

B2-5

アタックサーフェスのその先にあるもの

～リアルな攻撃、リアルな現状～

標的型メール開封後に起きていること

NTTフィールドテクノ (NTT西日本)

四方 直樹

自己紹介



西日本電信電話株式会社（NTT西日本）

四方 直樹 *SHIKATA Naoki*

- 2005年に新卒でNTT西日本に入社
- セキュリティエンジニア、クラウドのプロダクトマネージャや事業戦略立案、海外駐在、米国大学院において情報セキュリティ修士号の取得
- 2022/9よりオフensiveセキュリティ観点でセキュリティ対策を進める『**レッドチーム**』の立上げに従事

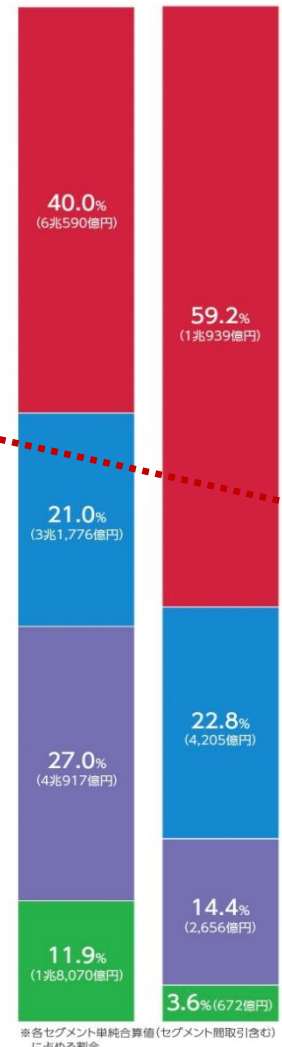
自社紹介



事業	内容と主な会社
総合ICT事業	<p>当事業は、携帯電話事業、国内電気通信事業における県間通信サービス、国際通信事業、ソリューション事業、システム開発事業及びそれに関連する事業を主な事業内容としています。</p>
地域通信事業	<p>当事業は、国内電気通信事業における県内通信サービスの提供及びそれに附帯する事業を主な事業内容としています。</p>
グローバル・ソリューション事業	<p>当事業は、システムインテグレーション、ネットワークシステム、クラウド、グローバルデータセンター及びそれに関連する事業を主な事業内容としています。</p>
その他 (不動産、エネルギー等)	<p>不動産事業、エネルギー事業等が含まれています。</p>

