The Industrial Revolution of Lateral Movement

Tal Be'ery, Independent
Tal Maor, Microsoft ATA

Speaker Info – Tal Be'ery

- Independent ☺
- Previously
  - Sr. Security Research Manager @Microsoft, Developing Microsoft ATA (Advanced Threat Analytics)
  - VP for Research @Aorato (Acquired by Microsoft)
- 15 years of security research
- Author of the TIME attack on SSL
- Twitter: @TalBeerySec

Speaker Info – Tal Maor

- Security Researcher @Microsoft
- Developing Microsoft ATA (Advanced Threat Analytics)
- Developed GoFetch ☺
- B.Sc degree in Computer Science.
- Twitter: @TalTheMaor

Agenda

- Intro
  - The Financially Motivated Hacker
    - From the Cyber Kill-Chain to the Cyber Value-Chain
    - Cyber Value Chain Optimization
      - Specialization
      - Automation
- Industrialization of the Lateral Movement phase
  - GoFetch! release
    - Open Source Lateral Movement Automation Tool
  - DEMO
- Implications of Lateral Movement Industrializatic
  - For Attackers: Dropping cost, increased velocity
  - For Defenders: Make Lateral Movement Hard Again
- Outro: Summary + Call for Action!

Intro

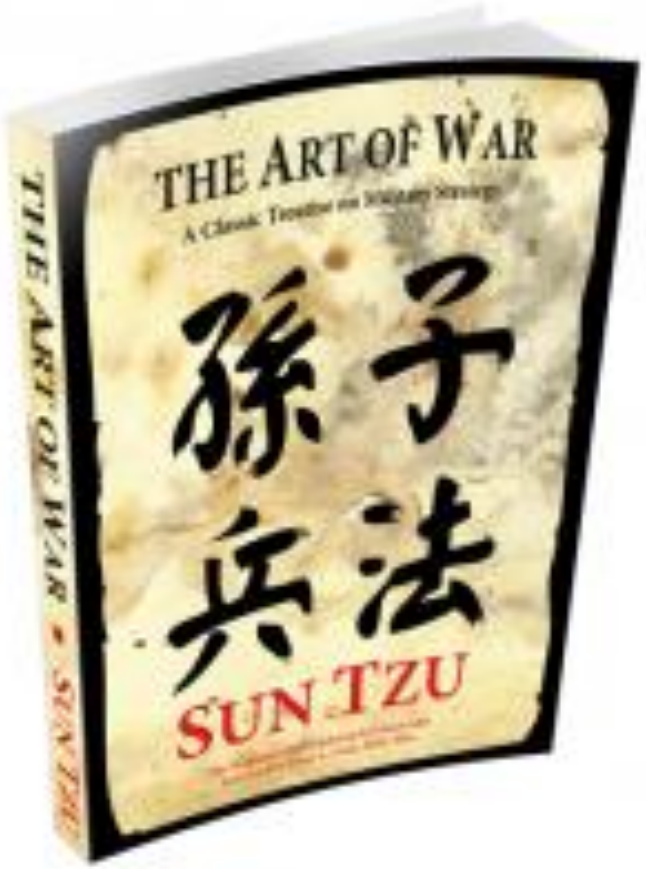
The Many Faces of Hacking

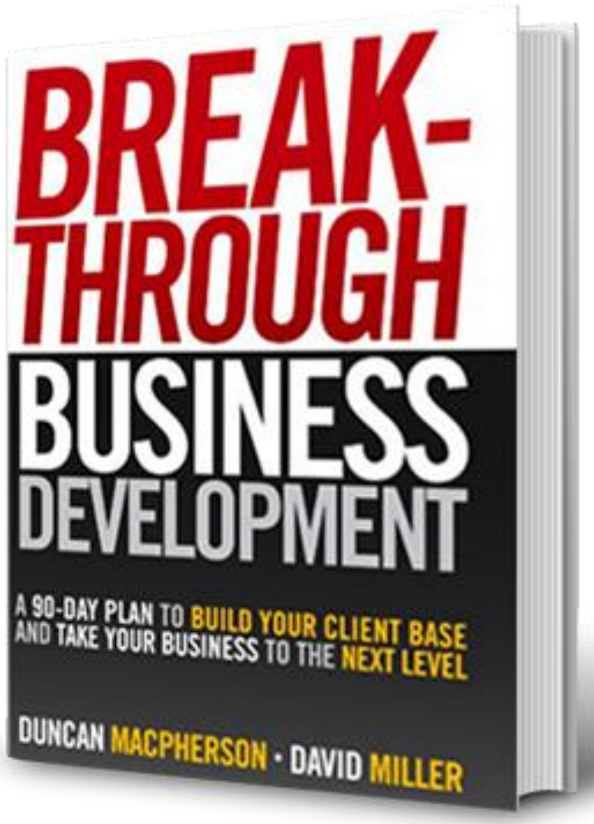
Hacktivism

Nation State

Financial

The Hacker CEO: Inspiration





The Hacker CEO Mission: Growth & Efficiency

The Business Process: The Cyber Value-Chain

- Cyber attacks proliferated from Nation state actors to Cyber Crime
  - **Cyber Kill-Chain → Cyber Value-Chain**
- The Value-Chain: Raw material → Product
- In the Cyber case:
  - **Raw Material: Target details**
  - **Product: Data**

