black hat® USA 2017

JULY 22-27, 2017
MANDALAY BAY / LAS VEGAS

The Industrial Revolution of Lateral Movement

Tal Be’ery, Independent
Tal Maor, Microsoft ATA

#BHUSA / @BLACKHATEVENTS

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
  - Improving Business Process through Innovation
- Industrialization of the Lateral Movement phase
  - GoFetch! Release
    - Open Source Lateral Movement Automation Tool
  - DEMO
- Implications of Lateral Movement Industrialization
  - For Attackers: Dropping cost, increased velocity
  - For Defenders: Make Lateral Movement Hard Again
- Outro
  - Summary + Recommendations

Intro

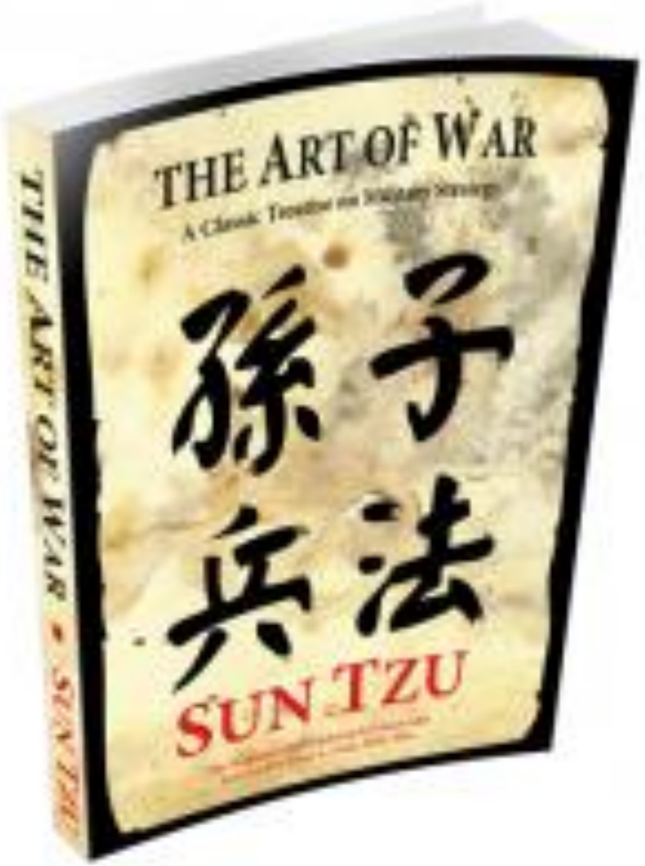
The Many Faces of Hacking

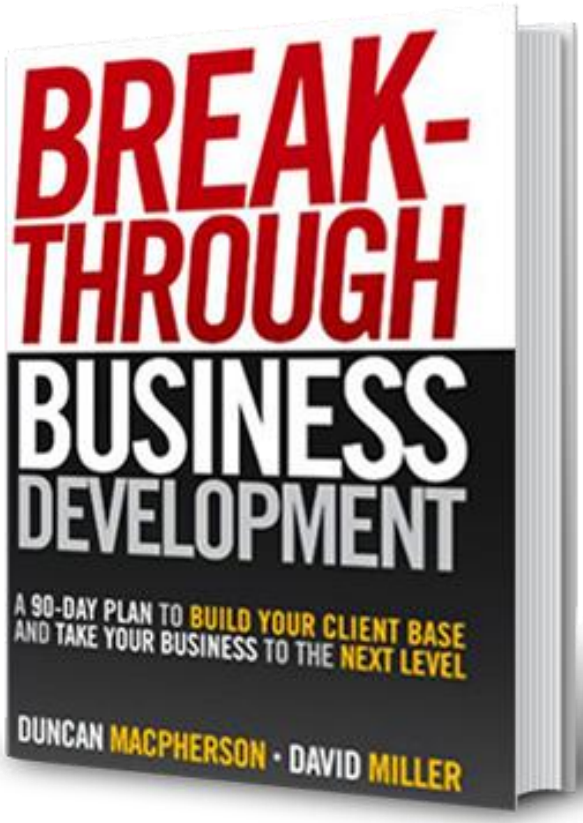
Hacktivism

Nation State

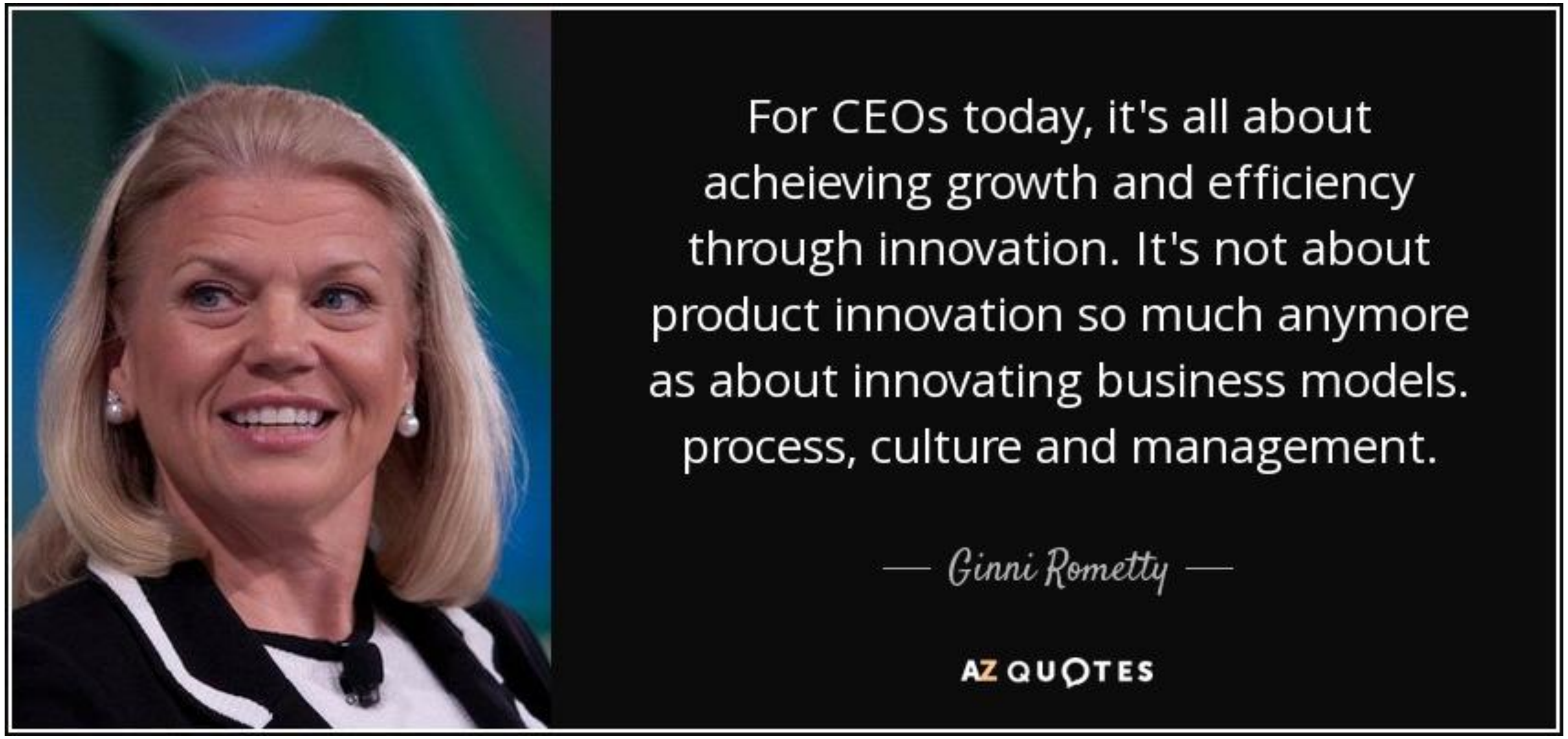
Financial

The Hacker CEO: Inspiration




BREAK-
THROUGH
BUSINESS
DEVELOPMENT
A 90-DAY PLAN TO BUILD YOUR CLIENT BASE
AND TAKE YOUR BUSINESS TO THE NEXT LEVEL
DUNCAN MACPHERSON · DAVID MILLER

The Hacker CEO Mission: Growth & Efficiency



For CEOs today, it's all about acheieving growth and efficiency through innovation. It's not about product innovation so much anymore as about innovating business models. process, culture and management.

— Ginni Rometty —

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

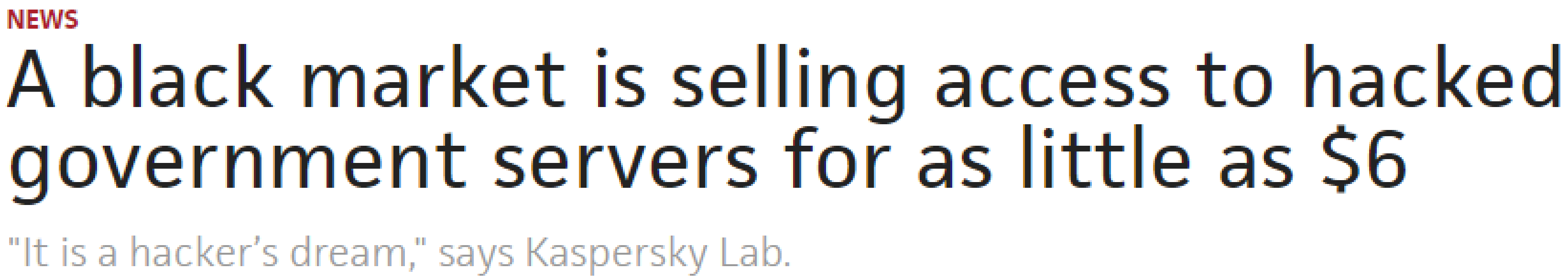
Domination

Actions on Data

Business Process Innovation: Automation

- The Penetration Value Chain is already highly automated
