“Internet en Iran : Une situation sous tension”

INFO731 - Sécurité et Cryptographie

MASSIT Clément - CAULLIREAU Dorian - PERROLLAZ Maverick

15 minutes pour comprendre la situation en Iran

1. Contexte interne et géopolitique
2. Des groupes d’acteurs contre l’organisation
3. Zoom sur Rocket Kitten, un groupe bien particulier
4. L’Iran et son “internet caché”

1. Comprendre la situation…

Puissance nucléaire

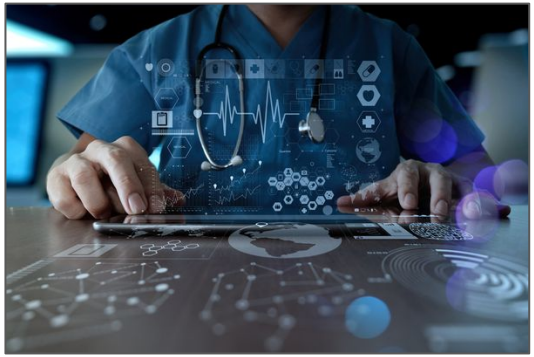
Conflits géopolitique

Formation dans la sécurité

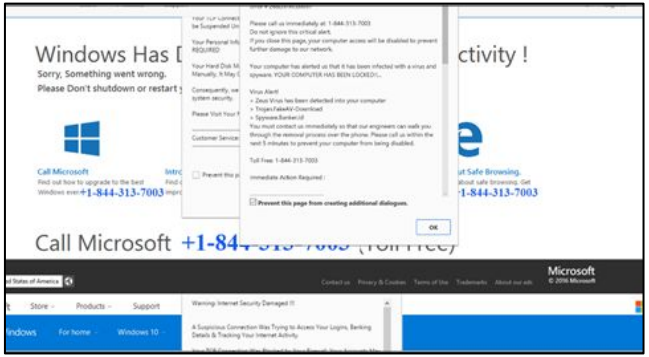
2. Infy, l’attaque aux infrastructures

Contre qui ? | **Pourquoi ?** | **Comment ?**

Gouvernement & Société civile

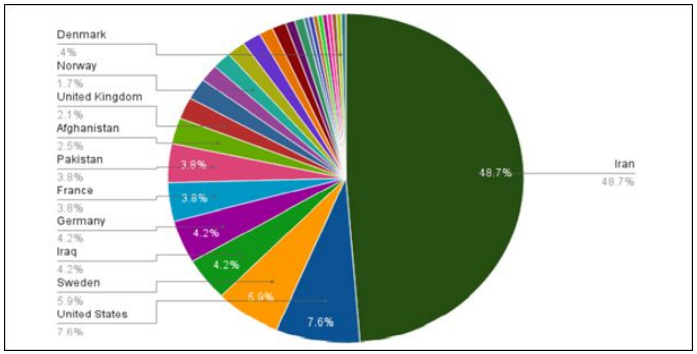


Vol et utilisation des données



Mail d’hameçonnage

2. Infy, un réseau de puissance



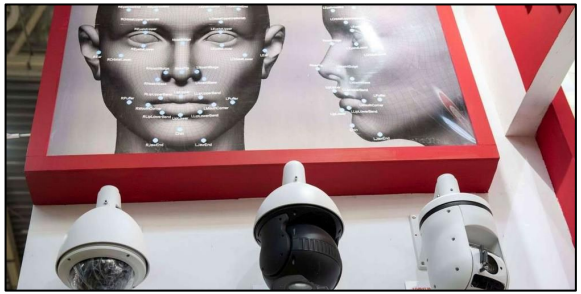
Une utilisation (presque) internationale

Comment ralentir le processus ?

