\Orchestrating a brighter world NEC

Hardening Designers Conference 2023
「濃厚なサイバーセキュリティ最前線:攻撃手法の解析とAnsibleによる堅牢化の自動化」

MITRE ATT&CKから見る攻撃のトレンド

2023年5月20日

NEC　サイバーセキュリティ戦略統括部　セキュリティ技術センター
サイバーインテリジェンスグループ

© NEC Corporation 2023

\Orchestrating a brighter world

NECは、安全・安心・公平・効率という社会価値を創造し、
誰もが人間性を十分に発揮できる持続可能な社会の実現を目指します。

目次

1. MITRE ATT&CKのおさらい
2. MITRE ATT&CKの更新点
3. 新規追加テクニック
4. 追加テクニックからトレンドを追う
5. 抑えておきたい補足情報
6. まとめ

MITRE ATT&CKのおさらい

MITRE ATT&CKのおさらい

サイバー攻撃の手口を体系化した知識ベースで、米国の政府系非営利団体であるMITREが開発・維持

- **A**dversarial **T**actics, **T**echniques, **and** **C**ommon **K**nowledge
  ⇒ **敵対的な戦術、技術および共通知識**
  - MITRE社が提供する脅威情報のナレッジベース/フレームワーク
    - 実際に観測されたサイバー攻撃に関する情報を基に作成
    - 継続的にアップデートされている（年2回ほど）

      2022年10月にv12、2023年4月にv13がリリース

体系的な攻撃手口・攻撃者・マルウェアの知識を共有

- 攻撃手法に名前とIDを与えることで共通言語化し、緩和策や検出方法を記載
  - 攻撃シナリオの理解や整理、レッドチーム演習などでも活用

MITRE ATT&CK

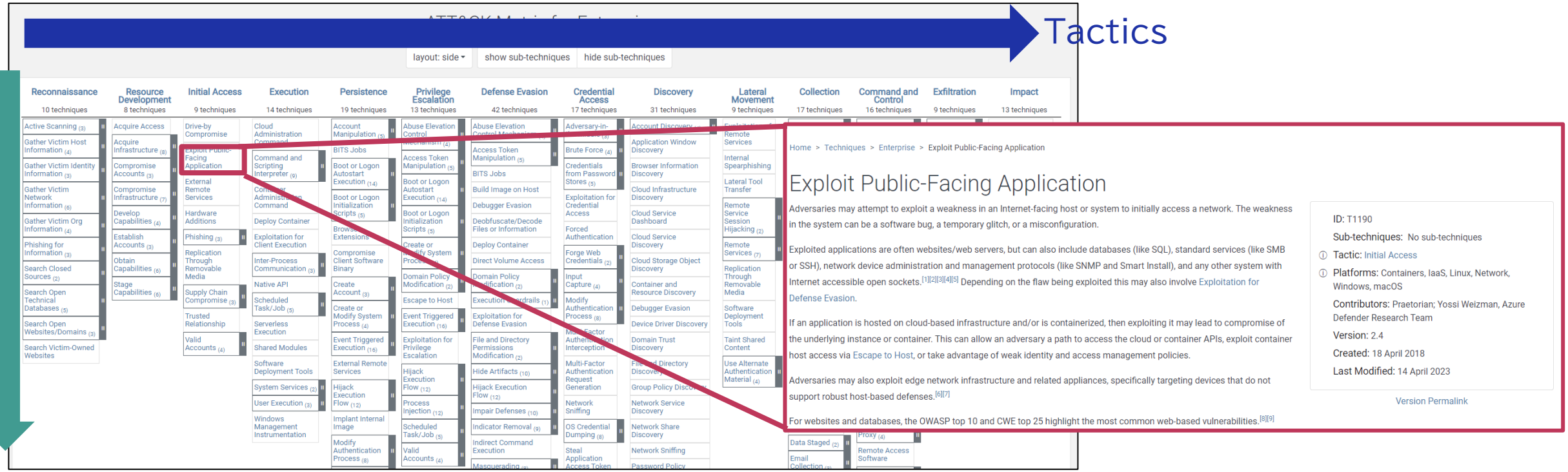
脅威情報のフレームワーク/ナレッジベース

© NEC Corporation 2023

MITRE ATT&CKのおさらい

目的となる戦術をキルチェーンで並べ、戦術毎にテクニックを整理

- 戦術毎にテクニックがまとまっており、マトリックス形式で整理
  - より細かい手法はサブテクニックとして一つのテクニックに包括



© NEC Corporation 2023

MITRE ATT&CKのおさらい

セキュリティベンダのみならず公的な機関も整理に使用、日本においてもインシデント報告書などで活用されている

- 攻撃シナリオ整理のスタンダードになっている

MITRE ATT&CK®

This advisory has been compiled with respect to the MITRE ATT&CK® framework, a globally accessible knowledge base of adversary tactics and techniques based on real-world observations.

For detailed TTPs, see the Malware Analysis Report .

Tactic	ID	Technique	Procedure
Initial Access	T1190	Exploit Public-facing Application.	APT28 exploited default/well-known community strings in SNMP as outlined in CVE-2017-6742 (Cisco Bug ID: CSCve54313).
Initial Access	T1078.001	Valid Accounts: Default Accounts.	Actors accessed victim routers by using default community strings such as “public.”
Reconnaissance	T1590	Gather Victim Network Information	Access was gained to perform reconnaissance on victim devices. Further detail of how this was achieved in available in the MITRE ATT&CK section of the Jaguar Tooth MAR.