- Web application vulnerability abuse example:
  - Web vulnerability scanner
  - SQLmap
  - WebShell
- Very easy → create surplus
- Surplus creates marketplaces

Penetration



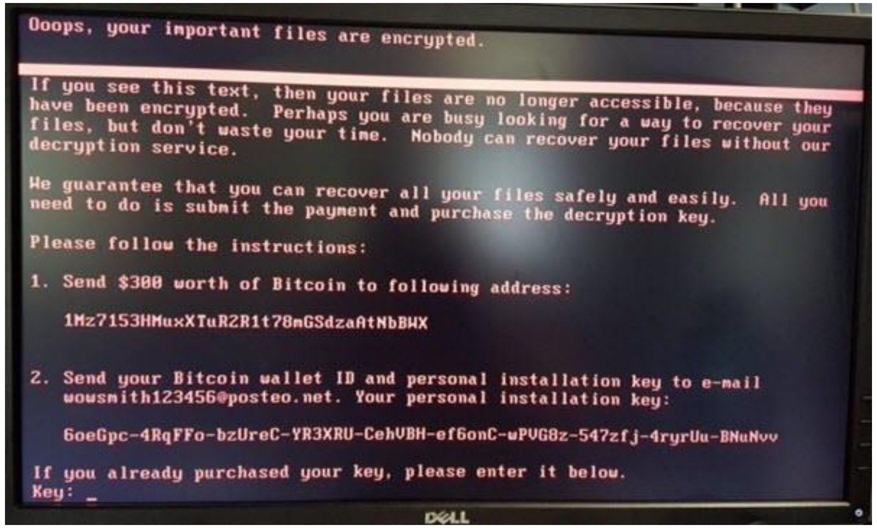
NEWS

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

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

Business Model Innovation: Ransomware

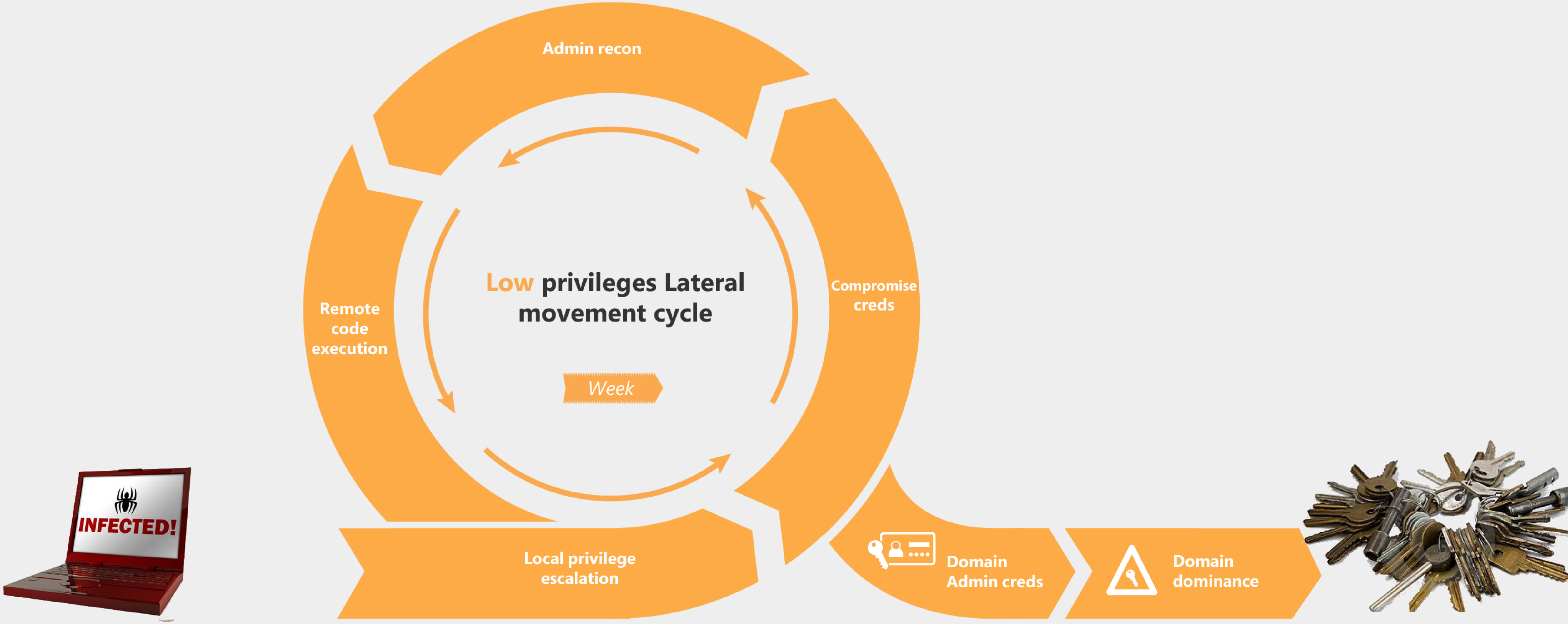
- Data Monetization is hard
  - Hard to understand what's interesting
  - Hard to find buyers
- Ransomware!
  - The victim is the buyer
  - Victim finds THEIR data interesting
  - Fast, Ubiquitous, Automatic



```
Ooops, your important files are encrypted.

If you see this text, then your files are no longer accessible, because they
have been encrypted.  Perhaps you are busy looking for a way to recover your
files, but don't waste your time.  Nobody can recover your files without our
decryption service.

We guarantee that you can recover all your files safely and easily.  All you
need to do is submit the payment and purchase the decryption key.

Please follow the instructions:

1. Send $300 worth of Bitcoin to following address:

   1Mz7153HMuxXTuR2R1t78mGSdzaAtNbBWX


2. Send your Bitcoin wallet ID and personal installation key to e-mail
   wowsmith123456@posteo.net. Your personal installation key:

   6oeGpc-4RqFFo-bzUreC-YR3XRU-CehVBH-ef6onC-wPVG8z-547zfj-4ryrUu-BNuNvv

If you already purchased your key, please enter it below.
Key: _
```

