“ROCKET KITTEN : A campaign with 9 lives”

INFO731 – Sécurité et Cryptographie

MASSIT Clément - IDU 4

Sommaire :

Sources :

- “ROCKET KITTEN : A campaign with 9 lives” - 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

Depuis 2014, un groupe d'attaque d'Iranien cible des personnes d'intérêt avec un logiciel malveillant. Ce groupe de cyber espionnage a été surnommé Rocket Kitten.

Les attaques de ce groupe ont été analysées des rapports. Leur méthodes, leur outils et leur technique ont pu être tirés :

- Grosse utilisation du phishing sur des personnes ou des groupes provenant des régions du Moyen Orient (y compris des cibles venant d'IRAN), d'Europe ou des Etats Unis.
- Parmi les victimes, des gens haut placés responsable de la défense, des ambassades, des chercheurs, des scientifiques dans les domaines de la physique et des sciences nucléaires.
-

La campagne d'attaque des Rocket Kitten a été analysée plusieurs fois par beaucoup d'organismes. Des noms de code et d'opérations reviennent fréquemment et ramènent vers une origine iranienne.
Avec tous les rapports qu'il y ait eu sur ce genre d'attaques, Check Point (une entreprise de sécurité) a détecté des attaques actives continues qui utilisent les mêmes méthodes et la même structure pour chaque attaque.

Exemple d'attaques

The May 2014 Operation Saffron Rose

La publication de cette opération un groupe de hackers iraniens 'AJAX SECURITY' dont le nom de code est 'Flying Kitten'. Il s'agit d'attaques de phishing contre des dissidents iraniens. Ce groupe est potentiellement lié aux attaques de ROCKET KITTEN (similarité dans le schéma de nommage des domaines, mode de fonctionnement et outils très similaires aux Rocket Kitten).

iSight Partners

Une autre publication a été publiée pour détailler des efforts similaires de phishing, et soutenus par de fausses identités sur les réseaux sociaux concernant les journalistes. Le rapport montre que les attaquants ciblent les décideurs politiques, les hauts responsables, le personnel militaire et les organisations de l'industrie de la défense aux États-Unis, au Royaume-Uni et en Israël. En revanche, aucune preuve n'a été trouvée qui relie ces attaques au Rocket Kitten.

ClearSky est une entreprise israélienne de cybersécurité, elle effectue des recherches sur les attaques du groupe de Rocket Kitten. Lors des investigations, ClearSky mentionne une

violation d'une institution universitaire israélienne pour servir de service d'hébergement pour le site Web de phishing. Cela à permis aux chercheurs de ClearSky de prendre connaissance d'une liste de cibles potentielles.
Les recherches avancent et décrivent 2 types de malwares que les attaquant utilisent :

- Le 'wrapper' Un outil permettant tester la capacité à pénétrer dans un système
- Un outil qui vole des infos d'identification depuis le stockage des ordinateurs infectés. Il semblerait que cet outil soit nommé 'FireMalv' selon les attaquants.

Avec cette liste on remarque un fort alignement avec les intérêts politiques de l'Etat-nation.

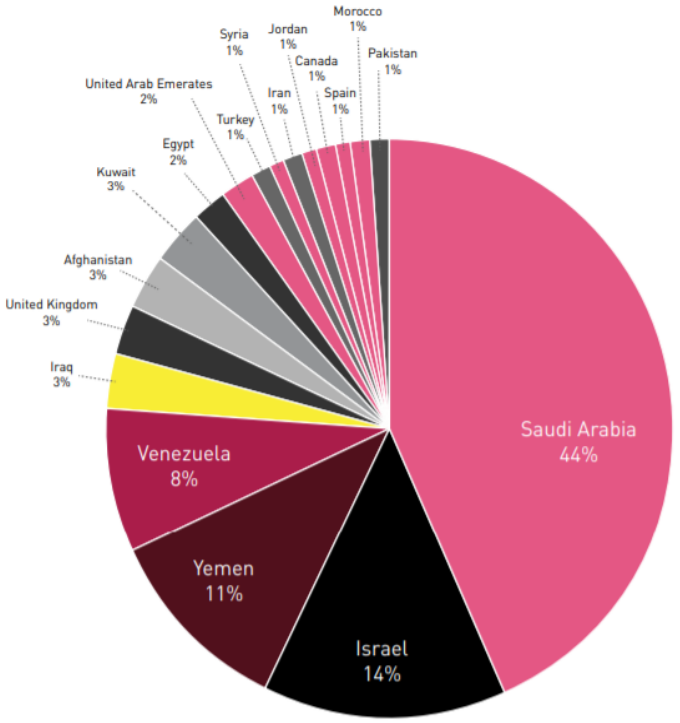


Image 5—Partial target country distribution as visible on the phishing server logs exposed by ClearSky

ClearSky a fourni plusieurs exemples de mails de phishing personnalisés, y compris des appels téléphoniques aux victimes de leurre. Cela montre la persistance et la volonté des opérations du groupe.

