

Denial of Service.... as a Service

Investigation and arrest of a DDoS attacker

About Me

The “call”

- Mid-sized ISP doing enterprise and personal
- Largest ISP in the geographic region
- Attacks started November 25 2012
- Started at 1 attack a week – escalated quickly
- Major outages occurred in 300km+ radius
 - Emergency services
 - VOIP
 - Chicken farms

The investigation

- Traffic would start during “business hours”
- Ramp up quickly into GB+ traffic
- Initial attack target customer of ISP
- Eventually ISP was targeted
- ISP did not use RFC 1918 addresses internally...
- Everything would go down
- VOIP conference calls going down..

Where to start?

- Logs
 - Looked for pre-attack activity from potential command and control
 - Nothing useful
- List Potential Suspects
 - One lead

The Suspect

- Network admin background
- Used to work for a company called "Concepta"
- Left Concepta to start his own company
- ... that specializes in DDOS protection
- Let's use some open source intelligence to see what we can find on the suspect
 - LinkedIn
 - Facebook
 - WHOIS
 - Message boards (always get hits on this for technical people)

Suspect LinkedIn page



Directeur Général
Canada | Technologies et services de l'informat

Rejoignez-vous sur LinkedIn et accédez au profil complet de [redacted]

Membre de LinkedIn, vous allez rejoindre des milliers d'autres professionnels qui partagent des relations et des idées et font progresser leur carrière. Et c'est gratuit ! Vous pourrez également :

- Voir qui vous [redacted] connaissez en commun
- Être présent [redacted] bis
- Contacter [redacted] tement

[Voir le profil complet](#)

Descriptif de

Poste actuel	Directeur Général chez [redacted] Inc.
Postes précédents	Administrateur Réseau chez <u>Concepta système informatique</u> Administrateur Réseau chez [redacted]
Formation	UQTR
Recommandations	2 personnes ont recommandé [redacted]
Relations	500+ relations [redacted]

Résumé de

Depuis quelques années le mot « cloud » revient partout. L'idée principale de ce service est de migrer nos données dans un endroit sécuritaire afin de ne jamais se les faire voler ou effacer par erreur. Ce nouveau concept prend beaucoup d'ampleur dans le domaine informatique et c'est avec raison. D'ici quelques années, toutes les entreprises auront migré vers ce service.

Le « cloud » offert actuellement par nos compétiteurs est très limité et non transparent. De plus, il nécessite une équipe de techniciens à votre disposition et ce en tout temps. Chez Sécurité Inc., nous avons innové et mis en place un système clé en main afin de faire profiter de ce nouveau concept à toute la population et ce avec une simplicité jamais vue.

Une fois le forfait choisi avec notre service à la clientèle, un technicien ira prendre une image des données de votre serveur, installera nos équipements de cryptage afin de sécuriser les données qui transigeront entre votre commerce et nos serveurs. Le tout prend approximativement 2 heures et se fait sans déranger vos employés. Nous assurons ensuite que chaque poste voit le nouveau serveur « nuagique », puis nous allons implanter cette image dans nos serveurs. En une demi-journée, vous pouvez dire adieu à votre serveur, à vos sauvegardes en ligne tout en vous assurant d'une redondance en cas de bris matériel et un accès en tout temps à vos dossiers, de partout dans le monde.

Ce service est aussi sécuritaire qu'une transaction à la banque. Chaque donnée étant cryptée en 256bits, soit le maximum possible mondialement et avec le meilleur algorithme possible. Notre équipement est à la fine pointe de la technologie et protège contre les attaques de type DDOS en filtrant ceux-ci.

Administrateur Réseau

Concepta système informatique

mai 2009 – mai 2012 (3 ans 1 mois) | Trois-Rivières

Hackforum & Hacksociety

- Found messages on hacker forums with “Concepta” user name
- Messages were written as a French Canadian speaking English
- Signed up November 25 2012 asking DDOS questions
- Same day as attacks started on ISP
- More activity in December 2012
- Likes “Demolition Stresser” around the exact same date and time on his Facebook