Actions on Data

The Domination Value Chain: Lateral Movement



Admin recon

Compromise creds

Remote code execution

Local privilege escalation

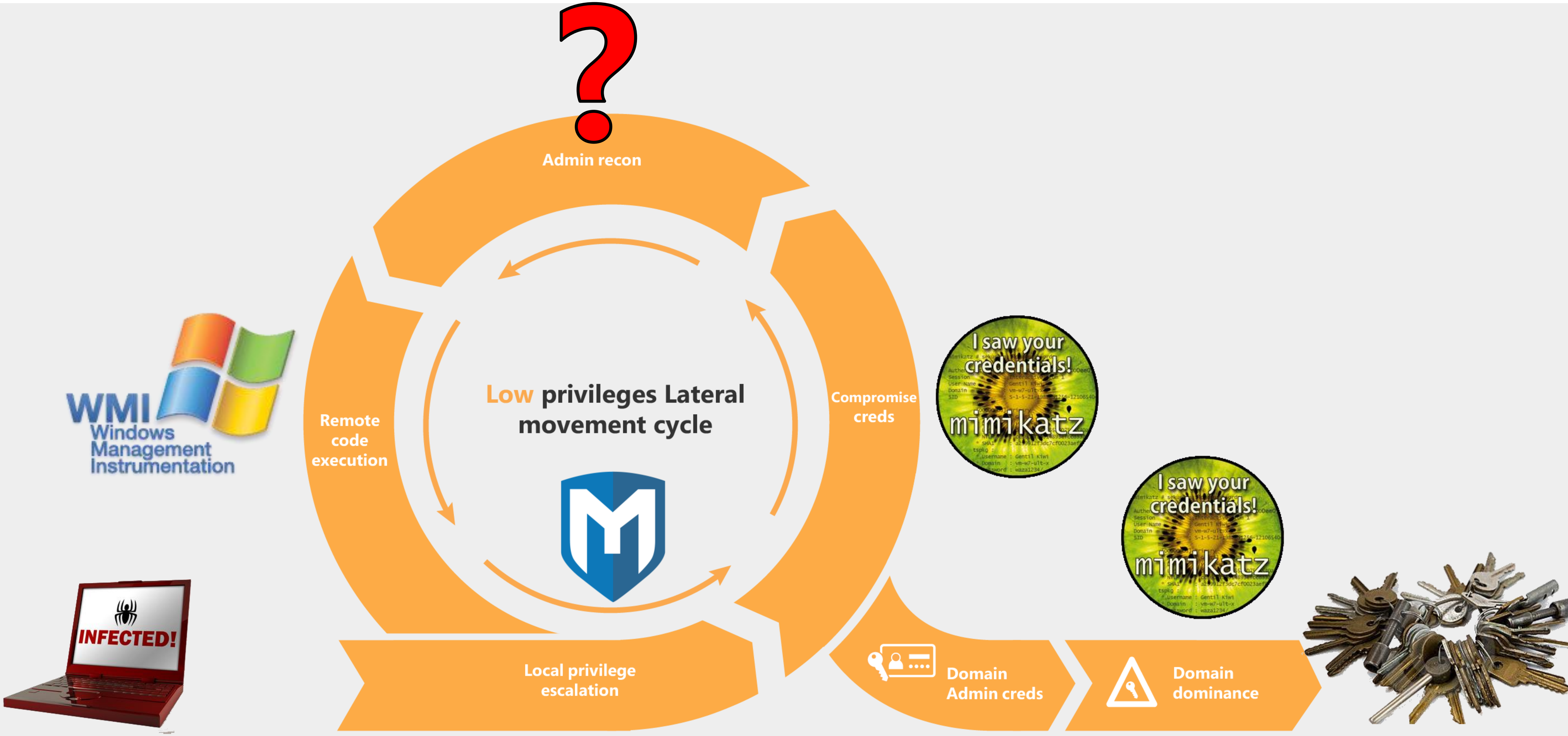
Low privileges Lateral movement cycle

Week

Domain Admin creds

Domain dominance

Business Process Innovation: Automation



Low privileges Lateral movement cycle

