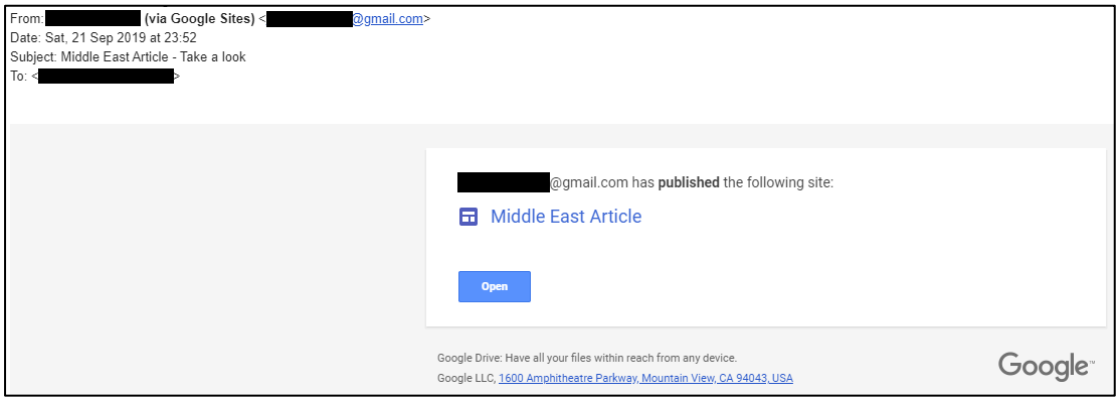
1. The first platform is sending an email message leveraging social engineering methods.
2. The second platform includes impersonation of social media websites, such as Facebook, Twitter and Instagram, as well as using these social medias to spread malicious links. Clearsky has observed a few social media entities that contacted their victims on these platforms in order to infect them via malicious websites.
3. The third platform is sending SMS messages to the cellular phone of the victim.

Impersonation Vectors

Analyzing this campaign, we identified four impersonation vectors that Charming Kitten uses in their recent attacks. Based on our investigation, Charming Kitten tried to carry out all of these vectors against the same victims, and in some cases a few of those on the same day.

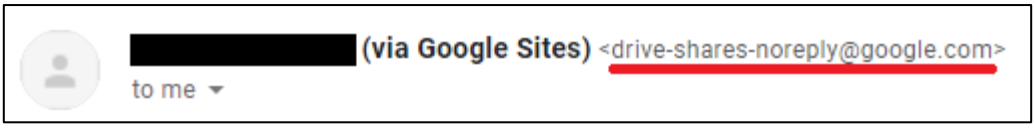
First Vector - A message with a link pretending to be Google Drive

During the first impersonation vector the attacked will receive an email with a link to Google Sites from an acquaintance; for example – a research fellow. Through this vector, the victim is tempted to download a file located at the addressing fellow's Google Sites, and thus collect the victim's Google credentials.



The phishing message that impersonated Google Drive service under the title 'Middle East Article'

The link shown above leads to a site built with the Google Sites platform. Additionally, the domain from which the link was allegedly shared is gmail.com, whereas the domain which should appear while sharing Google Sites' sites is google.com; Also, the sharing message should be sent from an address which contains 'noreply', and not the sender's address. For a **correct** sample of a Google Sites' site sharing message, see below:



*Correct Google Site's sharing message – the sender's email is **'drive-shares-noreplay@google.com'***

In another phishing case, a link to Google Drive is received, supposedly from an unknown person which claims to receive too many spam messages from the victim's address, and directs the victim to a Google Drive containing the proves to this:

Email sent allegedly from "Sandra Trentini', which is not related to any of the victims. In that case, Charming Kitten added a profile picture with 2 letters that represent the alleged sender (ST for Sandra Trentini), as part as their dissembling efforts

