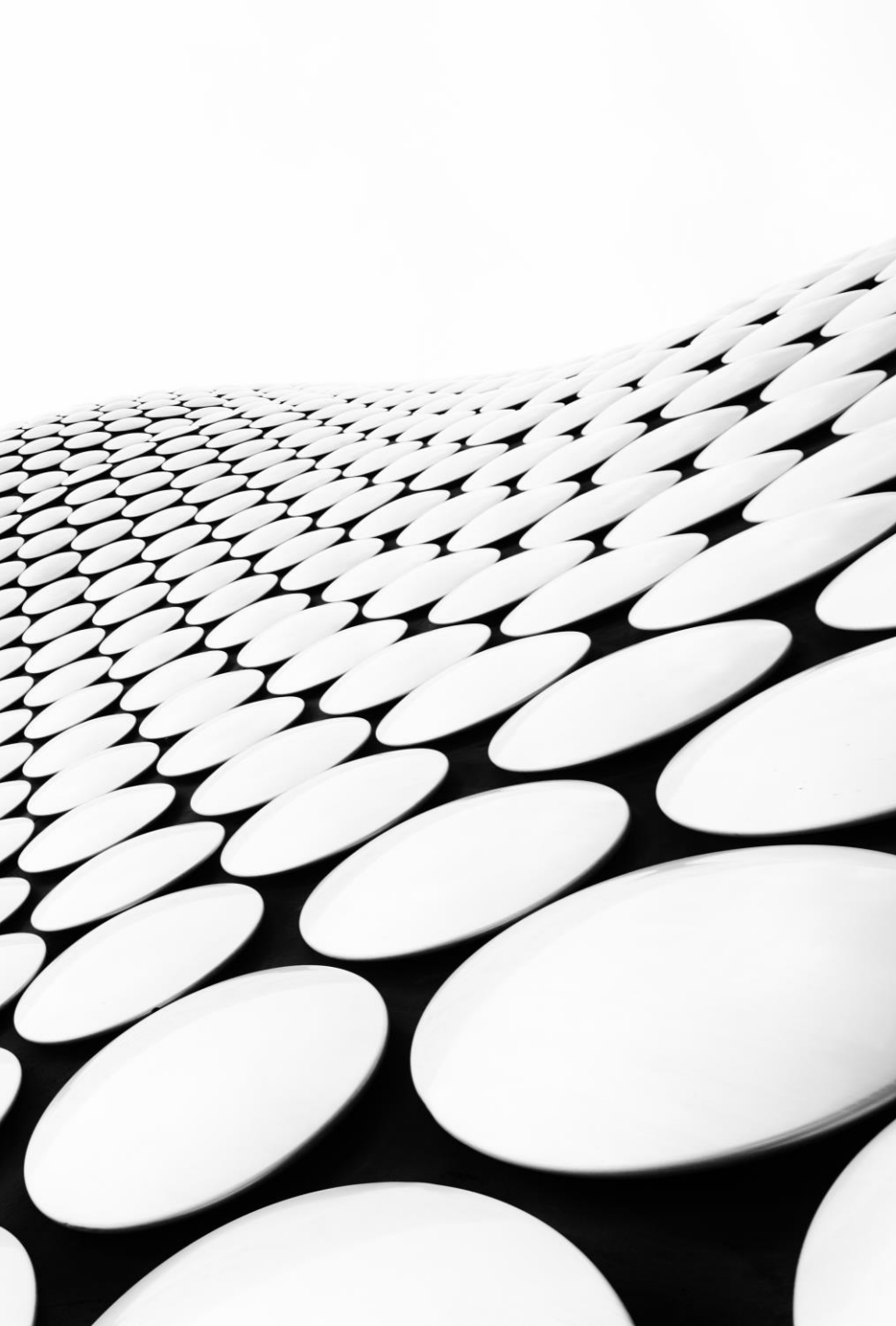


Active Directoryにおける LDAPの攻撃目線と防御目線の活用

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

① Tactic: Discovery

① Platforms: Windows

Contributors: Dave Westgard; Elia Florio, Microsoft; ExtraHop; Mnemonic; RedHuntLabs, @redhuntlabs

Version: 1.2

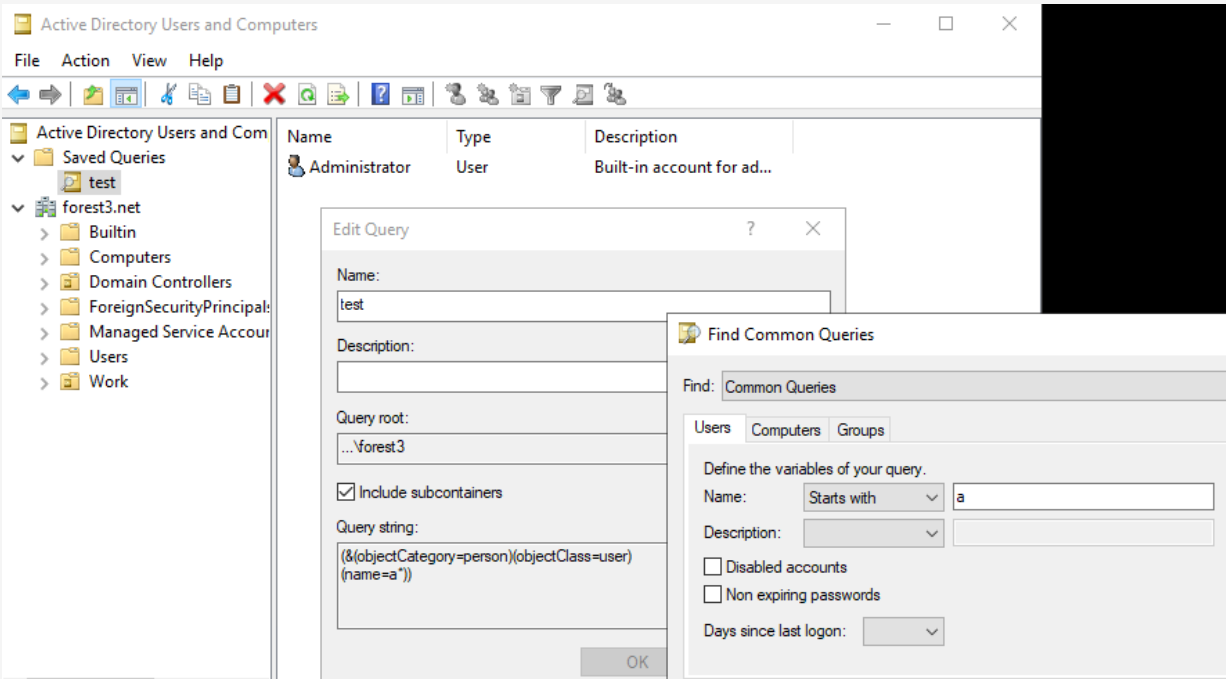
Created: 14 February 2019

Last Modified: 16 June 2022

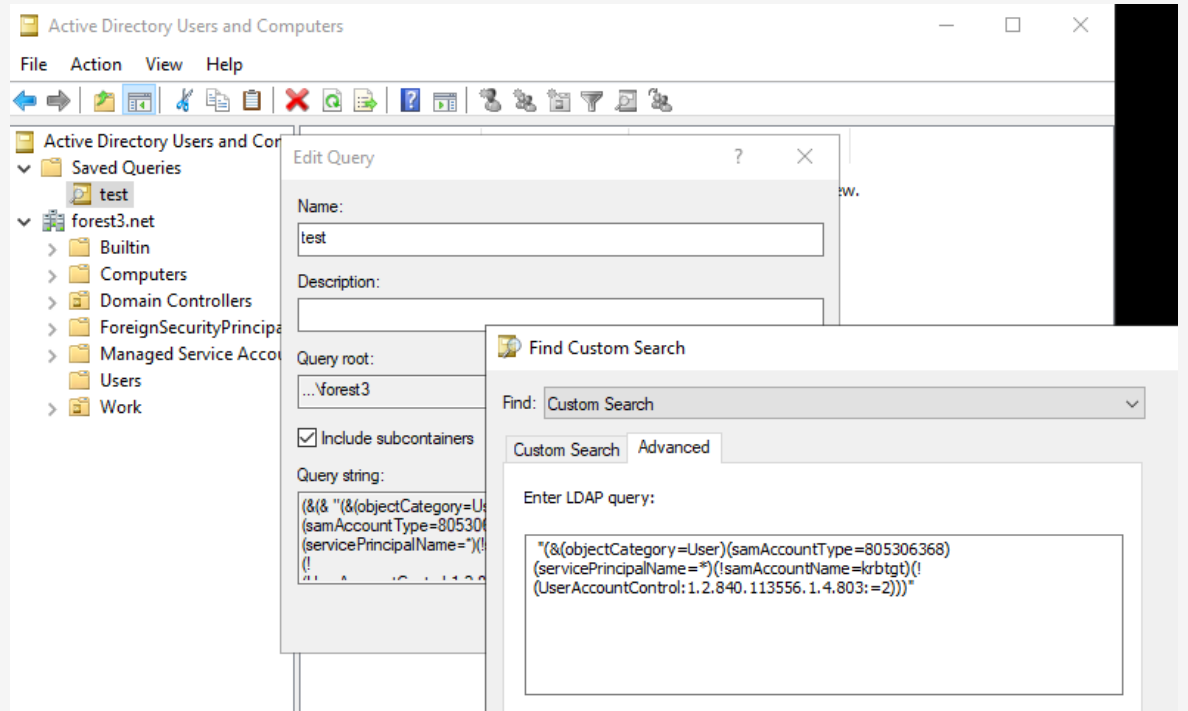
- また、攻撃者がActive Directoryに対する攻撃の初期段階でLDAPを用いた偵察活動を行っていることが報告されている。
 - 具体的にはSolarWinds事案でadfindを利用したドメイン探索
 - https://www.cisa.gov/sites/default/files/publications/Supply_Chain_Compromise_Detecting_APT_Activity_from_known_TTPs.pdf
 - Citrixの脆弱性（CVE-2023-3519）に関するCISA報告
 - [Threat Actors Exploiting Citrix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

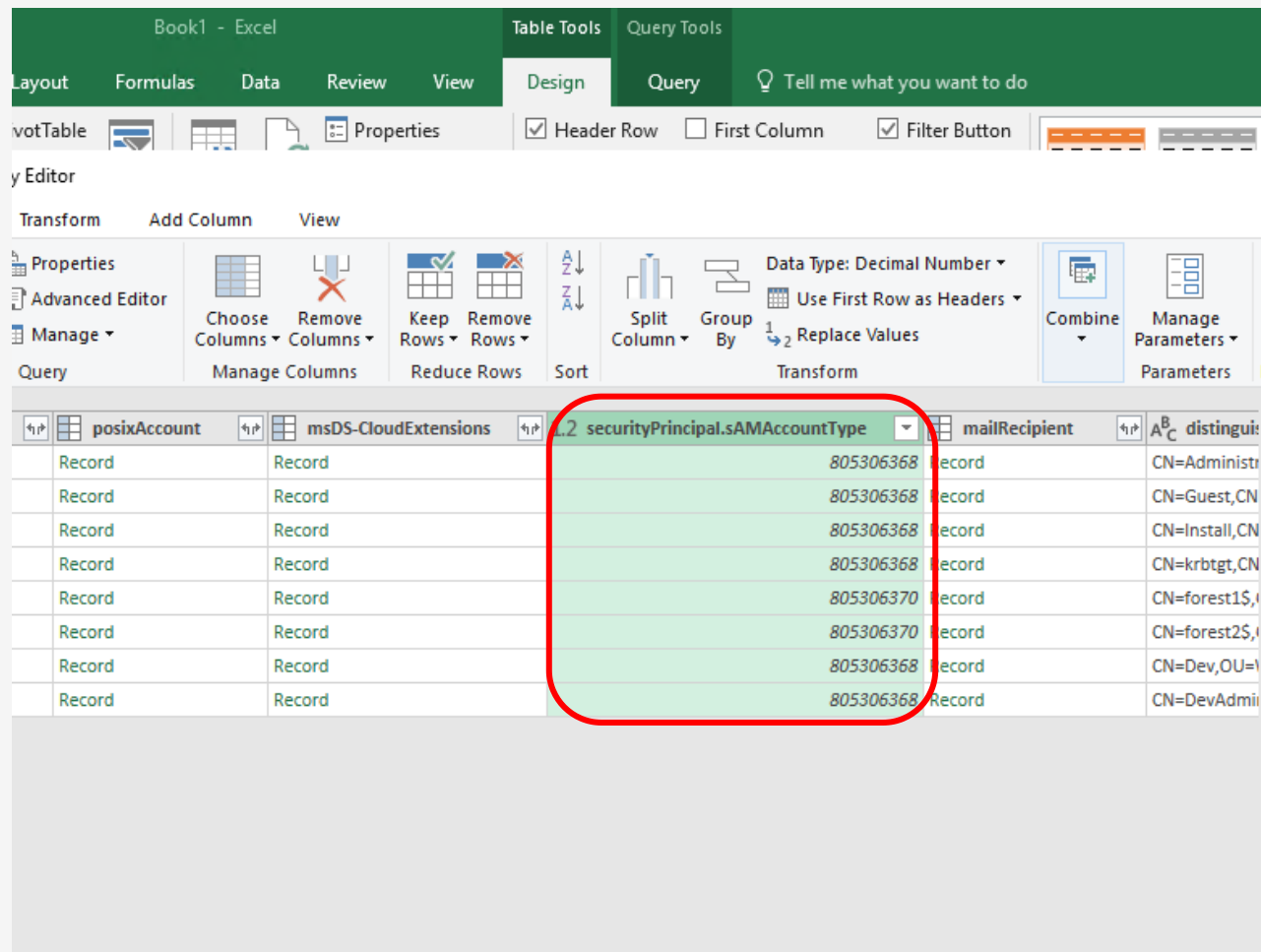
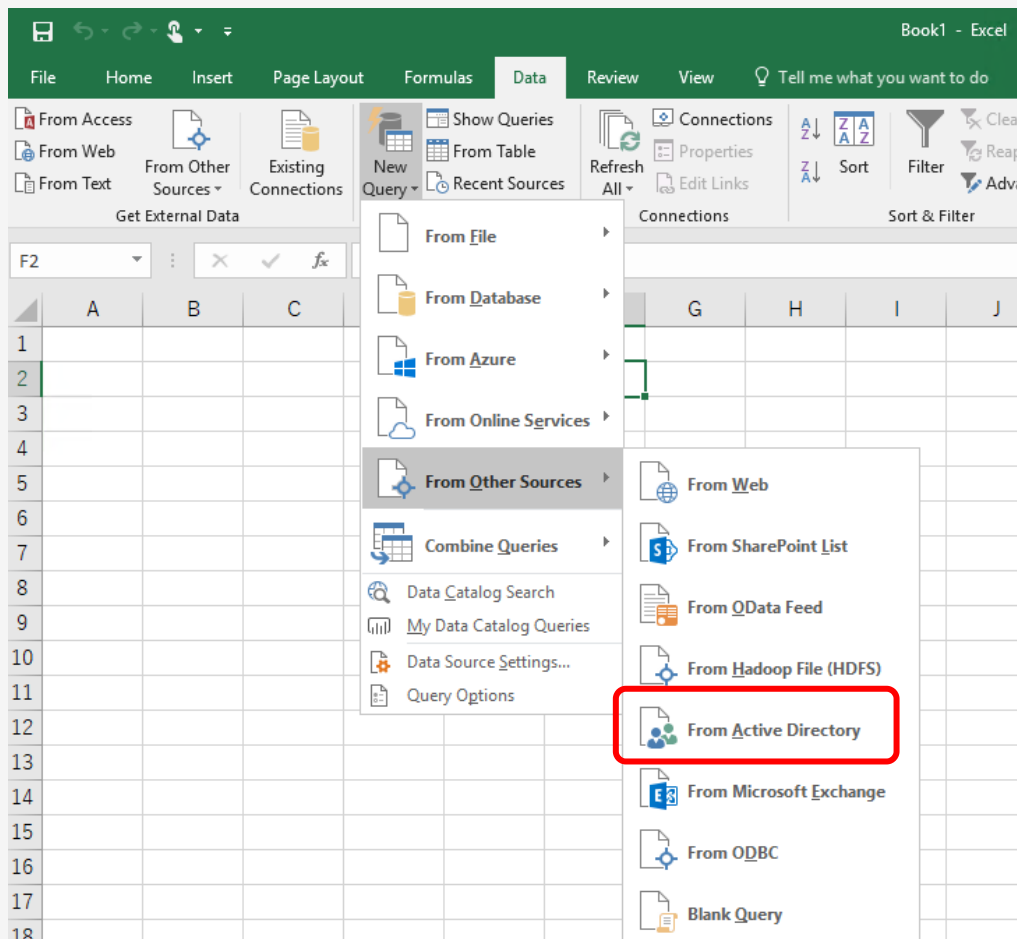


カスタムサーチとして自由なフィルタが作成可能

```
(&(&(&(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

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
10 techniques	14 techniques	20 techniques	14 techniques	43 techniques	17 techniques	32 techniques	9 techniques	17 techniques	17 techniques	9 techniques	14 techniques