Admin recon

Compromise creds

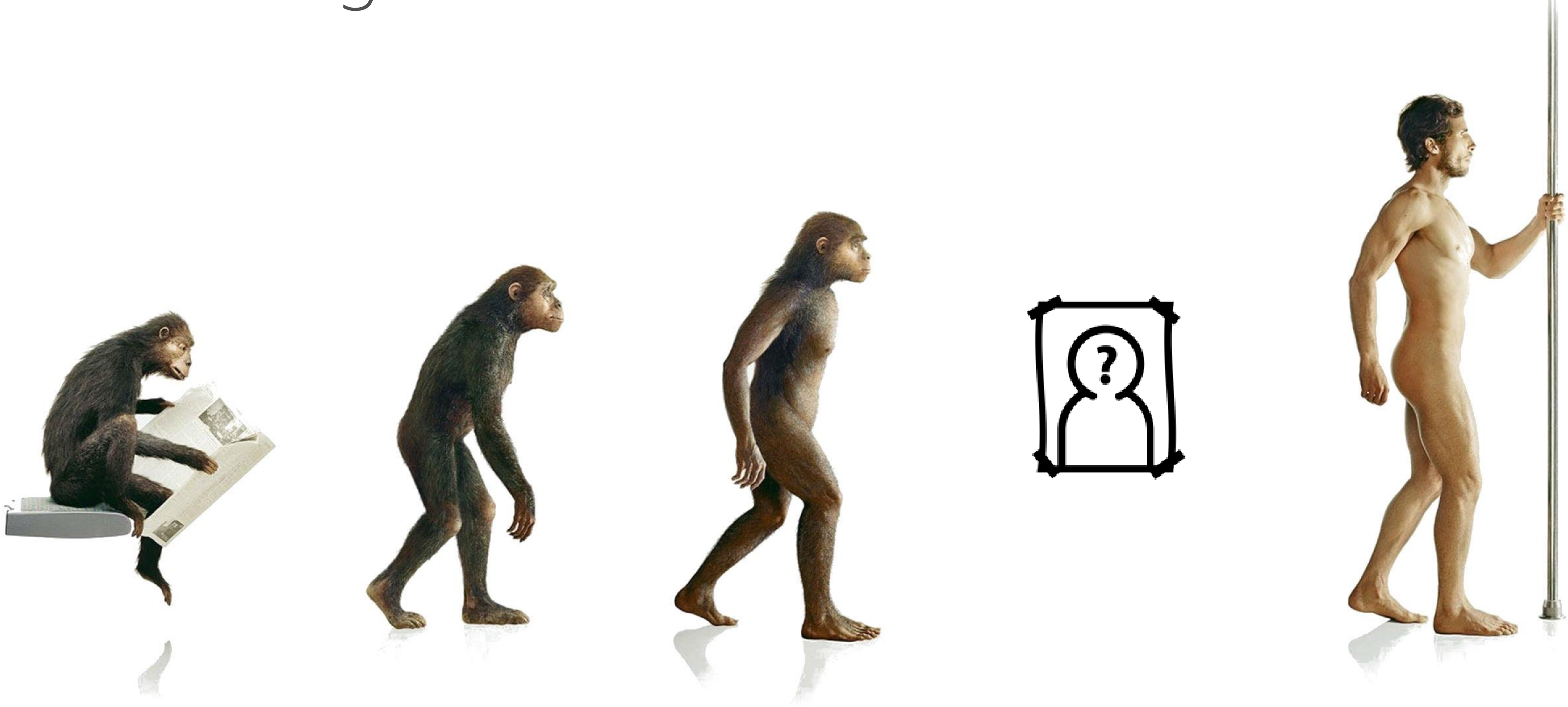
Local privilege escalation

Remote code execution

Domain Admin creds

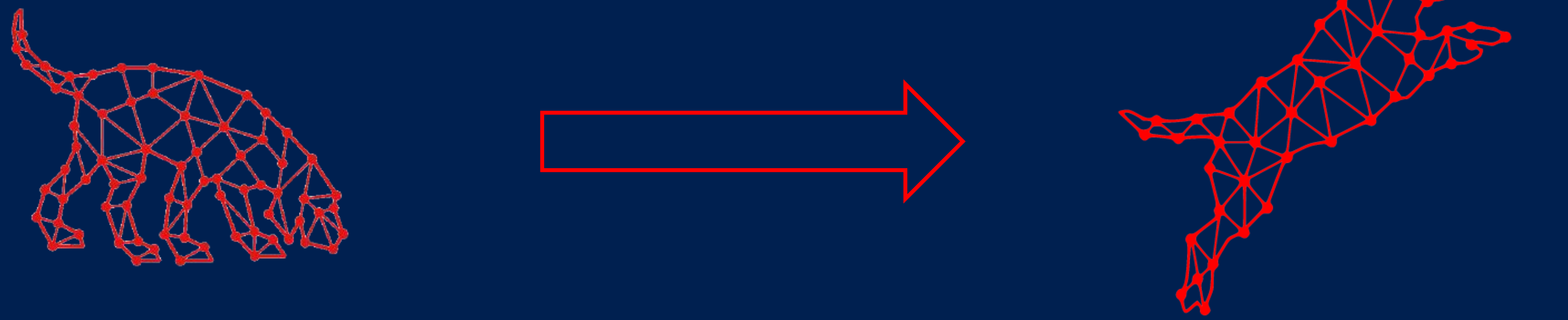
Domain dominance

The Missing Link: Admin Recon

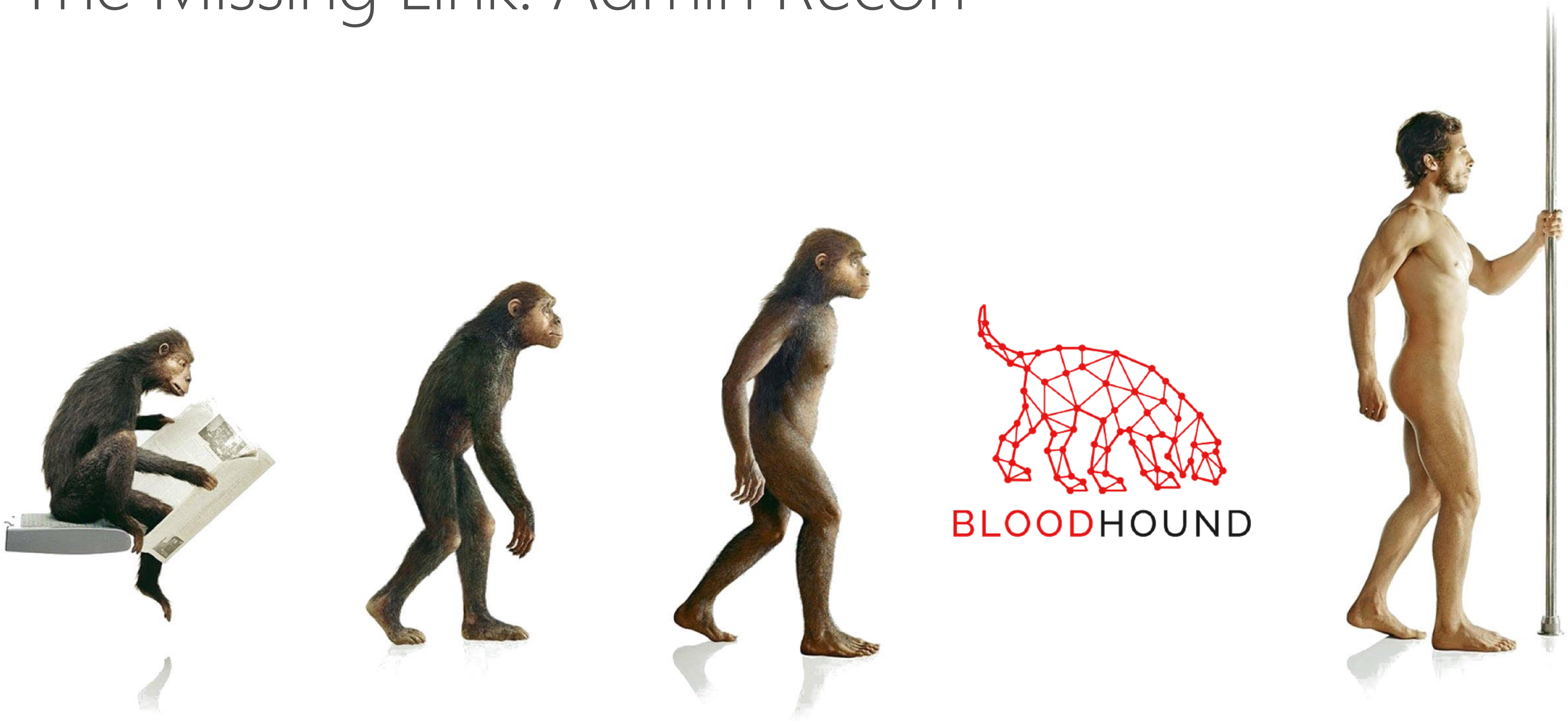


http://www.fanagrams.com/blog/wp-content/uploads/2011/03/Human-Evolution-Wallpaper2.jpg