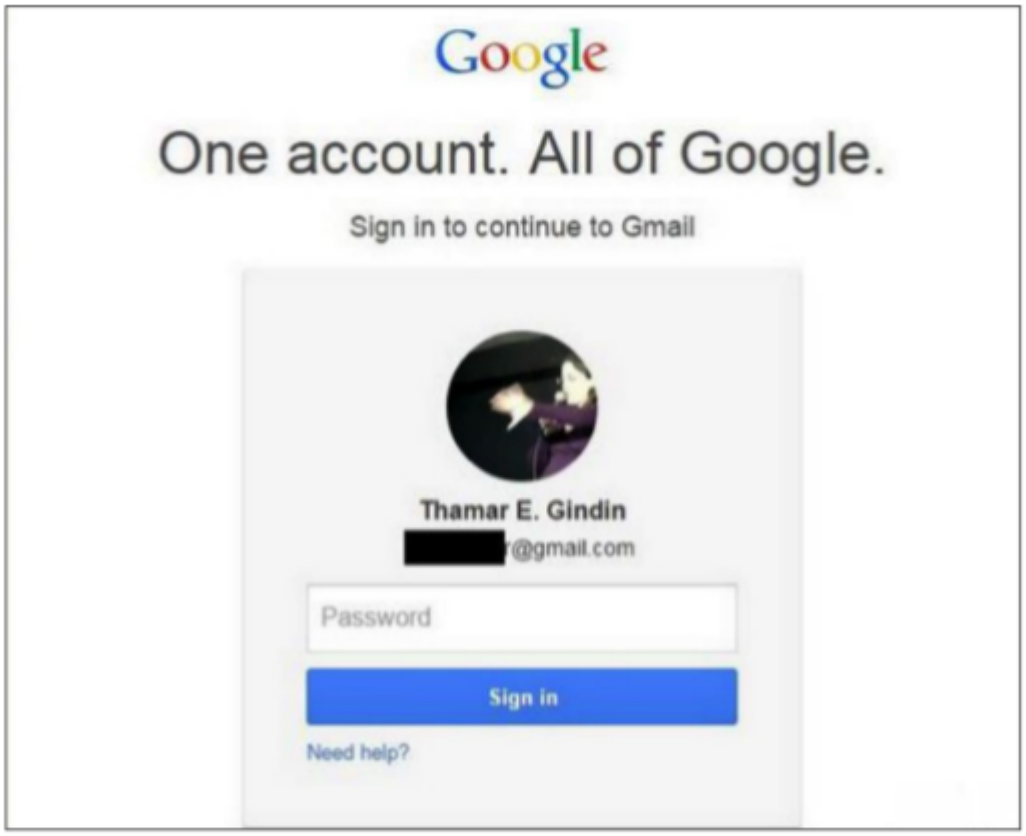


Image 6 – Custom- tailored phishing page as presented by ClearSky

Les outils & infrastructures de Rocket Kitten

La principale méthode d'attaque des rocket kitten c'est via du phishing. Une campagne de phishing bien efficace ne nécessite rien de plus qu'une page de phishing bien conçue qui est hébergée sur un serveur web.
Ils utilisent des formes variées de phishing : emails, appels téléphoniques

