CYBER SECURITY DIVISION

2013 PRINCIPAL INVESTIGATORS'

Introducing MESS

Telesis/Endeavor

Will Hickie

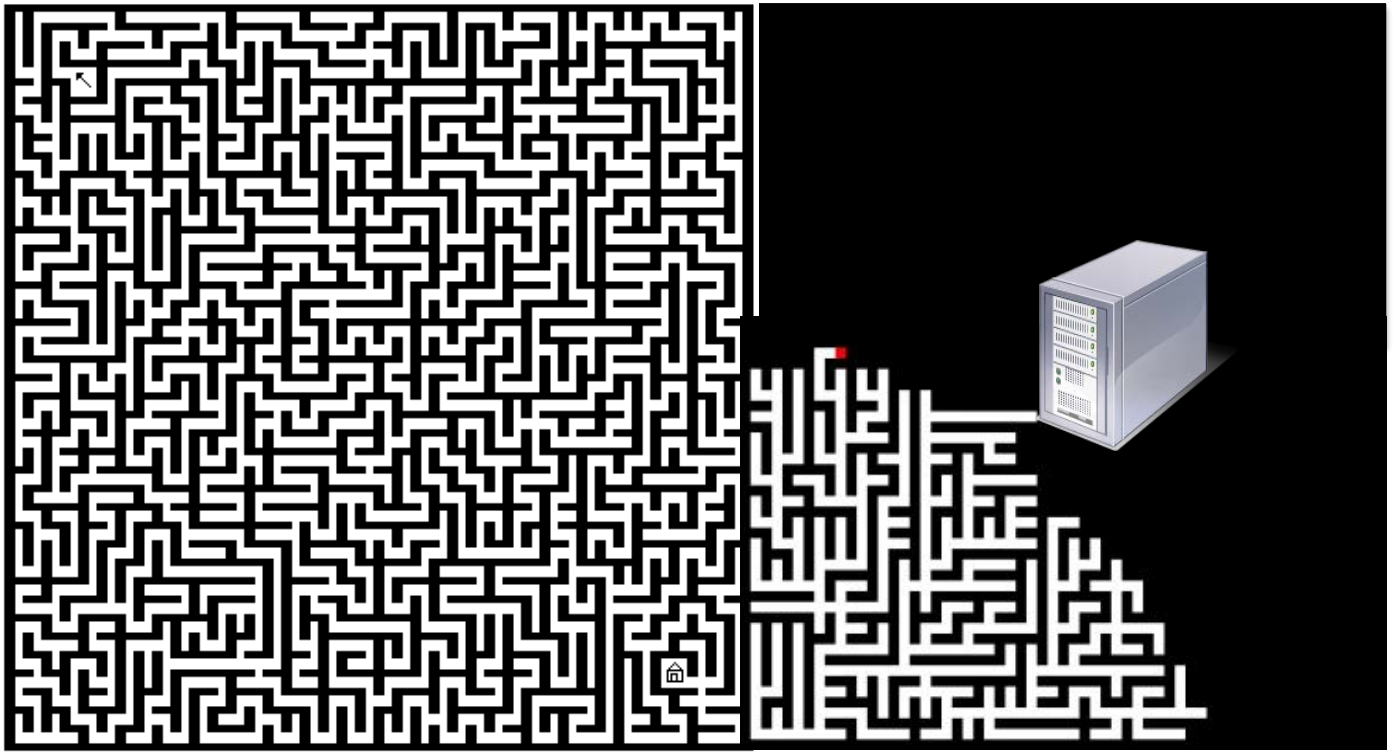
September 16, 2013

Homeland Security

Science and Technology

What is MESS?

- **M**ulti-layer, **E**ver-changing, resilient **S**elf-defense **S**ervice



Telesis/Endeavor

Established 1998
Headquarters in Beltsville, MD
- Beltsville, MD *(TS Cleared)*
- Colorado Springs, CO *(DHHS Level 5 Cleared)*
- Mclean, VA
- Cincinnati, OH
- Ft. Hood, TX

SDB; WOSB
200+ Professionals
DoD TS Cleared
CONUS and OCONUS Presence
DELTEK Accounting System
Debt Free; $5M Line of Credit
DUNS: 03-341-6244
CMMI Level 2 Appraised
ISO20000:2011; ITMS575932
ISO9001:2008
ITIL and PMP Trained / Certified

2011 TECH 200 WINNER

Inc. 500

TOP WOMEN BUSINESS OWNERS 2010

Customer Need

- Attacks happen

"*Washington confirms Chinese hack attack on White House computer*" -- FoxNews

"H*ackers steal U.S. weapons systems designs, report says*" – NBC News

Customer Need

- Attacks happen, even with:
  - Virus scanners
  - Malware scanners
  - Fire Walls
  - VPNs
  - Two-factor authentication
  - Educated users
  - Etc…

MESS: What it does

MESS interrupts attacks in different phases of the mission.

- Disrupt attacks during reconnaissance

  Be more like a submarine and less like a castle.

- Disrupt attacks after payload delivery

  Assume the zero-day exists.

