Fake Interview: The New Activity of Charming Kitten

The novel phishing campaign to steal email accounts of public figures around the world

Certfa Lab · 2020.1.30

Introduction

Certfa Lab has identified a new series of phishing attacks from the Charming Kitten[1], the Iranian hacking group who has a close relationship with Iran's state and Intelligence services. According to our investigation, these new attacks have targeted journalists, political and human rights activists. These phishing attacks are in line with the previous

activities of the group that companies like ClearSky[2] and Microsoft[3] have reported in detail in September and October 2019.

As we previously reported the activities of the Charming Kitten in 2018[4], our research indicates the Charming Kitten is still trying to target private and government institutions, think tanks and academic institutions, organizations with ties to the Baha'i community, and many others in European countries, the United States, United Kingdom, Saudi Arabia, to extract information from them.

Our findings show that these new attacks by Charming Kitten are focused on stealing email account information of the victims and finding information about their contacts/networks. Also, our research shows that the group has recently participated in designing a malware for Windows machines but the spectrum and the number of its targets is still not clear for us.

Phishing via Fake Interviews

Phishing is one of the main tactics that has been used by the Charming Kitten, and social engineering and fake emails are the usual methods of executing it. In this campaign, the Charming Kitten has used the identity of a former Wall Street Journal (WSJ) journalist and created a fake interview scenario to target their victims. It must be noted that in the recent months, the group has used scenarios like "Invitation to a Deutsche Welle Webinar" and "CNN Interview" with the related topics of Iran and international affairs in order to trick their targets.

Step 1 - Gaining Trust: In one of the cases, the hackers forged the New York Times journalist Farnaz Fassihi's identity as a Wall Street Journal reporter - where she used to work - to send interview request emails to victims and guide them to their phishing websites. In the first step of the fake interview, emails were sent from farnaz.fassihi [at] gmail [dot] com to gain the victims' trust. The below image is a sample of the content.

Von: Farnaz Fassihi <farnaz.fassihi@gmail.com>
Gesendet: Dienstag, 12. November 2019 12:50
An: [redacted]
Betreff: WSJ Interview

THE WALL STREET JOURNAL.

سلام و درود خدمت [redacted]

بنده فرناز فصیحی مقاله نویس روزنامه وال استریت ژورنال هستم.
تیم خاورمیانه روزنامه وال استریت ژورنال در نظر دارد تا به معرفی افراد غیر بومی* موفق در کشورهای پیشرفته بپردازد. فعالیت های شما در حوزه مطالعات و فلسفه علم باعث شد تا شما را به عنوان یک ایرانی موفق معرفی نمایم. به دستور مدیر گروه خاورمیانه روزنامه بر آن شدیم تا با رضایت شما مصاحبه ای را ترتیب دهیم و بخشی از موفقیتهای مهم شما را سمع و نظر خوانندگان بگذاریم. این مصاحبه می تواند برای جوانان کشور عزیزمان محرکی برای کشف استعدادها و حرکت به سوی موفقیت باشد.

ناگفته نماند که این مصاحبه برای شخص بنده افتخاری بزرگ است و به همین خاطر از شما تقاضا دارم تا دعوت بنده را برای مصاحبه پذیرا باشید.

سوالات بصورت کاملا حرفه ای توسط گروهی از همکاران بنده طراحی شده است و ماحصل این مصاحبه در بخش مصاحبه هفتگی خبرگزاری وال استریت ژورنال منتشر خواهد شد. تاریخ دقیق انتشار مصاحبه نیز در روز مصاحبه مشخص خواهد شد. در صورت موافقت سوالات و ملزومات مصاحبه را برای شما ارسال خواهم کرد.

* پ.ن: منظور از غیر بومی به معنی افراد متولد شده در کشورهای دیگر می باشد.

باتشکر از لطف و توجه شما.

فرناز فصیحی

DOW JONES | THE WALL STREET JOURNAL. Read ambitiously

Figure 1. A sample of the fake interview request via an email

Translation:

*Hello *** ***** ******
My name is Farnaz Fasihi. I am a journalist at the Wall Street Journal newspaper.
The Middle East team of the WSJ intends to introduce successful non-local individuals in developed countries. Your activities in the fields of research and philosophy of science led me to introduce you as a successful Iranian. The director of the Middle East team asked us to set up an interview with you and share some of your important achievements with our audience. This interview could motivate the youth of our beloved country to discover their talents and move toward success.
Needless to say, this interview is a great honor for me personally, and I urge you to accept my invitation for the interview.
The questions are designed professionally by a group of my colleagues and the resulting interview will be published in the Weekly Interview section of the WSJ. I will send you the questions and requirements of the interview as soon as you accept.
*Footnote: Non-local refers to people who were born in other countries.
Thank you for your kindness and attention.
Farnaz Fasihi*

In these emails, all the links in the footnotes (Figure 2), including social media links, WSJ and Dow Jones websites, are all in the short URL format. As a result, by clicking on them, the hackers can guide the victim to legitimate addresses while getting basic information about the victim's device such as IP address, the type of Operating System, and the browser. This is a common method of gathering information by hackers in order to prepare for the main attacks based on the victims' devices.