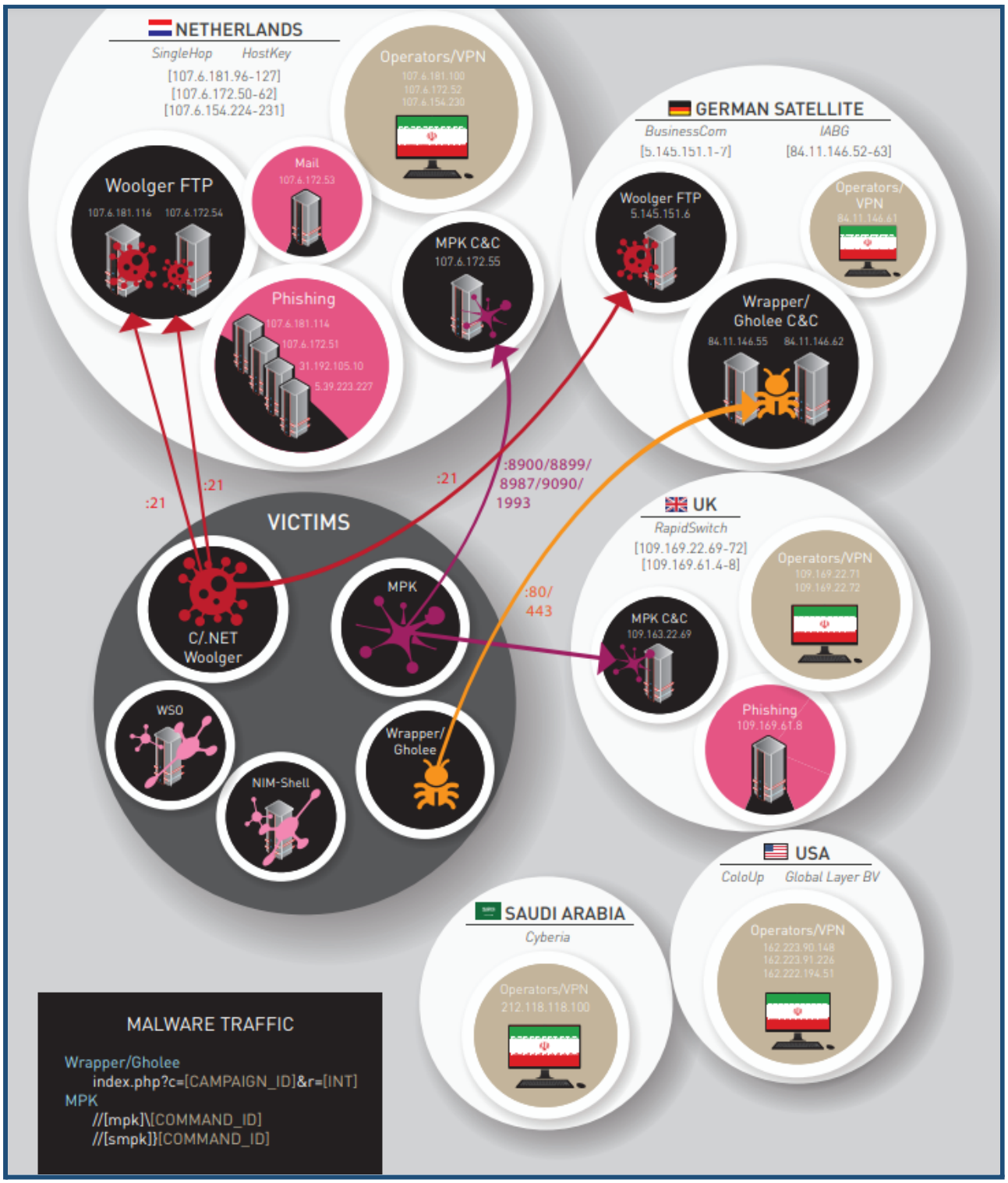
- CWoolger— un logiciel en C++ (keylogger). Il enregistre toutes les frappes sur le clavier et envoie les données sur un serveur.
- Wrapper/Gholee— un outil de pénétration de machine à distance
- FireMalv— un outil qui vole les informations d'identification. Il copie des mots de passe stockés dans Firefox.

Les investigations de Check Point ont montré grâce aux attaques, l'utilisation des outils suivants :

- .NETWoolger— un keylogger basé sur .NET. Fonctionnement similaire à CWoolger . Les attaquants alternent entre les deux outils au cas où l'un est détecté.
- MPK— un logiciel qui permet d'enregistrer les clés, l'exécution de commandes, les captures d'écran et la surveillance du trafic.

Il y a en plus d'autres outils que les attaquants utilisent pour cibler les sites Web.

- Metasploit— une plateforme d'intrusion open source. Il s'agit d'un exécutable qui permet l'accès à la machine. Cet exécutable est dans les mails de phishing des victimes.
- Havij & SQLMap— un outil d'injection SQL. Havij est basé en Iran et SQLMap est un outil open source.
- Acunetix & Netsparker— un outil de détection de vulnérabilités des sites Web.
- WSO Web Shell— un script PHP qui permet un accès au serveur et réaliser des actions dessus.
- NIM-Shell—un outil iranien similaire au WSO Web Shell. Il utilise des script Perl sur le serveur.