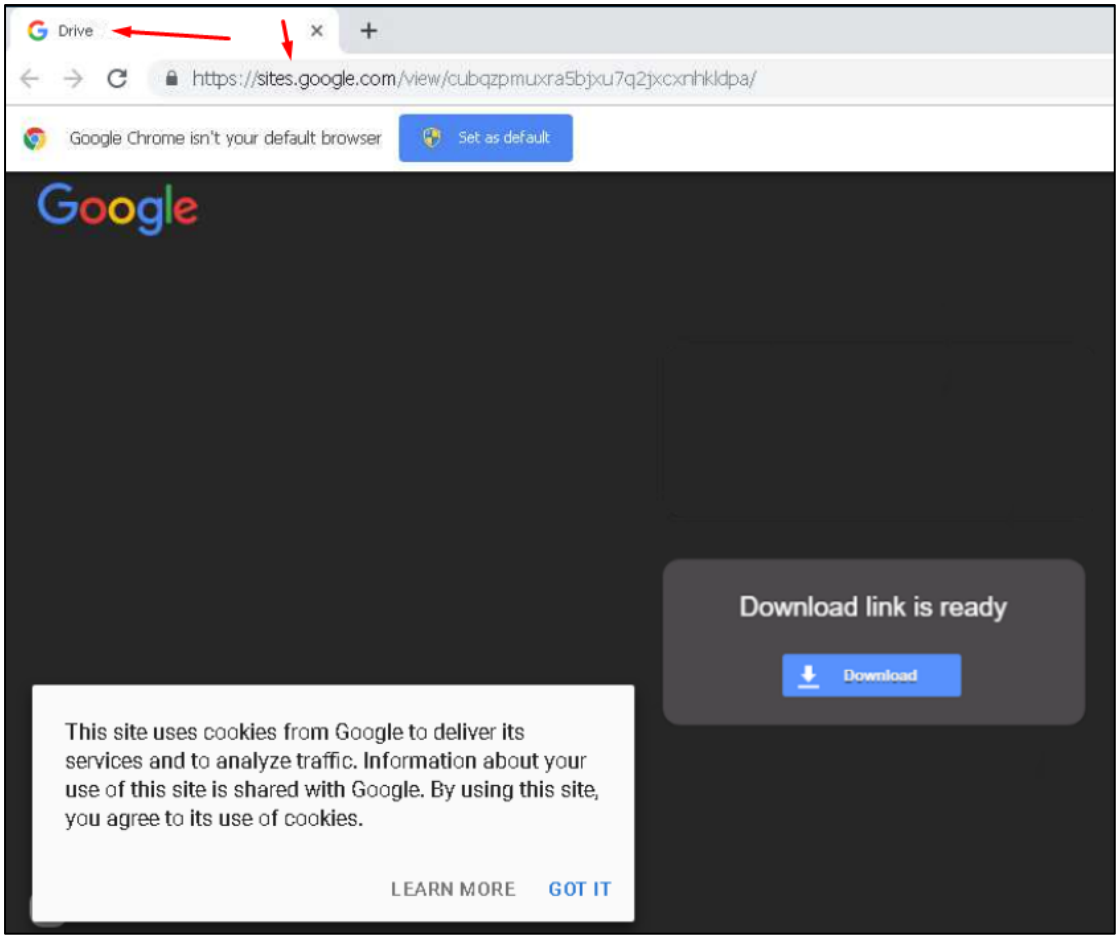
In a third case, the victim received a message from a colleague's email, personally addressing the victim to read an article this colleague is currently working on. To add credibility, the attacker also claims to have shared the research with another friend.

The links which appear in the mail lead to a dedicated Google Site, set up by the attacker; those links contain the word 'Drive', although they are Google Sites links, probably for additional camouflage:

hxxps://sites.google[.]com/view/cubqzpmuxra5bjxu7q2jxcxnhkldpa/drive/

hxxps://sites.google[.]com/screenshot-sharing-service/drive/

Yet, upon entering the site, the attackers try to manipulate the attacked to think that they are at a Google Drive site which contains a link to download the article.

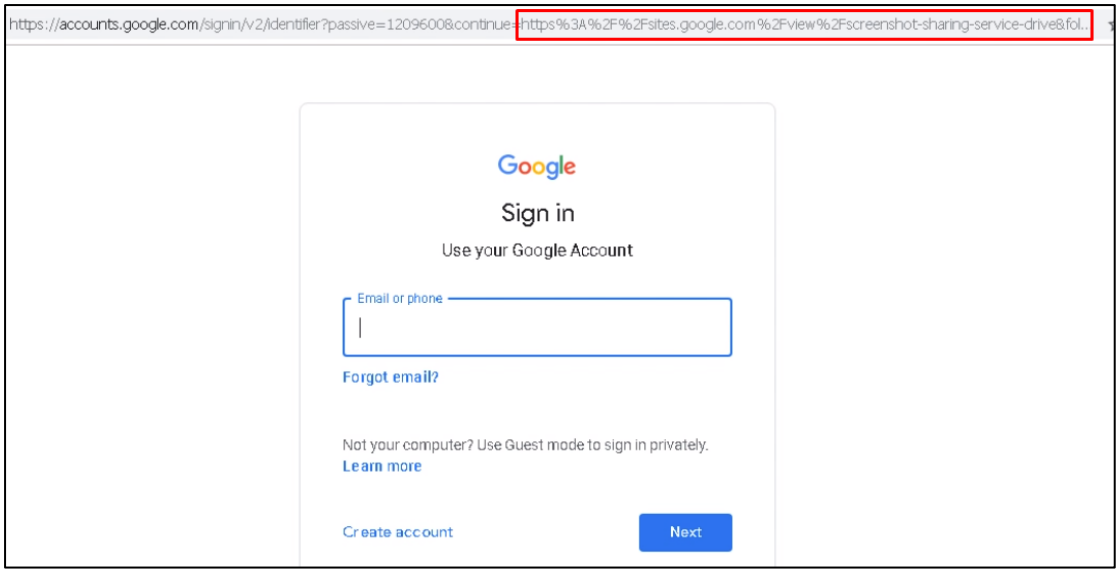


Google's Sites phishing page executed by the group. Note that the title of the site is 'Drive', which customized by the attackers.

Clicking the download link will make Google redirect to a domain shortened by a shortening service, which will not show the actual address to which the victim is taken, thus increasing camouflaging. Another important point – every page at Google Sites is unique to the attacked.

