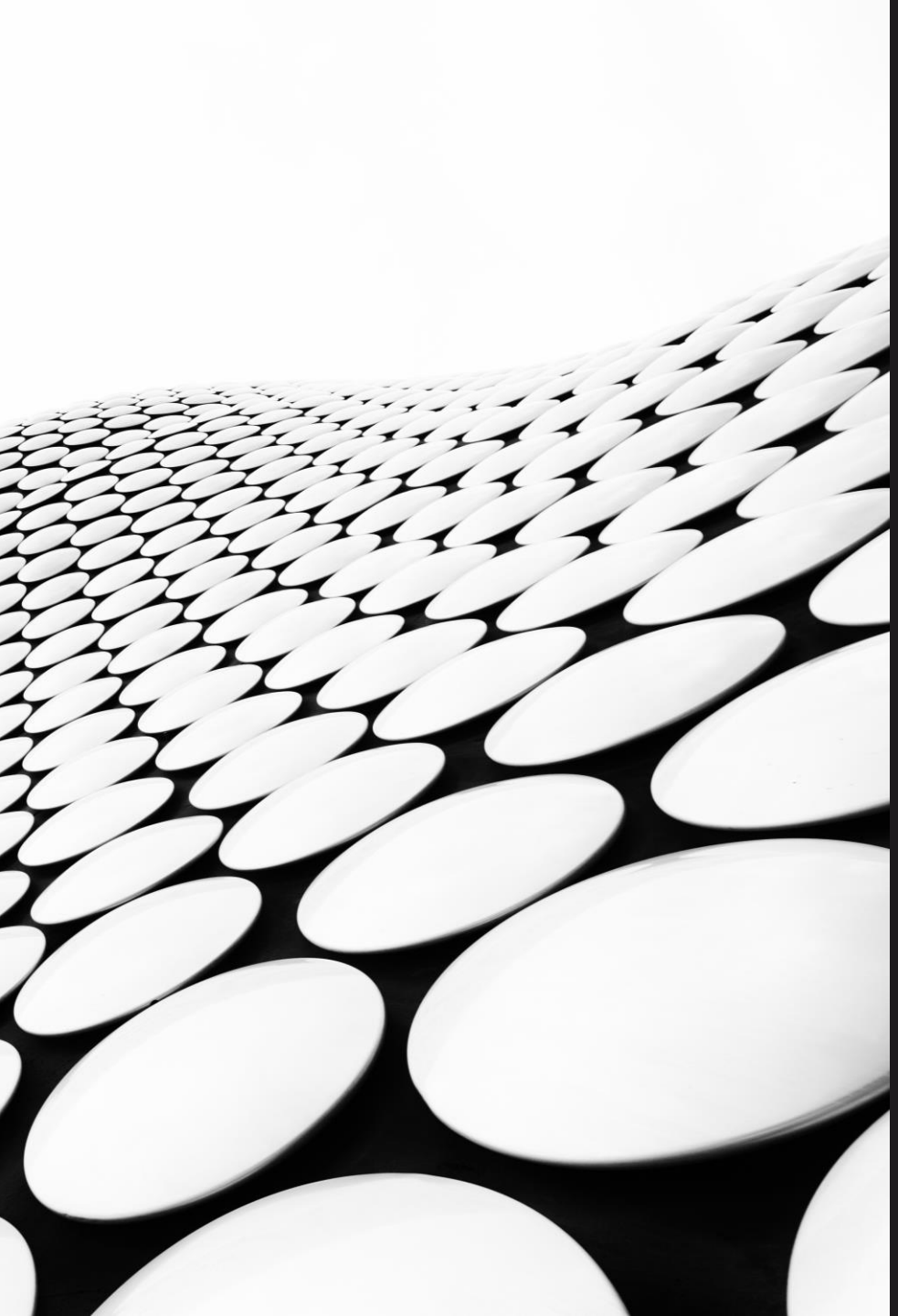
Active Directoryにおける LDAPの攻撃目線と防御目線の活用

鵜山　通夫



自己紹介
鵜山　通夫

経歴
開発・運用　10年程度
ユーザ企業にて業務
サイバーセキュリティ業務　3年程度
　-脅威分析・教育関連

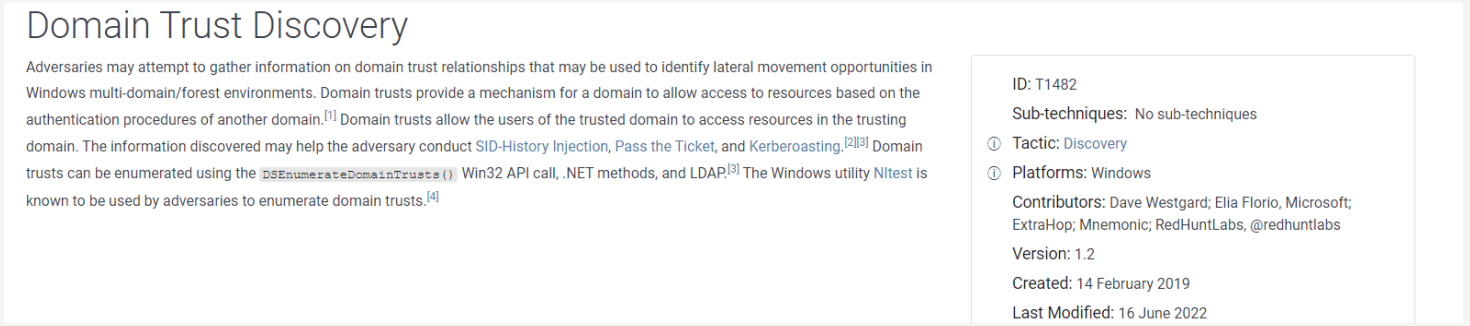
※本プレゼン内容は個人の考えをまとめたものとなります。

Ageda

- 背景
- LDAPについて
- 攻撃者目線
- 防御側目線
- まとめ

背景

- 標的型攻撃において、Active Directoryは偵察行為から侵害へとつながる重要な攻撃対象となっている。
- たとえば、MITRE ATT&CK　T1482では「Domain Trust Discovery」としてLDAPが記載されている。



Domain Trust Discovery

Adversaries may attempt to gather information on domain trust relationships that may be used to identify lateral movement opportunities in Windows multi-domain/forest environments. Domain trusts provide a mechanism for a domain to allow access to resources based on the authentication procedures of another domain.