APWG Malicious Domain Suspension Program

Mike D'Ambrogia – eCrime Exchange Lead Developer

Puerto Rico, October 2012

The AMDoS Program

APWG Malicious Domain Suspension

- Designed to create trusted relationships where none/few currently exist
- Major user roles: Interveners and Registry
- Benefits
  - Speed and Scalability
  - Trust based process
  - Tracking
  - Auditability
  - Metrics
  - False positives = 0%

The AMDoS Program

- What is the difference between DBL/UBL and an AMDoS?
- What kind of domains can be reported?
  - Maliciously registered domains
    - Registered specifically to perpetrate phishing, malware distribution, or some other form of criminal behavior

AMDoS Roles

- New users are invited into the eCrimeX system by enrollment manager
- Builds the community via trusted relationships
- Approved users within the system are granted a 'Role' which control their possible actions
- Interveners
- Registries
- Enrollment Manager
  - Accreditation Committee

Interveners

- Eyes in the field
- Users are extensively vetted prior to being promoted into the role
- Interveners report the malicious domains
- Using AMDoS, Interveners can be trusted by the Registries
- A notification with supporting information is submitted into ECX by the Intervener, and sent electronically to the registry in question

Who are Interveners?

- Large corporate entites
- Security outfits
- Users within Institutions targeted by criminals

Becoming an Intervener

- Completed Application Form
- Articles of Incorporation
- Certificate of incorporated entity's good standing in incorporated entity's jurisdiction
- Government issued IDs of employee representing applicant
- Manifest of employment status by applicant's company on employer's letterhead
- Commercial insurance policy, with current proof of good standing
- Accredited Intervener Participation Agreement

Domains Eligible for Suspension

- For use only with maliciously registered domains, i.e. domains registered specifically to perpetrate phishing, malware distribution, or some other form of criminal behavior
- Not for use with compromised/hacked domains
- Indicators of bad intent include:
  - Domain registered recently
  - suspect WHOIS data
  - The bad domain strives to spoof a financial institution's legitimate domain, or mimic well-known banking keywords.
  - No legitimate content has ever been associated with the domain.
  - Uses nameservers with a high reputation (usually 100%) for previous fraudulent domains.
  - Etc.

Manual Suspension Request

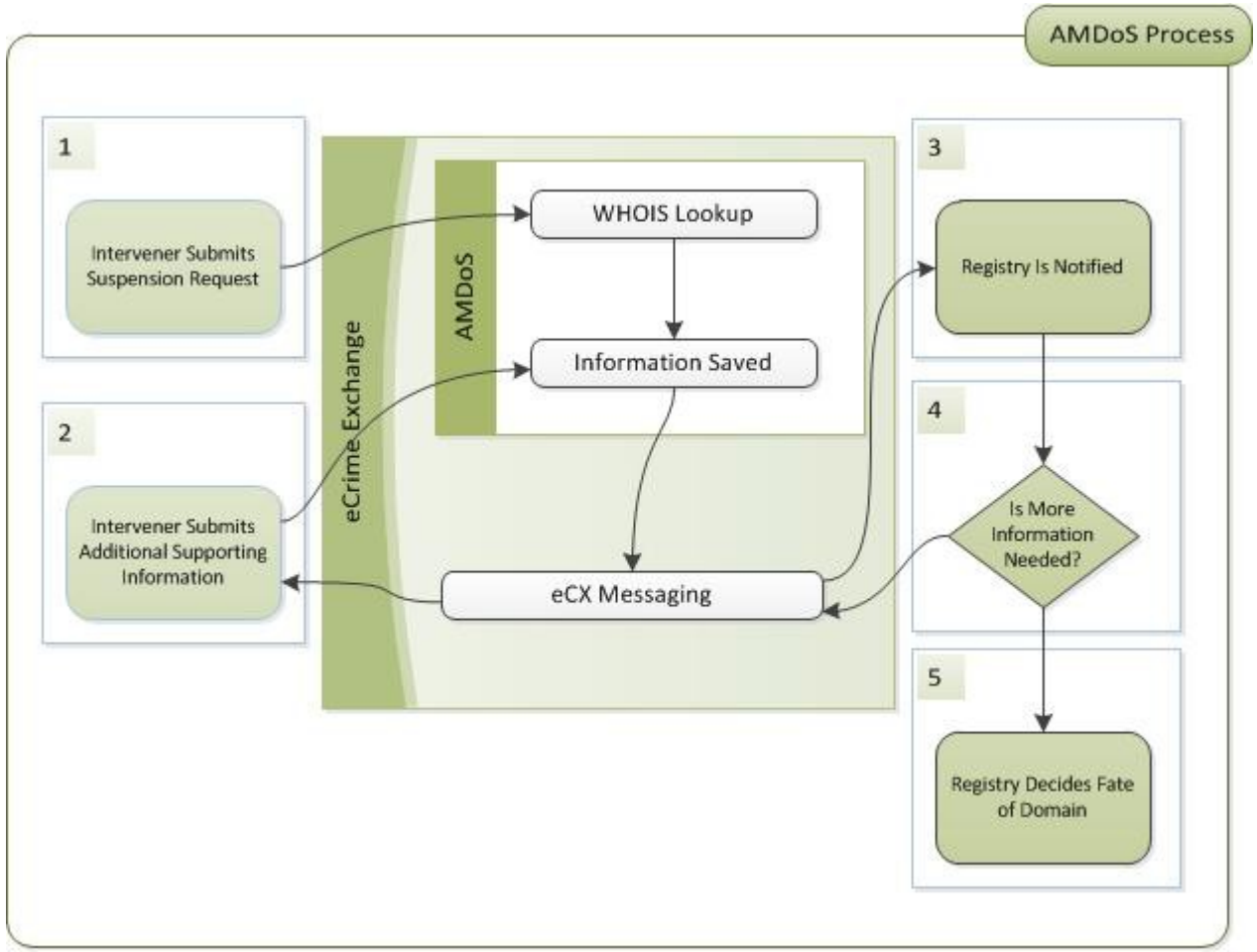
- Ad hoc email or phone call made between responders and Registries that may or may not know each other and probably don't have clear, shared criteria for suspension

- Works, but dependent upon ad hoc, experiential trust channel

- Can't be scaled

- Can't be accelerated

- Can't be audited systematically


AMDoS Process
1
Intervener Submits Suspension Request
2
Intervener Submits Additional Supporting Information
eCrime Exchange
AMDoS
WHOIS Lookup
Information Saved
eCX Messaging
3
Registry Is Notified
4
Is More Information Needed?
5
Registry Decides Fate of Domain

AMDoS Process
Registry View

- Registry user is notified that a suspension request is waiting at the eCrimeX website
- Registry user reads the attestation and examines the criteria within the submission
- Registry user can reject, suspend, or request more information from the Intervener

AMDoS Suspension Request Process Benefits

- Rigorous
- Routinizable
- Scalable
- Auditable

Suspension Demo

- Submit suspension request as an Intervener
- Understand how the registry side works

In closing...

- Ongoing tuning/enhancements of the application as we continue to get reactions from Interveners and Registries to make ongoing enhancements as relevant to user needs as possible
- Feedback, suggestions, usage scenarios, et al are incredibly important now, and in the future
- We're learning what we don't know
- Please consider getting involved

Mike D'Ambrogia - mike@apwg.org