APT40勧告

中華人民共和国国家安全部（PRC MSS）の諜報活動の実態

Australian Government

Australian Signals Directorate

National Cyber
Security Centre
a part of GCHQ

Communications
Security Establishment

**Canadian Centre
for Cyber Security**

Centre de la sécurité
des télécommunications

**Centre canadien
pour la cybersécurité**

目次

概要

背景

本勧告は、オーストラリア信号局（ASD）傘下のオーストラリアサイバーセキュリティセンター（ACSC）、米国サイバーセキュリティ・インフラセキュリティ庁（CISA）、米国国家安全保障局（NSA）、米国連邦捜査局（FBI）、英国国家サイバーセキュリティセンター（NCSC-UK）、カナダサイバーセキュリティセンター（CCCS）、ニュージーランド国家サイバーセキュリティセンター（NCSC-NZ）、ドイツ連邦情報局（BND）および連邦憲法擁護庁（BfV）、大韓民国国家情報院（NIS）および同院傘下の国家サイバー安全センター、日本の内閣サイバーセキュリティセンター（NISC）および警察庁（NPA）によって共同作成されたものです。以下、これらを「本勧告作成機関」と総称します。本勧告では、中華人民共和国（PRC）政府が支援するサイバー攻撃グループの概要と、オーストラリアのネットワークに対する現在の脅威について説明しています。本勧告は、本勧告作成機関が共有する脅威に関する認識および、ASD傘下のACSC（以下、「ASD-ACSC」）が実施したインシデント対応調査の結果に基づいています。

このPRC政府支援のサイバーグループは、これまでにオーストラリアやアメリカ合衆国を含む複数の国の組織を標的にしてきました。以下に示す手法は、世界中で他のPRC政府支援のアクターによって日常的に使用されています。したがって、本勧告作成機関は、このグループおよび類似の手法が、自国のネットワークに対しても引き続き脅威となっていると認識しています。

本勧告作成機関は、このグループがPRC国家安全部（MSS）のために悪意あるサイバー作戦を実行していると判断しています。このグループの活動および手法は、業界の報告において Advanced Persistent Threat（APT）40 として追跡されているグループのものと一致しています。また、このグループは Kryptonite Panda、GINGHAM TYPHOON、Leviathan、Bronze Mohawkなどの別名でも知られています。このグループは、過去の報告において、PRC海南省海口市を拠点とし、PRC MSS海南省国家安全庁から指示を受けているとされています。[2]本勧告では、2つの被害組織のネットワークに対して、この攻撃者が実際に用いた手法の重要なケーススタディを抜粋して紹介します。

これらのケーススタディは、サイバーセキュリティ担当者が自らのネットワークに対するAPT40の侵入を特定、防止、是正するための重要な手がかりとなります。選定されたケーススタディは、適切な是正措置が講じられ、この脅威アクターや他のアクターによる再侵害のリスクが低減された事例です。そのため、これらのケーススタディは、組織が必要な是正措置を講じるための十分な時間が確保されるよう、必然的にある程度古いものとなっています。

活動の概要

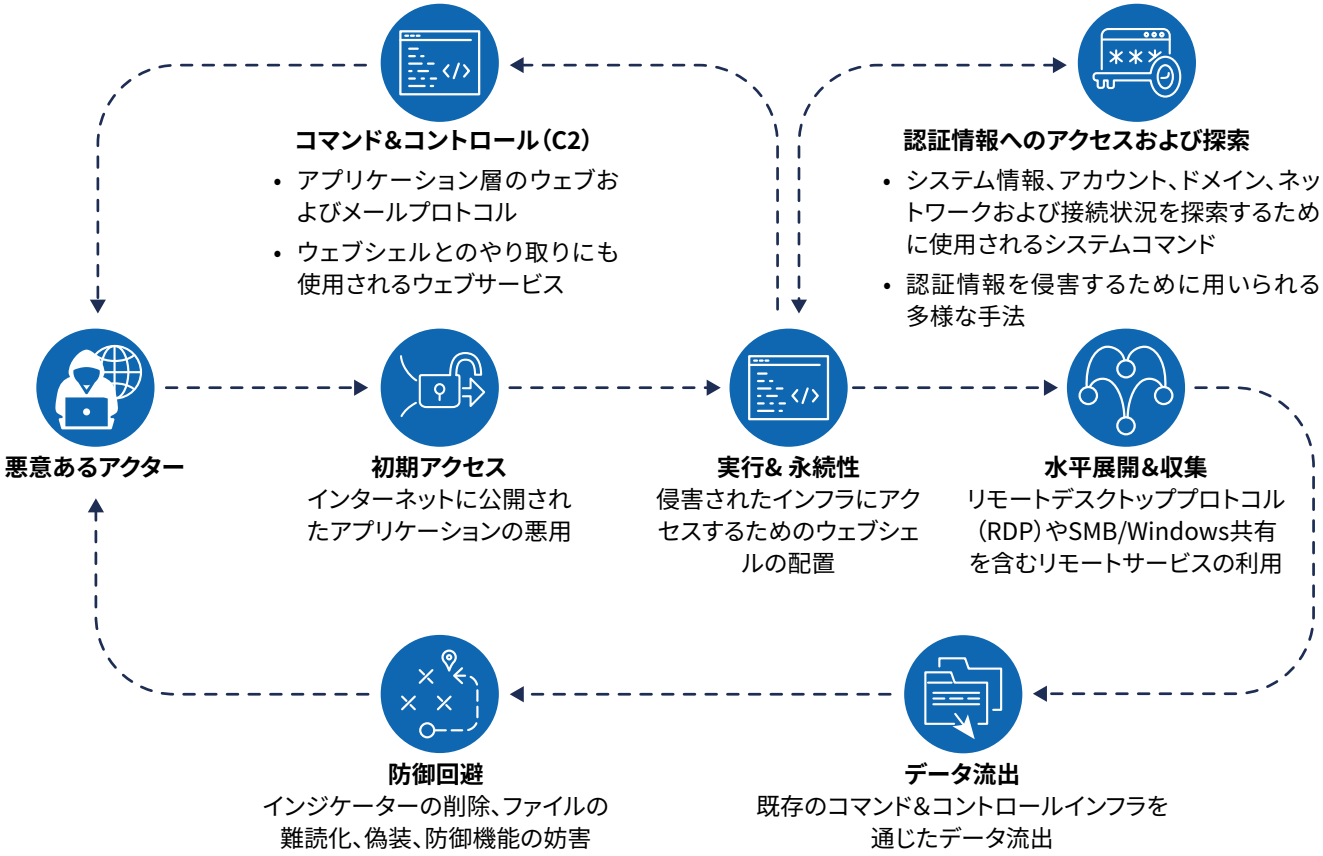
APT40は、オーストラリアのネットワークのみならず、地域内の政府および民間セクターのネットワークを繰り返し標的にしており、我々のネットワークに対する脅威は現在も継続しています。本勧告で示した攻撃手法は、オーストラリアのネットワークにおいて頻繁に確認されています。

特に注目すべきは、APT40が、新たに発見された脆弱性に対するエクスプロイト用の概念実証（POC）を迅速に改変・適応させ、当該脆弱性を有するインフラを備えた標的ネットワークに対して即座に利用できる能力を有している点です。APT40は、標的を侵害する機会を探るために、本勧告作成機関が所在する国々を含む関心対象のネットワークに対して、定期的に偵察活動を行っています。このような定期的な情報収集により、同グループは、関心対象のネットワーク上に存在する脆弱な機器や、サポートが終了した機器、保守されていない機器を特定し、迅速にエクスプロイトを展開できる態勢を整えています。APT40は、2017年頃から脆弱性を悪用して成功を収め続けています。

APT40は、Log4J（CVE-2021-44228）、Atlassian Confluence（CVE-2021-31207、CVE-2021-26084）、Microsoft Exchange（CVE-2021-31207、CVE-2021-34523、CVE-2021-34473）など、広く利用されているソフトウェアに関して新たに公表された脆弱性をすばやく悪用しています。ASD-ACSCおよび本勧告作成機関は、新たに公表された注目度の高い脆弱性について、このグループが公開から数時間から数日以内にPOCを活用し続けると予測しています。

2　米国司法省（2021年）感染症研究を含む知的財産および企業機密情報を標的にした世界的なコンピュータ侵入キャンペーンで、国家安全省と関係のある中国人4人を起訴。

図1：APT40の活動におけるTTP（戦術・技術・手順）フローチャート



このグループは、フィッシングキャンペーンのようにユーザーによる操作を必要とする手法よりも、脆弱な外部公開インフラの悪用を好む傾向があり、さまざまな後続の活動を可能にするために有効な認証情報を取得することを優先しています。APT40は、特に侵入の初期段階において、永続的なアクセス手段としてウェブシェル（T1505.003）を定期的に使用しています。通常、APT40は初期アクセスに成功した後、被害者の環境へのアクセスを維持するために永続的なアクセス確立に注力します。永続的なアクセスは侵入の初期段階で行われるため、侵害の深刻さやその後の行動の有無にかかわらず、ほぼすべての侵入で見られます。

