

# **MITRE ATT&CK FOR RED TEAMING**



# ABOUT ME

- Niklas Särökaari – @ukk1sec
- Red Teamer (Senior Security Consultant) @ F-Secure



**Dave Bell**

@operant

Follow



Red Team isn't all shells and champagne. It's long hours of analysis looking for that \*one\* flaw that gives you the access you need to move toward your objective. You'll even obsess in your sleep, and the answer will hit you in the shower. Then, repeat!

7:01 am - 24 May 2019

68 Retweets 268 Likes



12

68

268

# MITRE ATT&CK

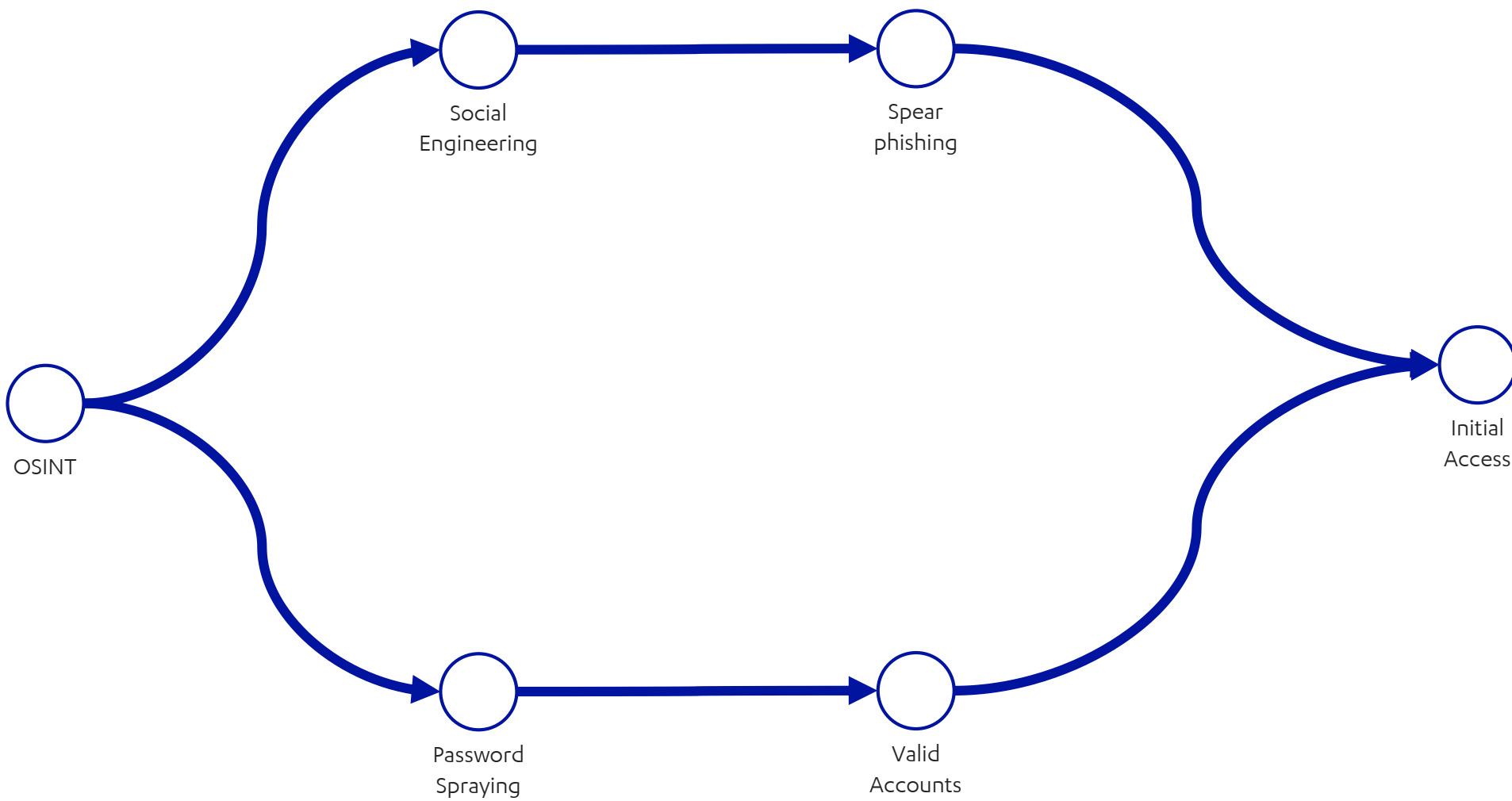
- Knowledge base of adversary tactics, techniques and procedures (TTPs)
- Develop skills for both offense and defense to perform adversary simulations and to detect and respond to on-going attacks performed by real-world adversaries
- <https://attack.mitre.org/>

