cythereal

Targeting Advanced Cyber Attacks

Early Warning System for Targeted Attack using Malware Intelligence

blackhat®

BLACK HAT | WEBCAST

Speaker:
Dr. Arun Lakhotia

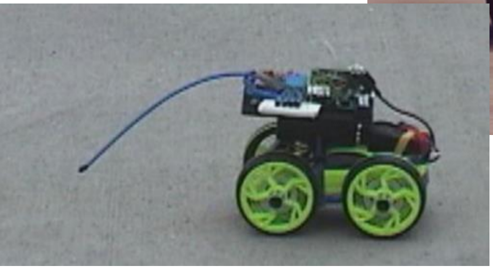
- Professor of Computer Science
- 16 Years in Malware Research
- Sponsored by:
  - US Department of Defense
  - DARPA, Air Force, Army

- Founder, CEO
- Mission:
  Targeting Advanced Targeted Attacks
- USP:
  - Automated Malware Analytics

My 15 minutes 2003-2007: CajunBot

DARPA GRAND CHALLENGE

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

Quiz?

Can we leverage **Indicators of Attack** to PREDICT potential breach?

Corporate Boundary

Hint

MAXIM

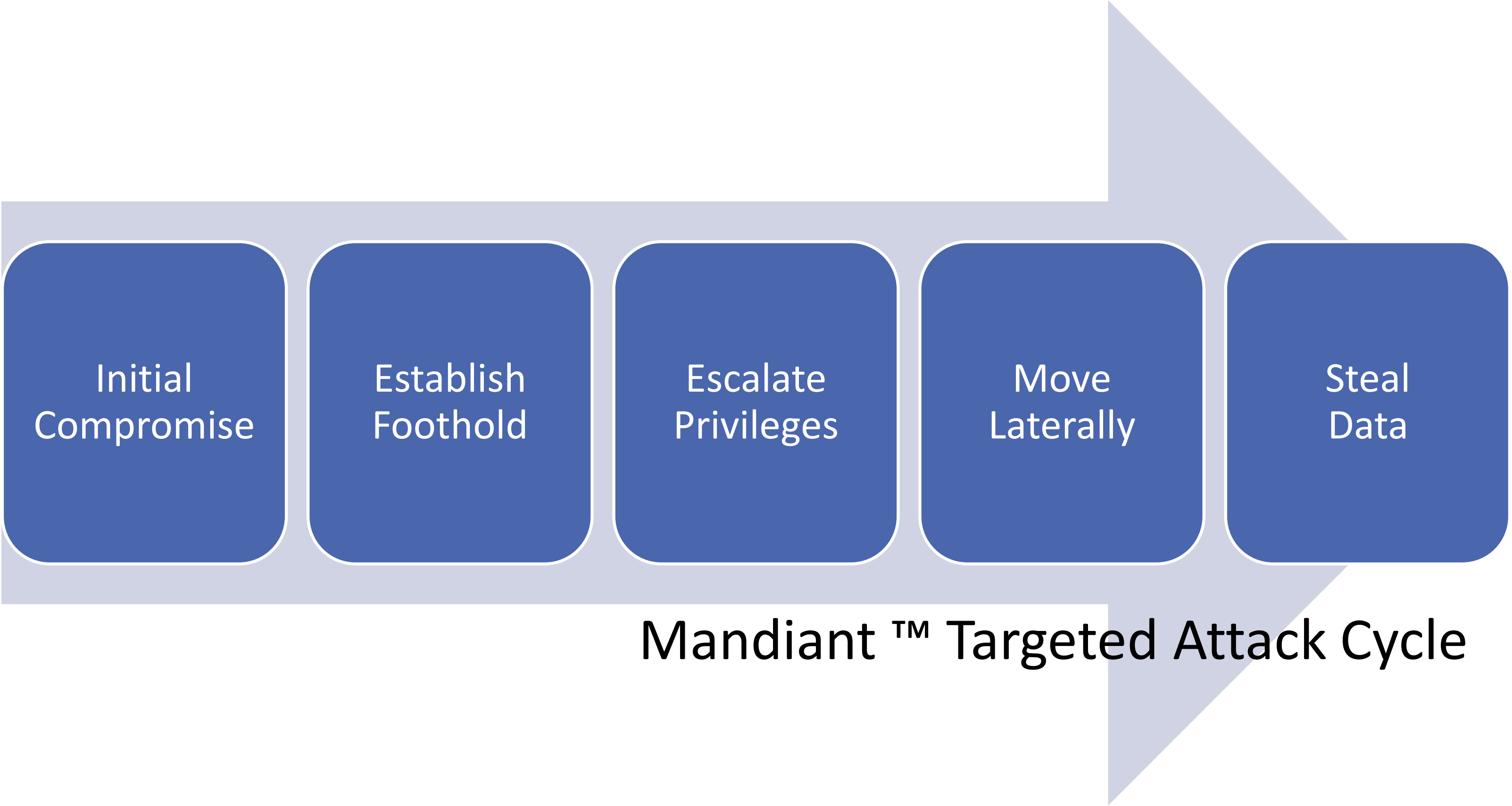
Defender must succeed 99 times Attacker only once