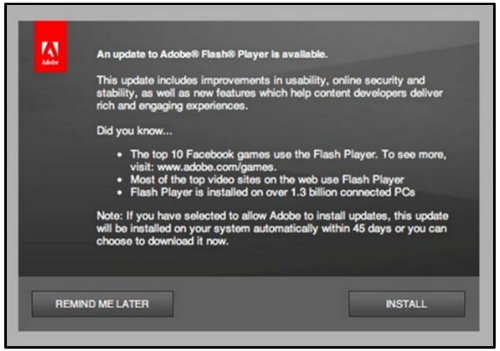
2. Ghambar, beaucoup de cibles et beaucoup d'actions

Contre qui ? → **Pourquoi ?** → **Comment ?**

Économie, défense, entreprises



Surveillance et vol de données

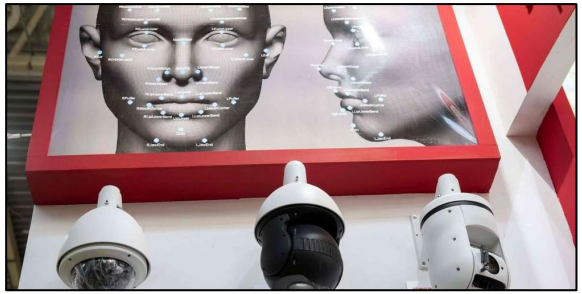


Faux logiciels

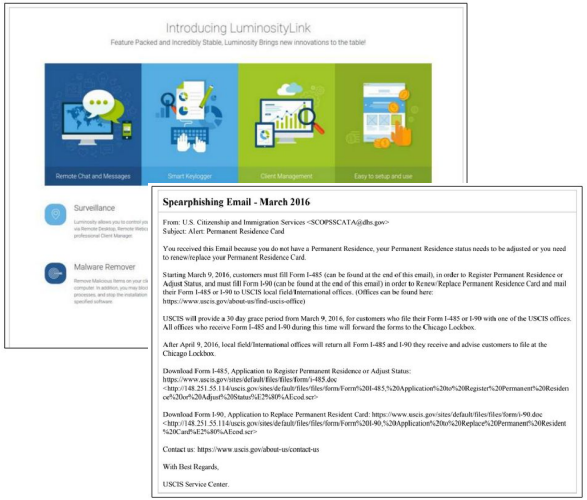
2. Sima, toujours et encore des mails

Contre qui ? | **Pourquoi ?** | **Comment ?**

Diaspora Iranienne



Surveillance des données



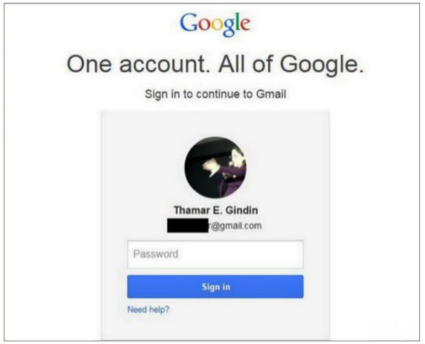
Mails douteux

3. Zoom sur le groupe Rocket Kitten

Utilisation de logiciels malveillants

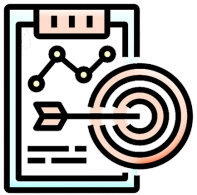
Cibles : responsable de la défense, ambassades, chercheurs, …

3. Rocket Kitten : Stratégie d’attaque



Exemple d’une page de phishing qu’ils ont pu réaliser

Les victimes se font avoir par des appels téléphoniques ou par mails



Pages de phishing

3. Rocket Kitten : outils utilisés

Cwoolger
&
.NETWoolger

Wrapper/Gholee

SQLMap

Metasploit

Et d’autres outils comme FireMalv, MPK, Havij, Netsparker ….

