Information Collection on DDoS Attacks

Anna Claiborne

Prolexic Technologies

Statistics

- United States Secret Service report less than 0.1% of DDoS attacks ending in an arrest
- A Major US corporation lost over 2 million in a 20 hour outage
- An Offshore gambling company lost an estimated 4 million in 3 days
- An Online payment processor lost 400 thousand in just under 72 hours
- An Online retailer lost 20 thousand per day

Basic Information Collection

- Get packet captures
- Determine the type of attack and duration (ex. SYN flood lasting 6 hours)
- Obtain a complete a list as possible of source ip addresses
- Save bandwidth graphs, flow data, pps graphs, any and all visual material relating to the attack
- Save any contact with the attacker, email, chat conversation, phone calls, etc.

Recommendations

- Have a plan! DDoS is stressful☐
- Put all attack information in a central location
- Good monitoring doesn’t have to be expensive, a simple fiber card in a 1U box can be a mirror port for a large volume of traffic
- Graphs and flow data can be retrieved from upstream

Find the Source

- Use list of source addresses, find a reputable hosting company, you may even see a friends ip
- Approach the network with the infected machine, give them as much information as possible, it can take time finding someone willing to help
- Obtaining information is dependent on who you are dealing with, be as helpful as possible
- Get information from the infected machine netstat, tcpdumps, who is logged in, web logs, access logs
- Get and save the source code responsible

Examine the Source Code

- Scripts are best, you know exactly what is going on
- Compiled code, run strings
- Best case, you can get a name or identification for who wrote it, passwords, domain names, port usage
- Worst case you can obtain information that doesn't make sense....yet

Locate Controlling Server

- Examine tcp connection table or source code to fine the controlling server
- Verify your information, scan or connect to the suspect machine
- Contact abuse where the server is hosted, explain the situation
- Have as much information possible to verify your conclusion and validate you identity
- Good luck, most abuse contacts are less than helpful
- Raises a good question: how to improve awareness and legitimate requests answered?

Hunting the Attacker (not for the faint of heart)

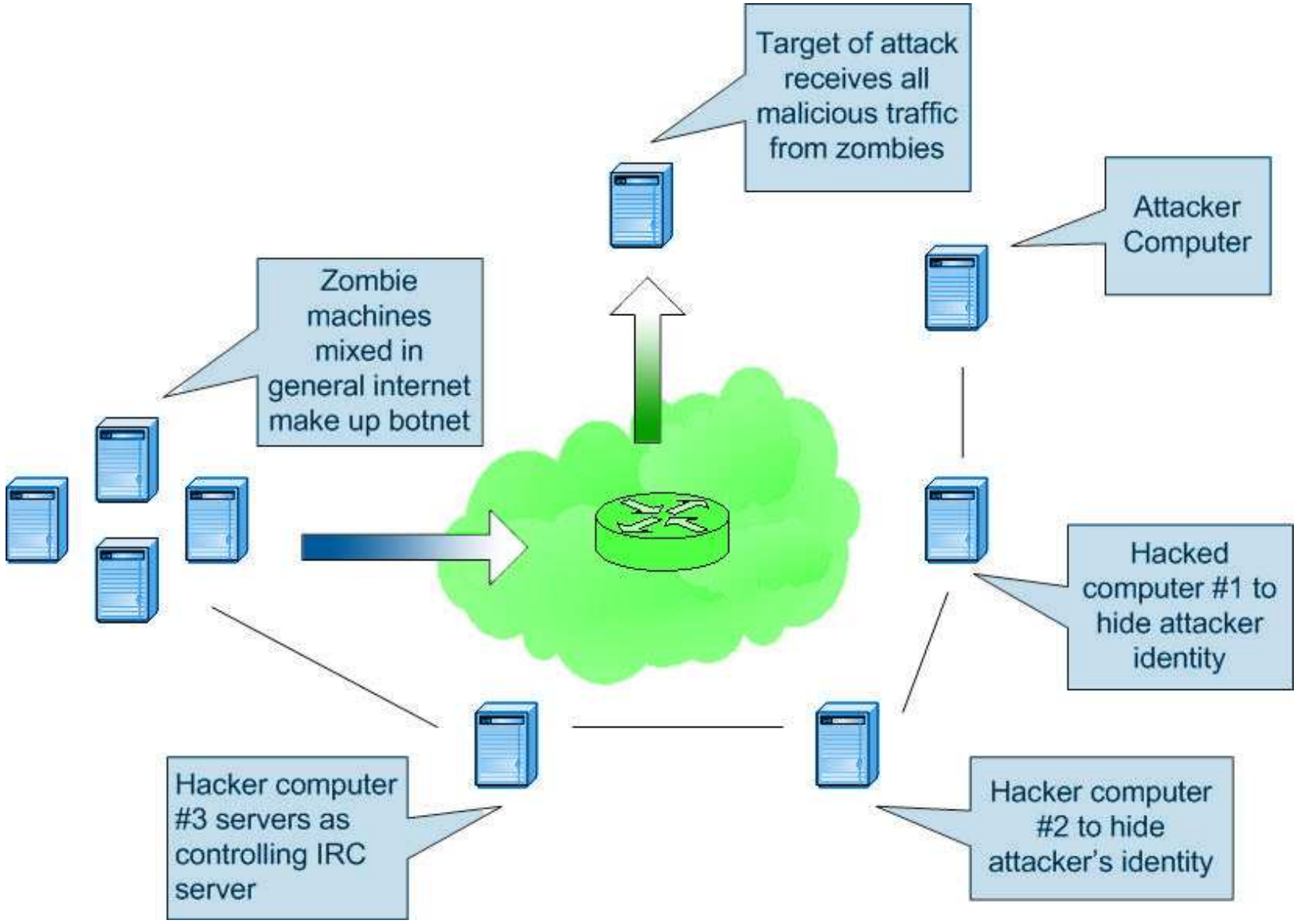
- Review all information gathered so far on the attack
- Contact the attacker, establish a report
- Save all information and/or conversations (important note, if conversations aren't on a public server, they can't be used)
- Piecing the information together to form a high level view of the exploit, attack, and attacker
- A long process, most attackers are highly motivated and skilled, you usually have to wait for them to slip up!