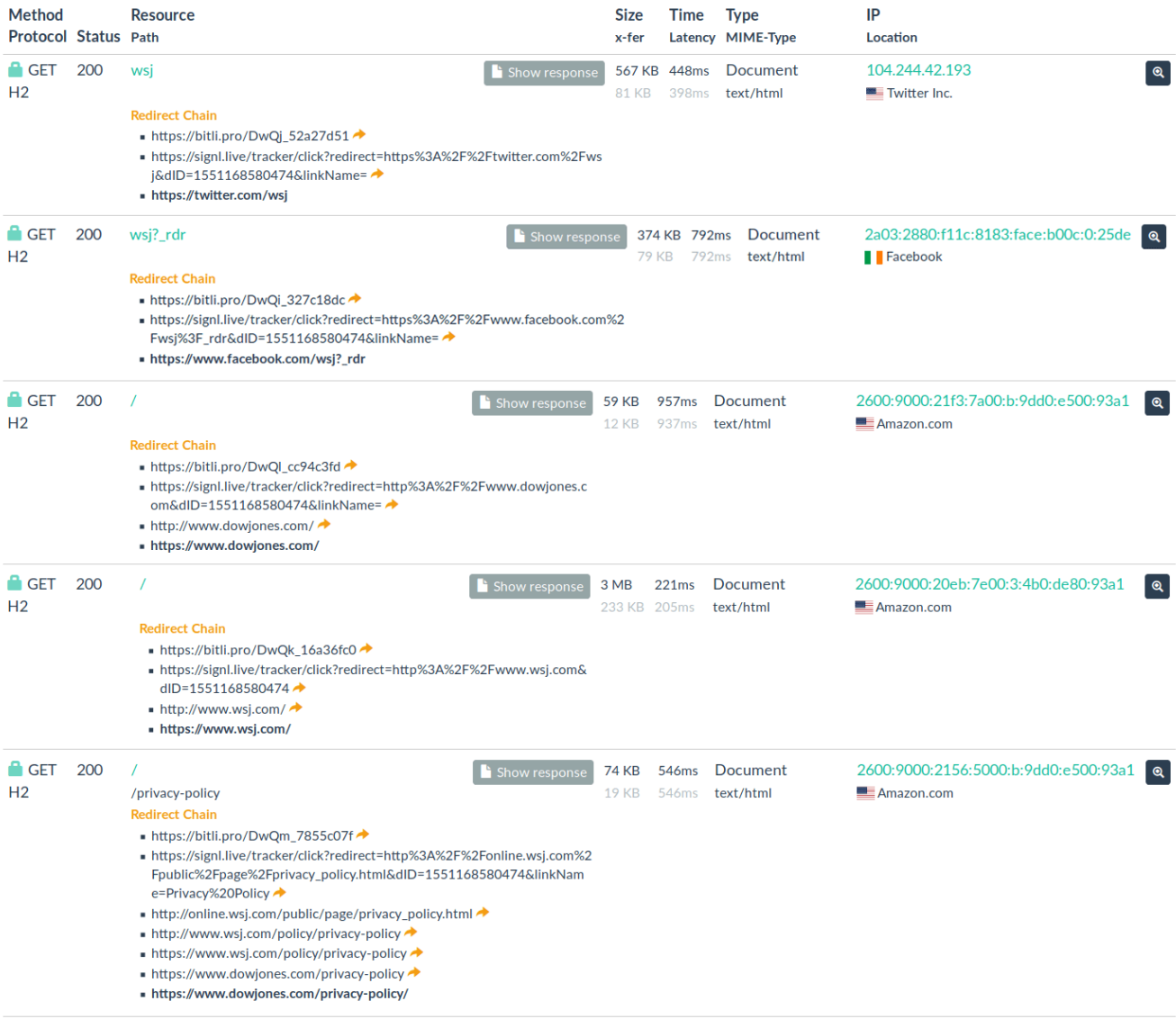

Figure 2. Details of short URL that allows hackers to collect basic information about the target[5]

Step 2, The Main Attack: After communication and relative trust are established through the initial email, hackers send their victim an exclusive link as a file that contains the interview questions. According to our samples, the Charming Kitten has been using a page that is hosted on Google Sites (Figure 3). This method is a relatively new tactic that has been widely used in phishing attacks by hackers in the past year[6] in order to make the targets trust the destination domain, for example this URL: hxxps://sites.google[.]com/view/the-wall-street/xxxx. By using this tactic, the hacker can evade the spam detections.