Content Injection	Cloud Administration Command	Account Manipulation (1/6)	Abuse Elevation Control Mechanism	Abuse Elevation Control Mechanism (0/5)	Adversary-in-the-Middle (0/3)	Account Discovery (1/4)	Exploitation of Remote Services	Adversary-in-the-Middle (0/3)	Application Layer Protocol (0/4)	Automated Exfiltration (0/1)	Account Access Removal
Drive-by Compromise	Command and Scripting Interpreter (0/9)	BITS Jobs		Access Token Manipulation (1/5)	Brute Force (3/4)	Application Window Discovery	Internal Spearphishing	Archive Collected Data (0/3)	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction
Exploit Public-Facing Application	Container Administration Command	Boot or Logon Autostart Execution (0/14)	Create Process with Token	BITS Jobs	Credentials from Password Stores (1/6)	Browser Information Discovery	Lateral Tool Transfer	Audio Capture	Content Injection	Exfiltration Over Alternative Protocol (0/3)	Data Encrypted for Impact
External Remote Services	Deploy Container	Boot or Logon Initialization Scripts (1/5)	Make and Impersonate Token	Debugger Evasion	Exploitation for Credential Access	Cloud Infrastructure Discovery	Remote Service Session Hijacking (0/2)	Automated Collection	Data Encoding (0/2)		Data Manipulation (0/3)