5.2.2. 重大インシデント発生全体図

以下に今回発生した重大インシデントの全体像をまとめる。脆弱性は CWE、攻撃手法は MITRE ATT&CK より選択した。

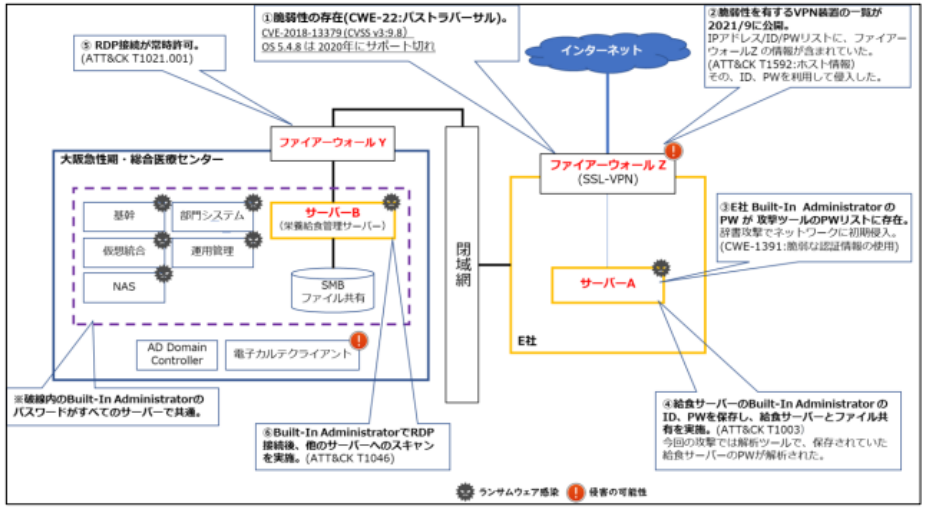


図 6 重大インシデント全体像

項番	内容
① CWE-22:パストラバーサル	ファイル名指定の実装に問題があり、攻撃者に任意のファイルを指定され、ウェブアプリケーションが意図しない処理を行ってしまう脆弱性。
② MITRE ATT&CK T1592:被害者ホスト情報の収集	攻撃者は被害者のホストに関する情報を収集する場合がある。ホストに関する情報は、オンライン等を介して攻撃者に公開される可能性がある。
③ CWE-1391:脆弱な認証情報の使用	攻撃者が計算、導出、再利用、または推測できる脆弱な資格情報の使用。
④ MITRE ATT&CK T1003:OS 資格情報のダンプ	ツールを使用した OS に保存されている資格情報の解析。
⑤ MITRE ATT&CK T1021.001:RDP	有効なアカウントを使用し、RDP で遠隔地のコンピューターにログオン。
⑥ MITRE ATT&CK T1046:ネットワークサービスの探索	ネットワーク上で公開されているサービスをツールでスキャンし、攻撃に利用する。

© NEC Corporation 2023

MITRE ATT&CKの更新点

v12で追加された新しいデータ構造

「キャンペーン」コレクションが追加

- ◆ 攻撃者グループが使用するテクニックを、時間軸に着目してキャンペーン単位で整理
  - ■ 攻撃者グループのテクニック欄は、テクニックの使用が確認されるたびに追加されていた
  - ■ しかし、攻撃者は常に同じテクニックを使用している訳ではなく、時間の経過とともに変化していく
  - ■ そこで、特定の期間に共通のターゲットと目的で実行された攻撃を「キャンペーン」として区別し、別のコレクションとして改めて整理