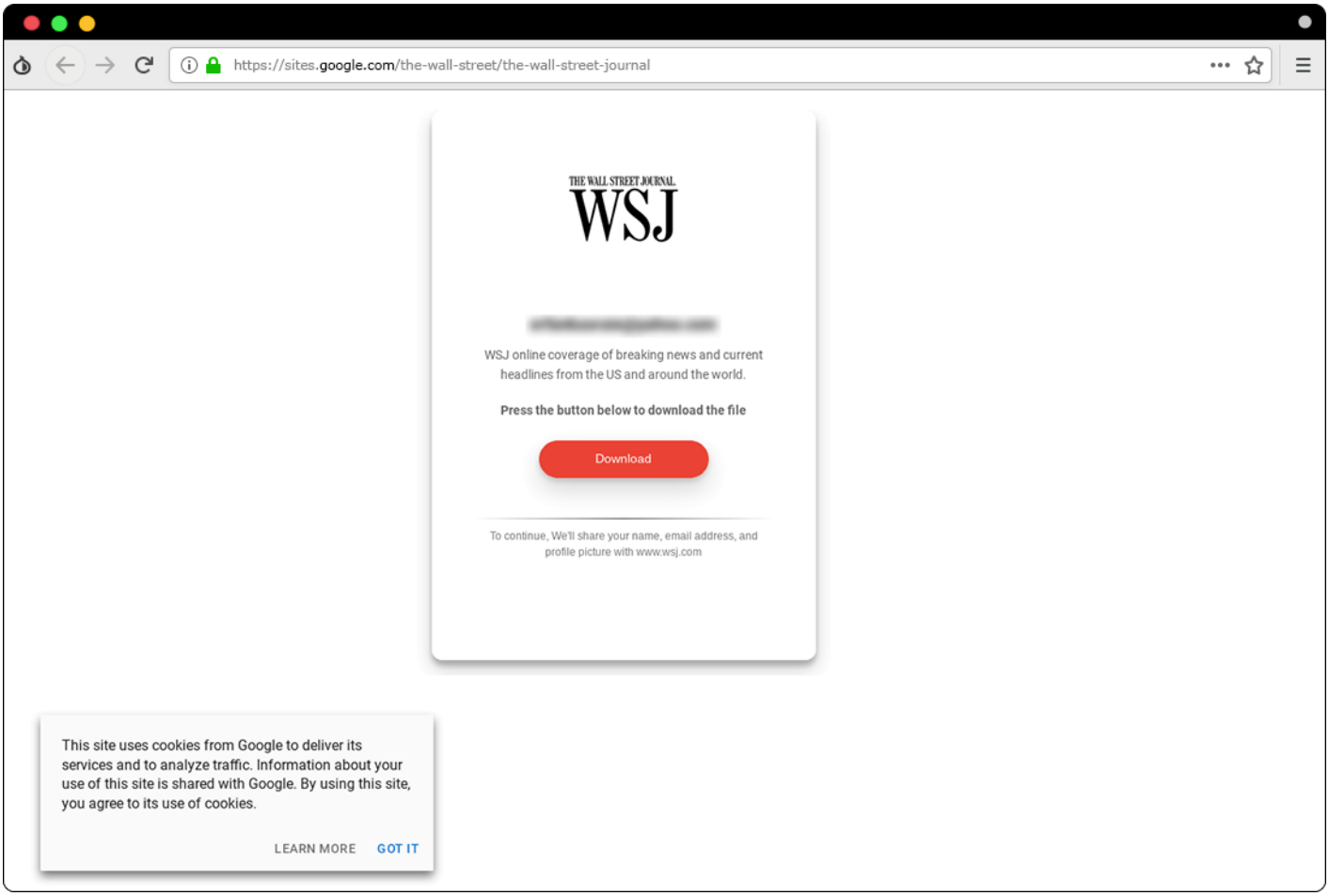

Figure 3. A sample of fake WSJ page that is hosted on Google Site.

After clicking the download button on the Google Site page (Figure 3), the target is sent to another fake page in two-step-checkup[.]site domain where login credential details of his/her email such as the password and two factor authentication (2FA) code are requested by phishing kits.

