APT40に関するアドバイザリー
中国MSSが実行している手法・技術

cyber.gov.au


Australian Government
Australian Signals Directorate


ASD
AUSTRALIAN SIGNALS DIRECTORATE
ACSC


CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY
CISA


NATIONAL SECURITY AGENCY
UNITED STATES OF AMERICA


DEPARTMENT OF JUSTICE
FEDERAL BUREAU OF INVESTIGATION


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


National Cyber Security Centre
PART OF THE GCSB


Bundesnachrichtendienst


Bundesamt für Verfassungsschutz


국가정보원
NATIONAL INTELLIGENCE SERVICE


국가사이버안보센터
NCSC
NATIONAL CYBER SECURITY CENTER


NISC
内閣サイバーセキュリティセンター
National center of Incident readiness and Strategy for Cybersecurity


警察庁
National Police Agency

目次

概要

背景

豪州通信電子局（ASD）・豪州サイバーセキュリティセンター（ACSC）、米国土安全保障省サイバーセキュリティ・インフラ庁（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）及び連邦憲法擁護庁（BfV）、韓国国家情報院（NIS）及びNISのサイバーセキュリティセンター、内閣サイバーセキュリティセンター（NISC）及び警察庁（NPA）（以降、「署名組織」とする）が作成した本アドバイザリーでは、中国の国家的な支援を受けたサイバーグループ及び当該グループがオーストラリアのネットワークに対して現在与えている脅威について概説する。本アドバイザリーは、ASD・ACSCのインシデント対応における調査、及び署名組織の当該脅威に対する共通の理解に基づいている。

中国の国家的な支援を受けたサイバーグループは、過去にもオーストラリア、米国を含む各国の組織を標的としており、以下に記載する技術は、中国の支援を受けた他のアクターによって世界中でたびたび使用されている。このため、署名組織は、このグループ及び同様の技術が依然として自国のネットワークへの脅威にもなっているとみている。

署名組織は、当該グループが中国国家安全部（MSS）と関係しているとみている。グループの活動及び技術は、高度標的型攻撃（APT）40であることが確認されているグループ（業界の報告書ではKryptonite Panda、GINGHAM TYPHOON、Leviathan及びBronze Mohawkとしても知られる）のものと重複している。当該グループは、過去に、中国海南省海口市を拠点に活動し、国家安全部海南支部から業務を請け負っているとされていた。[1]

以下のアドバイザリーでは、攻撃を受けた2つのネットワークに対するこの攻撃者の技術について、重要なケーススタディのサンプルを提供する。サイバーセキュリティの専門家にとって、これらのケーススタディは自国のネットワークに対するAPT40の侵入の特定、防止、および改善措置において重要である。選ばれたケーススタディでは、当該グループ又は他のグループによる再攻撃のリスクを軽減するための適切な改善措置が講じられている。故に、組織の改善措置に必要な時間を経ているため、これらは本質的に新しいケーススタディではない。