Resources

- Local FBI
- Department of Homeland Security
- Cert
- Cymru
- NHTCU
- Local US Secret Service
- DDoSDB.org

A Success Story

- The tracking of x3m1st/eXe
- Responsible for hundreds of extortion based □DDoS attacks
- Documented all information, tracked for months
- Lead to a successful arrest


Target of attack receives all malicious traffic from zombies
Attacker Computer
Zombie machines mixed in general internet make up botnet
Hacked computer #1 to hide attacker identity
Hacker computer #3 servers as controlling IRC server
Hacker computer #2 to hide attacker's identity

eXe's Mistake

Glenn Lembumfacil <[redacted]>

After looking at his chat information on EFNET IRC at Sat Mar 13 23:05:37 PST 2004, eXe was using the following data:

*** eXe is ~x3m1st@security-system.cc (¢Terr(0)rist][att(4)ck¢)
*** eXe is on channels #icq #conf @#xakep #moscow #ddos
*** eXe is on IRC via server efnet.demon.co.uk (Be excellent to each other.)

The domain security-system.cc is owned by:

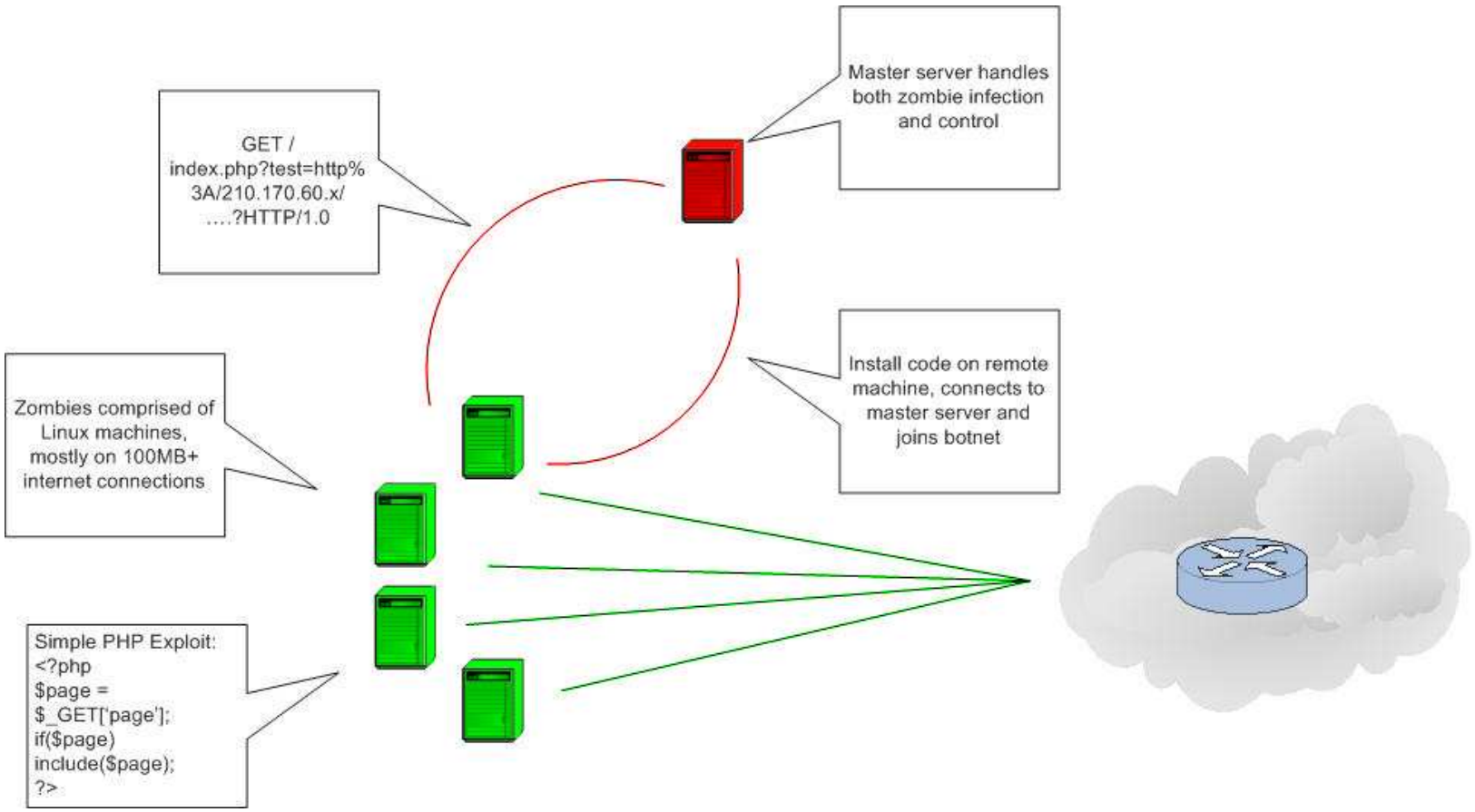
Registrant:
   Fizitheskoe lico
   Maksakov Ivan
   30 let pobedi45 43
   Balakovo, Saratovska 413864
   RU
   +7.8453323464
   Email: x3m1st@bk.ru