The structure of the phishing page is listed below:

- hxxps://two-step-checkup[.]site/securemail/secureLogin/challenge/url?ucode=xxxx-xxxx&service=mailservice&type=password
- hxxps://two-step-checkup[.]site/securemail/secureLogin/challenge/url?ucode=xxxx-xxxx&service=mailservice&type=smscode
- hxxps://two-step-checkup[.]site/ymail/secureLogin/challenge/url?ucode=xxxx-xxxx&service=mailservice&type=password

- hxxps://two-step-checkup[.]site/ymail/secureLogin/challenge/url?ucode=xxxx-xxxx&service=mailservice&type=smscode

Using phishing kits such as Modlishka[7] to steal passwords and two factor authentication codes is an important step in targeted attacks, which has been widely used by hackers in the past year and many reports have been written about them[8]. As mentioned, Certfa Lab published an extended report in 2018 about the Charming Kitten and their use of this method. Figure 4 is a sample of the phishing page that was used to steal the SMS authentication code.

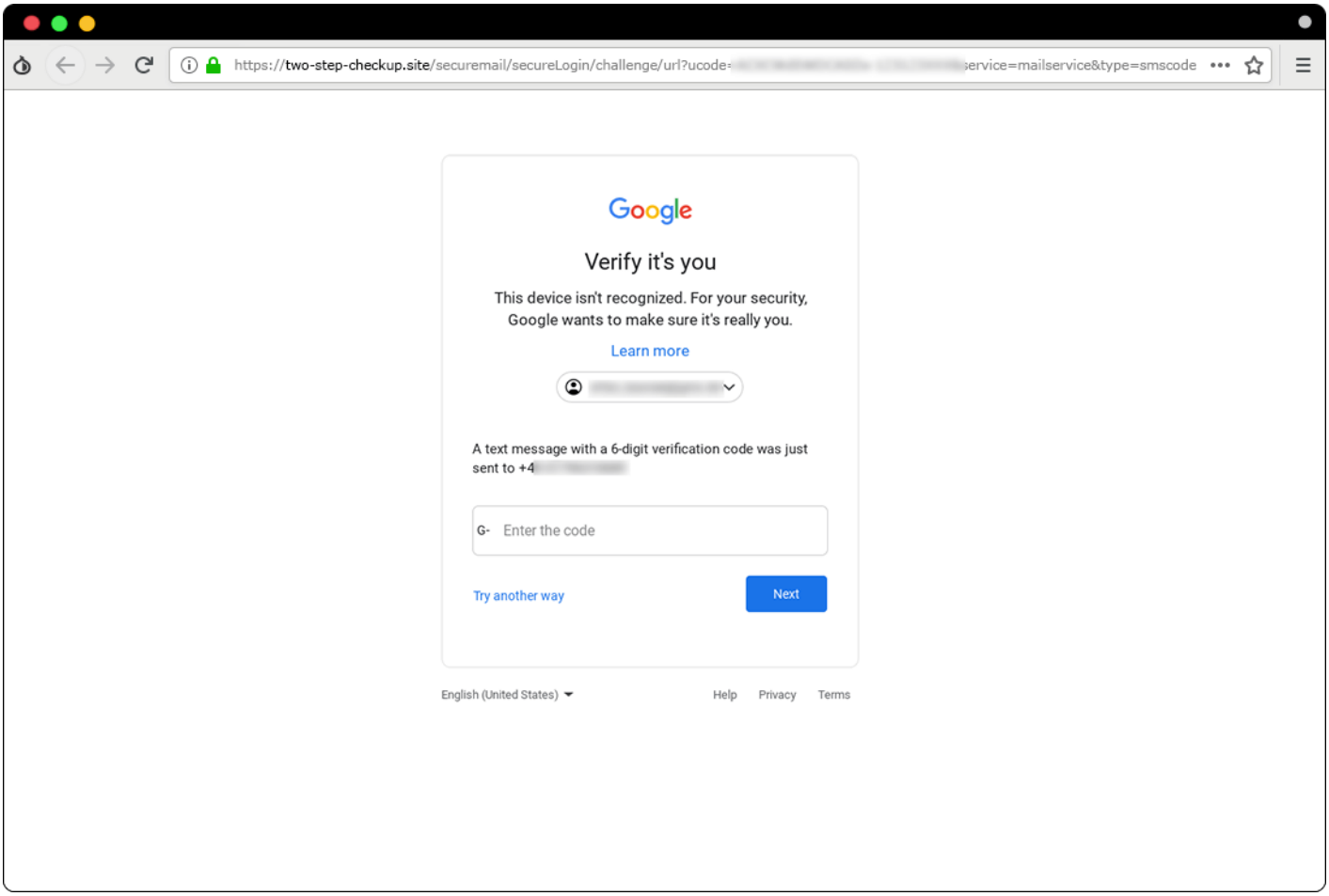

Figure 4. A sample of a phishing attack to steal 2FA code via SMS

Malware Development

One important point that caught our attention in this campaign was using “pdfreader.exe”, a piece of malware with a backdoor feature. Our investigation shows this file was first uploaded in VirusTotal by an anonymous user on 3 October 2019[9].

