Early Warning System for Targeted Attack using Malware Intelligence
Speaker: Dr. Arun Lakhhotia

- Professor of Computer Science
- 16 Years in Malware Research
- Sponsored by:
  - US Department of Defense
  - DARPA, Air Force, Army

- Founder, CEO
- Mission: Targeting Advanced Targeted Attacks
- USP:
  - Automated Malware Analytics
My 15 minutes
2003-2007: CajunBot

2003

2005

2007
My second 15 minutes
2010: Founded Lafayette
Holi
Current Security Industry Segmentation

**EPP**
- Prevent Breach using Indicators of Attack

**EDR**
- Detect Breach using Indicators of Compromise

Corporate Boundary
Can we leverage Indicators of Attack to PREDICT potential breach?

Corporate Boundary
Hint

MAXIM
Defender must succeed 99 times
Attacker only once

CORROLLARY
Attacker must TRY 99 times before succeeding once

Corporate Boundary
Targeted Attacks are multi-staged

Initial Compromise → Establish Foothold → Escalate Privileges → Move Laterally → Steal Data

Mandiant ™ Targeted Attack Cycle
Targeted Attacks Require Persistence

Attacker must try, and try, and try

Mandiant™ Targeted Attack Cycle

Initial Compromise
Establish foothold
Escalate Privileges
Move Laterally
Steal Data
Question?

How can we detect persistent attempts?

Mandiant™ Targeted Attack Cycle

Initial Compromise
Establish foothold
Escalate Privileges
Move Laterally
Steal Data
Malware (still) plays a dominant role in data breaches

72% phishes delivered via email

85% Include malware

Persistence involves beating AV defenses

Inundate the system

With Machine Generated Variants
Current Limitation: Each Malware is Independent

No connection between them
Cythereal’s MAGIC: Connect malware

Connected using shared “Genome”

Research Sponsored by: DARPA Cyber Genome program
DEMO

magic.cythereal.com

“Google” for Malware
Case Study: Discover Stages of Attack

Adware

Backdoor

Keylogger

Jul | Aug | Sep | Oct | Aug | Dec | Jan | Feb

Adware | Backdoor | Keylogger

6/15/2016 (C) 2016 CYTHEREAL
Cythereal’s Vision

MAGIC Threat Intelligence Exchange

Hub: Global Intelligence  Spokes: Local Intelligence

Indicators Exchanged: Malware Genome
Cythereal’s MAGIC

Learn from Adversary’s Failures

Turn Anti-Virus into an Intelligence Gathering Tool

Connect Malware to Connect Attacks
How can you get it?

Register on:

magic.cythereal.com

Giving away
FIVE Free One Year Subscription