営業収益*
(2022年度)
13兆1,362億円

営業利益*
(2022年度)
1兆8,290億円



NTT西日本グループの自社防衛に
資するセキュリティオペレーションを担当

はじめに

**標的型メールは開封するな、は認識しているものの
実際に開封したのち、どのようにデータ搾取に繋がっているのか！？**

というテーマに対して、（ランサムウェアはともかく）あまり現実感が無くイメージが付きにくい方もおられるのでは、と思われます。

本日は、攻撃者が内部侵入後に何をするのか、について一部触れたいと思います。

本日のスコープ

ATT&CK Matrix for Enterprise

layout: side ▾ show sub-techniques hide sub-techniques

Reconnaissance 10 techniques	Resource Development 8 techniques	Initial Access 9 techniques	Execution 14 techniques	Persistence 19 techniques	Privilege Escalation 13 techniques	Defense Evasion 42 techniques	Credential Access 17 techniques	Discovery 31 techniques	Lateral Movement 9 techniques	Collection 17 techniques	Command and Control 16 techniques	Exfiltration 9 techniques
Active Scanning (3)	Acquire Access	Drive-by Compromise	Cloud Administration Command	Account Manipulation (5)	Abuse Elevation Control Mechanism (4)	Abuse Elevation Control Mechanism (4)	Adversary-in-the-Middle (3)	Account Discovery (4)	Exploitation of Remote Services	Adversary-in-the-Middle (3)	Application Layer Protocol (4)	Automated Exfiltration
Gather Victim Host Information (4)	Acquire Infrastructure (8)	Exploit Public-Facing Application	Command and Scripting Interpreter (9)	BITS Jobs	Access Token Manipulation (5)	Access Token Manipulation (5)	Brute Force (4)	Application Window Discovery	Internal Spearphishing	Archive Collected Data (3)	Communication Through Removable Media	Data Transfer S Limits
Gather Victim Identity Information (3)	Compromise Accounts (3)	External Remote Services	Container Administration Command	Boot or Logon Autostart Execution (14)	Boot or Logon Autostart Execution (14)	BITS Jobs	Credentials from Password Stores (5)	Browser Information Discovery	Lateral Tool Transfer	Audio Capture	Data Encoding (2)	Exfiltration Over Alternative Protocol (3)
Gather Victim Network Information (6)	Compromise Infrastructure (7)	Hardware Additions	Deploy Container	Boot or Logon Initialization Scripts (5)	Boot or Logon Initialization Scripts (5)	Build Image on Host	Exploitation for Credential Access	Cloud Infrastructure Discovery	Remote Service Session Hijacking (2)	Automated Collection	Data Obfuscation (3)	Exfiltration Over C2 Channel
Gather Victim Org Information (4)	Develop Capabilities (4)	Phishing (3)	Exploitation for Client Execution	Browser Extensions	Create or Modify System Process (4)	Debugger Evasion	Forced Authentication	Cloud Service Dashboard	Remote Services (7)	Browser Session Hijacking	Dynamic Resolution (3)	Exfiltration Over Network Medium (1)
Phishing for Information (3)	Establish Accounts (3)	Replication Through Removable Media	Inter-Process Communication (3)	Compromise Client Software Binary	Domain Policy Modification (2)	Deobfuscate/Decode Files or Information	Forge Web Credentials (2)	Cloud Service Discovery	Replication Through Removable Media	Clipboard Data	Encrypted Channel (2)	Exfiltration Over Physical Medium (1)
Search Closed Sources (2)	Obtain Capabilities (6)	Supply Chain Compromise (3)	Native API	Create Account (3)	Domain Policy Modification (2)	Deploy Container	Input Capture (4)	Cloud Storage Object Discovery	Software Deployment Tools	Data from Cloud Storage	Fallback Channels	Exfiltration Over Web Service (3)
Search Open Technical Databases (5)	Stage Capabilities (6)	Trusted Relationship	Scheduled Task/Job (5)	Create or Modify System Process (4)	Escape to Host	Direct Volume Access	Modify Authentication Process (8)	Container and Resource Discovery	Taint Shared Content	Data from Configuration Repository (2)	Ingress Tool Transfer	Scheduled Transfer
Search Open Websites/Domains (3)	Valid Accounts (4)	Valid Accounts (4)	Serverless Execution	Event Triggered Execution (16)	Event Triggered Execution (16)	Domain Policy Modification (2)	Multi-Factor Authentication Interception	Debugger Evasion	Use Alternate Authentication Material (4)	Data from Information Repositories (3)	Multi-Stage Channels	Transfer Data to Cloud Account
Search Victim-Owned Websites			Shared Modules	Exploitation for Privilege Escalation	Exploitation for Privilege Escalation	Execution Guardrails (1)	Multi-Factor Authentication Request Generation	Device Driver Discovery		Data from Local System	Non-Application Layer Protocol	
			Software Deployment Tools	External Remote Services	Hijack Execution Flow (12)	File and Directory Permissions Modification (2)	Network Sniffing	Domain Trust Discovery		Data from Network Shared Drive	Non-Standard Port	
			System Services (2)	Hijack Execution Flow (12)	Hijack Execution Flow (12)	Hide Artifacts (10)		File and Directory Discovery		Data from Removable Media	Protocol Tunneling	
			User Execution (3)	Process Injection (12)	Process Injection (12)	Hijack Execution Flow (12)		Group Policy Discovery				
			Windows	Remote Internet	Process Injection (12)	Impair Defenses (10)		Network Service Discovery				