活動概要

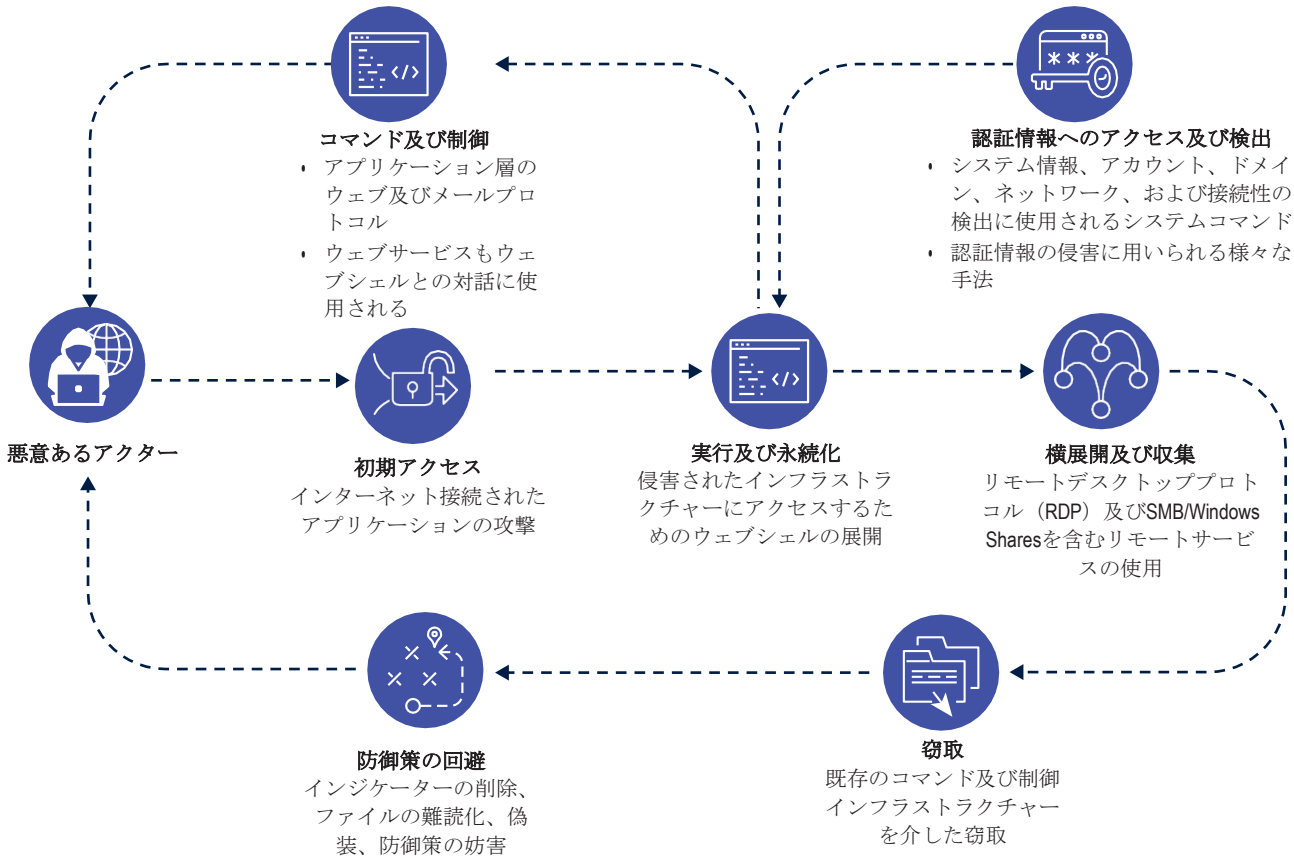
APT40は度々オーストラリアのネットワーク、政府及び地域の民間セクターのネットワークを標的としており、APT40が国内のネットワークに与える脅威は現在も進行中である。本アドバイザリーで説明されている手法・技術（以下「トレードクラフト」と記載）は、オーストラリアのネットワークに対して頻繁に行われていることが観測されている。

とりわけ、APT40は新しい脆弱性の概念実証エクスプロイト（POC）を迅速に変換・適応させ、関連する脆弱なインフラを持つネットワークを標的として即座に利用する能力を有している。APT40は、署名組織の国家のネットワークを含む関心の対象のネットワークに対する偵察を定期的に実施し、標的を侵害する機会を伺っている。この定期的な偵察は、関心の対象のネットワーク上にある脆弱な機器、サポートが終了した機器又は保守が行われていない機器を特定し、素早く不正なコードを展開する。APT40は、脆弱性の悪用に遅くとも2017年から成功し続けている。

APT40は、Log4J（CVE-2021-44228）、アトラシアンのConfluence（CVE-2021-31207、CVE-2021-26084）、及びMicrosoft Exchange（CVE-2021-31207、CVE-2021-34523、CVE-2021-34473）など、一般に使用されているソフトウェアに含まれる新しく公開された脆弱性を素早く悪用する。ACSC及び署名組織は、注目度の高い新規の脆弱性が公開されると、数時間又は数日以内に、当該脆弱性に対するPOCをグループが継続して使用すると予想している。

1 米国司法省、2021年Four Chinese Nationals Working with the Ministry of State Security Charged with Global Computer Intrusion Campaign Targeting Intellectual Property and Confidential Business Information, Including Infectious Disease Research.