The technical assessment of the malware’s function shows that the developers of malware are directly in contact with the people behind the recent phishing attacks, and it could be interpreted as all these malicious activities being done by one group, which we believe to be the Charming Kitten.

pdfReader.exe Function: This malware, which is identified as a Win32/Backdoor by antiviruses, is a mid-level piece of malware - due to lack of design sophistication - with various harmful capabilities. Our assessment shows the malware causes changes in the Windows’ Firewall and Registry settings in order to run automatically itself and gathers information from the victim’s device and sends it to its developer. This feature allows the hackers to run new malware and spyware remotely on the victim’s target. Figure 5 shows the process graph of this malware.

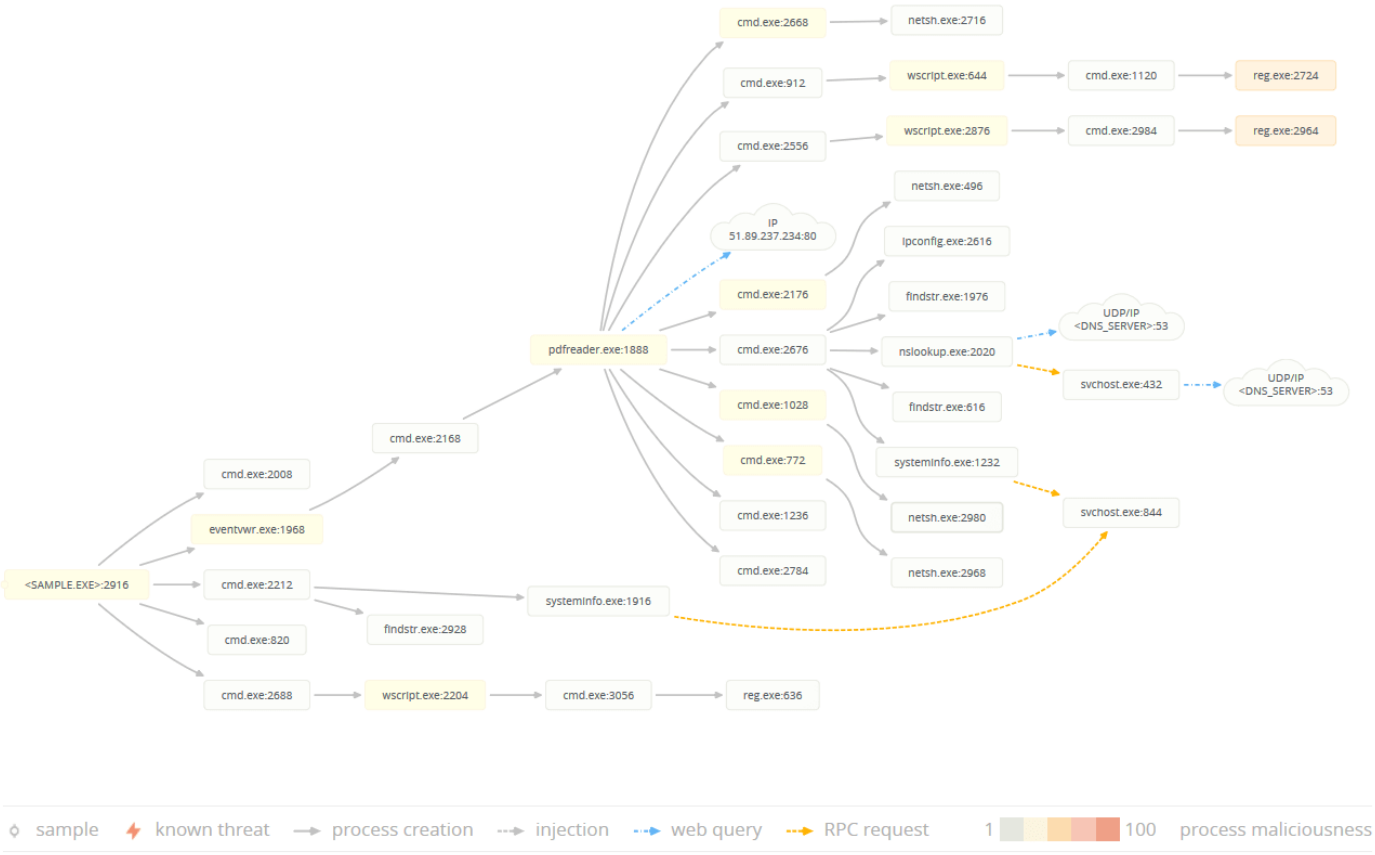

Figure 5. The process graph of pdfReader.exe

pdfReader.exe Connections: A noteworthy point about this malware is its connection and interaction with 51.89.237.234 on port 80. Before its original version was uploaded on VirusTotal on 03 October 2019 11:00:25GMT, pdfreader.exe was submitted on VirusTotal as a pdfreader.zip four hours earlier, on 3 October 2019 07:14:22GMT, which can be seen in the IP history 51.89.237.233 (Figure 6). Also, the server with IP address of 51.89.237.234 is used to host “software-updating-managers[.]site” and “malcolmrifkind[.]site”.