Hacksociety evidence

The screenshot shows a web browser window with the URL `hacksociety.net/Thread-Need-a-paid-botnet-for-1-week`. The browser's address bar and tabs are visible at the top. The forum page has a dark theme. At the top, there are navigation buttons for 'Buy Forum Gold' and 'TOP 10'. Below that, the breadcrumb trail reads: 'HackSociety's Forum » General Hacking » General Hacking Questions » Need a paid botnet for 1 week.' A grey bar contains the text 'Advertise your thread here' and 'Get your thread here'. The thread title 'Need a paid botnet for 1 week.' is displayed in a blue bar, followed by the date '11-26-2012, 03:35 AM' and 'Post: #1'. The user 'concepta' is identified as a 'Junior Member' with a profile picture. To the right of the user name, statistics are listed: 'Trade Count: (0)', 'Posts: 1', 'Joined: Nov 2012', 'Reputation: 0', and 'Forum Gold: 0.30'. The main text of the post reads: 'Need a paid botnet for 1 week. HI everyone, I don't have touch the hacking for a long time (sdbot on irc was my last operation). I need your help for attack a small web site without big connection or protection but with LOIC and 3-4 computer it is not enough. I can paid for this without any problem ! Please PM me if you have a nice botnet.' The name 'Andrew' is followed by a smiley face emoji. A yellow arrow points to the text 'I can paid'. At the bottom of the post, there are 'find' and 'reply' buttons.

hack society .net / Thread - Need a paid botnet for 1 week

Buy Forum Gold TOP 10

HackSociety's Forum » General Hacking » General Hacking Questions » Need a paid botnet for 1 week.

Advertise your thread here Get your thread here

reply Thread Rating: ★★★★★

Need a paid botnet for 1 week.

11-26-2012, 03:35 AM Post: #1

concepta Junior Member

Trade Count: (0)
Posts: 1
Joined: Nov 2012
Reputation: 0
Forum Gold: 0.30

Need a paid botnet for 1 week.
HI everyone,

I don't have touch the hacking for a long time (sdbot on irc was my last operation). I need your help for attack a small web site without big connection or protection but with LOIC and 3-4 computer it is not enough. **I can paid** for this without any problem ! Please PM me if you have a nice botnet.

Andrew 😊

find reply

Hackforum evidence

The screenshot shows a forum thread on Hackforums.net. The browser address bar displays the URL: `www.hackforums.net/showthread.php?tid=2996997&pid=29121309#pid29121309`. The forum interface includes a navigation bar with options like 'Désactiver', 'Cookies', 'CSS', 'Form', 'Images', 'Infos', 'Divers', 'Entourer', 'Redimension', 'Outils', 'Code source', and 'Options'. The thread title is '[FREE] DDOS/BOOTER SOURCE PACK [MediaFire]' and it has a 5-star rating. The thread options include 'New Reply' and 'Thread Options'. The first post is by user 'Ragescape' (Alpha, 1 star) dated 12-24-2012, 05:29 PM (Post #481). The post content is: 'i would really appreciate if you would give me the link and thank you in advanced and merry christmas!'. Below the post are buttons for 'PM', 'Find', 'Quote', and 'Report'. An advertisement for 'ShareCash' is displayed below the first post. The second post is by user 'swungspeedz' (Beta, 2 stars) dated 12-24-2012, 07:51 PM (Post #482). The post content is: 'Please send me this i really need this'. Below the post are buttons for 'PM', 'WWW', 'Find', 'Quote', and 'Report'. The third post is by user 'concepta' (Alpha, 1 star) dated 12-24-2012, 08:46 PM (Post #483). The post content is: 'i would like to have it. PM me please.'. A yellow arrow points to the 'concepta' user name. Below the post are buttons for 'PM', 'Find', 'Quote', and 'Report'. The fourth post is by user 'killer1434' (Alpha, 1 star) dated 12-24-2012, 09:10 PM (Post #484). The post content is empty. Below the post are buttons for 'PM', 'Find', 'Quote', and 'Report'. The forum footer includes a search bar with the text 'Rechercher: concept' and navigation links: 'Suivant', 'Précédent', 'Tout surligner', and 'Respecter la casse'.

Hackforum evidence

The screenshot shows a web browser window displaying a forum thread on Hackforums.net. The URL is www.hackforums.net/showthread.php?tid=3115781. The browser's toolbar includes various utility icons like Désactiver, Cookies, CSS, Form, Images, Infos, Divers, Entourer, Redimension, Outils, Code source, and Options. The forum interface features a thread rating of five stars and a 'New Reply' button. The thread title is 'hacking account'. The first post, dated 12-22-2012, 02:11 PM, is by user 'ahmed1ahmed1' (Alpha) and asks for a free course to hack Facebook accounts. The second post, dated 12-24-2012, 08:34 PM, is by user 'concepta' (Alpha) and states 'just read on the forum ... many post already exist !!'. A yellow arrow points to the name 'concepta' in this post. The third post, dated 12-25-2012, 11:34 PM, is by 'ahmed1ahmed1' (Alpha) and asks for a link. An advertisement for 'ShareCash' is visible between the second and third posts. The forum navigation bar at the bottom includes 'Next Oldest | Next Newest', a search box, and another 'New Reply' button.

Thread Rating: ★★★★★ [New Reply](#)

hacking account [Thread Options](#)

12-22-2012, 02:11 PM [Post: #1](#)

ahmed1ahmed1 Alpha
Prestige: 0
Posts: 11
Joined: Jul 2012
Reputation: 0

please i need free course to hack facebook accounts
please help me .