⇒ **攻撃者の使用するテクニックの変遷を追跡できるように構成予定**

既存の攻撃者グループページ

攻撃者の累積データ集に

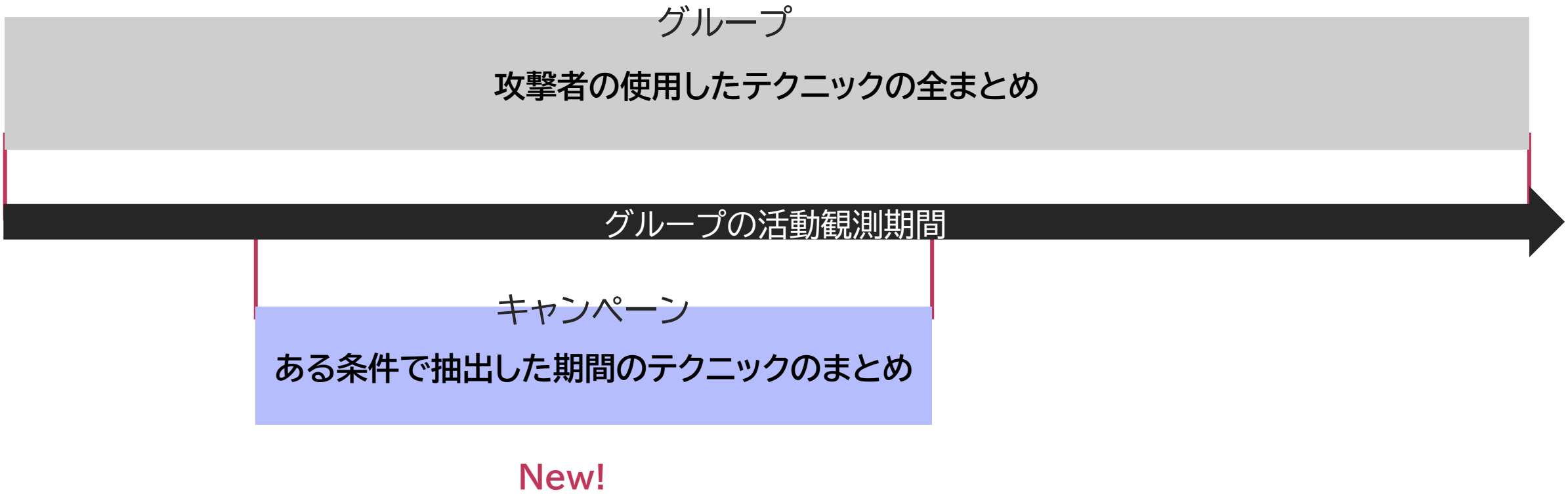
キャンペーンページ

帰属が不明確な攻撃や、SolarWindsのような攻撃も取り扱えるように

© NEC Corporation 2023

v12で追加された新しいデータ構造

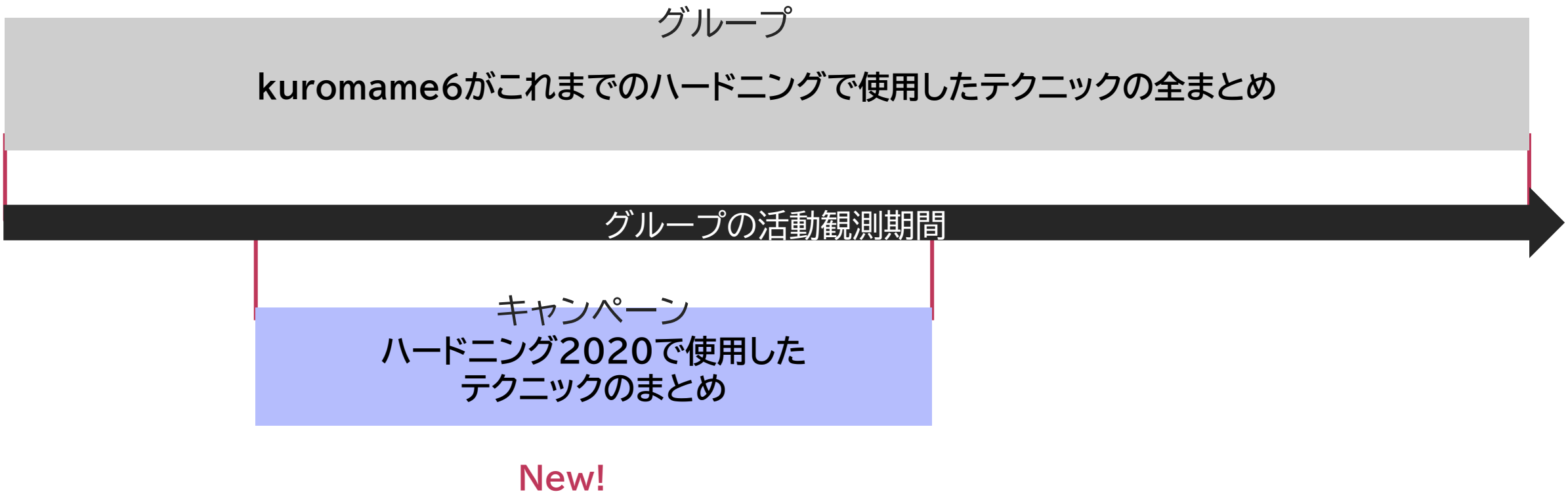
主体(グループ)にテクニックを紐つけるだけでなく、
条件を付与することでより実世界での形態に近づく



© NEC Corporation 2023

v12で追加された新しいデータ構造

キャンペーンのイメージ



© NEC Corporation 2023

v12で追加された新しいデータ構造

「キャンペーン」の数はまだまだ少ないものの、より帰属に有用なデータ構造になることを期待

- より特定の期間に焦点を当てているため、帰属に使いやすい
  - 現在22個

Home > Campaigns > SolarWinds Compromise

SolarWinds Compromise

The SolarWinds Compromise was a sophisticated supply chain cyber operation conducted by APT29 that was discovered in mid-December 2020. APT29 used customized malware to inject malicious code into the SolarWinds Orion software build process that was later distributed through a normal software update; they also used password spraying, token theft, API abuse, spear phishing, and other supply chain attacks to compromise user accounts and leverage their associated access. Victims of this campaign included government, consulting, technology, telecom, and other organizations in North America, Europe, Asia, and the Middle East. Industry reporting initially referred to the actors involved in this campaign as UNC2452, NOBELIUM, StellarParticle, Dark Halo, and SolarStorm.[1][2][3][4][5][6][7][8]

In April 2021, the US and UK governments attributed the SolarWinds Compromise to Russia's Foreign Intelligence Service (SVR); public statements included citations to APT29, Cozy Bear, and The Dukes.[9][10][11] The US government assessed that of the approximately 18,000 affected public and private sector customers of Solar Winds' Orion product, a much smaller number were compromised by follow-on APT29 activity on their systems.[12]

ID: C0024
First Seen: August 2019 [6]
Last Seen: January 2021 [13]
Version: 1.0
Created: 24 March 2023
Last Modified: 14 April 2023

Version Permalink

Groups

ID	Name	Description
G0016	APT29	[9][10][11]

Techniques Used

ATT&CK® Navigator Layers

Domain	ID		Name	Use
Enterprise	T1087		Account Discovery	During the SolarWinds Compromise, APT29 obtained a list of users and their roles from an Exchange server using `Get-ManagementRoleAssignment`.[4]
		.002	Domain Account	During the SolarWinds Compromise, APT29 used PowerShell to discover domain accounts by exectuing `Get-ADUser` and `Get-ADGroupMember`.[5][14]
Enterprise	T1098	.001	Account Manipulation: Additional Cloud Credentials	During the SolarWinds Compromise, APT29 added credentials to OAuth Applications and Service Principals.[15][5]
		.002	Account Manipulation: Additional Email Delegate Permissions	During the SolarWinds Compromise, APT29 added their own devices as allowed IDs for active sync using `Set-CASMailbox`, allowing it to obtain copies of victim mailboxes. It also added additional permissions (such as Mail.Read and Mail.ReadWrite) to compromised Application or Service Principals.[4][15][16]
		.003	Account Manipulation: Additional Cloud Roles	During the SolarWinds Compromise, APT29 granted `company administrator` privileges to a newly created service principle.[5]
		.005	Account Manipulation: Device Registration	During the SolarWinds Compromise, APT29 registered devices in order to enable mailbox syncing via the `Set-CASMailbox` command.[4]
Enterprise	T1583	.001	Acquire Infrastructure: Domains	For the SolarWinds Compromise, APT29 acquired C2 domains, sometimes through resellers.[17][18]
Enterprise	T1071	.001	Application Layer Protocol: Web Protocols	During the SolarWinds Compromise, APT29 used HTTP for C2 and data exfiltration.[4]
Enterprise	T1560	.001	Archive Collected Data: Archive via Utility	During the SolarWinds Compromise, APT29 used 7-Zip to compress stolen emails into password-protected archives prior to exfiltration; APT29 also compressed text files into zipped archives.[4][19][5]

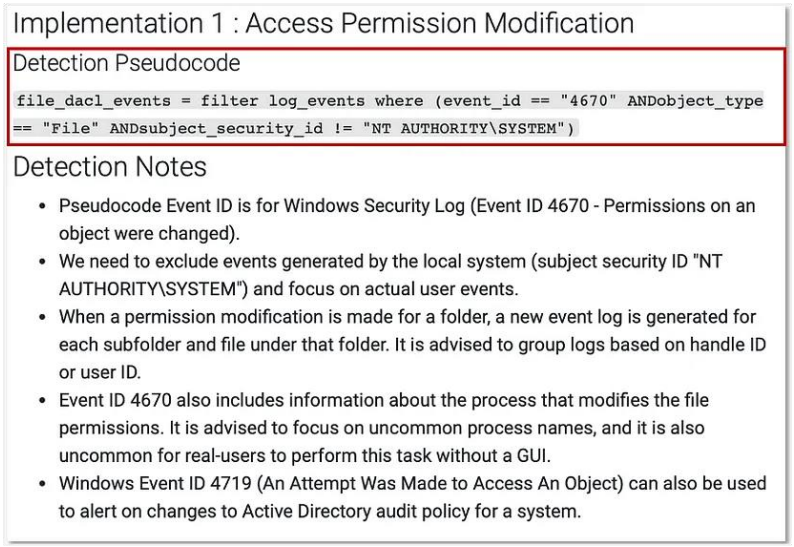
SolarWindsサプライチェーン攻撃のキャンペーン

© NEC Corporation 2023

v13で追加された新しい機能

疑似コードの提供や、検索の改善など、細かい機能改修がメイン

- 疑似コードの提供
  - 疑似コードが追加、検出のためのコード例として使用可能



Implementation 1 : Access Permission Modification

Detection Pseudocode

```
file_dacl_events = filter log_events where (event_id == "4670" ANDobject_type == "File" ANDsubject_security_id != "NT AUTHORITY\SYSTEM")
```