健著な手法

APT40はこれまでに、侵害したオーストラリアのウェブサイトをコマンド&コントロール（C2）用ホストとして利用してきましたが、このグループはこの手法を進化させています（T1594）。

APT40は、世界的な傾向に従い、オーストラリアにおける活動において、小規模オフィス／ホームオフィス（SOHO）機器を含む侵害されたデバイスを、作戦インフラやラスト・ホップリダイレクター（T1584.008）として活用しています。これにより、本勧告作成機関は当該グループの動向をより正確に把握し、追跡することが可能になりました。

これらのSOHO機器の多くはサポート終了やパッチ未適用のため、Nデイ脆弱性の悪用にとって格好の標的となっています。一度侵害されると、SOHO機器は正規の通信に紛れ込み、ネットワーク防御担当者の検知を困難にするよう設計された攻撃の発信拠点となります（T1001.003）。

この手法は、他のPRC政府支援のアクターによっても世界中で日常的に使用されており、本勧告作成機関はこれを共通の脅威と見なしています。追加情報については、共同勧告「中華人民共和国の国家支援によるサイバー行為者がネットワーク・プロバイダーおよびデバイスを悪用する」および「中華人民共和国の国家支援行為者が米国の重要インフラを侵害し、永続的なアクセスを維持する」を参照のこと。

APT40は、被害者向けのC2インフラとして調達またはリースしたインフラを使用することもありますが、この手口は相対的に減少傾向にあると見られます。

攻撃ツール群

ASD-ACSCは、以下に示す調査で特定された悪意あるファイルの一部を共有しています。これらのファイルは、より多くのネットワーク防御やサイバーセキュリティの関係者が対処すべき脅威をより的確に理解し、対応できるよう、VirusTotalにアップロードされています。

ケーススタディ

ASD-ACSCは、アクターがどのようにツールや手法を用いているかを広く周知するため、匿名化された2件の調査報告書を共有しています。

MD5	ファイル名	追加情報
26a5a7e71a601be991073c78d513dee3	horizon.jsp	1 kB | Javaソース
87c88f06a7464db2534bc78ec2b915de	Index_jsp$ProxyEndpoint$Attach.class	597 B | Javaバイトコード
6a9bc68c9bc5cefaf1880ae6ffb1d0ca	Index_jsp.class	5 kB | Javaバイトコード
64454645a9a21510226ab29e01e76d39	Index_jsp.java	5 kB | Javaソース
e2175f91ce3da2e8d46b0639e941e13f	Index_jsp$ProxyEndpoint.class	4 kB | Javaバイトコード
9f89f069466b8b5c9bf25c9374a4daf8	Index_jsp$ProxyEndpoint$1.class	3 kB | Javaバイトコード
187d6f2ed2c80f805461d9119a5878ac	Index_jsp$ProxyEndpoint$2.class	1 kB | Javaバイトコード
ed7178cec90ed21644e669378b3a97ec	Nova_jsp.class	7 kB | Javaバイトコード
5bf7560d0a638e34035f85cd3788e258	Nova_jsp$TomcatListenerMemShellFromThread.class	8 kB | Javaバイトコード
e02be0dc614523ddd7a28c9e9d500cff	Nova_jsp.java	15 kB | Javaソース

ケーススタディ1

本報告書は、より広範な共有を可能にするため匿名化されています。影響を受けた組織は、以後「当該組織」と記載します。被害者の身元およびASD-ACS9Cのインシデント対応手法を保護するため、一部の詳細は削除されています。

エグゼクティブサマリー

本報告書は、2022年7月から9月にかけて当該組織のネットワークが侵害された件について、ASD-ACSCが実施した調査結果の詳細をまとめたものです。本調査報告書は、確認された悪意ある活動の概要をまとめ、是正措置を推奨する目的で当該組織に提供されたものです。調査結果は、本件の侵害がAPT40によって行われたことを示しています。

8月中旬、ASD-ACSCは、8月下旬に当該グループが使用していたと見られる侵害デバイスから当該組織のネットワークへの悪意ある通信が確認されたことを通知しました。その後、組織の同意を得て、影響が及んでいる可能性のあるホストにホストベースのセンサーを展開しました。これらのセンサーにより、ASD-ACSCのインシデント対応アナリストは徹底したデジタル・フォレンジック調査を実施することができました。利用可能なセンサーデータを基に、ASD-ACSCの分析官は当該グループの活動を正確に把握し、確認された活動について詳細な時系列を作成しました。

7月から8月にかけて、ASD-ACSCが確認した主な活動は以下のとおりです。

- ホストの列挙（ネットワークの構成を把握するためにアクターが独自のマップを作成する行為）
- ウェブシェルの使用（アクターがネットワーク上に初期の足場を築き、コマンドを実行する能力を得る行為）
- アクターが悪意ある目的で利用するその他のツールの展開

調査の結果、大量の機密データへのアクセスの証拠や、アクターがネットワーク内を水平展開していた証拠（T1021.002）が確認されました。侵害が広範囲に及んだ要因としては、当該グループがネットワーク内に複数のアクセス経路を確立していたこと、ネットワークがフラットな構成であったこと、そしてファイルを任意にアップロードできる不適切に設計された内部開発ソフトウェアが使用されていたことが挙げられます。流出したデータには、グループのログインを可能にする特権認証情報だけでなく、元のアクセス経路がブロックされた場合にアクターが不正アクセスを再開できるようなネットワーク情報も含まれていました。最初に侵害されたマシンに存在していたもの以外に新たな悪意あるツールは確認されませんでしたが、グループが正規の権限認証情報にアクセスすることで、追加のツールは不要となります。調査結果によれば、当該組織は、公開されていた脆弱性を偶然突かれたのではなく、APT40によって意図的に標的にされた可能性が高いと考えられます。

調査結果

2022年8月中旬、ASD-ACSCは当該組織に対し、国家支援型のサイバーグループに関連すると見られる確認済みの悪意あるIPアドレスが、少なくとも7月から8月にかけて当該組織のコンピュータネットワークと通信していたことを通知しました。侵害されたデバイスは、小規模事業者または一般家庭のユーザーが所有していた可能性が高いと考えられます。

8月下旬、ASD-ACSCは、侵害の影響を受けた証拠が確認された当該組織のネットワーク上のホストに対し、ホストベースのエージェントを展開しました。

ログの設定やネットワーク設計の影響により、調査を支援し得た一部のアーティファクトは取得できませんでした。それにもかかわらず、当該組織が利用可能なすべてのデータを提供する体制を整えていたことで、ASD-ACSCのインシデント対応チームは包括的な分析を実施し、ネットワーク上でのAPT40の活動を把握することができました。

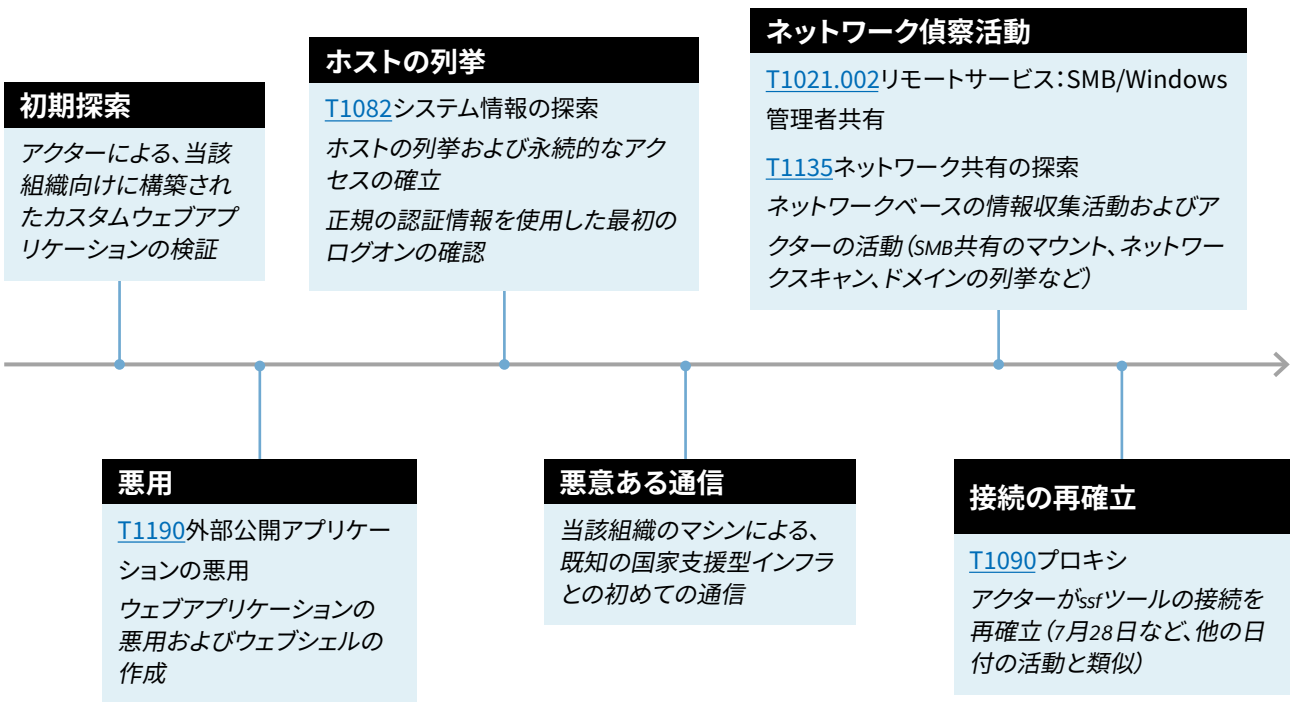
9月、ASD-ACSCとの協議の結果、当該組織は最初の通知で特定されたIPアドレスを拒否リストに登録することを決定しました。10月、当該組織は是正措置を開始しました。