# ATT&CK Matrix for Enterprise

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Commonly Used Port	Automated Exfiltration	Data Destruction
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	Binary Padding	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Communication Through Removable Media	Data Compressed	Data Encrypted for Impact
External Remote Services	Command-Line Interface	Account Manipulation	AppCert DLLs	BITS Jobs	Brute Force	Browser Bookmark Discovery	Distributed Component Object Model	Clipboard Data	Connection Proxy	Data Encrypted	Defacement
Hardware Additions	Compiled HTML File	AppCert DLLs	Applnit DLLs	Bypass User Account Control	Credential Dumping	Domain Trust Discovery	Exploitation of Remote Services	Data from Information Repositories	Custom Command and Control Protocol	Data Transfer Size Limits	Disk Content Wipe
Replication Through Removable Media	Control Panel Items	Applnit DLLs	Application Shimming	Clear Command History	Credentials in Files	File and Directory Discovery	Logon Scripts	Data from Local System	Custom Cryptographic Protocol	Exfiltration Over Alternative Protocol	Disk Structure Wipe
Spearphishing Attachment	Dynamic Data Exchange	Application Shimming	Bypass User Account Control	CMSTP	Credentials in Registry	Network Service Scanning	Pass the Hash	Data from Network Shared Drive	Data Encoding	Exfiltration Over Command and Control Channel	Endpoint Denial of Service
Spearphishing Link	Execution through API	Authentication Package	DLL Search Order Hijacking	Code Signing	Exploitation for Credential Access	Network Share Discovery	Pass the Ticket	Data from Removable Media	Data Obfuscation	Exfiltration Over Other Network Medium	Firmware Corruption
Spearphishing via Service	Execution through Module Load	BITS Jobs	Dylib Hijacking	Compile After Delivery	Forced Authentication	Network Sniffing	Remote Desktop Protocol	Data Staged	Domain Fronting	Exfiltration Over Physical Medium	Inhibit System Recovery
Supply Chain Compromise	Exploitation for Client Execution	Bootkit	Exploitation for Privilege Escalation	Compiled HTML File	Hooking	Password Policy Discovery	Remote File Copy	Email Collection	Domain Generation Algorithms	Scheduled Transfer	Network Denial of Service
Trusted Relationship	Graphical User Interface	Browser Extensions	Extra Window Memory Injection	Component Firmware	Input Capture	Peripheral Device Discovery	Remote Services	Input Capture	Fallback Channels		Resource Hijacking
Valid Accounts	InstallUtil	Change Default File Association	File System Permissions Weakness	Component Object Model Hijacking	Input Prompt	Permission Groups Discovery	Replication Through Removable Media	Man in the Browser	Multi-hop Proxy		Runtime Data Manipulation

# INITIAL ACCESS

## Initial Access



# OPEN SOURCE INTELLIGENCE

- Open Source Intelligence (OSINT) gathering is used as the first step in targeted attacks and attack simulations to map the attack surface presented by a target organisation
- May provide crucial information that can be used to obtain initial access:
  - Employee emails for phishing and username enumeration
  - Publicly exposed critical services, such as Citrix and VPN portals without 2FA
  - Lync service or Outlook Web Access, which can be abused for password spraying



# SPEAR PHISHING

osallistujalista [Suojattu näkymä] - Excel

Tiedosto Aloitus Lisää Sivun asettelu Kaavat Tiedot Tarkista Näytä Kerro, mitä haluat tehdä...

Jakaminen

**SUOJATTU NÄKYMÄ** Ole varovainen. Internetistä peräisin olevat tiedostot saattavat sisältää viruksia. Ellei tiedostoa tarvitse muokata, on turvallisempaa pysyä suojatussa näkymässä. Ota muokkaus käyttöön

A1    =REKISTERÖI([REDACTED])

A B C

1

2

3

4

5

6

7

8

9

10

11

12

13

14

15

16

17


18

19

20

21

22

 Tämä dokumentti on tehty käyttäen vanhempaa Microsoft Excel versiota.  
Nähdäksesi dokumentin paina **Ota sisältö käyttöön**

# PASSWORD SPRAYING

C:\> Command Prompt

```
Microsoft Windows [Version 10.0.17763.437]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\johnsmi>net accounts /domain
The request will be processed at a domain controller for domain

Force user logoff how long after time expires?:      Never
Minimum password age (days):                        1
Maximum password age (days):                        90
Minimum password length:                             8
Length of password history maintained:               10
Lockout threshold:                                   100
Lockout duration (minutes):                           30
Lockout observation window (minutes):                 30
Computer role:                                       BACKUP
The command completed successfully.
```