Hardware Additions	Exploitation for Client Execution	Browser Extensions	Parent PID Spoofing	Deobfuscate/Decode Files or Information	Forced Authentication	Cloud Service Dashboard	Remote Services (0/8)	Browser Session Hijacking	Data Obfuscation (0/3)	Exfiltration Over C2 Channel	Defacement (0/2)
Phishing (0/4)	Inter-Process Communication	Account Manipulation (1/6)	Token Impersonation/Theft	Deploy Container	Forge Web Credentials (1/2)	Cloud Service Discovery	Replication Through Removable Media	Clipboard Data	Dynamic Resolution (0/3)	Endpoint Denial of Service (0/4)	Disk Wipe (0/2)
Replication Through Removable Media	Native API	Boot or Logon Autostart Execution (0/14)		Direct Volume Access	Input Capture (0/4)	Cloud Storage Object Discovery	Container and Resource Discovery	Data from Cloud Storage	Encrypted Channel (0/2)	Exfiltration Over Other Network Medium (0/1)	Endpoint Denial of Service (0/4)
Scheduled Task/Job (0/5)	Scheduled Task/Job (0/5)	Create Account (1/3)		Domain Policy Modification (2/2)	Modify Authentication Process (3/8)	Debugger Evasion	Device Driver Discovery	Data from Configuration Repository (0/2)	Fallback Channels	Exfiltration Over Physical Medium (0/1)	Financial Theft
Supply Chain Compromise (0/3)	Serverless Execution	Create or Modify System Process (0/4)		Execution Guardrails (0/1)	Multi-Factor Authentication Interception	Device Driver Discovery	Domain Trust Discovery	Data from Information Repositories (0/3)	Ingress Tool Transfer	Exfiltration Over Web Service (0/4)	Firmware Corruption
Trusted Relationship	Shared Modules	Event Triggered Execution (0/16)		Exploitation for Defense Evasion	Multi-Factor Authentication Request Generation	File and Directory Permissions Modification (1/2)	File and Directory Discovery	Use Alternate Authentication Material (2/4)	Multi-Stage Channels	Exfiltration Over Web Service (0/4)	Inhibit System Recovery
Valid Accounts (2/4)	Software Deployment Tools	External Remote Services		File and Directory Permissions Modification (1/2)	Multi-Factor Authentication Request Generation	Hide Artifacts (0/11)	Group Policy Discovery	Data from Local System	Non-Application Layer Protocol	Scheduled Transfer	Network Denial of Service (0/2)