CORROLLARY

Attacker must TRY 99 times before succeeding once

Corporate Boundary

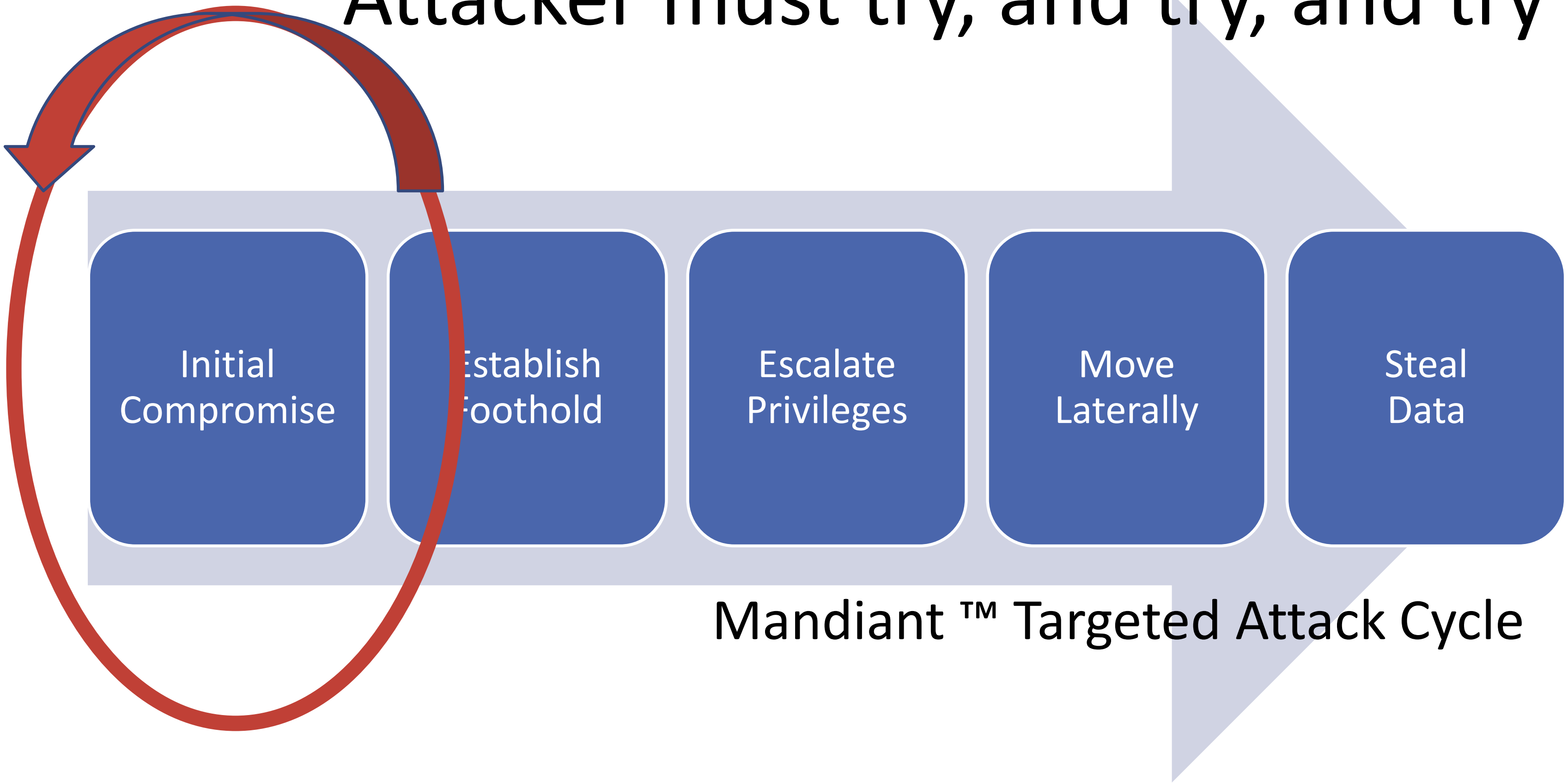
Targeted Attacks are multi-staged



Mandiant ™ Targeted Attack Cycle