[PM](#) [Find](#) [Quote](#) [Report](#)

ShareCash
The #1 PPD Network [Make Money Now!](#) Higher Payouts than ANY other PPD network.

12-24-2012, 08:34 PM [Post: #2](#)

concepta Alpha
Prestige: 0
Posts: 12
Joined: Nov 2012
Reputation: 0

just read on the forum ... many post already exist !!

[PM](#) [Find](#) [Quote](#) [Report](#)

12-25-2012, 11:34 PM [Post: #3](#)

ahmed1ahmed1 Alpha
Prestige: 0
Posts: 11
Joined: Jul 2012
Reputation: 0

where ??
i cannot find anything .
give me link please .

[PM](#) [Find](#) [Quote](#) [Report](#)

[« Next Oldest](#) | [Next Newest »](#) [Search Thread](#) [New Reply](#)

Hackforum evidence

www.hackforums.net/showthread.php?tid=2459684&pid=29145235#pid29145235

Désactiver Cookies CSS Form. Images Infos Divers Entourer Redimension. Outils Code source Options

2K+ Sites list for FREE

12-09-2012, 09:30 PM Post: #81

H3X4G0N Beta ★★ Prestige: 5
Posts: 177
Joined: Nov 2012
Reputation: 1

May I please have these shells? I'll do anything :(Thanks in advance!

Hey there, thanks for reading my post!

>>Visit Imtiyax Forums here!<<

Please use my link :)

PM Find Quote Report

amazon Top Laptops, Tablets and Desktops
Shop Amazon.com privacy

12-14-2012, 08:54 AM Post: #82

mohamedmangeducouscous Alpha ★ Prestige: 0
Posts: 3
Joined: Dec 2012
Reputation: 0

Does can i've this ? thanks sir. e

PM Find Quote Report

12-25-2012, 06:32 PM (This post was last modified: 12-26-2012 12:17 PM by concepta.) Post: #83

concepta Alpha ★ Prestige: 0
Posts: 12
Joined: Nov 2012
Reputation: 0

thanks to give it to me. Very appreciate !

I would like to have it. Thanks in advance.

PM Find Quote Report

01-07-2013, 11:40 PM Post: #84

Suspect Facebook page

s://www.facebook.com/

facebook Search for people, places and things Robert Masse Find Friends

Timeline 2012 Highlights Add Friend

www.musiqueplus.com
Kariane est-elle vraiment atteinte d'une contamination ?

Share

updated his cover photo.

