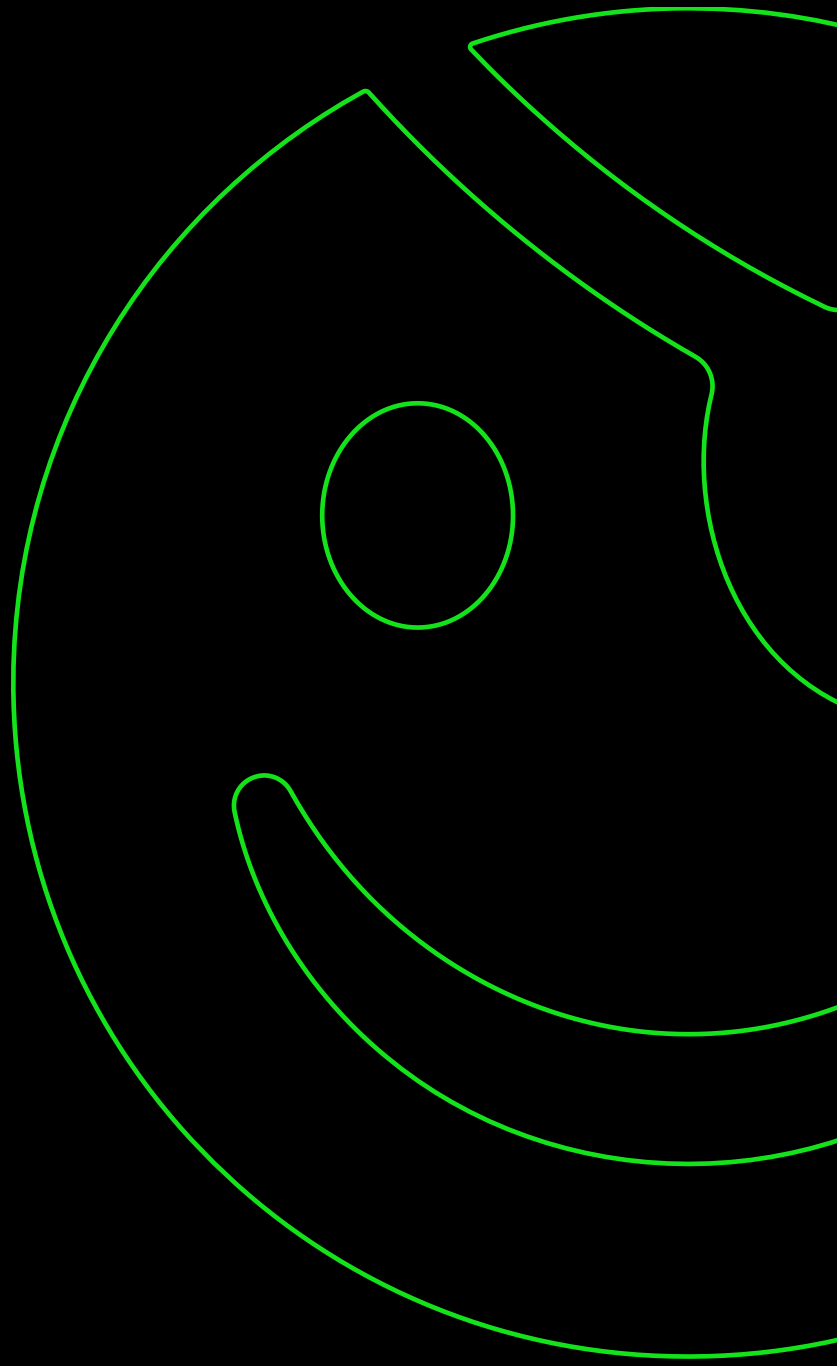
Identifying New Attack Paths via Password Analysis

Esteban Rodriguez – Senior Security Consultant @ TrustedSec

February 6th, 2025



Who am I?

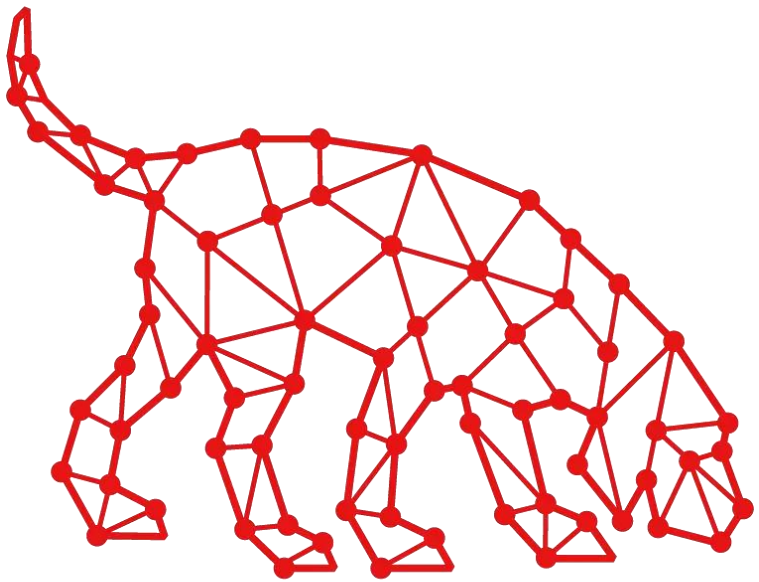
- Senior Security Consultant @ TrustedSec
- https://www.n00py.io/
- n00py1 on Twitter

Overview

- Who is this talk for?
  - Penetration Testers
  - Purple Teams
- What you need to know:
  - **This is for post-exploitation!** It will not help you get DA.
  - It will however make your reports better
- Tools involved:
  - **BloodHound** – Created by @_wald0, @CptJesus, @harmj0y
  - **Hashcathelper** - @mr_mitm
  - **CrackHound** - @Jean_Maes_1994
  - **Max** - @knavesec

BloodHound

- The tool you already know and love
- It makes pretty graphs – visualization of complex attack chains