Targeted Attacks Require Persistence

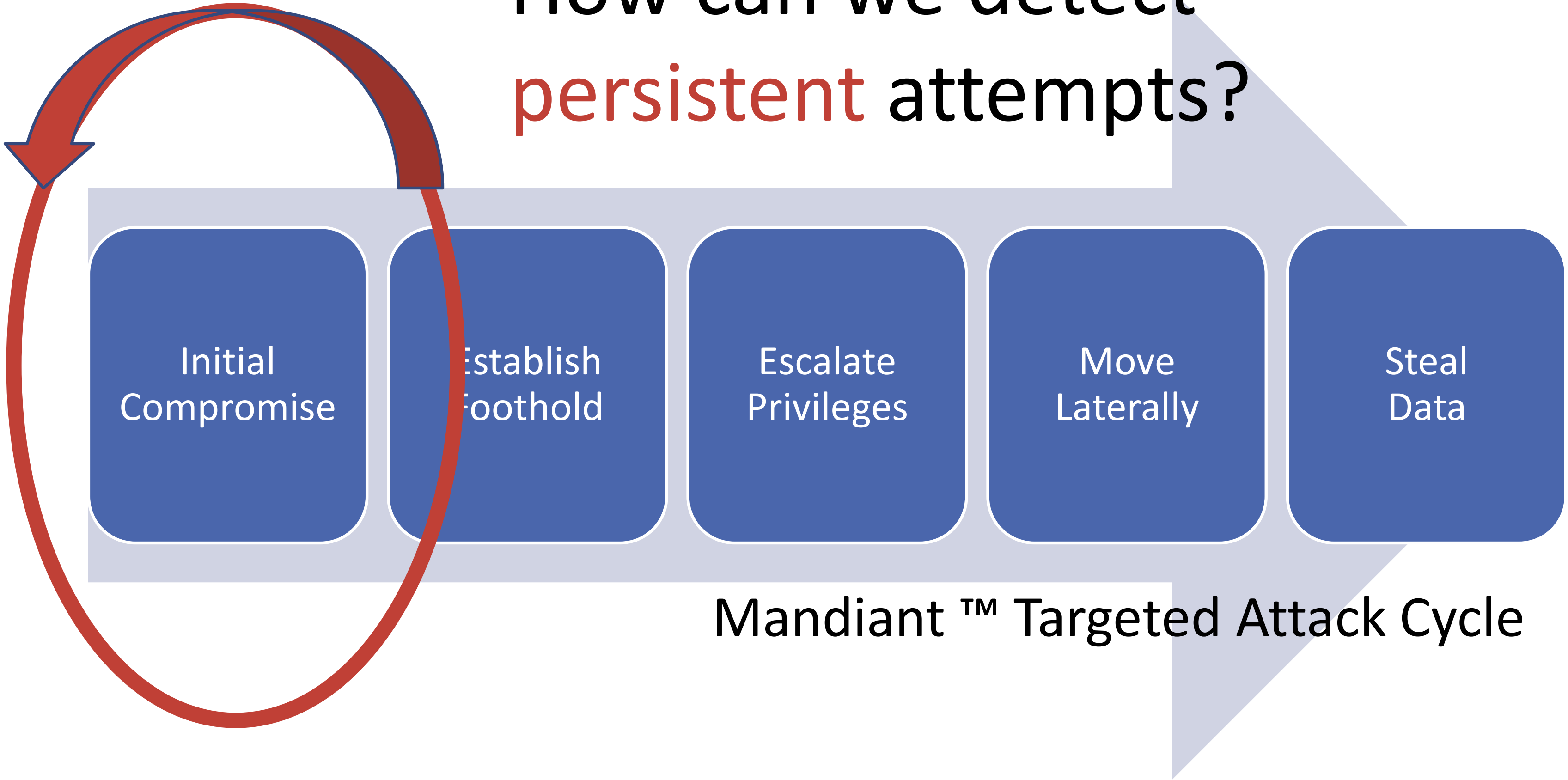
Attacker must try, and try, and try



Mandiant ™ Targeted Attack Cycle

Question?

How can we detect
persistent attempts?



