RSAConference2015

Abu Dhabi | 4–5 November | Emirates Palace

CHANGE

Challenge today's security thinking

SESSION ID: CIN-R06

Becoming the Adversary

Tyrone Erasmus

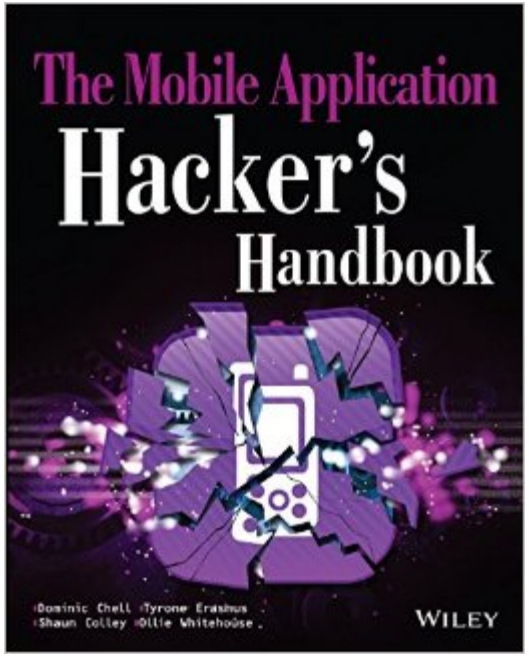
Managing Security Consultant
MWR InfoSecurity
@metall0id

#RSAC

/usr/bin/whoami

- Most public research == Android

drozer



- Something different today ☺

Overview

- Introduction
- Viewing your organisation from the outside
- The attacker mind-set
- Mechanics of a targeted attack
- Case studies
- Defenders vs. attackers

Security in organisations

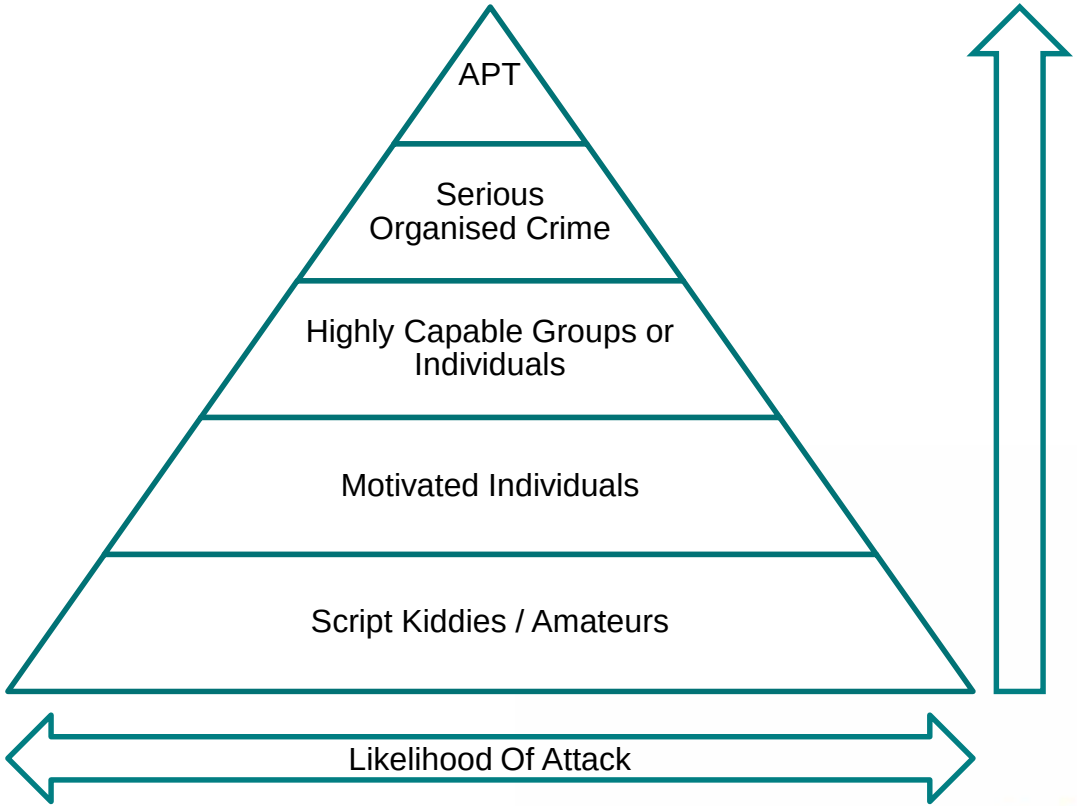
- What does “security” mean in your organisation?
  - Fixing vulnerabilities
  - Reaching some compliance standard
  - Buying security equipment: firewalls/IPS

- What are you actually trying to prevent?

Understanding your adversary

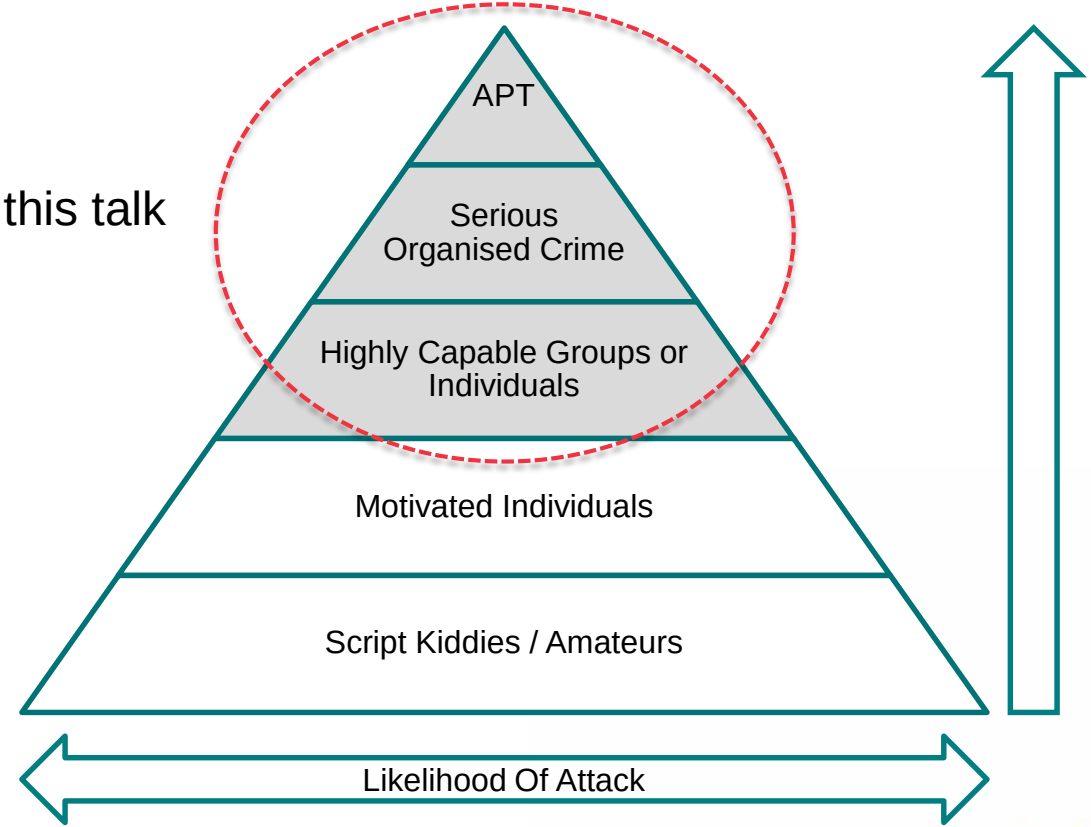
- Organisations don’t have unlimited money for security
- Defence must be tailored to the motivations of your most likely threat actor
- If you understand what they are after, you will understand how to prioritise your security spend

Threat actors



Threat actors

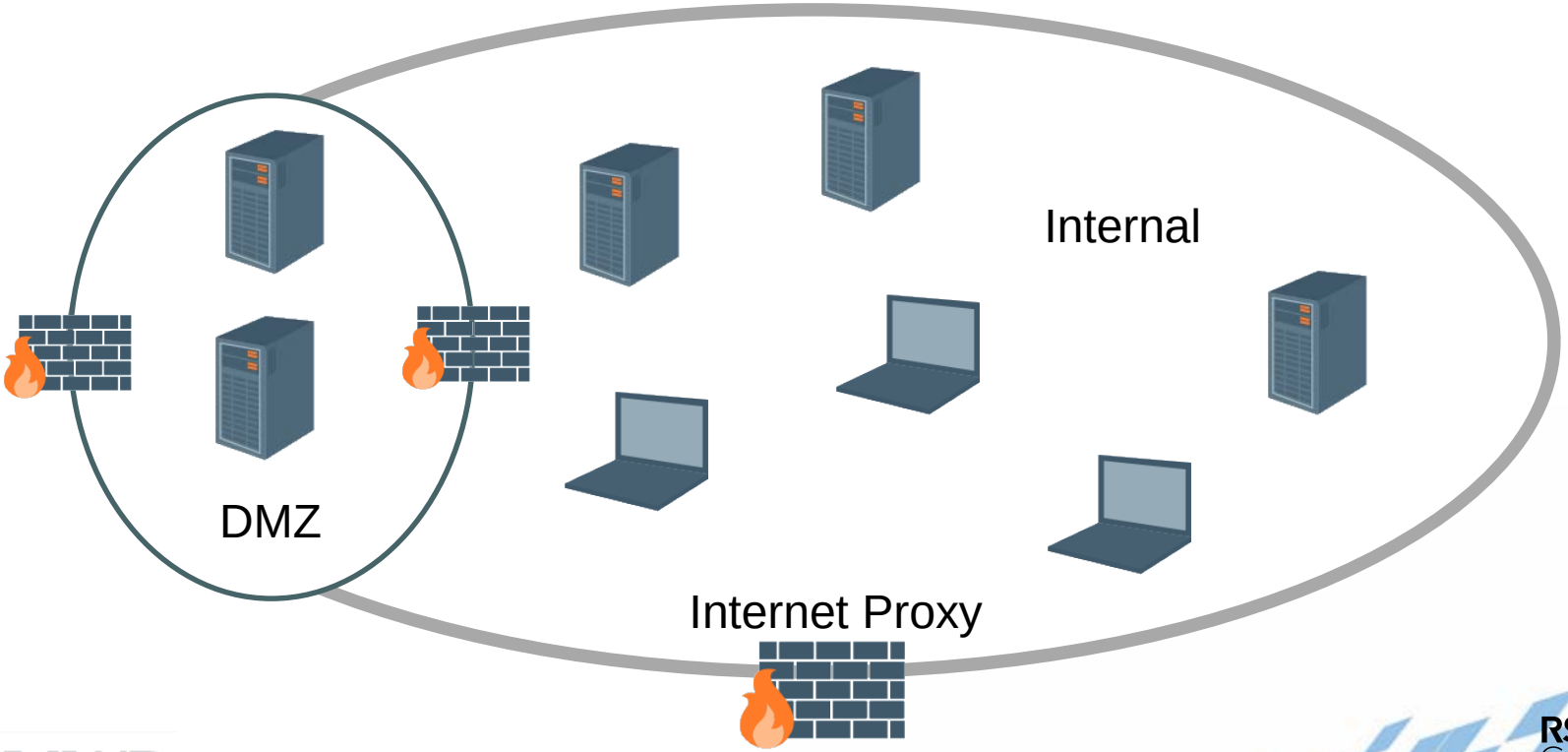
Focus of this talk



More Targeted

Likelihood of successful attack increases

Your organisation

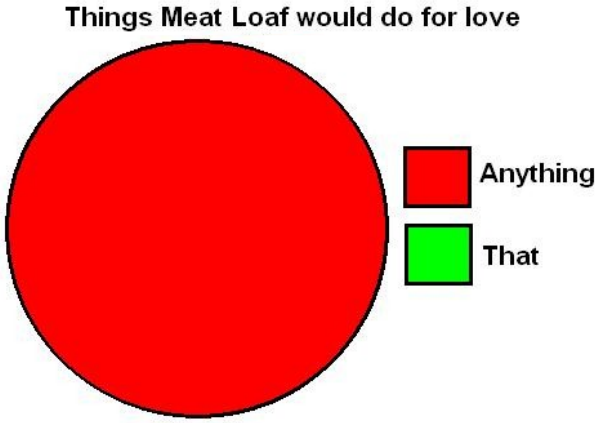


The attacker mind-set

- Attackers want what you have
  - Money
  - Intellectual property
  - Client data
  - Secret information
  - Reputation
  - <fill in your core assets here>

The attacker mind-set

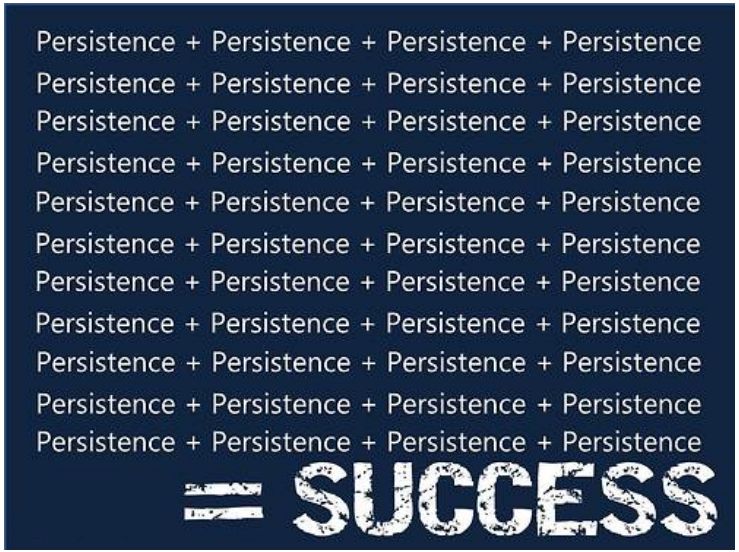
- This information is on your internal network
- Select **employees** have access to it



- Attackers are also constrained by money
  - Easier/quicker is always better
  - ROI is important

The attacker mind-set

- They don’t care about
  - What security testing you have done
  - “Out of scope” systems
  - Rules for “fair play”
- They are relentless



We are not opportunistic skids with DDoS or SQLi scanners or defacements. We are dedicated, focused, skilled, and we're never going away. If you profit off the pain of others, whatever it takes, we will completely own you.