共通認識

- 脆弱性をつく/侵入後に内部探索するための情報は世に溢れている -

EXPLOIT DATABASE

Microsoft Windows 11 - 'apds.dll' DLL hijacking (Forced)

EDB-ID: 51733	CVE: N/A	Author: MOEIN SHAHABI	Type: LOCAL	Platform: WINDOWS	Date: 2023-10-09
-------------------------	--------------------	---------------------------------	-----------------------	-----------------------------	----------------------------

EDB Verified: X **Exploit:** 1 / {} **Vulnerable App:**

Instructions:

1. Compile dll
2. Copy newly compiled dll "apds.dll" in the "C:\Windows\" directory
3. Launch cmd and Execute the following command to test HelpPane object "[System.Activator]::CreateInstance([Type]::GetTypeFromCLSID('{8CEC58AE-07A1-11D9-B15E-000D56BFE6EE}'))"
4. Boom DLL Hijacked!

```
#-----  
# Title: Microsoft  
# Date: 2023-09-01  
# Author: Moein Sh  
# Vendor: https://  
# Version: Windows  
# Tested on: Wind  
#-----  
-----Code_Poc-----  
#pragma once  
#include <Windows.h>  
  
// Function executed when the thread starts  
extern "C" __declspec(dllexport)  
DWORD WINAPI MessageBoxThread(LPVOID lpParam) {  
    MessageBox(NULL, L"DLL Hijacked!", L"DLL Hijacked!", NULL);  
    return 0;  
}  
  
PBYTE AllocateUsableMemory(PBYTE baseAddress, DWORD size, DWORD protection = PAGE_READWRITE) {  
#ifdef _WIN64  
    PIMAGE_DOS_HEADER dosHeader = (PIMAGE_DOS_HEADER)baseAddress;  
    PIMAGE_NT_HEADERS ntHeaders = (PIMAGE_NT_HEADERS)((PBYTE)dosHeader + dosHeader->e_lfanew);  
    PIMAGE_OPTIONAL_HEADER optionalHeader = &ntHeaders->OptionalHeader;  
  
    // Create some breathing room  
    baseAddress = baseAddress + optionalHeader->SizeOfImage;  
  
    for (PBYTE offset = baseAddress; offset < baseAddress + MAXDWORD; offset += 1024 * 8) {  
        PBYTE usable = (PBYTE)VirtualAlloc(  
            offset,  
            size,  
            MEM_RESERVE | MEM_COMMIT,  
            protection);  
    }  
}
```

infosecn1nja / AD-Attack-Defense Public

<> Code Issues Pull requests Actions Projects Security Insights

master 1 branch 0 tags Go to file Code

infosecn1nja Added BackupOperatorToolkit & Azure hacking resources a22795a on Mar 4 120 commits

README.md Added BackupOperatorToolkit & Azure hacking resources 8 months ago

Active Directory Kill Chain Attack & Defense

Summary

This document was designed to be a useful, informational asset for those looking to understand the specific tactics, techniques, and procedures (TTPs) attackers are leveraging to compromise active directory and guidance to mitigation, detection, and prevention. And understand Active Directory Kill Chain Attack and Modern Post Exploitation Adversary Tradecraft Activity.