Detection Notes

- Pseudocode Event ID is for Windows Security Log (Event ID 4670 - Permissions on an object were changed).
- We need to exclude events generated by the local system (subject security ID "NT AUTHORITY\SYSTEM") and focus on actual user events.
- When a permission modification is made for a folder, a new event log is generated for each subfolder and file under that folder. It is advised to group logs based on handle ID or user ID.
- Event ID 4670 also includes information about the process that modifies the file permissions. It is advised to focus on uncommon process names, and it is also uncommon for real-users to perform this task without a GUI.
- Windows Event ID 4719 (An Attempt Was Made to Access An Object) can also be used to alert on changes to Active Directory audit policy for a system.

- サイト内検索が改善、これまでビックリするくらい遅かった
- changelogもJSONで提供されるように

© NEC Corporation 2023

新規追加テクニック

v12で新規追加されたテクニックの一覧(Enterprise)

Techniques

Enterprise

計18

New Techniques

- Acquire Infrastructure: Serverless (v1.0)
- Compromise Accounts: Cloud Accounts (v1.0)
- Compromise Infrastructure: Serverless (v1.0)
- Establish Accounts: Cloud Accounts (v1.0)
- Event Triggered Execution: Installer Packages (v1.0)
- Indicator Removal: Clear Mailbox Data (v1.0)
- Indicator Removal: Clear Network Connection History and Configurations (v1.0)
- Indicator Removal: Clear Persistence (v1.0)
- Modify Authentication Process: Hybrid Identity (v1.0)
- Modify Authentication Process: Multi-Factor Authentication (v1.0)
- Obfuscated Files or Information: Dynamic API Resolution (v1.0)
- Obfuscated Files or Information: Embedded Payloads (v1.0)
- Obfuscated Files or Information: Stripped Payloads (v1.0)
- Search Open Websites/Domains: Code Repositories (v1.0)
- Serverless Execution (v1.0)
- Stage Capabilities: SEO Poisoning (v1.0)
- Steal or Forge Authentication Certificates (v1.0)
- Traffic Signaling: Socket Filters (v1.0)

© NEC Corporation 2023

v12で追加されたテクニック(抜粋)

- **Acquire Infrastructure: Serverless**
  - Cloudflare Workers・AWS Lambdaなどのサーバレスインフラを攻撃用に取得
- **Compromise Accounts: Cloud Accounts**
  - 被害者のクラウドアカウントを窃取
- **Event Triggered Execution: Installer Packages**
  - インストーラー実行時の高権限を悪用
- **Indicator Removal: Clear Network Connection History and Configurations**
  - ネットワーク接続の痕跡を削除

© NEC Corporation 2023

v12で追加されたテクニック(抜粋)

- **Modify Authentication Process: Multi-Factor Authentication**
  - 侵害したアカウントの多要素認証を無効に
- **Obfuscated Files or Information: Dynamic API Resolution**
  - マルウェアの使用するAPI関数をハッシュなどで難読化
- **Stage Capabilities: SEO Poisoning**
  - SEOポイズニング

© NEC Corporation 2023

v13で新規追加されたテクニックの一覧(Enterprise)

Techniques

Enterprise

計13

New Techniques

- Acquire Access (v1.0)
- Acquire Infrastructure: Malvertising (v1.0)
- Cloud Administration Command (v1.0)
- Command and Scripting Interpreter: Cloud API (v1.0)
- Device Driver Discovery (v1.0)
- Exfiltration Over Web Service: Exfiltration to Text Storage Sites (v1.0)
- Impair Defenses: Spoof Security Alerting (v1.0)
- Masquerading: Masquerade File Type (v1.0)
- Modify Authentication Process: Network Provider DLL (v1.0)
- Obfuscated Files or Information: Command Obfuscation (v1.0)
- Obfuscated Files or Information: Fileless Storage (v1.0)
- Remote Services: Cloud Services (v1.0)
- Unsecured Credentials: Chat Messages (v1.0)

© NEC Corporation 2023

v13で追加されたテクニック(抜粋)

◆ Acquire Access

- ■ 標的システムのアクセス権を取得
  - • アクセスブローカーからの購入など

◆ Acquire Infrastructure: Malvertising

- ■ オンライン広告経由でマルウェアなどを配布する手法
- ■ 2022年末にFBIが広告ブロッカーを推奨したため、改めて注目
  - • その後、この手法を使用するマルウェア配布事例が複数報告

◆ Command and Scripting Interpreter: Cloud API

- ■ 攻撃にクラウドAPIを悪用

© NEC Corporation 2023

v13で追加されたテクニック(抜粋)

- **Obfuscated Files or Information: Command Obfuscation**
  - コマンドやスクリプトを難読化し、検出を回避
- **Obfuscated Files or Information: Fileless Storage**
  - レジストリやイベントログなどにデータを隠し、ファイルレスとして利用
- **Remote Services: Cloud Services**
  - オンプレ環境と連携したクラウドサービスに侵入
- **Unsecured Credentials: Chat Messages**
  - 暗号化されていないチャットデータから資格情報を窃取

© NEC Corporation 2023

追加されたテクニックの傾向

クラウドや外部リソースに関係するテクニックが目立つ

◆ クラウドや外部リソースが関係するテクニックが新規の約1/3を占める

Acquire Infrastructure: Serverless
Compromise Accounts: Cloud Accounts
Compromise Infrastructure: Serverless
Establish Accounts: Cloud Accounts
Modify Authentication Process: Hybrid Identity
Search Open Websites/Domains: Code Repositories
Serverless Execution

Cloud Administration Command
Command and Scripting Interpreter: Cloud API
Exfiltration Over Web Service: Exfiltration to Text Storage Sites
Remote Services: Cloud Services
Unsecured Credentials: Chat Messages