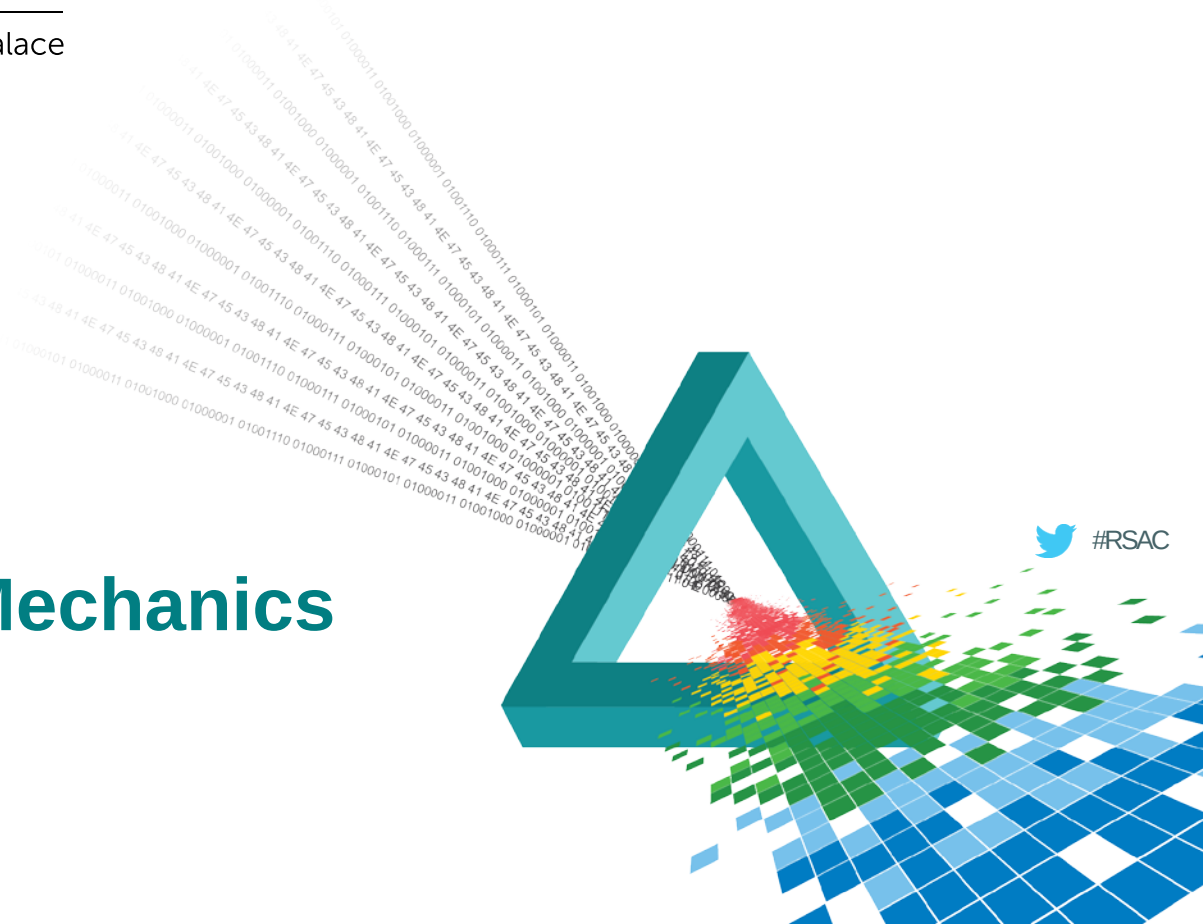
Our one apology is to Mark Steele (Director of Security). You did everything you could, but nothing you could have done could have stopped this.

Impact Team

Note to Ashley Madison from Impact Team

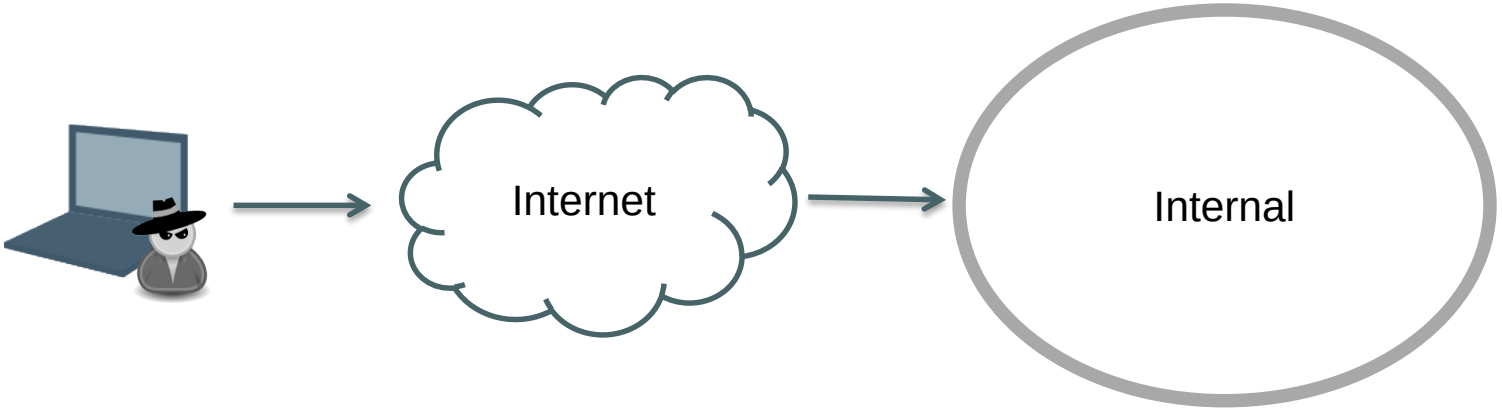
RSAConference2015

Abu Dhabi | 4–5 November | Emirates Palace



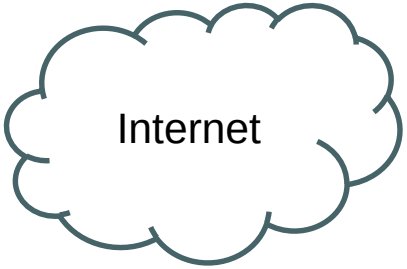
#RSAC

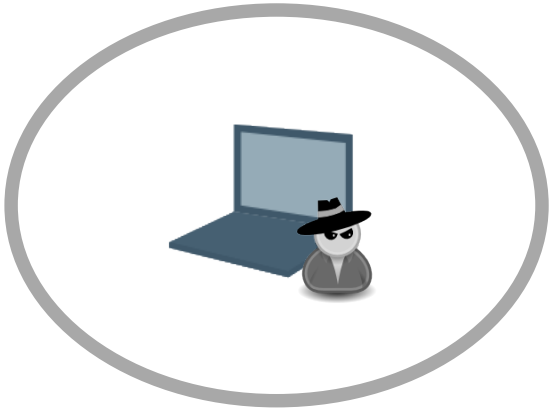
Targeted Attack Mechanics



Perimeter breach

What is it?



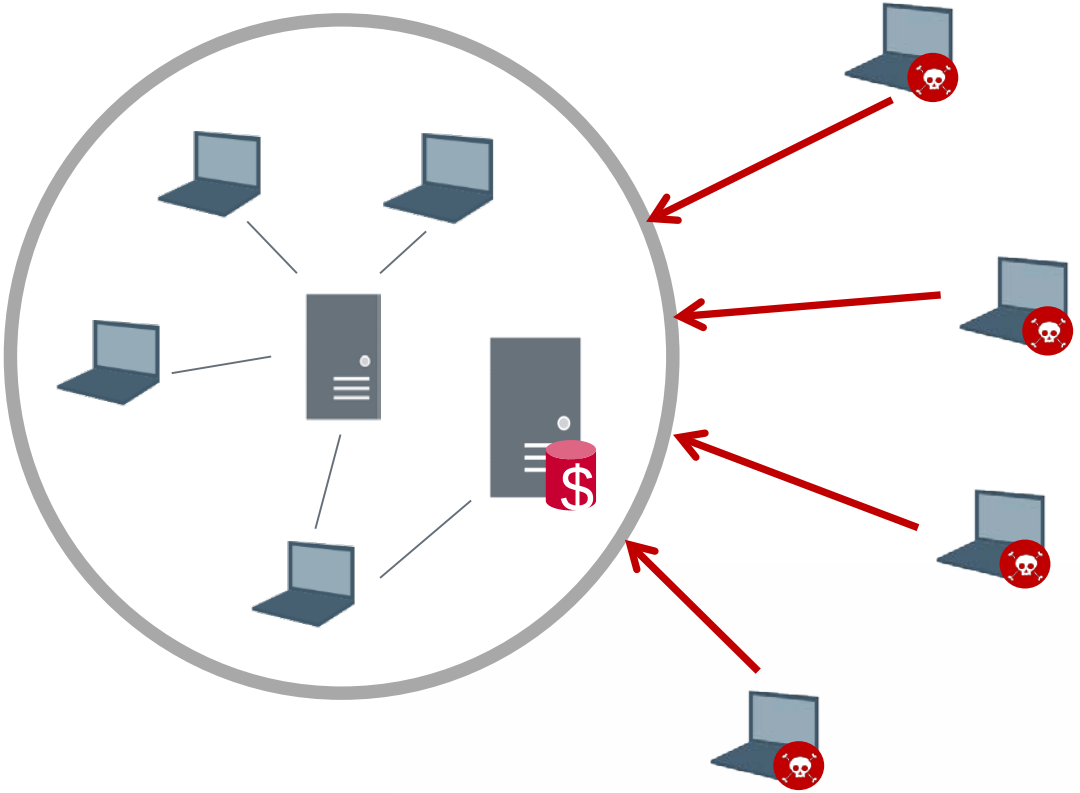


Perimeter breach

Internal network access from the internet!

Perimeter breach

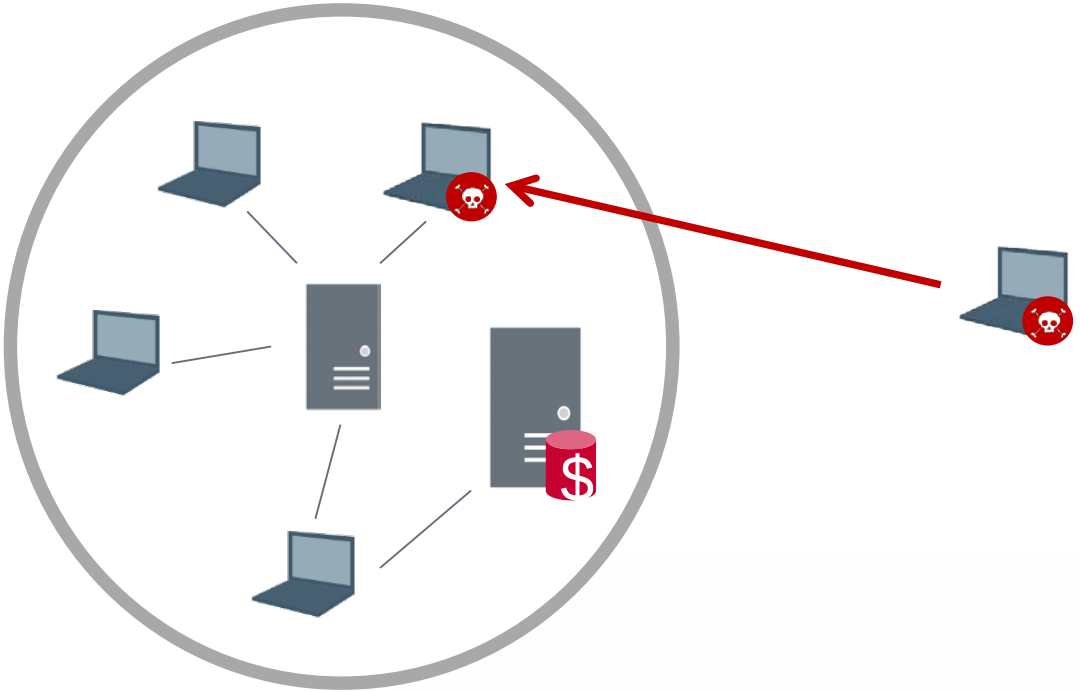
- Classic techniques
  - Attacking VPNs
  - Web application vulnerabilities
  - RDP
  - Other remote access services e.g. SSH