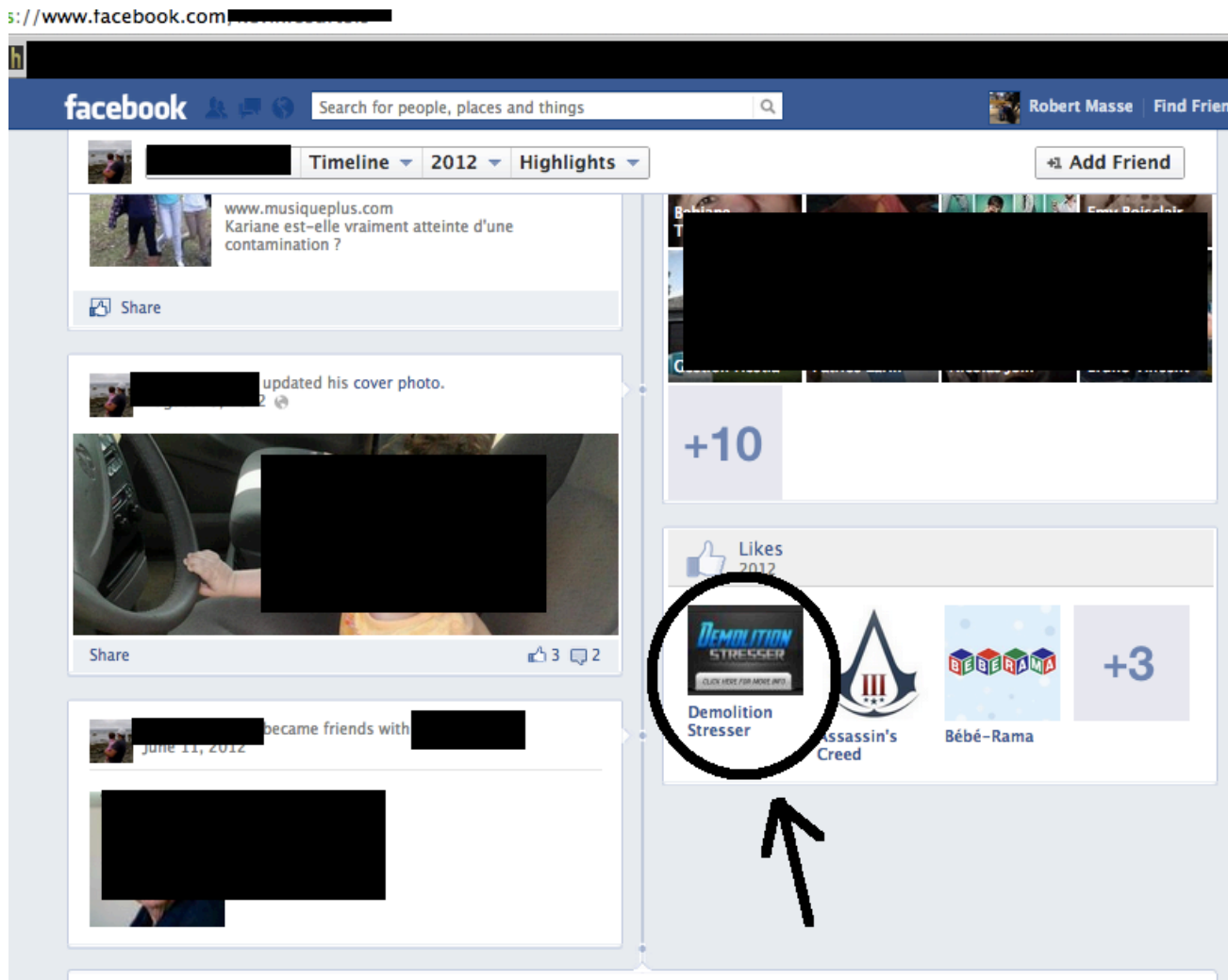
Share 3 2

became friends with June 11, 2012

+10

Likes 2012

Demolition Stresser Assassin's Creed Bébé-Rama +3



The image shows a screenshot of a Facebook profile page. The profile name is redacted with a black bar. The page features a blue navigation bar with the Facebook logo, a search bar, and the name 'Robert Masse' with a 'Find Friends' button. Below the navigation bar, there are tabs for 'Timeline', '2012', and 'Highlights', along with an 'Add Friend' button. The main content area displays a post from 'www.musiqueplus.com' with a question in French and a 'Share' button. Below that, a post shows a person updating their cover photo, with a photo of a car interior and a 'Share' button. Further down, a post indicates a friend was added on June 11, 2012. On the right side, there is a '+10' like count, a 'Likes 2012' section, and a row of app icons including 'Demolition Stresser', 'Assassin's Creed', and 'Bébé-Rama'. The 'Demolition Stresser' icon is circled in black, and a black arrow points to it from below.

Suspect Facebook page

The image shows a Facebook profile page with several sections. At the top right, there are buttons for "Ajouter" and a settings icon. The "Favoris" section is divided into "Musique", "Films", "Télévision", and "Autre". The "Autre" section contains a list of interests, with "Demolition Stresser" underlined and a yellow arrow pointing to it. The right side of the page has three sections: "Wrong" (redacted), "Autres personnes avec le nom Kevin" (redacted), and "Autres personnes portant un nom similaire" (Kevin St. Croix Schoenbohm).

Favoris

Musique

- Si l'amour te tourne le dos ,
- Major Lee

Films

- De père en flic
- Une Promenade

Télévision

- C.A.
- les Simpson
- ESPN Inside Deal
- Reboot

Autre

Parcs Québec, Microplay, Sa t'énèrve ceux qui regarde ta conversation au dessus de ton épaule :), On a qu'une vie alors il faut en profiter !!!, F*CK TON EX!, Poutine Québécoise, Rire, Feu de camps, Long Weekends, Subway, Canadiens de Montréal, Staminus Communications, Demolition Stresser, Bébé-Rama, Supers Blagues et 91 de plus

Wrong

Autres personnes avec le nom Kevin

Autres personnes portant un nom similaire.

- Kevin St. Croix Schoenbohm

Plus ▾

Demolition stresser link = Rage

The screenshot shows a web browser window with the URL <http://ragebooter.net/> in the address bar, which is circled in red. The browser tabs include "Demolition Stresser - À p...", "Rage Booter • Dashboard", "ragebooter.net Whois - r...", "RageBooter - New Them...", and "Rage Booter • Dashb...". The website header features the "Rage Booter" logo and navigation links for "DASHBOARD", "BUY NOW", and "REFERRAL SYSTEM". A dark banner at the top right contains "Live Chat", "Settings", and "Logout" options. The main content area is titled "Dashboard" and displays five statistics in a row: "4 Servers Online", "1221 Total Boots", "0 Users Total Boots", "860 Total Users", and "6 Boots Running". Below these statistics are two panels: "Added Extra Servers" with a message and date, and "Membership Info" with fields for "Name" and "Max Boot Time".