クラウドを使用したIDに需要がある

v11以前のMITRE ATT&CKでは、
クラウドが関係するシナリオを上手く
説明できていない可能性あり

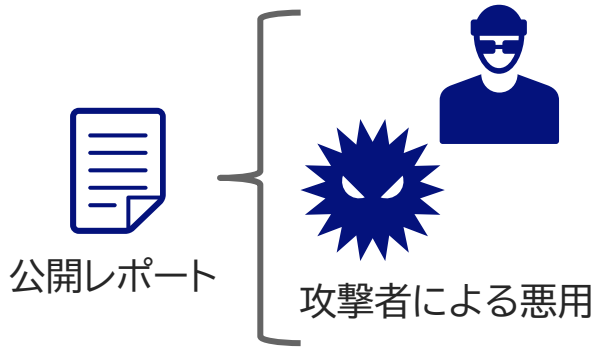
© NEC Corporation 2023

追加テクニックからトレンドを追う

MITRE ATT&CKで見るトレンド

実際に観測・報告された攻撃手法のみがテクニックとして追加される

- **攻撃に使用されたという報告（レポート等）が根拠として必要**
  - 研究・実証レベルではマトリックスに追加されない
  - ⇒ **記述テクニックは全て実環境に投入可能な手法**



- 2018年のv1から既に5年以上が経過しており、メジャーな攻撃手法はほぼ網羅済
  - **新規に登録されるテクニックは、比較的新しいorマイナーな手法の可能性あり**

新規登録テクニックから、攻撃のトレンドを捉えることが出来ないか？

© NEC Corporation 2023

MITRE ATT&CKで見るトレンド

根拠となっているリファレンスの報告日などから、新規テクニックの性質を判断

- テクニックページにて言及されているレポートへのリンクあり
  - 公開日が記載されており、新規テクニックでも数年前のリンクが使用されている場合がある
    - **新規テクニック≠新規攻撃手法**

⇒ **リファレンス集の公開日に着目しつつ、新規テクニックを確認する**

References

1. Michael Osakwe. (2020, November 18). 4 SaaS and Slack Security Risks to Consider. Retrieved March 17, 2023.
2. MSTIC, DART, M365 Defender. (2022, March 24). DEV-0537 Criminal Actor Targeting Organizations for Data Exfiltration and Destruction. Retrieved May 17, 2022.
3. Slack Help Center. (n.d.). View Access Logs for your workspace. Retrieved April 10, 2023.

v13で追加されたUnsecured Credentials: Chat Messagesのリファレンス欄

© NEC Corporation 2023

追加テクニックのリファレンスに着目

Indicator Removal: Clear Network Connection History and Configurations

- レジストリに保存されるRDP接続履歴などを削除
  - 横移動した痕跡を消し、インシデント対応を妨害

References

1. Microsoft. (2021, September 24). How to remove entries from the Remote Desktop Connection Computer box. Retrieved June 15, 2022.
2. Moran, B. (2020, November 18). Putting Together the RDPieces. Retrieved October 17, 2022.
3. rjben. (2012, May 30). How do you find the culprit when unauthorized access to a computer is a problem?. Retrieved August 3, 2022.
4. freedesktop.org. (n.d.). systemd-journald.service. Retrieved June 15, 2022.
5. Sarah Edwards. (2020, April 30). Analysis of Apple Unified Logs: Quarantine Edition [Entry 6] – Working From Home? Remote Logins. Retrieved August 19, 2021.
6. MSTIC, CDOC, 365 Defender Research Team. (2021, January 20). Deep dive into the Solorigate second-stage activation: From SUNBURST to TEARDROP and Raindrop . Retrieved January 22, 2021.

- 2020年、2021年の情報が中心
  - **2020年末発覚のSolarWindsサプライチェーン侵害でこの手法が使われたと報告されており、その情報をベースに今回追加**
    - 2012年の情報は、MacにおけるRemote Desktopの履歴がどこに残るかというフォーラムへの質問

© NEC Corporation 2023

追加テクニックのリファレンスに着目

Stage Capabilities: SEO Poisoning

- 検索結果の上位に偽サイトなどの悪意あるコンテンツを表示させる
  - これらを上位検索結果に表示させるには専門知識が必要
  - 広告のために使い込まれたGoogleアカウントが重宝されており、
    窃取されたアカウントは数千ドルで取引されることもあり
    https://blog.sekoia.io/overview-of-the-russian-speaking-infostealer-ecosystem-the-distribution/

References

1. Atlas Cybersecurity. (2021, April 19). Threat Actors use Search-Engine-Optimization Tactics to Redirect Traffic and Install Malware. Retrieved September 30, 2022.
2. Arntz, P. (2018, May 29). SEO poisoning: Is it worth it?. Retrieved September 30, 2022.
3. Wang, J. (2018, October 17). Ubiquitous SEO Poisoning URLs. Retrieved September 30, 2022.
4. The DFIR Report. (2022, May 9). SEO Poisoning – A Gootloader Story. Retrieved September 30, 2022.
5. Szappanos, G. & Brandt, A. (2021, March 1). "Gootloader" expands its payload delivery options. Retrieved September 30, 2022.

- 2018年～2022年までの情報が幅広く参照
  - 2000年代にもこの手のニュースは存在しており、特段トレンドとは言い難いが、
    マルバタイジングとの兼ね合いで改めて注目された

© NEC Corporation 2023

追加テクニックのリファレンスに着目

Obfuscated Files or Information: Dynamic API Resolution

- APIをハッシュ記述してマルウェアの実行時に解決するなどで、使用するAPIを隠す
  - あくまで時間稼ぎなので、ばらまき型など頻繁に更新されるマルウェアで使用される傾向がある

References

1. Brennan, M. (2022, February 16). Hackers No Hashing: Randomizing API Hashes to Evade Cobalt Strike Shellcode Detection. Retrieved August 22, 2022.
2. spotheplanet. (n.d.). Windows API Hashing in Malware. Retrieved August 22, 2022.
3. Choi, S. (2015, August 6). Obfuscated API Functions in Modern Packers. Retrieved August 22, 2022.
4. drakonia. (2022, August 10). HInvoke and avoiding PInvoke. Retrieved August 22, 2022.
5. Hasherezade. (2021, July 23). AvosLocker enters the ransomware scene, asks for partners. Retrieved January 11, 2023.
6. Cybereason Nocturnus. (2020, July 16). A BAZAR OF TRICKS: FOLLOWING TEAM9'S DEVELOPMENT CYCLES. Retrieved November 18, 2020.
7. Pantazopoulos, N. (2020, June 2). In-depth analysis of the new Team9 malware family. Retrieved December 1, 2020.
8. Harbison, M. and Renals, P. (2022, July 5). When Pentest Tools Go Brutal: Red-Teaming Tool Being Abused by Malicious Actors. Retrieved February 1, 2023.
9. Saini, A. and Hossein, J. (2022, January 27). North Korea's Lazarus APT leverages Windows Update client, GitHub in latest campaign. Retrieved January 27, 2022.
10. Microsoft Threat Intelligence Center. (2022, February 4). ACTINIUM targets Ukrainian organizations. Retrieved February 18, 2022.
11. Jason (jxb5151). (2021, January 28). findapihash.py. Retrieved August 22, 2022.