図1APT40による活動のTTPフローチャート



当該グループは、フィッシングキャンペーンといったユーザーの介在が必要な技術よりも、インターネット接続された脆弱なインフラの悪用を選択しているとみられ、続く活動を可能にするための有効な認証情報の獲得に高い優先度を置いているとみられる。APT40は、特に侵入のライフサイクルの初期段階で、永続化のためのウェブシェル（T1505.003）を度々使用する。通常、最初のアクセスに成功すると、APT40は被害を受けた環境へのアクセスを維持するための永続化に焦点を当てる。しかしながら、侵入の初期段階で発生するため、侵害の度合い又は実施された活動に関わらず、永続化はすべての侵入において観測される傾向が強い。

顕著なトレードクラフト

APT40は過去に、侵害されたオーストラリアのウェブサイトを制御用のコマンド及び制御（C2）サーバとして利用してきたが、同グループは当該技術（T1594）を進化させている。

APT40は、オーストラリア国内での活動において、小規模オフィス・家庭用機器（SOHO機器）を含む侵害された機器を攻撃インフラ及びラストホップリダイレクターとして利用する（T1584.008）という世界的なトレンドを取り入れている。これにより、署名組織は当該グループの動きの特性をより明らかにすることができた。

これらのSOHO機器の多くは、サポートが終了している機器又はパッチがあてられていない機器であり、Nデイ攻撃のためのソフトターゲットとなる。一度侵害されたSOHO機器は、正当なトラフィックに紛れてネットワーク防御を困難にする攻撃（T1001.003）の拠点となる。

また、この技術は、世界中で中国の国家の支援を受ける他のアクターにも度々使用されており、署名組織は当該技術を共有された脅威と見なしている。詳細については、共同アドバイザリー「People’s Republic of China State-Sponsored Cyber Actors Exploit Network Providers and Devices」及び「PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure」を参照すること。

APT40は、被害者側に公開される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があるが、このようなトレードクラフトは相対的に衰退しているとみられる。

ツール

ASD・ACSCは、以下に概説する調査によって特定された悪意あるファイルの一部を共有する。幅広いネットワーク防衛コミュニティー及びサイバーセキュリティコミュニティーが防御すべき脅威についての見識を深められるようにすることを目的に、これらのファイルはVirusTotalにアップロードされている。

ケーススタディ

ASD・ACSCは、アクターがツール及びトレードクラフトをどのように使用しているのかに関する気づきを提供するために、匿名化された2つの調査報告書を共有する。

MD5	ファイル名	付加情報
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

幅広い配布を可能にするため、この報告書は匿名化されている。影響を受けた組織は、以降、「組織」とする。被害を受けた組織の特定を避けるとともに、ASD・ACSCのインシデント対応手法を保護するため、詳細事項の一部は省かれている。

概要

この報告書では、2022年の7月から9月にかけて発生した組織のネットワークの侵害に対するASD・ACSCによる調査結果について詳述する。この調査報告書は、観測された悪意ある攻撃について要約し、改善のための推奨事項をまとめるために組織に提供された。調査結果は、本侵害がAPT40によってなされたものであることを示している。

8月中旬、ASD・ACSCは、当該グループが使用する侵害されたと思われる機器からの組織のネットワークに対する不正な通信について組織に通知し、8月下旬に組織の同意を得て、組織のネットワーク上の影響を受けたと思われるホストに、ホストベースのセンサーを設置した。当該センサーは、ASD・ACSCのインシデント対応分析官による徹底したデジタルフォレンジック調査を可能にした。ASD・ACSCの分析官は、入手したセンサーデータを使って、当該グループによる攻撃のマッピングを行い、観測された事象の詳細なタイムラインの作成に成功した。

ASD・ACSCが観測した7月から8月にかけてのアクターの主な攻撃は以下の通りである。

- ホストの列挙：アクターによるネットワークの構成図の作成を可能にする
- ウェブシェルの使用：ネットワーク上にアクターの攻撃の足がかりを提供し、コマンド実行を可能にする
- アクターにより悪意ある目的で利用されるその他のツールの展開