http://www.ourkids.net/blog/wp-content/uploads/2011/03/assembly-line.jpg

Business Process Innovation: Specialization

Penetration

Domination

Actions on Data

The Domination Value Chain: Lateral Movement

Admin recon

Compromise creds

Local privilege escalation

Remote code execution

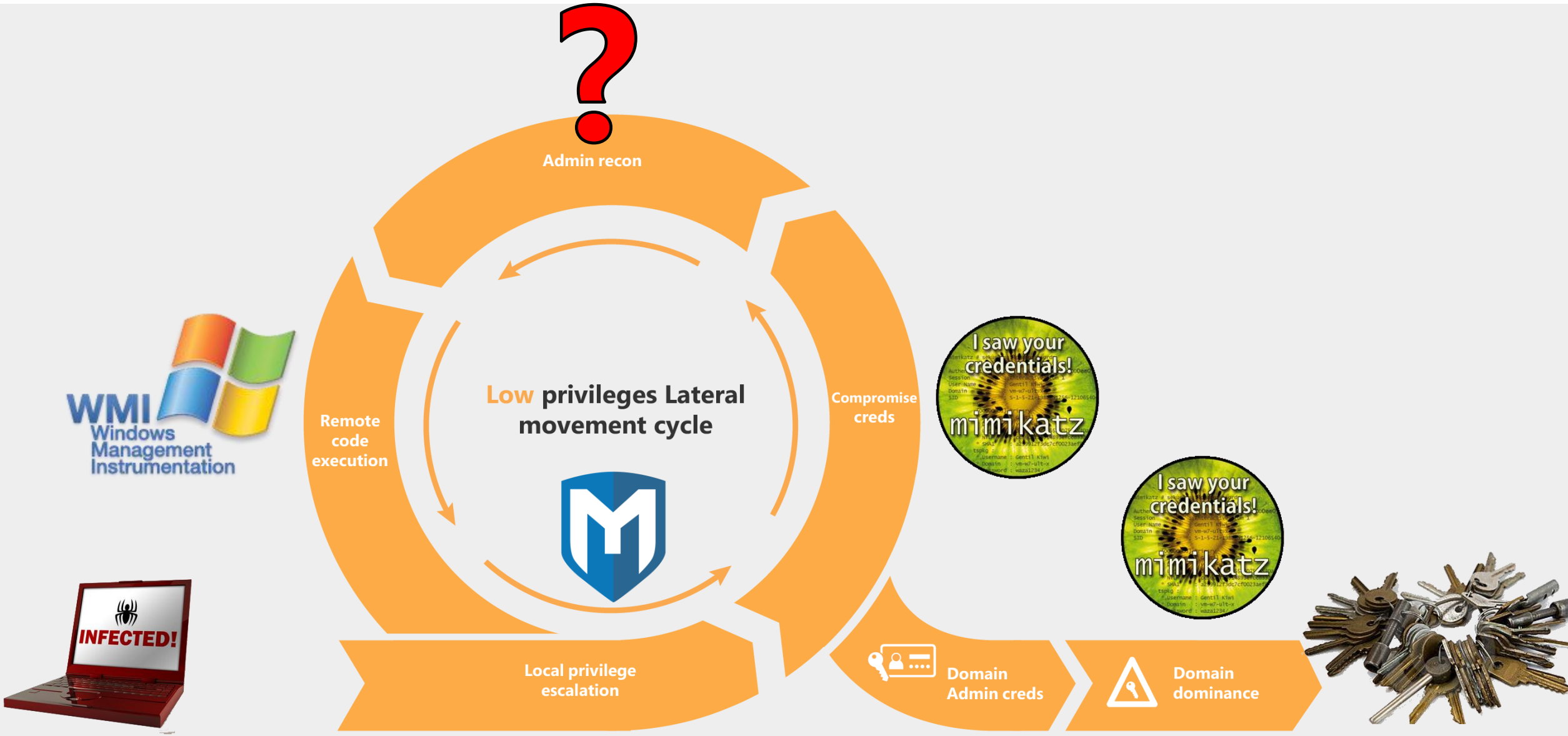
Low privileges Lateral movement cycle