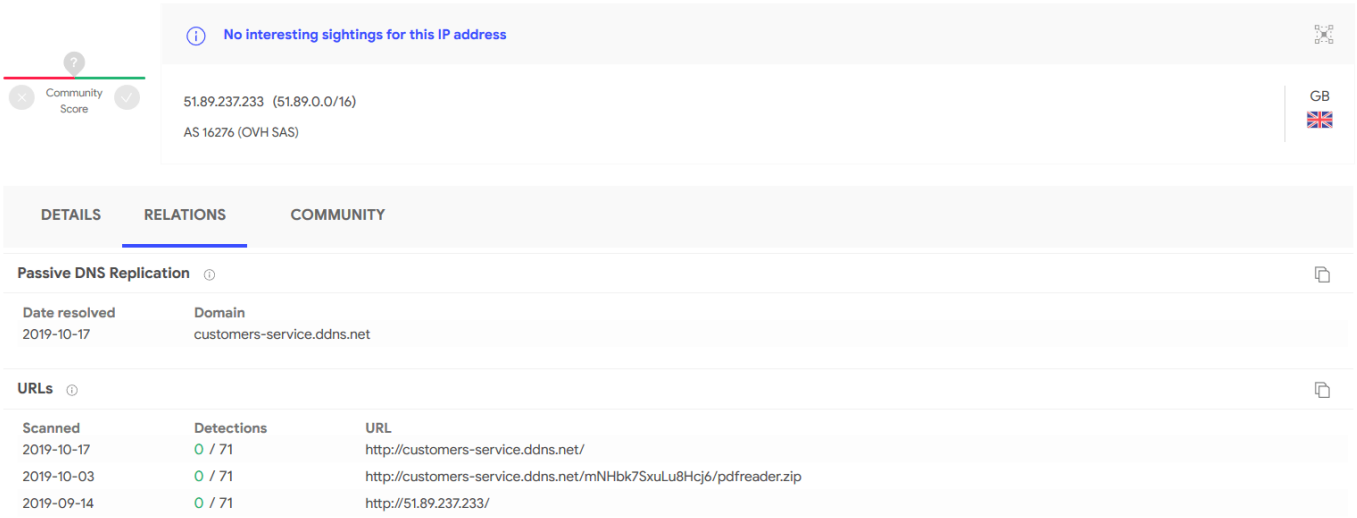

Figure 6. IP history of 51.89.237.233 on VirusTotal

Charming Kitten’s Footprints

Our research on the history of phishing websites in recent attacks, such as two-step-checkup[.]site, shows the attackers use “ns11025.ztomy[.]com” and “ns21025.ztomy[.]com” as the Name Servers (NS) on 14 October 2019. These servers were previously used for other phishing websites by the Charming Kitten.

The similarities between the method of managing and sending HTTP requests in “two-step-checkup[.]site” server with the latest techniques used by this group is further

evidence of Charming Kitten's connection to these attacks. In this technique, if sent requests to the host server of the phishing kit are denied, the user is directed to a legitimate website like Google, Yahoo!, or Outlook by "301 Moved Permanently" and "Found redirect 302" responses. As a result, this method makes it harder for different pages and sections of phishing websites to be exposed to the public.

Figure 7 is a sample of public requests from "two-step-checkup[.]site" that has been redirected to outlook.live.com. In this scenario, the user does not have a valid request according the phishing kit, therefore, the real webpage - not the phishing one - is shown to the target.

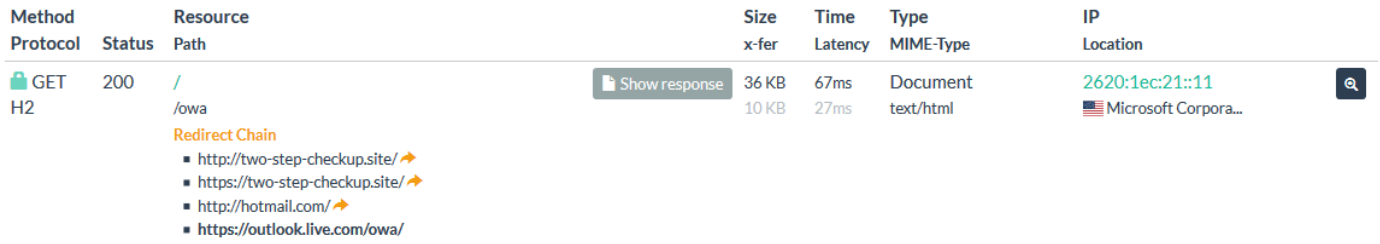

Figure 7. Management and redirecting invalid request on two-step-checkup[.]site[10]