Attacking the perimeter

Perimeter breach

- Modern techniques
  - Client-side memory corruption exploits
  - Abusing “features” in client software
  - Watering hole attacks



Attacking a user over email

Perimeter breach (for cheapskates)

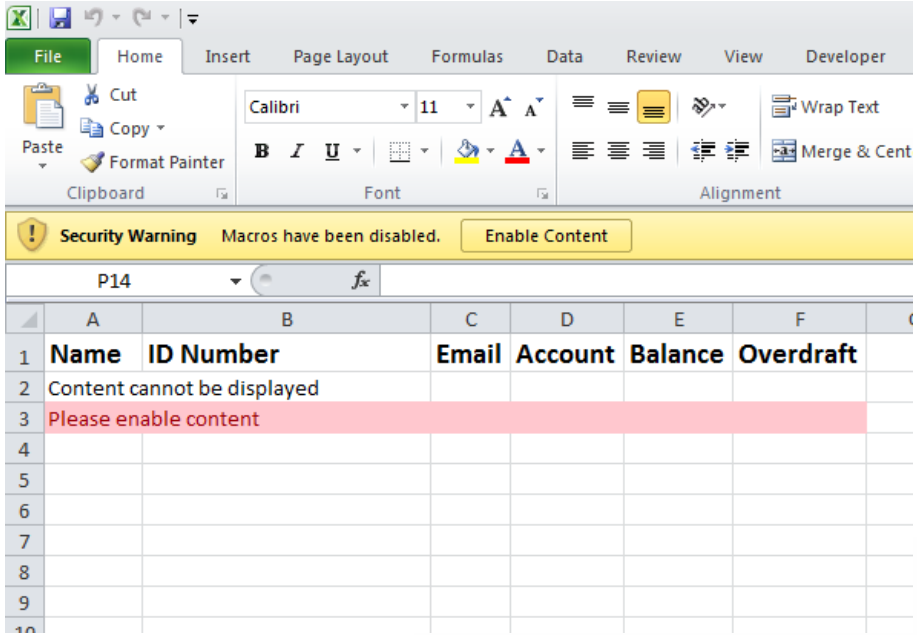
- Think less about memory corruption exploits
  - Software targeting has to be perfect
  - Exploit may fail
- Think more about features
  - Office macros
  - Java applets
  - Click-once applications
  - HTML applications
  - Browser extensions

Our quickest perimeter breach

- Find email addresses using free tools

```
$ python theHarvester.py -d mwrinfosecurity.com -l 200 -b google
```

```
[+] Emails found:
------------------
luke.jennings@mwrinfosecurity.com
James.Moore@mwrinfosecurity.com
georgi.geshev@mwrinfosecurity.com
nils@mwrinfosecurity.com
Chandler@mwrinfosecurity.com
pci.sa@mwrinfosecurity.com
ripe@mwrinfosecurity.com
martyn.ruks@mwrinfosecurity.com
rafa@mwrinfosecurity.com
whiterabbit2015@mwrinfosecurity.com
Ian.shaw@mwrinfosecurity.com
james.moore@mwrinfosecurity.com
Ian.shaw@mwrinfosecurity.com
info@mwrinfosecurity.com
Ruks@mwrinfosecurity.com
Levi@mwrinfosecurity.com
siebert.lubbe@mwrinfosecurity.com
Rhodes@mwrinfosecurity.com
```

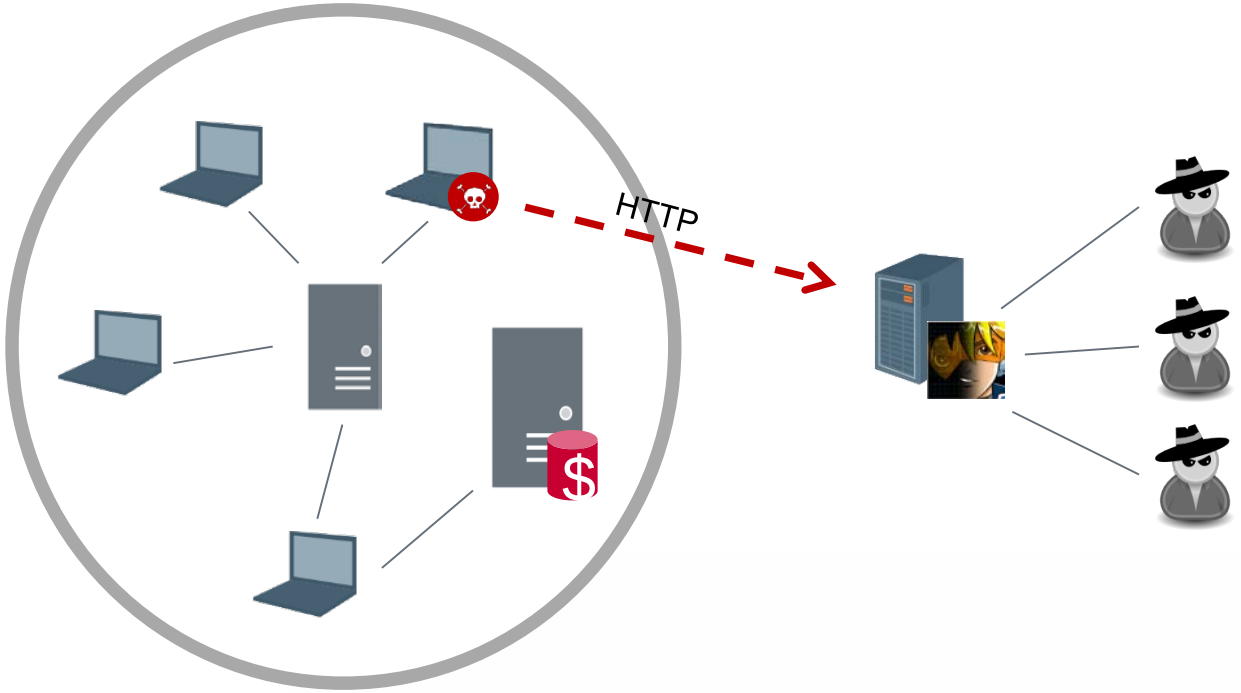


Our quickest perimeter breach

account-update.xlsm

Our quickest perimeter breach

4 minutes later…



Our quickest perimeter breach

4 minutes later…

Privilege Escalation

- Likely have limited access once inside
- Need to escalate your privileges
  - Either escalate on that host
  - Or move laterally

Local privilege escalation

- Obtain SYSTEM
- Shared local admin password?
- Processes from other domain users – steal token?
- More on this later…

Lateral movement

- Don’t use scanning and exploits
- This will get you caught

- Think
  - Misconfigurations
  - Active directory abuse

Lateral movement

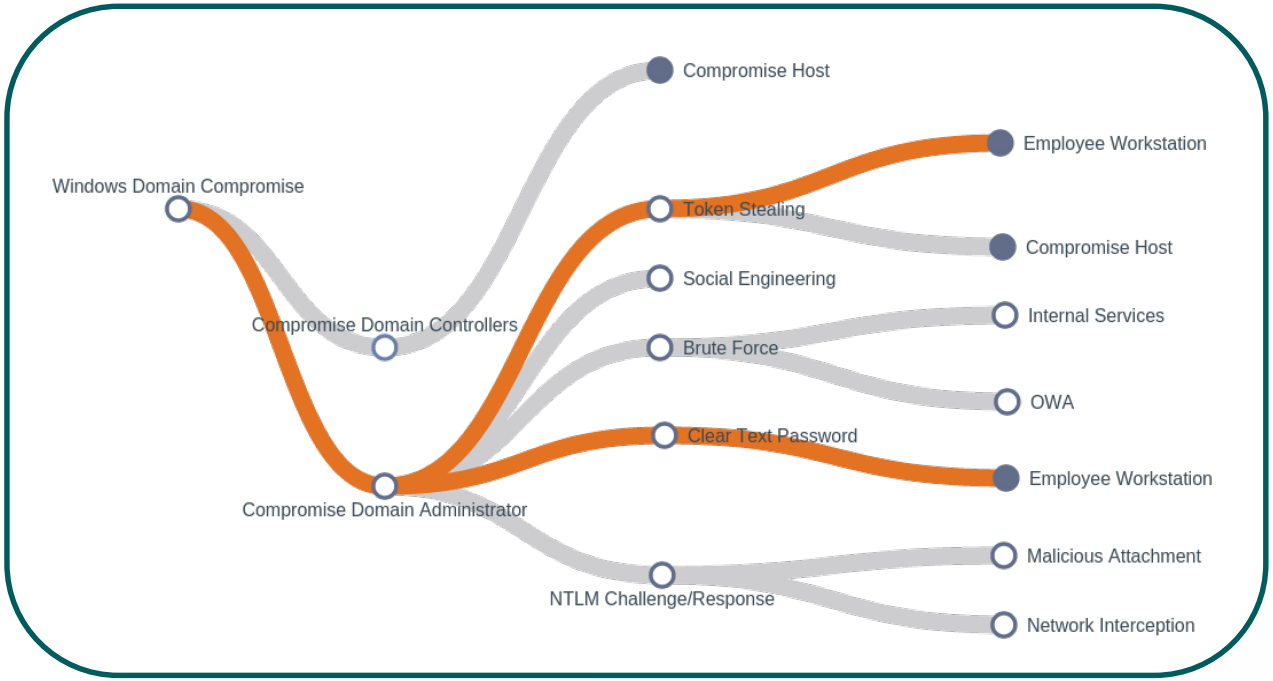
- Local Admin passwords stored in group policy?
- Passwords lying around on file shares?
- Current compromised computer have admin access on any other computers?
- If you have any passwords, does any useful account have same password?

Lateral movement

- Privilege escalations are about finding local admin access on computers where Domain Admins have logged in
- Perhaps Domain Admin access is not required to do your evil deeds

Lateral movement

- Things to do with local admin access
  - Steal user passwords (mimikatz)
  - Steal SATs (incognito)
- Rinse and repeat until getting domain admin



Some attack paths to Windows Domain compromise

Post domain admin

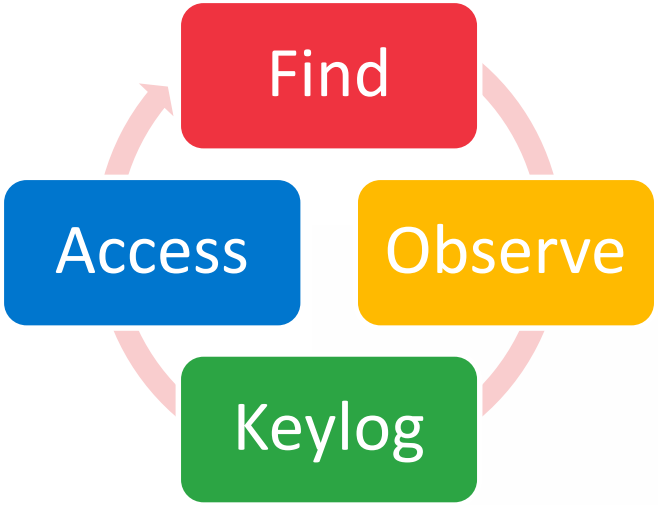
- Classic techniques
  - Dump domain hashes
  - Crack passwords
  - Pass the hash

```
meterpreter > hashdump
Administrator:500:e52cac67419a9a224a3b108f3fa6cb6d:8846f
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:f3f07224e22c
SUPPORT_388945a0:1001:aad3b435b51404eeaad3b435b51404ee:4
user:1003:b34ce522c3e4c8774a3b108f3fa6cb6d:a87f3a337d730
```

- Modern techniques
  - Golden tickets
  - Overpass-the-hash
  - DCSync
  - Skeleton key

User exploitation (Raphael Mudge™)