Mandiant ™ Targeted Attack Cycle

Malware (still) plays a dominant role in data breaches

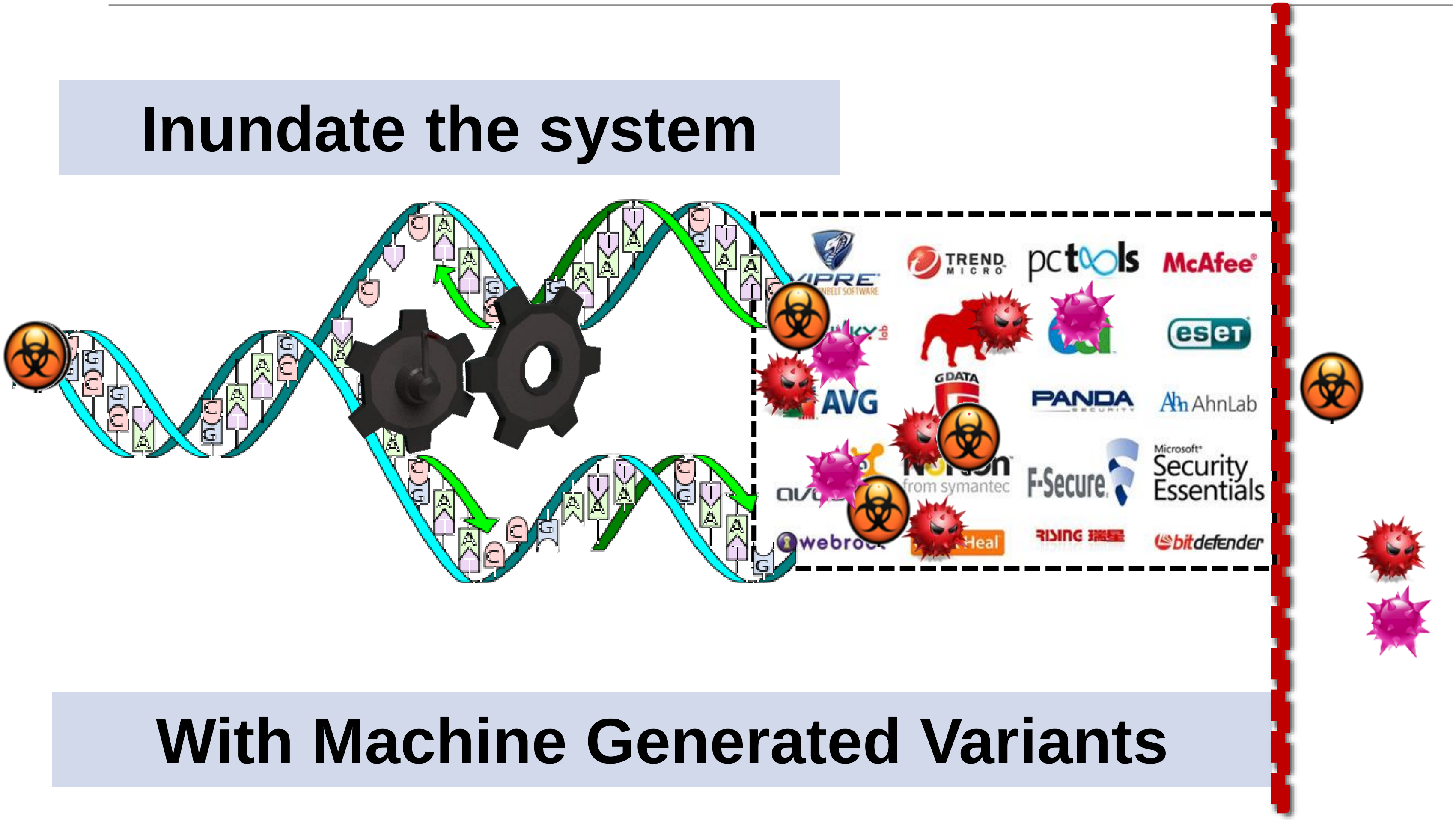
72% phishes delivered via email