調査により大量の機密データがアクセスされた痕跡及びアクターが同ネットワーク上で横展開を行った痕跡が明かになった（T1021.002）。侵害の大部分は、当該グループがネットワーク内への攻撃ベクトルを複数確立したこと、ネットワークが水平構造であったこと及びファイルを任意にアップロードするのに使用可能な脆弱な内製ソフトウェアを利用していたことによって容易になった。流出したデータには、当該グループによるログインが可能となる特権アカウントの認証情報や、たとえ元の攻撃ベクトルを塞いだとしても、アクターによる不正なアクセスを再度可能とするおそれのあるネットワーク情報が含まれていた。初期に侵害されたマシンからは、上記以外の悪意あるツールは発見されなかったが、これは、アクターによる正当な特権アカウントへのアクセスにより、追加のツールを必要としなかったためとみられる。調査の結果、この組織はAPT40によって意図的に標的にされた可能性が高く、既知の脆弱性によって日和見的に被害に遭ったわけではないことが判明した。

調査結果

2022年8月中旬、ASD・ACSCは、少なくとも7月から8月の間に、国家が支援するサイバーグループに関連すると思われる悪意のあるIPアドレスと組織のコンピュータネットワークが相互に通信していたことを組織に通知した。侵害された端末は、スモールビジネスユーザー又はホームユーザーが所有するものであったと考えられる。

8月下旬、ASD・ACSCは、組織のネットワーク上の侵害の影響を受けた痕跡を示したホストに、ホストベースのエージェントを配置した。

ログ設定又はネットワーク設計上の理由により、調査に有用であったと考えられるアーティファクトのいくつかは利用することができなかった。
それでも、組織による利用可能な全データの迅速な提供は、ASD・ACSCのインシデント対応者による包括的な分析及びAPT40によるネットワーク上の潜在的な攻撃の把握を可能にした。

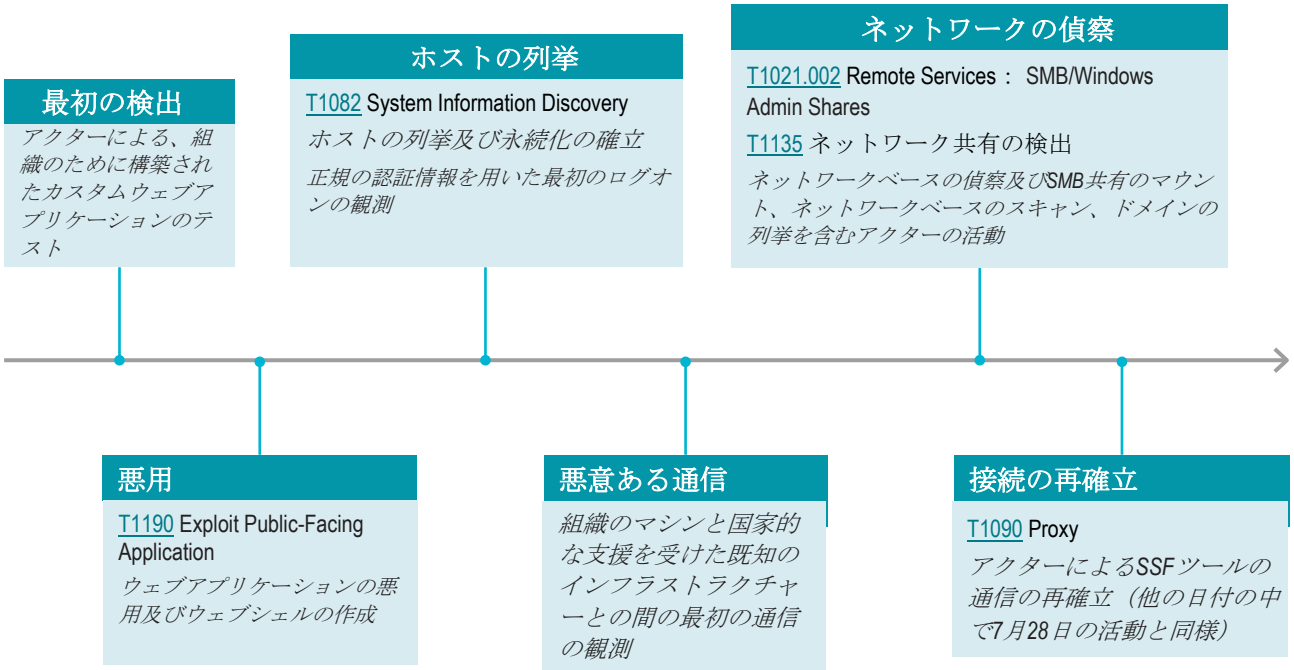
9月にASD・ACSCと相談した上で、組織はASD・ACSCからの最初の通知で特定されていたIPアドレスを拒否リストに追加することを決定した。10月に、組織は改善措置を開始した。