BLOODHOUND

TRUSTEDSEC

Hashcathelper

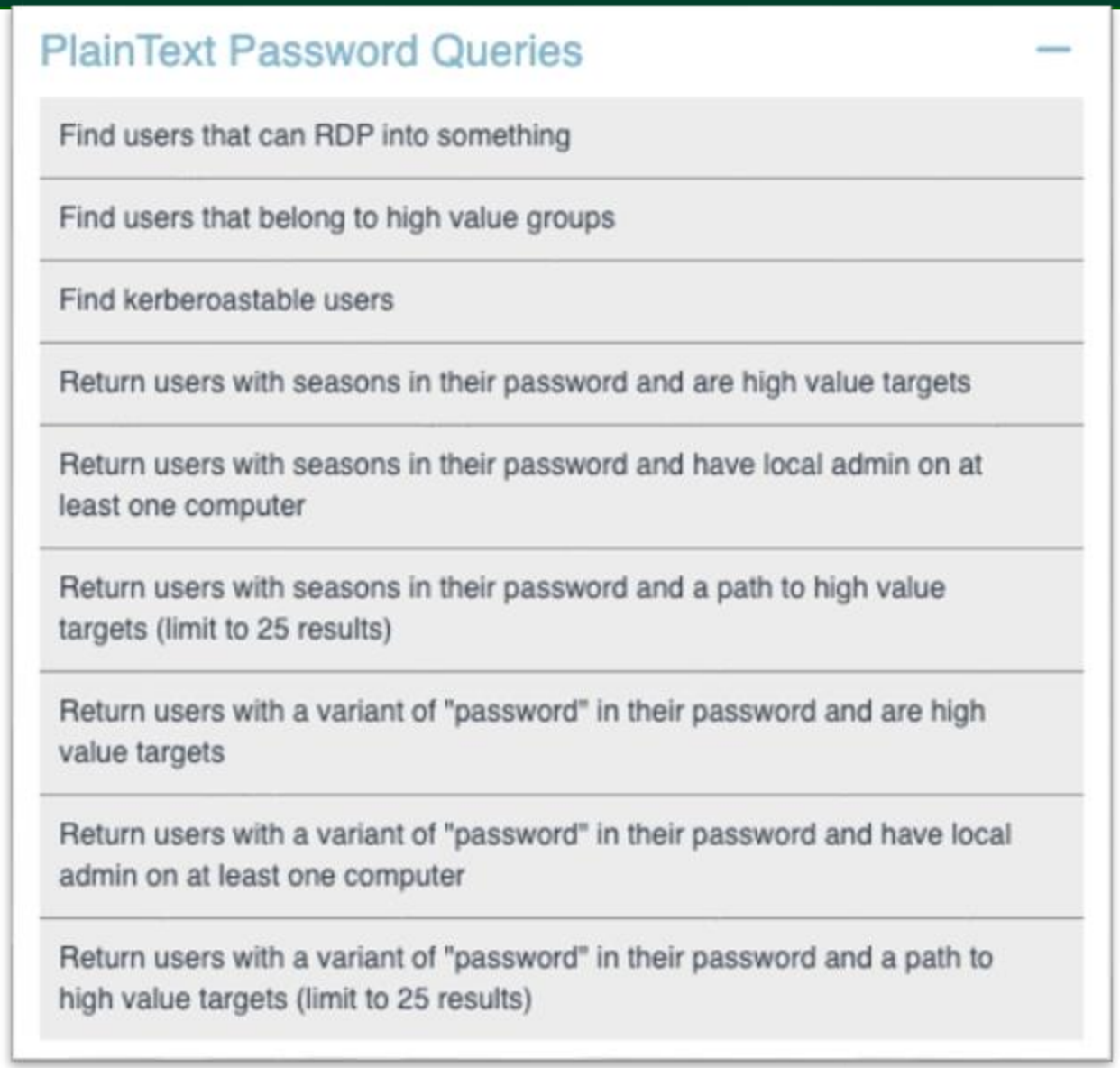
- Not just about Hashcat
- Can take an NTDS file and perform analytics
  - Password sharing clusters
- Can import data into BloodHound
- Creates a new Edge "*SamePassword*"
- Can identify password sharing clusters across multiple domains

https://github.com/SySS-Research/hashcathelper

CrackHound

- Puts password data into BloodHound
- Upload Hashcat cracked output into BloodHound
  - Use it to make queries against passwords
  - Find attack paths based off predicable passwords

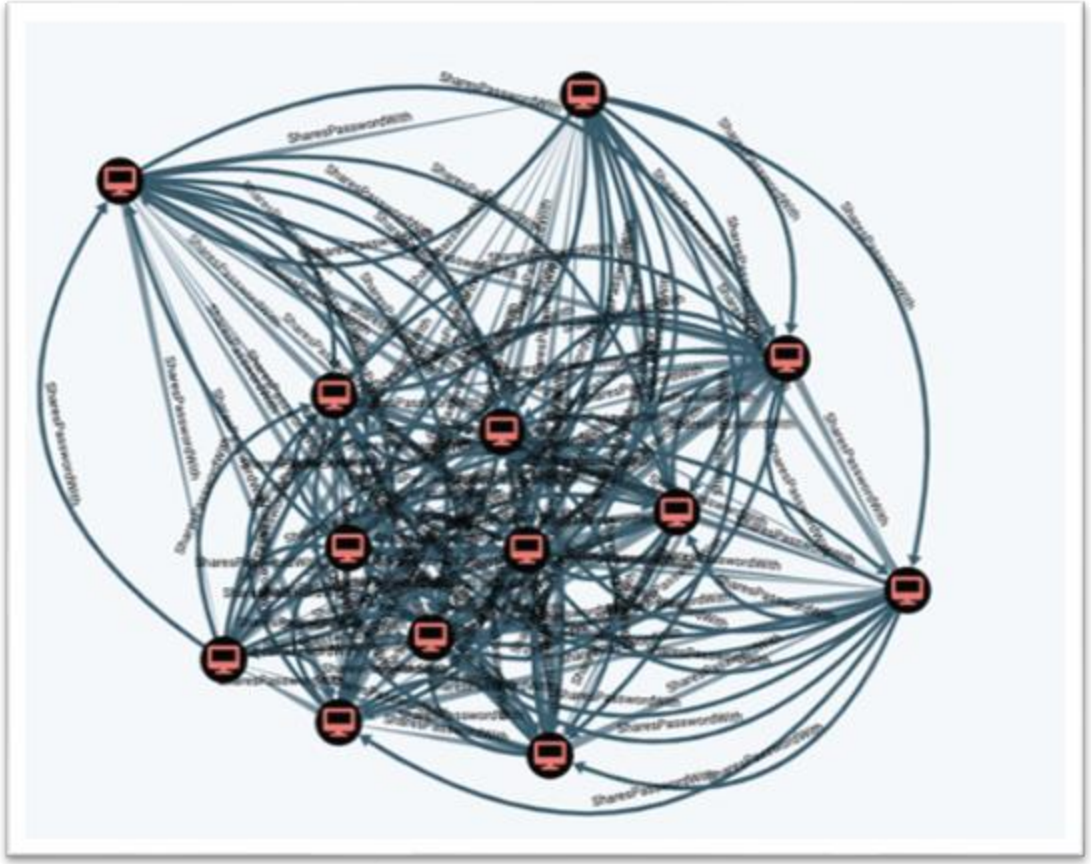
https://www.trustedsec.com/blog/expanding-the-hound-introducing-plaintext-field-to-compromised-accounts/