- Abusing user access to obtain goals
- Methodology



User exploitation

- Depends on goal of attackers
- Find user(s) with access to asset

Example: User exploitation

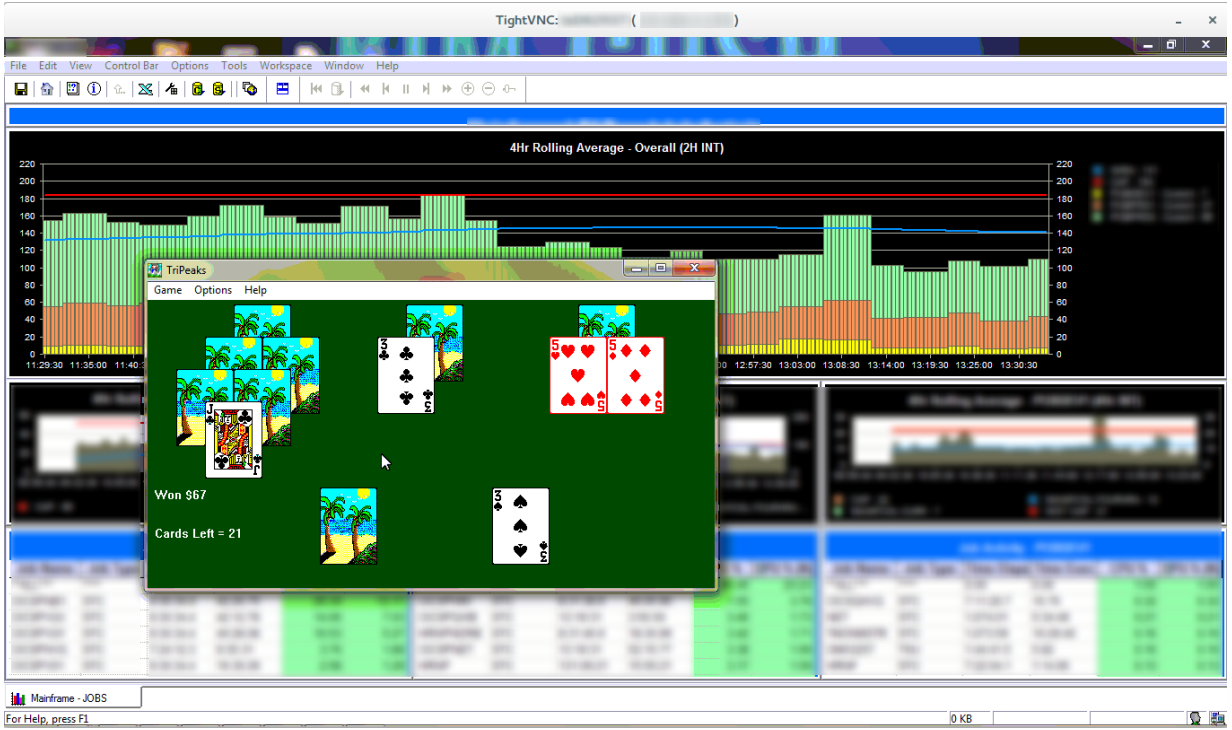
- Goal: Make a payment using finance systems
- Pull all active directory groups
- Read emails / Exchange groups
- Search for finance/disbursements group names

Example: User exploitation

- Get list of users in those groups
- Find them on network
  - Netsessions API
  - Event logs on Domain Controllers
  - Many more…
- Deploy secret VNC to machines

Example: User exploitation

- Start keylogger
- Watch them use applications
  - Learn
  - Learn
  - Learn
- Do their actions need authorisation?
  - Same process for authoriser



Solitaire session watched over VNC while waiting to see mainframe use

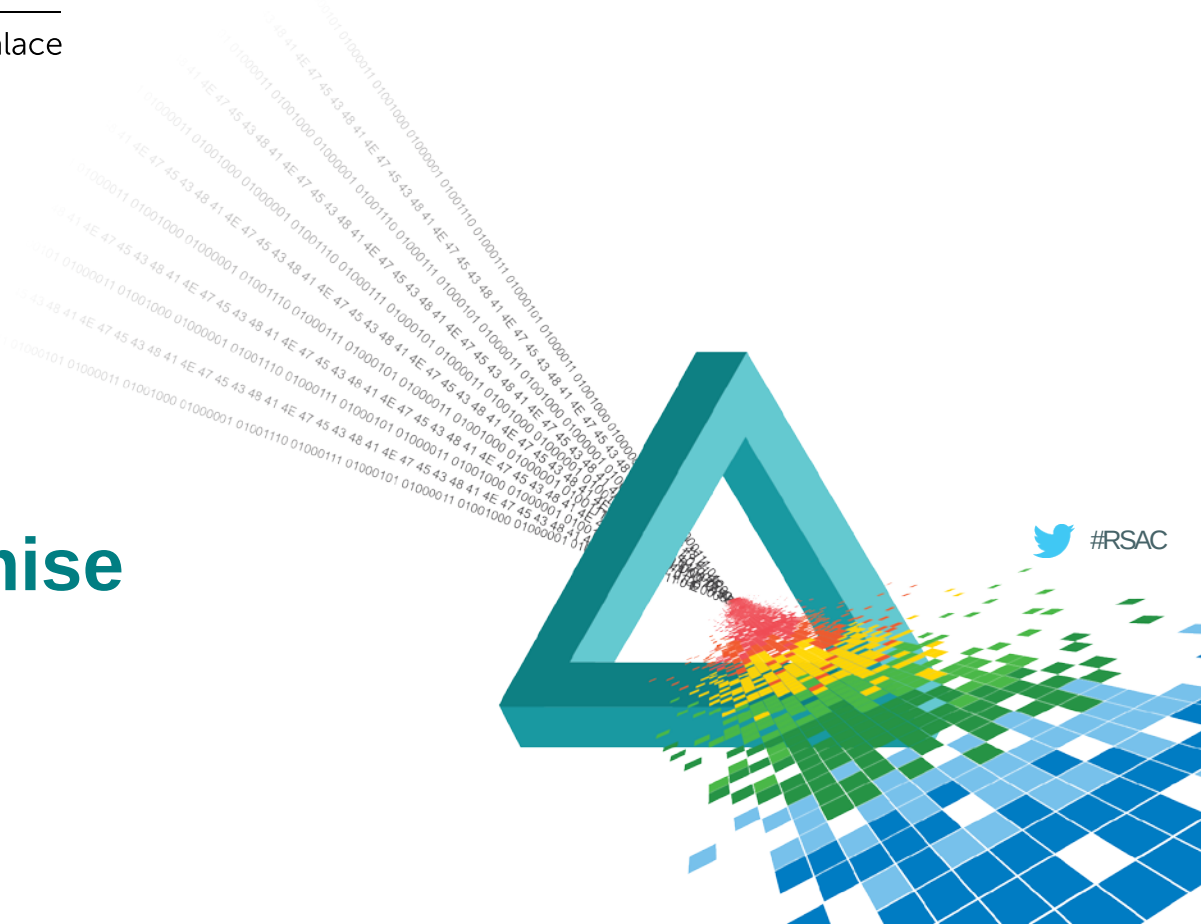
Example: User exploitation

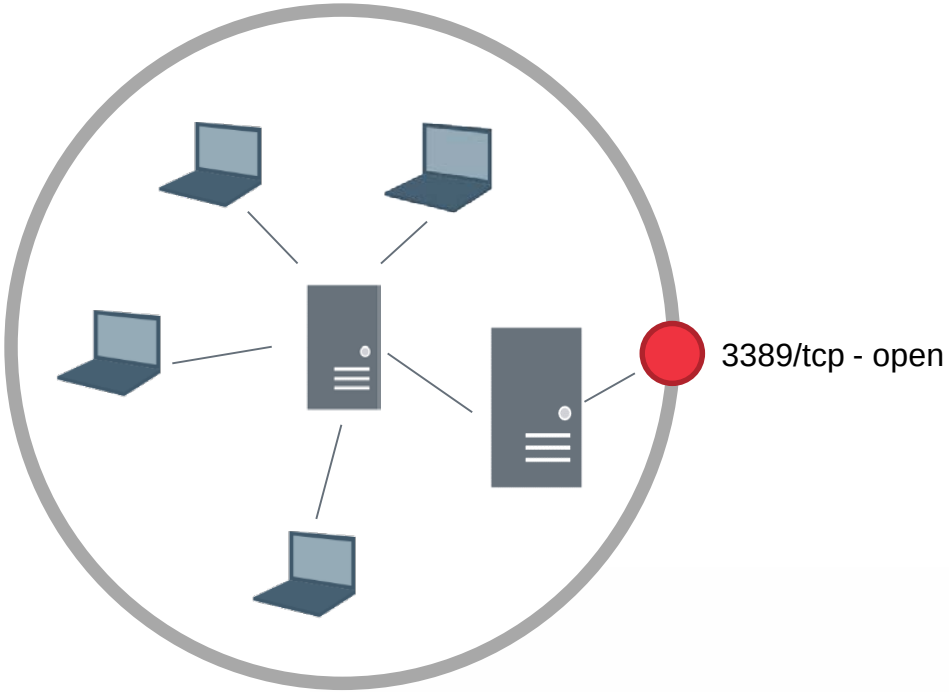
- Gather stolen credentials for all parties involved
- Replicate entire business process
- Make payment

RSAConference2015

Abu Dhabi | 4–5 November | Emirates Palace

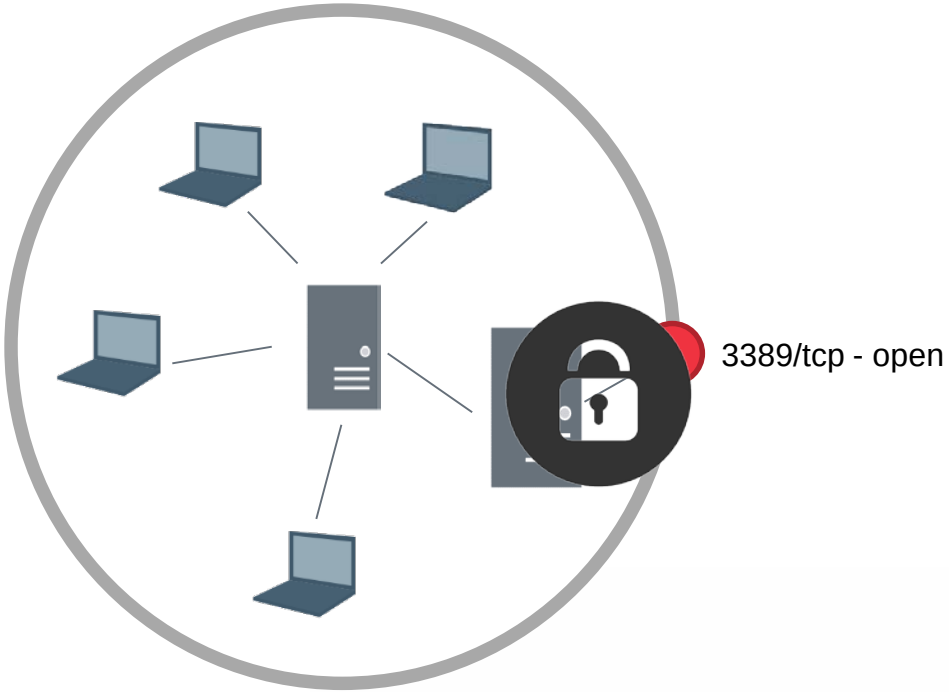
Domain Compromise Case Studies





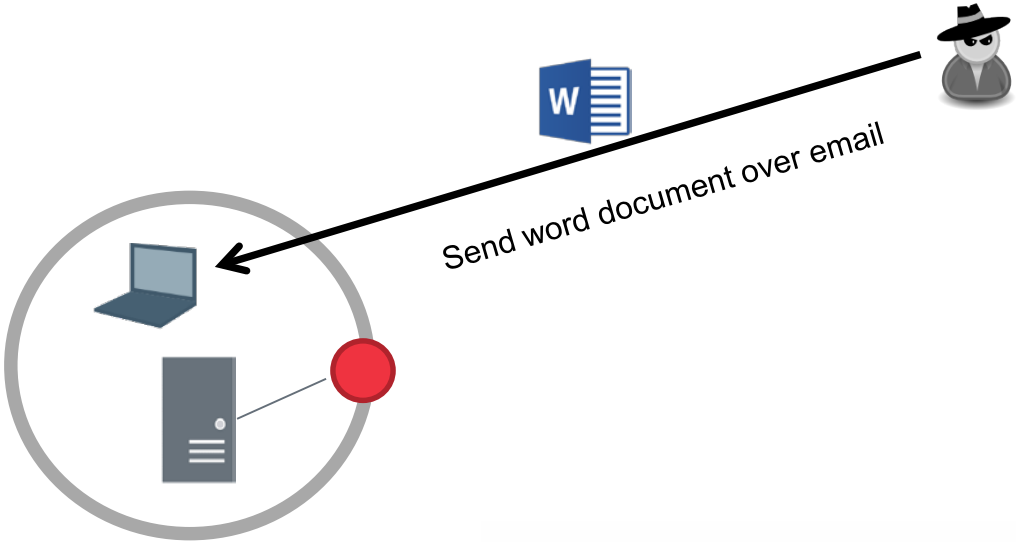
Case study 1 – RDP on perimeter

Found RDP exposed on perimeter



Case study 1 – RDP on perimeter

No credentials!