NETHERLANDS
SingleHop
HostKey
[107.6.181.96-127]
[107.6.172.50-62]
[107.6.154.224-231]
Operators/VPN
107.6.181.100
107.6.172.52
107.6.154.230
Woolger FTP
107.6.181.116
107.6.172.54
Mail
107.6.172.53
MPK C&C
107.6.172.55
Phishing
107.6.181.114
107.6.172.51
31.192.105.10
5.39.223.227
GERMAN SATELLITE
BusinessCom
[5.145.151.1-7]
IABG
[84.11.146.52-63]
Woolger FTP
5.145.151.6
Operators/VPN
84.11.146.61
Wrapper/
Gholee C&C
84.11.146.55
84.11.146.62
:21
:21
:21
:8900/8899/
8987/9090/
1993
VICTIMS
C/.NET
Woolger
MPK
WSO
NIM-Shell
Wrapper/
Gholee
:80/
443
UK
RapidSwitch
[109.169.22.69-72]
[109.169.61.4-8]
Operators/VPN
109.169.22.71
109.169.22.72
MPK C&C
109.163.22.69
Phishing
109.169.61.8
USA
ColoUp
Global Layer BV
Operators/VPN
162.223.90.148
162.223.91.226
162.222.194.51
SAUDI ARABIA
Cyberia
Operators/VPN
212.118.118.100
MALWARE TRAFFIC
Wrapper/Gholee
index.php?c=[CAMPAIGN_ID]&r=[INT]
MPK
//[mpk]\[COMMAND_ID]
//[smpk]}[COMMAND_ID]

Gefilte phish - best server cold

Check Point participe activement à l'enquête concernant un incident d'attaque active du groupe sur le réseau d'un client.

L'enquête est la suivante :
Pour comprendre comment l'attaque a été menée, il a fallu communiquer avec le serveur web de phishing, ils ont appris que l'adresse IP qui été utilisée est revenue plusieurs fois pour pleins de domaines malveillants.
Ils ont donc commencé à effectuer des requêtes GET sur le serveur web pour tenter de naviguer sur des pages connues.
Pour quelques réponses, un 200 OK était affiché pour le domaine /xampp.
Ainsi ils sont arrivés sur l'interface de phpmyadmin et ils ont compris que phpmyadmin avait été configuré pour permettre un accès root sans mot de passe pour tous les visiteurs.
Il se pourrait que cette configuration soit l'image d'un trou si béant. Cela ressemble fortement à un leurre.
Pourquoi des attaquants si rusés feraient preuves d'autant d'amateurisme, en laissant la base de données de leur serveur de phishing autant exposée.
La base de donnée avait le nom de **'phakeddb'**, il s'agit d'un set de tables et de dataset très croustillants pour les chercheurs de campagnes de lutte contre les logiciels malveillants.
En parcourant les tables, ils ont trouvé l'application web de phishing probablement développée par les attaquants des Rocket Kitten. Cette application génère la page de phishing personnalisée pour la cible pour les services du type Gmail, Youtube, … . Cette plateforme était nommée **'Oyun Management System'**.

Table des utilisateurs :

user_id	user_name	user_pass	user_nikname	user_created_date	user_lock	isadmin	pcount
49	admin	e10adc3949ba59abbe56e057f20f883e	super admin	2014-08-09	0	|UM|RT|P|MT|UPL|	22
50	anonymous	09d2b6cc9114ed718d9145fa40ed04f8	Anonymous	2014-08-09	0	||||||	8
51	merah	c12c563b4584be86a94dcba01aa80d0a	mire	2014-08-17	0	||||||	11
52	124	e87aa71e42c7de4780f448c8e92b50cd	razavi	2014-08-17	0	0	18
53	kaveh	46ec41ac0432182829250c0da50f89bb	kaveh	2014-08-17	0	0	10
54	ahzab	7a96925c26ec83a134f2014b77e01211	Ahzab	2014-08-20	0	||||||	40
55	attache	827ccb0eea8a706c4c34a16891f84e7b	irakli	2014-08-20	0	0	35
59	amirhosein	e89b359ba9008c1e1fda2bbe3374893e	ParsAAA	2014-08-21	0	0	10
60	john	e10adc3949ba59abbe56e057f20f883e	john	2014-08-24	0	||||||	10

Image 11—the 'users' table

Les attaquants se connectent sur la plateforme comme n'importe quelle plateforme web, dans le but de développer leur campagne de phishing. Ce serveur semble avoir été déployé en août 2014 quand tous les utilisateurs ont été créés.

Sur cette table, on voit que le hash code du mot de passe du super admin est **'e10adc3949ba59abbe56e057f20f883e'**. Les habitués de la cryptographie reconnaîtront la chaîne de caractères : **123456** (cette chaîne n'était pas la seule chaîne de caractère très simple à casser).
En regardant les utilisateurs de la database, on peut voir des noms Persans, tels que merah, kaveh, ahzan, ou amirhosein. Ces personnes étaient les potentiels opérateurs de la campagne chargé de l'ingénierie sociale et de la personnalisation d'une page de phishing pour les différentes cibles.