The Automation

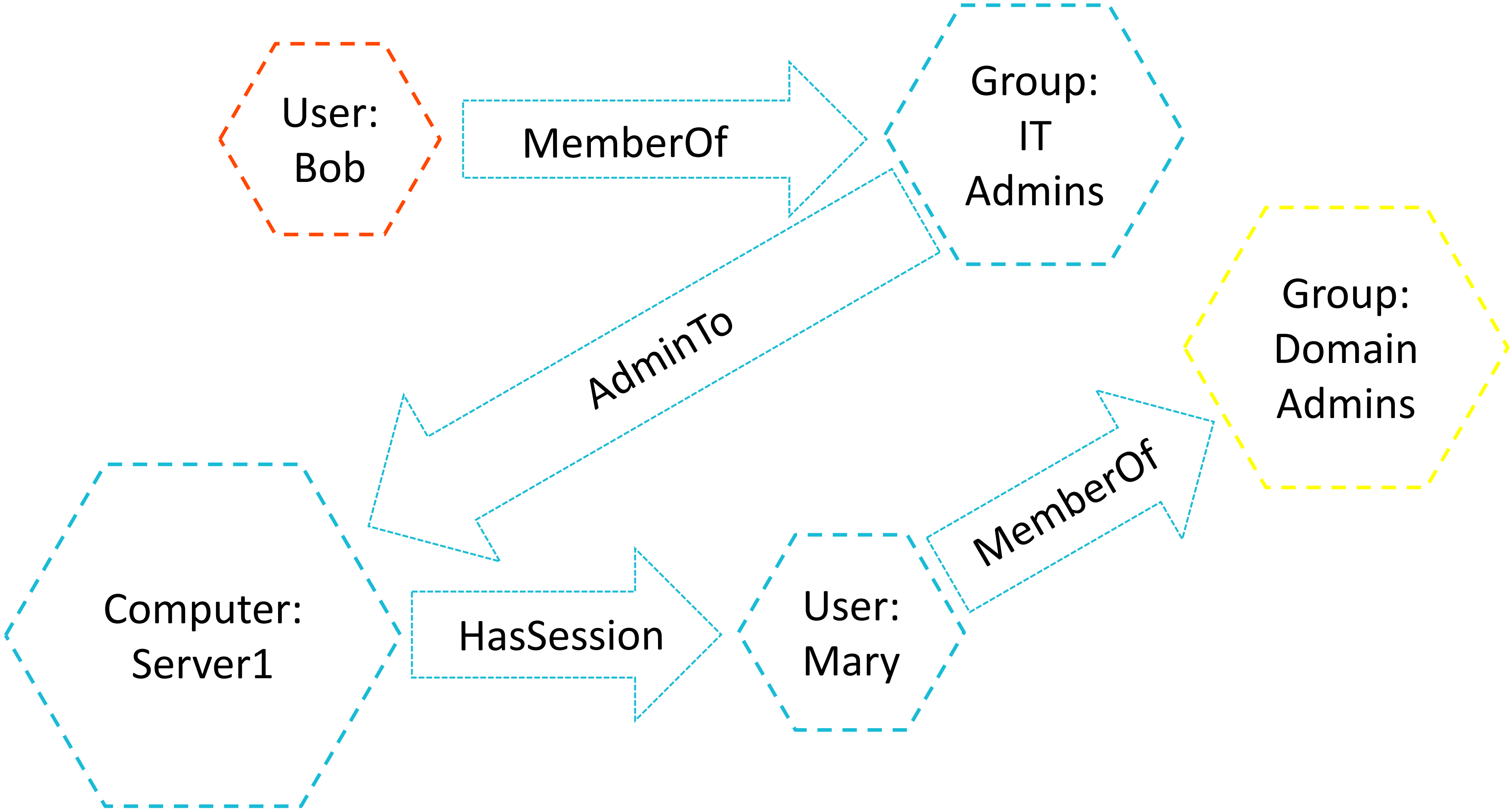


The Missing Link: Admin Recon



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

BloodHound In a Slide



User: Bob

MemberOf

Group: IT Admins

AdminTo

Computer: Server1

HasSession

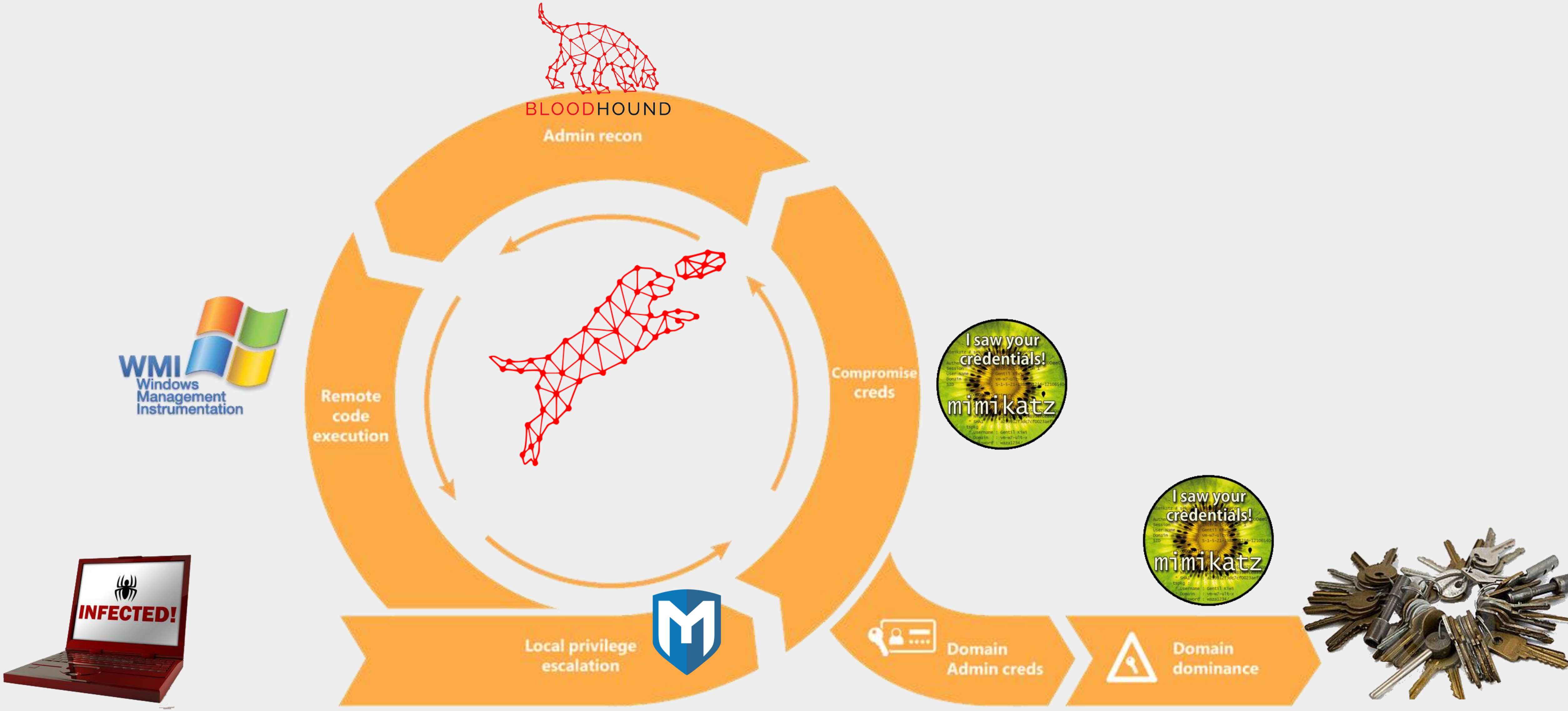
User: Mary

MemberOf

Group: Domain Admins

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

Attack Value-Chain



Admin recon

Compromise creds

Local privilege escalation