詳細

7月以降、アクターは`<webapp>2-ext`上で稼働していたカスタムウェブアプリケーション（T1190）を検証・悪用することに成功し、ネットワークの非武装地帯（DMZ）に足場を築きました。アクターはこれを利用して、ネットワークおよび可視化されたすべてのドメインを列挙しました。侵害された認証情報（T1078.002）が使用され、Active Directory（T1018）へのクエリ実行や、DMZ内の複数のマシンからファイル共有（T1039）をマウントしてのデータ流出が行われました。アクターは、サーバーから有効なネットワーク認証情報を取得するために、Kerberoasting攻撃（T1558.003）を実行しました。当該グループがDMZまたは内部ネットワーク内で新たな侵入拠点を得た形跡は確認されませんでした。

視覚的タイムライン

以下のタイムラインは、当該組織のネットワーク上で確認された悪意あるアクターの活動における主要フェーズの概要を示したものです。



詳細なタイムライン

7月：アクターが、当該組織向けに構築されたカスタムウェブアプリケーション（以下「ウェブアプリケーション」または「*webapp*」）のフロントページへ、トランスポート層セキュリティ（TLS）接続（T1102）を介して初回接続を確立する（T1190）。その他に特筆すべき活動は確認されなかった。

7月：アクターが、ウェブアプリケーションのウェブサイト上でエンドポイントを特定するための列挙を開始し、さらに調査を進める[2]。

7月：アクターが特定のエンドポイントの悪用を試みることに注力する。

7月：アクターが、おそらくは別のページに設置したウェブシェルを介して、ウェブサーバーへの `POST` に成功する。同じアクターが使用していると見られる2つ目のIPアドレスも、同じURLへの投稿を開始する。アクターが複数のウェブシェルを作成し、動作確認を行う。

正確な悪用手法は不明だが、特定のエンドポイントが狙われ、*<webapp>2*-ext上にファイルが作成されたことは明らかである。

ASD-ACSCは、両IPアドレスの接続が数分差で行われ、かつ同じ対象に関心を示していたことから、これらが同一の侵入活動の一環であると考えられる。

7月：グループが、引き続きホストの列挙を行い、権限昇格の機会を探るとともに、別のウェブシェルを展開する。アクターが、侵害された*<firstname.surname>@<organisation domain>*の認証情報を使用してウェブアプリケーションにログインする。

アクターの活動は、*<webapp>2*-ext上での権限昇格には成功しなかったものと考えられる。その代わりに、アクターはネットワークベースの活動に軸足を移す。

7月：アクターが、内部でアクセス可能なバイナリーにハードコードされていたと見られる[3]サービスアカウントの侵害認証情報をテストする。

7月：アクターが、悪意あるインフラへの接続に使用する目的で、オープンソースツールのSecure Socket Funnelling（SSF）を展開する。この接続が、アクターの攻撃用マシンから当該組織の内部ネットワークへのトラフィックをトンネリングするために使用されており、攻撃者がサービスアカウントの認証情報を使用しようとする過程で、そのマシン名がイベントログ上に記録され、露出する。

8月：アクターが、サービスアカウントを使用した接続の確立に失敗するなど、限定的な活動を行っていたことが確認される。

8月：アクターが、ネットワークおよびActive Directoryの大規模な列挙を実行する。その後、別の侵害されたアカウントが使用され、DMZ内のWindowsマシンで[4]共有フォルダがマウントされ、データ流出に成功する。

これは、DMZ内のマウント可能なマシンに対して、盗まれた認証情報を機会に乗じて使用したものと見られる。ファイアウォールによって、アクターが同様の活動を内部ネットワークに対して行うことが阻止される。

8月～9月 SSFツールが悪意あるIPアドレスへの接続を再確立する。当該グループが、アクセスを遮断されるまで追加活動を行った形跡は確認されていない。

9月：当該組織が、ファイアウォールで当該の悪意あるIPアドレスを拒否リストに登録し、通信を遮断する。

2 この文脈における「エンドポイント」とは、ウェブアプリケーションの機能の一部を指します。

3 サービスアカウントは個々のユーザーに紐づくものではなく、サービスに紐づくものです。Microsoftの企業ドメインには、さまざまな種類のアカウントがあります。

4 共有のマウントとは、ファイルシステム上のファイルをユーザーやユーザーグループがアクセスできるようにするプロセスを指します。

アクターの戦術と手法

MITRE ATT&CKフレームワークとは、サイバー空間において脅威アクターが用いる戦術や手法を体系的にまとめた知識ベースです。このフレームワークは、米国の非営利団体であるMITRE Corporationによって作成され、脅威アクターの行動に関する共通の国際言語として機能しています。

ASD-ACSCは、以下の手法および戦術が当該アクターの悪意ある活動に関連すると判断しています。

情報収集活動

T1594 - 被害者が所有するウェブサイトの検索

アクターは、ネットワークへのアクセス機会を特定するために、カスタムウェブアプリケーションのウェブサイトを列挙しました。

初期アクセス

T1190 – 外部公開アプリケーションの悪用（カスタムウェブアプリケーションの悪用に関して）

T1078.002 – 有効なアカウント：ドメインアカウント（侵害された認証情報を使用したログオンに関して）

インターネットに直接接続されたカスタムウェブアプリケーションの悪用が、アクターにとって初期アクセスの足掛かりとなりました。アクターはその後、侵害した認証情報を利用してネットワークへのアクセスをさらに拡大しました。

実行

T1059 – コマンド／スクリプトインタープリター（ウェブシェルを通じたコマンド実行に関して）

T1072 – ソフトウェアデプロイメントツール（アクターがオープンソースツールのSecure Socket Funnelling（SSF）を使用してIPに接続したことに関して）

永続的なアクセス

T1505.003 - サーバーソフトウェアコンポーネント：ウェブシェル（ウェブシェルおよびSSFを用いたアクセス確立に関して）

認証情報アクセス

T1552.001 – パスワードストアからの認証情報取得（ビル管理システム（BMS）に関連するパスワードファイルに関して）

T1558.003 – Kerberosチケットの窃取または偽造：Kerberoasting（ネットワーク認証情報を取得するための攻撃に関して）

水平展開

T1021.002 – リモートサービス：SMB共有（アクターが複数のデバイスからSMB共有をマウントしたことに関して）

収集

T1213 – 情報リポジトリからのデータ取得（BMSサーバー上にあるマニュアルや文書に関して）

データ流出

T1041 – C2チャネル経由のデータ流出（Active Directoryおよび共有マウントからのデータ流出）

ケーススタディ2

本報告書は、より広範な共有を可能にするため匿名化されています。影響を受けた組織は、以後「当該組織」と記載します。被害者の身元およびASD-ACSCのインシデント対応手法を保護するため、一部の詳細は削除されています。

エグゼクティブサマリー

本報告書は、2022年4月にかけて当該組織のネットワークが侵害された件について、ASD-ACSCが実施した調査結果の詳細をまとめたものです。本調査報告書は、確認された悪意ある活動の概要をまとめ、是正措置を推奨する目的で当該組織に提供されたものです。調査結果は、本件の侵害がAPT40によって行われたことを示しています。

2022年5月、ASD-ACSCは、当該組織に対し、2022年4月以降にその組織のネットワークに影響を与えていると見られる悪意ある活動の疑いについて通知しました。その後、当該組織は、同社の企業向けリモートアクセスソリューションのログインポータルを提供しているインターネット公開サーバー上で、悪意あるソフトウェアを発見したことをASD-ACSCに報告しました。このサーバーはリモートアクセスログインおよびID管理製品を使用しており、本報告書では「侵害されたアプライアンス」と呼びます。本報告書は、ASD-ACSCが実施した調査に基づき、当該組織向けに作成された調査結果および是正措置に関する助言の詳細をまとめたものです。