# PASSWORD SPRAYING

Command Prompt

```
Microsoft Windows [Version 10.0.17763.437]  
(c) 2018 Microsoft Corporation. All rights reserved.
```

```
[!] VALID CREDENTIALS: PXXXXXX, Password: Kevat2019, Time: 0.112485  
[!] VALID CREDENTIALS: TXXXXXX, Password: Kevat2019, Time: 0.226077  
[!] VALID CREDENTIALS: TXXXXXX, Password: Helmikuu2019, Time: 0.156721  
[!] VALID CREDENTIALS: AXXXXXX, Password: Helmikuu2019, Time: 0.145805  
[!] VALID CREDENTIALS: BXXXXXX, Password: Helmikuu2019, Time: 1.901968  
[!] VALID CREDENTIALS: TXXXXXX, Password: Helmikuu2019, Time: 0.141225  
[!] VALID CREDENTIALS: AXXXXXX, Password: Maaliskuu2019, Time: 0.111762  
[!] VALID CREDENTIALS: JXXXXXX, Password: Maaliskuu2019, Time: 0.959626  
[!] VALID CREDENTIALS: IXXXXXX, Password: Maaliskuu2019, Time: 0.186355  
[!] VALID CREDENTIALS: LXXXXXX, Password: Huhtikuu2019, Time: 0.124256  
[!] VALID CREDENTIALS: EXXXXXX, Password: Huhtikuu2019, Time: 1.90511  
[!] VALID CREDENTIALS: EXXXXXX, Password: Huhtikuu2019, Time: 0.133911  
[!] VALID CREDENTIALS: EXXXXXX, Password: Huhtikuu2019, Time: 0.119284
```

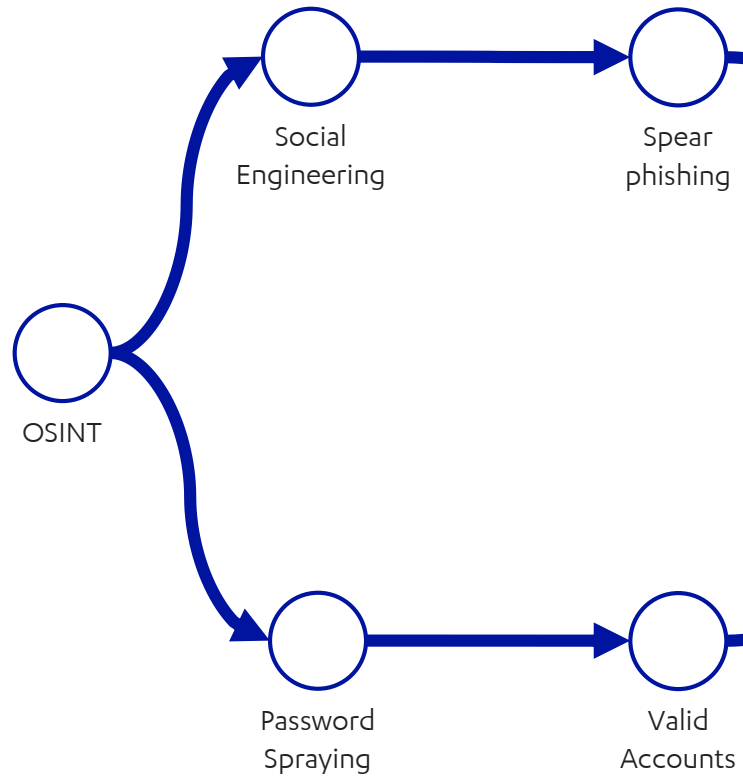
```
The command completed successfully.
```