Table des conversations

msg_id	sndr_id	date	content	viewed
17	51	2014-09-16 03:00:00	http://syntaxmarketing.com.au/wp-content/uploads/2...	1
18	51	2014-09-17 00:00:00	https://www.youtube.com/watch?v=VZmdhwd3axw	1
22	54	2014-09-22 00:00:00	http://profiles.googel.com.inc.gs/?_schema=1326&rn...	0
24	52	2014-10-01 12:10:25	https://mail.mail2.mod.gov.af/owa/auth/logon.aspx?...	0
25	52	2014-10-05 00:00:00	https://cid-c4351db11d15e77f.users.storage.live.co...	0
26	52	2014-10-05 00:00:00	10/r	0
28	51	2014-10-26 00:00:00	https://accounts.google.com/VA?c=COm3lJn_2-CSogEQ9...	0
29	51	2014-10-29 00:00:00	Adrese asli: http://outlook.com/owa/biu.ac.il redi...	0
30	51	2014-10-29 00:00:00	http://www.youtube.com/watch?feature=youtu.be&v=-S...	0
31	51	2014-10-29 00:00:00	http://www.youtube.com/watch?feature=youtu.be&v=-S...	0
32	51	2014-10-29 00:00:00	Sign in to continue to YouTube	0
33	55	2014-10-29 00:00:00	pleaze 20 subject for me. tank you attache	0
34	51	2014-11-24 00:00:00	http://profiles.faceboek.in/loginuser/?_schema=198...	0

Image 12—the 'conversation' table

Beaucoup de messages contiennent des liens vers de nombreuses pages de phishing et parfaitement corrélés avec des pages d'attaques signalées. Ce qui prouve que cette base de données est en effet en corrélation directe avec les attaques de Rocket Kitten.

On remarque alors beaucoup de template de codes pour les pages de phishing qui inclus le descriptif de 'Victim Full Name' ou 'Victim User Name'.

req_id	req_exp	req_desc	req_exam
18	%VEA%	Victime Email Address	wool3n.h4t@gmail.com
19	%VFN%	Victim Full Name	John Kerry
20	%VAU%	Victim Avatar Url	http://exam.com/avatar.jpg
21	%DESC_1%	Description (1)	No Example
22	%DESC_2%	Description (2)	No Example
25	%VF%	Victim Family	Kerry
26	%VN%	Victim Name	John
27	%FPLT%	Fake Page Link Text (For email message)	No Example
28	%FPLU%	Fake Page Link Url	No Example
29	%VUN%	Victim User Name	wool3n.h4t
30	%EMAIL_1%	Email Address (1)	No Example
31	%EMAIL_2%	Email Address (2)	No Example
32	%VNN%	Victim Nick Name	Woolen
33	%IMG_1%	Image Url (1)	No Example
34	%IMG_2%	Image Url (2)	No Example
35	%SFE%	Supervisor Email (Fake Mail)	supervisor@ybsoft.com
36	%TMP%	Temp Value	No Example

Image 13—the 'requiretypes' table

De plus, lorsque la table project a été étudiée, une découverte importante à été trouvée. Un ‘project’ est une simple victime (via l'email) avec un lien spécifique pour lequel il serait envoyé à la victime.

De plus, on a des informations sur les logs dans une table 'projectlogs'. Elle contient des logs pour chaque visite de toute page de phishing. Ainsi avec toutes ces données on a pu récolter les analyses des activités de phishing sur une année de août 2014 jusqu'à août 2015.

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
50976	2583	</br>Page viewed on Monday 2015-08-17 At 12:27:35<...	2015-08-17	1
50993	2585	</br>Page viewed on Monday 2015-08-17 At 14:11:0</...	2015-08-17	1
50994	2585	</br>Page viewed on Monday 2015-08-17 At 14:11:1</...	2015-08-17	1
50995	2586	</br>Page viewed on Monday 2015-08-17 At 14:17:43<...	2015-08-17	1
50996	2586	</br>Page viewed on Monday 2015-08-17 At 14:17:58<...	2015-08-17	1
50997	2586	</br>Page viewed on Monday 2015-08-17 At 14:18:11<...	2015-08-17	1
51000	2586	</br>Page viewed on Monday 2015-08-17 At 14:49:6</...	2015-08-17	1
51001	2586	</br>Page viewed on Monday 2015-08-17 At 14:51:44<...	2015-08-17	1
51002	2586	</br>Page viewed on Monday 2015-08-17 At 14:51:49<...	2015-08-17	1
51003	2586	</br>Page viewed on Monday 2015-08-17 At 14:52:38<...	2015-08-17	1
51106	2573	</br>Page viewed on Tuesday 2015-08-18 At 9:4:23</...	2015-08-17	0
51107	2588	</br>Page viewed on Tuesday 2015-08-18 At 9:38:39<...	2015-08-17	1
51108	2588	</br>Data sent from victim:</br></br>submitted = 1...	2015-08-17	1
51109	2588	</br>Page viewed on Tuesday 2015-08-18 At 9:39:36<...	2015-08-17	1
51110	2588	</br>Page viewed on Tuesday 2015-08-18 At 9:39:54<...	2015-08-17	1
51111	2588	</br>Page viewed on Tuesday 2015-08-18 At 9:41:22<...	2015-08-17	1
51112	2588	</br>Data sent from victim:</br></br>submitted = 1...	2015-08-17	1
51135	2579	</br>Page viewed on Tuesday 2015-08-18 At 14:4:50<...	2015-08-18	0