[1] Domain trusts allow the users of the trusted domain to access resources in the trusting domain. The information discovered may help the adversary conduct SID-History Injection, Pass the Ticket, and Kerberoasting.[2][3] Domain trusts can be enumerated using the `DSEnumerateDomainTrusts()` Win32 API call, .NET methods, and LDAP.[3] The Windows utility Nltest is known to be used by adversaries to enumerate domain trusts.[4]

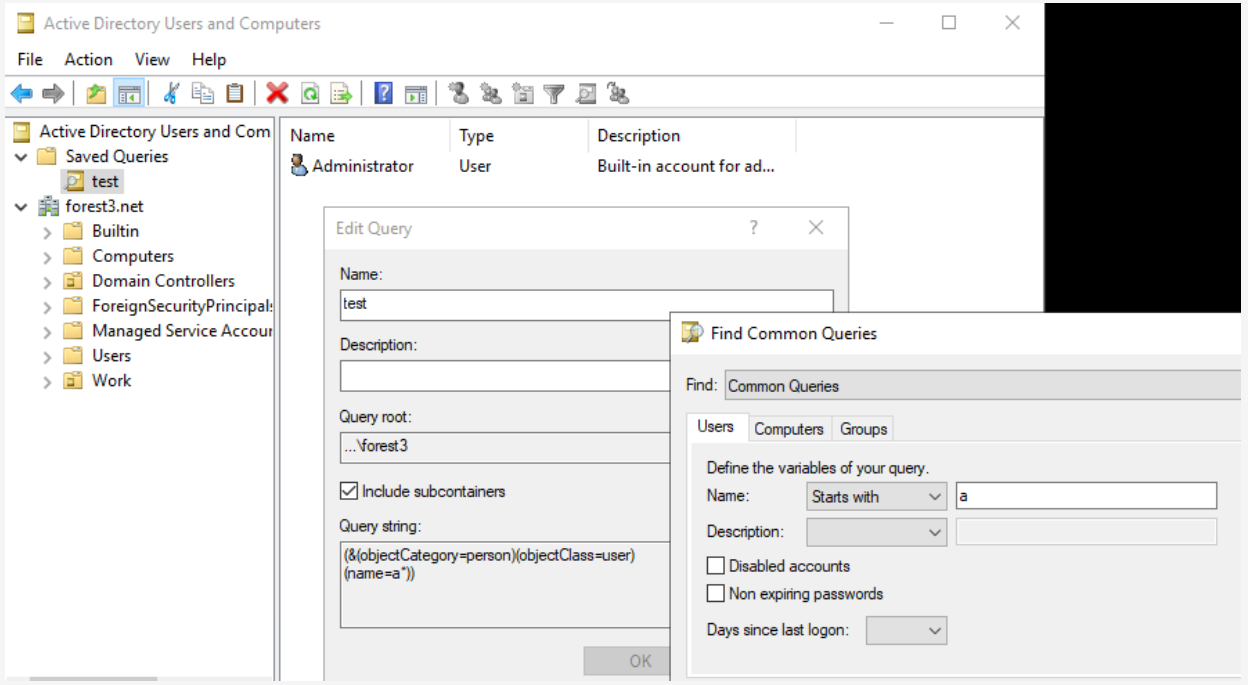
ID: T1482
Sub-techniques: No sub-techniques
Tactic: Discovery
Platforms: Windows
Contributors: Dave Westgard; Elia Florio, Microsoft; ExtraHop; Mnemonic; RedHuntLabs, @redhuntlabs
Version: 1.2
Created: 14 February 2019
Last Modified: 16 June 2022