# DATA COLLECTION

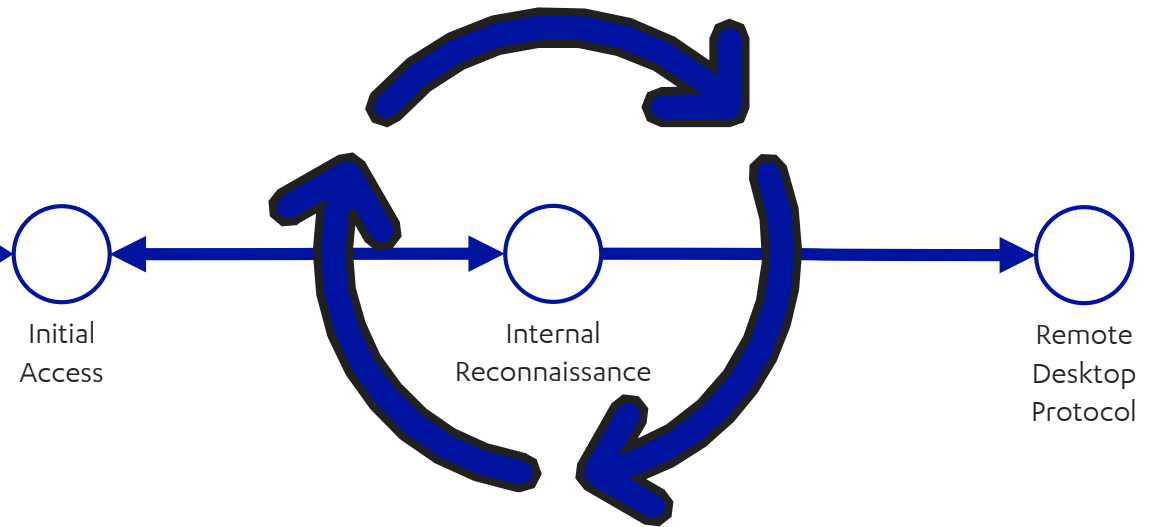
***“Defenders think in lists. Attackers think in graphs. As long as this is true, attackers win.”***