- 手法としては以前から存在しているが、2022年以降の記事が目立つ

⇒ **過去1年ほどで珍しいテクニックではなくなった可能性がある**

© NEC Corporation 2023

追加テクニックのリファレンスに着目

Acquire Access

- 初期アクセスブローカーなどから資格情報を入手し、攻撃に使用
  - ランサムウェア攻撃の分業制などで、数年前からその役割が注目

References

1. Microsoft. (2022, May 9). Ransomware as a service: Understanding the cybercrime gig economy and how to protect yourself. Retrieved March 10, 2023.
2. CrowdStrike Intelligence Team. (2022, February 23). Access Brokers: Who Are the Targets, and What Are They Worth?. Retrieved March 10, 2023.
3. Brian Krebs. (2012, October 22). Service Sells Access to Fortune 500 Firms. Retrieved March 10, 2023.
4. Cybersecurity Infrastructure and Defense Agency. (2022, June 2). Karakurt Data Extortion Group. Retrieved March 10, 2023.

- RaaSエコシステムが注目されるとともにその存在が広く認識され出したが、ここでは2022年の報告がリファレンスとして使用されている
  - 2019、2020年

  ⇒ このエコシステムが2022年時点でも活動中

しかし、上記の経緯はこのID説明ページだけでは把握できない…

© NEC Corporation 2023

追加テクニックのリファレンスに着目

Acquire Infrastructure: Malvertising

- ◆ 広告を入り口にマルウェアを配信するテクニック
  - ■ **2022年末から2023年にかけて多数のマルウェアが攻撃手法として採用**
  - ■ FBIが広告ブロッカーを推奨するなどで広く注目
    - ユーザー側が行える対処法が少ない
  - ■ SEOポイズニングとは同じ戦術に属するが、別々のテクニックとして登録
    - マルバタイジングをSEOポイズニングの一種と整理する場合もあるが、ATT&CKではそのような整理をしていない

1. Miller, Sarah. (2023, February 2). A surge of malvertising across Google Ads is distributing dangerous malware. Retrieved February 21, 2023.
2. Tal, Nati. (2022, December 28). "MasquerAds" — Google's Ad-Words Massively Abused by Threat Actors, Targeting Organizations, GPUs and Crypto Wallets. Retrieved February 21, 2023.
3. FBI. (2022, December 21). Cyber Criminals Impersonating Brands Using Search Engine Advertisement Services to Defraud Users. Retrieved February 21, 2023.
4. Hegel, Tom. (2023, January 19). Breaking Down the SEO Poisoning Attack | How Attackers Are Hijacking Search Results. Retrieved February 21, 2023.
5. BBC. (2011, March 29). Spotify ads hit by malware attack. Retrieved February 21, 2023.

- ■ **リファレンスには2011年の事例が掲載されており、決して新しい手法でないことも指摘されている**
  - SEOポイズニングの記事も使用しており、この切り分け境界が不明