Identity Safe

Cliquez ici pour afficher vos cartes et vos identifiants Identity Safe

Live Chat Settings Logout

Rage Booter

DASHBOARD

BUY NOW

REFERRAL SYSTEM

Dashboard

4	1221	0	860	6
Servers Online	Total Boots	Users Total Boots	Total Users	Boots Running

Added Extra Servers

We added a few servers and hope you enjoy the power. Need anything let us know!

Thank You,
RAGE TEAM

On 01-12-2013

Membership Info

Name:	None
Max Boot Time:	None

Enough evidence?

- Contact local police
- Referred us to Provincial/State police
- No local expert available
- But officer was nice and sympathetic
- Unfortunately we had no “meat”
- We were on our own
- We needed more information
- Time to learn more about Ragebooter...

DDoS as a Service - awesome

- We have all heard of or been victim of DDOS
- But where do you start finding out where the attacks are coming from?
- Logs are useless
- Luckily we had an initial clue with Ragebooter
- Booters are the name for the attack tools
- Went to Ragebooter, signed up for 200\$ "Lifetime" membership!
- Messed with a few friends "testing" ...

Easy plans and pricing!

PLANS & PRICING

<p>Rage Day Trial</p> <p>\$2.50 /mo</p> <p>Skype Resolver</p> <p>Cloudflare Resolver</p> <p>Geo Ip Locator</p> <p>120 Second Boot time</p> <p>BUY NOW</p>	<p>Rage Bronze Monthly</p> <p>\$5.00 /mo</p> <p>Skype Resolver</p> <p>Cloudflare Resolver</p> <p>Geo Ip Locator</p> <p>640 Second Boot time</p> <p>BUY NOW</p>	<p>Rage Silver Monthly</p> <p>\$10.00 /mo</p> <p>Skype Resolver</p> <p>Cloudflare Resolver</p> <p>Geo Ip Locator</p> <p>940 Second Boot time</p> <p>BUY NOW</p>	<p>Rage Gold Monthly</p> <p>\$15.00 /mo</p> <p>Skype Resolver</p> <p>Cloudflare Resolver</p> <p>Geo Ip Locator</p> <p>1240 Second Boot time</p> <p>BUY NOW</p>
<p>Rage Platinum Monthly</p> <p>\$50.00 /mo</p> <p>Skype Resolver</p>	<p>RAGE ULTIMATE MONTHLY</p> <p>\$75.00 /mo</p> <p>Skype Resolver</p>	<p>RAGE OMEGA MONTHLY</p> <p>\$125.00 /mo</p> <p>Skype Resolver</p>	<p>RAGE BRONZE LIFETIME</p> <p>\$20.00</p> <p>Skype Resolver</p>

Easy to use GUI! Everyone can be Mafiaboy!

MY ATTACK LOGS

CHAT ROOM

FRIENDS AND ENEMY

SKYPE RESOLVER

STEAM RESOLVER

CLOUDFLARE RESOLVER

IP LOGGER

GEOLOCATION

BUY NOW

REFERRAL SYSTEM

Settings Logout

Stress Test Tool

Host

Port

Time

Method

- UDP-LAG
- Layer4
 - UDP
 - UDP-LAG**
 - SSYN
- Layer-7
 - RUDY
 - ARME
 - GET
 - HEAD
 - POST

SEND ATTACK

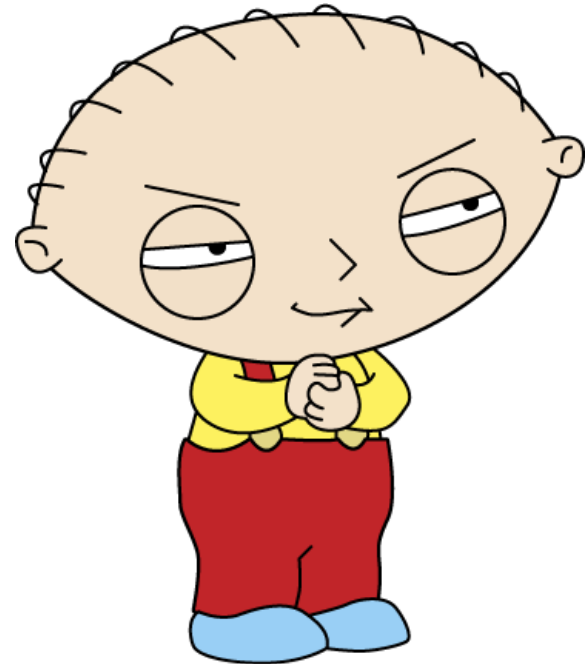
STOP ATTACK

Asymmetrical warfare

- 50\$ can take down a multi million dollar infrastructure
- 99% of my customers would be negatively impacted by RageBooter, almost impossible to stop quickly
- Even RageBooter was protected by Cloudflare anti-ddos service 😊
- Even buying all the standard “anti-ddos” equipment doesn’t defy physics
- 10GB peak of traffic is 10GB of traffic – how many companies run a 1GB Internet pipe let alone 10?
- You have to work with upstream providers

Thinking out of the box

- Sales guy from the company called “Bro, ask the guy for the logs”
- Dumb idea!
- Uuh wait..
- What did we have to lose?
- Let’s call contact customer support!