Week

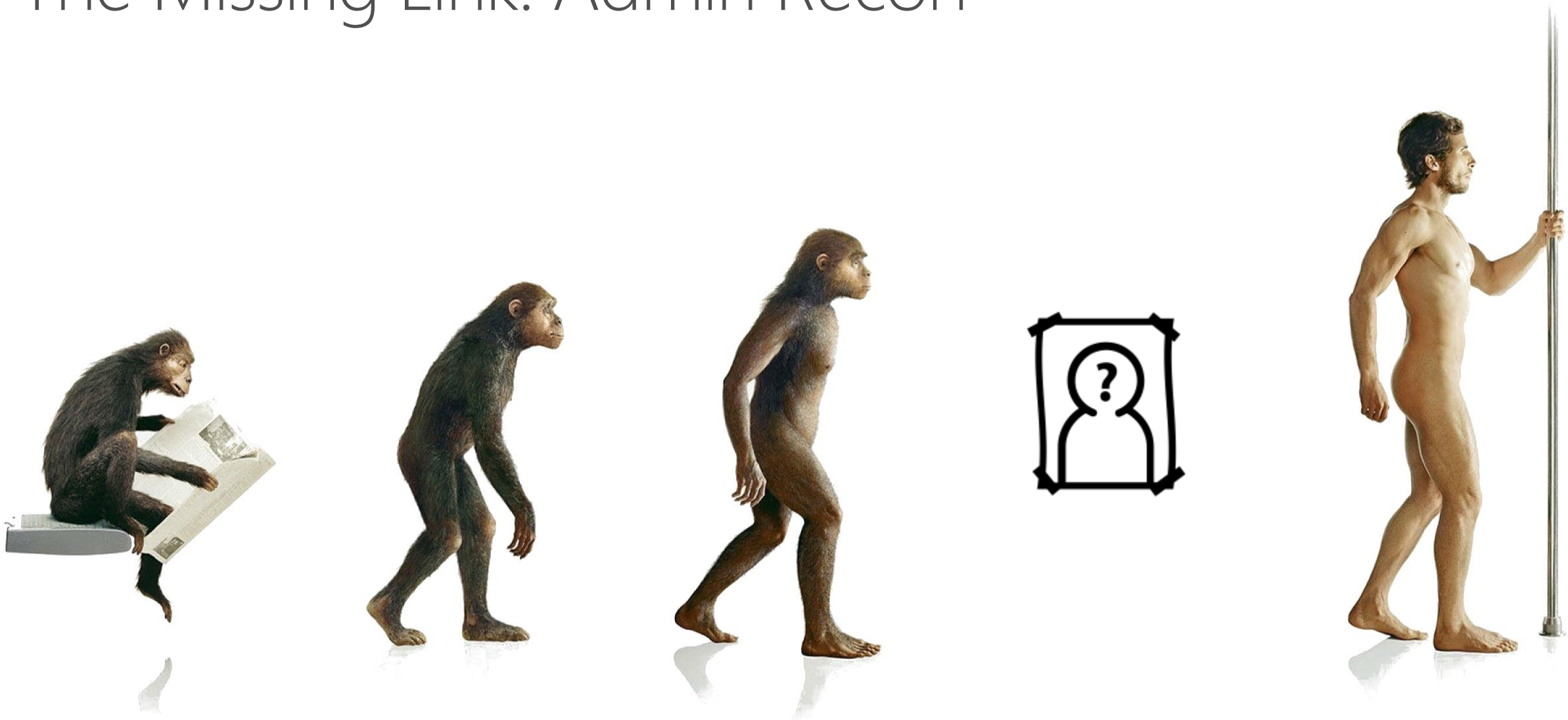
Domain Admin creds

Domain dominance

Business Process Innovation: Automation

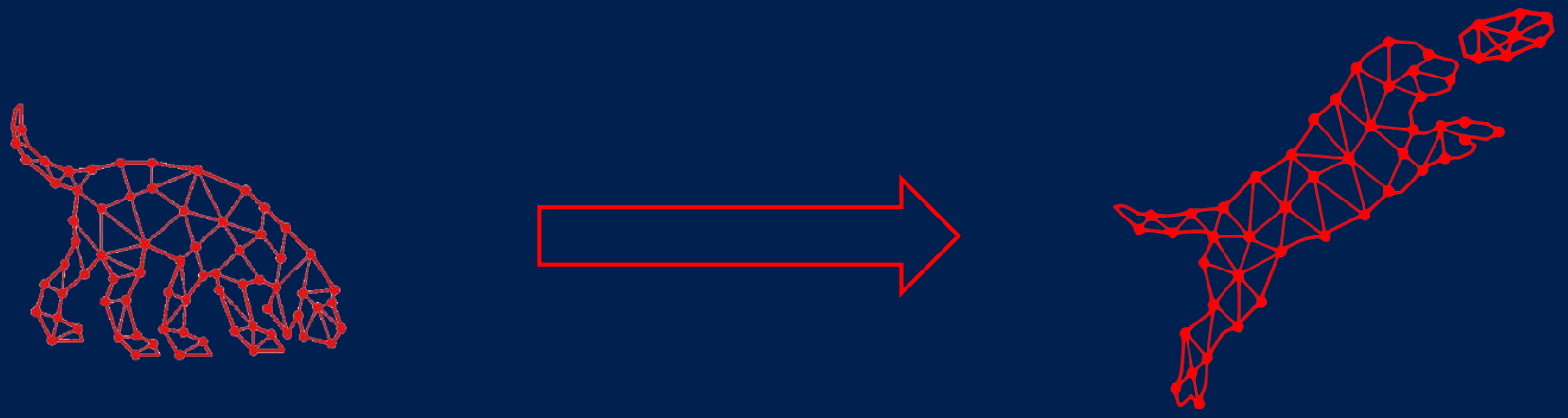


The Missing Link: Admin Recon

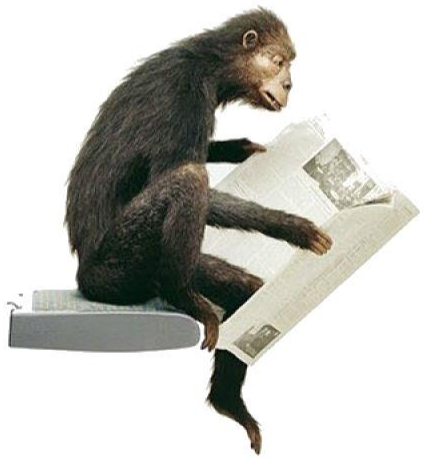


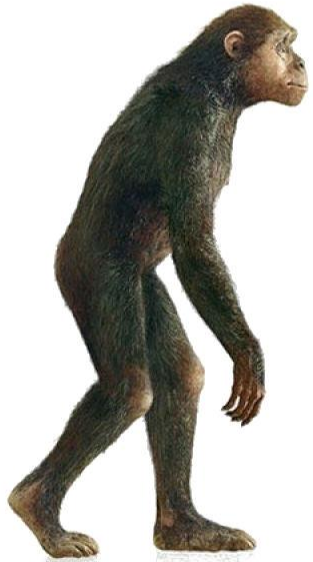
http://www.fanagrams.com/blog/wp-content/uploads/2011/03/Human-Evolution-Wallpaper2.jpg