詳細

7月初旬、アクターは*<webapp>2-ext*上で動作しているカスタムウェブアプリケーションをテストし当該アプリケーションの悪用が可能であったため（T1190）、DMZ内に足場を築くことができた。これは同ネットワーク及び把握可能な全てのドメインを列挙するのに利用された。侵害された認証情報（T1078.002）は、アクティブディレクトリの検索（T1018）及びファイル共有のマウントによるDMZ内にある複数のマシンからのデータの窃取（T1039）に悪用された。アクターは、有効なネットワークの認証情報をサーバから取得するために、Kerberoasting攻撃を行った（T1558.003）。当該グループよる、DMZ又はその他の内部ネットワークにおける追加のポイントオブプレゼンス（POP）の獲得は観測されなかった。

視覚的な時系列

以下のタイムラインは、組織のネットワーク上で観測された悪意あるアクターによる攻撃の概観を示す。



詳細な時系列

7月：アクターが、組織のために作ら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」又は「ウェブアプリ」）のフロントページへの最初の接続（T1190）を、TLS接続を経由して確立する（T1102）。それ以外の目立った活動は観測されていない。

7月：アクターがさらなる調査のためにエンドポイント[2]を探索し、ウェブアプリケーションのウェブサイトの列挙を開始する。

7月：アクターが特定のエンドポイントを攻撃する試みに集中する。

7月：アクターが、別のページに設置したウェブシェルを経由して、ウェブサーバへの「POST」コマンドの送信に成功する。おそらく同じアクターによって用いられたと思われる2番目のIPアドレスも、おなじURLに「POST」コマンドの送信を始める。アクターは多数のウェブシェルとみられるプログラムを作成しテストした。

正確な攻撃手法は不明。しかし、*<webapp>2-ext*上にファイルを作成するために特定のエンドポイントを標的としたのは明らかである。

共通した関心および初期接続が数分違いで発生していることから、ASD・ACSCは2件のIPアドレスによる接続は同じ侵入活動の一部であるとみている。

7月：グループは、権限昇格の機会を探り、異なるウェブシェルを展開しながら、ホストの列挙を続ける。アクターは、侵害した下記の認証情報を使ってウェブアプリケーションにログインする：*<firstname.surname>@<organisation domain>*.

アクターは、活動において*<webapp>*2-extにおける権限昇格には成功しなかったと考えられる。一方で、アクターは、ネットワークベースの攻撃に方向転換した。

7月：アクターが内部でアクセス可能なバイナリにハードコーディングされていた可能性が高い侵害されたサービスアカウント[3]の認証情報をテストする。

7月：アクターは、オープンソースツールであるSSFを展開し、同ツールを使用して悪意あるインフラに接続させた。この接続は、アクターの攻撃用の端末から組織の内部のネットワークへの通信をトンネルするのに用いられる。当該端末名は、攻撃者がサービスアカウントの認証情報の使用を試みた際のイベントログに現れている。

8月：アクターは、サービスアカウントを含む接続の確立に失敗するなど限られた活動しかしていないとみられる。

8月：アクターが重要なネットワーク及びアクティブディレクトリの列挙を実施する。新たに侵害されたアカウントは、その後DMZ内のWindows端末への共有のマウント[4]に利用され、アクターによるデータ窃取を可能とした。

これは、DMZ内でマウント可能なマシンにおける、窃取認証情報の機に乗じた使用とみられる。アクターによる内部ネットワークを標的とした同様の活動はファイアウォールによりブロックされた。