証拠により、少なくとも2022年4月以降、当該組織のリモートアクセスログインポータルを通じて、組織のネットワークの一部が悪意あるサイバーアクターによって侵害されていたことが示されました。このサーバーは複数のアクターによって侵害された可能性があり、侵害が発生した当時に広く公表されていたリモートコード実行（RCE）の脆弱性の影響を受けたと考えられます。

ASD-ACSCが確認した主な活動は以下のとおりです。

- ホストの列挙により、ネットワークの構成を把握するためにアクターが独自のマップを作成する
- インターネットに公開されたアプリケーションの悪用およびウェブシェルを使用し、アクターがネットワーク上に初期の足場を築き、コマンドを実行できるようにする
- ソフトウェアの脆弱性を悪用した権限昇格
- 水平展開を可能にする認証情報の収集

ASD-ACSCは、2022年4月に侵害されたアプライアンス上から、数百組の固有のユーザー名とパスワードのペア、複数の多要素認証コード、そしてリモートアクセスセッションに関連する技術的アーティファクトが悪意あるアクターによって持ち出されていたことを確認しました。当該組織による確認の結果、これらのパスワードは正規のものであることが判明しました。ASD-ACSCは、アクターがこれらの技術的アーティファクトを収集したのは、正規ユーザーになりすましてリモートログインセッションを乗っ取る、あるいは新たに作成し、正規のユーザーアカウントを用いて当該組織の内部ネットワークにアクセスするためであったと判断しています。

調査結果

調査の概要

ASD-ACSCは、アクターが組織スタッフにリモートログインセッションを提供するアプライアンスを侵害し、この侵害を足掛かりにさらに活動を試みたことを確認しました。これらのアプライアンスは、ロードバランシング構成の3台のホストで構成されており、最初の侵害の証拠はそのうち1台のホストで確認されました。当該組織は、最初の侵害が確認された後まもなく、ロードバランシング構成の3台のホストのうち2台をシャットダウンしました。その結果、以降のすべての活動は1台のホスト上で行われました。侵害されたアプライアンスに関連する他のサーバーも、同様の方法でロードバランシング構成になっていました。読みやすさのため、本報告書の大部分では、すべての侵害されたアプライアンスを「単一のアプライアンス」として記載しています。

アクターは、2022年4月以降、公に知られていた脆弱性を利用して、侵害されたアプライアンスにウェブシェルを展開したと考えられています。当該グループの脅威アクターは、アプライアンス上で権限昇格を達成したと判断されています。ASD-ACSCは、ログの入手ができないため、その活動の全容を特定することはできませんでした。しかし、デバイス上の証拠から、アクターが以下の行為を行ったことが示されています。

- 数百組に及ぶ正規のユーザー名とパスワードのペアの収集
- 悪意あるアクターが正規のユーザーとして仮想デスクトップインフラ（VDI）セッションにアクセスできた可能性のある技術的アーティファクトの収集

ASD-ACSCは、アクターが当該組織のネットワークへの侵害をさらに拡大しようとしていたと判断しています。アクターが持ち出したアーティファクトにより、正規ユーザーとして、場合によっては管理者を含む任意のユーザーになりすまして、仮想デスクトップセッションを乗っ取ったり開始したりできた可能性があります。アクターは、このアクセス経路を利用して組織のサービスをさらに侵害し、永続的なアクセスやその他の目的を達成しようとした可能性があります。

ホスティングプロバイダーが管理する環境内にある当該組織の他のアプライアンスには、侵害の証拠は確認されませんでした。

アクセス

侵害されたアプライアンスが設置されていたホストは、Active Directoryおよびウェブサーバーを通じて、VDIセッションに接続するユーザーに対する認証を提供していました（T1021.001）。

場所	侵害されたアプライアンスのホスト名（ロードバランシング構成）
データセンター1	HOST1、HOST2、HOST3

このアプライアンスのインフラには、ユーザーがアプライアンスで生成・ダウンロードした認証トークンを取得した後に、VDIへのトンネル接続を提供するアクセスゲートウェイホストも含まれていました。

これらのホストに関しては、侵害の証拠は確認されませんでした。しかし、アクセスゲートウェイホストのログには、既知の悪意あるIPアドレスとの重大な通信の証拠が確認されました。これは、おそらく当該ホスト上で発生した活動、またはこのホストに到達した脅威アクターのインフラとのネットワーク接続を反映したものであると考えられます。この活動の性質は、入手可能な証拠からは特定できませんでしたが、当該グループが組織のネットワーク内での水平展開（TA0008）を試みていたことを示しています。

内部ホスト

ASD-ACSCは、当該組織の内部ネットワークセグメントから得られた限られたデータを調査しました。当該組織の内部ネットワークセグメントに影響を与えたことが分かっている試行または成功した悪意ある活動には、アクターによるVDI関連アーティファクトへのアクセス、内部SQLサーバーのスクレイピング（T1505.001）、および既知の悪意あるIPアドレスからアクセスポイントのゲートウェイアプライアンスを経由して発生した原因不明の通信（TA0011）が含まれます。

当該グループは、侵害されたアプライアンスへのアクセスを利用して、正規のユーザー名、パスワード（T1003）、およびMFAトークンの値（T1111）を収集しました。当該グループは、仮想デスクトップのログインセッションを作成するために使用された認証アーティファクトであるJSON Web Token（JWT）（T1528）も収集していました。アクターは、これらの情報を利用して仮想デスクトップセッションを新たに作成したり、既存のセッションを乗っ取ったりすることで

(T1563.002)、正規ユーザーになりすまして当該組織の内部ネットワークセグメントへアクセスできた可能性があります(T1078)。

アクターはまた、侵害されたアプライアンスへのアクセスを利用して、組織の内部ネットワーク内に存在するSQLサーバーをスクレイピング(T1505.001)しました。アクターがこのデータにアクセスしていた可能性が高いと考えられます。

アクセスゲートウェイアプライアンスから得られた証拠から、既知の悪意あるIPアドレスから、このデバイスを経由または宛先とするネットワークトラフィックが発生していたことが確認されました。上述のとおり、これは悪意あるサイバーアクターがこのデバイスに影響を与えた、あるいは利用した可能性を示しており、内部ネットワークへ侵入するための足掛かりとされた可能性があります。

調査タイムライン

以下は、調査で判明した主な活動のタイムラインです。

時期	事象
2022年4月	既知の悪意あるIPアドレスが、アクセスゲートウェイホスト「HOST7」と通信。その通信の性質は特定できなかった。
2022年4月	すべてのホスト(HOST1、HOST2、HOST3)が悪意あるアクターによって侵害され、各ホストにウェブシェルが設置される。 HOST2上でログファイルが作成または改ざんされる。このファイルには、悪意あるアクターによって取得された可能性のある認証情報が含まれていた。 HOST1およびHOST3において、/etc/security/opasswdファイルおよび/etc/shadowファイルが改ざんされており、パスワードが変更されたことを示している。HOST1上の証拠から、「sshuser」ユーザーのパスワードが変更されたことが示唆される。
2022年4月	HOST2が当該組織によって閉鎖される。 追加のウェブシェル(T1505.003)がHOST1およびHOST3上に作成される。HOST1が、HOST3からのSSHブルートフォース攻撃を受ける。 HOST3上でログファイルが改ざんされる(T1070)。このファイルには、悪意あるアクターによって取得された可能性のある認証情報が含まれている(T1078)。 JWTが取得され(T1528)、HOST3上のファイルに出力される。 HOST3が当該組織によって閉鎖される。この時点以降のすべての活動はHOST1上で発生。
2022年4月	追加のウェブシェル(T1505.003)がHOST1に作成される。JWTが取得され、HOST1上のファイルに出力される。
2022年4月	追加のウェブシェルがHOST1に作成され(T1505.003)、既知の悪意あるIPアドレスが同ホストと通信する(TA0011)。 既知の悪意あるIPアドレスがアクセスゲートウェイホスト「HOST7」と通信する。
2022年5月	既知の悪意あるIPアドレスがアクセスゲートウェイホスト「HOST7」と通信する(TA0011)。 HOST1上のログにおいて、あるユーザーの認証イベントが既知の悪意あるIPアドレスと関連付けられる。追加のウェブシェルがこのホスト上に作成される(T1505.003)。
2022年5月	HOST1上のスクリプトがアクターによって改ざんされる(T1543)。このスクリプトには、内部SQLサーバーからデータをスクレイピングする機能が含まれている。
2022年5月	HOST1上の追加のログファイルが最後に改ざんされる(T1070)。このファイルには、組織ネットワークの正規のものであると考えられるユーザー名とパスワードの組み合わせが含まれている(T1078)。
2022年5月	追加のログファイルが最後に改ざんされる(T1070)。このファイルには、HOST1から取得されたJWTが含まれている。
2022年5月	追加のウェブシェル(T1505.003)がHOST1に作成される。この日、当該組織が、2022年4月に作成されたウェブシェルが発見されたことをASD-ACSCに報告する。
2022年5月	HOST1上で複数のスクリプトが作成され、その中には「Log4jHotPatch.jar」という名前のものも含まれている。
2022年5月	アクセスゲートウェイホストに対して、iptables-saveコマンドが使用され、2つのオープンポートが追加される。追加されたポートは9998番と9999番(T1572)。