Another noteworthy point about the footprints of the Charming Kitten in this campaign is the similar settings that have been used for servers. Our research shows that in the second half of 2019, most servers used by the Charming Kitten were based on Windows machines and OpenSSL, PHP, Apache, and Microsoft-HTTP API or similar versions. Although this point is not enough to prove this claim, the default settings in response to HTTP requests can be the group's footprint. A few examples are listed below.

Apache httpd 2.4.39 51.89.237.234

```
HTTP/1.1 302 Found
Date: Tue, 12 Nov 2019 23:57:53 GMT
Server: Apache/2.4.39 (Win64) OpenSSL/1.1.1b PHP/7.3.4
Location: http://www.yahoo.com
Content-Length: 307
Content-Type: text/html; charset=iso-8859-1
```

Apache httpd 2.4.39 51.89.237.235

```
HTTP/1.1 302 Found
Date: Tue, 01 Oct 2019 10:22:33 GMT
Server: Apache/2.4.39 (Win64) OpenSSL/1.1.1b PHP/7.3.4
Location: http://www.yahoo.com
Content-Length: 307
Content-Type: text/html; charset=iso-8859-1
```

Apache httpd 2.4.39 51.68.200.126

```
HTTP/1.1 302 Found
Date: Tue, 06 Aug 2019 15:08:02 GMT
Server: Apache/2.4.39 (Win64) OpenSSL/1.1.1b PHP/7.3.4
Location: http://www.yahoo.com
Content-Length: 307
Content-Type: text/html; charset=iso-8859-1
```

Apache httpd 2.4.39 185.141.63.135

```
HTTP/1.1 302 Found
Date: Tue, 16 Jul 2019 08:26:06 GMT
Server: Apache/2.4.39 (Win64) OpenSSL/1.1.1b PHP/7.3.5
X-Powered-By: PHP/7.3.5
location: http://leslettrespersanes.fr
Content-Length: 3
Content-Type: text/html; charset=UTF-8
```

The Range of Attacks

Assessments of the network infrastructure that was used in these attacks shows the Charming Kitten uses a variety of servers and domains to trap its targets. Some of these servers and domains are related to the recent attacks and some occurred during the second half of 2019. Table 1 lists the latest domains and IPs of the Charming Kitten and Table 2 lists the related domains and IPs.

Servers	New Domains	Scope and Purpose
51.38.87[.]199	finance-usbnc[.]info	Baha'i Center Assistance (finance@usbnc.org)
51.38.87[.]199	service-activity-checkup[.]site	Google
Current IP: 51.38.87[.]199 Previous IP: 51.89.237[.]235	two-step-checkup[.]site	Yahoo!, Google and Outlook
51.89.237[.]235	service-issues[.]site	Yahoo!, Google and Outlook
51.89.237[.]235	phonechallenges-submit[.]site	Yahoo!, Google and Outlook
51.89.237[.]234	malcolmrifkind[.]site	Sir Malcolm Rifkind (Chairman of the Intelligence and Security Committee UK) malcolmrifkind.com email
51.89.237[.]234	Software-updating-managers[.]site	Malware C&C
51.89.237[.]233	customers-service.ddns[.]net	Malware C&C
---	yah00[.]site	Yahoo
---	cpanel-services[.]site	Hosting Cpanel
---	instagram-com[.]site	Instagram
---	recovery-options[.]site	Yahoo!, Google and Outlook

Table 1. List of latest domains and IPs of the Charming Kitten

Servers	New Domains	Scope and Purpose
185.141.63[.]8	Skynevvs[.]com	Sky News Skynews.com
185.141.63[.]135	Leslettrespersanes[.]net	Les lettres persanes (Iranian news website in French) leslettrespersanes.fr
185.141.63[.]135	Inztaqram[.]ga	Instagram
185.141.63[.]156	niaconucil[.]org	NIAC (National Iranian American Council) niacouncil.org
185.141.63[.]157	drive-accounts[.]com	Google drive
185.141.63[.]160	unirsd[.]com	UNRISD (United Nation Research Institute for Social Development) unrisd.org
185.141.63[.]162	isis-online[.]net	ISIS (Institute for Science and International Security) isis-online.org
185.141.63[.]170	accounts-drive[.]com	Google drive
185.141.63[.]170	w3-schools[.]org	W3Schools w3schools.com
185.141.63[.]172	Seisolarpros[.]org	SEI Professional Services seisolarpros.com
---	bahaius[.]info	official websites of the Bahais in the United States Bahai.us
185.141.63[.]161	acconut-verify[.]com	Google Account Verification
51.255.157[.]110	customers-activities[.]site	Gmail, Outlook
51.255.157[.]110	system-services[.]site	---

Table 2. List of related domains and IPs of the Charming Kitten[11]

Conclusion

This new series of phishing attacks by the Charming Kitten are in line with previous activities seen from their group. For example, we identified similar settings for the servers used in this attack with their previous campaigns.