8月～9月：SSFツールは再び悪意あるIPアドレスとの接続を確立した。当該グループのアクセスがブロックされるまでの間、グループが攻撃を追加で実行している様子は観測されていない。

9月：組織は、悪意あるIPアドレスを組織のファイアウォールで拒否リストに加え、当該IPアドレスをブロックする。

2 この文脈におけるエンドポイントは、ウェブアプリケーションの機能である。

3 サービスアカウントは、個別のユーザーではなく、サービスに紐づいている。マイクロソフトのコーポレートドメインには、多様な種類のアカウントがある。

4 共有のマウントは、ユーザー又はユーザーグループがアクセス可能なシステム構成へのファイル作成のプロセスである。

アクターの戦術及び技術

MITRE ATT&CKフレームワークは、脅威アクターがサイバー空間で利用する戦術と技術に関するナレッジベースである。同フレームワークは米国の非営利組織であるMITREコーポレーションによって作成され、脅威アクターの振る舞いに関する共通のグローバル言語として機能している。

ASD・ACSCは、アクターの悪意ある行動
以下の技術及び戦術に関連すると判断する。

Reconnaissance

T1594 - Search Victim-Owned Websites

アクターは、ネットワークにアクセスする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の列挙を行った。

Initial access

T1190 - Exploit Public-Facing Application （カスタムウェブアプリケーションへの攻撃に関連）

T1078.002 - Valid Accounts: Domain Accounts（侵害した認証情報でのログオンに関連）

アクターは、インターネット上に公開されたカスタムウェブアプリケーションを悪用し、最初のアクセスポイントを得た。その後、アクターは侵害した認証情報を用いて、ネットワークへのアクセスをさらに進めることができた。

Execution

T1059 - Command and Scripting Interpreter（ウェブシェルを介したコマンドの実行に関連）

T1072 - Software Deployment Tools（アクターがオープンソースツール「Secure Socket Funnelling(SSF)」を使用してIPへ接続したことに関連）

Persistence

T1505.003 - Server Software Component: Web Shell（アクセスを確立するためのウェブシェル及びSSFの利用に関連）

Credential access

T1552.001 - Credentials from Password Stores（ビルディングマネジメントシステム（BMS）に係るパスワードファイルに関連）

T1558.003 - Steal or Forge Kerberos Tickets: Kerberoasting（ネットワークの認証情報を得るための攻撃に関連）

Lateral movement

T1021.002 - Remote Services: SMB Shares（アクターが複数端末からSMB共有をマウントしたことに関連）

Collection

T1213 - Data from Information Repositories（BMSサーバ上の手順書／文書に関連）

Exfiltration

T1041 - Exfiltration Over C2 Channel （アクターによるアクティブディレクトリ及びマウントした共有からのデータの窃取）

ケーススタディ2

幅広い配布を可能にするため、この報告書は匿名化されている。影響を受けた組織は、以降、「組織」とする。被害を受けた組織の特定を避けるとともに、ASD・ACSCのインシデント対応手法を保護するため、詳細事項の一部は省かれている。

概要

この報告書では、2022年4月に発生した組織のネットワークへの侵害に関するASD・ACSCによる調査結果について詳述する。この調査報告書は、観測された悪意ある攻撃について要約し、改善のための推奨事項をまとめるために、組織に提供された。調査結果は、本侵害がAPT40によってなされたものであることを示している。

2022年5月、ASD・ACSCは、組織に対し、組織のネットワークに影響を与える悪意ある活動が、2022年4月以降に行われた疑いがあることを通知した。その後、組織は、組織が所有するコーポレートリモートアクセスソリューションへのログインポータルを提供するインターネット接続されたサーバ上に悪意あるソフトウェアを発見したとACSCに伝えた。
同サーバは、リモートアクセスログイン及びアイデンティティ管理製品を使用していた。以後、報告書ではこのサーバを「侵害された機器」と記載する。本報告書は、ASD・ACSCが実施した調査に対応して組織のために作成された調査結果及び改善措置に関するアドバイザリーにつき詳述する。

