

FLYING KITTEN TO ROCKET KITTEN, A CASE OF AMBIGUITY AND SHARE

PUBLIC NOTICE (5 DECEMBER 2017)

BACKGROUND

In our most recent post, ["iKittens: Iranian Actor Resurfaces with Malware for Mac"](#), the inadvertent disclosure of macOS Keychains from a long dormant group through references to an alias "mb_1986" (a hacker named Mojtaba Borhani that we have tracked since at least April) more generalizable theme: the ecosystem of Iranian actors is chaotic and ever-changing, making disambiguating different campaigns and actors. The reference to Mojtaba isn't the only call back to previous groups that we have come across in our time monitoring Iranian actors.

One of the first reports to systematically describe Iranian intrusion campaigns as persistent threat actors was FireEye's ["Operation Saffron"](#) espionage operation targeting the defense sector through malware. Later labeled "Flying Kitten," the group had engaged in extensive surveillance of domestic dissidents. Flying Kitten was prolific at spearphishing account credentials, targeting at least hundreds of individuals over more than a year before the June 2013 Presidential election. The tactics and infrastructure involved in these campaigns evolved over time, but kept to basic tactics of social engineering and platform providers about account security. The use of the "Stealer" described by FireEye was also much more extensive than previously disclosed. When the report was released in May 2014, the domains and servers connected with the group were taken down or lapsed, not to be used again. We later surfaced that summer that were potentially connected to the group, by most accounts Flying Kitten ceased to exist.

Five months later, in September 2014, ClearSky published a blog post ["Gholee – a "protective edge" themed spear phishing campaign"](#) that described attacks originating out of Iran. As these campaigns continued, they were attributed to a group labeled "Rocket Kitten." The infrastructure and tactics of these campaigns represent a visible break from Flying Kitten with the domains connected to Rocket Kitten largely registered after July 2014. From these espionage campaigns were also directed against Iranian activists. The lull in intrusion attempts against these communities after Flying Kitten's activity months, until an Iranian journalist received notifications purporting to be from Google claiming that their accounts had been accessed from a predecessor, while the publications shaped Rocket Kitten's behavior, it did not end the campaigns.

The case of mb_1986 is not the first time that researchers have seen similarities in supposedly different Iranian groups. Check Point notes ["Rocket Kitten: A Campaign With 9 Lives"](#) that the Rocket Kitten group maintained a "very similar mode of operation and phishing domain" but noted a lack of concrete evidence to link the two. In this post, we document two recent disclosures of attacker-developed infrastructure for both Flying Kitten and Rocket Kitten. While we cannot assert that the groups are the same, we can establish that there was direct exchanges of information and an overlap in membership.

CASE 1: PHISHING INFRASTRUCTURE

The commonalities between externally-visible components of the attacks conducted by both Flying Kitten and Rocket Kitten are notable. One example is a domain naming scheme, for example Drive-Google.com.co (created April 2014, connected to Flying Kitten) compared to Drive-Google.com.co (connected to Rocket Kitten). A comparison of the content of credential theft attempts adds more suspicion about a relationship. However, without more information, these are weak indicators, and could as easily suggest that members learned from the FireEye report. Through the disclosure of spearphishing, we demonstrate that these commonalities are more than superficial – that Rocket Kitten has used Flying Kitten tools for credential theft.

IRAN THREATS

researchers were able to observe a year’s worth of phishing attempts, starting in August 2014. Screenshots from the database show some often following a schema of:

```
http://profiles.google.com.inc.gs/?_schema=([0-9]+)&rnd=([0-9]+)
```

This parallels first-hand observation of attempts against Iranian journalists during September and October 2014. The pattern also provides evidence of Rocket Kitten attacks. However, the tactics and tools in phishing campaigns attributed to Rocket Kitten were not homogenous, even at the same time. For example, the spearphishing attempts we have observed occurred at the start of August 2014, and a different pattern in the URLs of phishing sites is apparent.

```
http://account-google.co/EditPassd?pli=([A-Z0-9]+)
http://drive-google.co/Check?pli=([A-Z0-9]+)
```