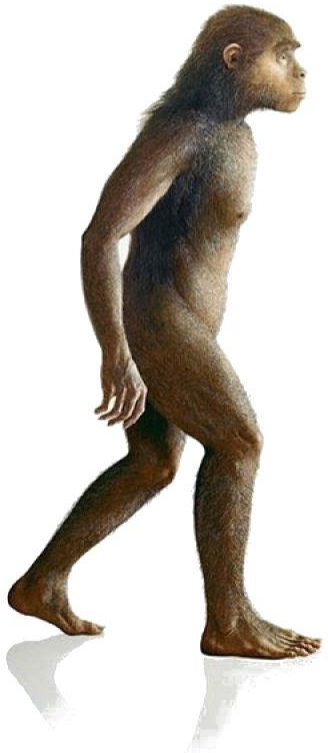
The Automation



The Missing Link: Admin Recon



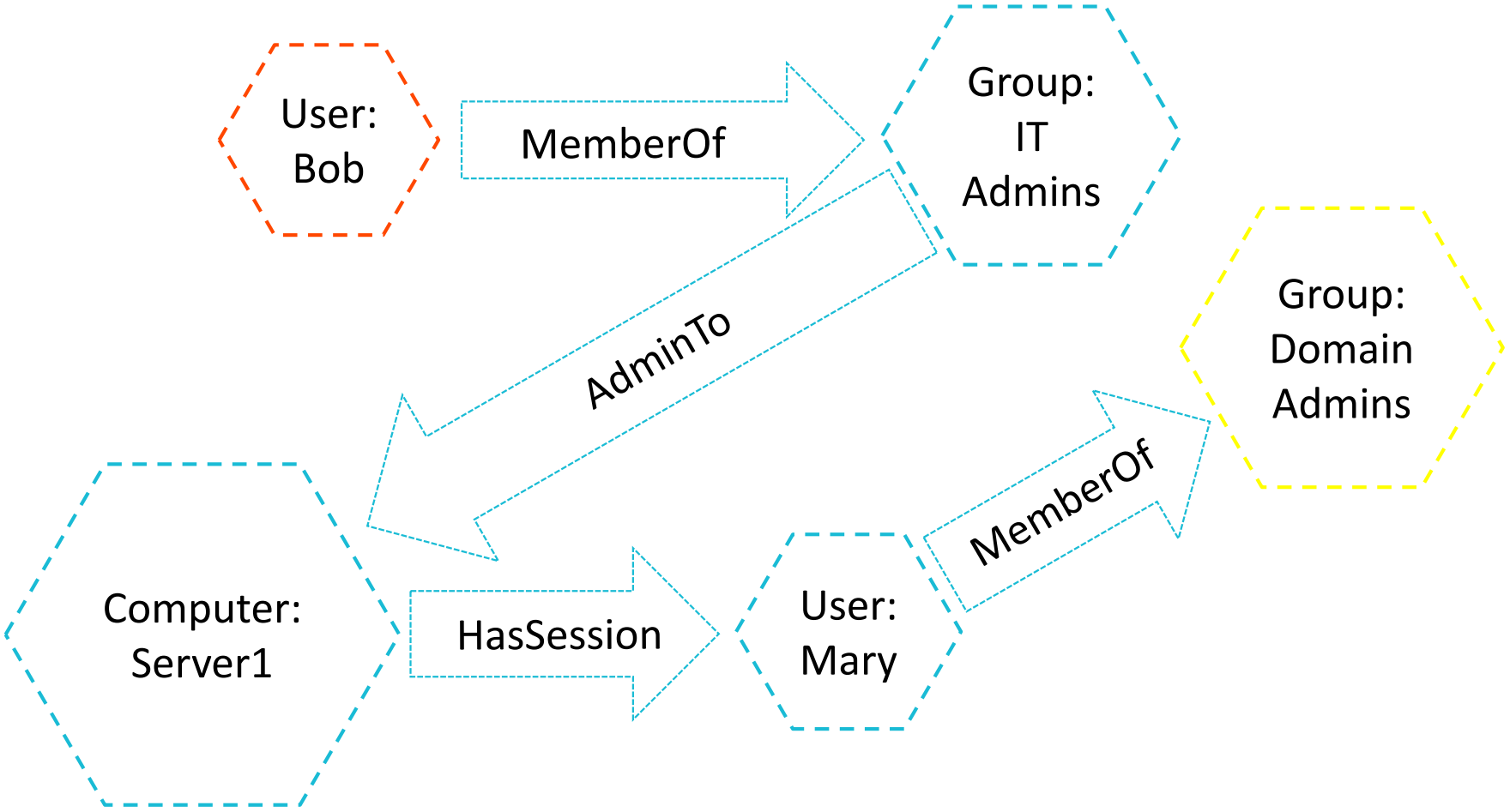




BLOODHOUND

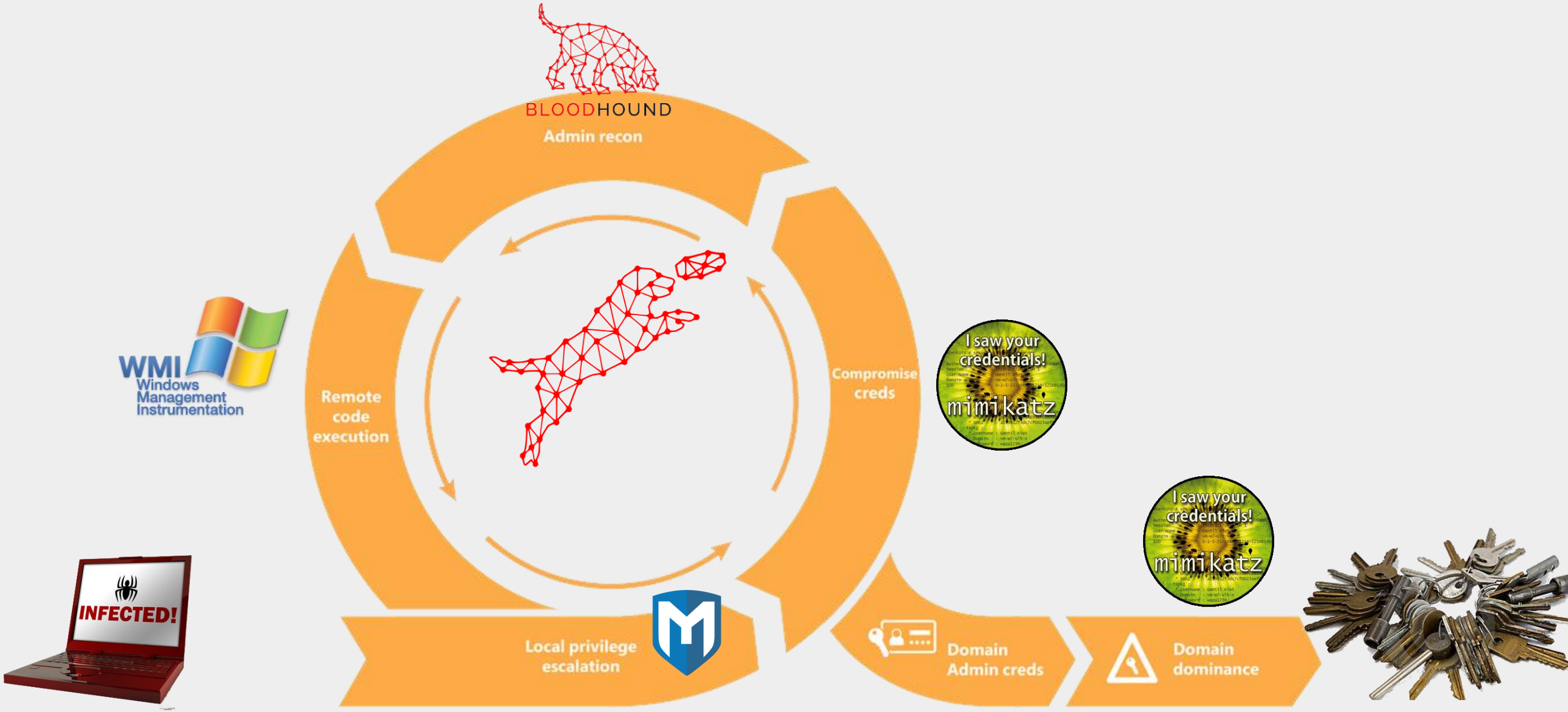
http://www.fanagrams.com/blog/wp-content/uploads/2011/03/Human-Evolution-Wallpaper2.jpg

BloodHound In a Slide



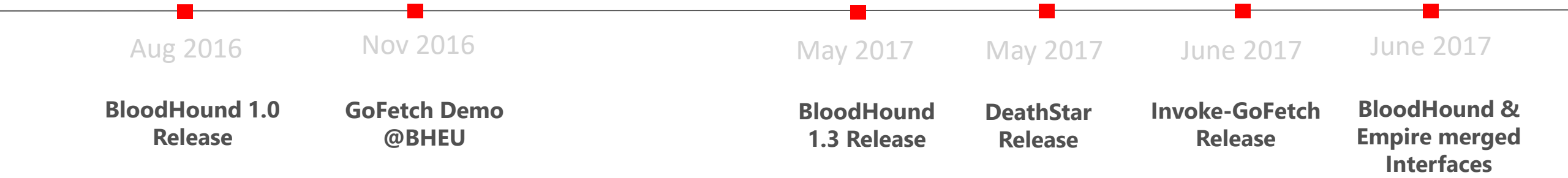
http://www.slideshare.net/AndyRobbins3/six-degrees-of-domain-admin-bloodhound-at-def-con-24