85% Include malware

Verizon Data Breach Report 2016

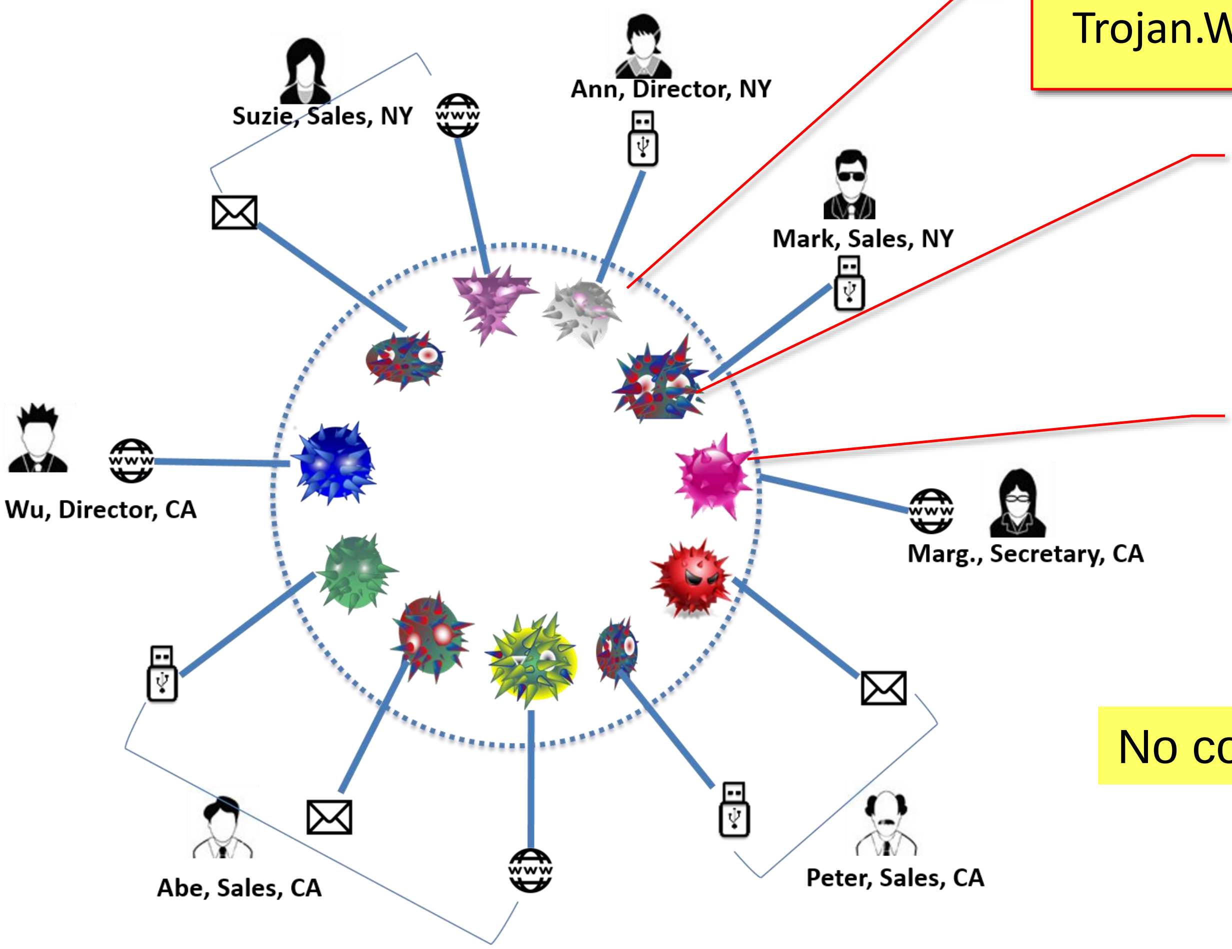
Persistence involves beating AV defenses