Max

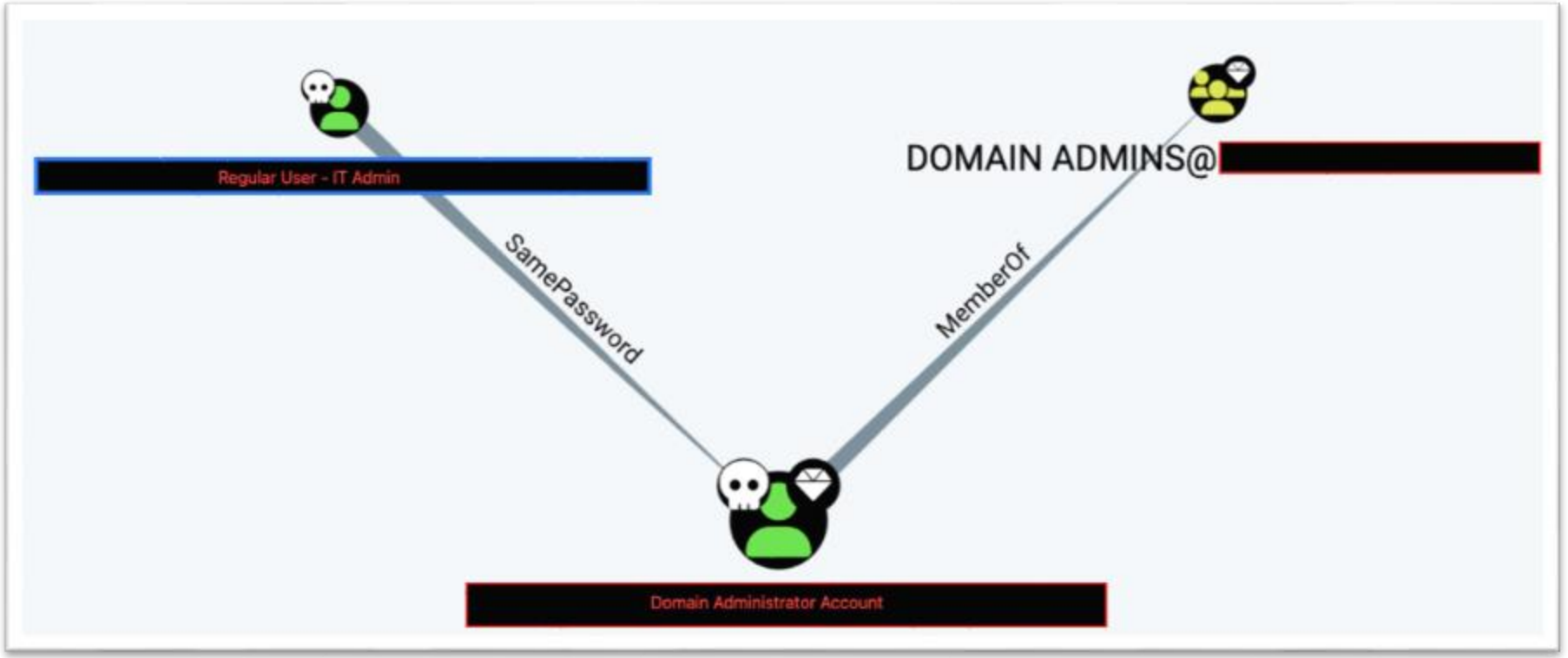
- BloodHound Extension
- Can create new edges such ash *HasSPNConfigured* and *SharesPasswordWith*
- Can be used to visualize attack paths via shared local administrator passwords