**@JohnLaTwC**

## Initial Access



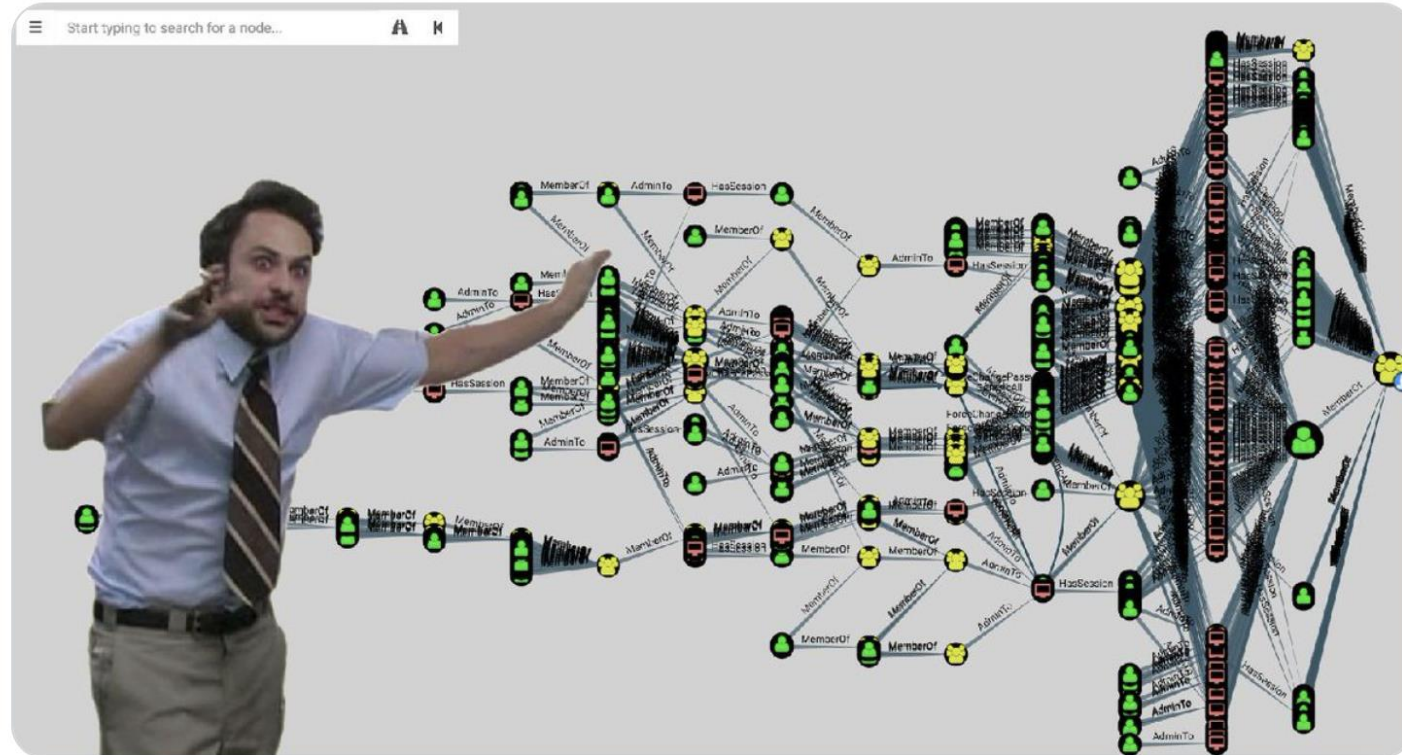
## Discovery



dude  
@dudeslce



Me explaining a priv esc path



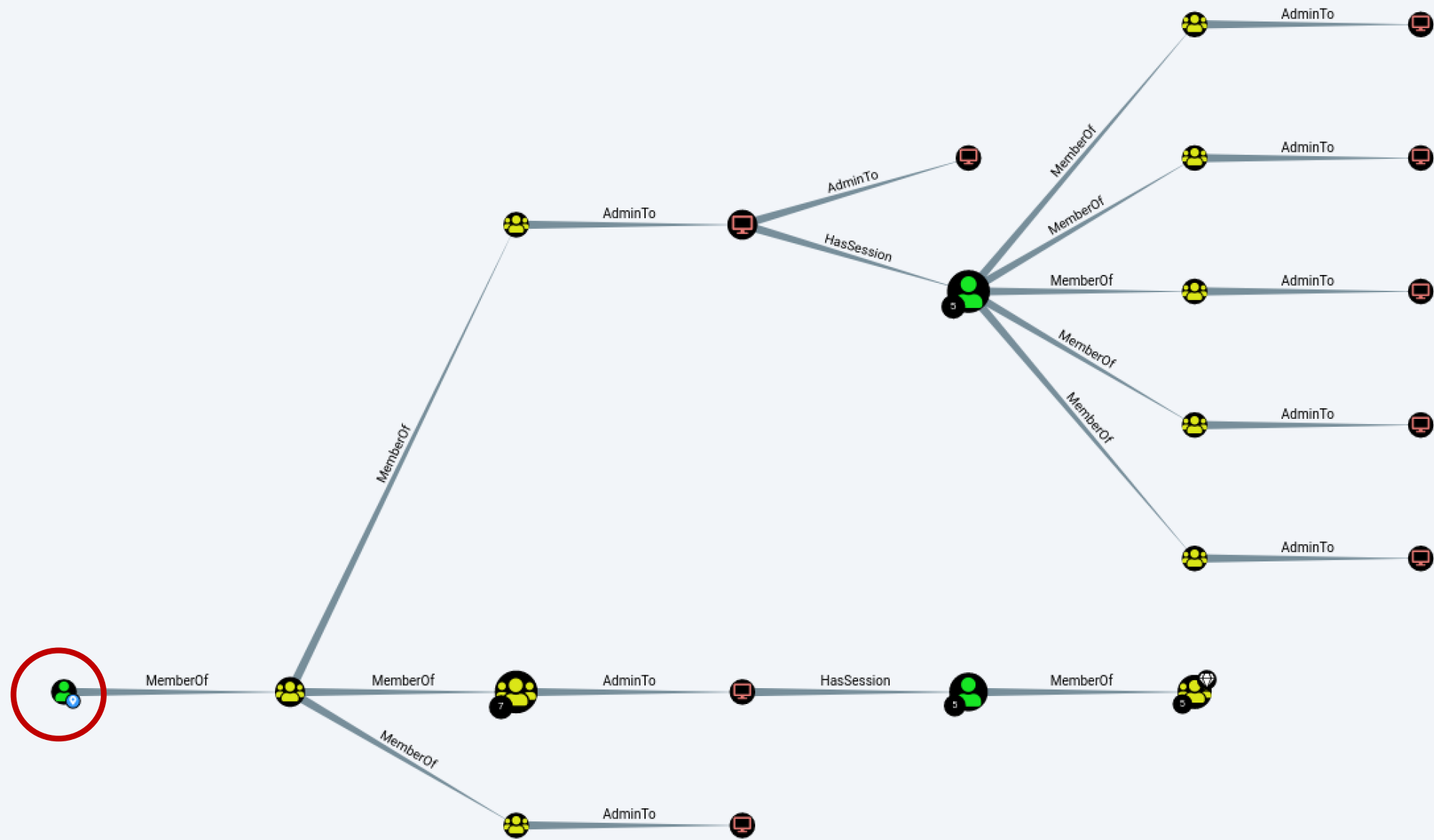
9:13 AM · Mar 29, 2019 · [Twitter Web Client](#)