Attack Value-Chain



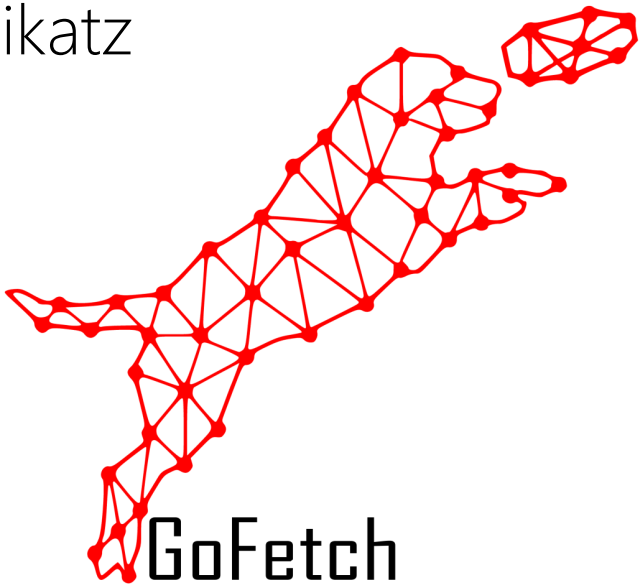
2017: Summer of Lateral Movement Automation

- GoFetch: Alpha version
  - One computer to run them all
- DeathStar
  - Reconnaissance & Expansion on the fly.
- Invoke-GoFetch
  - Replicates itself according to a pre-determined attack path.
- BloodHound 1.3
  - Automation for additional attack surface