<https://www.exploit-db.com/exploits/51733>

<https://github.com/infosecn1nja/AD-Attack-Defense#defense-evasion>

思い浮かぶ疑問

様々な脆弱性に対するexploitコードやハッキングツールが公開されているのは知ってるが、、、

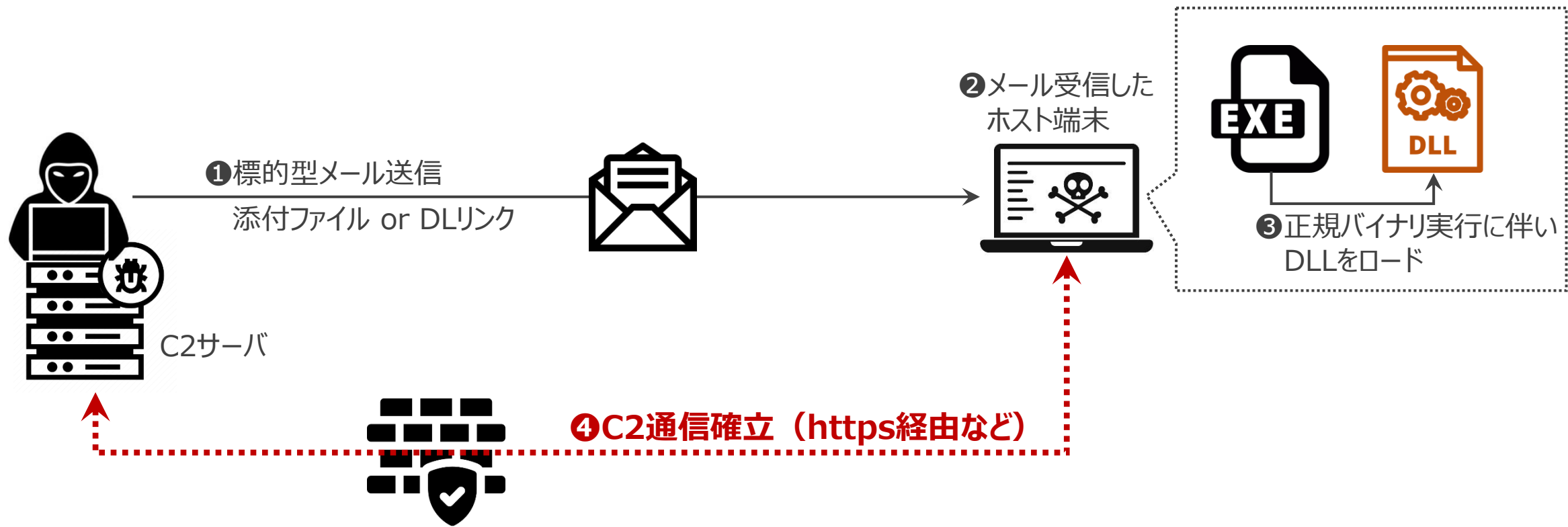
“エンドポイント端末にEPP/EDRなどが導入されている環境でもホントに攻撃は成立するんだっけ？”