https://whynotsecurity.com/blog/max2/



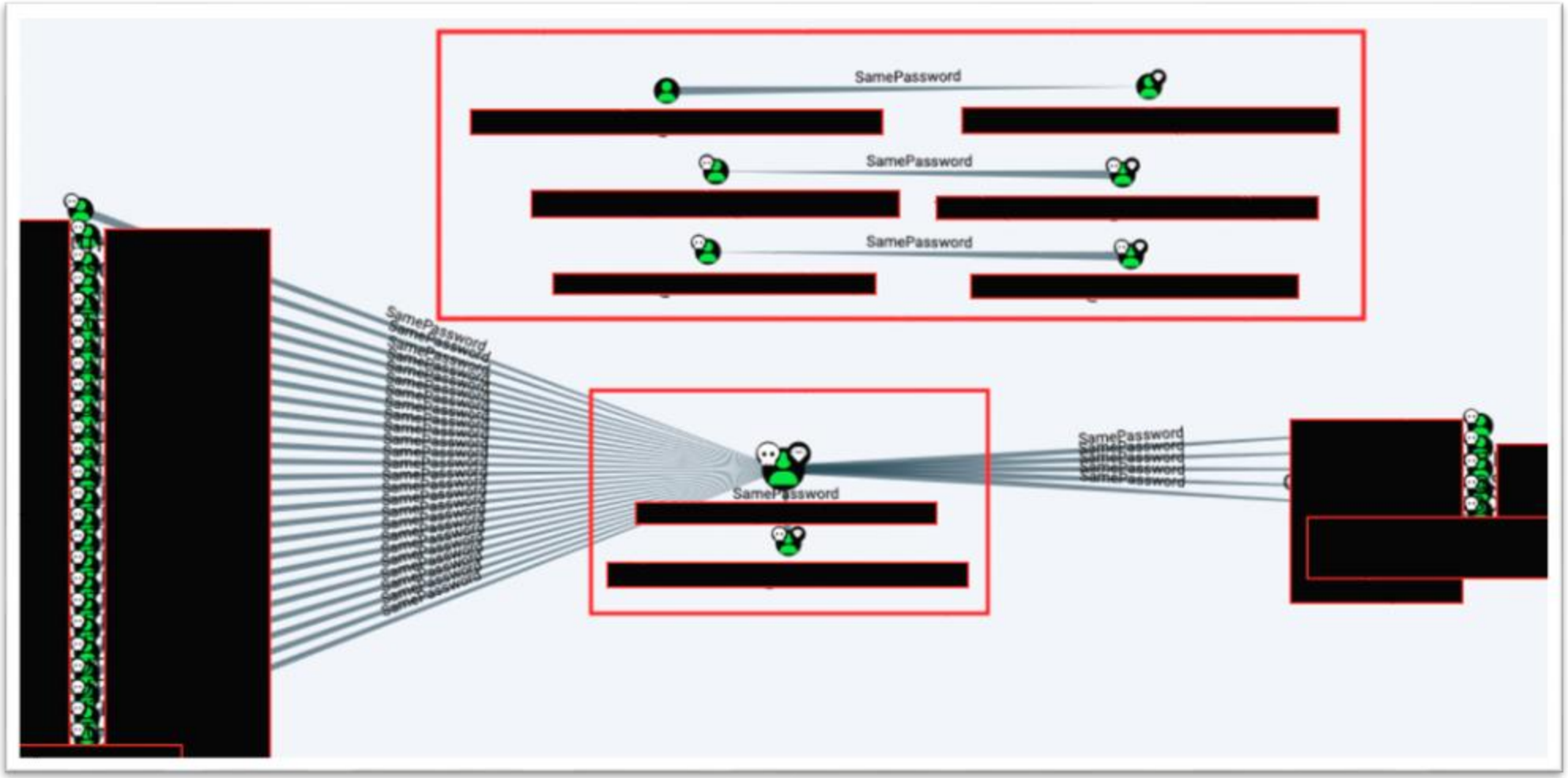
Real Life Scenarios – Client 1

- **Scenario:** Administrators sharing passwords between their regular and administrative accounts
- Administrator accounts use pseudonyms to hide relationship
- Discovered Easily via the graph



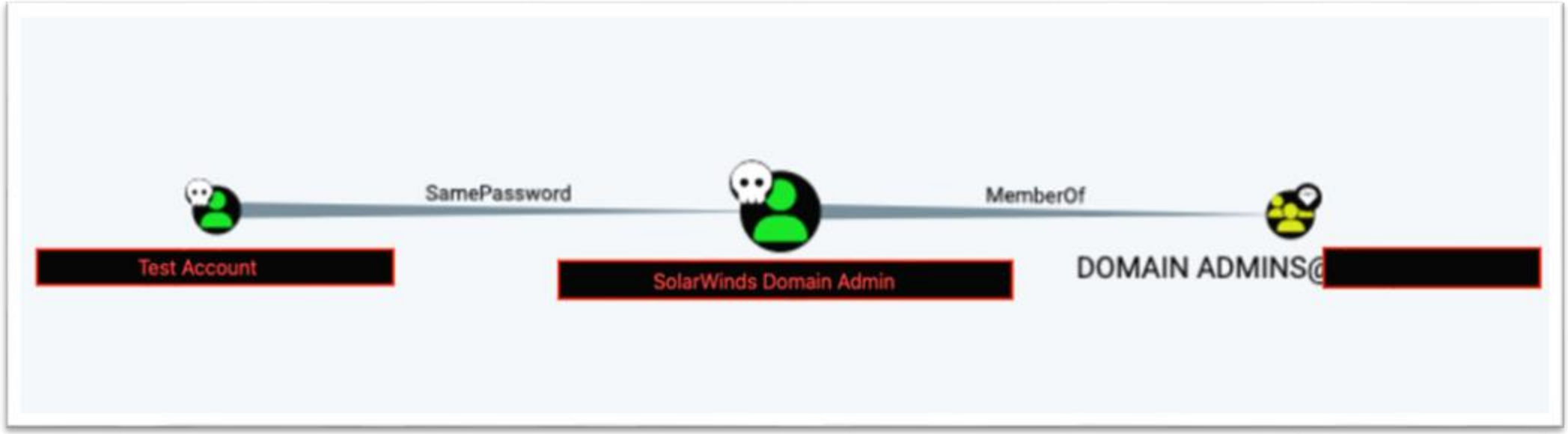
Real Life Scenarios – Client 1

- Password also shared between generic shared accounts and domain administrator service accounts