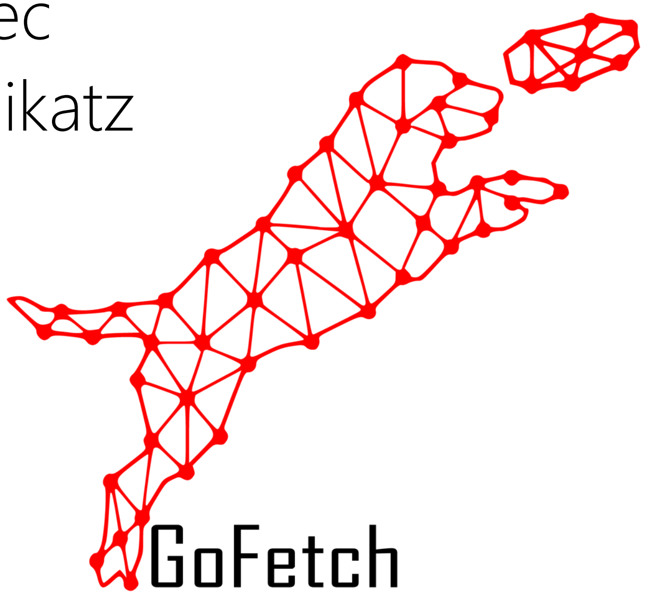
Remote code execution

Domain Admin creds

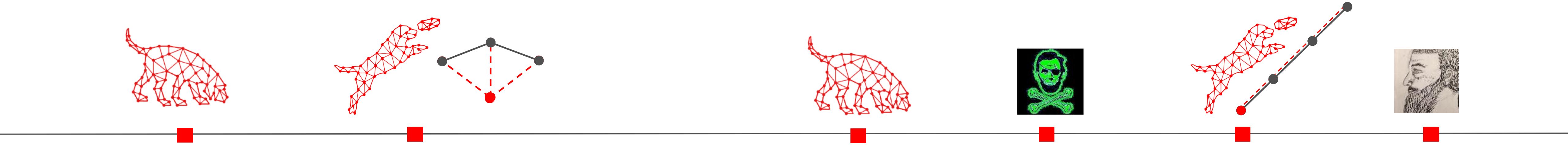
Domain dominance

Invoke-GoFetch

- Targeted Lateral Movement by a pre-determined path
  - Input:
    - Requested Network Path (e.g. BloodHound's output)
    - Payload to be run on the machines (optional)
  - Outputs
    - Credentials along the path
- Open Source! Coded in PowerShell
- Remote code execution 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