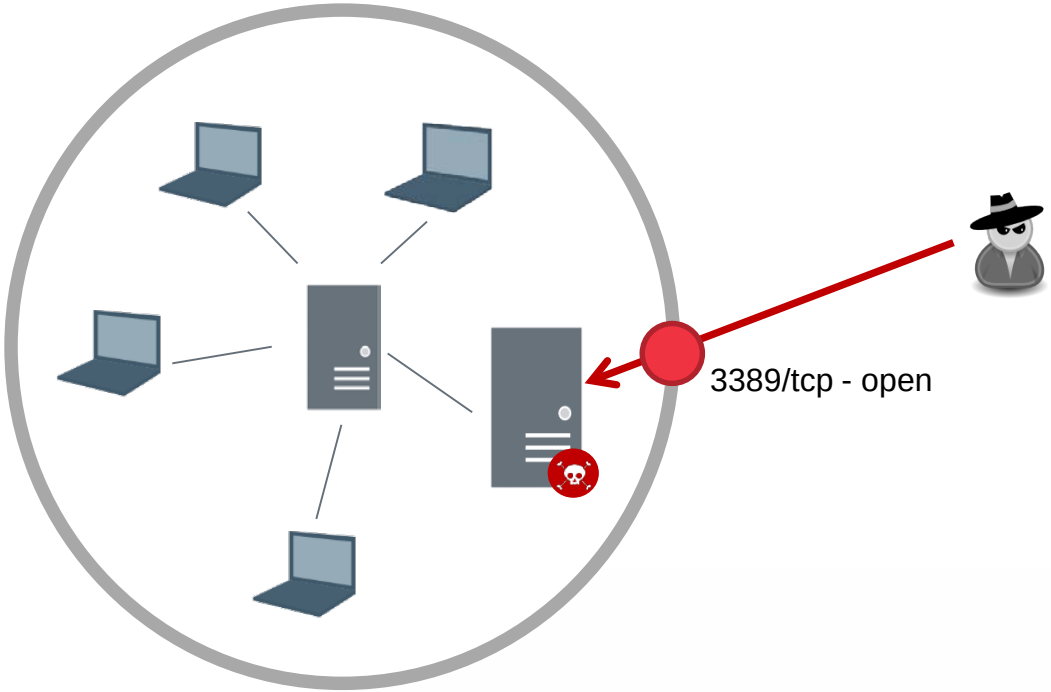


Case study 1 – RDP on perimeter

Sent word document with image loading from UNC path

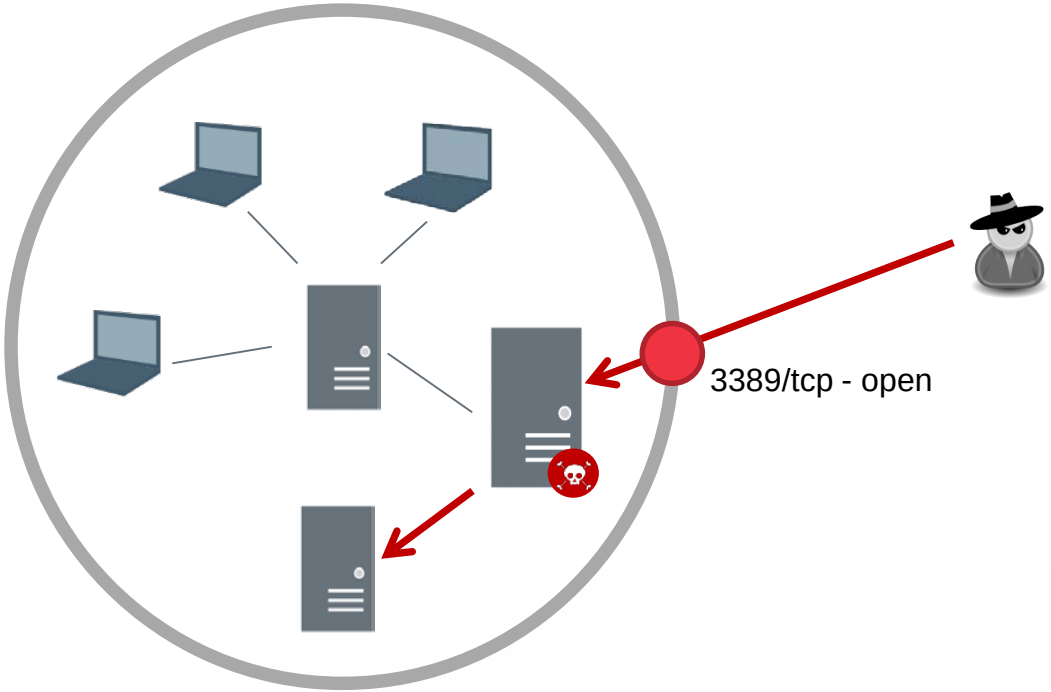
Case study 1 – RDP on perimeter

Capture NTLM challenge/response



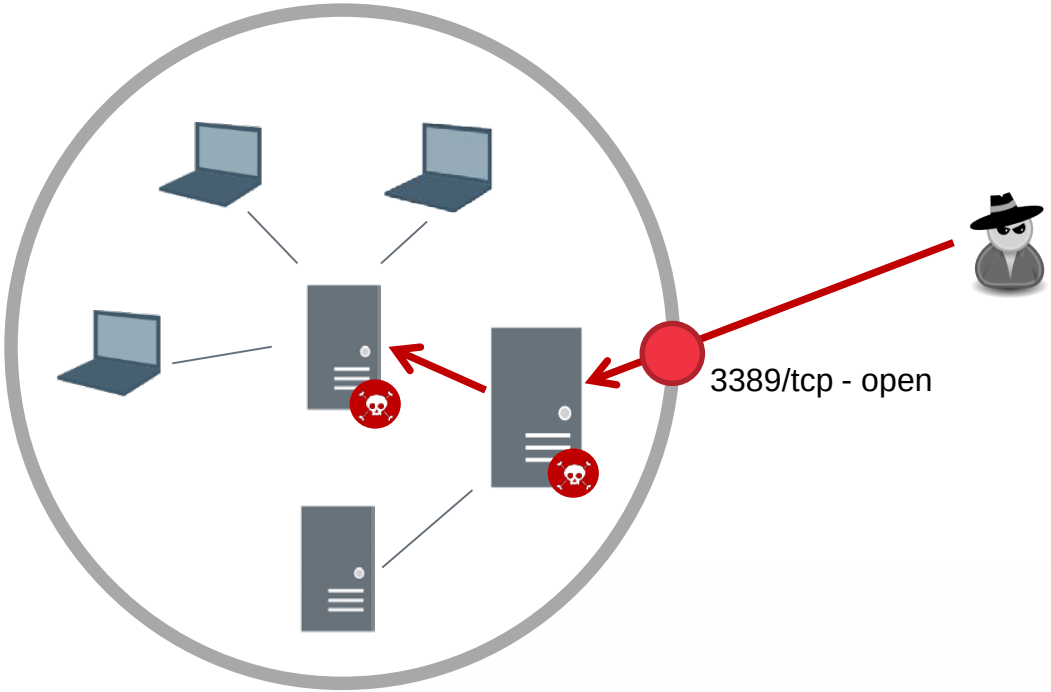
Case study 1 – RDP on perimeter

Cracked password and logged in!



