godaddy.com

Make a name with us!

Botnet Mitigation

Ben Butler
Director of Network Abuse
GoDaddy.com
bbutler@godaddy.com

Botnets

- Go Daddy recognizes the position Registrars are in as a choke point for abuse.
- Registrar-based efforts are usually focused on Botnet C&C domains.
- SOC attempts to identify suspect traffic connections and malware in hosted environment.
- Historically, most efforts start with Security groups, AV, Researchers, etc.
  - We have to make sure the evidence and documentation are sound
  - Have an understanding with 3rd party should legal actions arise as a result of our actions

Malicious A-Records

- Compromised customer accounts with legit domains
- New A-records created directing to Malware, etc.
  - IP's used to create records changes extremely quickly.
  - Use of Botnets, supsected use of TOR nodes and Socks5Proxies as well.

Malicious A-Record Mitigation

- Identify and disable malicious records
- Two-ended Blocklist
  - Deny DNS changes attempting to resolve to internal list of malicious IP's
  - Deny any future changes to any domains connection IP's
- Contact customers to encourage better security
  - Change / Stronger passwords
  - Scan for key-loggers and other malware
- Relatively effective in mitigating threats like Redkit, Blackhole Exploit kit(s).

Mitigation - What We Need

- Evidence that shows connection between malicious activity and the GD Service(s) involved.
  - Log Files
  - Packet Captures
  - Research Tools
  - How can we re-create or verify?

What We Don't Need

- Emails like this.

From: xxxxxxxxxx

Subject: Possible botnet 72.167.137.190

Message:

"Something bad going on here. Please check it out"

Fast Reponse Factors

- Emails always required to start investigation, but follow up calls to 480-624-2505 (Option 2) are always appreciated.
- Provide as much evidence as you can.
- Be patient, not combative. We are on the same team.
- Evidence should be clear and easy to follow.
  - May need to be shared with customer if legit domain / website has been compromised
- Needs to be something we can rely on. (When the excrement strikes the rotating ventilation device)
- Consider willingness to talk to the legit customer directly.
- Understand that we cannot keep a domain down ***forever*** without a court order.

Sinkholing

- Requests from AV, Security Vendors, Researchers, Law Enforcement, etc.
- Issues with multiple requests from different parties for the same domain
- Currently handled on “First come, First serve” basis, assuming we can establish legitimacy.
- Will disclose the previous sinkhole request with later parties

FLAME On!

5/25 – 5/28 2012

- GD Abuse contacted by Kaspersky concerning a few .INFO and .IN domains requesting sinkhole.
- SOC blocks purchase / setup IPs
- Point DNS of C&C domains to target IP for monitoring by Kaspersky.
- Data shared with Go Daddy

FLAME On!

- Requests for many of same domains from ESET, Symantec, Spamhaus.
- Requests for domains not requested by Kaspersky directed to respective sinhole IP's.
- Other domains in Botnet identified from captured traffic and suspended.

Contact Info

New Email Addresses:

Malware@GoDaddy.com

Phishing@GoDaddy.com

Botnet@GoDaddy.com

When in doubt:

Abuse@GoDaddy.com

Phone:

480-624-2505 (Option 2)