	System Services (0/2)	Hijack Execution Flow (0/12)		Hijack Execution Flow (0/12)	Network Sniffing	Hijack Execution Flow (0/12)	Log Enumeration	Data from Network Shared Drive	Non-Standard Port	Transfer Data to Cloud Account	Resource Hijacking
	User Execution (0/3)	Implant Internal Image		Impair Defenses (0/11)	OS Credential Dumping (3/8)	Impair Defenses (0/11)	Network Service Discovery	Data from Removable Media	Protocol Tunneling		Service Stop
	Windows Management Instrumentation	Modify Authentication Process (3/8)		Indicator Removal (0/9)	Steal Application Access Token	Indicator Removal (0/9)	Network Sniffing	Data Staged (0/2)	Remote Access Software		System Shutdown/Reboot
		Office Application Startup (0/6)		Indirect Command Execution	Steal or Forge Authentication Certificates	Indirect Command Execution	Password Policy Discovery	Email Collection (0/3)	Traffic Signaling (0/2)		
		Power Settings		Masquerading (0/9)	Modify Authentication Process (3/8)	Masquerading (0/9)	Peripheral Device Discovery	Input Capture (0/4)	Web Service (0/3)		
		Pre-OS Boot (0/5)		Modify Authentication Process (3/8)	Steal or Forge Kerberos Tickets (4/4)	Modify Authentication Process (3/8)	Permission Groups Discovery (0/3)	Screen Capture			
		Scheduled Task/Job (0/5)		Modify Cloud Compute Infrastructure (0/5)		Modify Cloud Compute Infrastructure (0/5)	Process Discovery	Video Capture			
		Server Software Component (0/5)		Modify Registry		Modify Registry	Query Registry				
		Traffic Signaling		Modify System Image (0/2)		Modify System Image (0/2)	Remote System Discovery				
				Network Boundary		Network Boundary	Software Discovery (0/1)				

攻撃者目線

攻撃手法としてKerberoastingが注目されている。

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY



AMERICA'S CYBER DEFENSE AGENCY

Search

Topics ▾

Spotlight

Resources & Tools ▾

News & Events ▾

Careers ▾

About ▾

REPORT A CYBER ISSUE

Home / News & Events / Cybersecurity Advisories / Cybersecurity Advisory

SHARE:    

CYBERSECURITY ADVISORY

NSA and CISA Red and Blue Teams Share Top Ten Cybersecurity Misconfigurations

Release Date: October 05, 2023

Alert Code: AA23-278A

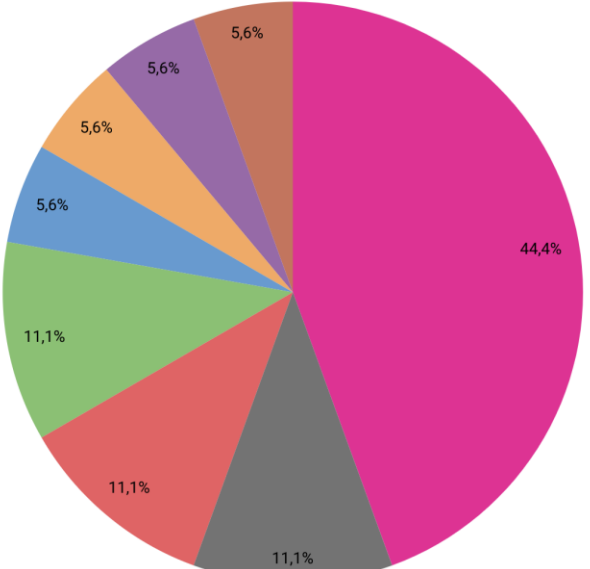
A plea for network defenders and software manufacturers to fix common problems.