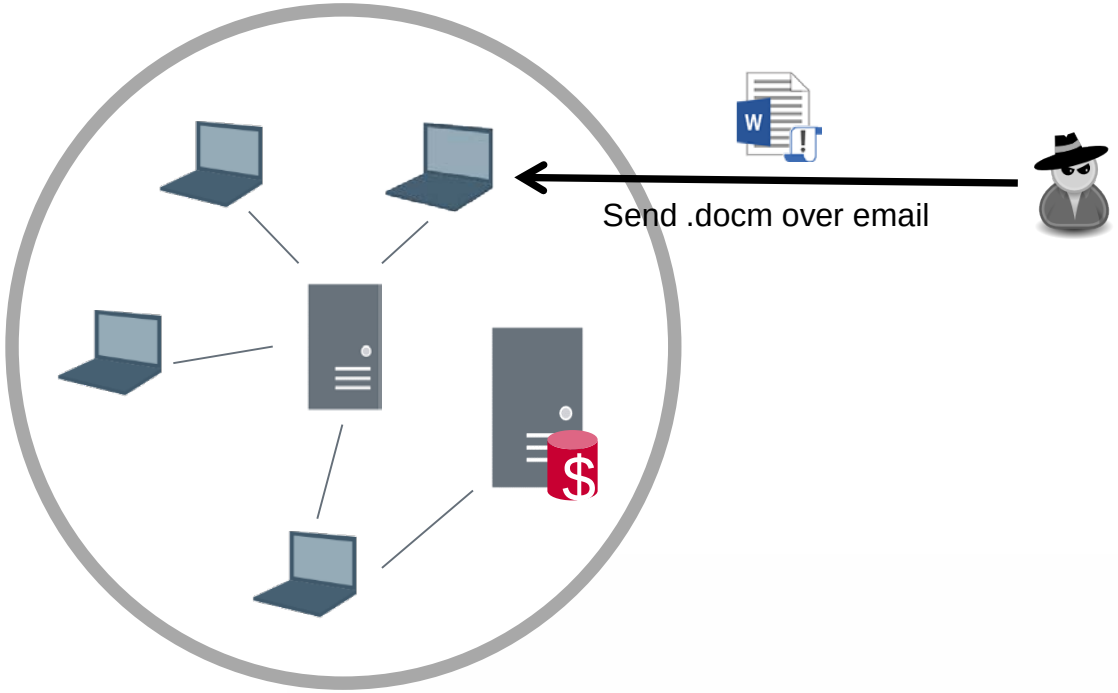
Case study 1 – RDP on perimeter

Searched file servers – found service account password



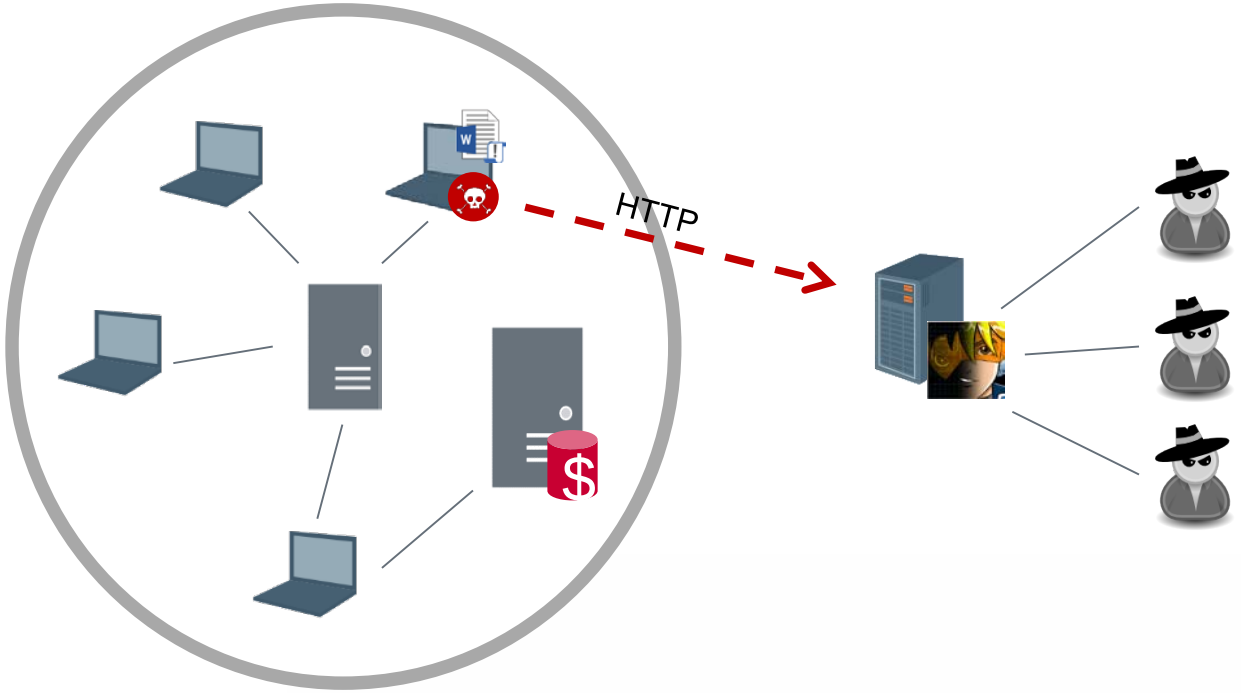
Case study 1 – RDP on perimeter

Shared password with Domain Administrator



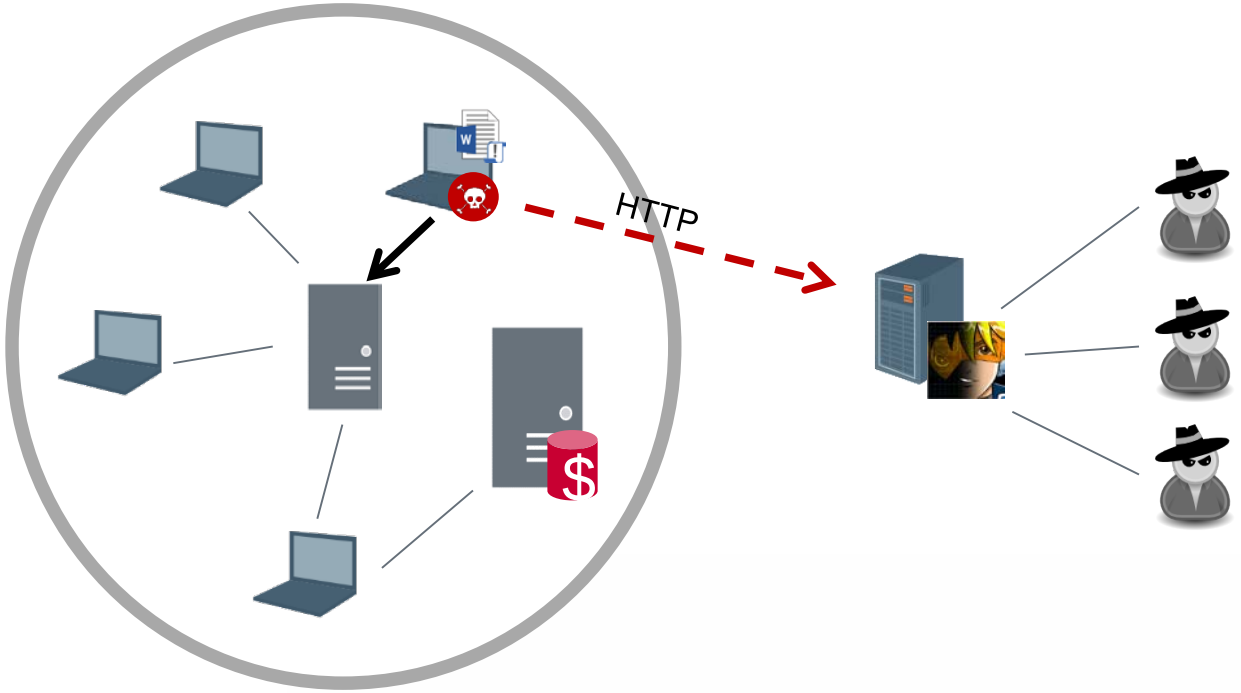
Case study 2 – Malicious macro

Send word document with payload inside macro



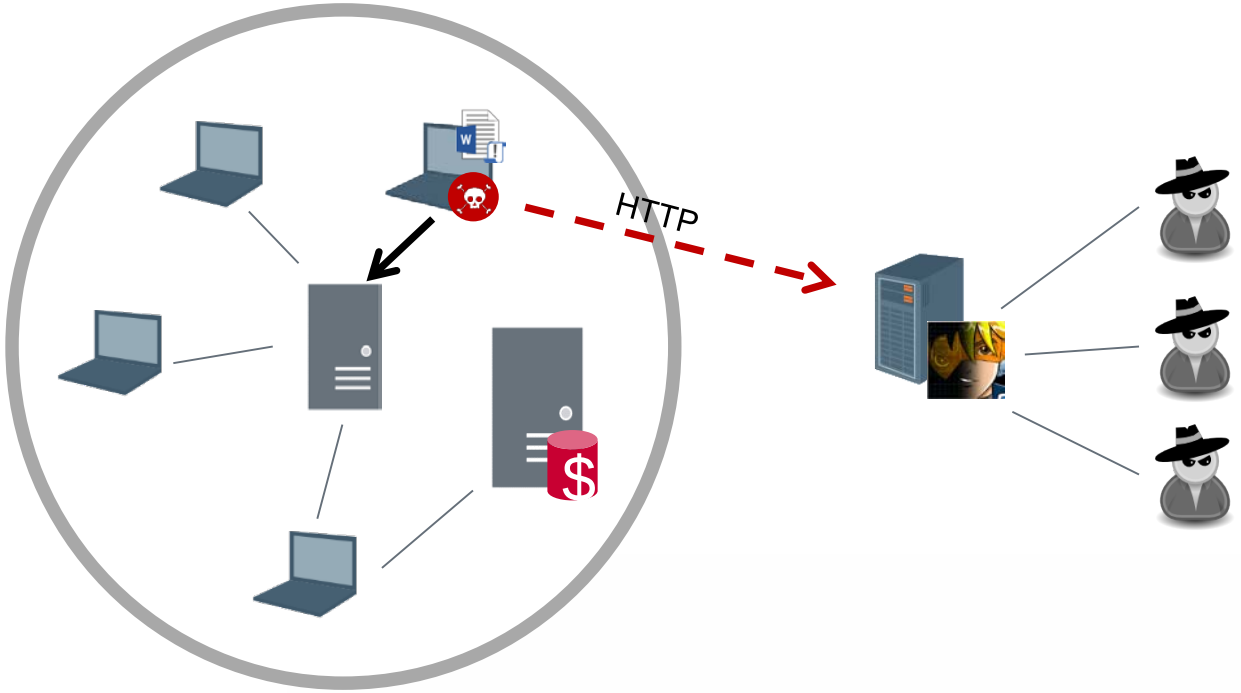
Case study 2 – Malicious macro

Receive connection from compromised laptop



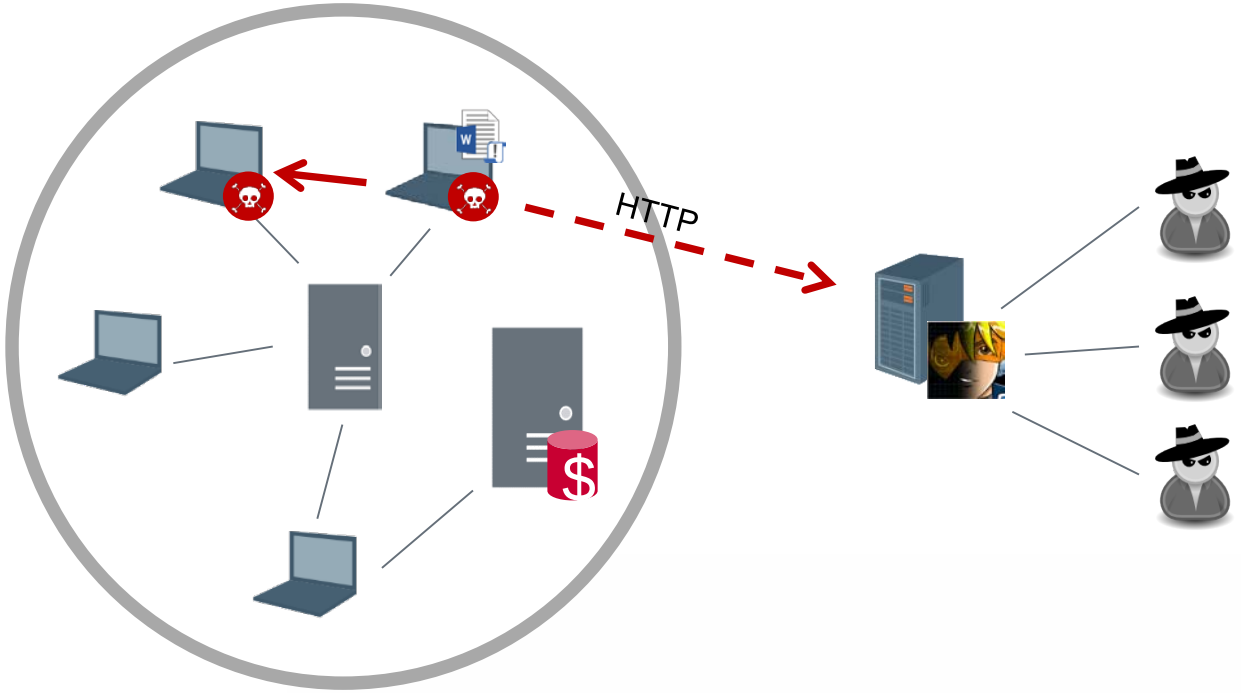
Case study 2 – Malicious macro

Group policy preferences contained local admin password for laptops



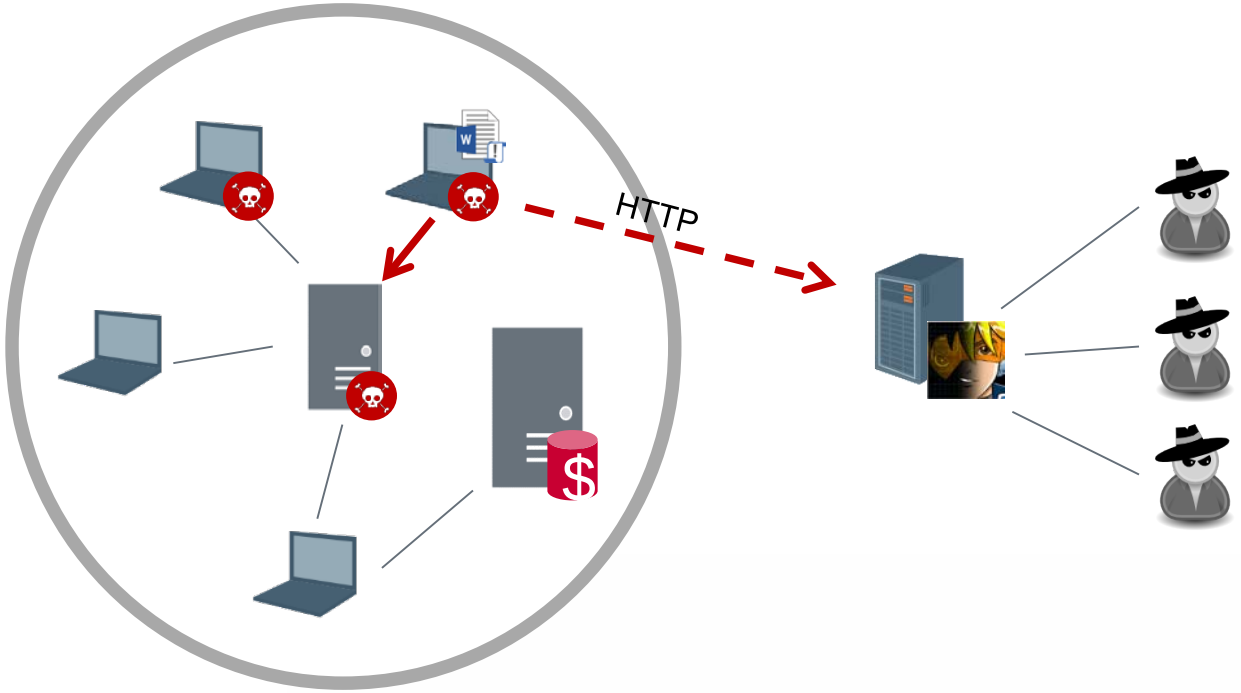
Case study 2 – Malicious macro

Hunted logged in domain administrators to their laptops



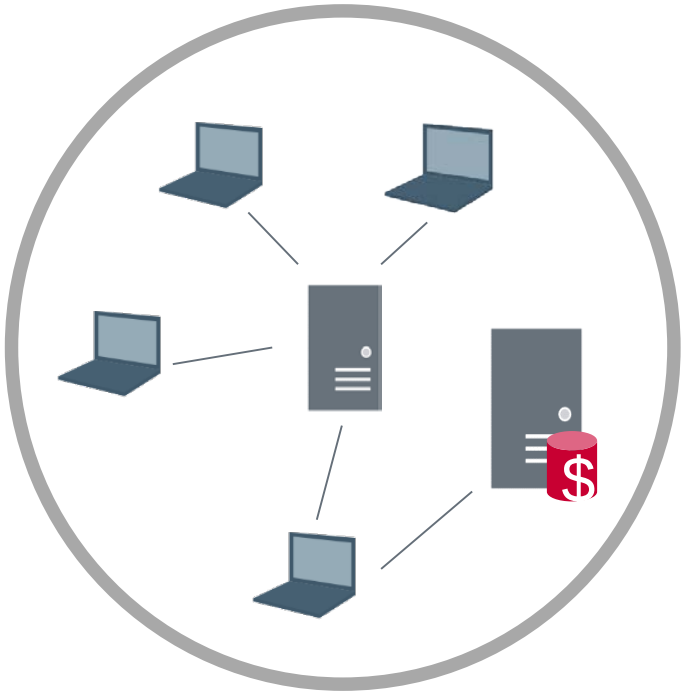
Case study 2 – Malicious macro

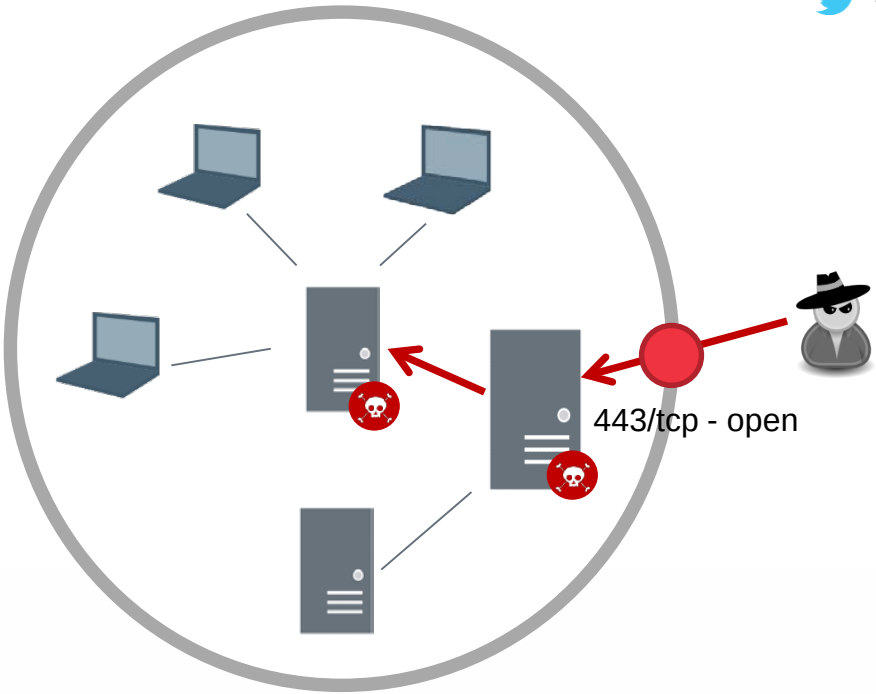
Logged into administrator laptops and stole token