The main focus of this phishing campaign was stealing email account information of the victims, and finding information about their contacts/networks. One example detailed in this report is there impersonation of public figures such as a WSJ reporter.

The Charming Kitten used Google Sites for their phishing attack, and Certfa believes that they work on the development of a series of malware for their future phishing attack campaign.

IOCs

- 51.38.87[.]199
- 51.89.237[.]235
- 51.89.237[.]233
- 51.89.237[.]234
- 51.255.157[.]110
- 185.141.63[.]8
- 185.141.63[.]135
- 185.141.63[.]156
- 185.141.63[.]157
- 185.141.63[.]160
- 185.141.63[.]161
- 185.141.63[.]162
- 185.141.63[.]170
- 185.141.63[.]172
- finance-usbnc[.]info
- service-activity-checkup[.]site
- two-step-checkup[.]site
- service-issues[.]site
- phonechallenges-submit[.]site
- malcolmrifkind[.]site

- software-updating-managers[.]site
- customers-service.ddns[.]net
- yah00[.]site
- cpanel-services[.]site
- instagram-com[.]site
- recovery-options[.]site
- skynevvs[.]com
- leslettrespersanes[.]net
- inztaqram[.]ga
- niaconucil[.]org
- drive-accounts[.]com
- unirsd[.]com
- isis-online[.]net
- accounts-drive[.]com
- w3-schools[.]org
- seisolarpros[.]org
- bahaius[.]info
- acconut-verify[.]com
- customers-activities[.]site
- system-services[.]site
- 3d67ce57aab4f7f917cf87c724ed7dab
- 542128ab98bda5ea139b169200a50bce

Footnotes:

1. Mitre, “Charming Kitten”. Accessed December 17, 2019. https://s.certfa.com/pccOGX ⇆
2. ClearSky Cyber Security (2019), “The Kittens Are Back in Town Charming Kitten – Campaign Against Academic Researchers”. Accessed December 10, 2019. https://s.certfa.com/JPUSoz
   ClearSky Cyber Security (2019), “The Kittens Are Back in Town 2 – Charming Kitten Campaign Keeps Going on, Using New Impersonation Methods”. Accessed December 10, 2019. https://s.certfa.com/z0NdFI ⇆

3. Microsoft (2019), “Recent cyberattacks require us all to be vigilant”. Accessed December 16, 2019. https://s.certfa.com/II3VLH ⇆
4. Certfa Lab (2019). “The Return of The Charming Kitten”. Accessed December 12, 2019. https://s.certfa.com/i8Ad16 ⇆
5. URLScan.io, “A Shorten link sample to collect basic info of victims”. Accessed December 16, 2019. https://s.certfa.com/x8IsaI ⇆
6. Certfa Lab (2019). “Weaponizing of Google Cloud Storage for phishing attacks”. Accessed December 16, 2019. https://s.certfa.com/5myHcV ⇆
7. Latest Hacking News (2019). “Modlishka – The Tool That Can Bypass Two-Factor Authentication Via Phishing”. Accessed December 17, 2019. https://s.certfa.com/iIJQbl ⇆
8. Certfa Lab (2019). “The Return of The Charming Kitten”. Accessed December 12, 2019. https://s.certfa.com/i8Ad16 ⇆
9. First Submission of the sample on VirusTotal on 3 October 2019 at 11:00 GMT. Accessed December 12, 2019. https://s.certfa.com/hZxpoH ⇆
10. URLScan.io, “Redirecting invalid request on two-step-checkup[.]site”. Accessed December 16, 2019. https://s.certfa.com/oPa1mY ⇆
11. ClearSky Cyber Security (2019), “The Kittens Are Back in Town Charming Kitten – Campaign Against Academic Researchers”. Accessed December 10, 2019. https://s.certfa.com/JPUSoz
    ClearSky Cyber Security (2019), “The Kittens Are Back in Town 2 – Charming Kitten Campaign Keeps Going on, Using New Impersonation Methods”. Accessed December 10, 2019. https://s.certfa.com/z0NdFI ⇆

Charming Kitten APT Iran Phishing