369 Retweets 1.5K Likes

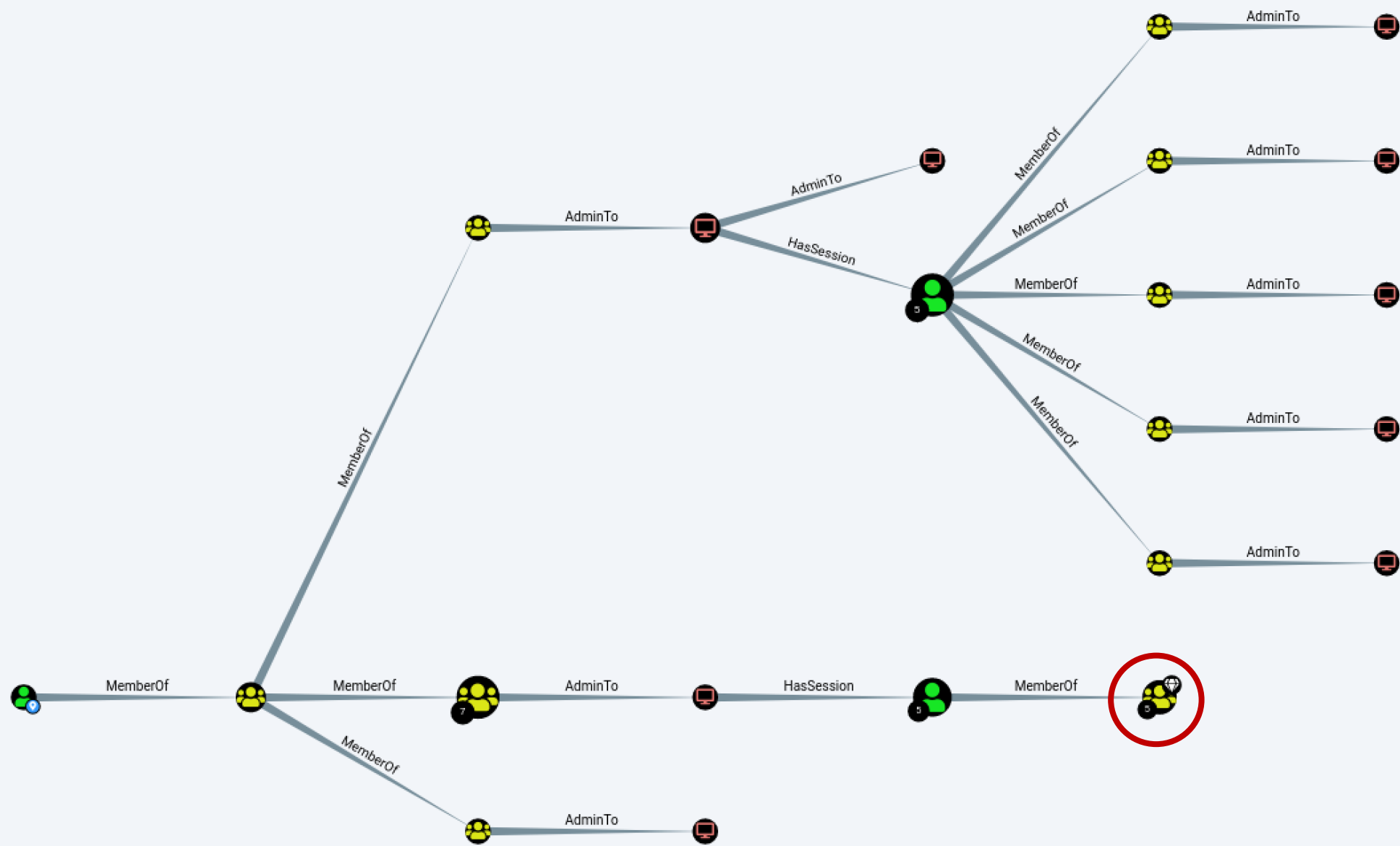


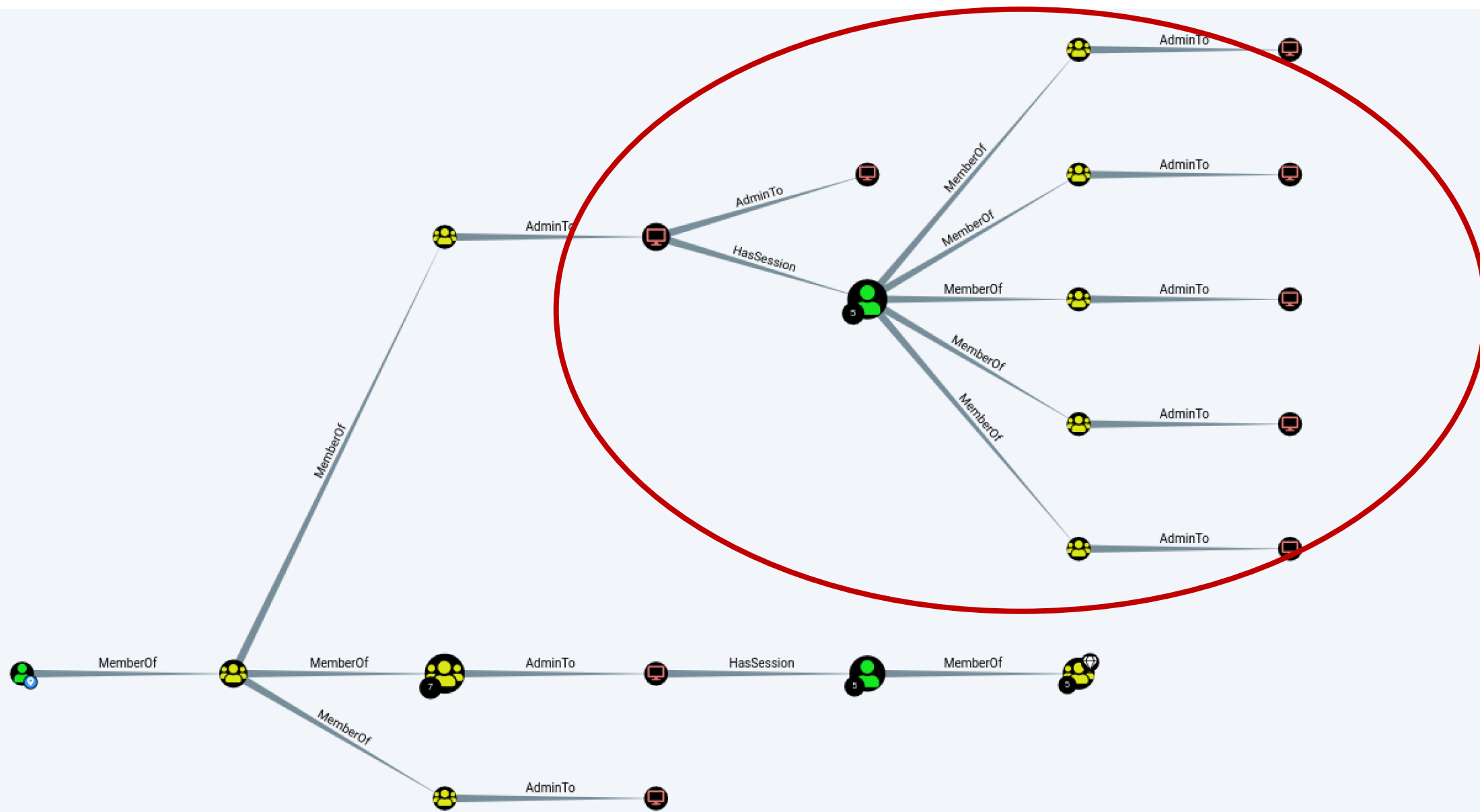
# BLOODHOUND + SHARPHOUND

- Provides means to collect and analyze data to identify potential attack paths
- SharpHound can be used to collect information such as:
  - Local admin & user session info
  - Group memberships
  - Domain trusts
  - Group Policy Objects
  - Access Control List info
- Repetition is key