The conversation

The screenshot displays a Skype chat interface. At the top left, the contact name is 'bob stevens' with a green checkmark and the text 'Add Credit'. To the right is a search bar with a magnifying glass icon and the text 'Search'. Below the contact name, there are navigation options: 'Skype Home' and 'Contacts'. A 'RECENT' list is visible on the left side, containing three entries: a contact with a blacked-out name, 'Untitled', and 'History'. The main chat area shows a message from 'ragebooter question. bob stevens' at '7:55 AM'. The message content is partially obscured by a black redaction box. At the bottom of the chat window, there is a text input field with a microphone icon on the left and a smiley face icon on the right. A 'Call Phone' button is visible in the top right corner of the chat area.

The "ask"

The screenshot shows a Skype chat window. The contact name is redacted. The chat history includes:

- bob stevens: question for you (13-01-22 8:03 AM)
- Redacted contact: is it possible to buy a specific log entry of ragebooter.. (13-01-22 8:04 AM)
- Redacted contact: ? (13-01-22 12:23 PM)
- Redacted contact: you mean? (8:46 AM)
- bob stevens: Your system is being used to attack some specific IP addresses. I need to know the source IP that is launching these IP addresses. It might be behind a proxy but I have my doubts. Obviously I am not a cop/LE/etc as this would be useless in court. I have already made arrangements like these before on similar services and it's just a question of a price. (8:48 AM)
- Redacted contact: Discretion assured of course. (8:48 AM)
- Redacted contact: [Redacted] (8:49 AM)
- Redacted contact: I really do not give out attack logs for the safety of my clients (8:49 AM)
- Redacted contact: but (8:49 AM)
- Redacted contact: if you can tell me the ip being attacked (8:49 AM)
- Redacted contact: I would be more the happy to blacklist it. (8:49 AM)
- bob stevens: That is appreciated and I might take you up on the offer however there are several other services like yours that I believe they would switch to. The IP addresses being attacked are a small rural ISP with 13,000 customers .. they have been attacked for the last month. It's important for me in my role to stop the attacks and identify the person (once again, not for legal reasons). That being said, if you are interested, I am willing to pay - name me a price. In the meantime, I will get you the IP addresses. (8:52 AM)

The input field at the bottom contains the text: "If you can't give me the actual IP address, any intelligence about the netblock would be great. We already have an idea who it is and just identifying the netblock would help."

The "ask"

The screenshot shows a Skype chat window. The contact's name is redacted with a black box. The chat history includes several messages from the contact and bob stevens. A yellow circle highlights two redacted messages and the text 'apparently there are attacks being sent to the ips you mentioned'. The chat ends with bob stevens expressing interest in paying for information about the origin IPs.

bob stevens
Add Credit

Skype Home
Contacts

RECENT

History

RIPTS: <http://pastebin.com/dCL7GbLg>

Video Call

Sure, [REDACTED].167 (december), [REDACTED].190, 192 (january). [REDACTED]/24 actually 8:58 AM

I believe there might be an attack now 8:59 AM

For sure this morning 8:59 AM

First attack November 25 8:59 AM

[REDACTED] This message has been removed. 9:03 AM

[REDACTED] This message has been removed. 9:02 AM

apparently there are attacks being sent to the ips you mentioned

bob stevens
I saw the IPs 9:04 AM

[REDACTED]
we at this time do not log users ips who send the attacks 9:04 AM

but the ips you said have been attacked from Rage Productions 9:04 AM

bob stevens
so you do see the ips being attacked 9:05 AM

can you block the attacks asap please? 9:05 AM

[REDACTED]
I have blocked the ones being attacked 9:06 AM

bob stevens
thanks. if you ever do get the origin IPs, as mentioned I am interested in paying for the information. I appreciate your cooperation. I understand your business model and DDOS people is cool for some lulz but taking out people for a month is another story where people lose their jobs. thanks again. 9:07 AM

The "ask"