Inundate the system



With Machine Generated Variants

Current Limitation: Each Malware is Independent



Suzie, Sales, NY

Ann, Director, NY

Mark, Sales, NY

Wu, Director, CA

Marg., Secretary, CA

Abe, Sales, CA

Peter, Sales, CA

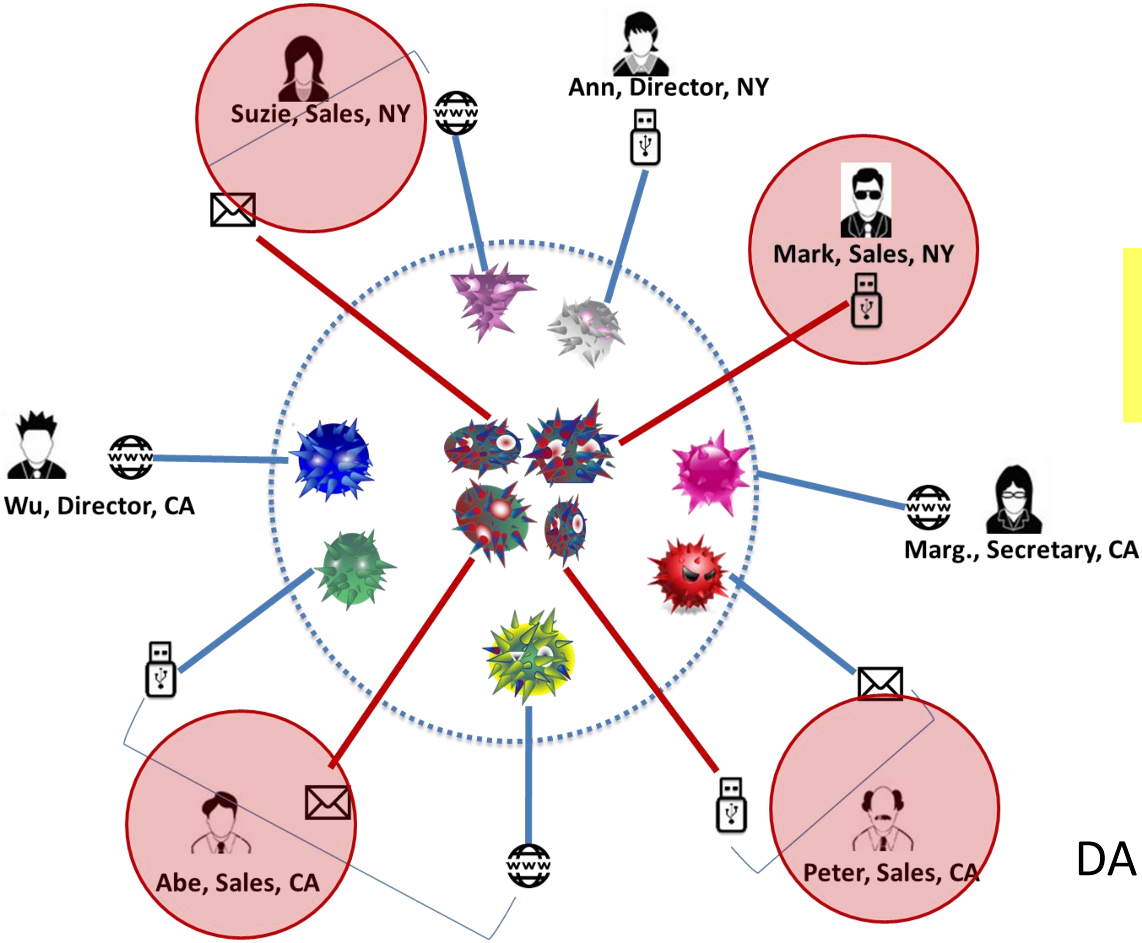
Trojan.Win.5265

KeyLog.Win.HAB

BadThing.abac

No connection between them

Cythereal's MAGIC: Connect malware



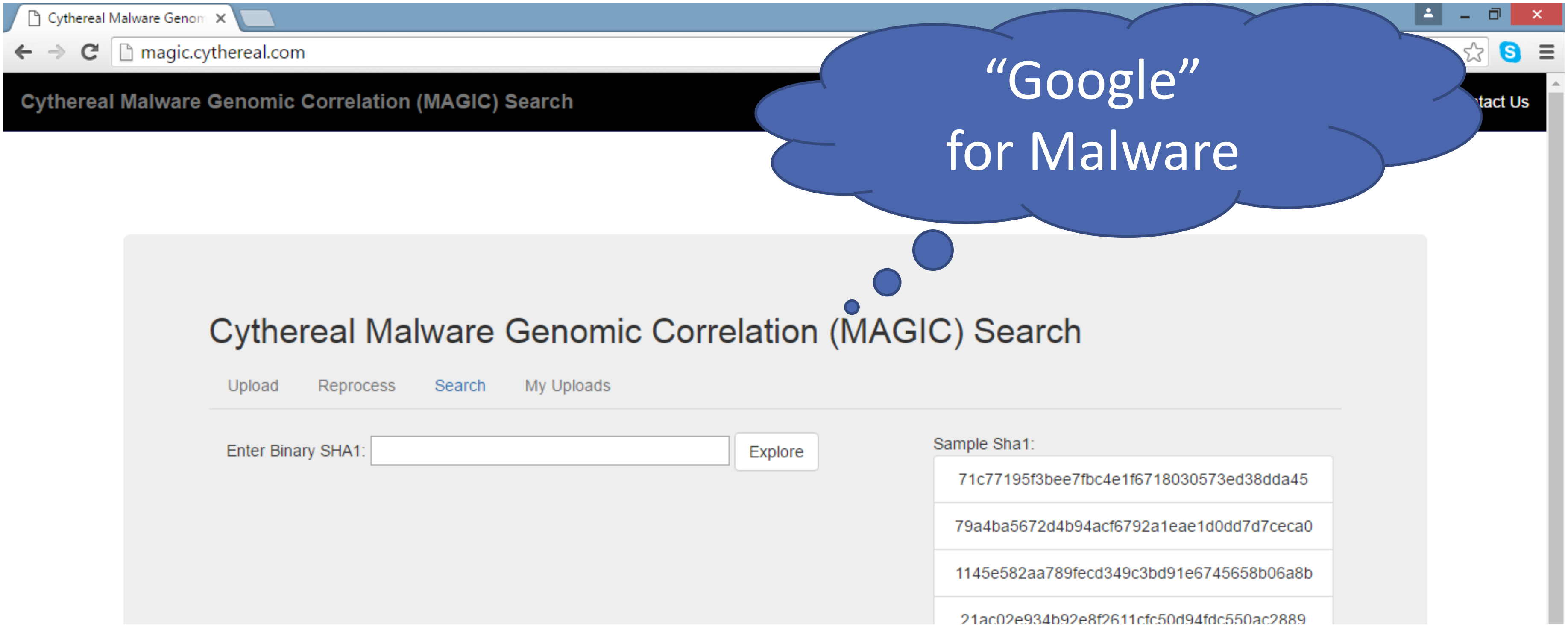
Patent Pending

Connected using shared "Genome"