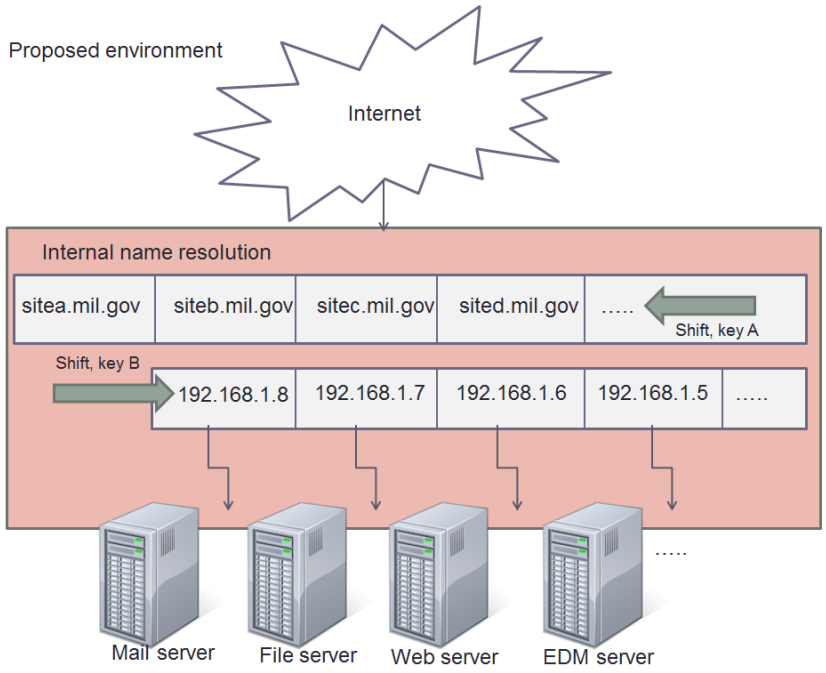
MESS: Protecting interfaces

Step 1. Public Interface Obfuscation

IP and Port numbers change every minute;

65535 port combination
* 255 IP combinations

16.7 million places a service can hide each minute

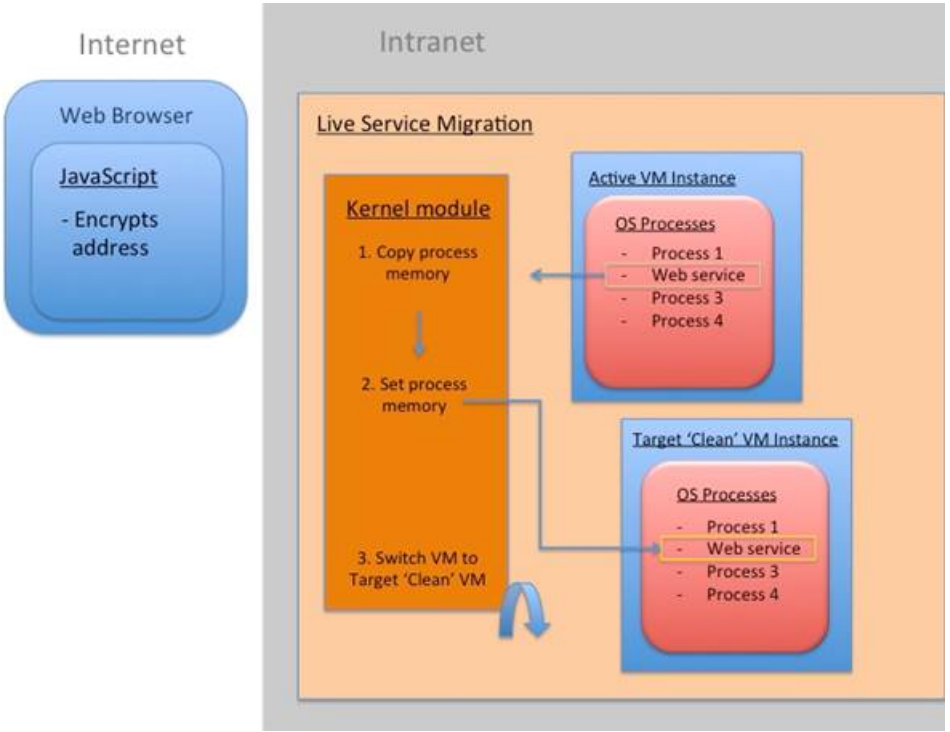


MESS: Protecting services

Step 2. Live Service Migration

Running processes migrate to pristine platforms at regular intervals;

Anything not in process memory dies.



Benefits

First through Public Interface Obfuscation

- MESS protected systems are hard to see
- Compromised Username/passwords less valuable
- Payloads on the inside cannot be contacted

Then, through Live Service Migration

- Zero-days happen, but they stop persisting
- Higher-chance of detection
- Lower risk to legitimate users

Current Status

- Developed working POCs in Phase I. Started Phase II in May, 2013.
  - Building network layer and integrating crypto
  - Building migration tool for a popular web server

- In 8 months will have a full product that can obfuscate multiple services, and migrate a specific web server.

- After that: Expand scope to other services, introduce Attribute Randomization.

Next Steps

- Continue software development.

- Looking for partners:
  - Beta deployments
  - Live trials
  - Marketing partnerships

Contact Information

Will Hickie

Will.Hickie@endeavorsystems.com