3. Rocket Kitten, une enquête menée sur ce groupe

Checkpoint
Retail Technology Solutions

Requêtes GET effectuées sur le serveur web de phishing

phakeddb

génère les pages web de phishing

3. Rocket Kitten, une plateforme : Oyun Management System

user_id	user_name	user_pass	user_nikname
49	admin	e10adc3949ba59abbe56e057f20f883e	super admin
50	anonymous	09d2b6cc9114ed718d9145fa40ed04f8	Anonymous
51	merah	e42e563b4504be66a94dcba01aa80d0a	mire
52	124	e87aa71e42c7de4780f448c8e92b50cd	razavi
53	kaveh	46ec41ac0432182829250c0da50f89bb	kaveh

Table des utilisateurs

e10adc3949ba59abbe56e057f20f883e = 123456

Noms Persans = opérateurs chargés du design des pages de phishing

un projet = une victime = une url personnalisée

proj_id	proj_name	page_id	user_id	proj_date	proj_url	time_stamp
1148	[redacted]gmail.com	41	54	2014-09-14	http://google-profiles.com/?_schema=1148&rnd=32331	1432651592
1149	[redacted]il.com	41	54	2014-09-14	http://google-profiles.com/?_schema=1149&rnd=24266	
1151	[redacted]ans@hotmail.com	48	50	2014-09-14	http://outlook.profile.hmail.us/new/?_schema=1151&...	1410751030
1152	[redacted]ail.com	48	50	2014-09-14	http://outlook.profile.hmail.us/new/?_schema=1152&...	1410804467
1153	[redacted]ail.com	48	50	2014-09-14	http://outlook.profile.hmail.us/new/?_schema=1153&...	
1154	[redacted]otmail.com	48	50	2014-09-14	http://outlook.profile.hmail.us/new/?_schema=1154&...	

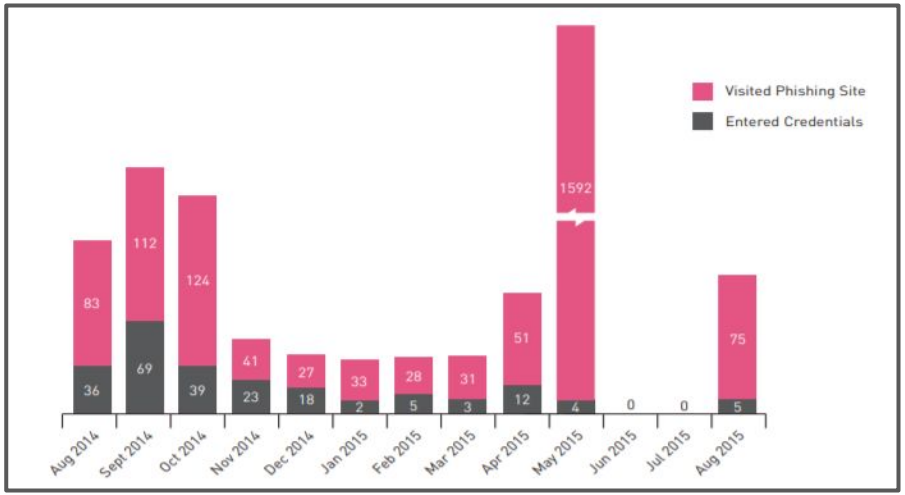
Table des projets

log_id	proj_id	log	date	viewed
50971	2583	</br>Page viewed on Monday 2015-08-17 At 12:19:45<...	2015-08-17	1
50972	2583	</br>Page viewed on Monday 2015-08-17 At 12:21:50<...	2015-08-17	1
50973	2583	</br>Page viewed on Monday 2015-08-17 At 12:23:42<...	2015-08-17	1
50974	2583	</br>Page viewed on Monday 2015-08-17 At 12:23:56<...	2015-08-17	1