Ivan is the name that was given to us via eXe during ICQ chat. His last name, address, and phone number are now known.

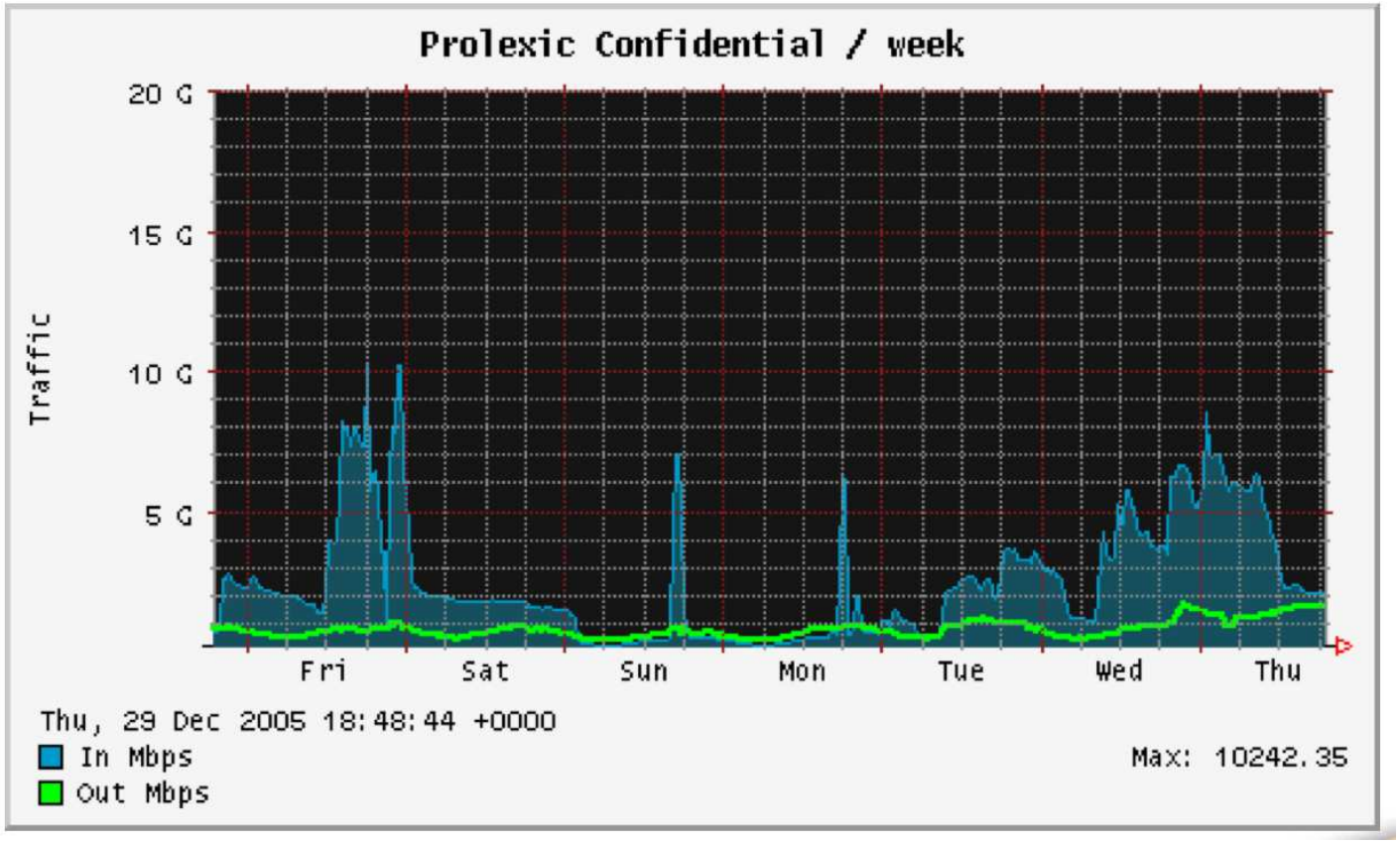
We will try to add this to our full report.