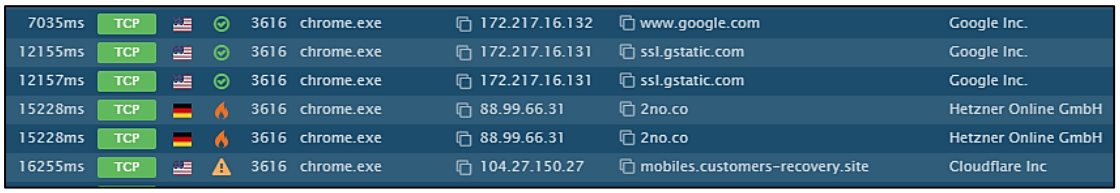
When the specific attack will end, the attackers will remove the site from the address shortening service or will redirect the address to a true email service. Here are two examples:

Attempt to enter the domain leads to the original Google site

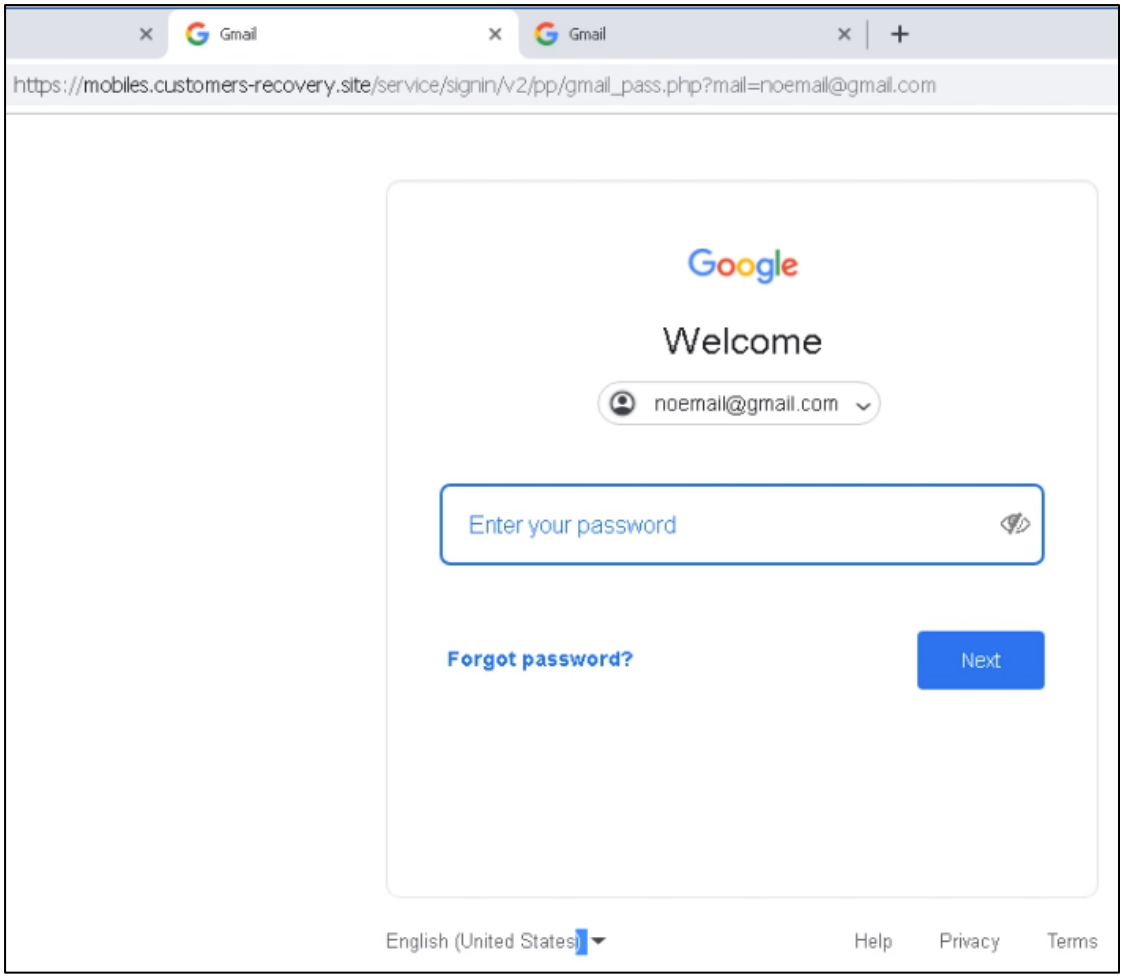


Upon an attempt to enter, a Redirect is performed to the Google Account login page, while the malicious site appears in the address line

If the attacked has opened the aforementioned link, they will be directed to the malicious site. At the present attack wave, we have identified a '.site' TLD dominance. Among the newly opened site:



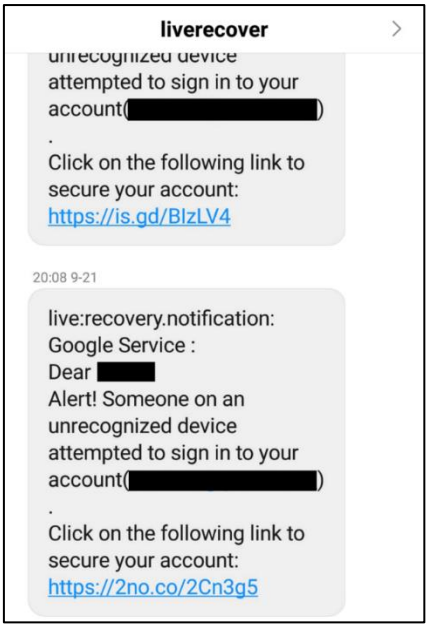
The site, which the attacked will visit, impersonates entrance to Google services. The attackers try to manipulate the victims to believe, that in order to download the file they need to log in to their Google account (for the file is allegedly from Google Drive). Another social engineering technique is to identify the Google Site from which the victim was directed and to pair the phishing page with its (the site's) email. In other words, the victim receives an email from the attacker with a link which was prepared for them personally. Identifying the attack – at the address line, the victim's email appears, and if it will be changed, the email presented at the site will change as well.