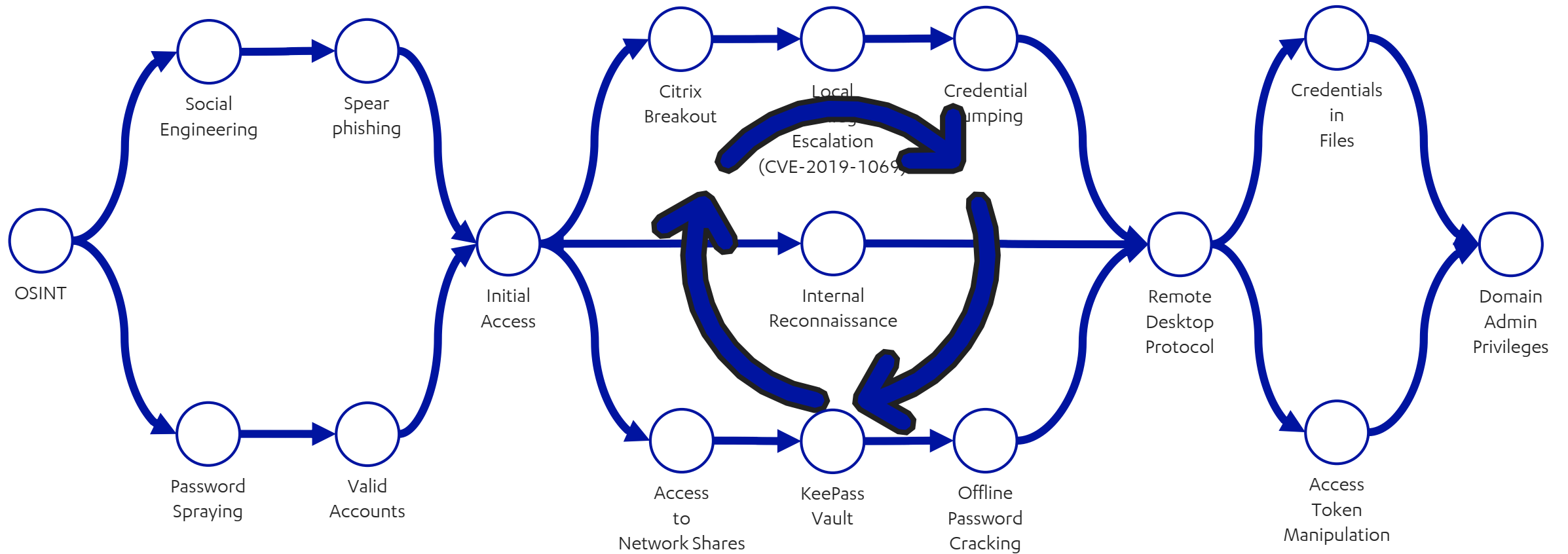




# PRIVILEGE ESCALATION

## Initial Access

## Discovery, Privilege Escalation, Credential Access & Lateral Movement



# PRIVILEGE ESCALATION

- Objective is to gain higher-level permissions and access on a targeted system or network
- Common approaches include abusing misconfigurations, exploiting known or unknown weaknesses or taking advantage of poor account management
- Administrative access in an environment provides wider options for an adversary to steal information and move laterally

# CITRIX BREAKOUT

- Citrix is commonly deployed in corporate environments
- It is also commonly misconfigured, providing easy methods for attackers to breakout from the “sandbox”
- Initial access is usually a low-level user; thus escalation of privilege is required to move towards the objective

# CVE-2019-1069

- Previously unknown vulnerability with a proof-of-concept exploit was published affecting Windows 10 and Windows 2016/2019 servers in May 2019 by SandboxEscaper
- F-Secure repurposed the published PoC-exploit to create a local administrator user in Citrix servers to dump credentials for lateral movement.
- <https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1069>

# CREDENTIAL ACCESS



# CREDENTIAL ACCESS

- Objective is to steal credentials, which can be used for privesc and lateral movement
- Commonly used techniques include:
  - Searching files for credentials
  - dumping LSASS with admin privileges, using Mimikatz or other similar tools
- Or just simple, plain old bruteforce and password spraying attacks

# KEEPASS PASSWORD VAULT

- KeePass password vaults can be attacked with tools like John the Ripper and Hashcat
- “Expired” password vault that was “protected” with a 7-character password was cracked roughly in a day
- The passwords recovered from the vault was then used to move laterally in the network

# PASSWORD CRACKING



**Tinker**  
@TinkerSec

Seuraa



~=8 Character Passwords Are Dead=~

New benchmark means that the entire  
keyspace, or every possible  
combination of:

- Upper
- Lower
- Number
- Symbol

...of an 8 character password can be  
guessed in:

~2.5 hours

(8x 2080 GPUs against NTLM Windows  
hash)



**hashcat** @hashcat

hand-tuned hashcat 6.0.0 beta and 2080Ti (stock clocks)  
breaks NTLM cracking speed mark of 100GH/s on a  
single compute device

6.00 - 14. helmik. 2019

# LATERAL MOVEMENT

# LATERAL MOVEMENT

- Purpose is to move across the target network using obtained credentials and either legitimate administrator tools or using adversaries own tooling to achieve the objective
- Especially in Windows environments using RDP and administrative credentials provide wide access in the environment
- Environments are rarely properly segregated, which allows adversaries easily to move between systems and networks
  - **Bi-directional AD forest trusts**

# CONCLUSIONS

# TAKEAWAYS

- Identify potential attack paths in your environment
  - Unused accounts, number of high-privileged accounts, group delegated access rights, forest trust relationships
- Review password policies
- Implement 2FA for critical services
- Invest in detection and response capabilities
  - And evaluate these actively

**BUILDING AND MAINTAINING  
A ROBUST AND SECURE AD  
FOREST IS VERY, VERY  
DIFFICULT**





**F-Secure®**