Arrests Can Happen With Through Information

Tracking Pkeglhema/aaabaa



The Result


Prolexic Confidential / week
20 G
15 G
10 G
5 G
Traffic
Fri
Sat
Sun
Mon
Tue
Wed
Thu
Thu, 29 Dec 2005 18:48:44 +0000
In Mbps
Out Mbps
Max: 10242.35

Some Conversation

[msg(aaabaa)] lame nick man
[msg(aaabaa)] :)
[aaabaa(~a@coelang.tufs.ac.jp)] yes :)
[msg(aaabaa)] hold on, mom is calling me
[aaabaa(~a@coelang.tufs.ac.jp)] well, i don't want that you come my ircd again... :)
[aaabaa(~a@coelang.tufs.ac.jp)] if you understand
[msg(aaabaa)] okay, i guess, but it was on my box
[aaabaa(~a@coelang.tufs.ac.jp)] :(
[aaabaa(~a@coelang.tufs.ac.jp)] we must share
[aaabaa(~a@coelang.tufs.ac.jp)] because i need for ddos
[msg(aaabaa)] so what site are you ddosing?
[msg(aaabaa)] i saw lots of connections in netstat to 209.200 something
[aaabaa(~a@coelang.tufs.ac.jp)] its LAME SHOP
[msg(aaabaa)] what does it do?
[aaabaa(~a@coelang.tufs.ac.jp)] they sell
[aaabaa(~a@coelang.tufs.ac.jp)] dvd shit
[msg(aaabaa)] what domain?
[msg(aaabaa)] is it movies?
[msg(aaabaa)] and if ur getting paid, i want to make some money too :)
[msg(aaabaa)] i'm sure i can help
[aaabaa(~a@coelang.tufs.ac.jp)] do u ddos then?
[msg(aaabaa)] never done it before, but i can learn
[aaabaa(~a@coelang.tufs.ac.jp)] very lot of boxes is needed for ddos...
[aaabaa(~a@coelang.tufs.ac.jp)] i think soon i run out
[aaabaa(~a@coelang.tufs.ac.jp)] and i've to stop
[aaabaa(~a@coelang.tufs.ac.jp)] but maybe with 0day
[aaabaa(~a@coelang.tufs.ac.jp)] new 0day could help
[msg(aaabaa)] i could find more
[msg(aaabaa)] i will work on it, but what can you give me?
[aaabaa(~a@coelang.tufs.ac.jp)] i must think
[aaabaa(~a@coelang.tufs.ac.jp)] if you are able to keep some shop down
[aaabaa(~a@coelang.tufs.ac.jp)] ill ask my "eployeer"
[aaabaa(~a@coelang.tufs.ac.jp)] he tell then what to do
[aaabaa(~a@coelang.tufs.ac.jp)] and pay for you
[

Pkeglhema/aaabaa - A Fish That Got Away

- Information able to be determined (employed, English second language, always logged in from university servers, etc)
- Tracked for weeks and spoke aaabaa with for weeks, never slipped
- Difficult to obtain further information due to the countries involved (China, Japan)
- End result turning over all information gather to the FBI for continued investigation

Matters to Address

- Better abuse contacts, perhaps one specifically for DDoS?
- Centralized repository specifically for DDoS profiling
- Information gathering is extremely resource intensive, but worth it
- Null routing ip space due to large amounts of outbound malicious traffic is not a good option
- DDoS is everyone's problem, get more ISPs involved in information gathering