アクターの戦術と手法

以下に、調査で確認された複数の戦術および技術を示します。

初期アクセス

T1190 外部公開アプリケーションの悪用

同グループは、リモートアクセスログインおよびID管理製品に存在するRCE（リモートコード実行）、権限昇格、認証バイパスの脆弱性を悪用し、ネットワークへの初期アクセスを獲得した可能性が高いと考えられます。

この初期アクセス手法が最も有力と考えられる理由は、以下のとおりです。

- 当時、サーバーはこれらのCVEに対して脆弱であったこと。
- 既知のアクターインフラから、これらの脆弱性を悪用しようとする試みが確認されたこと。
- 既知の最初の内部における悪意ある活動が、悪用の試みが行われた直後に発生したこと。

実行

T1059.004 コマンドおよびスクリプトインタープリター：Unixシェル

同グループは上記の脆弱性を悪用することに成功し、影響を受けたアプライアンス上で利用可能なUnixシェルにおいてコマンドを実行できた可能性があります。アクターが実行したコマンドの詳細は、アプライアンスによってログが記録されていなかったため、把握することができません。

永続的なアクセス

T1505.003 - サーバーソフトウェアコンポーネント：ウェブシェル

アクターは、影響を受けたアプライアンス上に複数のウェブシェルを展開しました。複数の異なるアクターがウェブシェルを設置した可能性がありますが、これらのウェブシェルを実際に使用して活動を行ったのは、限られた一部のアクターだったと考えられます。ウェブシェルは、侵害されたアプライアンス上でアクターが任意のコマンドを実行することを可能にしたと考えられます。

権限の昇格

T1068 権限昇格のための悪用

得られた証拠からは、アクターが取得した権限のレベルは特定されていません。ただし、ウェブシェルを使用することで、アクターは侵害されたアプライアンス上のウェブサーバーと同等の権限を取得していたと考えられます。侵害されたアプライアンスに存在していたと考えられる脆弱性により、アクターはルート権限を取得できた可能性があります。

認証情報アクセス

T1056.003 入力の取得：ウェブポータルの取得

侵害されたアプライアンス上の証拠から、アクターが平文のまま数百件に及ぶユーザー名とパスワードの組み合わせを取得していたことが確認されており、これらは正規の資格情報であると考えられます。これらの情報は、正規の認証プロセスに何らかの改変を加え、認証情報をファイルに出力することで取得された可能性が高いと考えられます。

T1111 多要素認証の傍受

アクターは、正規のログインに対応する多要素認証（MFA）トークンの値も取得していました。これらの値も、正規の認証プロセスを改変し、ファイルに出力することで取得された可能性が高いと考えられます。MFAトークンのセキュリティを担保する一意の値を保存している「シークレットサーバー」が侵害された証拠は確認されていません。

T1040 ネットワークスニッフィング

アクターは、侵害されたアプライアンス上でHTTPトラフィックを傍受することにより、JWTを取得したと考えられます。侵害されたアプライアンス上でユーティリティ「tcpdump」が実行された証拠があり、アクターがこれを用いてJWTを取得した可能性があります。

T1539 ウェブセッションクッキーの窃取

上述のとおり、アクターはJWTを取得しており、これはウェブセッションクッキーに相当するものです。これらのJWTは、アクターがさらなるアクセスを確立するために再利用した可能性があります。

探索

T1046 ネットワークサービスの探索

侵害されたアプライアンス上で、ネットワークスキャンツール「nmap」が実行され、同じネットワークセグメント内の他のアプライアンスがスキャンされた証拠があります。これは、アクターが到達可能な他のネットワークサービスを特定し、水平展開の機会を探るために使用したと考えられます。

収集

得られた証拠からは、アクターがどのようにデータを収集したのか、また侵害されたアプライアンスや他のシステムから正確に何が収集されたのかは判明していません。しかし、アクターは侵害されたアプライアンス上のすべてのファイルにアクセスできた可能性が高く、そこには認証情報（T1003）、MFAトークンの値（T1111）、および前述のJWTも含まれていたと考えられます。

コマンド&コントロール（C2）

T1071.001 アプリケーション層プロトコル：ウェブプロトコル

アクターは、ウェブシェルをコマンド＆コントロールの手段として使用していました。ウェブシェルのコマンドは、アプライアンス上の既存のウェブサーバーを通じて、HTTPS経由で送信されていたと考えられます（T1572）。

T1001.003 データの難読化：プロトコルの偽装

アクターは、侵害したデバイスを起点として、正規のトラフィックに紛れるよう設計された攻撃を実行していました。

検知および緩和に関する推奨事項

ASD-ACSCは、ASDが策定したエッセンシャルエイトコントロールおよび関連するサイバーセキュリティインシデント緩和戦略の実施を強く推奨しています。以下に、APT40による侵入の検知および防止のために実施すべきネットワークセキュリティ対策を示します。続いて、表1にまとめた4つの主要なTTP（戦術・技術・手順）に対する具体的な緩和策を記載しています。

検知

上記で特定されたファイルの一部は、C:\Users\Public* や C:\Windows\Temp* などの場所に展開されていました。これらの場所は通常「全ユーザー書き込み可」であるため、データの書き込みに都合の良い場所といえます。つまり、Windowsに登録されているすべてのユーザーアカウントが、これらのディレクトリおよびそのサブディレクトリにアクセスできる状態です。多くの場合、これらのファイルには他のユーザーも後からアクセス可能であり、その結果、水平展開、防御回避、低権限での実行、さらにはデータ持ち出しのための準備に利用される可能性があります。

以下のシグマルールは、不審な場所からの実行を異常な活動の兆候として検知することを目的としています。いずれの場合も、悪意のある活動の確認や、攻撃者の特定には、追加の調査が必要です。

タイトル：全ユーザー書き込み可の実行 - Tempフォルダ

ID: d2fa2d71-fbd0-4778-9449-e13ca7d7505c

説明：C:\Windows\Tempからのプロセス実行を検知する。

背景：

このルールは、特にC:\Windows\Temp*からの実行を検知することを目的としています。Tempフォルダは正規のアプリケーションによって広く使用されているため、C:\Windows内の他の全ユーザー書き込み可のサブディレクトリからの実行と比べると、悪意のある活動を示す指標としての信頼性は低くなります。

SYSTEMユーザーやNETWORK SERVICEユーザーによって実行されたアプリケーションを除外することで、このルールによって検知される正規の活動の件数を大幅に減らすことができます。

これは、より高い権限レベルでの悪意ある実行については、このルールでは検知を逃す可能性があることを意味しますが、ユーザーがSYSTEM権限への昇格を試みているかどうかを確認するためには、他のルールと併用することが推奨されます。

調査：

1. このファイルの実行に直接関連する情報、たとえばユーザーコンテキスト、実行時の整合性レベル、後続のアクティビティ、およびファイルによって読み込まれたイメージなどを確認してください。
2. そのアクティビティが悪意のあるものかどうかを判断するために、ホスト上のコンテキスト・プロセス、ネットワーク、ファイル、その他の補足情報を調査してください。
3. 必要に応じて、そのファイルのコピーを取得し、リバースエンジニアリングを行うことで正規のものかどうかを確認してください。

参考文献：

https://www.elastic.co/guide/en/security/current/process-execution-from-an-unusual-directory.html

著者： ASD-ACSC
日付:2024年6月19日
ステータス：実験的
タグ:

- tlp.green
- classification.au.official
- attack.execution

ログソース：

カテゴリ：process_creation
製品: windows

検知：

```
temp：
    Image|startswith：'C:\\Windows\\Temp\\'
common_temp_path：
    Image|re|ignorecase：'C:\\Windows\\Temp\\\
    {[a-fA-F0-9]{8}-([a-fA-F0-9]{4}-){3}[a-fA-F0-9]
    {12}\}\\'
system_user：
    ユーザー：
    - 'SYSTEM'
    - 'NETWORK SERVICE'
```

dismhost:

Image|endswith: 'dismhost.exe'

known_parent:

ParentImage|endswith:

- '\\esif_uf.exe'
- '\\vmtoolsd.exe'
- '\\cwainstaller.exe'
- '\\trolleyexpress.exe'

condition: temp and not (common_temp_path or system_user or dismhost or known_parent)