Table des logs

logs des connexions d'août 2014 - août 2015

3. Des logs qui prouvent l'efficacité

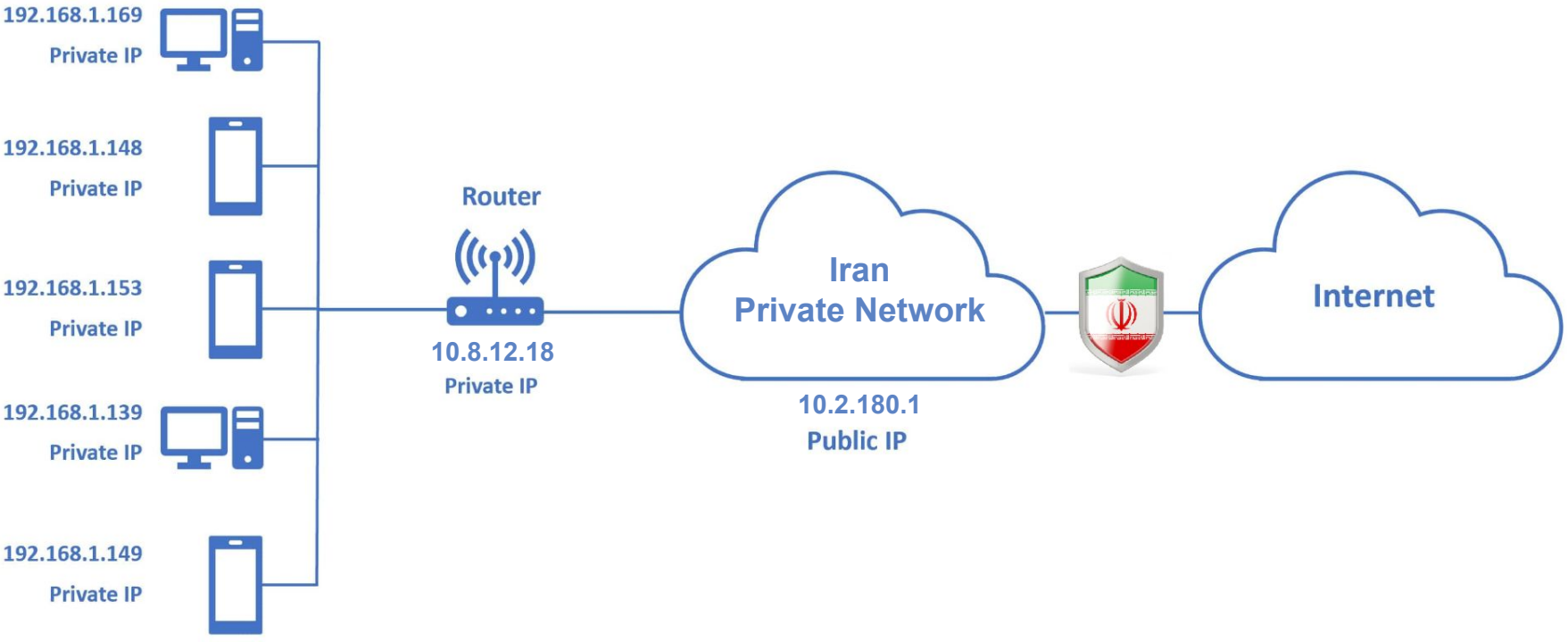


pages de phishing ont été un "succès"

