



攻撃者視点で学ぶ サイバー攻撃の対策ポイント



CYBER COMMAND



横濱 悠平(ヨコハマ ユウヘイ)

プログラマー

- web、モバイルアプリやセキュリティツールの開発
- python, rust, php, java, ruby, nextjs
- 多くのプログラマーを育成

セキュリティエンジニア

- 脆弱性診断
- SOCインフラ構築
- セキュリティ人材育成の講師
- 認定ホワイトハッカー(CEH)

“ 攻撃者視点で学ぶ、サイバー攻撃の対策ポイント ”

なぜ、攻撃者視点??

- 実際の攻撃シナリオ
- 守り方の精度
- プロファイリング

情報漏洩やランサムウェアなど様々なサイバー攻撃が取り上げられていますが、このテーマでは攻撃者視点に立って実際に使われているシナリオやパターンを説明しながら守る側の視点を養います。

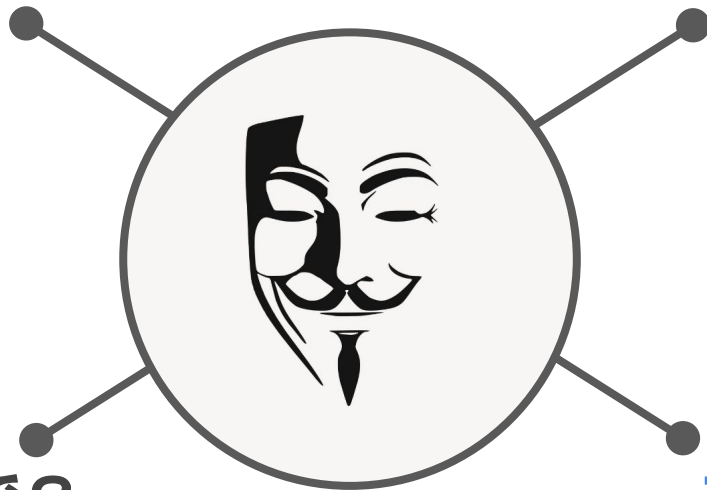
“

プロファイリング

”

動機は？

リソースは
どれくらい？



どのぐらいの時間で？

プロ意識は高い？

“

プロファイリング

”

サイバー攻撃者

```
graph TD; A[サイバー攻撃者] --> B[外部犯]; A --> C[内部犯]; B --> D[組織的な攻撃者]; B --> E[ハッカー]; B --> F[素人]; D --> D1[・テロリスト]; D --> D2[・ハクティビス]; D --> D3[・国家]; D --> D4[・犯罪集団]; E --> E1[・グレー]; E --> E2[・ブラック]; F --> F1[・グリーン]; F --> F2[・ブルー]; C --> C1[・不満を抱えた従業員]; C --> C2[・金銭的動機(窃盗)]; C --> C3[・故意ではない犯行];
```

外部犯

組織的な攻撃者

- ・テロリスト
- ・ハクティビス
- ・国家
- ・犯罪集団

ハッカー

- ・グレー
- ・ブラック

素人

- ・グリーン
- ・ブルー

内部犯

- ・不満を抱えた従業員
- ・金銭的動機(窃盗)
- ・故意ではない犯行

“

APT(Advanced Persistent Threat)

”

偵察

組織について必要な情報を集める

初期侵害

脆弱性を利用して組織への侵入路を得る

権限昇格

管理者権限やWindowsの管理者アカウントを得る

水平展開

ネットワークのいたるところに広がって他のシステムへのアクセスを獲得する

任務遂行

目的を達成し、悪意ある行動が行われる

拠点確立

システムへのアクセスを提供するためのマルウェアをインストールする

内部偵察

次のフェーズのための内部情報を収集する

存在維持

被害者の支配を維持し続ける

“

MITRE

”