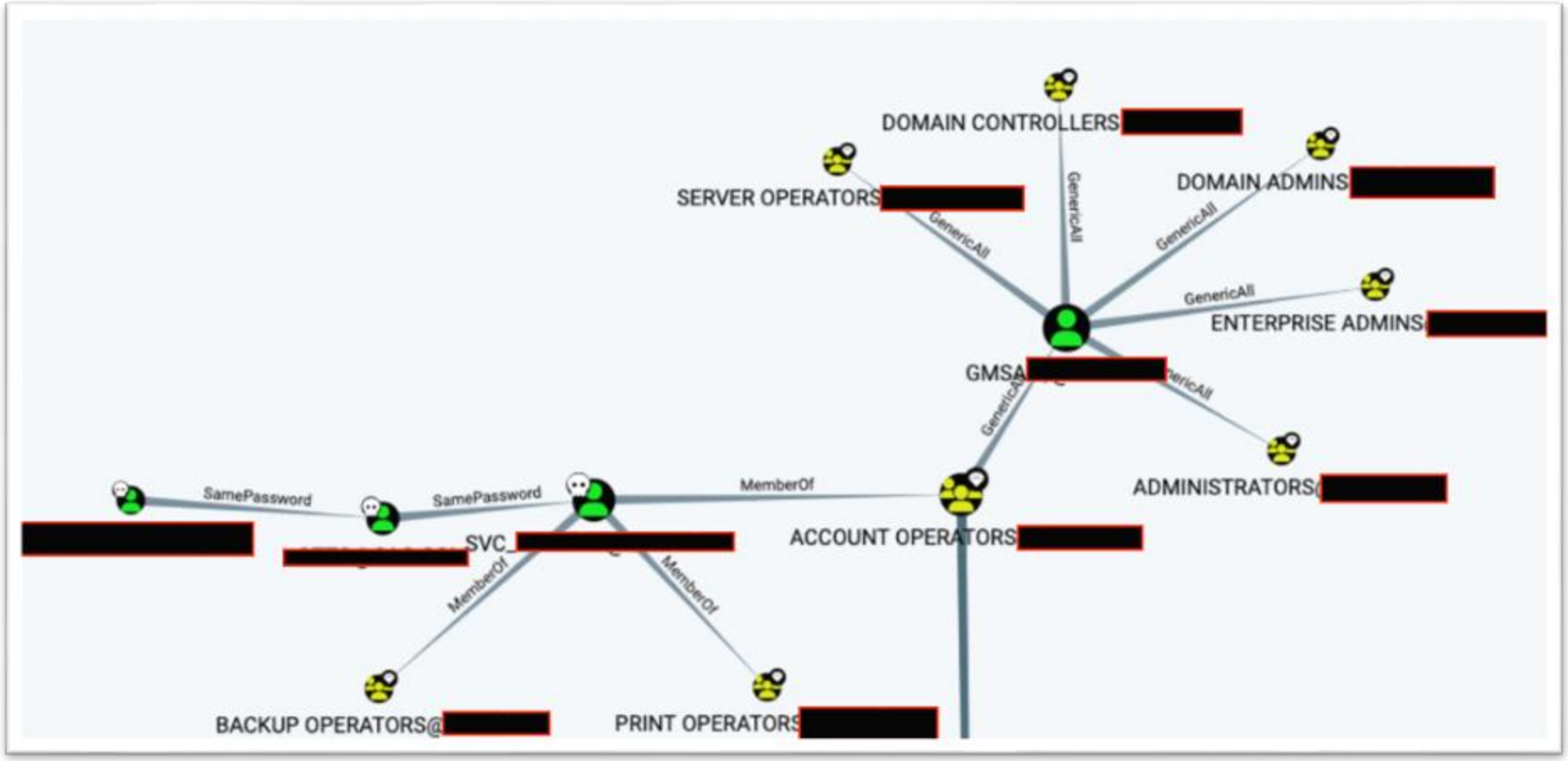
Real Life Scenarios – Client 2

- Useless Test account vulnerable to Kerberoasting – but no privileges
- Used the same password as The SolarWinds Domain Account
- SolarWinds account was not vulnerable to Kerberoasting



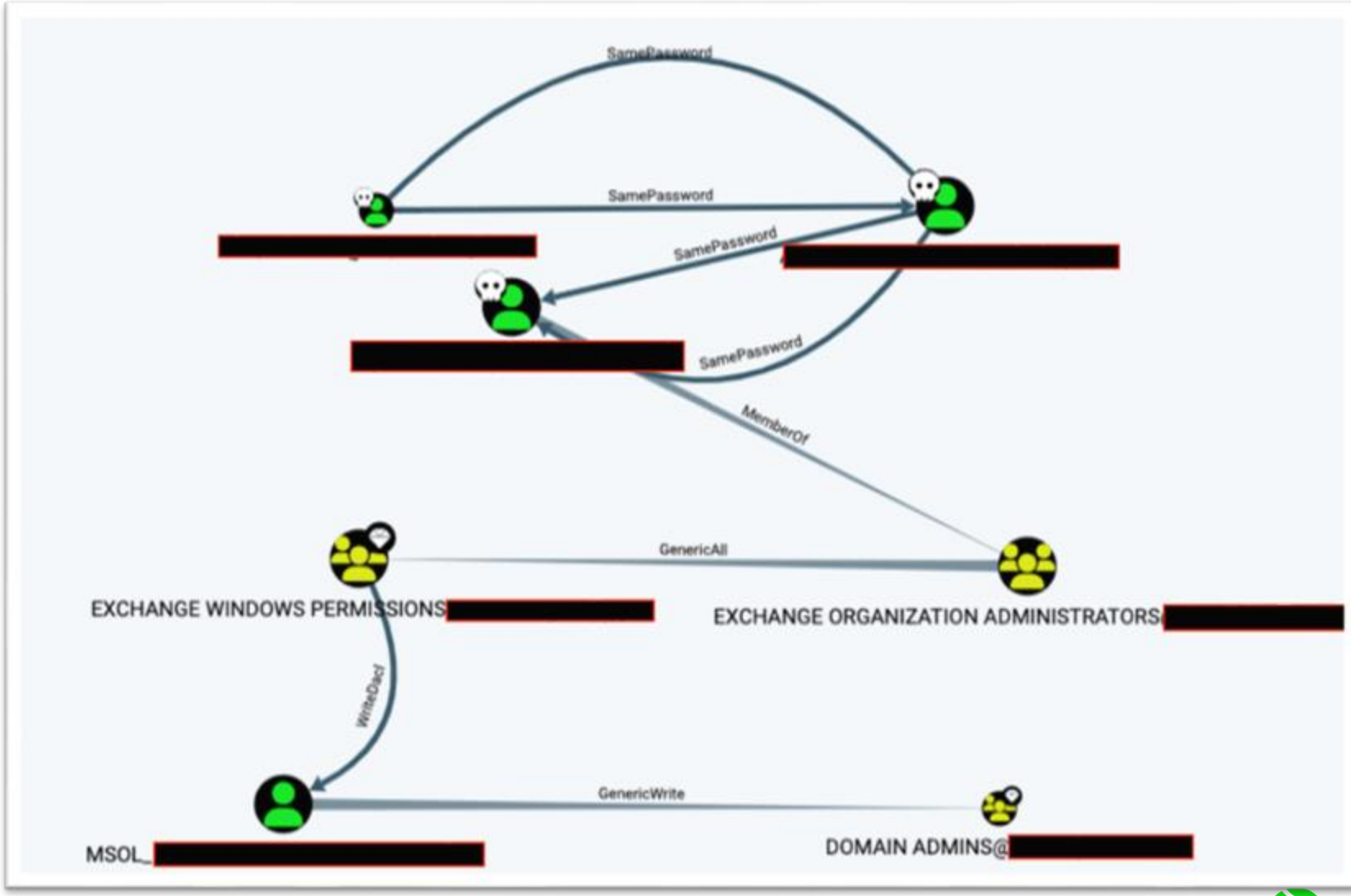
Real Life Scenarios – Client 3

- Attack paths don't have to be direct – can be part of longer attack chains containing multiple hops