EXECUTIVE SUMMARY

The National Security Agency (NSA) and Cybersecurity and Infrastructure Security Agency (CISA) are releasing this joint cybersecurity advisory (CSA) to highlight the most common cybersecurity misconfigurations in large organizations, and detail the tactics, techniques, and procedures (TTPs) actors use to exploit these misconfigurations.

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>



Misconfiguration	Percentage
LSASS Memory - T1003.001	44.4%
Kerberoasting - T1558.003	11.1%
Credentials from Web Browsers - T1555.003	11.1%
OS Credential Dumping - T1003	11.1%
Credentials from Password Stores - T1555	5.6%
Windows Credential Manager - T1555.004	5.6%
Security Account Manager - T1003.002	5.6%
Brute Force - T1110	5.6%

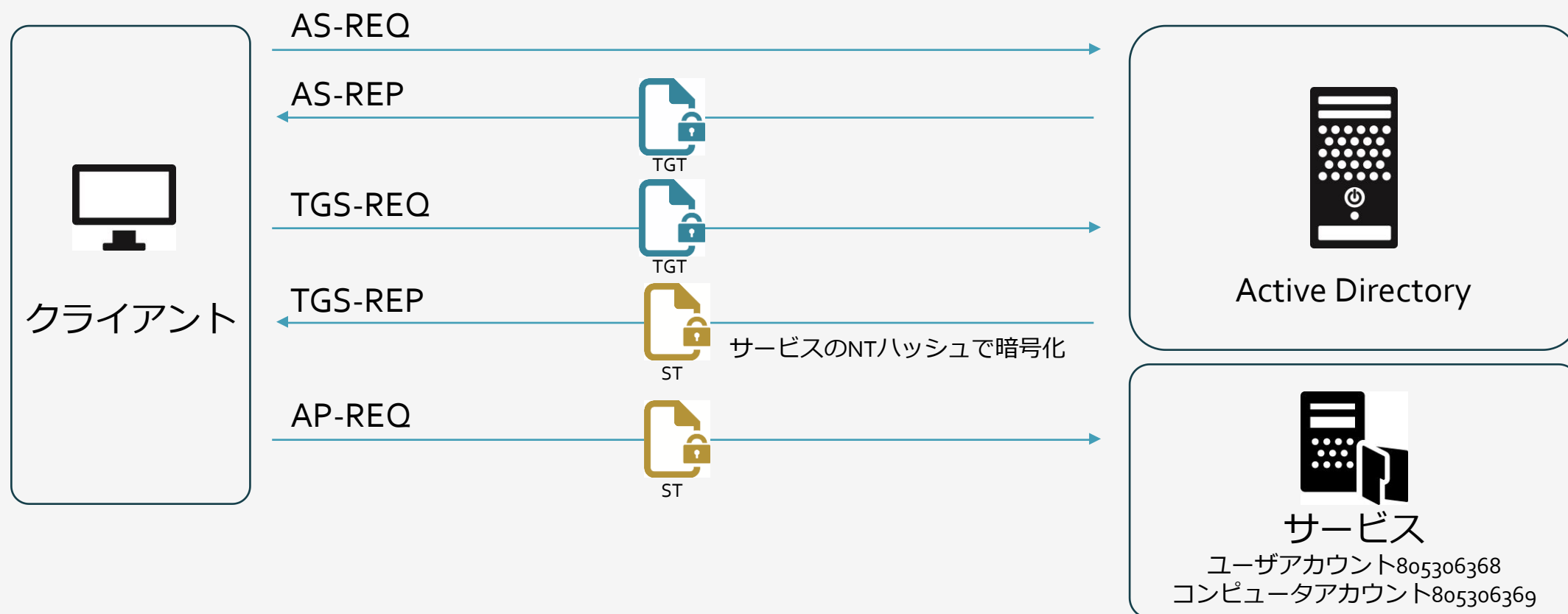
Credential Access

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
 - PingCastle
 - 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

ActiveDirectoryログ

Computer Management

File Action View Help

Computer Management (Local)

- System Tools
 - Task Scheduler
 - Event Viewer
 - Custom Views
 - Windows Logs
 - Applications and Services Logs
 - Active Directory Web Services
 - DFS Replication
 - Directory Service
 - DNS Server
 - Hardware Events
 - Internet Explorer
 - Key Management Service
 - Microsoft
 - OpenSSH
 - Windows PowerShell
 - Saved Logs
 - Subscriptions
 - Shared Folders
 - Performance
 - Device Manager
 - Storage
 - Windows Server Backup
 - Disk Management
 - Services and Applications

Level	Date and Time	Source	Event ID	Task Cat...