攻撃は成立します。

ただ、成功させるためには重要なポイント^{【※】}があります

【※】 攻撃者にとっての攻撃侵害コスト

C2サーバとの通信確立 #C2 Establishment

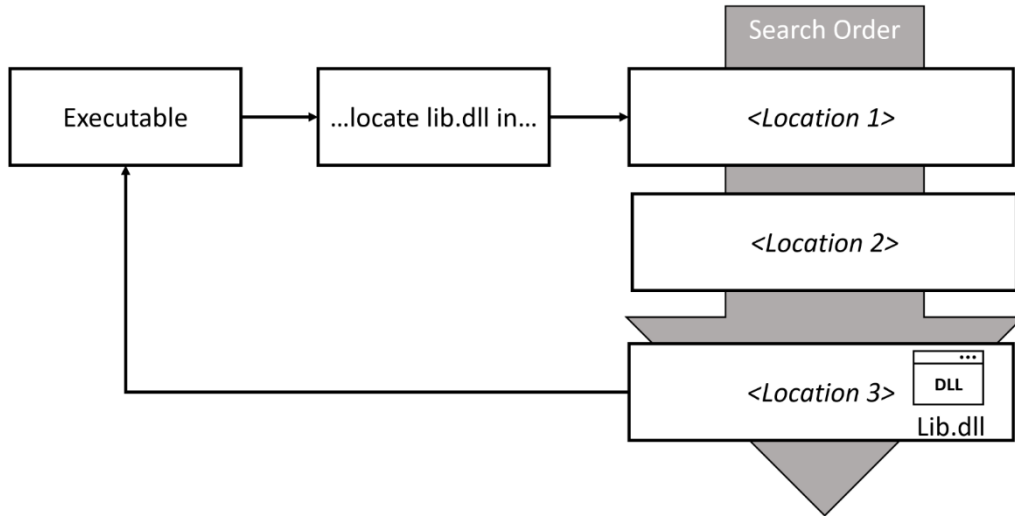


具体的な手法

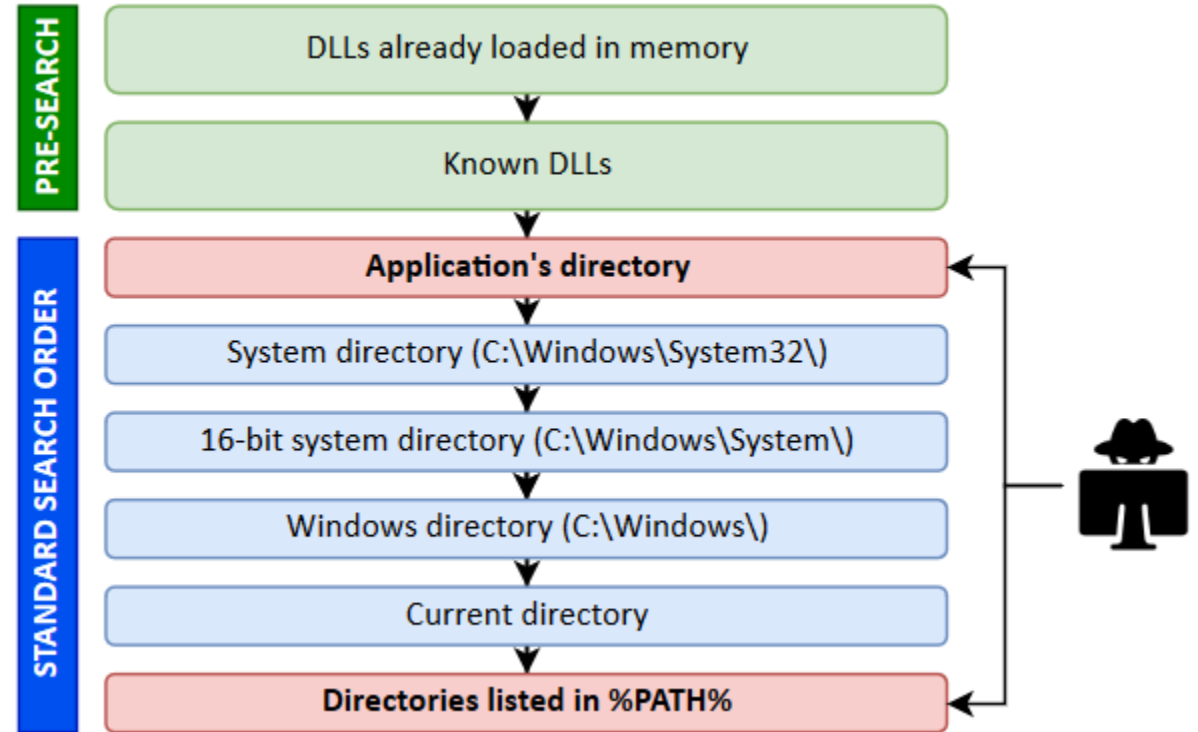
- 正規実行ファイルで悪性DLLをロード (悪性DLLにC2サーバのbeacon埋め込み)
- 実行ファイル群の偽装 (ショートカット/アイコンの偽装、隠しファイル等)