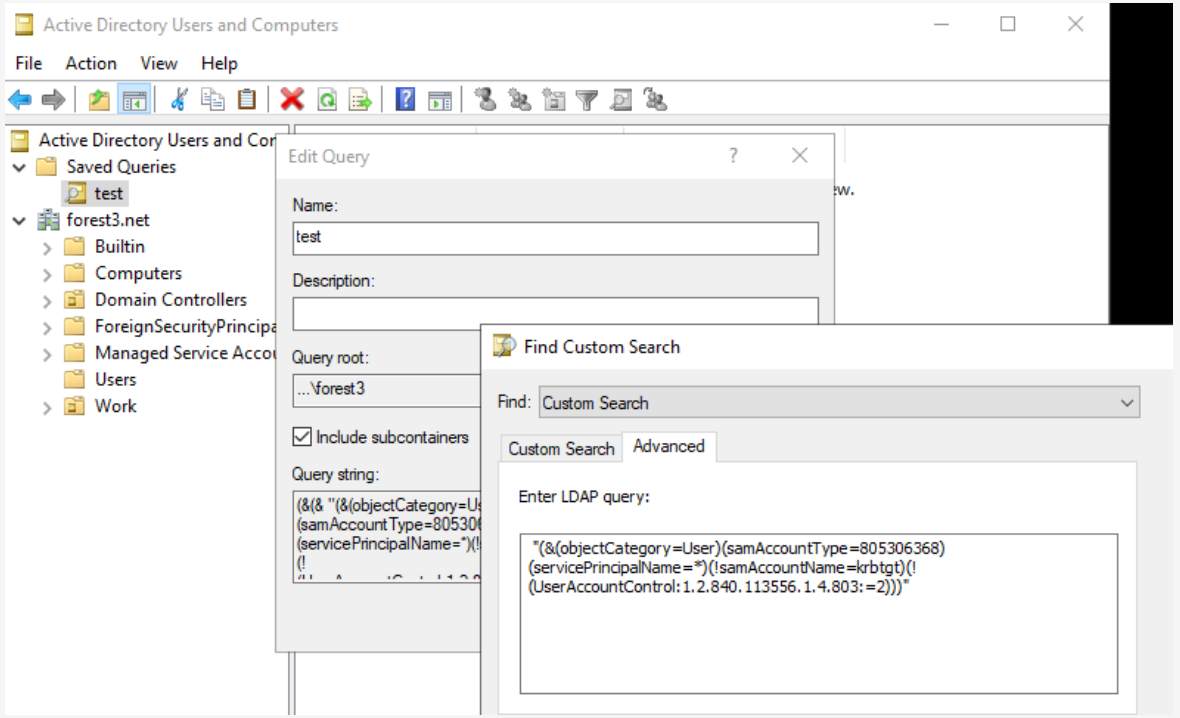
- また、攻撃者がActive Directoryに対する攻撃の初期段階でLDAPを用いた偵察活動を行っていると報告がされている。
  - 具体的にはSolarWinds事案でadfindを利用したドメイン探索
    - https://www.cisa.gov/sites/default/files/publications/Supply_Chain_Compromise_Detecting_APT_Activity_from_known_TTPs.pdf
  - Citrixの脆弱性（CVE-2023-3519）に関するCISA報告
    - Threat Actors Exploiting Citrix CVE-2023-3519 to Implant Webshells