An example of a phishing site to which the victim will go. We have changed the original victim's email address to noemail@gmail.com

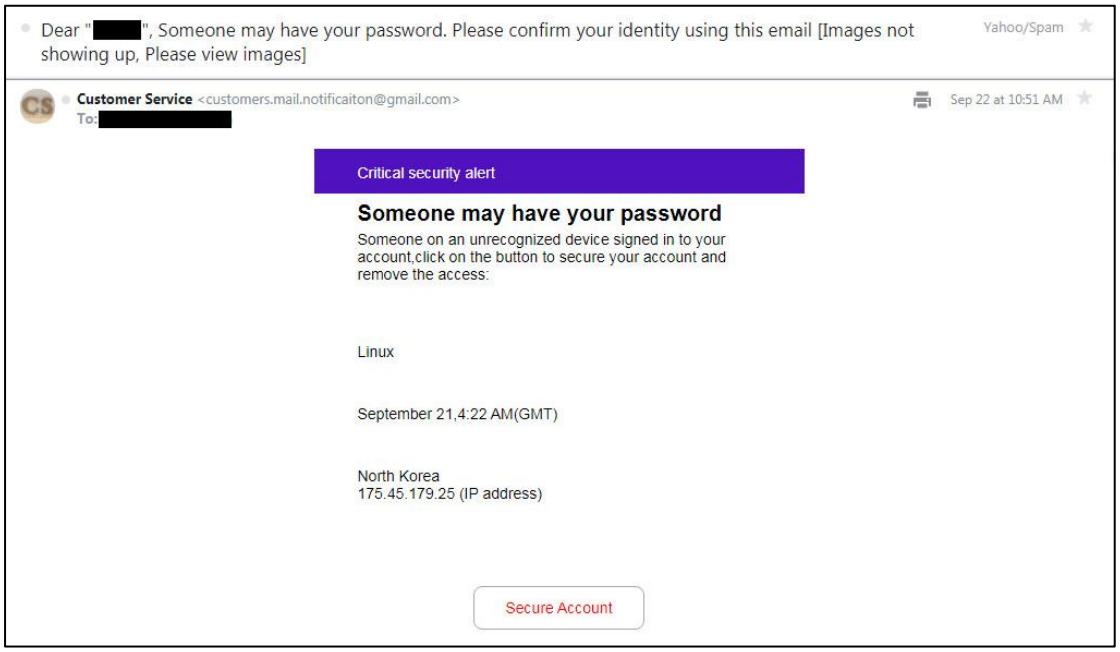
Second Vector – An SMS message

Through this vector, the victim will receive an SMS message which uses a Sender ID of 'Live Recover' and contains an alert about a stranger, who has attempted to compromise the victim's email, and the victim has to verify it through an attached link. The link will lead to the address shortening service presented earlier. Notice that the victim in the following example has received two messages with different links:



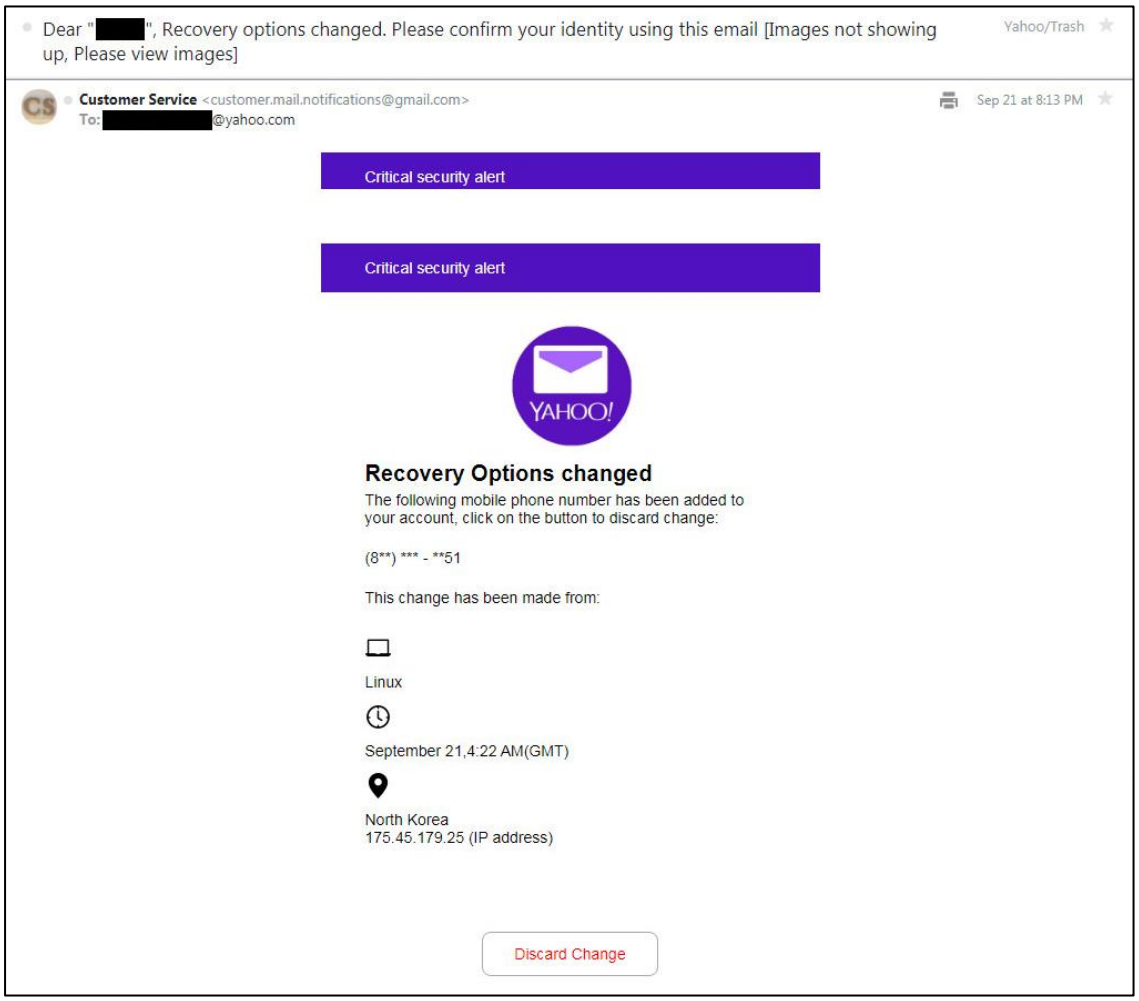
Third Vector – Login attempt alert message