(参考) DLLサイドローディング #DLL Side-Loading

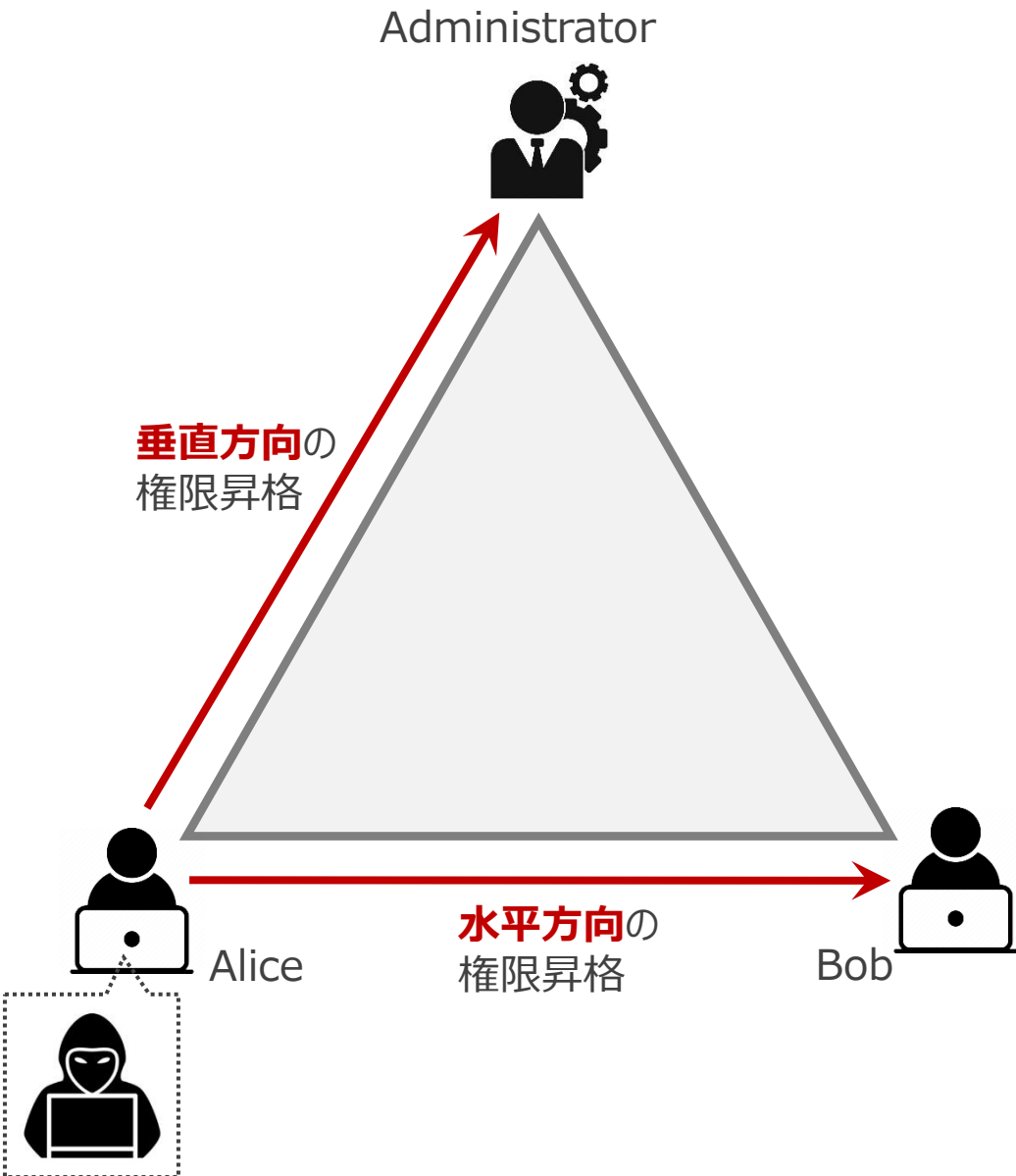
Mechanism



Search Order



権限昇格 #Privilege Escalation



水平方向

- ファイルサーバ等に保管されているCredential情報利用
→一般権限であっても各種社内資産にアクセス可能
になることで、社内システムの権限不備を活用
- 情報の搾取
→パケットキャプチャなど

垂直方向

EPP/EDRが入っていると有名なハックツール利用はNGなため
Sticky Keys (sethc.exe等) の利用は難しい

- UACバイパス
→UACバイパス後は、C2フレームワーク内蔵コマンド利用
- プロセスインジェクション/ハイジャッキング
→DLLインジェクション
- 内製アプリケーション
→権限設定の不備が散見される