- 攻撃の初期段階においてLDAPを用いた偵察は、防御側にとって極めて重要な情報であり理解を深めることが必要

LDAPについて

- Active Directory Users and Computers





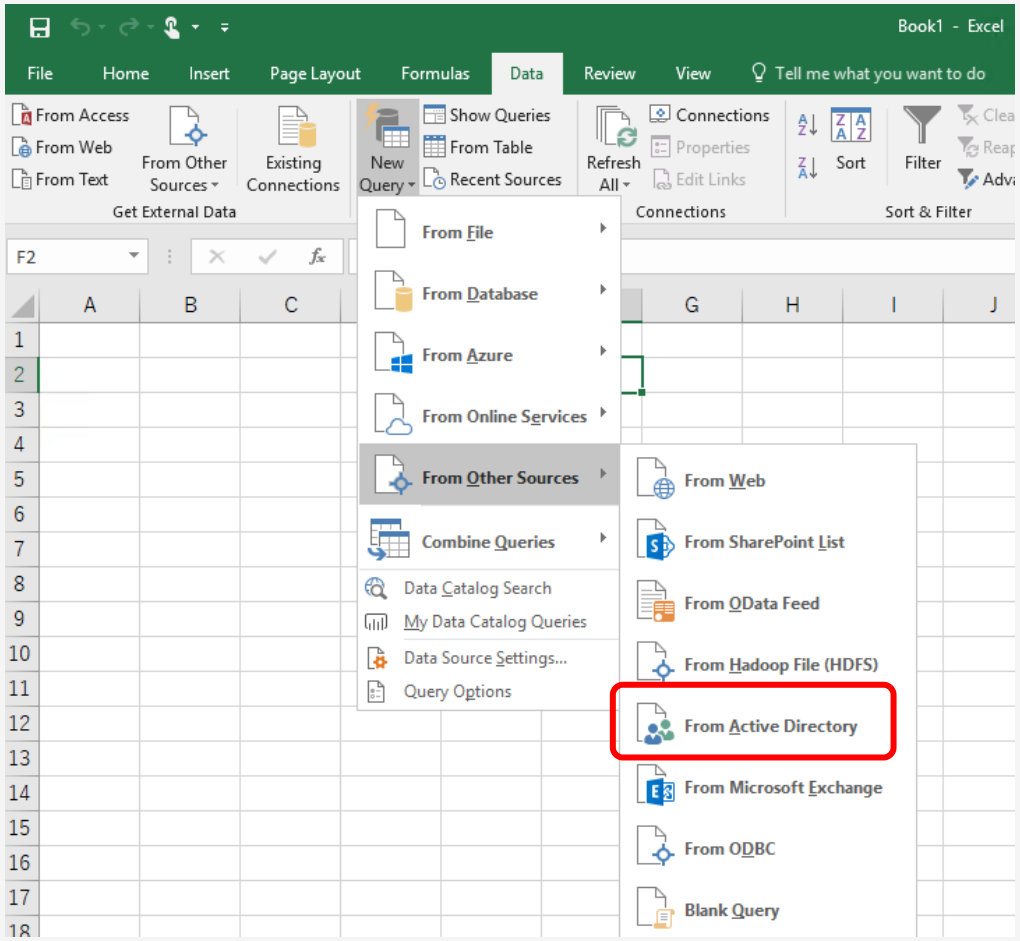
定型的なクエリを作成することが可能
例）ユーザ名が「a」で始まる

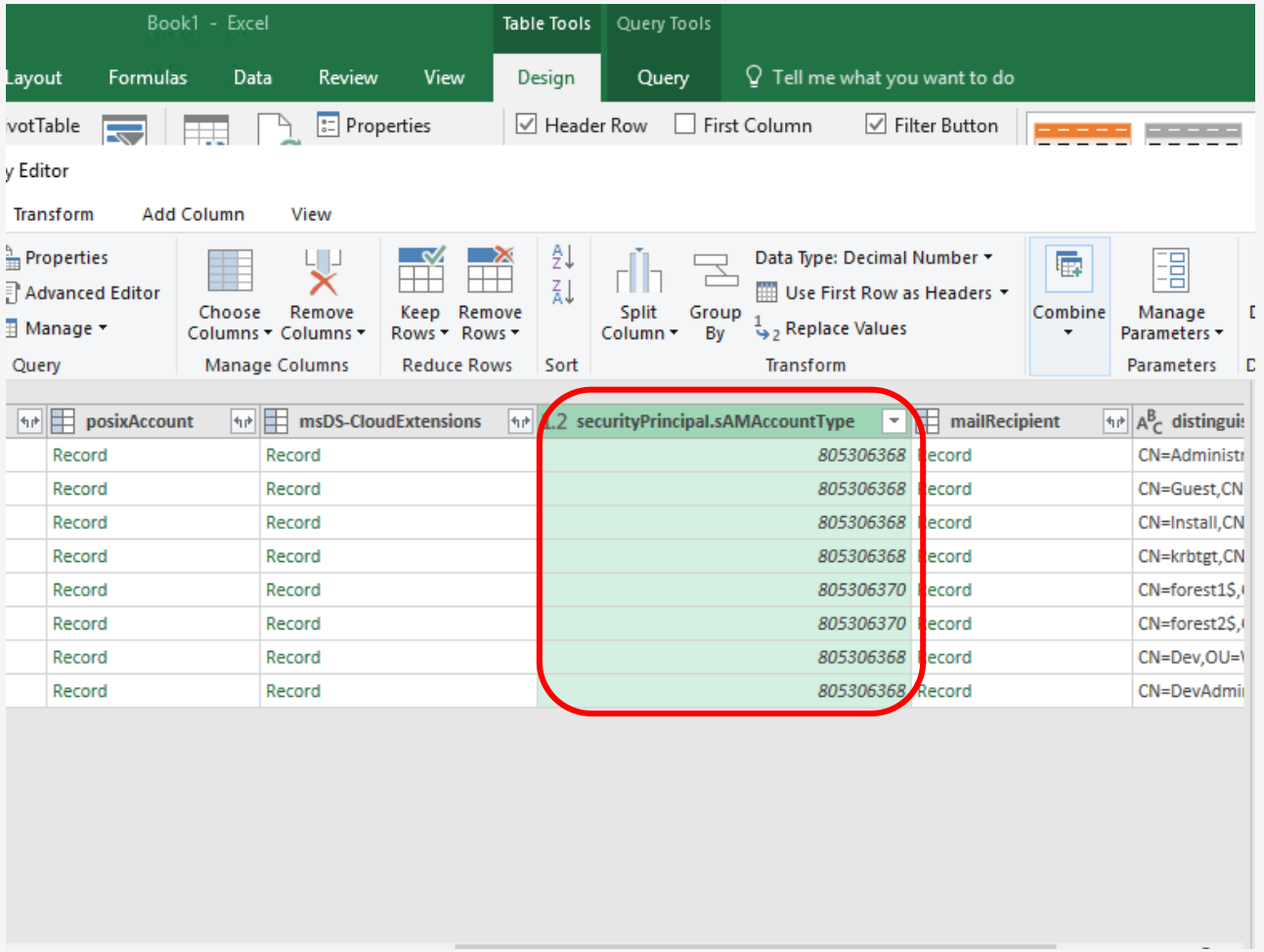
カスタムサーチとして自由なフィルタが作成可能

```
(&(&
"(&(objectCategory=User)(samAccountType=805306368)(servicePrincipalName=*)(!samAccountName=krbtgt)(!(UserAccountControl:1.2.840.113556.1.4.803:=2)))"))
```