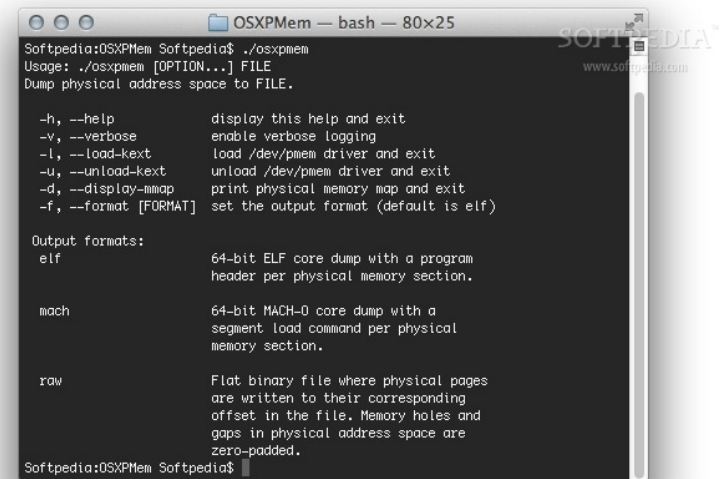
The screenshot shows a WhatsApp chat interface. At the top left, the contact is identified as "bob stevens" with a profile picture and a green checkmark, and the option "Add Credit" is visible. A search bar is located at the top right. The left sidebar shows navigation options: "Contacts", "RECENT", and "History". The main chat area contains the following messages:

- Redacted contact: [REDACTED] SCRIPTS: <http://pastebin.com/dCL7GbLg> (9:17 AM)
- bob stevens: Can you tell me the others just for my education? if not that's ok (9:17 AM)
- Redacted contact: *This message has been removed.* (9:18 AM)
- Redacted contact: *This message has been removed.* (9:18 AM)
- Redacted contact: and a fw others (9:18 AM)
- Redacted contact: *This message has been removed.* (9:18 AM)
- Redacted contact: I really cant give that info sir. Since I am banned from hf and do not know who you are it is hard for me to tell you names for the problem that you could be someone trying to figure out other stressers so you can get them banned from hf as well (9:19 AM)
- Redacted contact: sorry (9:19 AM)
- bob stevens: [REDACTED] is still being attacked (9:19 AM)
- Redacted contact: no problem (9:19 AM)
- Redacted contact: Not from our setressers (9:20 AM)
- Redacted contact: stressers* (9:20 AM)
- bob stevens: lol i am not on hf (9:20 AM)
- Redacted contact: or these sites but i respect your privacy (9:20 AM)
- Redacted contact: as long as you can block those ips I send you positive karma. (9:21 AM)
- Redacted contact: take care (9:21 AM)

A yellow oval highlights the redacted contact's messages: "and a fw others" and the two "This message has been removed." messages above it.

Asymmetrical warfare

- Our friend copy/pastes the logs into the chat as well as other Booter sites belonging to Rage Productions
- Logs included
 - Destination
 - Username
 - Attack variables
- He realizes it and deletes
- Is the chat still in memory?
- Google “dump OSX memory”
- OSXPmem looks good
- Run the tool and pray



```
OSXPmem — bash — 80x25
Softpedia:OSXPmem Softpedia$ ./osxpmem
Usage: ./osxpmem [OPTION...] FILE
Dump physical address space to FILE.

-h, --help          display this help and exit
-v, --verbose       enable verbose logging
-l, --load-kext     load /dev/pmem driver and exit
-u, --unload-kext  unload /dev/pmem driver and exit
-d, --display-mmap print physical memory map and exit
-f, --format [FORMAT] set the output format (default is elf)

Output formats:
elf                64-bit ELF core dump with a program
                   header per physical memory section.

mach               64-bit MACH-0 core dump with a
                   segment load command per physical
                   memory section.

raw                Flat binary file where physical pages
                   are written to their corresponding
                   offset in the file. Memory holes and
                   gaps in physical address space are
                   zero-padded.

Softpedia:OSXPmem Softpedia$
```

Run strings for November - bingo

The screenshot shows a Skype chat window with a contact named 'bob stevens'. The chat history includes several messages from an anonymous user (represented by a blacked-out profile picture) and 'bob stevens'. A yellow circle highlights a message that has been removed. A blue overlay on the right side of the chat displays terminal output from a 'strings' command, which includes the text 'I believe there might be an attack now' and 'First attack November 25', matching the chat messages. The terminal output also shows various system and network-related strings.

bob stevens
Add Credit

Skype Home
Contacts

RECENT
History

ESSYN ATTACK SCRIPTS: <http://pastebin.com/dCL7G>

Sure, [redacted].167 (december), [redacted].6.190, 15

I believe there might be an attack now

For sure this morning

First attack November 25

This message has been removed.

This message has been removed.

apparently there are attacks being sent to the ips you

bob stevens
I saw the IPs

[redacted]
we at this time do not log users ips who send the att

but the ips you said have been attacked from Rage

bob stevens
so you do see the ips being attacked

can you block the attacks asap please?