The attackers try to present a sham show about a **North Korean** attacker who has attempted to compromise the victim's Yahoo mail. The message says that a person from North Korea has logged into the email of the victim. In addition, the IP address of the alleged intruder is attached to the message (the IP is indeed North Korean), and also a button which the victim is asked to push to secure their account.



The first email impersonated 'Yahoo Login Attempt' email. Note that similar to the impersonation in the first vector, this email address has a profile picture with 2 letters that represent the email sender (CS for Customer service)

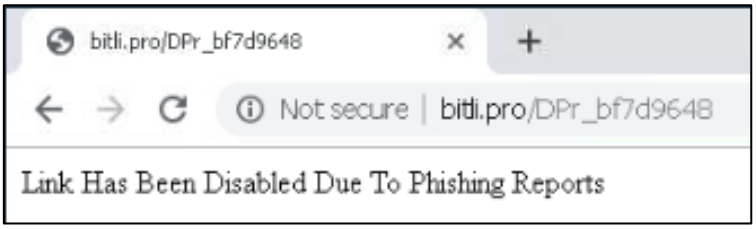
This victim has received another message earlier that day about a North Korean person which made changes to the victim's account password recovery settings, so they (the victim) have to approve those changes.



This message, like in the group's previous events, is full of errors. First, the sender's email address is a Gmail address, while the approval message pretends to be a security alert from Yahoo. Second, the sentence marked in purple – "Critical Security Alert" – appears twice. Also, the button is changed from "Discard Change" in the earlier message to "Secure Account" in the later message; the time, date, and IP stay the same. Pressing this button will lead to an address shortening service which will lead to the phishing page:

```
hxxps://bitli[.]pro/B7ZI_f56f7c3f
```

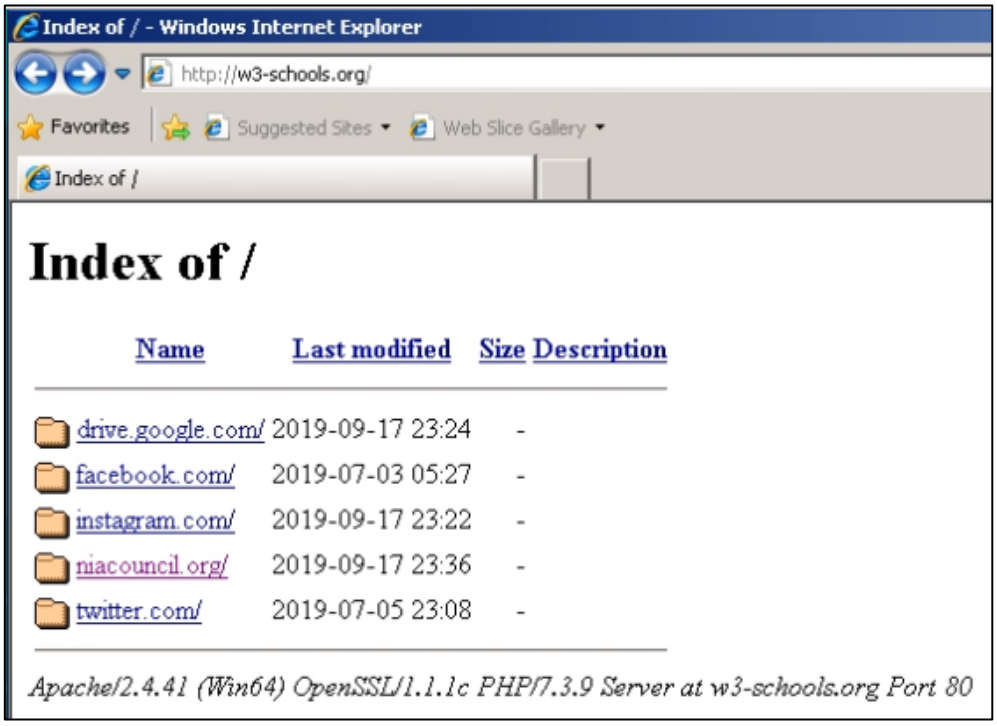
Some of the addresses we have identified in this campaign have already been blocked.