LDAPについて

エクセル





SAM-Account-Type 属性

- SAM-Account-Type はアカウントがどの種類に属するかを示す

Name	16進数	10進数	説明
SAM_DOMAIN_OBJECT	0x0	0	
SAM_GROUP_OBJECT	0x10000000	268435456	
SAM_NON_SECURITY_GROUP_OBJECT	0x10000001	268435457	
SAM_ALIAS_OBJECT	0x20000000	536870912	
SAM_NON_SECURITY_ALIAS_OBJECT	0x20000001	536870913	
SAM_USER_OBJECT	0x30000000	805306368	ユーザーアカウント
SAM_MACHINE_ACCOUNT	0x30000001	805306369	コンピューターアカウント
SAM_TRUST_ACCOUNT	0x30000002	805306370	信頼関係があるアカウント
SAM_APP_BASIC_GROUP	0x40000000	1073741824	
SAM_APP_QUERY_GROUP	0x40000001	1073741825	
SAM_ACCOUNT_TYPE_MAX	0x7fffffff	2147483647	

- https://learn.microsoft.com/ja-jp/windows/win32/adschema/a-samaccounttype

UserAccountControl 属性

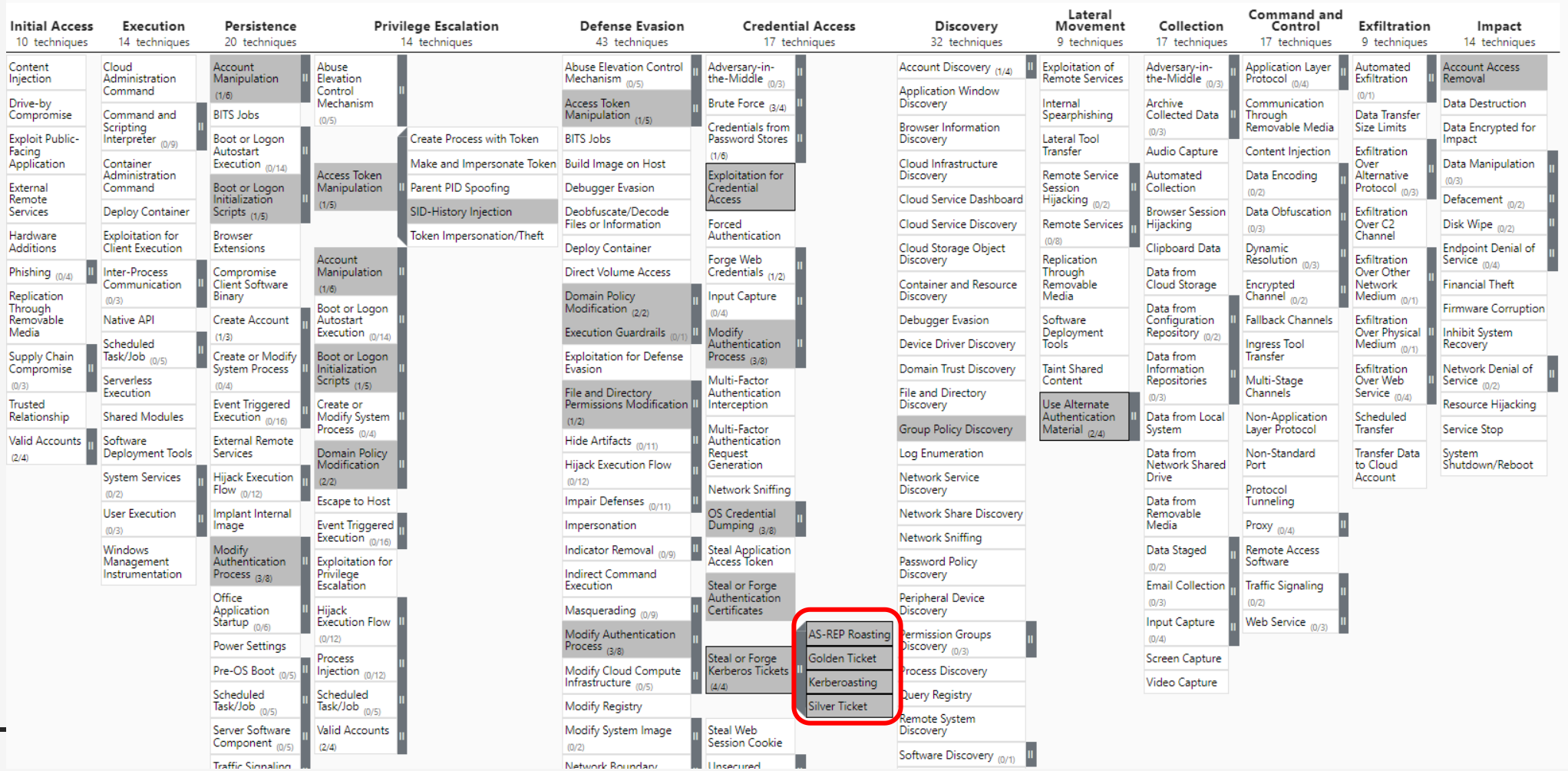
- アカウントに関する様々な設定や属性を示すフラグ

プロパティ フラグ	16 進数	10 進数	説明
SCRIPT	0x0001	1	
ACCOUNTDISABLE	0x0002	2	ユーザー アカウントが無効
HOMEDIR_REQUIRED	0x0008	8	
LOCKOUT	0x0010	16	
PASSWD_NOTREQD	0x0020	32	
PASSWD_CANT_CHANGE	0x0040	64	
ENCRYPTED_TEXT_PWD_ALLOWED	0x0080	128	
TEMP_DUPLICATE_ACCOUNT	0x0100	256	
NORMAL_ACCOUNT	0x0200	512	一般的なユーザーを表す
INTERDOMAIN_TRUST_ACCOUNT	0x0800	2048	
WORKSTATION_TRUST_ACCOUNT	0x1000	4096	
SERVER_TRUST_ACCOUNT	0x2000	8192	
DONT_EXPIRE_PASSWORD	0x10000	65536	
MNS_LOGON_ACCOUNT	0x20000	131072	
SMARTCARD_REQUIRED	0x40000	262144	
TRUSTED_FOR_DELEGATION	0x80000	524288	制約なしKerberos委任
NOT_DELEGATED	0x100000	1048576	
USE_DES_KEY_ONLY	0x200000	2097152	
DONT_REQ_PREAUTH	0x400000	4194304	ログオンに Kerberos 事前認証を必要としない（AS-Reproasting攻撃）
PASSWORD_EXPIRED	0x800000	8388608	
TRUSTED_TO_AUTH_FOR_DELEGATION	0x1000000	16777216	制約付きKerberos 委任
PARTIAL_SECRETS_ACCOUNT	0x04000000	67108864	

- https://learn.microsoft.com/ja-JP/troubleshoot/windows-server/identity/useraccountcontrol-manipulate-account-properties