[redacted]
I have blocked the ones being attacked

bob stevens
thanks. if you ever do get the origin IPs, as mentioned I am interested in paying for the information. I appreciate your cooperation. I understand your business model and DDOS people is cool for some lulz but taking out people for a month is another story where people lose their jobs. thanks again.

```
I believe there might be an attack now
ph`o
+\[s
i+=t
For sure this morning
First attack November 25
^L'bL
8-)>
concepta2
7,200
01-23-2013, 02:28:46 am
0y:.U
e%\
concepta2
7,200
01-23-2013, 2:28:46 am )
BmI1
w@p9
P8%U
apparently there are attacks being sent to the ips you mentioned
`]Rt
```

9:05 AM
9:05 AM
9:06 AM
9:07 AM

Now we have enough evidence

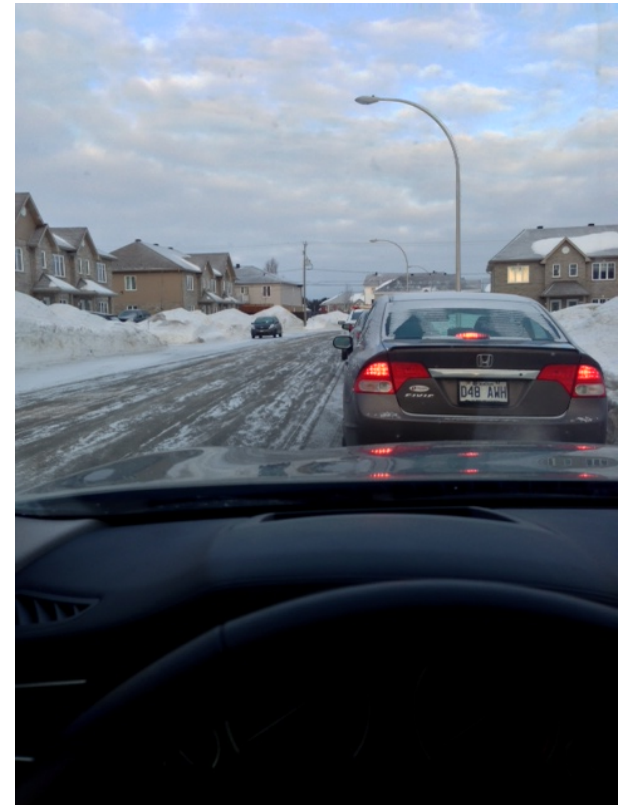
- Suspect is an ex-employee of Concepta who previously admitted to owner he has DDOS botnets
- Suspect started a new company after leaving Concepta that specializes in “DDOS protection”
- Suspect has a “LIKE” on his open Facebook page for Demolition Stresser that points to Ragebooter
- As per the admin on Ragebooter, his website is being used to attack the IPs of my customer
- We have 2 log entries that show a user “Concepta2” launching attacks against customer

Legal strategy – civil first

- After all the evidence collected, we can now act
- First step is to go the Civil route
- Anton Piller order
- A good analogy is a Civil search warrant
 - Allows you to search and seize evidence
 - Tough to get from a judge
- We were granted the order to search two locations:
 - House
 - Office (shared space)
- Judge wanted execution Sunday morning
- Off we go!

The hammer of justice

- Bright and early, -4F morning
- Each location:
 - Police
 - Bailiffs
 - Locksmith
 - Computer forensic expert
 - Lawyer of customer
 - Customer
 - Independent lawyer
 - Me
- Police show up, confirm identity with bailiff
- We go in – Bad news...



Leaked intel...

- The suspect wasn't surprised
- His wife was surprised (just annoyed)
- Suspect visited my LinkedIn 2 days before...
- What does that mean?
- How did he know?
- Set expectations with customer that he most likely wiped data
- Finished house, went to office
- Suspect smiling the whole time

Criminal investigation

- We leave the office and head back home
- The next day we get word about a crown prosecutor in Quebec who is interested in what we found
- Suspect's legal team attempts to quash the Anton Piller
- Prosecutor requests a copy of our evidence
- We went from no interest to lots of interest in 1 day
- Judge denies quashing Anton Piller, customer provides hard disk to prosecutor
- A few days later...

Perp walk



Lessons learned

- When you wipe the drive, wipe the whole drive
- Don't create accounts with your name
- Police can only do so much – you need to be proactive
- Don't "Like" web sites you use to commit a crime
- Don't pay with paypal
- Don't think you're that smart – everyone makes mistakes
- Think out of the box

Thank you!

Please fill out speaker feedback!

Contact info:

rmasse@swiftidentity.com

Follow me on Twitter [#rob_masse](#)