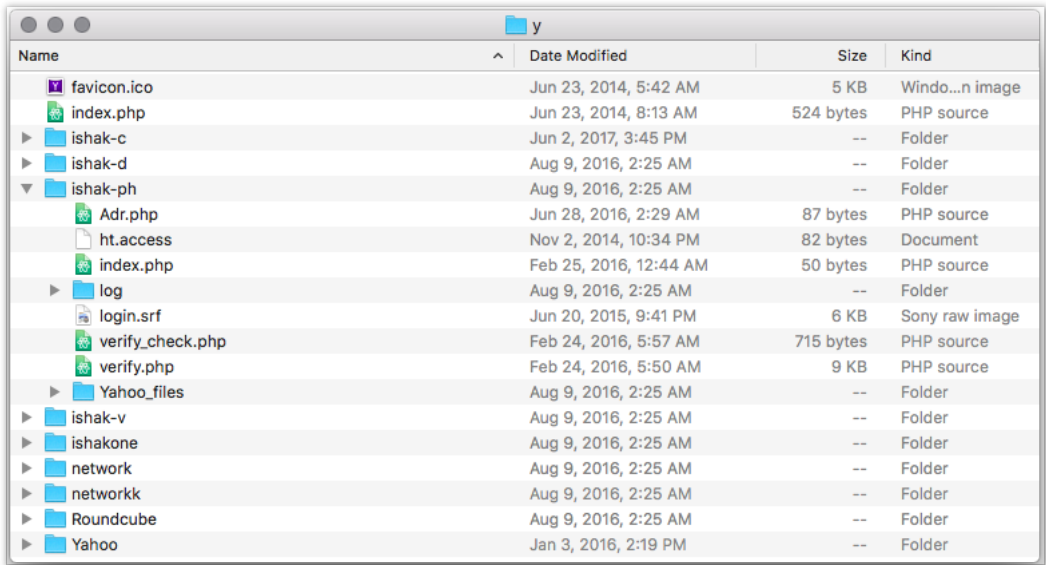
ClearSky notes these domains in its ["Thamar Reservoir" report](#), despite the different parameter schema. On face value, this would not entirely rule out the possibility of their being two different phishing toolkits.

The August 2014 attempts have more similarities with Flying Kitten attempts than Check Point’s Rocket Kitten. The same parameter schema was used in a message that "hackers recently want to hijack your account," conducted by Flying Kitten:

```
http://accounts.privacy-google.com/EditPassd?pli=([A-Z0-9]+)&Service=mail&TTL=True
```

There are many other tactical and stylistic differences between these "Rocket Kitten" attempts, including meaningful differences in templates. Whereas Rocket Kitten had registered Gmail accounts that appeared to be official (e.g. "accountr.noreply" and "team.mail.secure"), both Flying Kitten and Rocket Kitten messages used compromised sites to relay messages spoofed to appear as Google (e.g. "Services-Team@accounts.google.com"). Aside from the differences in templates, both of the latter sets of messages shared common grammatical failures, focused on common targets, and used similar social engineering tactics.

Despite these differences in tools and behaviors, the seemingly distinct patterns are commonly lumped in as "Rocket Kitten."



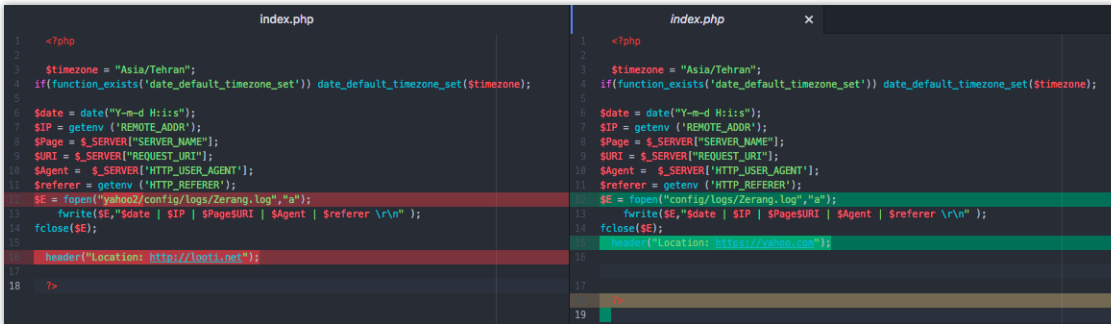
codebase as "Ishak" – reflecting the naming of the folders in the archive.