Research Sponsored by:
DARPA Cyber Genome program

DEMO

magic.cythereal.com



“Google”
for Malware

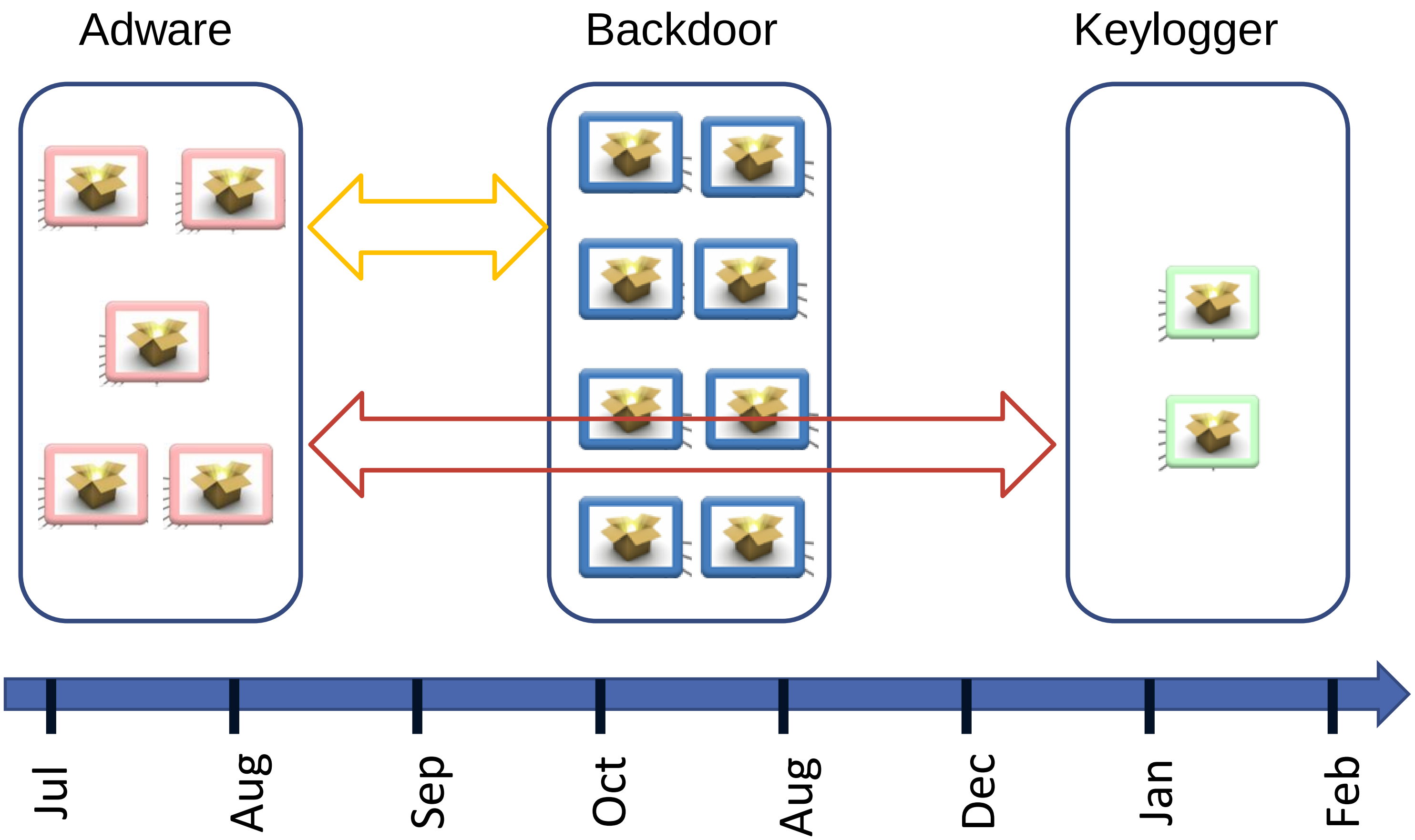
Cythereal Malware Genomic Correlation (MAGIC) Search

