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

Descriptif de
Poste actuel
Directeur Général chez rice war... Inc.
Postes précédents
Administrateur Réseau chez Concepta système informatique
Formation
UQTR
Résidences
2 personnes ont recommandé
500+ relations

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 » offre 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. C Sécurité Inc., nous avons innové et mis en place un système dédié 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 transigent entre votre commerce et nos serveurs. Le tout prend approximativement 2 heures et ne 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 256 bits, 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.
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
Hello everyone,

I don't have much experience with hacking for a long time (scbot on IRC was my last operation). I need your help to attack a small website without a big connection or protection, but with LOIC and 3-4 computers. It is not enough. I can **paid** for this without any problem! Please PM me if you have a nice botnet.
Hackforum evidence
Hackforum evidence

A screenshot of a discussion thread on Hackforums with the following posts:

1. **ahmed1ahmed1**: I need a free course to hack Facebook accounts. Please help me.
2. **concepta**: Just read on the forum... many posts already exist!
3. **ahmed1ahmed1**: Where? I cannot find anything. Give me a link please.

In the background, there is an advertisement for ShareCash, which claims higher payouts than any other PPD network.
Hackforum evidence

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

Hey there, thanks for reading my post!

>>>Visit Imtiax Forums here!<<<

Please use my link :)

Does can I've this? thanks sir. e

thanks to give it to me. Very appreciate !
I would like to have it. Thanks in advance.
Suspect Facebook page
Demolition stresser link = Rage
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!

<table>
<thead>
<tr>
<th>Plan</th>
<th>Price</th>
<th>Features</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Rage Day Trial</strong></td>
<td>$2.50</td>
<td>Skype Resolver, Cloudflare Resolver, Geo Ip Locator, 120 Second Boot time</td>
</tr>
<tr>
<td><strong>Rage Bronze Monthly</strong></td>
<td>$5.00</td>
<td>Skype Resolver, Cloudflare Resolver, Geo Ip Locator, 640 Second Boot time</td>
</tr>
<tr>
<td><strong>Rage Silver Monthly</strong></td>
<td>$10.00</td>
<td>Skype Resolver, Cloudflare Resolver, Geo Ip Locator, 940 Second Boot time</td>
</tr>
<tr>
<td><strong>Rage Gold Monthly</strong></td>
<td>$15.00</td>
<td>Skype Resolver, Cloudflare Resolver, Geo Ip Locator, 1240 Second Boot time</td>
</tr>
<tr>
<td><strong>Rage Platinum Monthly</strong></td>
<td>$50.00</td>
<td>Skype Resolver, Cloudflare Resolver, Geo Ip Locator, 120 Second Boot time</td>
</tr>
<tr>
<td><strong>RAGE ULTIMATE MONTHLY</strong></td>
<td>$75.00</td>
<td>Skype Resolver, Cloudflare Resolver, Geo Ip Locator, 640 Second Boot time</td>
</tr>
<tr>
<td><strong>RAGE OMEGA MONTHLY</strong></td>
<td>$125.00</td>
<td>Skype Resolver, Cloudflare Resolver, Geo Ip Locator, 940 Second Boot time</td>
</tr>
<tr>
<td><strong>RAGE BRONZE LIFETIME</strong></td>
<td>$20.00</td>
<td>Skype Resolver, Cloudflare Resolver, Geo Ip Locator, 1240 Second Boot time</td>
</tr>
</tbody>
</table>

- **Savings**: 120 Second Boot time vs. 1240 Second Boot time.
Asymmetrical warfare

- $50 can take down a multi million dollar infrastructure
- 99% of my customers would be negatively impacted by RageBoofter, almost impossible to stop quickly
- Even RageBoofter 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!
- Uuuh wait..
- What did we have to lose?
- Let’s call contact customer support!
The conversation
bob stevens

question for you

is it possible to buy a specific log entry of ragebooster..

?

[Redacted]
you mean?

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.

Discretion assured of course.

[Redacted]

I really do not give out attack logs for the safety of my clients

but

if you can tell me the ip being attacked

I would be more than happy to blacklist it.

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.

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"

Sure, 167 (december), 1190, 192 (january), 24 actually.

I believe there might be an attack now.

For sure this morning.

First attack November 26.

This message has been removed.

apparently there are attacks being sent to the ips you mentioned.

bob stevens
I saw the IPs.

we at this time do not log users who send the attacks

but the ips you said have been attacked from Rage Productions.

bob stevens
so you do see the ips being attacked.

can you block the attacks asap please?

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.
The “ask”

bob stevens
Can you tell me the others just for my education? if not that’s ok
9:17 AM

[Message has been removed.]

I really can’t 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

bob stevens
.12 is still being attacked
9:19 AM

no problem
9:20 AM

[Message has been removed.]

Not from our stressers
9:20 AM

stressers*
9:20 AM

bob stevens
lol I am not on hf
9:20 AM

or these sites but I respect your privacy
9:21 AM

as long as you can block those ips I send you positive karma.
9:21 AM

take care
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
Run strings for November - bingo

---

**bob stevens**

**This message has been removed.**

**This message has been removed.**

---

Then, apparently there are attacks being sent to the IPs you mentioned.

---

bob stevens

I saw the IPs.

---

bob stevens

so you do see the IPs being attacked?

can you block the attacks asap please?

---

bob stevens

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 lutz but taking out people for a month is another story where people lose their jobs. Thanks again.
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 Rageboother
- As per the admin on Rageboother, 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
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...
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
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