Mai 2015 pic de visite, brute-force sur les pages

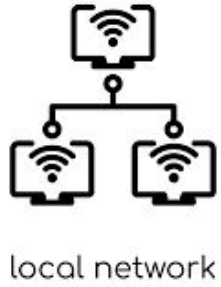
opérations fermées en juin et juillet

4. L'Iran et son "internet caché"



4. L’Iran et son “internet caché”

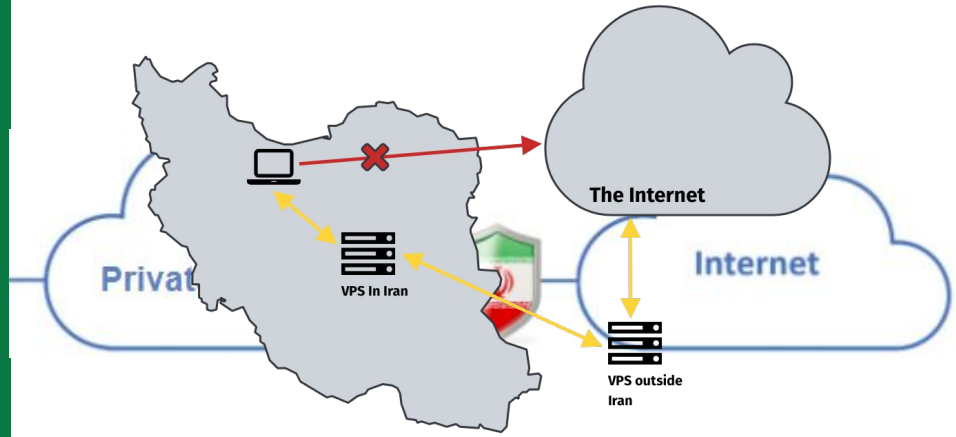
d’hôtes différents



IP Range : 10.0.0.1 - 10.255.255.254

Masque de sous-réseau : 255.0.0.0

Nombre d'hôtes possible : 16,777,216



Activités, médias, politique, etc

Gouvernement

Population

4. Difficulté d’estimé l’utilisation du réseau privé

Les fichiers qui répertorient les domaines enregistrés en **.ir** ne sont pas partagé.

Si on utilise seulement les DNS publics, l’étude serait alors très limitée.

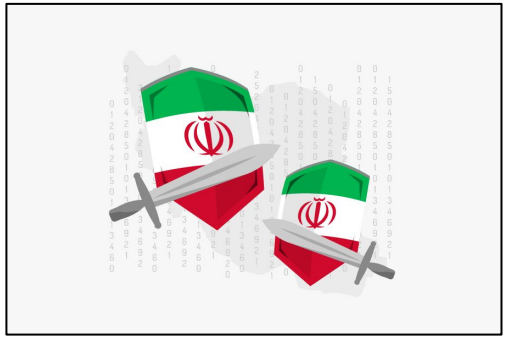
Extraction massive des données

Totalité des hôtes : 16 777 216

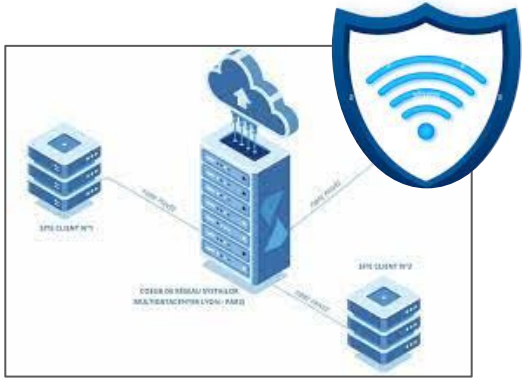
Service (Port)	Number of Host
FTP (21)	12672
SSH (22)	8029
Telnet (23)	20060
SMTP (25)	183
DNS (53)	2510
POP (110)	78
HTTP (80)	9960
IMAP (143)	44
HTTPS (443)	1366
HTTP-Alt (8080)	601

Conclusion

Contexte favorisant les attaques



Beaucoup d’attaquants



Un internet caché

Nos recherches, nos sources

Evidence Emerges That Iran Is Building Its Own Hidden Internet | MIT Technology Review

"The Hidden Internet of Iran, Private Address Allocations on a National Network", Collin Anderson, 28 Sep 2012 - https://arxiv.org/pdf/1209.6398.pdf

"Iran and the Soft Ware for Internet Domiance"

https://www.blackhat.com/docs/us-16/materials/us-16-Guarnieri-Iran-And-The-Soft-War-For-Internet-Dominance-wp.pdf

"Iran's Soft War Get Harder" – **InfoSecurity Magazine**

https://www.infosecurity-magazine.com/news/iran-soft-war/

"ROCKET KITTEN : A campaign with 9 lives" - ***CheckPoint***

https://blog.checkpoint.com/wp-content/uploads/2015/11/rocket-kitten-report.pdf

"*Rocket Kitten Showing Its Claws: Operation Woolen-GoldFish and the GHOLE campaign*" - *https://www.trendmicro.com/vinfo/fr/security/news/cyber-attacks/operation-woolen-goldfish-when-kittens-go-phishing*