Information	2023/10/30 20:46:20	ActiveDi...	1138	LDAP Int...
Information	2023/10/30 20:46:20	ActiveDi...	1139	LDAP Int...
Information	2023/10/30 20:46:20	ActiveDi...	1644	Field En...
Information	2023/10/30 20:46:20	ActiveDi...	1138	LDAP Int...
Information	2023/10/30 20:46:20	ActiveDi...	1139	LDAP Int...
Information	2023/10/30 20:46:20	ActiveDi...	1644	Field En...
Information	2023/10/30 20:46:20	ActiveDi...	1138	LDAP Int...
Information	2023/10/30 20:46:20	ActiveDi...	1139	LDAP Int...

Event 1644, ActiveDirectory_DomainService

General Details

Internal event: A client issued a search operation with the following options.

Client: 192.168.11.100-49823

Starting node: DC=forest1,DC=net

Filter: (& (sAMAccountType=805306368) (servicePrincipalName=*) (! (sAMAccountName=krbtgt)) (! (userAccountControl&2)))

Search scope: subtree

Attribute selection:

Log Name: Directory Service

Source: ActiveDirectory_DomainServ

Event ID: 1644

Level: Information

User: forest1\user001

OpCode: Info

Logged: 2023/10/30 20:46:20

Task Category: Field Engineering

Keywords: Classic

Computer: F1DC1.forest1.net

LDAPMon

Computer Management

File Action View Help

Computer Management (Local)

- System Tools
 - Task Scheduler
 - Event Viewer
 - Custom Views
 - Windows Logs
 - Applications and Services Logs
 - Hardware Events
 - Internet Explorer
 - Key Management Service
 - LDAPMon
 - Operational
 - Microsoft
 - Microsoft Office Alerts
 - OpenSSH
 - Windows PowerShell
 - Subscriptions
 - Shared Folders
 - Shares
 - Sessions
 - Open Files
 - Local Users and Groups
 - Users
 - Groups

Level	Date and Time	Source	Event ID	Task C...
Information	1/2/2024 4:20:54 PM	LDAP...	1	None
Information	10/30/2023 8:46:21 PM	LDAP...	1	None
Information	10/30/2023 8:46:21 PM	LDAP...	1	None
Information	10/30/2023 8:46:21 PM	LDAP...	1	None
Information	10/30/2023 8:46:21 PM	LDAP...	1	None
Information	10/30/2023 8:46:21 PM	LDAP...	1	None
Information	10/30/2023 8:46:21 PM	LDAP...	1	None
Information	10/30/2023 8:46:21 PM	LDAP...	1	None
Information	10/30/2023 8:46:21 PM	LDAP...	1	None

Event 1, LDAPMon

General Details

LDAP Search

EventTime: 2023-10-31T03:46:21.916412900Z

ScopeOfSearch: 2

SearchFilter: (& (samAccountType=805306368) (servicePrincipalName=*) (!samAccountName=krbtgt) (! (UserAccountControl:1.2.840.113556.1.4.803:=2)))

DistinctiveName: DC=forest1,DC=net

AttributeList:

ProcessId: 672

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べきクエリやデコイ（罠）の有効性の検討を深める
-