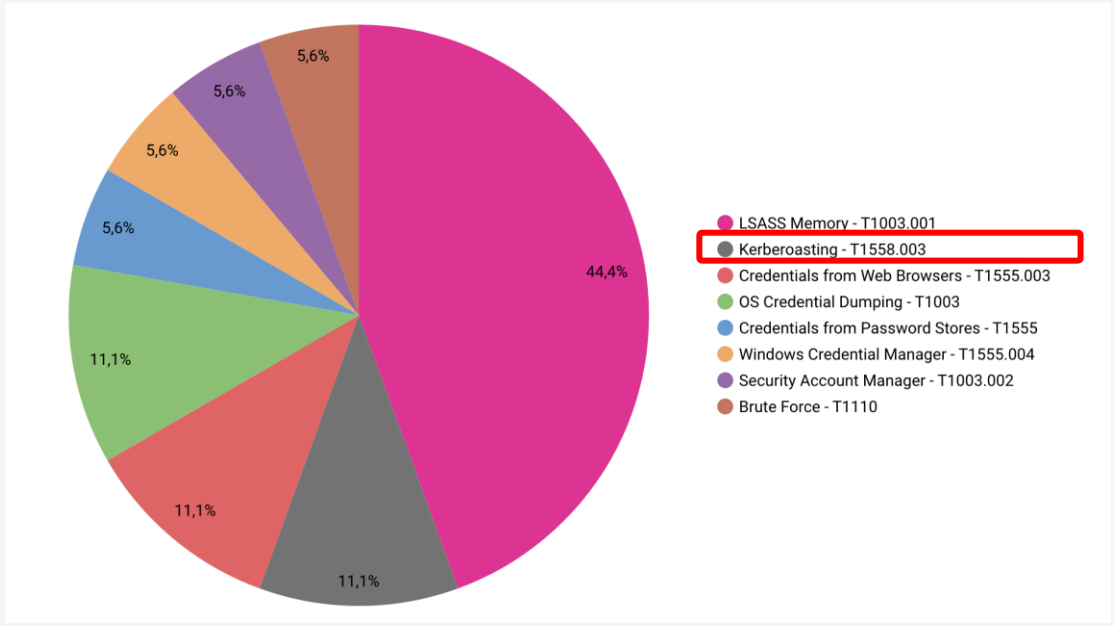
攻撃者目線

- MITRE ATT&CK NavigatorにてActive Directoryを検索



攻撃者目線

攻撃手法としてKerberoastingが注目されている。



***9. Poor Credential Hygiene*として*Kerberoasting*に記載あり**

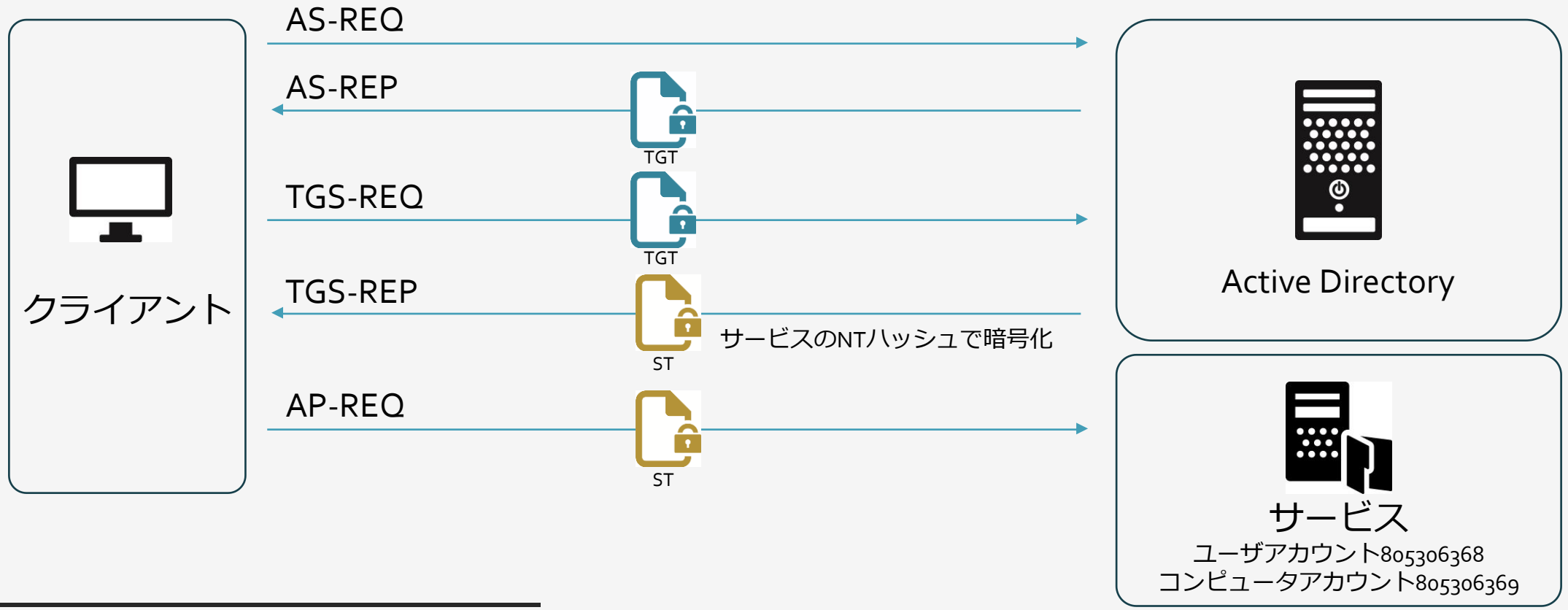
NSA and CISA Red and Blue Teams Share Top Ten Cybersecurity Misconfigurations
https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-278a

Credential Access

2022 Year in Review
https://thedfirreport.com/2023/03/06/2022-year-in-review/

攻撃者目線（Kerberoasting攻撃）

- サービスアカウントのパスワードが脆弱な場合はブルートフォースによるオフラインでのパスワード解析が可能
- どのようなサービスアカウントがあるのか把握するためにLDAPを利用するケースがある



防御側目線

- Kerberoastingの視点からLDAPクエリを通じて潜在的なKerberoasting対象のユーザを調査
- 以下のツールから攻撃に悪用される可能性の高いLDAPクエリについて調査

ツール	概要
Rubeus	Windows環境で動作するKerberosチケット攻撃ツール
SharpHound	Active Directory環境の攻撃シナリオや権限昇格のパスを可視化するために情報収集するツール