© NEC Corporation 2023

追加テクニックのリファレンスに着目

Obfuscated Files or Information: Fileless Storage

- 2014年～2023年までリファレンスが多数
  - ⇒ **新規でもマイナーでもないテクニック**

References

1. Microsoft. (2023, February 6). Fileless threats. Retrieved March 23, 2023.
2. Legezo, D. (2022, May 4). A new secret stash for "fileless" malware. Retrieved March 23, 2023.
3. Dumont, R. (2019, March 20). Fake or Fake: Keeping up with OceanLotus decoys. Retrieved April 1, 2019.
4. Salem, E. (2020, November 17). CHAES: Novel Malware Targeting Latin American E-Commerce. Retrieved June 30, 2021.
5. FireEye. (2015). APT28: A WINDOW INTO RUSSIA'S CYBER ESPIONAGE OPERATIONS?. Retrieved August 19, 2015.
6. Faou, M. (2020, May). From Agent.btz to ComRAT v4: A ten-year journey. Retrieved June 15, 2020.
7. CISA. (2020, October 29). Malware Analysis Report (AR20-303A). Retrieved December 9, 2020.
8. Smith, S., Stafford, M. (2021, December 14). DarkWatchman: A new evolution in fileless techniques. Retrieved January 10, 2022.
9. Cherepanov, A., Lipovsky, R. (2018, October 11). New TeleBots backdoor: First evidence linking Industroyer to NotPetya. Retrieved November 27, 2018.
10. Dupuy, T. and Faou, M. (2021, June). Gelsemium. Retrieved November 30, 2021.
11. ESET. (2020, April 28). Grandoreiro: How engorged can an EXE get?. Retrieved November 13, 2020.
12. ESET, et al. (2018, January). Diplomats in Eastern Europe bitten by a Turla mosquito. Retrieved July 3, 2018.
13. Lambert, T. (2020, January 29). Intro to Netwire. Retrieved January 7, 2021.
14. Cybereason Nocturnus. (2022, May 4). Operation CuckooBees: Deep-Dive into Stealthy Winnti Techniques. Retrieved September 22, 2022.
15. Trustwave SpiderLabs. (2020, June 22). Pillowmint: FIN7's Monkey Thief . Retrieved July 27, 2020.
16. Tartare, M. et al. (2020, May 21). No "Game over" for the Winnti Group. Retrieved August 24, 2020.
17. Faou, M., Tartare, M., Dupuy, T. (2019, October). OPERATION GHOST. Retrieved September 23, 2020.
18. Rainey, K. (n.d.). Qbot. Retrieved September 27, 2021.
19. Group IB. (2020, September). LOCK LIKE A PRO. Retrieved September 27, 2021.
20. Lee, B., Falcone, R. (2018, July 25). OilRig Targets Technology Service Provider and Government Agency with QUADAGENT. Retrieved August 9, 2018.
21. Lunghi, D. et al. (2020, February). Uncovering DRBControl. Retrieved November 12, 2021.
22. Global Threat Center, Intelligence Team. (2020, December). APT27 Turns to Ransomware. Retrieved November 12, 2021.
23. Cylance. (2019, July 3). hreat Spotlight: Sodinokibi Ransomware. Retrieved August 4, 2020.
24. Secureworks . (2019, September 24). REvil: The GandCrab Connection. Retrieved August 4, 2020.
25. McAfee. (2019, October 2). McAfee ATR Analyzes Sodinokibi aka REvil Ransomware-as-a-Service – What The Code Tells Us. Retrieved August 4, 2020.
26. Intel 471 Malware Intelligence team. (2020, March 31). REvil Ransomware-as-a-Service – An analysis of a ransomware affiliate operation. Retrieved August 4, 2020.
27. Counter Threat Unit Research Team. (2019, September 24). REvil/Sodinokibi Ransomware. Retrieved August 4, 2020.
28. Kaspersky Lab. (2017, August). ShadowPad: popular server management software hit in supply chain attack. Retrieved March 22, 2021.
29. Chen, J., et al. (2022). Delving Deep: An Analysis of Earth Lusca's Operations. Retrieved July 1, 2022.
30. Nafisi, R., Lelli, A. (2021, March 4). GoldMax, GoldFinder, and Sibot: Analyzing NOBELIUM's layered persistence. Retrieved March 8, 2021.
31. Lunghi, D. and Lu, K. (2021, April 9). Iron Tiger APT Updates Toolkit With Evolved SysUpdate Malware. Retrieved November 12, 2021.
32. Vyacheslav Kopeytsev and Seongsu Park. (2021, February 25). Lazarus targets defense industry with ThreatNeedle. Retrieved October 27, 2021.
33. Cisco Talos. (2021, September 21). TinyTurla - Turla deploys new malware to keep a secret backdoor on victim machines. Retrieved December 2, 2021.
34. Faou, M. and Dumont R.. (2019, May 29). A dive into Turla PowerShell usage. Retrieved June 14, 2019.
35. Symantec DeepSight Adversary Intelligence Team. (2019, June 20). Waterbug: Espionage Group Rolls Out Brand-New Toolset in Attacks Against Governments. Retrieved July 8, 2019.
36. US-CERT. (2018, June 14). MAR-10135536-12 – North Korean Trojan: TYPEFRAME. Retrieved July 13, 2018.
37. Salem, E. et al. (2020, May 28). VALAK: MORE THAN MEETS THE EYE . Retrieved June 19, 2020.
38. Duncan, B. (2020, July 24). Evolution of Valak, from Its Beginnings to Mass Distribution. Retrieved August 31, 2020.
39. Reaves, J. and Platt, J. (2020, June). Valak Malware and the Connection to Gozi Loader ConfCrew. Retrieved August 31, 2020.
40. US-CERT. (2017, November 22). Alert (TA17-318B): HIDDEN COBRA – North Korean Trojan: Volgmer. Retrieved December 7, 2017.
41. Yagi, J. (2014, August 24). Trojan.Volgmer. Retrieved July 16, 2018.

それなりにメジャーと思われるテクニックもまだ追加がある

© NEC Corporation 2023

リファレンスに着目しよう

変更ログがJSONでも提供されるようになったので、既存テクニックの新規リファレンスを見つけやすくなった

- 既存テクニックでもリファレンスが変更される場合がある
  - リファレンスの変更はアップデートページを見ただけでは分からないため、v13から追加されたJSON変更ログが便利


```
"revoked": false,
"external_references": [
    {
        "source_name": "mitre-attack",
        "url": "https://attack.mitre.org/techniques/T1217",
        "external_id": "T1217"
    },
    {
        "source_name": "Chrome Roaming Profiles",
        "description": "Chrome Enterprise and Education Help. (n.d.). Use Chrome Browser with Roaming User Profiles. Retrieved March 28, 2023.",
        "url": "https://support.google.com/chrome/a/answer/7349337"
    },
    {
        "source_name": "Kaspersky Autofill",
        "description": "Golubev, S. (n.d.). How malware steals autofill data from browsers. Retrieved March 28, 2023.",
        "url": "https://www.kaspersky.com/blog/browser-data-theft/27871/"
    }
],
```


STIX Field	Old value	New Value
external_references		{'source_name': 'Chrome Roaming Profiles', 'description': 'Chrome Enterprise and Education Help. (n.d.). Use Chrome Browser with Roaming User Profiles. Retrieved March 28, 2023.', 'url': 'https://support.google.com/chrome/a/answer/7349337'}
external_references		{'source_name': 'Kaspersky Autofill', 'description': 'Golubev, S. (n.d.). How malware steals autofill data from browsers. Retrieved March 28, 2023.', 'url': 'https://www.kaspersky.com/blog/browser-data-theft/27871/'}

© NEC Corporation 2023

リファレンスに着目しよう

現在のトレンドを反映したテクニックなのか、既存のトレンドが改めて登録されたのかが判別できる

◆ 日付の若いリファレンスが多数だが、古いリファレンスも存在

⇒ 手法としては新しくないが、ここ最近多数の悪用事例が報告

◆ 幅広い日付のリファレンスが存在

⇒ メジャーな攻撃手法が改めて登録された可能性が高い

◆ 数年前のリファレンスのみ

⇒ マイナーな手法だが、攻撃例は存在

© NEC Corporation 2023

抑えておきたい補足情報

TIPS: IDが付与されていないテクニック

全てのテクニックやグループが登録されている訳ではない

- Mutex
  - マルウェアの感染確認に使用される文字列
  - 感染確認等に有用だが、直接の攻撃手法ではない
  - 新規テクニックとして推薦したが採用されなかったので、痕跡系は登録されないと思われる

- Ransomware-as-a Service(RaaS)で活動している犯罪者はあまり追跡できていない
  - ランサムウェアは登録されているが、個別RaaSまでは攻撃者グループとして整理するほどではない
  - 「キャンペーン」がこの隙間を埋めてくれるかも

