Defense against Rapidly Morphing DDOS
**Santana and Yakou botnet services**

[*] SPOT PRICE

* Spot: 10% for 500 sec attacks and 60 sec cooldown
  custom spot: if you need a specific attack duration or cooldown just hmc (the price will go up, don't be surprised)
  offer: give us 1 server and you will get a free spot! (120 sec attack and 300 sec cooldown)

[*] SOURCE PRICE

* 10$ for build [must provide server]
  25$ for source

[*] BOTNET INFO

* hitting more than 40gb (tested with a 40gb nfo) and power is still going up!

[*] CONTACT

* Santana#9421
  or
  yakou#2850 [always on]

[*] PAYMENT METHODS [USD only]

* PayPal
  * Bitcoin

[*] NOTE: BE READY WITH THE MONEY, YOU CAN ASK QUESTION BUT DON'T BE TOXIC

---

**OTHER SERVICES**

---

* Contact Yakou for this, my discord is yakou#2850

  * qbot setup = $3 (you must provide the source)
  * mirai setup = $6 (you must provide the source)
  * zmap setup = $4 (it's ok i already have the files)
  * [MUST PROVIDE SERVER (2CPU AND 4GB)]

COMING: I will sell digital ocean accounts with 1000$ credit on them
COMING: Might sell some vps for 2cpu and 4gb for 25 (digital ocean)
DOS Busters

Mudit Tyagi
Architect,
F5 Networks
m.tyagi@f5.com

Mikhail Fedorov
Engineer,
F5 Networks
m.Fedorov@f5.com
Model T-1000

A mimetic poly-alloy. Liquid metal.
Rapidly morphing...
...multiple attack vectors...
...changes within minutes.
SODA for Red Team

SODA

TARGET

L7 attacks on 'OPEN' ports
Stateful Attacks
Valid Sources of BOTs

L3/L4 Floods
FW busy 'DENYing'
Stateless Attacks
Random Sources
Tools for Blue Team

Static Vectors
Manually generated RegEx
Packet Capture Analysis
Packet Capture Tool recommendations

Too slow for morphing attacks
False Positives
Tools for Blue Team

Much faster than human

False Positives
Tools for Blue Team

- Much faster than human
- Low False Positives
- Mitigate only with proof of harm
SODA Sleeping

- User Latency
- Attacker Traffic Volume
- Firewall CPU Load
- Backend CPU Load
- Completed HTTP Requests
SODA sends morphing L3/L4 attacks

“…network layer floods kill infrastructure…”
ML defends using L3/L4 Predicates

"... ML takes only few seconds to prevent network floods..."
SODA sends morphing L7 attacks

User Latency

Attacker Traffic Volume

Firewall CPU Load

Backend CPU Load

Completed HTTP Requests

“…app floods kill backends directly…”
ML defends using L3/L4 Predicates

“...L3/4 Signatures are too wide for app level attacks...”
ML defends using L7 Predicates

ML takes only few seconds to prevent app level attacks…
If you can beat SODA, you are doing well!

- Must check DOS posture using morphing attacks
- Layers 3/4 signatures are too broad for L7 attacks
- Anomaly detection mechanism needs supervision
Intelligent Mitigation

1. Tell the clients to slow down
2. Use Dynamic Signatures
3. Human vs. BOT
4. Drop the slow connections
5. Drop sessions with heavy URL
6. Rate limit most active source IP
7. Rate limit heavily used URI
8. Rate limit based on CPS/TPS/BW
Thank You

Mark Campbell
Product Marketing at F5 Networks

Rachael Haaland
Product Marketing Intern at F5 Networks

Sara Boddy
Director of F5 Labs at F5 Networks

Lidia Giuliano
BHUSA Speaker Coach
Questions?

Contribute to SODA here: https://github.com/464d41/soda

Mudit Tyagi
m.tyagi@f5.com

Mikhail Fedorov
m.fedorov@f5.com
Mikhail Fedorov is a security expert focused on researching DDoS attacks and effectiveness of available detection and mitigation techniques. In his previous project, Mikhail worked on crafting tools to perform penetration testing for evaluating WAF technologies. He has a masters in Physics and a Bachelors in Information Technology, from Tomsk State University, and also has CCDA, CCNP, and CCNP Security certifications. Prior to working at F5, Mikhail designed and implemented secure application infrastructure as a consultant at Depo Electronics, a system integrator in Russia.
Mudit Tyagi is a Strategic Architect with the F5 Product Management team. He has 20 years of experience in Software Engineering and System Architecture design for delivery of secure applications for Financial and HealthCare services. In his current role at F5, Mudit advises CIOs and Enterprise Architects in the use of Cloud and Open Source Technologies, emerging trends such as Software Defined Networking, and modern API based application architectures utilizing microservices. He works with CISOs to evaluate strategies for delivering secure applications. Prior to F5, Mudit was the Founder and CEO of Confiserve, a secure application development firm focused on Financial Services and HealthCare. Mudit was also an early employee at various Networking and Security startup companies including Rapid City(BayNetworks), Nevis Networks(Qualys), Damballa Networks(Core Security), Inkra Networks(Cisco). He has Bachelor's degrees in Physics and Electrical Engineering from Columbia University and a Masters in Computer Engineering from University of New Mexico.