Ldapdomaindump	Active Directoryの情報をHTML形式等でダンプすることが可能
LdapSearch-ad	LDAP サービスを通じてActive Directoryからさまざまな情報を迅速に取得するためのスクリプト
PingCastle	Active Directory のセキュリティ レベルを迅速に評価するように設計されたツール
Purple Knight	Active DirectoryやEntra ID等のセキュリティ評価ツール
AD Explorer	Active Directory内のオブジェクトや属性を探索するためのグラフィカルなツールでスナップショットを作成可能

防御側目線(Kerberoasting攻撃につながる偵察)

- Rubeus
- Ldapseach-ad
- PurpleKnight
  - (&(objectCategory=User)(samAccountType=805306368)(servicePrincipalName=*)(!samAccountName=krbtgt)(!(UserAccountControl:1.2.840.113556.1.4.803:=2)))
  - (&(objectClass=user)(servicePrincipalName=*)(!(objectClass=computer))(!(cn=krbtgt))(!(userAccountControl&2)))
  - (&(adminCount=1)(servicePrincipalName=*)(!(servicePrincipalName=kadmin/changepw)))
- SharpHound
- PingCasle
- Ldapdomaindump
- AD Explorer
  - LDAPクエリは発行するもののobjectClass=*として取得するため特徴が見られない