2017: Summer of Lateral Movement Automation



Aug 2016

BloodHound 1.0 Release

Nov 2016

GoFetch Alpha Demo @BHEU

May 2017

BloodHound 1.3 Release

May 2017

DeathStar Release

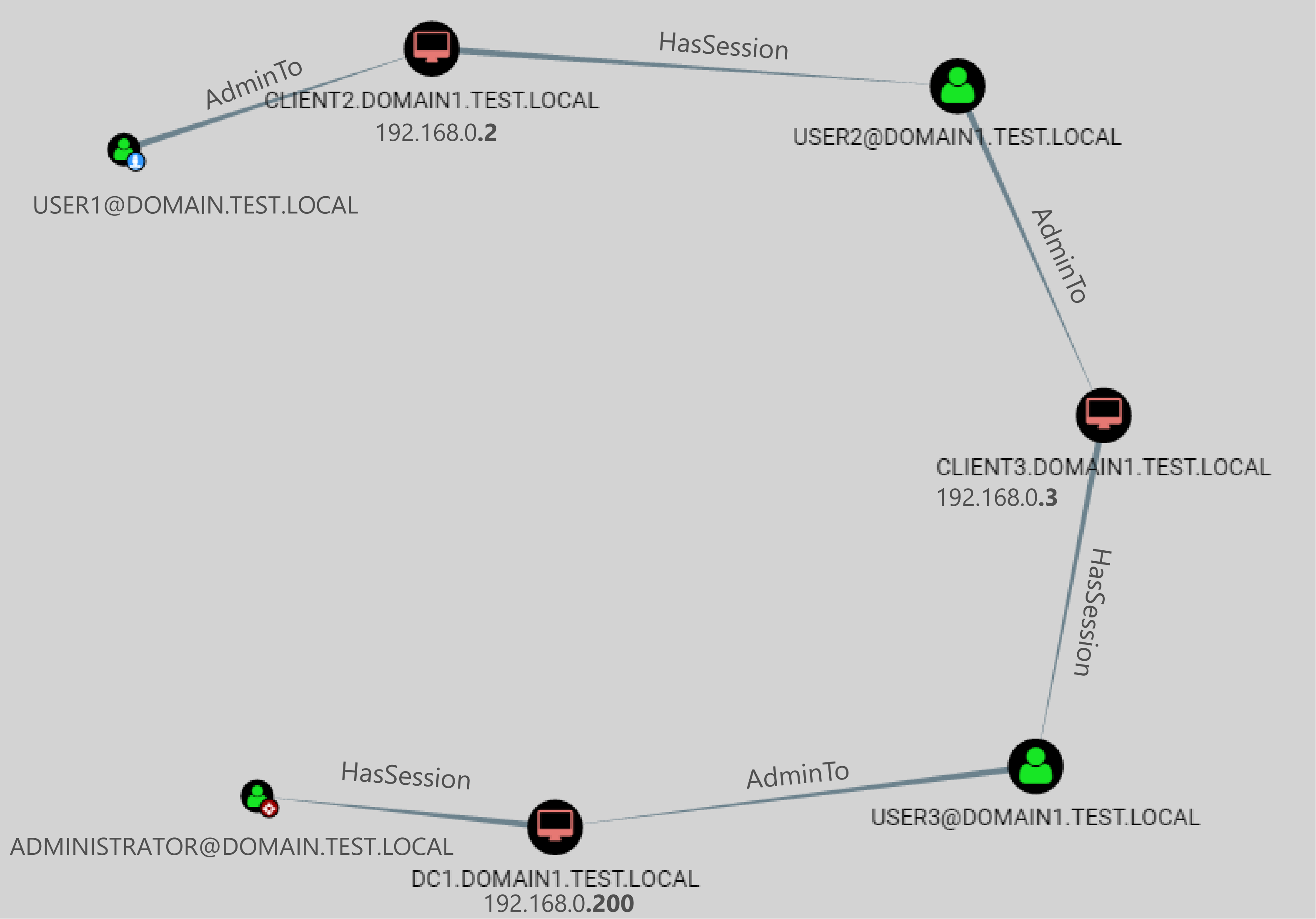
June 2017

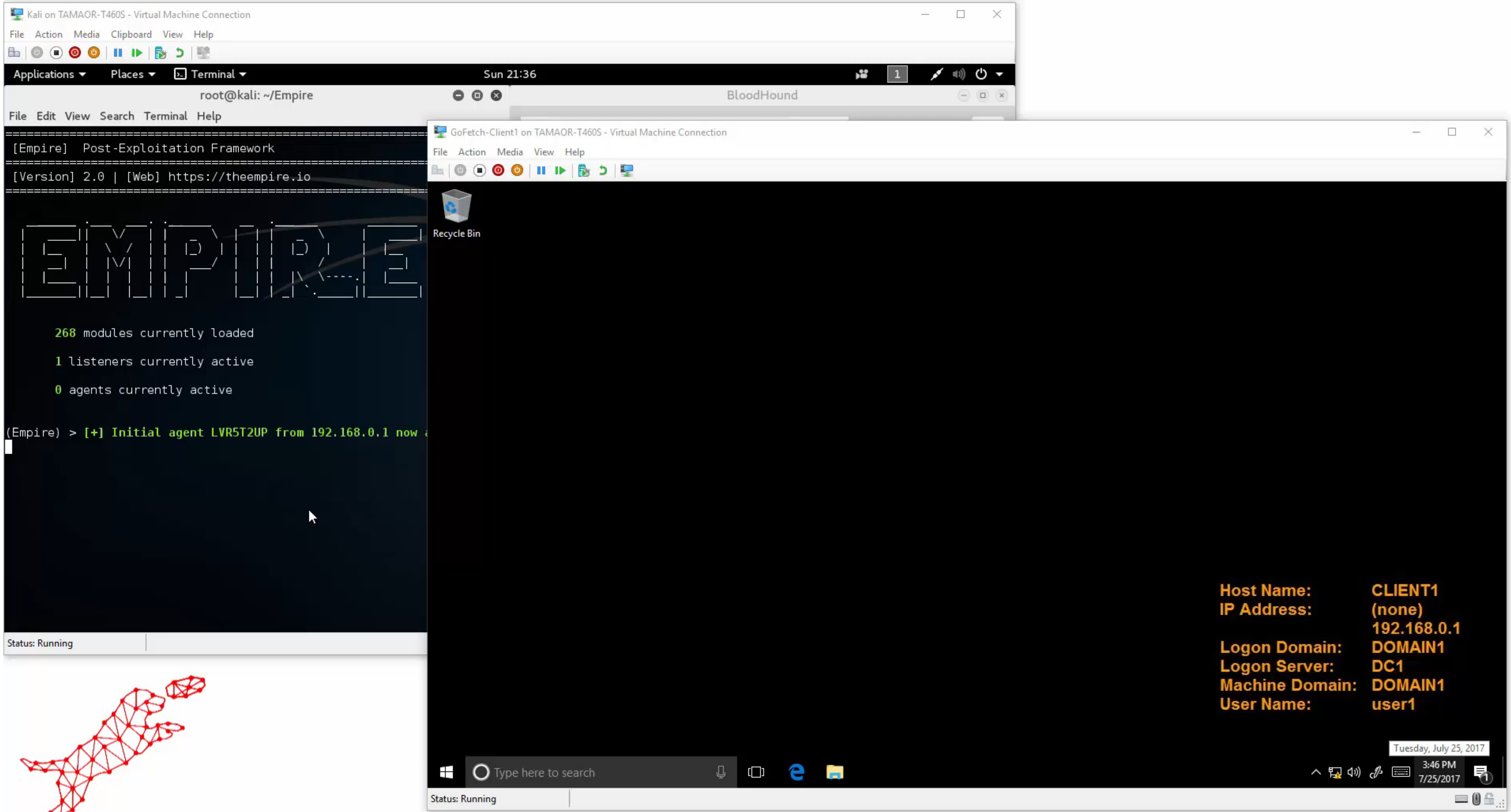
Invoke-GoFetch Release

June 2017

Integration of BloodHound & Empire

DEMO SETUP


AdminTo
CLIENT2.DOMAIN1.TEST.LOCAL
192.168.0.**2**
HasSession
USER2@DOMAIN1.TEST.LOCAL
USER1@DOMAIN.TEST.LOCAL
AdminTo
CLIENT3.DOMAIN1.TEST.LOCAL
192.168.0.**3**
HasSession
HasSession
AdminTo
USER3@DOMAIN1.TEST.LOCAL
ADMINISTRATOR@DOMAIN.TEST.LOCAL
DC1.DOMAIN1.TEST.LOCAL
192.168.0.**200**


Kali on TAMAOR-T460S - Virtual Machine Connection
File Action Media Clipboard View Help
Applications Places Terminal
Sun 21:36
root@kali: ~/Empire
File Edit View Search Terminal Help
BloodHound
GoFetch-Client1 on TAMAOR-T460S - Virtual Machine Connection
File Action Media View Help
Recycle Bin
Type here to search
Tuesday, July 25, 2017
3:46 PM
7/25/2017
Status: Running
Status: Running

```
[Empire]  Post-Exploitation Framework

[Version] 2.0 | [Web] https://theempire.io

      268 modules currently loaded

      1 listeners currently active

      0 agents currently active

(Empire) > [+] Initial agent LVR5T2UP from 192.168.0.1 now a
```

```
Host Name:          CLIENT1
IP Address:         (none)
                    192.168.0.1
Logon Domain:       DOMAIN1
Logon Server:       DC1
Machine Domain:     DOMAIN1
User Name:          user1
```