Real Life Scenarios – Client 4

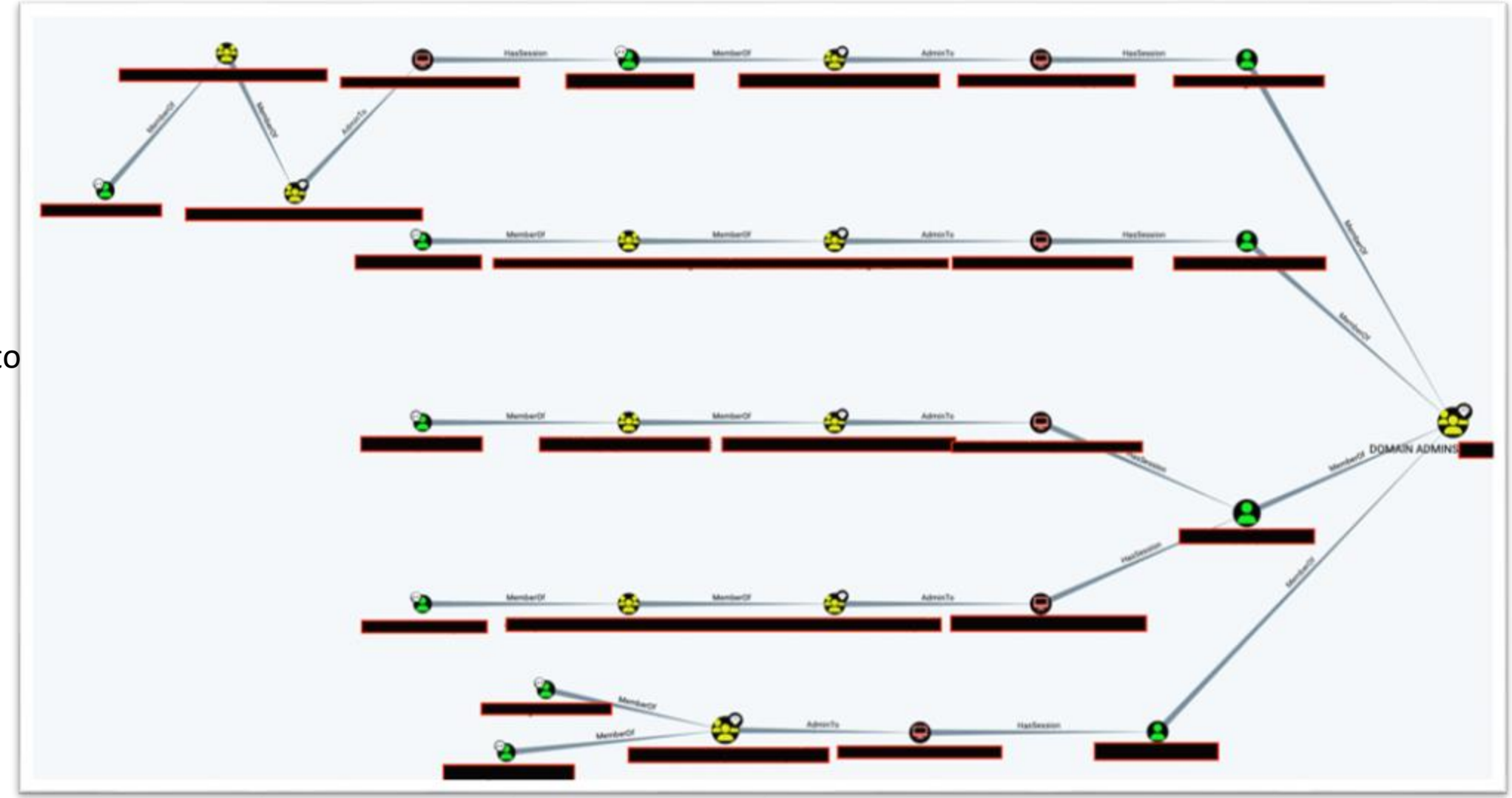
- Attack paths don't have to be direct – can be part of longer attack chains containing multiple hops



Real Life Scenarios – Client 5

- Spring2024 Yields multiple attack paths to Domain Admin

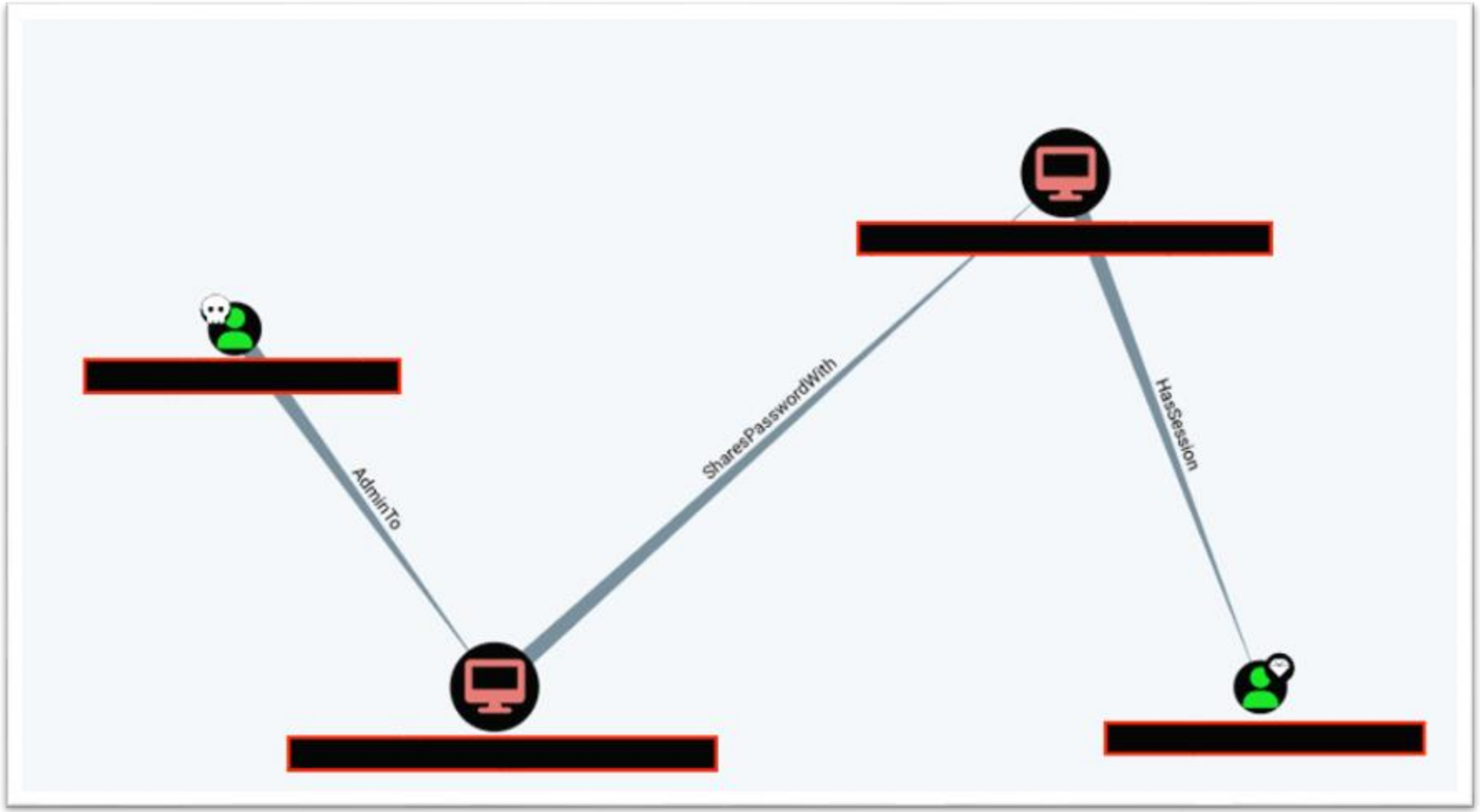
Multiple unique paths to Domain Admin from single weak password