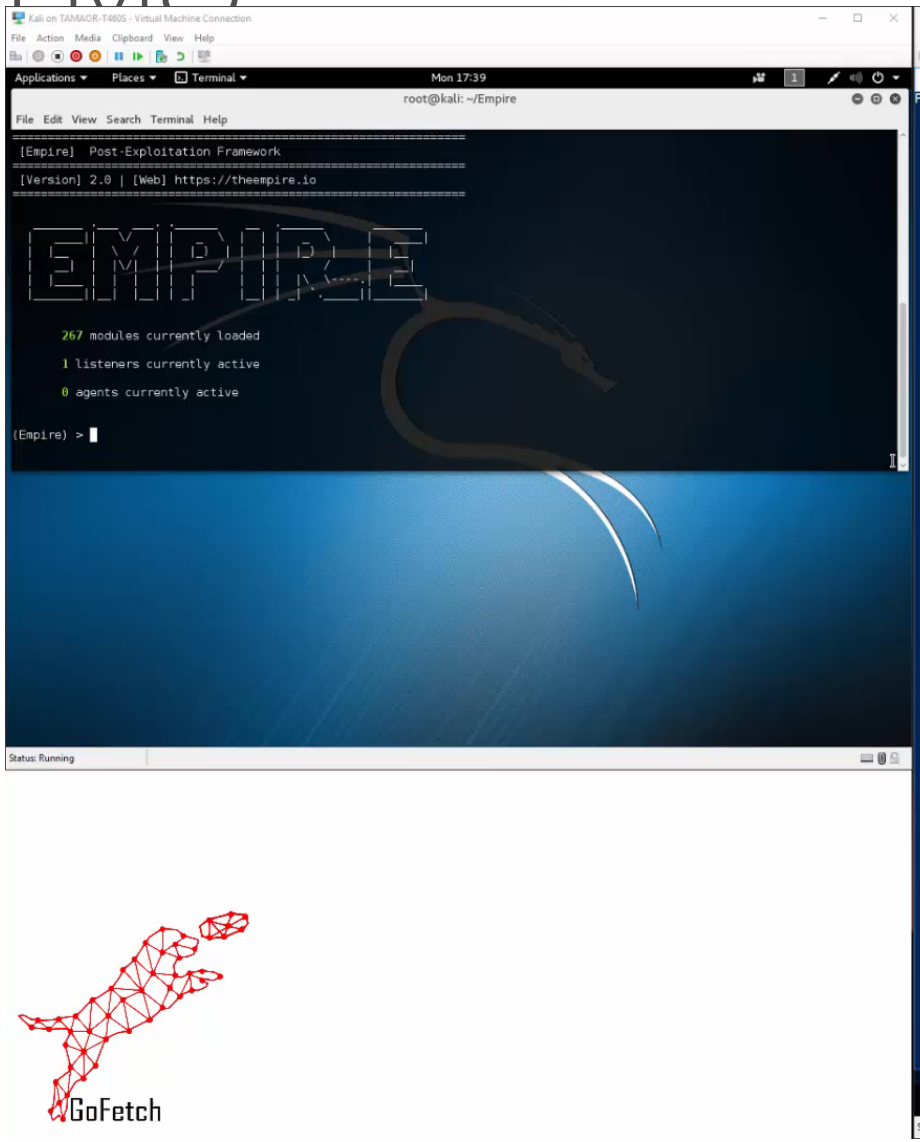


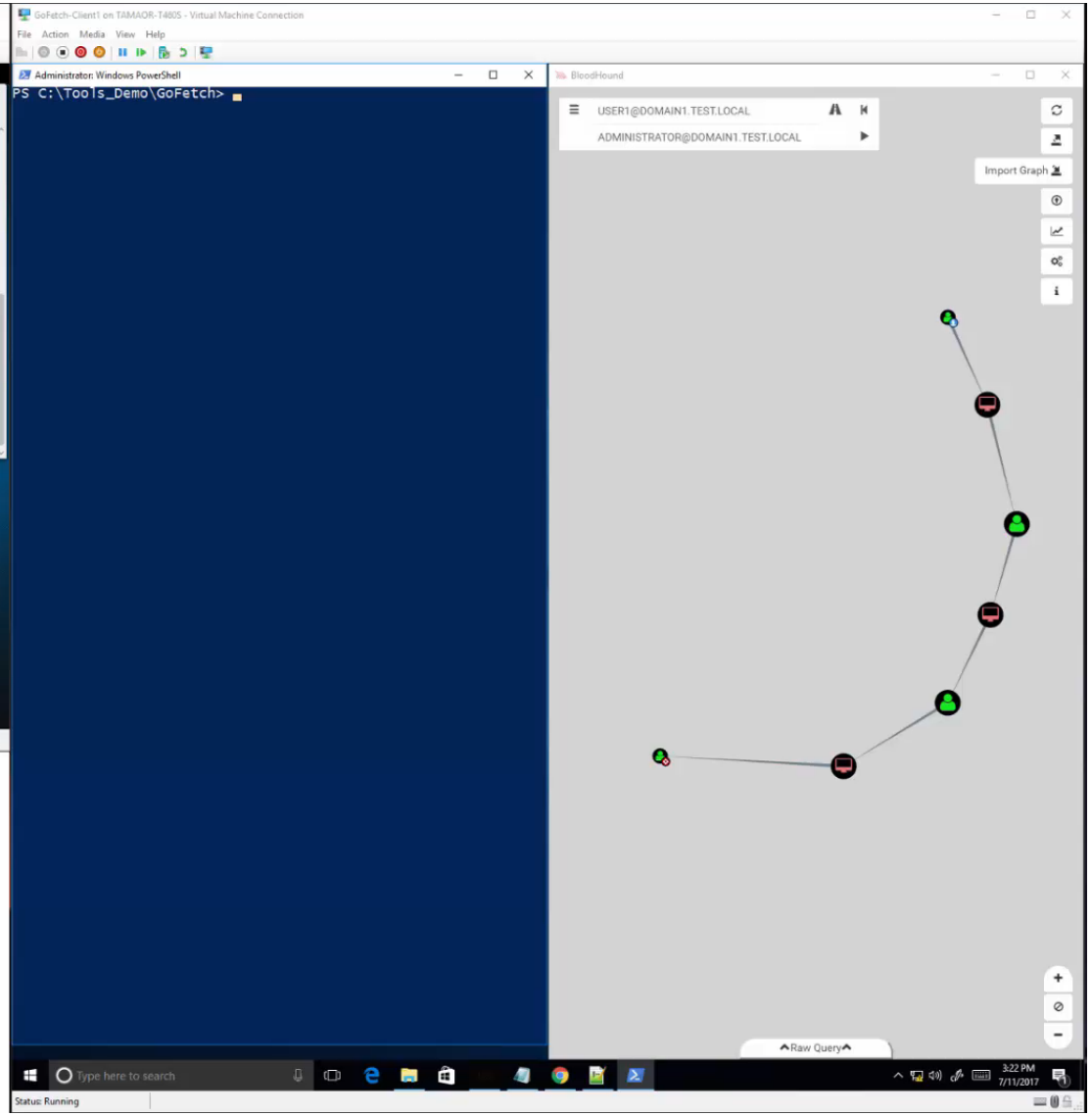
Invoke-GoFetch

- Targeted Lateral Movement by a pre-determined path
  - Input: Requested Network Path (e.g. BloodHound's output)
  - Outputs
    - Credentials along the path
    - Configurable payload along the path
- Open Source! Coded in PowerShell
- Lateral Movement method: PowerSploit's Invoke-PsExec
- Compromise creds: A variation of PowerSploit's Invoke-mimikatz
- Configurable payload
  - None (Just harvest creds)
  - Generic reverse shell: Empire, Cobalt Strike, Metasploit…
  - Other executables



DEMO


Kali on TAMAOR-T480S - Virtual Machine Connection
File Action Media Clipboard View Help
Applications Places Terminal Mon 17:39
root@kali: ~/Empire
File Edit View Search Terminal Help