What was immediately striking is how closely the Ishak source code resembled previously obtained copies of Flying Kitten’s Hotmail, Yahoo most basic level, the folder that contained victims’ passwords and other logs controlled external access with the same .htpasswd entry:

```
admin:$apr1$.M.6gO9b$HKm8rKGouMsesWMq14QsG/
```

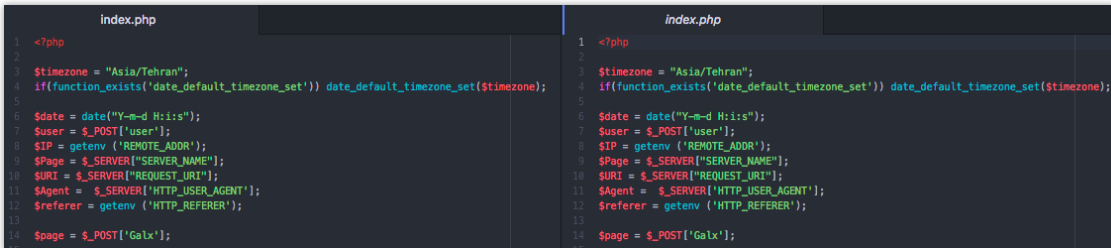
The differences extend further into the code. The earliest file creation date in the Ishak codebase was December 2012 – a file named "all. back the visitor’s IP address. This exact file also present in in the Flying Kitten codebase. Still other files and folders have the same structu "Zerang.log" ("clever"). Both have blocked roughly the same sets of IP addresses through the Apache .htaccess file (mostly search engine researchers as well).

While the codebases are not the same, there are substantial similarities elsewhere, especially in components that would not require updat the user interfaces of the sites they mimic. For example, in the page that logs unexpected attempts to access the site (such as expired c change was to push users to the Yahoo! homepage rather than a Persian-language pornographic site (the latter which was common acro



Flying Kitten, November 2013 (xn--facebook-06k.com)

Rocket Kitten, August 2016 (yahoo-reset.signi



Flying Kitten, March 2014 (drive.yahoomail.com.co)

Rocket Kitten, August 2016 (yahoo-drive.signi

The Ishak scripts are substantially different from the Oyun spearphishing platform that Check Point documented. Tthe latter of which uses a database to store the target information that populates the phishing page. Instead, both the Flying Kitten and Ishak toolkits are more simple – victim identifiers are stored as an array in a file that is essentially a phone book for the platform. The victim identifiers appear to be manually set, which explains why in-the-wild attacks sometimes appeared with victim IDs as non-random, "asdf"-style sequences of characters, or target names – instead of Oyun’s number-based identifier.

Ishak was almost certainly used in-the-wild in attacks attributed to Rocket Kitten. The difference in parameter schemas provides indicatio used in attacks documented by others in 2015, as the difference in URLs for those sites resembles Ishak’s approach rather the Oyun.

IRAN THREATS

[Home](#)

Oyun (e.g. profiles.google.com.inc.gs in September 2014): `/?_schema=([0-9]+)&rnd=([0-9]+)`

Ishak (e.g. user-setting.com in March 2015): `/Drive-Auto/AutoSecond?Chk=([A-Z0-9]+)`

Other similarities exist between Ishak and past reports. ClearSky also notes that a log file was publically accessible in the attacks they observed:

Interestingly, the log file for the previous pages was hosted publicly on the same virtual folder. The log contained the false credentials the target submitted (as she recognized this was a fake):

```
page1 | id:86216574 | email:[REDACTED]@gmail.com | pass:-77.125.242.112 | סקר בדשחור | www.
UTM=1&id=86216574&email=[REDACTED]@gmail.com&pass=-77.125.242.112&id=86216574&email=[REDACTED]@gmail.com&pass=-77.125.242.112
```

ClearSky's logs strongly resemble the format found both on Flying Kitten and the Ishak phishing pages, which follow a somewhat unique format, for example in Ishak:

```
$data = "$date | user:$user | email:$email | pass:-$password- | $IP | $Page$URI | $Agent | $referer \r\n";
```

One addition to the Ishak codebase related to logging and authentication that was not previously seen in Flying Kitten kit, which appears to be:

```
.htaccess
1 AuthUserFile C:/xampp/htdocs/input/.htpasswd
2 AuthName "Hey Fuck Yourself Please"
3 AuthType Basic
4 require user admin
```

```
22 if ($SetAddress[$id] == true) {
23 else
24 {
25     $rec = fopen("input/Fucker.log", "a");
26     fwrite($rec, "$date | $TarAddress | $Agent | $referer \r\n");
27     fclose($rec);
28     // Replace redirect link in header
29     header( 'Location: https://goo.gl/WszKaa' );
30 }
```

The scripts have changed over time. The different folders capture iterative versions up to August 2016. While there are phishing-related files in the code, the actual spearphishing activity reflected in logs begins around February 2016. These logs reflect an active group targeting a broad range of targets, with a clear focus on Iranian domestic politics. Since no publications have focused on Rocket Kitten since the Check Point report, there is no external corroboration of these campaigns. However, our direct observation of Rocket Kitten attacks against the human rights community runs unbroken from August 2016 to the present. As there are shifts over time, there is also a fair amount of congruency.

Examples of recorded hostnames within the Ishak logs include:

- network.us14-userfile-permission-account-signin.com (created 2016-06-28)
- onedrive.signin-useraccount-mail.com (created 2016-07-26)
- verify-your-password-for-secure-your-account.cf (accessed 2016-06-28)
- mg5-myfile-available-signin.ga (accessed 2016-02-28)
- yahoo-drive.signin-useraccount-mail.com (created 2016-07-26)
- yahoo-reset.signin-useraccount-mail.com (created 2016-07-26)
- your-file-drive-permission-for-download.cf (accessed 2016-05-28)
- drive-useraccount-signin-mail.ga (accessed 2016-08-28)
- userfile-need-permission-download-signin.com (created 2016-06-28)

Aside from the popular communications platforms, namely Yahoo!, Microsoft, Facebook and Google, the repository includes sites modified to include attempts to target:

IRAN THREATS

[Home](#)

- The Roundcube webmail service of an Iranian medicine company;
- Cox webmail, directed against an unknown individual; and
- American and British universities, targeting Iran-focused scholars.

The preference of the Ishak scripts over Oyun may be explained by a change in behavior we observed in Fall 2015, when Rocket Kitten was publishing. After these incidents, Rocket Kitten was more circumspect about its activities. Prior to the change, Rocket Kitten provided a certain infrastructure was used across multiple targets for extended periods of time (several months).

After the heightened level of exposure, Rocket Kitten shifted techniques to reduce the linkability and hide infrastructure. Rather than operating leased servers and clever domains for months, later spearphishing attempts conducted by the group treated hosts and names as more disposable. Attempts were stood up for short-term episodes with a specific set of targets in mind. Upon indication of discovery, success, or suspicion, the infrastructure was not reused. It stands to reason that if a server would only be used against a few targets over a couple of days, Oyun's requirements of database became costly. Thus Ishak would be a more flexible approach, even if not as sophisticated.