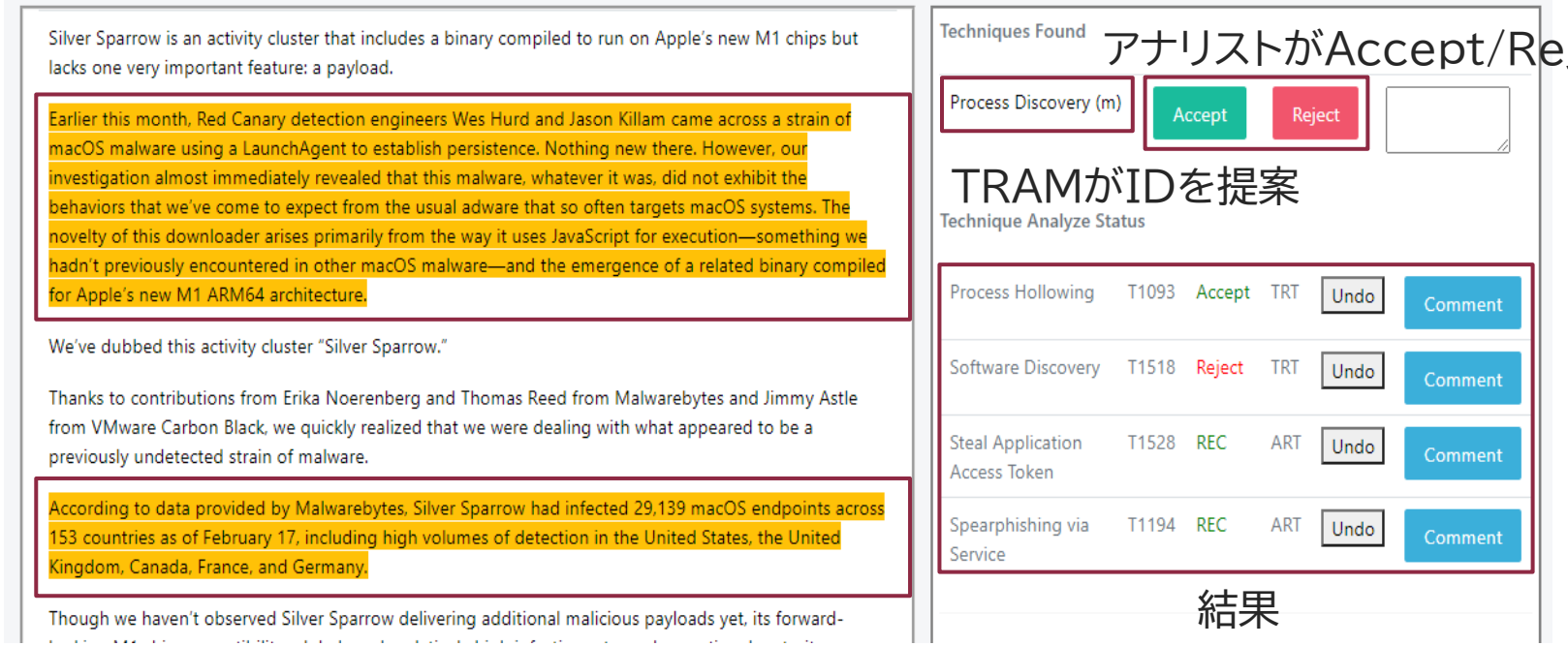
© NEC Corporation 2023

TIPS: ATT&CK ID付与のヒント

TRAM(Threat Report ATT&CK Mapping)による補助

- 脅威情報からATT&CK IDへのマッピングを半自動化
  - MITREは、マッピング補助ツールTRAM(Threat Report ATT&CK Mapping)を公開
    https://github.com/center-for-threat-informed-defense/tram/

ID付与に該当する
フレーズをハイライト



© NEC Corporation 2023

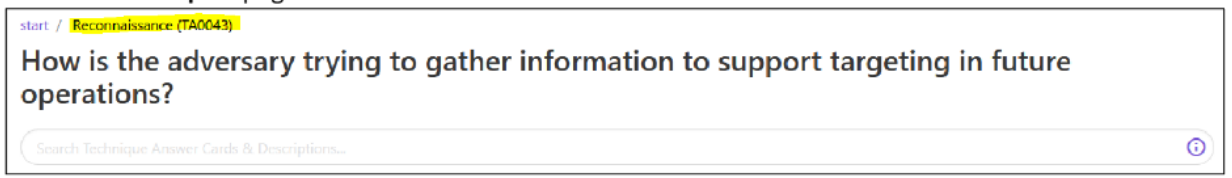
TIPS: ATT&CK ID付与のヒント

CISAが公開しているツールDeciderによるID付与の補助

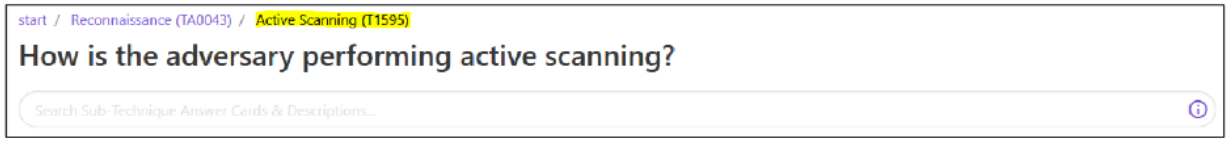
- 質問に答えていくことで適切なIDを見つけていく
  - MITREなどと連携して作成
    https://github.com/cisagov/Decider/

start→Tactics page – basic search

Tactic→Techniques page – advanced search



Technique→SubTechniques page – advanced search



© NEC Corporation 2023

TIPS: コントリビューションしよう！

サイバーセキュリティコミュニティへの貢献&Contributorとして名前が残る

- 新たな脅威&既存の未登録脅威が存在
  - 新規登録によるナレッジベースの改善は、サイバーセキュリティコミュニティへの貢献に繋がる
- 新規テクニックの推薦はそんなに難しくない
  - 公開レポートの中に未登録の攻撃手法があれば推薦出来るので、自分たちが体験した攻撃手法でなくてもよい
  - MITREも提出例を書いてくれている
    https://attack.mitre.org/resources/contribute/
- Contributorとして名前を残そう
  - **名前が載ると嬉しい**

- Yonatan Gotlib, Deep Instinct
- Yonatan Gotlib, Talon Cyber Security
- Yoshihiro Kori, NEC Corporation
- Yossi Nisani, Cymptom
- Yossi Weizman, Azure Defender Research Team
- Yusuke Kubo, RedLark, NTT Communications

© NEC Corporation 2023

まとめ

まとめ

- MITRE ATT&CKのv13が4月に公開
  - 擬似コードや検索の改善が実施
  - 半年前のv12では「キャンペーン」コレクションが追加
- v12とv13で追加されたテクニックにはクラウド関係が目立つ
  - v11以前ではクラウドを使用した攻撃シナリオが上手く表現出来ていない可能性
- トレンドを踏まえたテクニックが追加されていたものの、まだまだ既存の攻撃手法も追加されている
  - Contributorになるチャンス

© NEC Corporation 2023

Orchestrating a brighter world
NEC