Enter Binary SHA1:

Sample Sha1:

- 71c77195f3bee7fbc4e1f6718030573ed38dda45
- 79a4ba5672d4b94acf6792a1eae1d0dd7d7ceca0
- 1145e582aa789fecd349c3bd91e6745658b06a8b
- 21ac02e934b92e8f2611cfc50d94fdc550ac2889

Case Study: Discover Stages of Attack

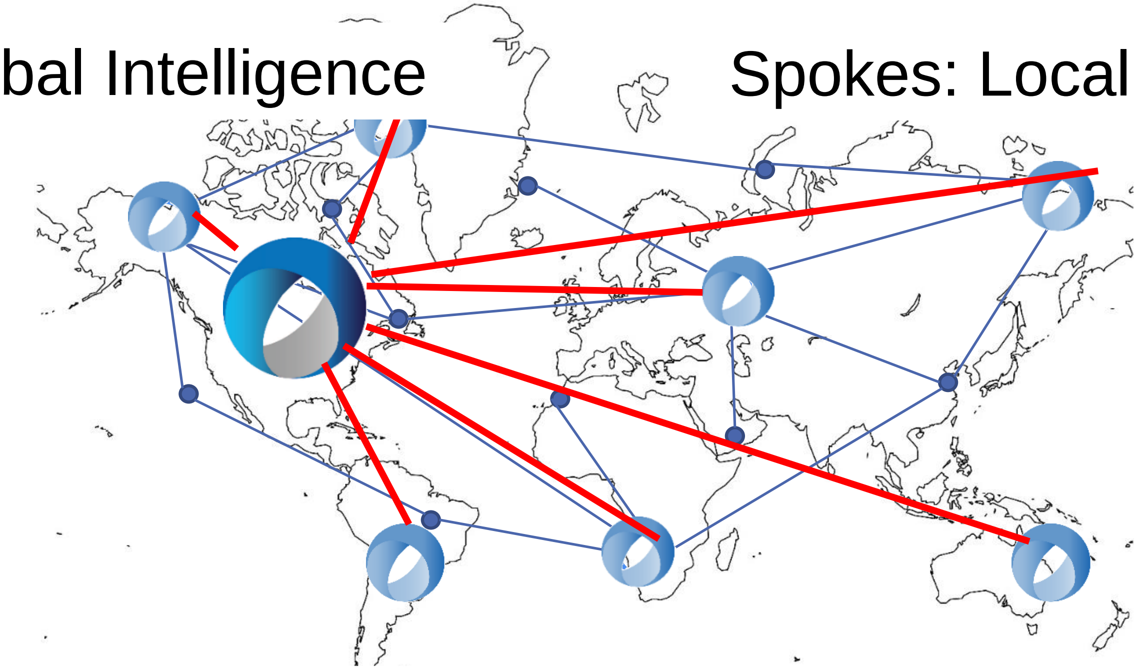


Cythereal's Vision

MAGIC Threat Intelligence Exchange

Hub: Global Intelligence

Spokes: Local Intelligence

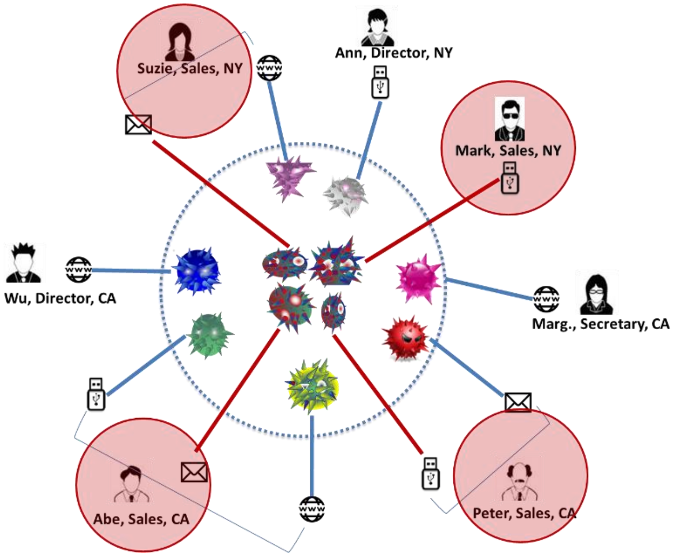


Indicators Exchanged: Malware Genome

Cythereal's MAGIC

Learn from Adversary's Failures

Turn Anti-Virus into an Intelligence Gathering Tool



Connect Malware to Connect Attacks

cythereal

How can you get it?

Register on:

magic.cythereal.com

Giving away
FIVE Free One Year Subscription