Image 16 —log of every access to any phishing page on that server

En continuant d'analyser le serveur, une interface a été découverte, il s'agit de **'Webalizer'**. Elle fournit des analyses utiles, des statistiques concernant les liens fréquemment consultés. Des analyses ont permis de poursuivre l'enquête notamment avec l'accès de l'attaquant aux sites. Des headers de références ont été trouvés, ce qui mène à un chemin sur un même serveur de connexion :

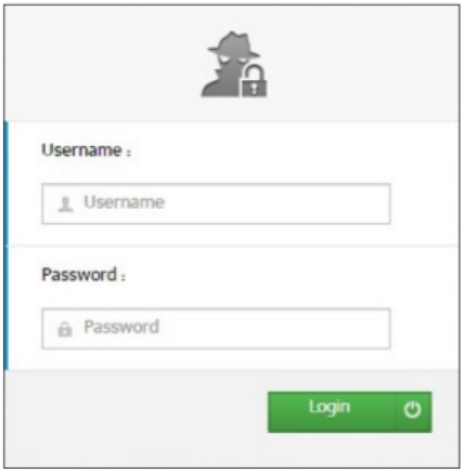


Image 18—login screen

C’est ce qui ressemble au portail d’accès secret à la plateforme de phishing. Ainsi avec l’ensemble des informations obtenues depuis le début de cette enquête il a été possible de se connecter en tant qu’administrateur :

Image 19—the “Oyun Mangement System (OMS)” [sic]

Il s’agit du système **‘Oyun’**, qui a pour photo de profil Larry Page, l’un des pères fondateurs de Google. Le reste de la page permet un accès vers la base de données ‘phakeddb’ avec une plateforme de messagerie interne comme nous l’avons vu avec la table ‘conversation’.

Woolgered

Les attaquants de Rocket Kitten avaient infecté leur propre poste de travail, pour des tests de type ‘test-run’.
En inspectant les users dans les captures d'écran enregistrées à partir d'un ordinateur infecté, un nom d'utilisateur est ressorti : 'ingénieur Balaghi'
Ensuite après plusieurs requêtes et des résultats croisés pour vérifier qu'il s'agit du même Yaser Balaghi, désormais le principal suspect de détenir l'identité Wool3n.H4T.

Yaser Balaghi, diplômé en ingénieur software, directeur technique et leader de l'équipe de développement de logiciel privé. Il sera mentionné certains projets achevés tel que le développement et la conception d'un ‘Phishing Attacks System’ commandé par une ‘cyber-organisation’