GoFetch

Invoke-GoFetch Lateral Movement

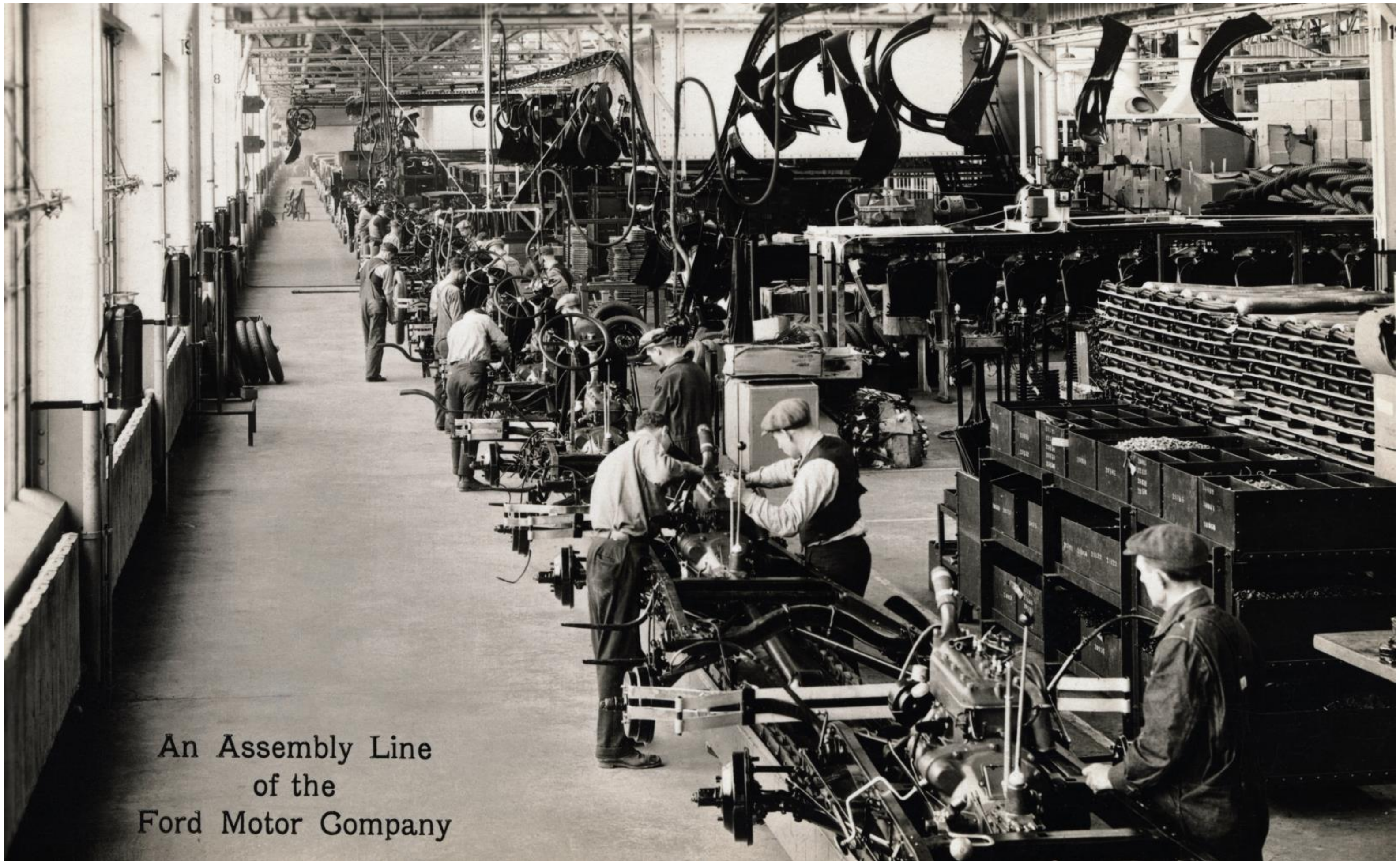
- Targeted expansion means less machines are touched
  - Stealthier
  - Faster
- No C2 connectivity needed
  - Fire and Forget: Expansion logic (next target) is transmitted to the edges
  - Less communication -> stealthier

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

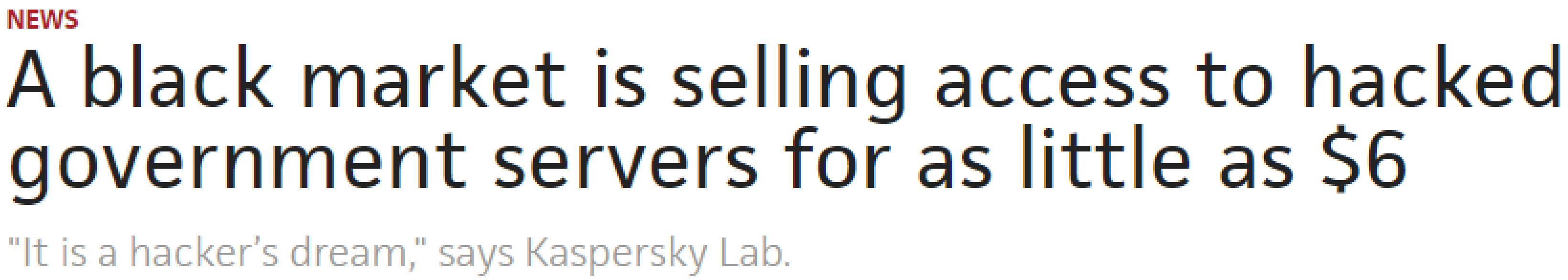
Mass Production



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.

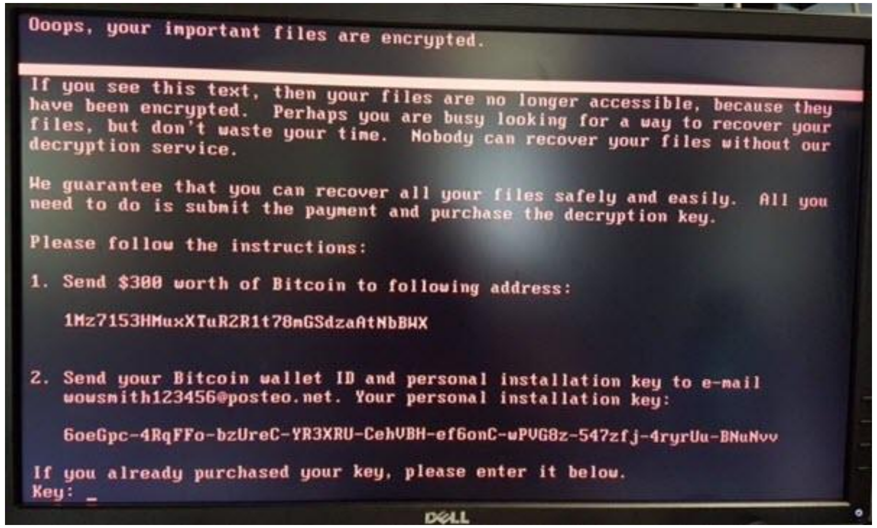
Defense Reactions to Industrialization

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



```
Ooops, your important files are encrypted.

If you see this text, then your files are no longer accessible, because they
have been encrypted.  Perhaps you are busy looking for a way to recover your
files, but don't waste your time.  Nobody can recover your files without our
decryption service.

We guarantee that you can recover all your files safely and easily.  All you
need to do is submit the payment and purchase the decryption key.

Please follow the instructions:

1. Send $300 worth of Bitcoin to following address:

   1Mz7153HMuxXTuR2R1t78mGSdzaAtNbBWX


2. Send your Bitcoin wallet ID and personal installation key to e-mail
   wowsmith123456@posteo.net. Your personal installation key:

   6oeGpc-4RqFFo-bzUreC-YR3XRU-CehVBH-ef6onC-wPVG8z-547zfj-4ryrUu-BNuNvv

If you already purchased your key, please enter it below.
Key: _
```

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

GoFetch

Questions?

GoFetch