

# CrowdStrike Tracks Reported Iranian Actor as FLYING KITTEN

[crowdstrike.com/blog/cat-scratch-fever-crowdstrike-tracks-newly-reported-iranian-actor-flying-kitten/](http://crowdstrike.com/blog/cat-scratch-fever-crowdstrike-tracks-newly-reported-iranian-actor-flying-kitten/)

Matt Dahl

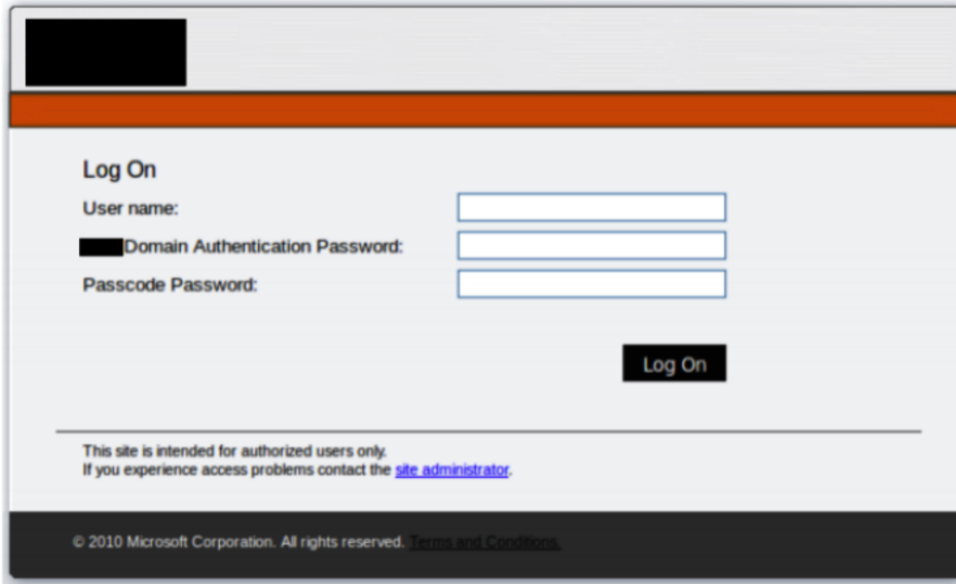
May 13, 2014



Today, our friends at FireEye released a [report](#) on an Iran-based adversary they are calling Saffron Rose. [CrowdStrike Intelligence](#) has also been tracking and reporting internally on this threat group since mid-January 2014 under the name FLYING KITTEN, and since that time has seen targeting of multiple U.S.-based defense contractors as well as political dissidents.

## **Flying Kitten Targeted Intrusion**

FireEye's report notes that this adversary's targeted intrusion activity consists of credential theft and malware delivery individually. The FLYING KITTEN campaigns investigated by CrowdStrike Intelligence showed that the actor actually combines the two. For example, the adversary will register a domain that spoofs the name of the targeted organization and then host a spoofed login page on that site.



The page is used to steal legitimate credentials, but once users enter the credentials, they are often redirected to a new page that prompts them to download a “Browser Patch” or other similar type of file. The downloaded file is actually the Stealer malware that exfiltrates stolen data to an FTP server.

In addition to the aerospace/defense and dissident targeting, it also appears that FLYING KITTEN is also engaged in broader targeting via the website parmanpower[.]com. This website is registered via the same registrant email (info[@]usa.gov.us) and other Whois information as some of the other domains related to the activity discussed above. It purports to be the website of a business engaged in recruiting, training, and development in Erbil, Iraq.

HOME ABOUT US NEWS & EVENTS CONTACT US REGISTER LOGIN



**Parman Power**  
Is a professionally managed search firm in Erbil, providing recruitment consultancy as well as training and development to our client companies and applicants of Erbil Market.

Our search services are supported through a dynamic team of experienced professionals servicing through various industries like BFSI, Consumer and Non Consumer Durable, Telecom, Healthcare, Media & Entertainment, Manufacturing, etc.

**Stepping into the Workplace via parman power**  
parman power aims to land you that dream job at the soonest time and guide you through work related issues such as finding the right job, processing pre-employment requirements, and give out expert advice.

Be the first to gain;

- > Practical advice and useful job-hunting tips,
- > Training and OJT Opportunities,
- > Workshops and Seminars together with a whole list of Fresh
- > Graduate job positions.

send your CV to share our hundreds of solution jobs: **SEND CV**



The flowchart illustrates the 'Work Methodology' process. It starts with 'Client' at the top, which branches into two paths. The left path includes 'Agreement with the client', 'Focus Search Brief', and 'Form Search Team'. The right path includes 'Coordinate Interviews with Clients', 'Reference Check', and 'Feedback & Closure of Assignments'. Both paths converge back to 'Client'. A central box labeled 'Work Methodology' is connected to these steps. A large red arrow points left towards the 'Coordinate Interviews with Clients' step, and the text 'TALENT ACQUISITION' is written in red above it.