MITRE | ATT&CK®

Matrices ▾

Tactics ▾

Techniques ▾

Defenses ▾

CTI ▾

Resources ▾

Benefactors

Blog ↗

Search Q

ATT&CK Matrix for Enterprise

layout: side ▾

show sub-techniques

hide sub-techniques

Reconnaissance 10 techniques	Resource Development 8 techniques	Initial Access 11 techniques	Execution 16 techniques	Persistence 23 techniques	Privilege Escalation 14 techniques	Defense Evasion 45 techniques	Credential Access 17 techniques	Discovery 33 techniques	Lateral Movement 9 techniques	Collection 17 techniques	Command and Control 18 techniques	Exfiltration 9 techniques	Impact 15 techniques
Active Scanning (3)	Acquire Access	Content Injection	Cloud Administration Command	Account Manipulation (7)	Abuse Elevation Control Mechanism (6)	Abuse Elevation Control Mechanism (6)	Adversary-in-the-Middle (4)	Account Discovery (4)	Exploitation of Remote Services	Adversary-in-the-Middle (4)	Application Layer Protocol (5)	Automated Exfiltration (1)	Account Access Removal
Gather Victim Host Information (4)	Acquire Infrastructure (6)	Drive-by Compromise	Command and Scripting Interpreter (12)	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 Size Limits	Data Destruction (1)
Gather Victim Identity Information (3)	Compromise Accounts (3)	Exploit Public-Facing Application	Container Administration Command	Boot or Logon Autostart Execution (14)	Account Manipulation (7)	BITS Jobs	Credentials from Password Stores (6)	Browser Information Discovery	Lateral Tool Transfer	Audio Capture	Content Injection	Exfiltration Over Alternative Protocol (3)	Data Encrypted for Impact
Gather Victim Network Information (6)	Compromise Infrastructure (6)	External Remote Services	Deploy Container	Boot or Logon Initialization Scripts (5)	Boot or Logon Autostart Execution (14)	Build Image on Host	Exploitation for Credential Access	Cloud Infrastructure Discovery	Remote Service Session Hijacking (2)	Automated Collection	Data Encoding (2)	Exfiltration Over C2 Channel	Data Manipulation (3)
Gather Victim Org Information (4)	Develop Capabilities (4)	Hardware Additions	ESXi Administration Command	Cloud Application Integration	Boot or Logon Initialization Scripts (5)	Debugger Evasion	Forced Authentication	Cloud Service Dashboard	Remote Services (8)	Browser Session Hijacking	Data Obfuscation (3)	Exfiltration Over Other Network Medium (1)	Defacement (2)
Phishing for Information (4)	Establish Accounts (3)	Phishing (4)	Exploitation for Client Execution	Compromise Host Software Binary	Create or Modify System Process (6)	Deobfuscate/Decode Files or Information	Forge Web Credentials (2)	Cloud Service Discovery	Replication Through Removable	Clipboard Data	Data from Cloud Storage	Exfiltration	Disk Wipe (2)
Search Closed Sources (2)	Obtain Capabilities (7)	Replication Through				Deploy Container	Input Capture (4)	Cloud Storage Object Discovery					Email Bombing
	ISane					Direct Volume Access		Container and					Endpoint Denial of Service (4)
						Domain or Tenant Policy Modification (4)							

[APTでざっくり版]

ステップ毎の

 攻撃者 vs  防御者
の戦い 

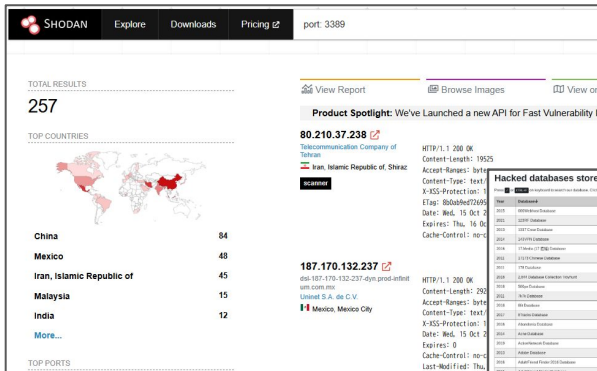
“

偵察 Recon

”

攻撃側

防御側

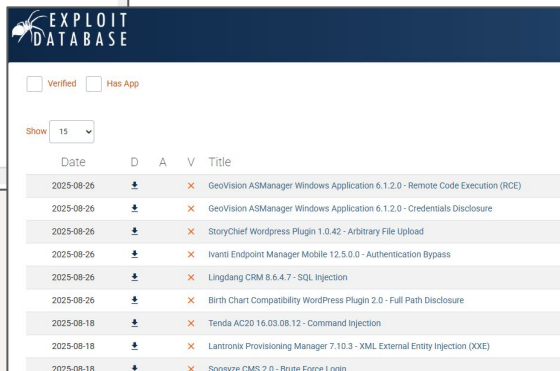


Hacked databases store

初期侵害 & 拠点確立 Initial Access

“

防衛側



- 教育、標的型攻撃訓練(定期演習)などの人間的な対策。メールゲート(URL/添付のサンドボックス検査などのシステムの対策。
- 使用しているクラウドサービスの管理。SGWやCASB等仕組みで。



定期的な診断サービスを利用

“

権限昇格 Privilege Escalation

”