Case study 2 – Malicious macro

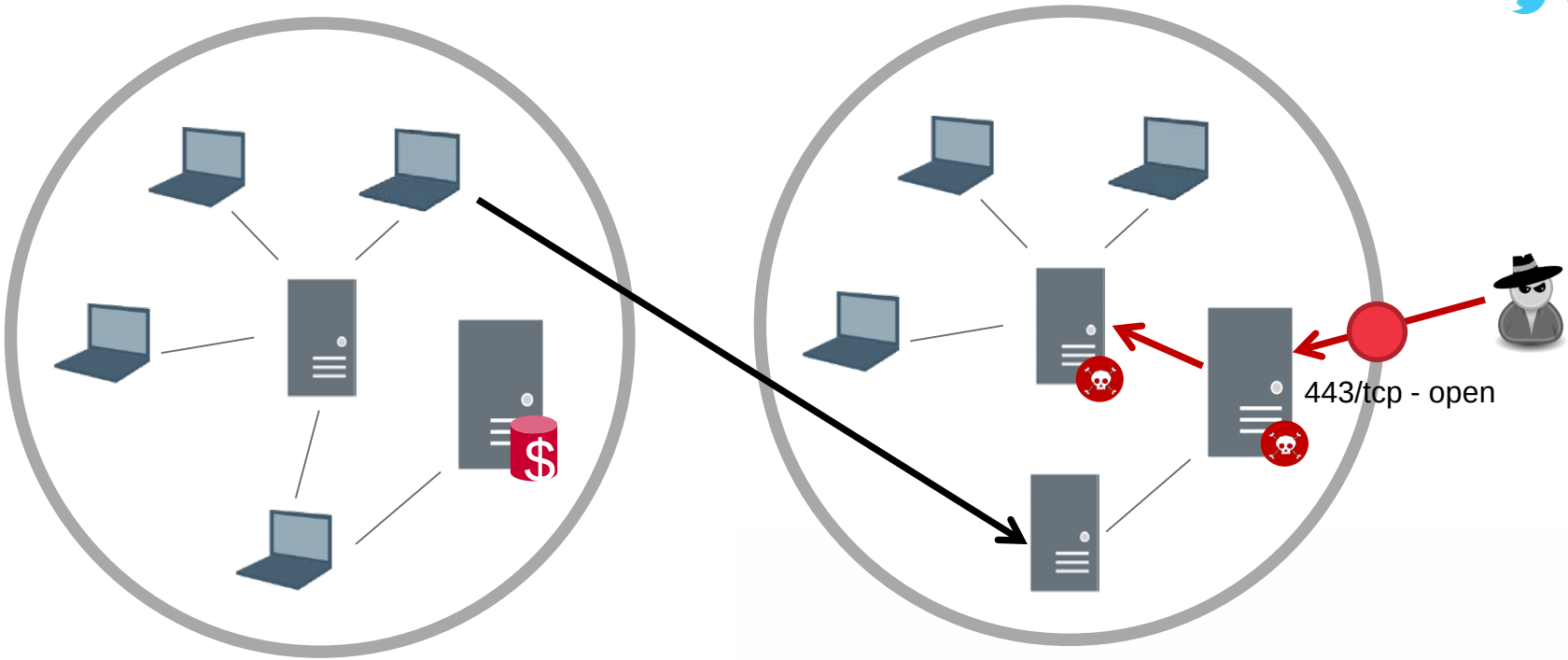
Domain Controller access!