偽陽性:

- 監査用の許可リストアプリケーションが、Tempフォルダから実行ファイルを実行している例が確認されています。
- Tempフォルダには、正規のセットアップアプリケーションやランチャーが多数存在するため、このルールを適用する前に、監視対象のネットワークにおいてこの動作がどの程度一般的か(および許可リストに登録可能か)を検討する価値があります。

レベル:低

タイトル:全ユーザー書き込み可の実行 - Temp以外のシステムサブディレクトリ

ID: 5b187157-e892-4fc9-84fc-aa48aff9f997

説明: Windows OSのインストール場所にあるサブディレクトリ内の「全ユーザー書き込み可」の場所からのプロセス実行を検知する。

背景:

このルールは、C:\内、特にC:\Windows*下の「全ユーザー書き込み可」のディレクトリからの実行を重点的に検知することを目的としています。ただし、C:\Windows\Tempは正規のアプリケーションによって広く利用されているため、悪意のある活動の指標としての信頼性が低く、このルールの対象からは除外されています。

AppDataフォルダについては、ファイルがSYSTEM権限で実行された場合は除外されます。これは、多くの一時的なアプリケーションファイルが正規の手段で実行される一般的な方法であるためです。

初期のネットワークベースラインを作成し、これらの場所からの正規の実行を特定した後は、このルールが発動することはほとんどないはずです。

調査:

1. このファイルの実行に直接関連する情報、たとえばユーザーコンテキスト、実行時の整合性レベル、直後のアクティビティ、およびファイルによって読み込まれたイメージなどを確認してください。
2. そのアクティビティが悪意のあるものかどうかを判断するために、ホスト上のコンテキスト・プロセス、ネットワーク、ファイル、その他の補足情報を調査してください。
3. 必要に応じて、そのファイルのコピーを取得し、リバースエンジニアリングを行うことで正規のものかどうかを確認してください。

参考文献:

https://gist.github.com/mattifestation/5f9de750470c9e0e1f9c9c33f0ec3e56

https://www.elastic.co/guide/en/security/current/process-execution-from-an-unusual-directory.html

著者: ASD-ACSC

日付:2024年6月19日
ステータス:実験的

タグ:

- tlp.green
- classification.au.official
- attack.execution

ログソース:

カテゴリ: process_creation
製品: windows

検知:

writable_path:

Image|contains:

- ':\\$Recycle.Bin\\'
- ':\\AMD\\Temp\\'
- ':\\Intel\\'
- ':\\PerfLogs\\'
- ':\\Windows\\addins\\'
- ':\\Windows\\appcompat\\'
- ':\\Windows\\apppatch\\'
- ':\\Windows\\AppReadiness\\'
- ':\\Windows\\bcastdvr\\'
- ':\\Windows\\Boot\\'
- ':\\Windows\\Branding\\'
- ':\\Windows\\CbsTemp\\'
- ':\\Windows\\Containers\\'
- ':\\Windows\\csc\\'
- ':\\Windows\\Cursors\\'
- ':\\Windows\\debug\\'
- ':\\Windows\\diagnostics\\'
- ':\\Windows\\DigitalLocker\\'
- ':\\Windows\\dot3svc\\'
- ':\\Windows\\en-US\\'
- ':\\Windows\\Fonts\\'
- ':\\Windows\\Globalization\\'
- ':\\Windows\\Help\\'
- ':\\Windows\\IdentityCRL\\'
- ':\\Windows\\IME\\'
- ':\\Windows\\ImmersiveControlPanel\\'

- ':\\Windows\\INF\\'
- ':\\Windows\\intel\\'
- ':\\Windows\\L2Schemas\\'
- ':\\Windows\\LiveKernelReports\\'
- ':\\Windows\\Logs\\'
- ':\\Windows\\media\\'
- ':\\Windows\\Migration\\'
- ':\\Windows\\ModemLogs\\'
- ':\\Windows\\ms\\'
- ':\\Windows\\OCR\\'
- ':\\Windows\\panther\\'
- ':\\Windows\\Performance\\'
- ':\\Windows\\PLA\\'
- ':\\Windows\\PolicyDefinitions\\'
- ':\\Windows\\Prefetch\\'
- ':\\Windows\\PrintDialog\\'
- ':\\Windows\\Provisioning\\'
- ':\\Windows\\Registration\\CRMLog\\'
- ':\\Windows\\RemotePackages\\'
- ':\\Windows\\rescache\\'
- ':\\Windows\\Resources\\'
- ':\\Windows\\SchCache\\'
- ':\\Windows\\schemas\\'
- ':\\Windows\\security\\'
- ':\\Windows\\ServiceState\\'
- ':\\Windows\\servicing\\'
- ':\\Windows\\Setup\\'
- ':\\Windows\\ShellComponents\\'
- ':\\Windows\\ShellExperiences\\'
- ':\\Windows\\SKB\\'
- ':\\Windows\\TAPI\\'
- ':\\Windows\\Tasks\\'
- ':\\Windows\\TextInput\\'
- ':\\Windows\\tracing\\'
- ':\\Windows\\Vss\\'
- ':\\Windows\\WaaS\\'
- ':\\Windows\\Web\\'
- ':\\Windows\\wlansvc\\'
- ':\\Windows\\System32\\Com\\dmp\\'
- ':\\Windows\\System32\\FxsTmp\\'
- ':\\Windows\\System32\\Microsoft\\Crypto\\RSA\\MachineKeys\\'
- ':\\Windows\\System32\\Speech\\'
- ':\\Windows\\System32\\spool\\drivers\\color\\'
- ':\\Windows\\System32\\spool\\PRINTERS\\'
- ':\\Windows\\System32\\spool\\SERVERS\\'
- ':\\Windows\\System32\\Tasks_Migrated\\Microsoft\\Windows\\PLA\\System\\'
- ':\\Windows\\System32\\Tasks\\'
- ':\\Windows\\SysWOW64\\Com\\dmp\\'
- ':\\Windows\\SysWOW64\\FxsTmp\\'
- ':\\Windows\\SysWOW64\\Tasks\\'

appdata:

Image|contains: '\\AppData\\'
ユーザー: 'SYSTEM'

condition: writable_path and not appdata

偽陽性:

監査用の許可リストアプリケーションが、これらのディレクトリから実行ファイルを実行している例が確認されています。

監視対象の環境においては、スクリプトや管理ツールがこれらのディレクトリのいずれかに配置されている可能性があり、その場合は個別に対応する必要があります。

レベル: 高

タイトル:全ユーザー書き込み可の実行 - Usersフォルダ

ID: 6dda3843-182a-4214-9263-925a80b4c634

説明: C:\Users\Public* および Users フォルダ内のその他の「全ユーザー書き込み可」のフォルダからのプロセス実行を検知する。

背景:

AppDataフォルダについては、ファイルがSYSTEM権限で実行される場合は除外されます。これは、多くの一時的なアプリケーションファイルが正規の手段で実行される一般的な方法であるためです。

調査:

1. このファイルの実行に直接関連する情報、たとえばユーザーコンテキスト、実行時の整合性レベル、直後のアクティビティ、およびファイルによって読み込まれたイメージなどを確認してください。
2. そのアクティビティが悪意のあるものかどうかを判断するために、ホスト上のコンテキスト・プロセス、ネットワーク、ファイル、その他の補足情報を調査してください。
3. 必要に応じて、そのファイルのコピーを取得し、リバースエンジニアリングを行うことで正規のものかどうかを確認してください。

参考文献:

https://www.elastic.co/guide/en/security/current/process-execution-from-an-unusual-directory.html

著者: ASD-ACSC
日付: 2024年6月19日
ステータス: 実験的
タグ:

- tlp.green
- classification.au.official
- attack.execution

ログソース:

カテゴリ: process_creation
製品: windows

検知：

ユーザー：

Image|contains:

- ':\\Users\\All Users\\'
- ':\\Users\\Contacts\\'
- ':\\Users\\Default\\'
- ':\\Users\\Public\\'
- ':\\Users\\Searches\\'

appdata：

Image|contains: '\\AppData\\'
ユーザー：'SYSTEM'

condition: users and not appdata

偽陽性：

- 監視対象の環境においては、スクリプトや管理ツールがPublic フォルダやそのサブディレクトリに配置されている可能性があり、その場合は個別に対応する必要があります。

レベル：中

緩和策

ロギング

ASD-ACSCによる調査において、調査の効果や迅速さを損なう一般的な要因の一つは、ウェブサーバーのリクエストログ、Windowsイベントログ、インターネットプロキシログなど、複数の領域における包括的かつ過去のログ情報が不足していることです。