Fourth Vector – Social Networks imperonation

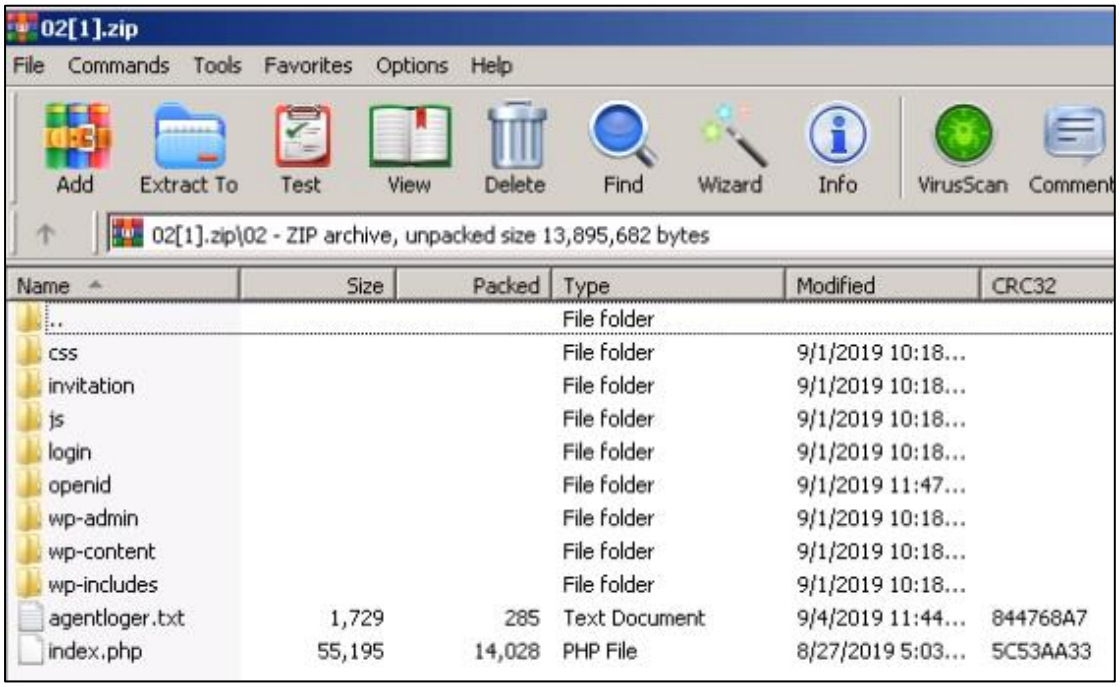
In our previous report about Charming Kitten, we have discovered that they are impersonating security teams of social networks in order to get authentication factors. Unlike the previous cases, this group has acted mostly against email boxes. In the group's activity since July-August, we have identified a shift towards social networks, such as Instagram.

As a part of our monitoring of suspicious activity, we have discovered this week that the group has built additional phishing sites, pretending to be not only Instagram but also Facebook and Twitter. In one of the sites of the infrastructure, discovered by us, w3-schools[.]org, we have found an open directory at port 80 which contains files relevant for the deployment of different phishing sites.



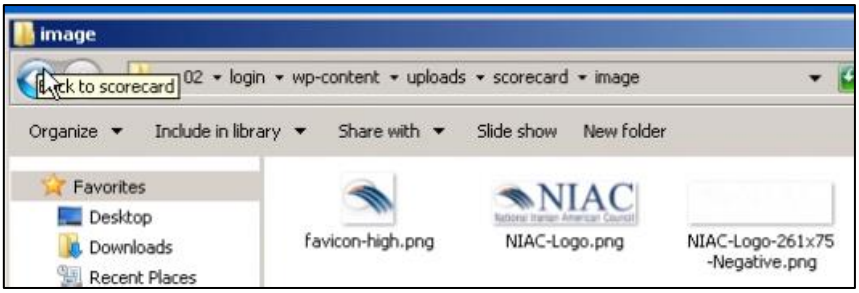
Note that the domains that are presented in the directory are related to the impersonation subject and not the malicious domain.

As seen from the picture, the first uploaded files were Facebook and Twitter impersonations. Impersonations of Instagram, Google, and the National Iranian-American Council (and Iranian organization sitting in the US), were uploaded later. At every such site directory, there is a ZIP file with a ready infrastructure for a phishing site:



As it reads from the ZIP files, the attackers prepare their phishing sites with WordPress and CrunchPress interfaces. Every folder contains relevant files, such as logos, persons to impersonate (for instance, one Nooshin Sadegh-Samimi[5], and Iranian who has joined NAIC in February 2019 and works as an organizing fellow) etc.

[5] https://www.niacouncil.org/about-niac/staff-board/nooshin-sadegh-samimi/



Digital Infrastructure

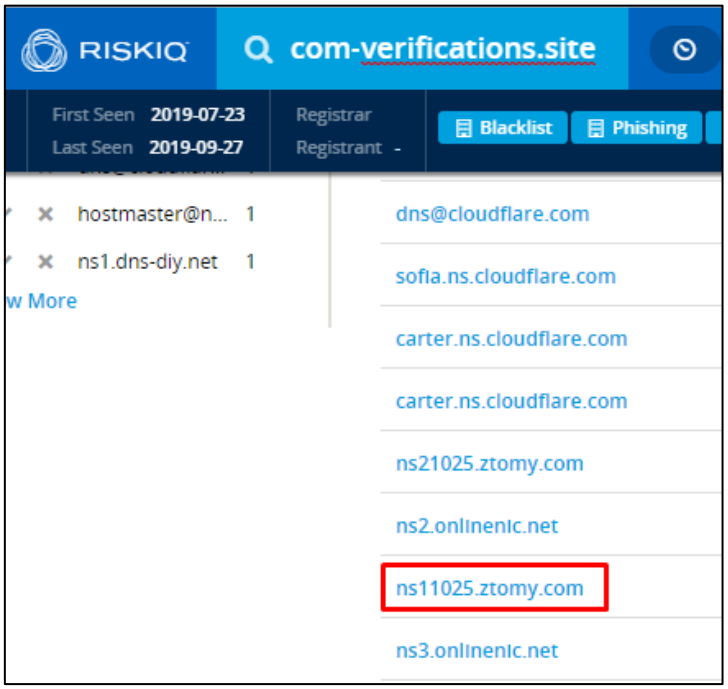
Through a pivot we have conducted on the main domain that we have identified in our research we have found more than eight new and unknown domains, all of which bear the '.site' TLD. For instance:

customers-recovery[.]site

com-verifications[.]site

com-session[.]site

Each of these domains resolves to a different IP, yet almost all of them point – through DNS research – at the same Nameserver - ns11025[.]ztomy[.]com:

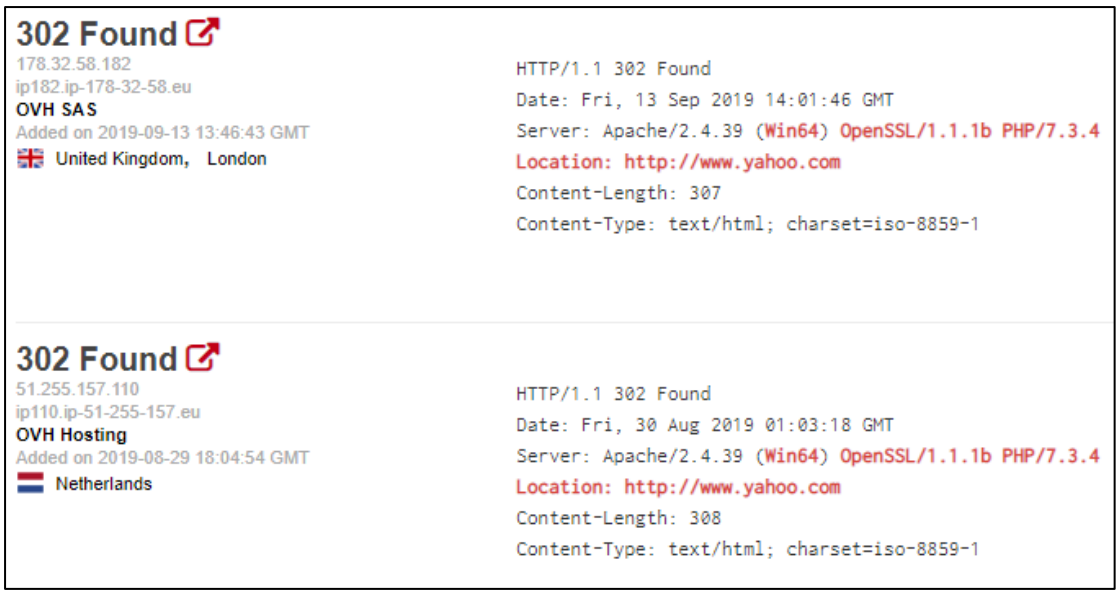


We have succeeded to identify the new domains through this Nameserver.

As we pointed out, we identified a step up in the recent campaign regarding the targeting of Yahoo accounts. The group has acted in the past, in 2017, to acquire the usernames and passwords for those accounts, yet it seems that in the recent years it has moved its focus to Google accounts. In this research, we found that the threat actor focuses again in Yahoo accounts and impersonation to Yahoo services. Below an example to an URL address of one of the group's phishing sites which depicts an impersonation to Yahoo services such as YMail.

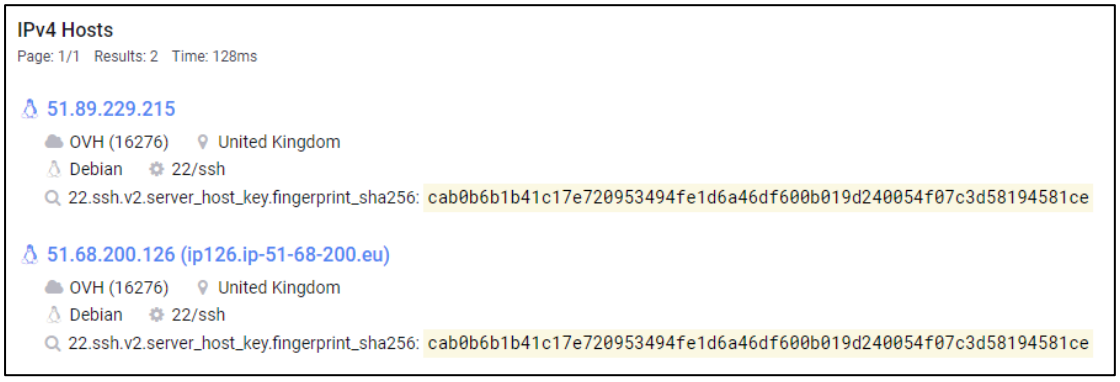
hxxps://mobiles.com-identifier[.]site/**ymail**/secureLogin/challenge/url?ucode=d105ad2b-2f7d-4193-a303-03eb32967133&service=mailservice&type=password

In our previous report we uncovered a server-registered method which in, the malicious server will redirect the client from the phishing website to the original website (HTTP 302 in port 442 or 301 in port 80). In this time too it has set its server in a way that redirects to the original Yahoo site, if a not-dedicated (i.e. specifically authorized) entrance is attempted.