痕跡は、遅くとも2022年4月以降、組織のネットワークの一部が継続して組織のリモートアクセスログインポータルを経由し悪意あるアクターによって侵害されていたことを示唆している。同サーバは、複数のアクターによって侵害されていた可能性があり、かつ侵害の発生前後に広く公表されたリモートコード実行（RCE）の脆弱性の影響を受けた可能性がある。

ASD・ACSCが観測したアクターの主な攻撃には、以下が含まれる。

- ホストの列挙：アクターによる同ネットワークの構成図の作成を可能にする
- インターネットに接続しているアプリケーションへの攻撃及びウェブシェルの使用：同ネットワーク上にアクターの攻撃の足がかりを提供し、コマンド実行を可能にする
- ソフトウェアの脆弱性を悪用した権限昇格
- 横展開を可能にするための認証情報の収集

ASD・ACSCは、2022年4月にある悪意あるアクターが、侵害された機器上で数百件の一意のユーザー名とパスワードのペア、リモートアクセスセッションに関連する多数の多要素認証コード及び技術的アーティファクトを窃取したことを発見した。組織による確認の結果、パスワードは正規のものであることが判明した。ASD・ACSCは、アクターが、リモートログイン接続のハイジャック又は正規ユーザーとしてのリモートログイン接続の作成による、正規ユーザーアカウントを使用した組織のコーポレートネットワークへのアクセスを企図して、当該技術的アーティファクトを収集した可能性があると評価している。

調査結果

調査の概要

ASD・ACSCは、組織の従業員にリモートログイン接続を提供する機器を当該アクターが侵害し、さらなる攻撃を試みるためにこの侵害を利用したと判断した。

同機器は、負荷分散されている3台のホストで構成されている。最も初期の侵害の痕跡は複数の負荷分散されたホストでみられる。組織は、初期の侵害の直後に3台の負荷分散されたホスト群のうち2台をシャットダウンした。
その結果、その後のすべての攻撃は、1台のホスト上で発生した。侵害された機器に関係するサーバも、同様の方法で負荷分散されている。

アクターは、2022年4月以降に、既知の脆弱性を利用して侵害された機器にウェブシェルを展開したとみられる。当該グループのアクターは、同機器上で権限の昇格に成功したものと判断される。使用可能なログの不足のため、ASD・ACSCは攻撃の全容を特定できなかったが、端末上の痕跡は、あるアクターが以下を実施したことを示している。

- 実在する数百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ユーザーとしてVDIセッションへアクセスすることを可能にしたと考えられる技術的アーティファクトの収集

ASD・ACSCは、アクターが組織のネットワークへの侵害をさらに進めようと企図したと評価している。アクターによって窃取されたアーティファクトは、おそらく管理者を含む任意のユーザーアカウントを用いた正規ユーザーとしての仮想デスクトップ接続のハイジャック又は実行を可能にしたとみられる。アクターは、この攻撃ベクトルを使い、永続化及び他の目標を達成するために、同組織のサービスをさらに侵害した可能性がある。

ホスティングプロバイダーが管理する環境内の他の機器には、侵害の痕跡は見られなかった。

アクセス

侵害された機器のホストは、仮想デスクトップ（VDI）セッションに接続するユーザーに対して、アクティブディレクトリ及びウェブサーバを通じた認証を提供する（T1021.001）。

場所	侵害された機器のホスト名（負荷分散）
データセンター1	HOST1、HOST2、HOST3

機器のインフラには、同機器により生成され、ダウンロードされた認証トークンを取得すると、当該ユーザーに対するVDIへのトンネルを提供するアクセスゲートウェイホストを含む。

当該ホストのいずれにも侵害の痕跡はなかった。しかし、アクセスゲートウェイホスト上のログに既知の悪意あるIPアドレスとの顕著な通信の痕跡があった。これは、同ホスト上で発生した攻撃又はこのホストに到達したアクターのインフラとのネットワーク接続を反映している可能性がある。同攻撃の性質については、入手可能な痕跡では特定できなかったが、アクターが組織のネットワーク内で横展開を企図したことを示唆している（TA0008）。

内部ホスト

ASD・ACSCは、内部組織のネットワークセグメントから得た限られたデータを調査した。内部組織のネットワークセグメントに影響を与えたと認められた、企図された又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、内部のSQLサーバの抽出（T1505.001）、及び観測された既知の悪意あるIPアドレスからアクセスゲートウェイ機器を経由した説明のつかない通信（TA0011）を含む。