ASD-ACSCは、「Windowsイベントログの記録および転送」に関するガイダンスの確認と実装を推奨しています。これには、「Windows Event Logging Repository」にある設定ファイルやスクリプト、そして「情報セキュリティマニュアル（ISM）」の「システム監視に関するガイドライン」が含まれます。これらのガイダンスは、ログの集約や適切な期間のログ保管を含む内容となっています。

パッチ管理

ウェブサーバー、ウェブアプリケーション、リモートアクセスゲートウェイなど、インターネットに直接接続されたすべてのデバイスやサービスに、速やかにパッチを適用してください。プロセスの自動化と迅速化のために、集中型のパッチ管理システムの導入を検討してください。ASDのACSCは、「情報セキュリティマニュアル（ISM）」の「システム管理に関するガイドライン」、特に「システムへのパッチ適用」に関する対策を推奨しています。

アクターが使用したほとんどのエクスプロイトは公開されているものであり、既にパッチや緩和策が提供されていました。組織は、インターネットに接続されているインフラに対して、セキュリティパッチや緩和策を48時間以内に適用するよう確認し、可能な限り最新バージョンのソフトウェアやオペレーティングシステムを使用するべきです。

ネットワーク・セグメンテーション

ネットワークをセグメント化することで、攻撃者が組織の機密データを特定し、アクセスすることが著しく困難になります。ネットワークをセグメント化し、必要な場合を除いてコンピュータ間の通信を遮断することで、水平展開を制限または阻止してください。Active Directoryやその他の認証サーバーなどの重要なサーバーは、限られた数の中継サーバーや「ジャンプサーバー」からのみ管理できるようにするべきです。これらのサーバーは、厳重な監視と十分なセキュリティ対策を施すとともに、接続を許可するユーザーやデバイスを限定する必要があります。

水平展開が阻止された事例があったとしても、さらなるネットワーク・セグメンテーションを実施していれば、アクターがアクセス・取得できたデータの量をさらに制限できた可能性があります。

追加の緩和策

本勧告作成機関は、APT40およびその他の攻撃者による以下のTTPへの対策として、以下の緩和策も推奨しています。

- 使用していない、または不要なネットワークサービス、ポート、プロトコルは無効化してください。
- ウェブサーバーやアプリケーションを保護するために、適切にチューニングされたウェブアプリケーションファイアウォール（WAF）を使用してください。
- サーバー、ファイル共有、その他のリソースへのアクセスを制限するために、最小権限の原則を徹底してください。
- 認証情報のクラックや再利用を困難にするために、多要素認証（MFA）やマネージドサービスアカウントを活用してください。MFAは、以下を含む、インターネットでアクセス可能なすべてのリモートアクセスサービスに適用してください。
  - ウェブおよびクラウドベースのメール
  - コラボレーションプラットフォーム
  - 仮想プライベートネットワーク接続
  - リモートデスクトップサービス
- サポートが終了した機器は交換してください。

表1：緩和策／手法

TTP	エッセンシャルエイト緩和策	ISM管理策
初期アクセス T1190 公開アプリケーションの悪用	パッチの適用 オペレーティングシステムへのパッチ適用 多要素認証 アプリケーション制御	ISM-0140 ISM-1698 ISM-1701 ISM-1921 ISM-1876 ISM-1877 ISM-1905
実行 T1059 コマンドおよびスクリプトインタープリター	アプリケーション制御 Microsoft Officeマクロの制限 管理者権限の制限	ISM-0140 ISM-1490 ISM-1622 ISM-1623 ISM-1657 ISM-1890
永続的なアクセス T1505.003 サーバーソフトウェアコンポーネント：ウェブシェル	アプリケーション制御 管理者権限の制限	ISM-0140 ISM-1246 ISM-1746 ISM-1249 ISM-1250 ISM-1490 ISM-1657 ISM-1871
初期アクセス／権限昇格／永続化 T1078 有効なアカウント	オペレーティングシステムへのパッチ適用 多要素認証 管理者権限の制限 アプリケーション制御 ユーザーアプリケーションの強化	ISM-0140 ISM-0859 ISM-1546 ISM-1504 ISM-1679

追加の一般的な検知および緩和策については、本勧告の末尾にあるMITRE ATT&CKのサマリーで特定された各手法に対応する、MITRE ATT&CK公式サイトの「Mitigations and Detection（緩和策および検知）」セクションをご参照ください。

免責事項

本報告書に記載されている情報は、あくまで情報提供のみを目的として「現状のまま」提供されるものです。本勧告作成機関は、本文書内でリンクされている団体、製品、サービスを含め、いかなる営利団体、製品、企業、サービスについても、それを推奨・支持するものではありません。サービスマーク、商標、製造業者名その他の方法によって、特定の商業団体、製品、プロセス、またはサービスへの言及がなされている場合であっても、それは本勧告作成機関による支持、推奨、または支持を意味するものではありません。

本書はTLP:CLEARに分類されています。開示に制限はありません。TLP:CLEARは、情報の悪用リスクが最小限またはほぼない場合に、公開に関する適用ルールや手続きに従って使用することができます。標準的な著作権規定に従う限り、TLP:CLEARの情報は制限なく配布することができます。トラフィックライトプロトコル（TLP）に関する詳細は、cisa.gov/tlpをご参照ください。

MITRE ATT&CK — 注目すべきAPT40の過去の攻撃手法

情報収集活動（TA0043）	
被害者が所有するウェブサイトの検索（T1594）	被害者の身元情報を収集する：認証情報（T1589.001）
アクティブスキャン：脆弱性スキャン（T1595.002）	被害者ホスト情報の収集（T1592）
公開ウェブサイト／ドメインの検索：検索エンジン（T1593.002）	被害者ネットワーク情報の収集：ドメインプロパティ（T1590.001）
被害者の身元情報を収集する：メールアドレス（T1589.002）	

リソース開発（TA0042）	
インフラの取得：ドメイン（T1583.001）	インフラの取得（T1583）
インフラの取得：DNSサーバー（T1583.002）	アカウントの侵害（T1586）
攻撃能力の開発：コード署名証明書（T1587.002）	インフラの侵害（T1584）
攻撃能力の開発：デジタル証明書（T1587.003）	攻撃能力の開発：マルウェア（T1587.001）
能力の取得：コード署名証明書（T1588.003）	アカウントの作成：クラウドアカウント（T1585.003）
インフラの侵害：ネットワークデバイス（T1584.008）	能力の取得：デジタル証明書（T1588.004）

初期アクセス（TA0001）	
有効なアカウント（T1078）	フィッシング（T1566）
有効なアカウント：デフォルトアカウント（T1078.001）	フィッシング：スピアフィッシング添付ファイル（T1566.001）
有効なアカウント：ドメインアカウント（T1078.002）	フィッシング：スピアフィッシングリンク（T1566.002）
外部リモートサービス（T1133）	外部公開アプリケーションの悪用（T1190）
ドライブバイ型侵害（T1189）	

実行（TA0002）	
Windows Management Instrumentation（T1047）	コマンドおよびスクリプトインタープリター：Python（T1059.006）
スケジュールされたタスク／ジョブ：At（T1053.002）	コマンドおよびスクリプトインタープリター：JavaScript（T1059.007）
スケジュールされたタスク／ジョブ：スケジュールされたタスク（T1053.005）	ネイティブAPI（T1106）
コマンドおよびスクリプトインタープリター（T1059）	プロセス間通信（T1559）
コマンドおよびスクリプトインタープリター：Windowsコマンドシェル（T1059.003）	システムサービス：サービス実行（T1569.002）
コマンドおよびスクリプトインタープリター：PowerShell（T1059.001）	クライアント実行のための悪用（T1203）
コマンドおよびスクリプトインタープリター：Visual Basic（T1059.005）	ユーザーによる実行：悪意のあるファイル（T1204.002）
コマンドおよびスクリプトインタープリター：Unixシェル（T1059.004）	コマンドおよびスクリプトインタープリター：AppleScript（T1059.002）
スケジュールされたタスク／ジョブ：Cron（T1053.003）	ソフトウェア展開ツール（T1072）

永続的なアクセス（TA0003）	
有効なアカウント（T1078）	サーバーソフトウェアコンポーネント：ウェブシェル（T1505.003）
Officeアプリケーションのスタートアップ：Officeテンプレートマクロ（T1137.001）	システムプロセスの作成または変更：Windowsサービス（T1543.003）
スケジュールされたタスク／ジョブ：At（T1053.002）	起動またはログオン時の自動実行：レジストリのRunキー／スタートアップフォルダ（T1547.001）
スケジュールされたタスク／ジョブ：スケジュールされたタスク（T1053.005）	起動またはログオン時の自動実行：ショートカットの改ざん（T1547.009）
外部リモートサービス（T1133）	実行フローのハイジャック：DLL検索順序のハイジャック（T1574.001）
スケジュールされたタスク／ジョブ：Cron（T1053.003）	実行フローのハイジャック：DLLサイドローディング（T1574.002）
アカウント操作（T1098）	有効なアカウント：クラウドアカウント（T1078.004）
有効なアカウント：ドメインアカウント（T1078.002）	