検知回避 #Defense Evasion

MITRE | ATT&CK®

Matrices ▾ Tactics ▾ Techniques ▾ Data Sources Mitigations ▾ Groups Software Campaigns Resources ▾ Blog ↗ Contribute Search 🔍

ATT&CK Matrix for Enterprise

layout: side ▾ show sub-techniques hide sub-techniques

Reconnaissance 10 techniques	Resource Development 8 techniques	Initial Access 9 techniques	Execution 14 techniques	Persistence 19 techniques	Privilege Escalation 13 techniques	Defense Evasion 42 techniques	Credential Access 17 techniques	Discovery 31 techniques	Lateral Movement 9 techniques	Collection 17 techniques	Command and Control 16 techniques	Exfiltration 9 techniques
Active Scanning (3) Gather Victim Host Information (4) Gather Victim Identity Information (3) Gather Victim Network Information (6) Gather Victim Org Information (4) Phishing for Information (3) Search Closed Sources (2) Search Open Technical Databases (5) Search Open Websites/Domains (3) Search Victim-Owned Websites	Acquire Access Acquire Infrastructure (8) Compromise Accounts (3) Compromise Infrastructure (7) Develop Capabilities (4) Establish Accounts (3) Obtain Capabilities (6) Stage Capabilities (6)	Drive-by Compromise Exploit Public-Facing Application External Remote Services Hardware Additions Phishing (3) Replication Through Removable Media Supply Chain Compromise (3) Trusted Relationship Valid Accounts (4)	Cloud Administration Command Command and Scripting Interpreter (9) Container Administration Command Deploy Container Exploitation for Client Execution Inter-Process Communication (3) Native API Scheduled Task/Job (5) Serverless Execution Shared Modules Software Deployment Tools System Services (2) User Execution (3)	Account Manipulation (5) BITS Jobs Boot or Logon Autostart Execution (14) Boot or Logon Initialization Scripts (5) Browser Extensions Compromise Client Software Binary Create Account (3) Create or Modify System Process (4) Event Triggered Execution (16) External Remote Services Hijack Execution Flow (12)	Abuse Elevation Control Mechanism (4) Access Token Manipulation (5) BITS Jobs Build Image on Host Debugger Evasion Deobfuscate/Decode Files or Information Deploy Container Direct Volume Access Domain Policy Modification (2) Execution Guardrails (1) Exploitation for Defense Evasion File and Directory Permissions Modification (2) Hide Artifacts (10) Hijack Execution Flow (12) Impair Defenses (10)	Abuse Elevation Control Mechanism (4) Access Token Manipulation (5) BITS Jobs Build Image on Host Debugger Evasion Deobfuscate/Decode Files or Information Deploy Container Direct Volume Access Domain Policy Modification (2) Execution Guardrails (1) Exploitation for Defense Evasion File and Directory Permissions Modification (2) Hide Artifacts (10) Hijack Execution Flow (12) Impair Defenses (10)	Adversary-in-the-Middle (3) Brute Force (4) Credentials from Password Stores (5) Exploitation for Credential Access Forced Authentication Forge Web Credentials (2) Input Capture (4) Modify Authentication Process (8) Multi-Factor Authentication Interception Multi-Factor Authentication Request Generation Network Sniffing	Account Discovery (4) Exploitation of ... Adversary-in-... Application Automate...				

具体的な手法

- 難読化
→悪性コードの難読化/暗号化、packerの利用
- 正規ファイル利用
→OSにBuilt-inされたバイナリを用いて、悪性スクリプトを呼び出す
- 通知の妨害

<https://attack.mitre.org/>

さいごに

先述の侵害後も、“水平展開”、“情報搾取”などで様々な手法を現実の環境でも適用するが、それら含め、攻撃を防ぐためには（攻撃者にとっての）攻撃侵害コストを高めることが大切

Thank you