A redirection to Yahoo services identified in Charming Kitten servers leveraged to impersonate Yahoo

Unlike our previous research efforts, this time we have succeeded in finding those servers before the redirect, so the 302 protocol appears as 'found'. Additionally, this time the group uses a self-signed digital certificate for its phishing sites.



As a part of Clearsky monitoring on DNS changes of suspicious and malicious infrastructure, we have identified phishing domains that impersonate Microsoft services, part of which were exposed by Microsoft[6]. On March 2019, Microsoft filed an official complaint against Phosphorus (known as Charming Kitten), which includes 99 websites targeting Microsoft users. Clearsky has been monitoring this infrastructure and identified several changes, such as new suspicious domains and new IPs.

[6] https://blogs.microsoft.com/on-the-issues/2019/03/27/new-steps-to-protect-customers-from-hacking/

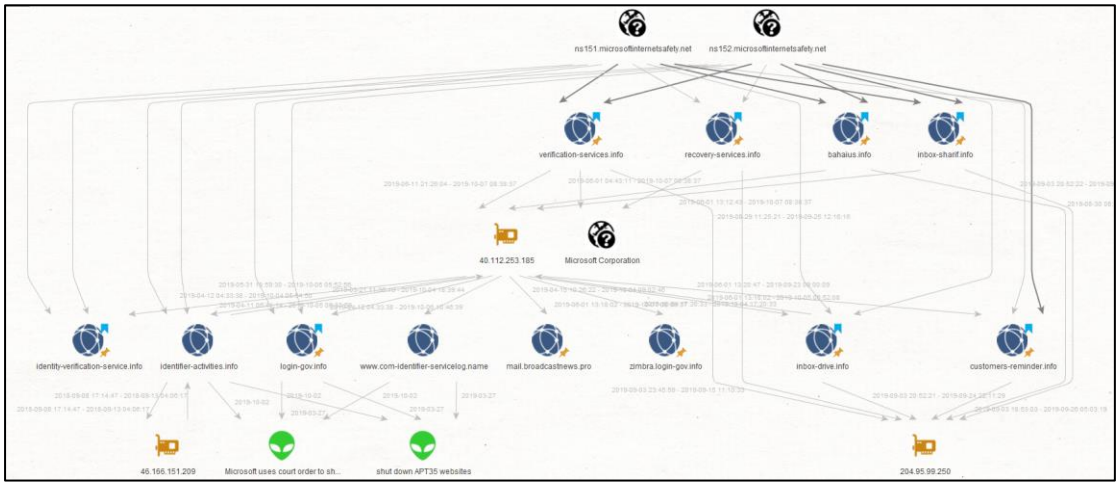
Removed records:
A:
204.95.99.250
MX:
0 mail.identifier-activities.info.

New records:
A:
40.112.253.185

All records:
A:
40.112.253.185
NS:
ns2.microsoftinternetsafety.net.
ns1.microsoftinternetsafety.net.

This photo presents one of these DNS changes within the malicious infrastructure. The domain 'identifier-activities[.]info' moved from one IP to another and the NS of it changed to the malicious NS 'ns2[.]microsoftinternetsafety[.]net'. This domain is currently resolved to the IP address 40.112.253[.]185.

Following a Maltego graph summarized the changes in the infrastructure:



This IP address currently resolves two highly suspicious domains that are attributed to the group – 'login-gov[.]info', and broadcastnews[.]pro'. We assess with a medium level of certainty that the domains may be utilized for the continuation of the campaign against governmental entities in the US, and against journalists, respectively.

Moreover, under this IP we identified the domain 'bahaius[.]info' which impersonates to the official websites of the Bahais in the United States of America, 'bahai.us'.

Indicators of Compromise

my[.]en-gb[.]home-access[.]online

notification-accountservice[.]com

recovery-services[.]info

recoverysuperuser[.]info

see-us[.]info

sessions-identifier-memberemailid[.]network

smarttradingfast[.]com

system-services[.]site

telagram[.]net

uploaddata[.]info

verification-services[.]info

40[.]112[.]253[.]185

91[.]109[.]22[.]53

136[.]243[.]195[.]229

178[.]32[.]58[.]182

185[.]177[.]59[.]240

46[.]166[.]151[.]209

51[.]68[.]200[.]126

51[.]89[.]229[.]215

51[.]255[.]157[.]110

181[.]177[.]59[.]240

bahaius[.]info

bailment[.]org

com-activities[.]site

com-identifier[.]site

com-session[.]site

com-verifications[.]site

customers-activities[.]site

customers-recovery[.]site

customers-reminder[.]info

documentsfilesharing[.]cloud

document-sharing[.]online

gomyfiles[.]info

identifier-activities[.]info

identifier-activities[.]online

identity-verification-service[.]info

inbox-drive[.]info

inbox-sharif[.]info

magic-delivery[.]info

microsoftinternetsafety[.]net

mobilecontinue[.]network

mobile-messengerplus[.]network

ClearSky Cyber Intelligence Report

Email: info@clearskysec.com
Website: clearskysec.com

CLEARSKY
Cyber Security

Ahead of the Threat Curve

Photo by 42 North on Unsplash
https://unsplash.com/photos/OE7H8Zp1mw8