An alternative hypothesis is that Rocket Kitten is internally uncoordinated, or certain campaigns were misattributed. Check Point's report records no activity for June and July 2015, however, we see "Rocket Kitten" spearphishing attempts during this time. Similarly, while IP addresses of German satellite provider IABG are documented in multiple Rocket Kitten reports, we only see that ISP in attacks in September 2014 and

CASE 2: MALWARE

In January 2017, a domain "IranianUkNews[.]com" was created with registration information that matched previously identified Rocket Kitten IP address adjacent to a Rocket Kitten credential theft site. The domain was noteworthy since it bore a resemblance to the independent Iranian news outlet (iranianuk.com) that covers Iranian politics. The new domain was not the first case of Iranian UK being impersonated. A series of credentials stolen in September 2013 using the domain "qooqle.com[.]co" were hosted and registered alongside a domain "iraniannuk[.]com" – a campaign that was a phase in Flying Kitten's activities.

Having flagged the domain early, we were privy to the process of the site being set up. From our monitoring of the IranianUkNews, there was content hosted on the suspicious domain:

- a Persian-language page impersonating Iranian UK that we were not able to directly observe; and,
- a fake Adobe Flash site containing a malicious Windows executable.

The Adobe Flash page that was hosted on the IranianUkNews bore immediate similarities in content to another Flying Kitten resource – the one that FireEye documented in Operation Saffron Rose. In the case of Operation Saffron Rose, this domain was used to host malware, and the page that impersonated BBC Persian (domain: "persian-bbc.co[.]uk") in order to deceive the visitor to install malware to supposedly view a

The full path for Flash site on new IranianUkNews domain was the following:

```
iranianuknews.com/adobe/flashplayer/Download/78923582514/index.php?id=7892358
```

Similar to the case of the Flying Kitten phishing script, we had a copy of the backend of Plugin-Adobe[.]com. Timestamps of the Flying Kitten page was initially created in August 2013. A comparison of the structure and content of the Flying Kitten page and the new site strongly indicated

```
$exists = false;
if (isset($_GET['id']))
{
    // $userid = $_GET['id'];
    $exists = url_exists("http://plugin-adobe.com/logs/$userid-log.log");
}
```

Logging Functions on a Fake BBC Persian Malware Site

The functionality and behavior of the sites is similar despite the code being undisclosed. Flying Kitten was often meticulous about logging and in that spirit their fake Adobe site would maintain logs separated out in different files based on campaigns (defined based on URL predictable behavior, we were able to retrieve the logs from the new Rocket Kitten site. These logs also bear a similarity to between them logs.

Flying Kitten (2013)

```
2013-08-07 16:39:21 | user:demo | 81.91.146.232 | plugin-adobe.com/tst.php?id=demo | Mozilla/2.0 (compatible; MSIE 6.0; Windows NT 5.2)
2013-08-07 17:24:11 | user:demo | 81.91.146.232 | plugin-adobe.com/tst.php?id=demo | Mozilla/2.0 (compatible; MSIE 6.0; Windows NT 5.2)
2013-08-07 17:37:01 | user:demo | 81.91.146.232 | plugin-adobe.com/tst.php?id=demo | Mozilla/2.0 (compatible; MSIE 6.0; Windows NT 5.2)
```

Rocket Kitten (2017)

```
2017-01-04 21:03:33 | id=[78923582514] | 127.0.0.1 | 127.0.0.1/adobe/flashplayer/Download/78923582514/index.php?id=78923582514 | Mozilla/5.0 (Windows NT 10.0
2017-01-24 13:59:09 | id=[78923582514] | 185.81.40.230 | iranianuknews.com/adobe/flashplayer/Download/78923582514/index.php?id=78923582514 | Mozilla/5.0 (Win
```

The January 2017 logs demonstrate that an individual had engaged in a fair amount of testing earlier in the month on a local machine prior to Internet. After posting the page on the IranianUkNews domain, IP addresses associated with the PureVPN service and the Iranian ISP "Parsdade" began to test the site again. Parsdade has been observed repeatedly within Rocket Kitten operations, and is not a very large ISP. This demonstrates that staging the new IranianUkNews site had both the original scripts used by Flying Kitten and was based in Iran, therefore lowering the possibility of a security researchers doing testing.