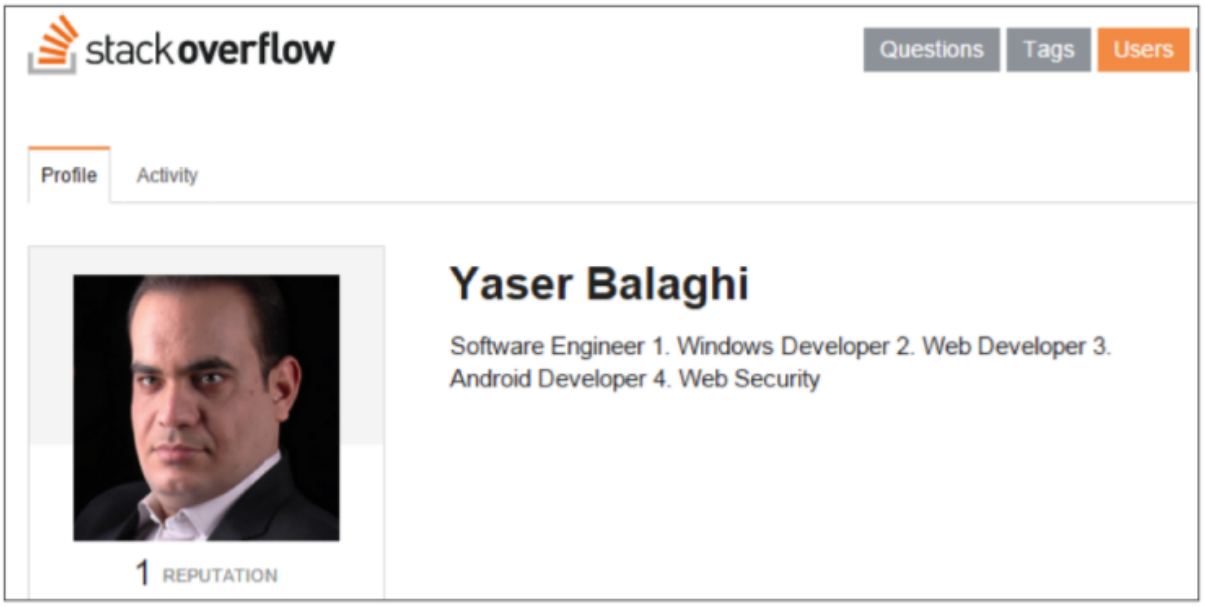


Image 30—Yaser Balaghi's stackoverflow account

Analyse des logs de phishing

Les attaquants agissent de la manière suivante : email, appels téléphoniques avec fausses identités, etc. Ils étudient leur victime avant d'agir, adaptent leur stratégie, et construisent les mails de phishing de manière minutieuse.

Il y a un cas où un attaquant a agit en utilisant la vraie identité d'un chercheur de ClearSky faisant référence à un rapport récent concernant les Rocket Kitten, en joignant un logiciel de détection qui fait exactement le contraire. Ainsi si on reçoit ce rapport avec une pièce jointe exécutable, il s'agit probablement d'un leurre malveillant.

L'analyse de la base de données met en évidence que le volume de cette base de données suggère une opération étendue, ou encore le travail d'un groupe de personnes pendant des mois. Ainsi avec les logs on a les informations concernant l'IP de visite du pays géolocalisé.

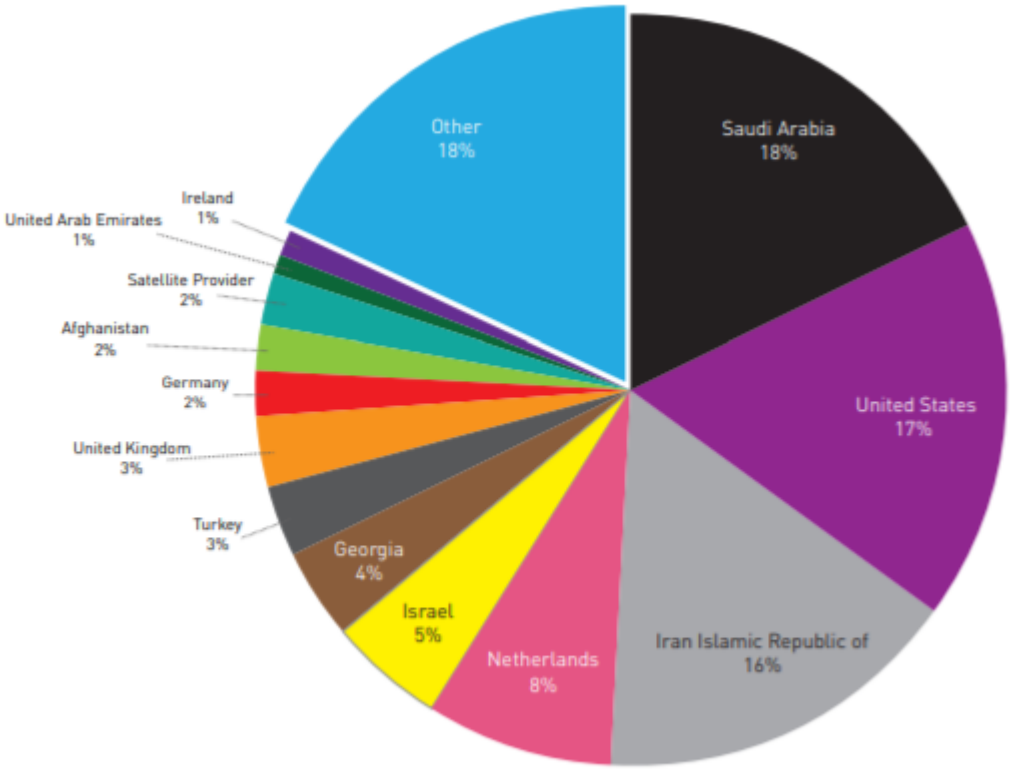


Chart 1—Phishing visitors' country distribution

On a donc la répartition suivante :

On sait que les attaquants utilisent des adresses venant de l'Iran, mais aussi des VPN depuis les Etats Unis, l'Allemagne, l'Arabie Saoudite et les Pays-Bas.
Ensuite un autre diagramme montre les logs de phishing avec les succès au fil du temps sur la période de août 2014 à août 2015:

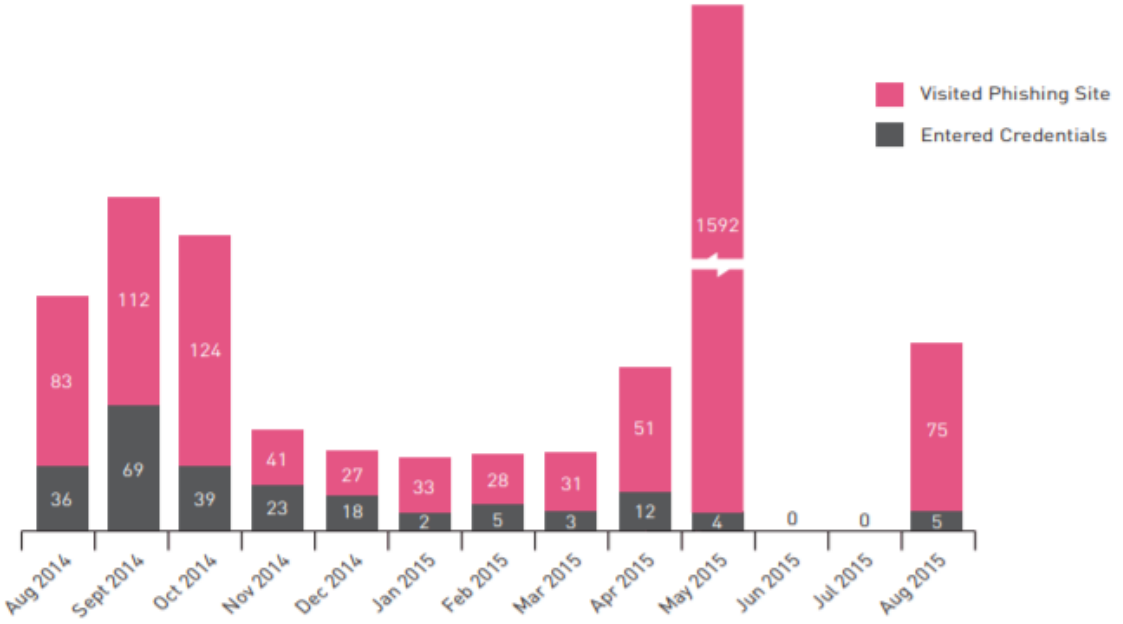


Chart 2—Phishing logs and successes over time

- ➔ En moyenne toutes les pages de phishing ont réussi à 26% à tromper les victimes pour qu'elles entrent leurs informations d'identification. On remarque que ces résultats sont plutôt élevés, ce qui prouve la pertinence de leurs cibles et les mails bien adaptés.
- ➔ En Mai 2015, on observe un pic de visite de sites avec très peu de succès. En effet, ces requêtes proviendraient d'IP Israéliennes où aucune donnée n'est fournie. Il s'agit donc des tentatives de brute-force sur les pages de phishing.
- ➔ Les attaquants semblent avoir fermé leur plateforme en juin et juillet 2015 à cause des différentes publications ayant été publiées. Ils ont repris leur activité, avec la particularité que la base de données avait été migrée à partir d'un serveur utilisé précédemment.

Conclusion :

Les attaques de Rocket Kitten est une étude intéressante pour le milieu de la recherche de logiciels malveillants. Aujourd'hui le cyberespionnage n'est plus réservé aux organisations avec des budgets monstrueux, où les équipes de hackers sont gigantesques. Maintenant, il s'agit de moyens plus simples pour contourner les failles telles que le phishing bien ciblé.

D'une part, ce sont des organismes officiels qui recrutent des pirates locaux dans le but de réaliser un espionnage ciblé au service de leur pays. D'autre part, le manque de sensibilisation à la sécurité du personnel représente un panel de possibilité pour les attaquants.

Cependant malgré les publications, les articles, les analyses de codes, les Rocket Kitten continuent à attaquer. Les changements minimes apportés aux logiciels malveillants échappent à la plupart des solutions existantes pour contrer ce genre de logiciels.
Pour stopper ces attaques il faudrait doubler d'effort en plus de l'analyse des attaques. Des mesures en coopération avec des organismes officiels pour la protection et la suppression de ce genre d'attaques seront mises en place.

Avec toutes les enquêtes, les rapports, les témoignages concernant le groupe d'attaque des Rockets Kitten on peut affirmer que ce groupe a établi une stratégie d'attaque particulièrement bien construite. C'est ce qui peut représenter une menace d'ampleur pour l'Iran, en effet avec l'ensemble des données volées et des différents outils malveillants utilisés. Il se pourrait que des personnes d'intérêt soient ciblés par d'autres groupes de cyberattaques. Il est évident que d'autres groupes émergent avec d'autres intentions, d'autres convictions et d'autres ambitions