TRUSTEDSEC

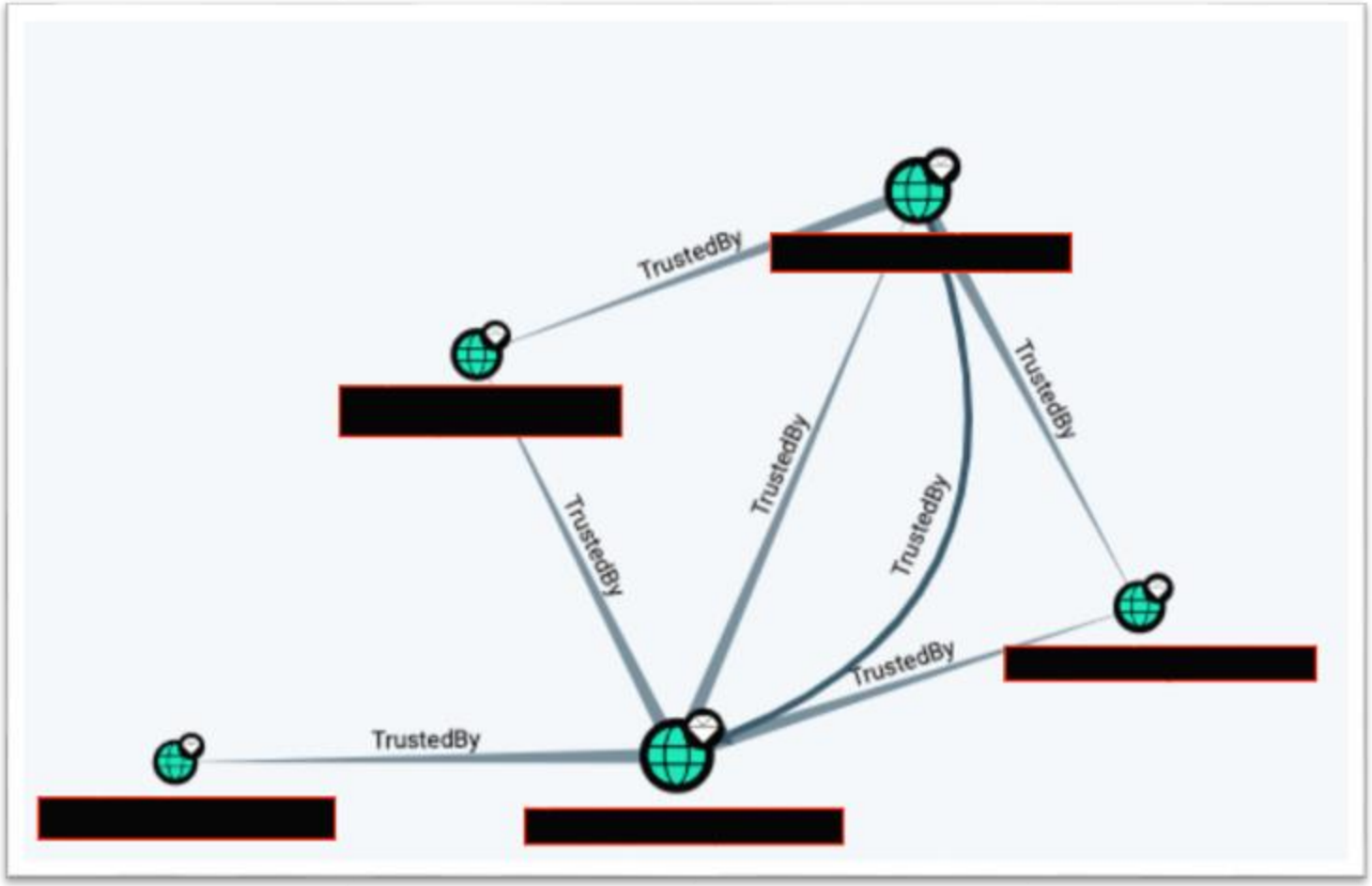
Real Life Scenarios – Client 6

- User has admin to one system, however no path to DA
- By exploiting a shared local Administrator password, is able reach DA session