MALWARE

The departure between our observations of Flying Kitten and the Rocket Kitten site begins at the malware downloaded by the [fake Flash Player](#). The IranianUkNews site would download a file with an Android application (.APK) extension. In reality, the binary was a mislabelled Windows executable. The parameters would prompt the site to offer a .EXE file (the same file). No actual Android malware was observed. Flying Kitten was never observed using Android malware, and this aspect appears to be a newer enhancement. Rocket Kitten has been observed using Android malware as [we noted last year](#).

In Operation Saffron Rose, FireEye documents Flying Kitten's malware agent, "Stealer," a simple keylogger with an easy-to-use builder application. The new IranianUkNews is not Stealer, but rather appears to be a predecessor that is in certain respects better designed than Stealer. The existence of this malware agent would account for why we found files on their command and control FTP servers in 2013 that appeared to be malware logs. Unlike Stealer, including files with the name "mb_1986." Once again, Mojtaba. Based on static references in the malicious library, we will refer to this as TKeylogger. Since TKeylogger is extremely old, and has not been observed being actively used in attacks, a writeup of the malware agent is not in scope for this report.

IRAN THREATS

[Home](#)

The mozalloc.dll library itself has a compilation timestamp of "2013-08-07 07:02," a couple of hours prior to the file modification time and from Flying Kittens' site.

TKeylogger Beacon

```
GET /tst.php?id=14258974894 HTTP/1.1
User-Agent: Mozilla/2.0 (compatible; MSIE 6.0; Windows NT 5.2)
Host: plugin-adobe.com
Cache-Control: no-cache
```

One behavior not seen in Stealer is an initial beacon upon infection to an HTTP endpoint. Stealer simply exfiltrated logs over FTP, although incomplete code for HTTP POST, SFTP and SMTP communications. The unchanging value provided as an "id" in the beacon appears to be "14258974894". The date for this "timestamp" would be November 2412, but shifting the value one place puts the date at a more reasonable (but unexplained) date of November 24, 2012. TKeylogger acquired beacons back to the old "plugin-adobe[.]com," which we believe is still sinkholed by researchers, and there are static IP addresses 5.9.244[.]137 on Hetzner with a username of "father" and the password "AzInjaBoro" ("get out of here"). The Hetzner address also appears in Flying Kitten for other previously identified domains four years ago.

It is also notable that within our observation of Flying Kitten, much of the activity was conducted from IP addresses within the small range 81.9.244[.]137 ("World Leading"). The sample conducting the test in the old Flying Kitten captured logs also originated from the Jahan Pishro range (81.9.244[.]137) with this beacon with the unusual user agent "Mozilla/2.0 (compatible; MSIE 6.0; Windows NT 5.2)" – which again appears in the old captured logs reflect the testing of TKeylogger by its developer, and that our sample is similar to the original malware.

Here as well, disclosure of previously undocumented malware indicates that Rocket Kitten had direct access to Flying Kitten's tools.

INFRASTRUCTURE OVERLAP

The registration of IranianUkNews and the credential theft sites follows within a long chain of domains connected to the Rocket Kitten group's indicators. For example, the registration name Hiram Ryan, a name that appears to have been taken from the registration of a small aviation-related credential theft domains. The domain also reflects a fingerprint of Rocket Kitten domains present since around the Check Point report, with

```
Registrant Name: (First) (Last)
Registrant Organization: (First or Last).co
```

Example:

```
Domain Name: logins-mydrive-useraccount.com
Creation Date: 2015-12-17T04:00:00Z
Registrant Name: William Morse
Registrant Organization: William.co
```

IranianUkNews[.]com Registration:

```
Registrant Name: Hiram Ryan
Registrant Organization: Ryan.co
Registrant Email: admin@iranianuknews.com
```

IRAN THREATS

[Home](#)

- display-ganavaro-abrashimchi.com
- iforget-memail-user-account.com
- change-mail-accounting-register-single.com
- change-user-account-mail-permission.com
- display-error-runtime.com

The nature of some of these domains are unclear, but several have been observed in credential theft attempts, and likely use the Ishak co

These activities are importantly connected to the Telegram-focused credential theft and reconnaissance we disclosed in [our Black Hat pr](#) address that logged onto the IranianUkNews site was also observed conducting Telegram phishing attempts using the domain telegram[. the tracyreed.cfl@gmail.com involved in the "shaftool" and other API scraper domains. In fact, the ghalpaq.com domain that was originally enumeration attempts was originally pointed to a LeaseWeb host identified by ClearSky in "Thamar Reservoir."