権限の昇格（TA0004）	
スケジュールされたタスク／ジョブ：At（T1053.002）	システムプロセスの作成または変更：Windowsサービス（T1543.003）
スケジュールされたタスク／ジョブ：スケジュールされたタスク（T1053.005）	起動またはログオン時の自動実行：レジストリのRunキー／スタートアップフォルダ（T1547.001）
プロセスインジェクション：スレッド実行のハイジャック（T1055.003）	起動またはログオン時の自動実行：ショートカットの改ざん（T1547.009）
プロセスインジェクション：プロセスホロウイング（T1055.012）	実行フローのハイジャック：DLL検索順序のハイジャック（T1574.001）

権限の昇格（TA0004）	
有効なアカウント：ドメインアカウント（T1078.002）	権限昇格のための悪用（T1068）
アクセストークンの操作：トークンのなりすまし／窃取（T1134.001）	イベントトリガーによる実行：Unixシェル設定の改ざん（T1546.004）
プロセスインジェクション：ダイナミックリンクライブラリ・インジェクション（T1055.001）	有効なアカウント：ドメインアカウント（T1078.002）
有効なアカウント：ローカルアカウント（T1078.003）	

防御回避（TA0005）	
ルートキット（T1014）	間接的なコマンド実行（T1202）
難読化されたファイルまたは情報（T1027）	システムバイナリのプロキシ実行：Mshta（T1218.005）
難読化されたファイルまたは情報：ソフトウェアパッキング（T1027.002）	システムバイナリのプロキシ実行：Regsvr32（T1218.010）
難読化されたファイルまたは情報：ステガノグラフィ（T1027.003）	信頼制御の回避：コード署名（T1553.002）
難読化されたファイルまたは情報：納品後のコンパイル（T1027.004）	ファイルおよびディレクトリの権限変更：Linuxおよび Macのファイル・ディレクトリ権限の変更（T1222.002）
偽装：正規の名称または場所の模倣（T1036.005）	仮想化／サンドボックス回避：システムチェック（T1497.001）
プロセスインジェクション：スレッド実行のハイジャック（T1055.003）	偽装（T1036）
リフレクティブコードローディング（T1620）	防御機能の無効化：システムファイアウォールの無効化または変更（T1562.004）
プロセスインジェクション：プロセスホロウイング（T1055.012）	アーティファクトを隠す：隠しファイルおよびディレクトリ（T1564.001）
インジケーターの除去：ファイルの削除（T1070.004）	アーティファクトを隠す：隠しウィンドウ（T1564.003）
インジケーターの除去：タイムスタンプ改ざん（T1070.006）	実行フローのハイジャック：DLL検索順序のハイジャック（T1574.001）
インジケーターの除去：Windowsイベントログの消去（T1070.001）	実行フローのハイジャック：DLLサイドローディング（T1574.002）
レジストリの改ざん（T1112）	ウェブサービス（T1102）
ファイルまたは情報の難読化解除・デコード（T1140）	偽装：タスクまたはサービスの偽装（T1036.004）
防御機能の妨害（T1562）	

認証情報アクセス（TA0006）	
OS認証情報ダンピング：LSASSメモリ（T1003.001）	保護されていない認証情報：ファイル内の認証情報（T1552.001）
OS認証情報ダンピング：NTDS（T1003.003）	ブルートフォース攻撃：パスワード推測（T1110.001）
ネットワークスニッフィング（T1040）	強制認証（T1187）

認証情報アクセス（TA0006）	
パスワードストアからの認証情報取得：キーチェーン（T1555.001）	Kerberosチケットの窃取または偽造：Kerberoasting（T1558.003）
入力の取得：キー入力記録（T1056.001）	多要素認証の傍受（T1111）
ウェブセッションクッキーの窃取（T1539）	アプリケーションアクセストークンの窃取（T1528）
認証情報アクセスのための悪用（T1212）	ブルートフォース攻撃：パスワードクラッキング（T1110.002）
入力の取得：ウェブポータルの取得（T1056.003）	OS認証情報ダンピング：DCSync（T1003.006）
パスワードストアからの認証情報取得（T1555）	パスワードストアからの認証情報取得：ウェブブラウザからの認証情報の取得（T1555.003）

探索（TA0007）	
システムサービスの探索（T1007）	システム情報の探索（T1082）
アプリケーションウィンドウの探索（T1010）	アカウントの探索：ローカルアカウント（T1087.001）
レジストリの照会（T1012）	システム情報の探索、技術（T1082）- エンタープライズ	MITRE ATT&CK®
ファイルおよびディレクトリの探索（T1083）	システム時刻の探索（T1124）
ネットワークサービスの探索（T1046）	システムの所有者／ユーザーの探索（T1033）
リモートシステムの探索（T1018）	ドメイントラストの探索（T1482）
アカウントの探索：メールアカウント（T1087.003）	アカウントの探索：ドメインアカウント（T1087.002）
システムネットワーク接続の検出（T1049）	仮想化／サンドボックス回避：システムチェック（T1497.001）
プロセスの探索（T1057）	ソフトウェアの探索（T1518）
権限グループの探索：ドメイングループ（T1069.002）	ネットワーク共有の探索、技術（T1135） - エンタープライズ	MITRE ATT&CK®
システムのネットワーク構成の探索：インターネット接続の探索（T1016.001）	

水平展開（TA0008）	
リモートサービス：リモートデスクトッププロトコル（T1021.001）	リモートサービス（T1021）
リモートサービス：SMB/Windows管理者共有（T1021.002）	代替認証情報の使用：Pass the Ticket（T1550.003）
リモートサービス：Windows Remote Management（1021.006）	ラテラルツール転送（T1570）

収集（TA0009）	
ローカルシステムからのデータ（T1005）	収集データのアーカイブ：ライブラリを使用したアーカイブ（T1560.002）
ネットワーク共有ドライブからのデータ（T1039）	メールの収集リモートメール収集（T1114.002）

収集（TA0009）	
入力の取得：キー入力記録（T1056.001）	クリップボードデータ（T1115）
自動化された収集（T1119）	情報リポジトリからのデータ（T1213）
入力の取得：ウェブポータルの取得（T1056.003）	データのステージング：リモートデータステージング（T1074.002）
データのステージング：ローカルデータステージング（T1074.001）	収集データのアーカイブ（T1560）
メールの収集（T1114）	

データ流出（TA0010）	
C2チャネル経由のデータ流出（T1041）	代替プロトコル経由のデータ流出：非C2プロトコルの非対称暗号化通信によるデータ流出（T1048.002）
代替プロトコル経由のデータ流出（T1048）	ウェブサービス経由のデータ流出：クラウドストレージへの流出（T1567.002）

コマンド&コントロール（TA0011）	
データの難読化：プロトコルの偽装（T1001.003）	ウェブサービス：デッドドロップリゾルバ（T1102.001）
一般的に使用されるポート（T1043）	ウェブサービス：一方向通信（T1102.003）
アプリケーション層プロトコル：ウェブプロトコル（T1071.001）	イングレスツール転送（T1105）
アプリケーション層プロトコル：ファイル転送プロトコル（T1071.002）	プロキシ：内部プロキシ（T1090.001）
プロキシ：外部プロキシ（T1090.002）	非標準ポート（T1571）
プロキシ：マルチホッププロキシ（T1090.003）	プロトコルトンネリング（T1572）
ウェブサービス：双方向通信（T1102.002）	暗号化チャネル（T1573）
暗号化チャネル：非対称暗号（T1573.002）	イングレスツール転送（T1105）
プロキシ、技術（T1090） - エンタープライズ | MITRE ATT&CK®	

インパクト（TA0040）	
サービス停止（T1489）	ディスクワイプ（T1561）
システムのシャットダウン/再起動（T1529）	リソースのハイジャック（T1496）

備考

免責事項

このガイドブックの内容は一般的なものであり、特定の事情や緊急事態においては 法的な助言や依存すべき助言とみなされるべきものではありません。重要な事柄については、独立した専門家からご自身の状況に則した適切な助言を仰ぐべきです。

このガイドブックに含まれる情報に依存した結果生じた損害、損失や費用に対して豪連邦政府はいかなる責任も負いません。

著作権

豪連邦政府紋章の使用について

豪連邦政府紋章の使用が許される条件については首相内閣省ホームページに掲載の「連邦政府の紋章に関する情報および指針」(pmc.gov.au)に詳述があります。

さらに詳細な情報について、またはサイバーセキュリティ事件の報告は以下まで連絡してください。

cyber.gov.au | 1300 CYBER1 (1300 292 371)

この電話番号はオーストラリア国内でのみご利用いただけます。

ASD AUSTRALIAN SIGNALS DIRECTORATE

ACSC Australian Cyber Security Centre