

RSA CONFERENCE 2014

FEBRUARY 24 - 28 | MOSCONE CENTER | SAN FRANCISCO

Share.
Learn.
Secure.

Capitalizing on
Collective Intelligence

Hacking Exposed: The Art of Deterrence (AoD)

SESSION ID: EXP-T09

Stuart McClure

Brian Wallace

Cylance, Inc.



Agenda

- ◆ Setting the stage
- ◆ Demo a working attack – Ripped from the Headlines!
 - ◆ Target-esqe breach
 - ◆ POS Malware (Dexter)
- ◆ Countermeasures
 - ◆ Art of Deterrence (AoD)
 - ◆ Mathematical Prevention

Setting the Stage

- ◆ Corporate Network, pop an admin box with PDF exploit via email
- ◆ Drops C2 server .exe and run it *
- ◆ Connect to C2 and remote control box, find POS systems nearby
- ◆ Push Dexter to POS, run it *
- ◆ Show hijacked data

RSACONFERENCE2014

FEBRUARY 24 - 28 | MOSCONE CENTER | SAN FRANCISCO



Demo of Exploit

RSA[®]CONFERENCE2014

FEBRUARY 24 - 28 | MOSCONE CENTER | SAN FRANCISCO



Countermeasures

AoD Options

- ◆ Deterrence
 - ◆ Distraction and Disruption*
 - ◆ Discouragement
 - ◆ Attribution
- ◆ Vengeance
 - ◆ Exposure
 - ◆ Humiliation
 - ◆ Takedown
 - ◆ Hack Back (and counter-attack)*

Demo AoD

- ◆ Identify source (Group A)
- ◆ Identify source's competitive peer (Group B)
- ◆ Discover remote SQLi in Group A's C2 to dump credentials and bypass authentication
- ◆ Option #1: Incite war
 - ◆ Pose as a legitimate, competitive hacker group
- ◆ Option #2: Release vulnerability to the public (thank you metasploit!)
 - ◆ SQLi on UID in gateway.php

RSA CONFERENCE 2014

FEBRUARY 24 - 28 | MOSCONE CENTER | SAN FRANCISCO



Demo of AoD

Botnet 0-days

- ◆ MadnessPro (DDoS) – SQLi (bypass authentication, RCE)
- ◆ HerpesNet (DDoS) – SQLi (bypass authentication, RCE)
- ◆ MultiLocker (Ransomware) – Hidden Backdoor (RCE)

Traditional Countermeasures

- ◆ Detect and Block on the IN
 - ◆ At the perimeter (email/web gateway, firewalls)
- ◆ Detect and Block on the endpoint or “at the user”
 - ◆ AV/HIPS/WL, Device Control, EMET
- ◆ Detect and Block on the OUT
 - ◆ Beaconsing and communication outbound


Non-Traditional Countermeasures

Prevention – Evolving from Signatures to Math...

- ◆ Signature World
 - ◆ See an attack after it's too late (Sacrificial Lamb required)
 - ◆ Identify specific (or generic) characteristics of the attack
 - ◆ Write a signature to detect the next attack
 - ◆ Unscalable, untenable, ineffective
- ◆ Math World
 - ◆ Collect, Extract, Transform and Train, Classify.
 - ◆ Math future proofs

RSA CONFERENCE 2014

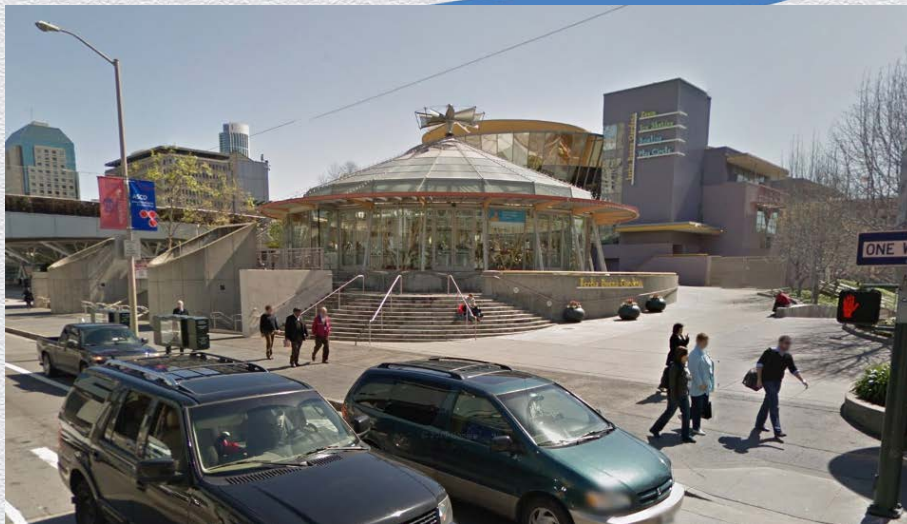
FEBRUARY 24 - 28 | MOSCONE CENTER | SAN FRANCISCO



Demo of Mathematical Prevention

RSACONFERENCE2014

FEBRUARY 24 - 28 | MOSCONE CENTER | SAN FRANCISCO



HE7 Book Signing:

Now @ 5:00pm
Children's Creativity
Museum