Passive DNS Record: 178.162.203.56

- 2015-09-23 www.google-verify.com
- 2015-08-10 profiles-verify.com
- 2015-06-09 ghalpaq.com
- 2015-03-17 www.google-setting.com
- 2015-03-03 google-setting.com
- 2015-03-03 google-verify.com
- 2015-03-03 verify-ycervice.com
- 2015-03-03 verify-yservice.com
- 2015-03-03 ymail-service.com

CONCLUSION

Rocket Kitten has been substantially less active after the successive reports in Fall 2015, often nearly dormant for months. Whereas Rocket Kitten, a prolific group, the spearphishing attempts posed to civil society have shifted to other operators. In the lead up to the February 2016 parliament elections, "Infy" became the most active threat in our monitoring, with only a few Rocket Kitten attempts. Since then, the mantle has been taken by C and others.

Unfortunately, it is not always clear why researchers assert that certain domains are related, imposing hurdles to scrutinizing claims. Similar to the challenges toward establishing attribution – Iranian groups generally maintain the same focus.

On the other hand, the efforts that were labeled Rocket Kitten could have been organized in a more nebulous arrangement – and Rocket Kitten to begin with. Like Iran's "mosaic defense" military organizing structure, the hacking efforts are clearly more decentralized and fluid than conventional warfare operations. This makes tracking and attributing attacks originating from Iran all the more complex. These two cases touch on the challenges to understand it with code was either repurposed or experimented with by Rocket Kitten.

The group, whatever we call it, has still engaged in spearphishing campaigns, however, the level of professionalism has declined and the risk of exposure. This could indicate that just as Flying Kitten appears to have disbursed, so has Rocket Kitten. Taken together, these differences start to de

IRAN THREATS

[Home](#)

If our version of Rocket Kitten is not the real Rocket Kitten, then what is? Is it still Flying Kitten?

Moving forward, this also tells a cautionary tale as researchers find fingerprints of multiple Iranian groups involved in attacks such as [those](#) history of Iranian actors has shown that toolkits move, and so do people.

CONTACT

EMAIL

CLAUDIO (NEX@AMNESTY.ORG)

Fingerprint: E063 75E6 B9E2 6745 656C 63DE 8F28 F25B AAA3 9B12

COLLIN (CDA@CDA.IO)

PGP Key: <https://cda.io/key.asc>

Fingerprint: 510E 8BFC A60E 84B4 40EA 0F32 FAFB F2FA

INDICATORS OF COMPROMISE

MALWARE

Filename	MD5
mozalloc.dll	8ad0485fd3509042b0a477f65507f711

CREDENTIAL THEFT FROM ISHAK LOGS

account-signin-myaccount-users.ga
aol.userfile-need-permission-download-signin.com
changepassword.userfile-need-permission-download-signin.com
cox.userfile-need-permission-download-signin.com
drive-signin-permissionsneed.ml
drive-useraccount-signin-mail.ga
drive.signin-account-privacymail.com
dropebox.co
durham-ac-uk.userfile-need-permission-download-signin.com
hangouting-signin-to-chat.ga
mg5-myfile-available-signin.ga
network.us14-userfile-permission-account-signin.com
onedrive.signin-useraccount-mail.com
security-supportteams-mail-change.ga
singin-your-drive.ga
userfile-need-permission-download-signin.com
verify-account-for-secure.ga
verify-google-password.userfile-need-permission-download-signin.com

IRAN THREATS

Home

yahoodrive.signin-account-privacymail.com
your-file-drive-permission-for-download.cf

2016, Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International | Ion Template by [TEMPLAT](#)