攻撃側

防御側



```

Hostname: WINDOWS2.lab.local / -
##### mimikatz 2.8.alpha (x64) release "Kiwi en C" (May 23 2015) :25:0
## ~ ##
## ^ ## /* * *
## \ ## Benjamin DELPY "gentilkiwi" ( benjamin@gentilkiwi.com )
## v ## http://blog.gentilkiwi.com/mimikatz (os, eo)
##### with 15 modules * * *

mimikatz(powershell) # sekurlsa:logonpasswords

Authentication Id : 0 : 787553 (00000000:00000000)
Session : Interactive from 0
Name : justin
n : LAB
Server : LABDC
Time : 7/29/2015 10:11:04 AM
S-1-5-21-1099725566-223127814-2387084846-1189

msv :
[00000003] Primary
* Username : justin
* Domain : LAB
* NTLM : 786f30085fa9cd3f9d9888a57138d40
* SHA1 : 8e4ff45cbf381a543ba0985c268392c6af5d95d9
[00010000] CredentialKeys
* NTLM : 786f30085fa9cd3f9d9888a57138d40
* SHA1 : 8e4ff45cbf381a543ba0985c268392c6af5d95d9
tpkg :
wdigest :
* Username : justin
* Domain : LAB
* Password : !J12134567890
  
```

GTFOBins

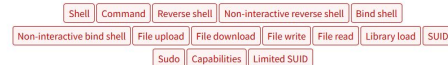
GTFOBins is a curated list of Unix binaries that can be used to bypass local security restrictions in misconfigured systems.

The project collects legitimate functions of Unix binaries that can be abused to get the *nix break out restricted shells, escalate or maintain elevated privileges, transfer files, spawn bind and reverse shells, and facilitate the other post-exploitation tasks.

It is important to note that this is **not** a list of exploits, and the programs listed here are not vulnerable per se, rather, GTFOBins is a compendium about how to live off the land when you only have certain binaries available.

GTFOBins is a **collaborative** project created by **Emilio Pinna** and **Andrea Cardaci** where everyone can contribute with additional binaries and techniques.

If you are looking for Windows binaries you should visit [LOLBAS](#).



- 資格情報の防護。パスワードの複雑化。使いまわし禁止。短い有効期間。
- 最小権限化。サービス/アカウントに最小権限を適用。



EDRなどを使用した認証挙動
の監視と分離 — ログ監視

“

内部偵察&水平展開

”

攻撃側**防御側**

RPC サービス

共有ファイル

Powershell

パーミッション



SMB サービス

脆弱性



- ネットワーク分割（マイクロセグメンテーション）。
- 管理プロトコルの制限（RDP/SMBの利用制御・踏み台制限）

**EDRで水平展開の挙動検出**

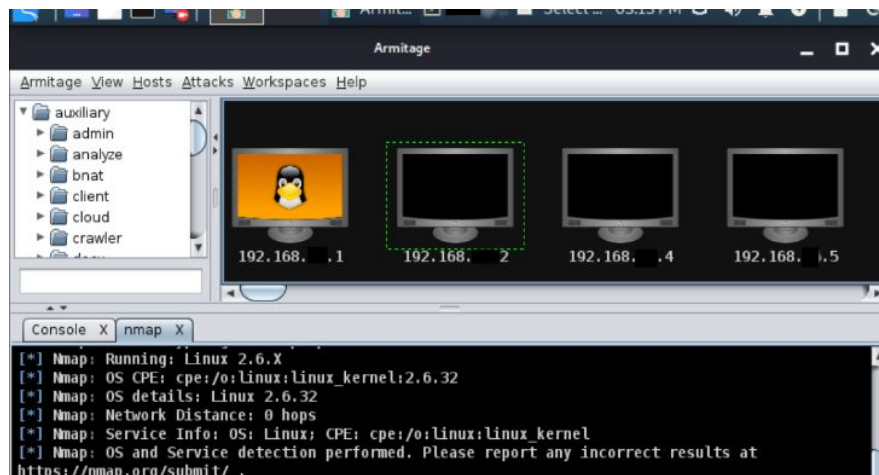
“

永続化

”

攻撃側

防御側



- システムの構成変更の監視とアラート。解放ポート、常駐プロセス、デーモン、ユーザー等



EDRでシステムの構成変更の
検出

“

目標達成

”

攻撃側

防御側



- 重要データの把握と不正持ち出しのブロック&アラート。DLP。
- 通信の監視と異常検知。大量の転送や不審なエンドポイントへの接続を検知。
- 暗号化バックアップとオフライン保管。



資産とリスクの棚卸とバックアップ。

“

チームで守る

”

防御側

- SOC (Security Operation Center)
- 専門の外部サービスに任せる
- 何を守るべきか？の大切な資産の棚卸から始める
- まずは一番大切なものから小さく始めていく
- 継続的な社員教育と訓練