[Empire] Post-Exploitation Framework
[Version] 2.0 | [Web] https://theempire.io
267 modules currently loaded
1 listeners currently active
0 agents currently active
(Empire) >
Status: Running


GoFetch-Client1 on TAMAOR-T480S - Virtual Machine Connection
File Action Media View Help
Administrator: Windows PowerShell
PS C:\Tools_Demo\GoFetch>
BloodHound
USER1@DOMAIN1.TEST.LOCAL
ADMINISTRATOR@DOMAIN1.TEST.LOCAL
Import Graph
Raw Query
Type here to search
3:22 PM
7/11/2017
Status: Running

GoFetch

Invoke-GoFetch Lateral Movement

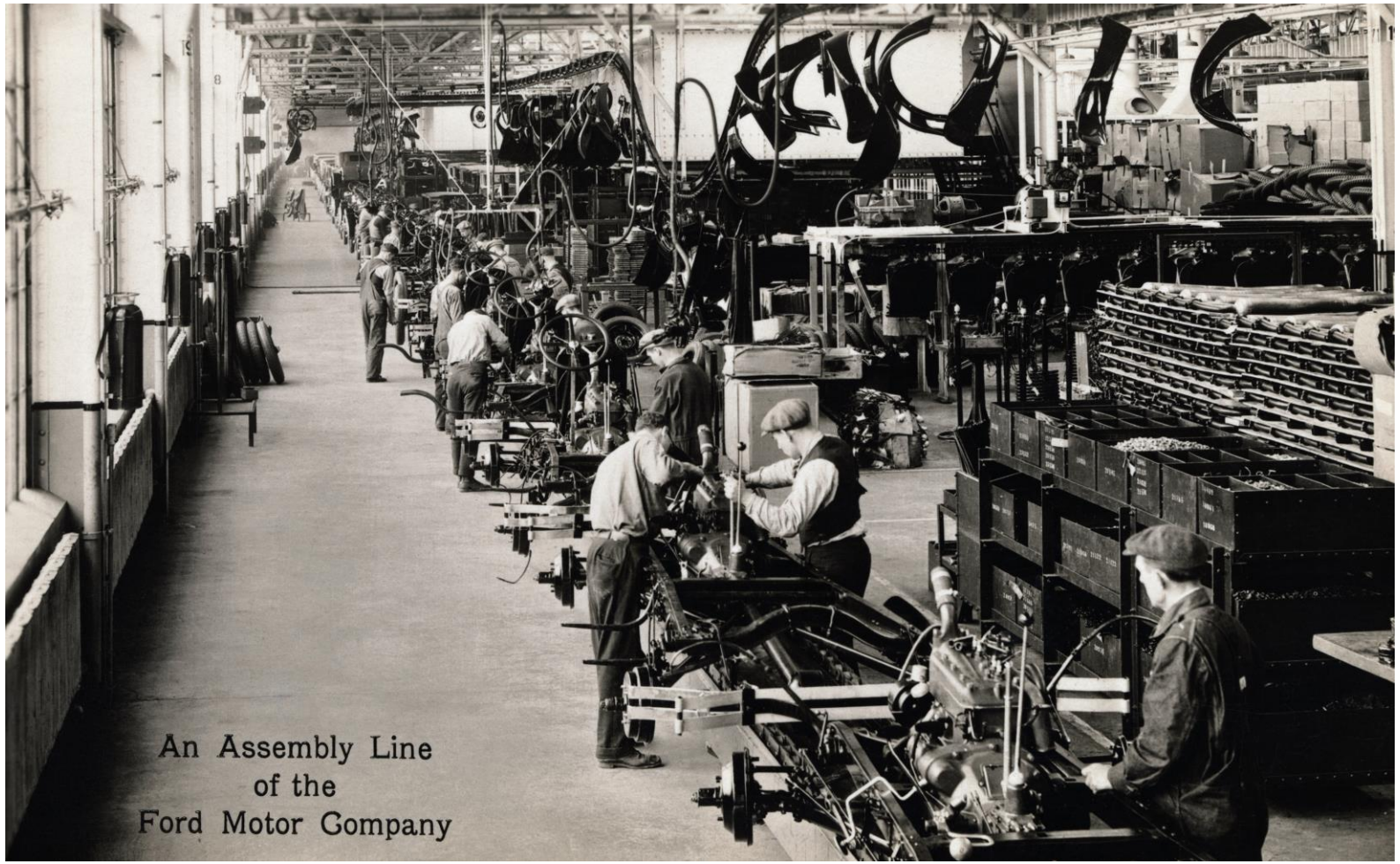
- Targeted expansion means less machines are touched
  - Stealthier
  - Faster
- No C2 connectivity needed
  - Fire and Forget: Expansion logic (next target) is transmitted to the edges
  - Less communication -> stealthier

