Drawing the Foul

Operation of a DDoS Honeypot

Damian Menscher, Google
Information Security Triad

Confidentiality

Integrity

Availability

Where's the love?
Site Reliability Engineers
Look! Graphs!

Look! Spikes!
Considerations
Pipe size not to scale.
GET / HTTP/1.1
Host: www.google.com
User-Agent: I AM BOTNET

GET / HTTP/1.1
Host: www.google.com
User-Agent: I AM BOTNET

GET / HTTP/1.1
Host: www.google.com
User-Agent: I AM BOTNET

Application Layer: kqps
Attack Trends
Russo-Georgian War Anniversary

Twitter crippled by denial-of-service attack
Microblogging service says it's recovering but still defending itself against the attack. Facebook has also confirmed it was targeted by a DoS attack.

botnet
08/2009

Georgian blogger Cyxymu blames Russia for cyber attack
Blogger claims attack on Twitter, Facebook and LiveJournal was part of plot to silence his criticism of the Kremlin
Russo-Georgian War Anniversary

(600 kqps)

Capital One Targeted Again in Cyber Attack Spree

Customers reporting BofA website problems

botnet 08/2009

servers 09/2012

BroBot Attacks US Banks

(125 Gbps)

BB&T
October 17, 2012

BBT.com is experiencing intermittent delays and outages. We apologize for the inconvenience and assure you that your accounts and personal information remain secure. Please know that we are working diligently to restore service as soon as possible.
Russo-Georgian War Anniversary

(600 kqps)

botnet 08/2009

servers 09/2012

DNS amp 03/2013

Russo-Georgian War Anniversary

(600 kqps)

BroBot Attacks US Banks

(125 Gbps)

Spamhaus Attack

(300 Gbps)

The DDoS That Almost Broke the Internet

27 Mar 2013 by Matthew Prince.
Russo-Georgian War Anniversary (600 kqps)

BroBot Attacks US Banks (125 Gbps)

Spamhaus Attack (300 Gbps)

Google says Chinese Great Cannon shows need to encrypt web

China's Great Cannon vs. GitHub (400k IPs)
- Russo-Georgian War Anniversary (600 kqps)
- BroBot Attacks US Banks (125 Gbps)
- Spamhaus Attack (300 Gbps)
- China's Great Cannon vs. GitHub (400k IPs)
- Javascript 04/2015
- IoT 08/2016

Timeline:
- botnet 08/2009
- servers 09/2012
- DNS amp 03/2013
- javascript 04/2015
- IoT 08/2016
Moore's Law: Up and to the right
Defense
Shield servers protect the origin
Google Cloud HTTP(S) Load Balancing protects Shield
Google Cloud

Origin Server

Shield

Load Balancer

Network
Assembling the pieces ...
Meet Brian Krebs

Krebs on Security
In-depth security news and investigation

25 Reports: Liberty Reserve Founder Arrested, Site Shuttered
MAY 13

18 Sources: Target Investigating Data Breach
DEC 13

29 True Goodbye: ‘Using TrueCrypt Is Not Secure’
MAY 14

19 Online Cheating Site AshleyMadison Hacked
JUL 15
It's looking likely that KrebsOnSecurity will be offline for a while. Akamai's kicking me off their network tonight.
“I spoke with multiple DDoS mitigation firms. One offered to host KrebsOnSecurity for two weeks at no charge, but after that they said the same kind of protection I had under Akamai would cost between $150,000 and $200,000 per year.

A number of other providers offered to help, but it was clear that they did not have the muscle to be able to withstand such massive attacks.”

Brian Krebs
The Democratization of Censorship
Unknown threat to primary business
Unknown Attack Volumes
Can others help
How can we help
Public Relations concerns

Opportunity to find out
Opportunity to measure
Most are afraid of the risks
Existing product offering
Nothing to lose (no expectations)
Domain Name: KREBSONSECURITY.COM
...
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
Domain Status: serverDeleteProhibited https://icann.org/epp#serverDeleteProhibited
Domain Status: serverTransferProhibited https://icann.org/epp#serverTransferProhibited
Domain Status: serverUpdateProhibited https://icann.org/epp#serverUpdateProhibited
...
Name Server: NS-CLOUD-D1.GOOGLEDOMAINS.COM
Name Server: NS-CLOUD-D2.GOOGLEDOMAINS.COM
Name Server: NS-CLOUD-D3.GOOGLEDOMAINS.COM
Name Server: NS-CLOUD-D4.GOOGLEDOMAINS.COM
Brian Krebs vs. Mirai Botnet

Come at me, bro.
130Mpps SYN flood + 60Mpps of RSTs

@briankrebs · Sep 24
KrebsOnSecurity.com should be coming back up gradually now and over the next 48 hours.
130Mpps SYN flood +
60Mpps of RSTs

250kqps Mirai attack
from 145k IPs
130Mpps SYN flood + 60Mpps of RSTs

40Gbps TCP flood

250kqps Mirai attack from 145k IPs

140Gbps DNS amplification attacks

4Mpps SYN-ACK flood
130Mpps SYN flood + 60Mpps of RSTs

14 mins

40Gbps TCP flood

140Gbps DNS amplification attacks

15 mins

4Mpps SYN-ACK flood

1 hour

250kqps Mirai attack from 145k IPs

140Gbps DNS amplification attacks

4 hours

450kqps Mirai attack from 175k IPs
Cache-busting attacks, WordPress pingback attacks, DNS attacks, HTTP/UDP/POST/GRE floods oh my...

130Mpps SYN flood + 60Mpps of RSTs

250kqps Mirai attack from 145k IPs

40Gbps TCP flood

140Gbps DNS amplification attacks

4Mpps SYN-ACK flood

14 mins

15 mins

1 hour

4 hours

And on...

450kqps Mirai attack from 175k IPs
Lessons
Defending a small site ... is hard.
I got 99.999 problems

but availability ain't one.
Shared debugging

... Is hard.
Who is Anna-Senpai, the Mirai Worm Author?
Questions?