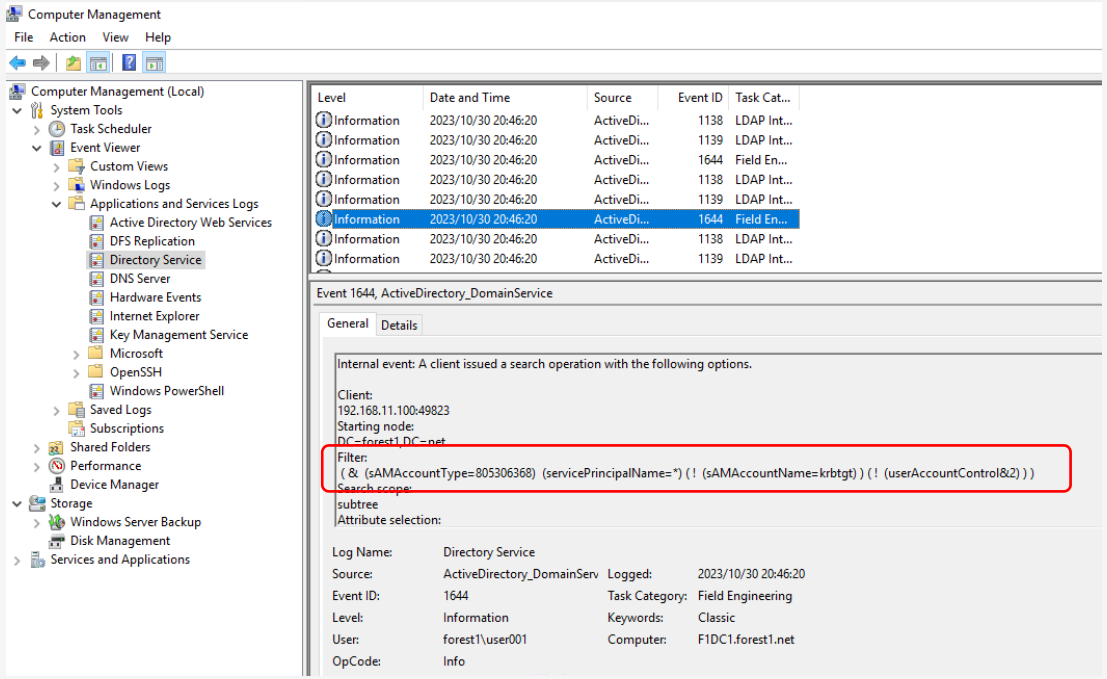
防御側目線(注目するLDAPクエリ)

- servicePrincipalName=*
- userAccountControl
  - userAccountControl:1.2.840.113556.1.4.803:=2など
- admincount
- sIDHistory
- msDS-AllowedToDelegateTo
- msDS-AllowedToActOnBehalfOfOtherIdentity

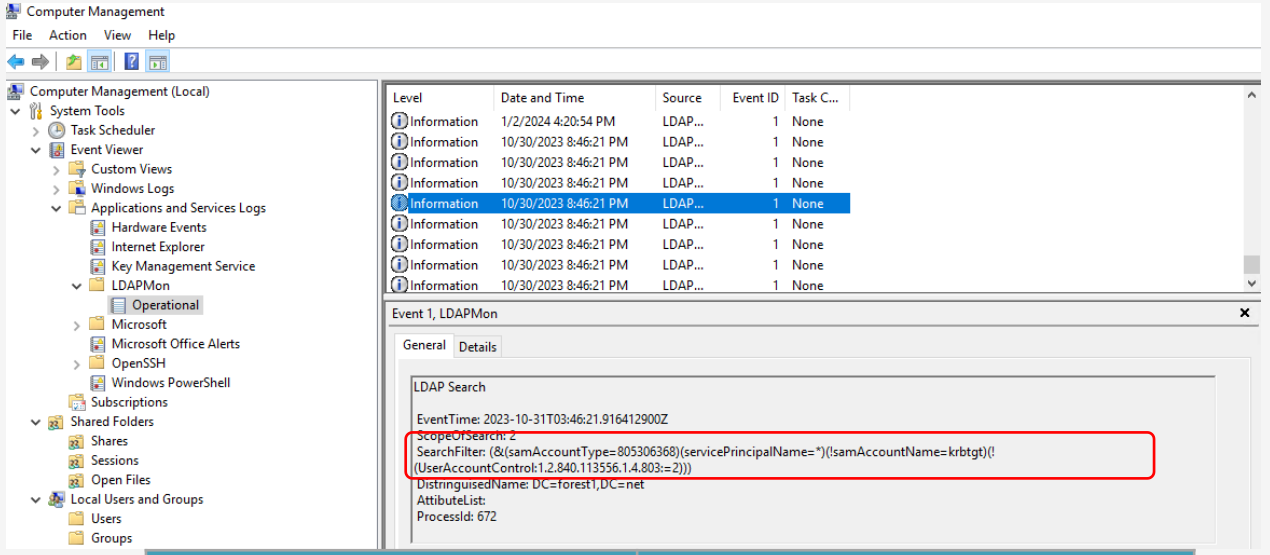
防御側目線(LDAPクエリの検知)

- Active Directoryのログ設定（systemユーザのログなどが多く出力される）
- LDAPMonによるクライアント側のログ収集

ActvieDirectoryログ



LDAPMon



ツール	イベントログ発生件数（概算）
SharpHound	232
PingCastle	3
Purple Knight	4251
AD Explorer	57

1イベントログ当たり約0.5KB

まとめ

- 標的型攻撃等で攻撃者に狙われるActive Directory対して発行されるLDAPクエリの特徴を紹介
- 自社環境をLDAPを利用して調査・アセスメントの実施ができることを考察
  - Active Directoryの構成についてLDAPクエリで容易に確認できる
- 早期のインシデント対応を促進するために、LDAPのログ分析による可能性を示した
- 今後は、脅威ハンティングで注目するべきクエリやデコイ（囮）の有効性の検討を深める