No malicious activity has been linked to this domain, however, the fact that it was registered under the same registrant email at the same time as other FLYING KITTEN domains linked to malicious activity, it is likely that the adversary is using this site for malicious purposes as well. The website does not appear to deliver any malware, so its most likely purpose is to act as a credential-collection mechanism much like the spoofed Institute of Electrical and Electronics Engineers (IEEE) Aerospace Conference website (aeroconf2014[.]org) the adversary used earlier this year. This spoofed recruiting company website could be used to target entities across a wide range of sectors.

## Attribution

Attribution in this case is interesting, as the adversary appears to have made a mistake when registering its malicious domains. The registrant email that currently appears in the Whois records of some of the FLYING KITTEN domains is info[@]usa.gov.us, however historical records show that the domains were originally registered under the email address keyvan.ajaxtm[@]gmail.com.

2013-12-31	2014-01-13
1 Domain Name:parmanpower.com	1 Domain Name:parmanpower.com
2 Name Server:ns2.persiandns.net	2 Name Server:ns2.persiandns.net
3 Name Server:ns1.persiandns.net	3 Name Server:ns1.persiandns.net
4 Created On:2013-12-30 12:51:57.0	4 Created On:2013-12-30 12:51:57.0
5 Last Updated On:2013-12-30 12:54:53.0	5 Last Updated On:2014-01-04 12:51:57.0
6 Expiration Date:2014-12-30 12:51:57.0	6 Expiration Date:2014-12-30 12:51:57.0
7 Sponsoring Registrar:REALTIME REGISTER B.V.	7 Sponsoring Registrar:REALTIME REGISTER B.V.
8 Reseller:Realtime Register B.V.	8 Reseller:Realtime Register B.V.
9 Status:ADD_PERIOD	
10 Status:OK	9 Status:OK
11 Registrant ID:RP01EKHW6VycG8CyTfjHbYE9	10 Registrant ID:RP01EKHW6VycG8CyTfjHbYE9
12 Registrant Name:no name	11 Registrant Name:no name
13 Registrant Organization:no name	12 Registrant Organization:no name
14 Registrant Street1:420 Stevens Ave Ste 170	13 Registrant Street1:420 Stevens Ave Ste 170
15 Registrant City:Longmont	14 Registrant City:Longmont
16 Registrant State:CO	15 Registrant State:CO
17 Registrant Postal Code:80504	16 Registrant Postal Code:80504
18 Registrant Country:US	17 Registrant Country:US
19 Registrant Phone:+1.3042416466	18 Registrant Phone:+1.3042416466
20 Registrant Fax:+1.3042416466	19 Registrant Fax:+1.3042416466
21 Registrant Email:keyvan.ajaxtm@gmail.com	20 Registrant Email:info@usa.gov.us
	21 BILLING ID:RP01EKHW6VycG8CyTfjHbYE9
	22 BILLING Name:no name
	23 BILLING Organization:no name
	24 BILLING Street1:420 Stevens Ave Ste 170

As FireEye's report notes, the keyvan.ajaxtm@gmail.com email address ties back to an Iran-based entity called Ajax Security Team. Earlier this year, Ajax Security had an easily identifiable presence on the Internet with its own website and related Facebook pages.



This Internet presence has decreased significantly since early 2014, likely due to a desire to keep a lower profile now that the group is engaged in targeted intrusion activity.

The following Yara rules will provide detection for the adversary remote access toolkit and exfiltration tool:

```
rule CrowdStrike_FlyingKitten : rat
{
meta:
    copyright = "CrowdStrike, Inc"
    description = "Flying Kitten RAT"
    version = "1.0"
    actor = "FLYING KITTEN"
    in_the_wild = true

    strings:
        $classpath = "Stealer.Properties.Resources.resources"
        $pdbstr = "\Stealer\obj\x86\Release\Stealer.pdb"

    condition:
        all of them and
            uint16(0) == 0x5A4D and uint32(uint32(0x3c)) == 0x4550 and
            uint16(uint32(0x3C) + 0x16) & 0x2000 == 0 and
            ((uint16(uint32(0x3c)+24) == 0x010b and
            uint32(uint32(0x3c)+232) > 0) or
            (uint16(uint32(0x3c)+24) == 0x020b and
            uint32(uint32(0x3c)+248) > 0))
}

rule CrowdStrike_CSIT_14003_03 : installer
{
    meta:
        copyright = "CrowdStrike, Inc"
        description = "Flying Kitten Installer"
        version = "1.0"
        actor = "FLYING KITTEN"
```

```
    in_the_wild = true

    strings:

        $exename = "IntelRapidStart.exe"

        $confname = "IntelRapidStart.exe.config"

        $cabhdr = { 4d 53 43 46 00 00 00 00 }

    condition:

        all of them

}
```

You can use this rule with CrowdStrike's free [CrowdResponse](#) tool to easily scan your systems for presence of FLYING KITTEN. Interested in learning about other threat actors? [Visit our threat actor center](#) for details on nation-state and eCrime adversaries.

If you have any questions about these signatures or want to hear more about Flying Kitten and their tradecraft, please contact: [intelligence@crowdstrike.com](mailto:intelligence@crowdstrike.com) and inquire about Falcon Intelligence, our Cyber Threat Intelligence subscription.