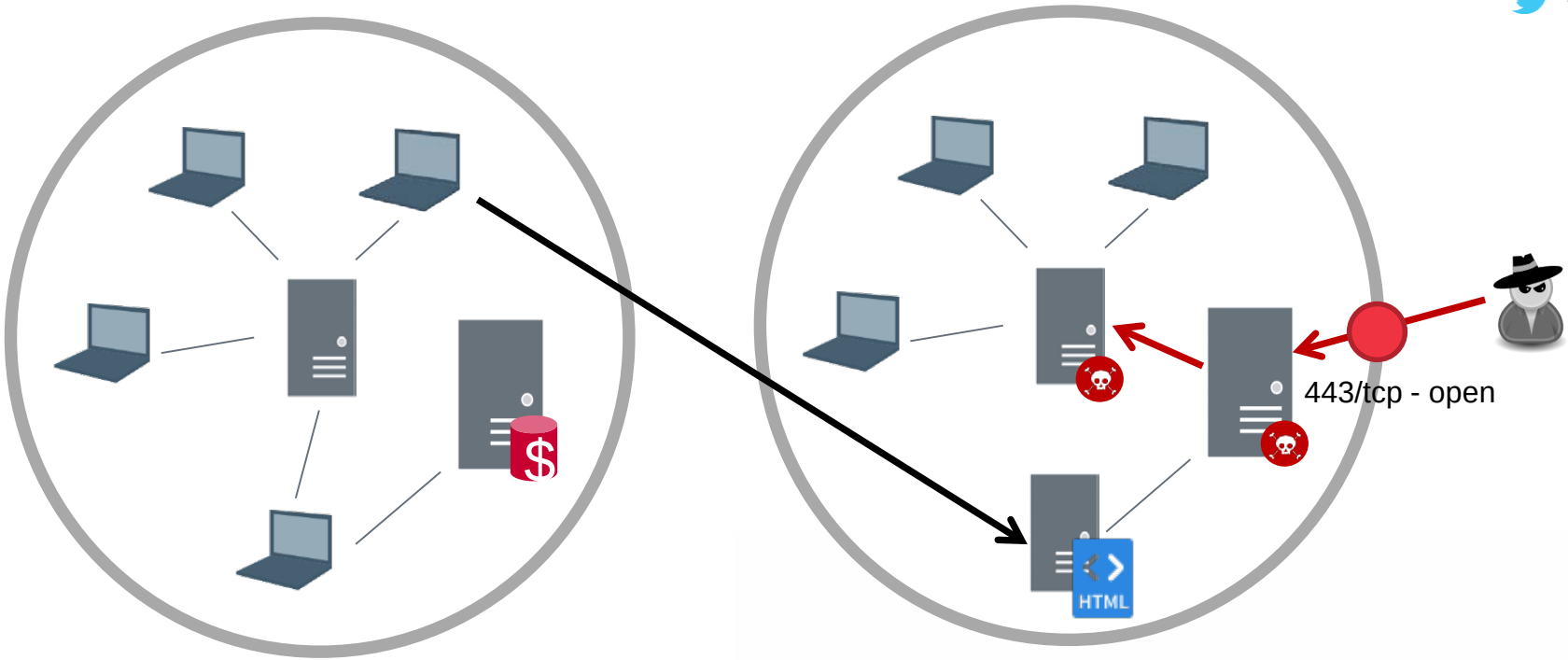
Case study 3 – Watering hole attack

Compromise immature subsidiary of mature company



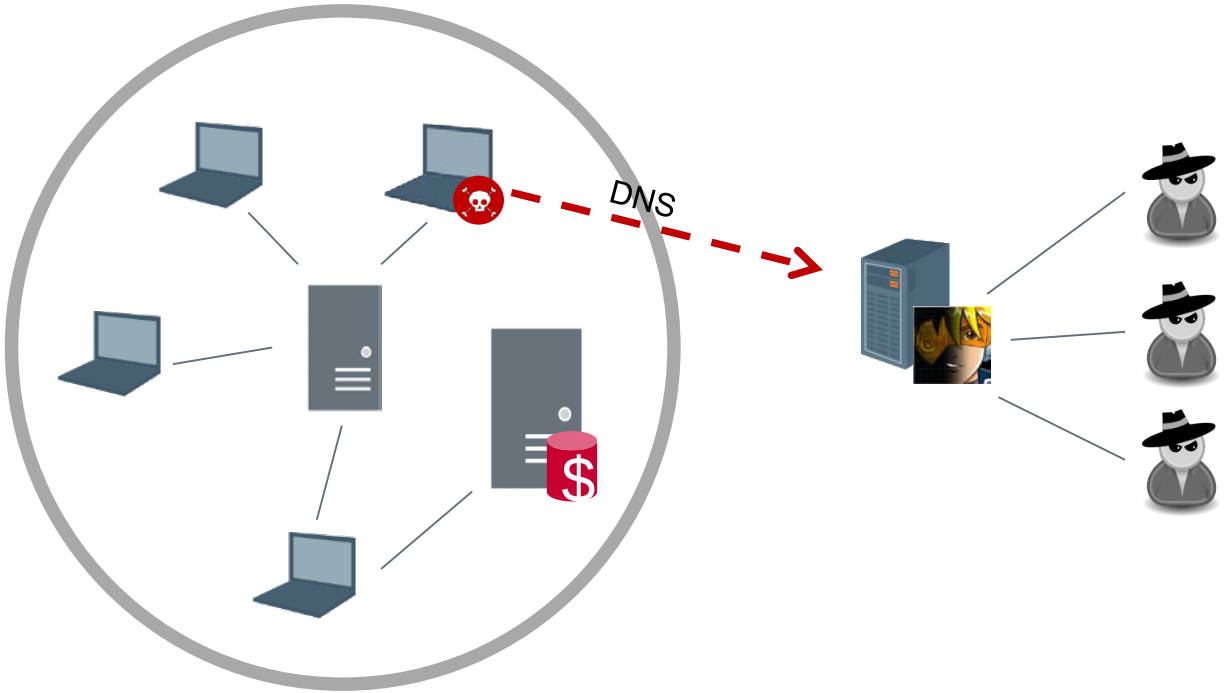
Case study 3 – Watering hole attack

Employees of parent company use web application on subsidiary network



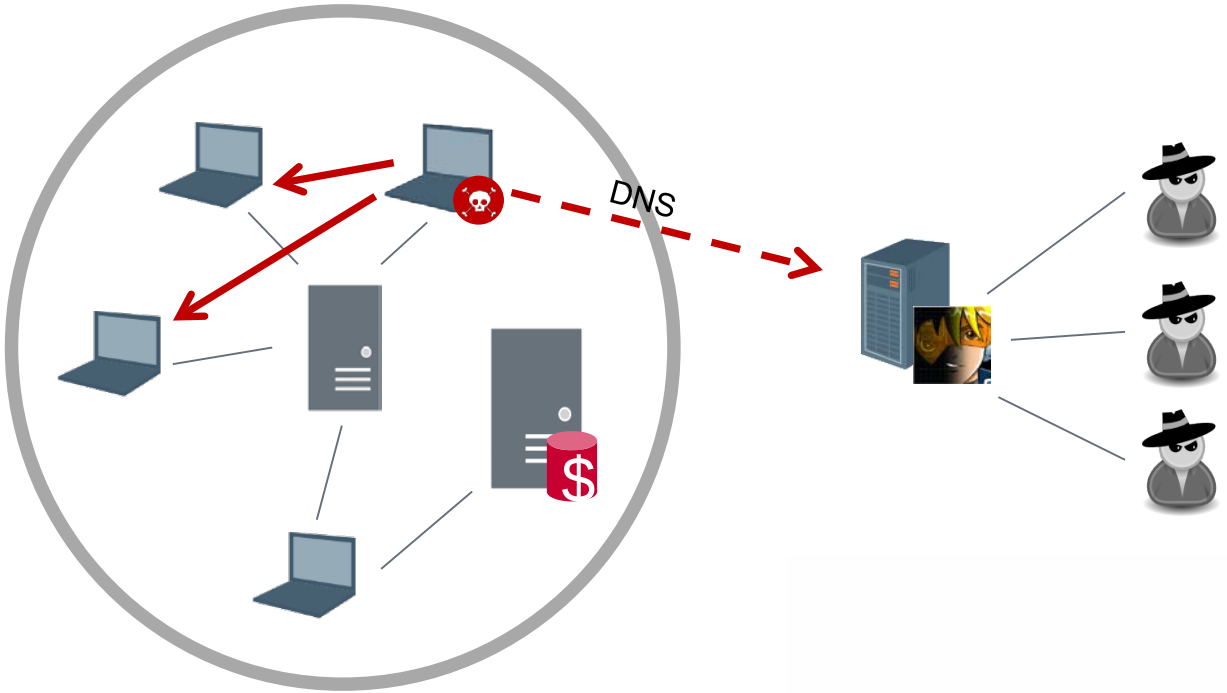
Case study 3 – Watering hole attack

Changed login page to include HTML application



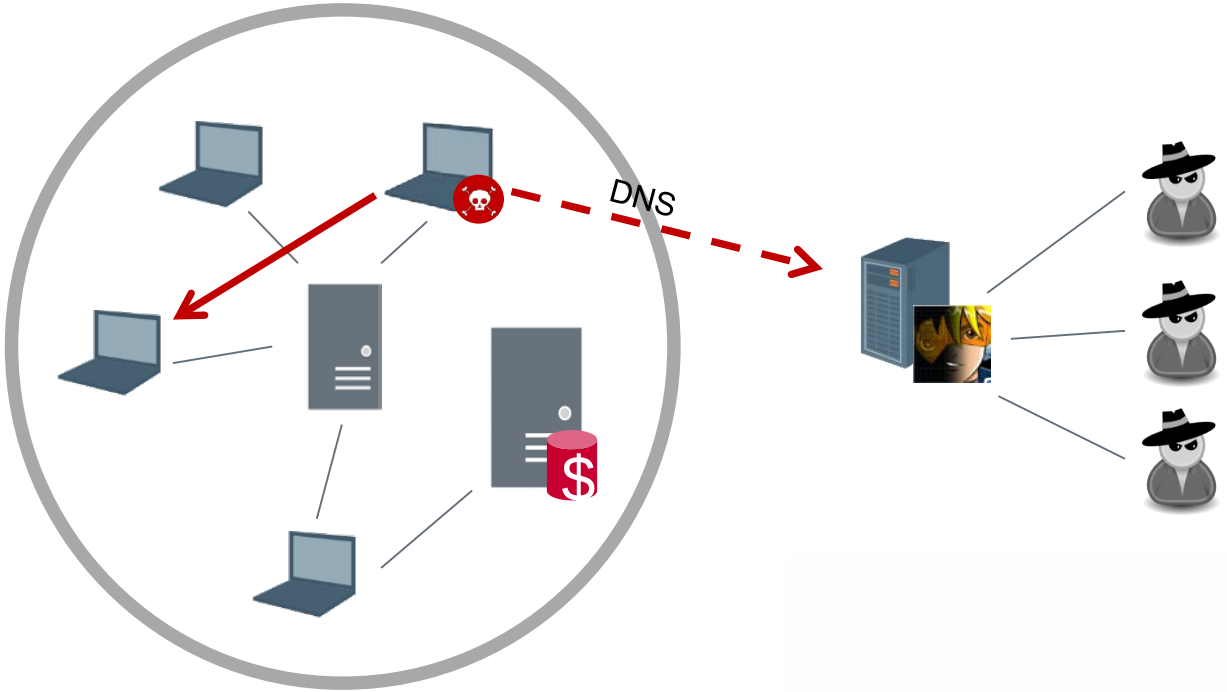
Case study 3 – Watering hole attack

Compromised user on parent company



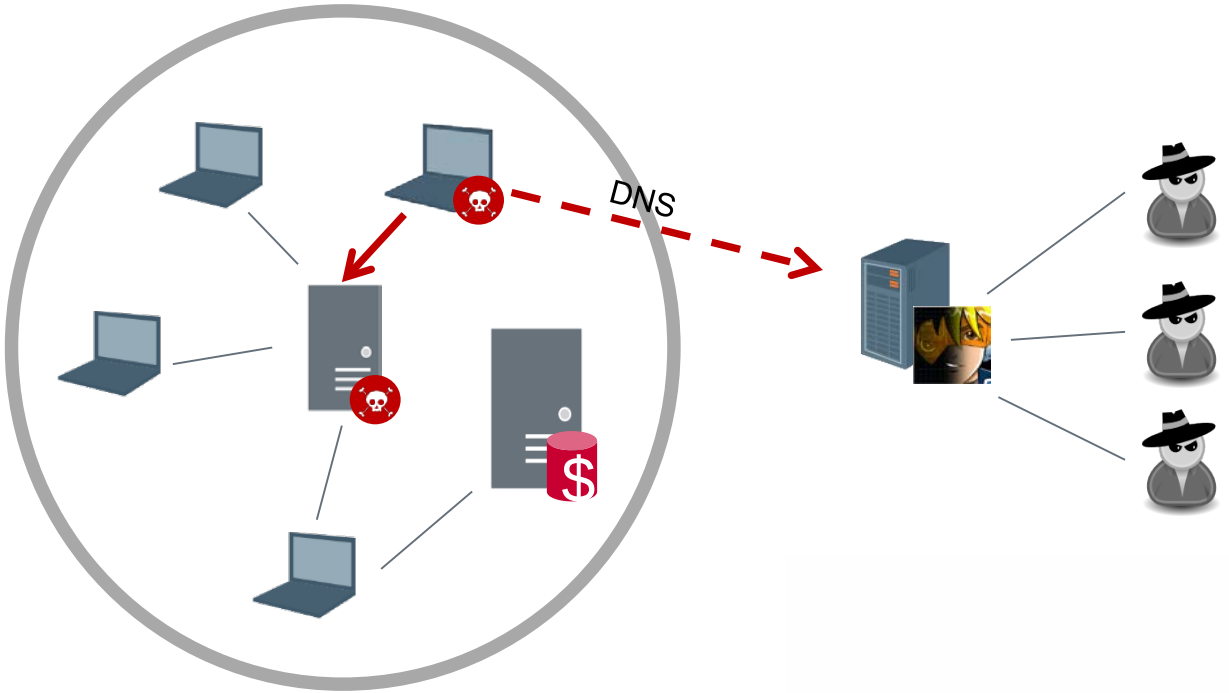
Case study 3 – Watering hole attack

User had administrator access on many machines



Case study 3 – Watering hole attack

Found a domain administrator logged in on one machine and stole token

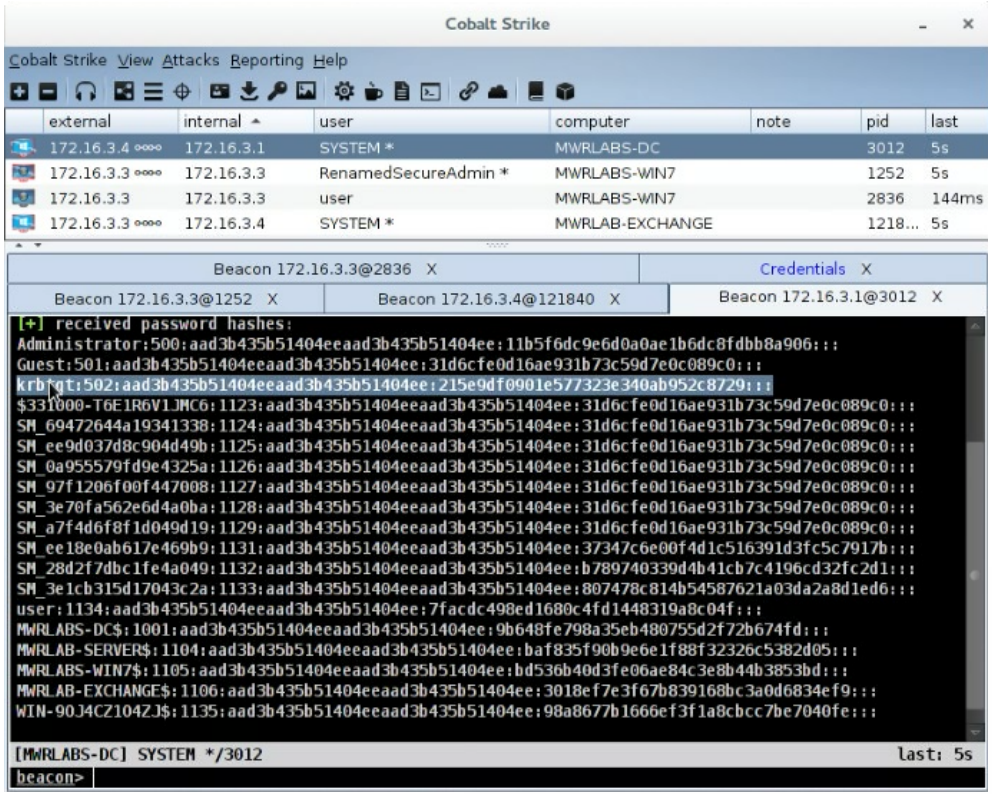


Case study 3 – Watering hole attack

Compromise domain controller

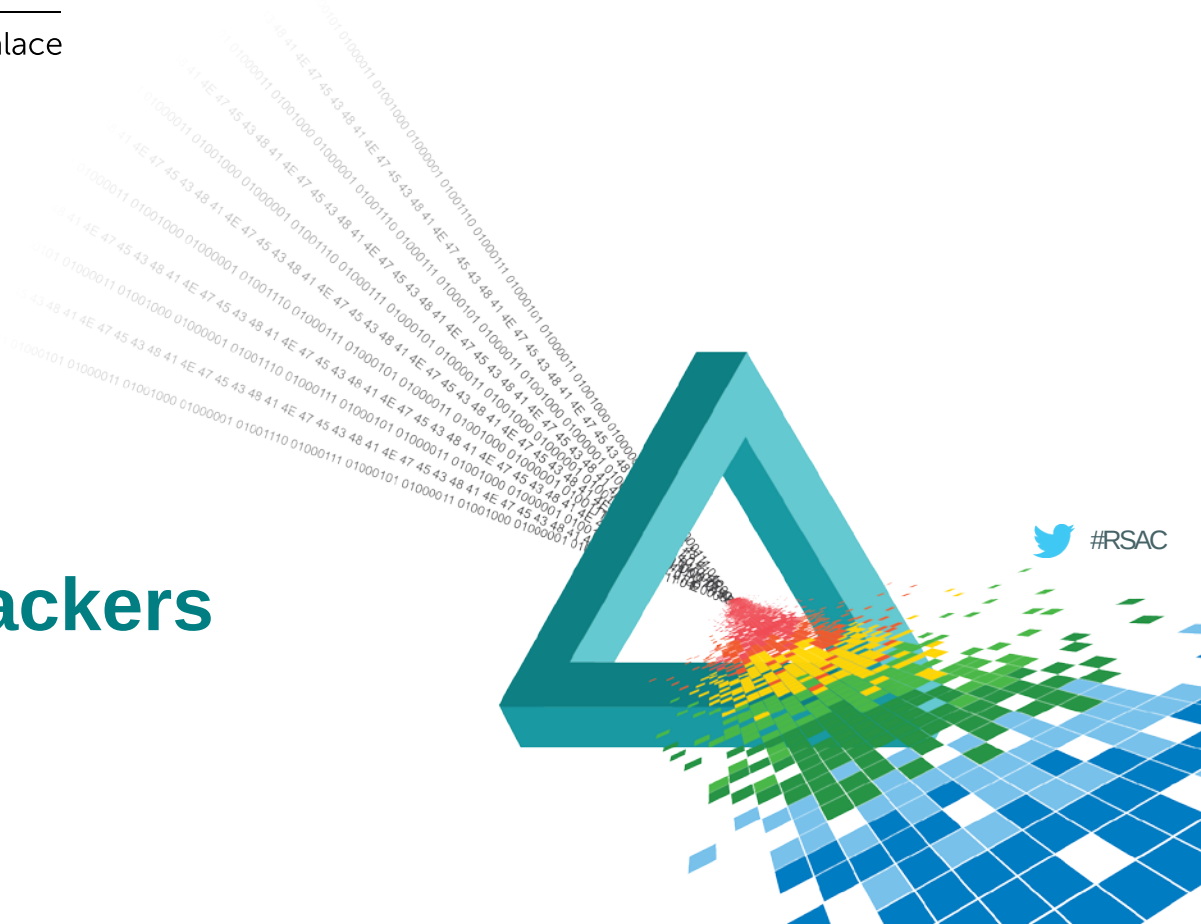
Things to note

- None of these were memory corruption issues
- No 0-days
- Abusing features and misconfiguration allow attackers to perform low(er) cost compromises



Demo: domain compromise using no exploits

Defenders vs. attackers



Technologies and bypasses

Defenders

- Perimeter firewalls

Attackers

- Client-side attacks

Technologies and bypasses

Defenders

- Perimeter firewalls
- Proxies

Attackers

- Client-side attacks
- Proxy-aware payloads

Technologies and bypasses

Defenders

- Perimeter firewalls
- Proxies
- Anti-virus

Attackers

- Client-side attacks
- Proxy-aware payloads
- Bypassed binaries

Technologies and bypasses

Defenders

- Perimeter firewalls
- Proxies
- Anti-virus
- IDS/IPS

Attackers

- Client-side attacks
- Proxy-aware payloads
- Bypassed binaries
- Encrypted/modelled traffic

Technologies and bypasses

Defenders

- Perimeter firewalls
- Proxies
- Anti-virus
- IDS/IPS
- Vulnerability scanners

Attackers

- Client-side attacks
- Proxy-aware payloads
- Bypassed binaries
- Encrypted/modelled traffic
- Abuse software features

Defender vs. attacker mind-sets

Defenders

- Block direct incoming and outgoing connections
- Block known bad binaries
- Block exploits and payload signatures on the network
- Detect port scans

Attackers

- Abuse features and misconfigurations
- Never trigger AV
- Never scan
- Wherever possible, don’t touch disk

The difference

Do you see the gap?

The difference

- Being a good defender means understanding what attackers are doing
- Security products have their place
  - But need to be tuned to be useful
- Detecting subtle events can be crucial to kicking out attackers before they plant roots

Conclusion

- Completely securing an organisation is impossible
- Making it more expensive for an attacker should be the goal
- It is much harder to attack an organisation that understands their assets, likely attackers and average level of skill
- Targeted Attack Simulations can help identify problem areas, validate security spend and train your SOC team

Next steps

Short term

- List what your most sensitive assets are
- Theorize your most likely adversary

Medium Term

- Does your organization consider the following
  - Prevention measures
  - Detection points
  - Response to incidents
  - Security awareness

Next steps

Long term

- Protect your core assets with prevention measures, detection points, security awareness and have a response plan
- Validate your efforts with a Targeted Attack Simulation