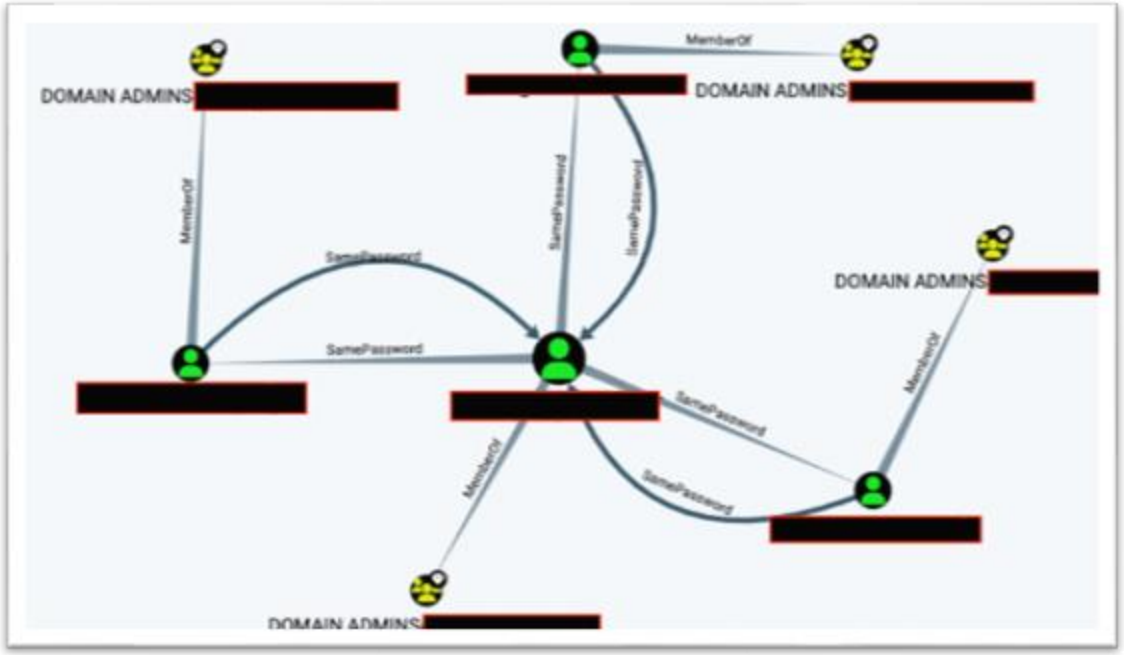
Real Life Scenarios – Client 7

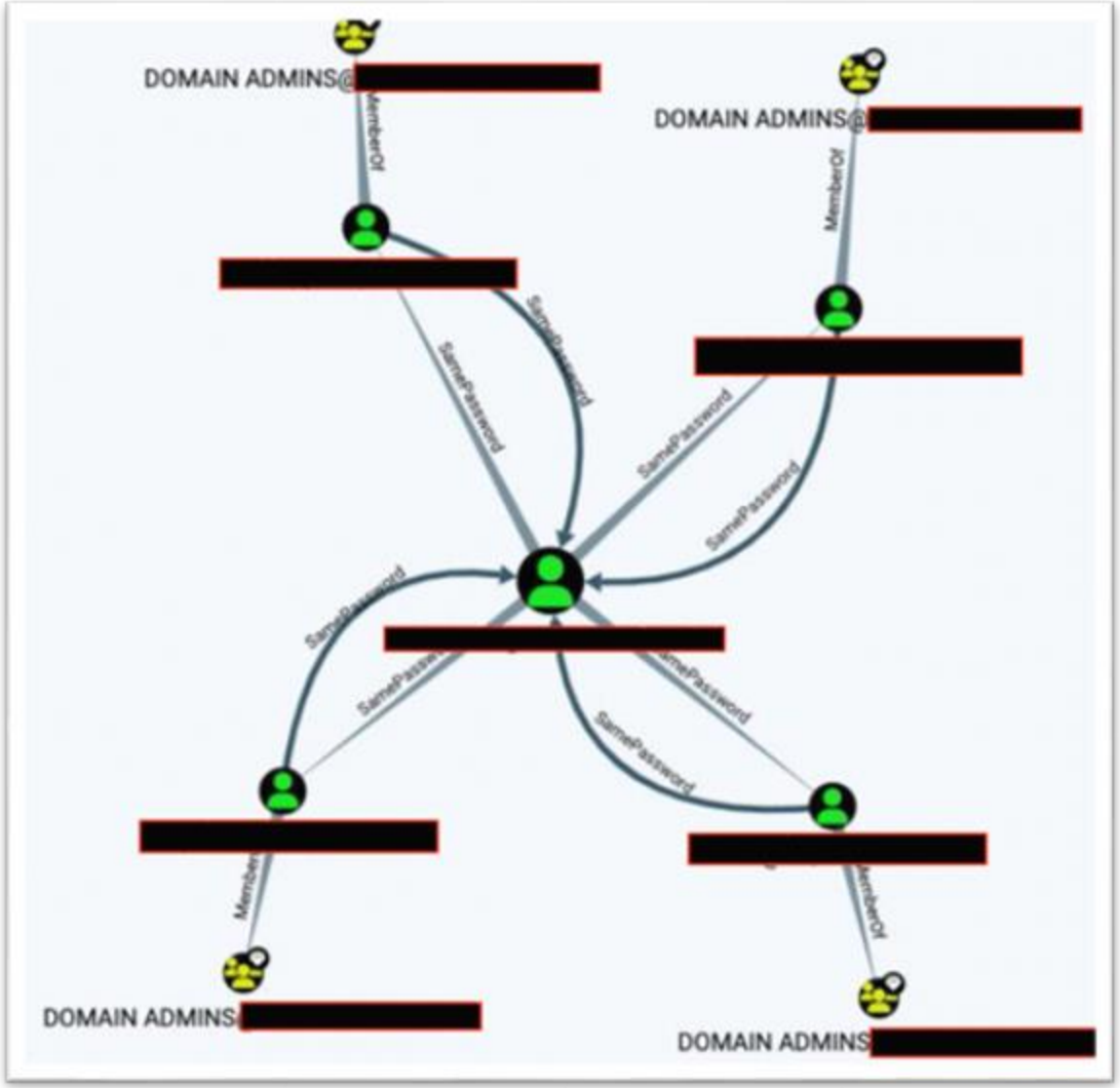
- Five separate domains – all in separate forests
- Normally, you would have to Pwn them one by one



Real Life Scenarios – Client 7

- Multiple cases of separate accounts across different forests all sharing the same password





TRUSTEDSEC

Conclusion

- You may have compromised the domain one way, but there are likely tons of other ways you could have also done so
- Many of these involve weak and shared passwords
- More paths = More good
- Clients love visuals