Future Work

- Add more Remote Code Execution methods
  - WMI, WinRM, AtExec,…
- More Compromise Identity methods
  - Migrate to process, Impersonation
- Make it File-less
- Add as an extension to Post-exploitation Platforms:
  - Metasploit, Empire, Cobalt-Strike,…
- Support ACL traversal (Bloodhound 1.3)
- Please contribute!
  - https://github.com/GoFetchAD/GoFetch

Industrial Revolution

Mass Production



Mass Production of Lateral Movement

- The product is “Domain Domination”
- Fully automated, no manual labor, results:
  - Cheaper: Cost is negligent
  - Faster: Domain Dominance within minutes
- Results:
  - Many more potential victims
  - Surplus will create marketplaces

Domination

NEWS

A black market is selling access to hacked government servers for as little as $6

"It is a hacker’s dream," says Kaspersky Lab.

Defense Reactions to Industrialization

FIGHT

FLIGHT ooh la la!

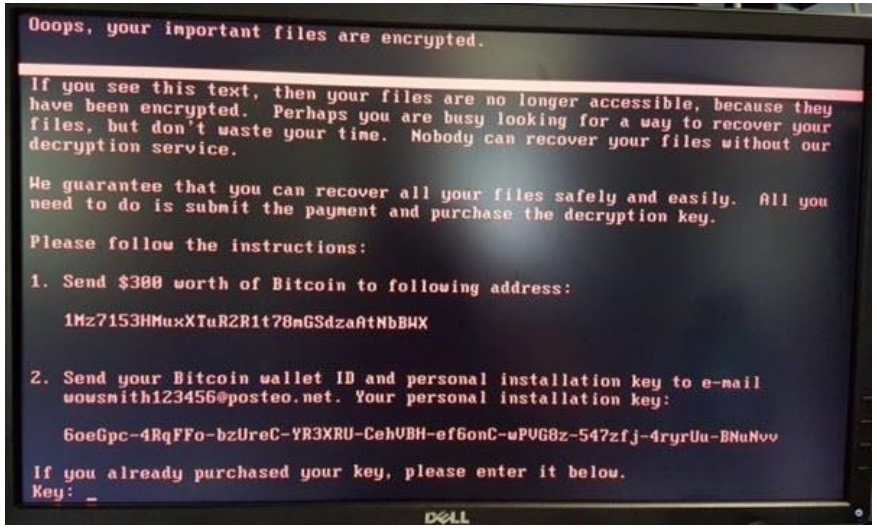
FREEZE

Defense Reactions: Freeze

- “We will just to continue to do what we always did”
- Hunt manually, have manual Incident Response etc.

Defense Reaction: Flight

- "Lateral Movement battle is lost"
- Concentrate on protecting the data itself
  - Encryption
  - Data access monitoring
  - Exfiltration protection, DLP
- What about attacks on data availability
  - Ransomware, wipers



Actions on Data

Defense Reactions: Fight!

Make Lateral Movement Hard (=Expensive) Again!

Fight: Reduce Attack Surface

- Make Reconnaissance (Attack graph generation) hard again
  - Harden information gathering APIs
  - Tools (Created by MicrosoftATA researcher, Itai Grady)
    - SMARi10 - https://gallery.technet.microsoft.com/SAMRi10-Hardening-Remote-48d94b5b
    - NetCease - https://gallery.technet.microsoft.com/Net-Cease-Blocking-Net-1e8dcb5b
- Make finding path hard again
  - Reduce the number of Domain Admins / highly privileged accounts
    - Less targets → longer paths
  - Reduce the attack graph's connectivity degree to break paths
    - Network segmentation
    - Multifactor authentication

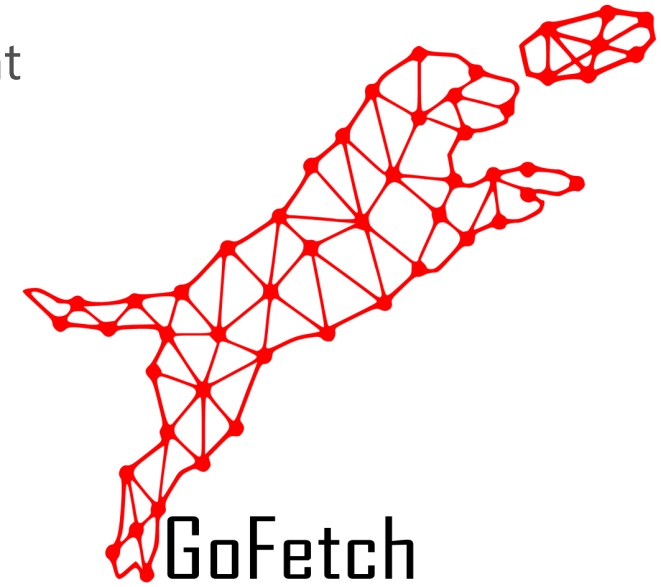
Fight: Attack the Automation

- Automation detection
  - Automatically monitor access patterns
    - Who connects to what, when
    - Detect abnormal rapid path traversal
  - Create fake shortest paths in advance
    - Honey-pots
    - Honey-Tokens
- Automation mitigation
  - Automation traps & baits: deception along the rapid path traversal
  - Adaptive Authentication: Dynamically enforce Multifactor Authentication along the rapid path traversal

Outro

Take Aways

- (Some) Attackers are financially motivated
- Therefore they strive for efficiency
- Lateral movement can, and therefore will, be automated
  - Use GoFetch! on your network to understand the implications
- Manual defense procedures will become obsolete
- Fighting Lateral Movement Industrialization
  - Reduce attack surface
  - Detect automation
  - Use GoFetch! on your network to make sure your defenses are relevant



Questions?