アクターは、侵害した機器へのアクセスを用いて、実在するユーザー名、パスワード（T1003）及びMFAトークンの値（T1111）を収集した。また、同アクターは仮想デスクトップログイン接続を生成するために用いられる認証アーティファクトであるJSON Web Token（JWT）（T1528）を収集した。アクターは、これらを用いて仮想デスクトップセッションを作成又はハイジャックし（T1563.002）、正規ユーザーとして内部組織ネットワークセグメントへアクセス（T1078）できた可能性がある。

また、アクターは、侵害された機器へのアクセスを組織の内部ネットワーク上のSQLサーバを抽出する（T1505.001）ためにも利用した。アクターがこのデータにアクセスした可能性がある。

アクセスゲートウェイ機器から入手可能な痕跡から、既知の悪意あるIPアドレスからこの端末を通したネットワークトラフィック又はこの端末へのネットワークトラフィックが発生したことが示されている。

前述のとおり、これは、内部ネットワークにピボットする方法として、悪意あるサイバーアクターがこの端末に影響を与えた又は利用したことを示している可能性がある。

調査のタイムライン

調査の過程で発見された主要な攻撃のタイムラインを下表に示す。

日付	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。この通信の性質は判断できなかった。
2022年4月	すべてのホスト、すなわちHOST1、HOST2及びHOST3が、一つ以上の悪意あるアクターによって侵害され、ウェブシェルがこれらのホストに配置された。 HOST2上でログファイルが作成もしくは修正された。このファイルには悪意あるアクターがキャプチャしたと考えられる認証情報が含まれている。 /etc/security/opasswdファイル及び/etc/shadowファイルがHOST1及びHOST3上で修正され、複数のパスワードが変更されたことを示している。HOST1上で利用可能な痕跡は、ユーザー「sshuser」のパスワードが変更されたことを示唆している。
2022年4月	組織によりHOST2がシャットダウンされた。 追加のウェブシェル（T1505.003）がHOST1及びHOST3上で作成された。HOST1はHOST3からSSHブルートフォース攻撃を受けた。 HOST3上のログファイルが修正された（T1070）。このファイルには悪意あるアクターがキャプチャしたと考えられる認証情報が含まれている（T1078）。 JWTがキャプチャされ（T1528）、HOST3上のファイルに出力された。 組織によりHOST3がシャットダウンされた。以降の全ての攻撃はHOST1上で発生する。
2022年4月	HOST1上で追加のウェブシェルが作成された（T1505.003）。JWTがキャプチャされ、HOST1上のファイルに出力された。
2022年4月	HOST1上で追加のウェブシェルが作成され（T1505.003）、既知の悪意あるIPアドレスが同ホスト（HOST1）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である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であるHOST7と通信した（TA0011）。 あるユーザーに対する認証のイベントが、HOST1上のログで既知の悪意あるIPアドレスにリンクされている。追加のウェブシェルがこのホスト上で作成される（T1505.003）。
2022年5月	HOST1上のスクリプトがアクターによって修正された（T1543）。このスクリプトには、内部SQLサーバからデータを抽出したであろう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修正された（T1070）。このログファイルには正当であるとみられる組織のネットワークに対するユーザー名とパスワードのペアが含まれている（T1078）。
2022年5月	追加のログファイルが最後に修正された（T1070）。このファイルはHOST1から収集されたJWTを含んでいる。

2022年5月	HOST1上で追加のウェブシェルが作成された（T1505.003）。この日、組織は作成日が2022年4月であるウェブシェルを発見したことをACSCに報告した。
2022年5月	HOST1上で、Log4jHotPatch.jarという名称のスクリプトを含む、多数のスクリプトが作成された。
2022年5月	アクセスゲートウェイホストに対して2つのオープンポートを追加するために、iptables-saveコマンドが使用された。これらのポートは、9998及び9999だった（T1572）。

アクターの戦術及び技術

調査中に判明したいくつかの戦術と技術を以下に示す。

Initial access

T1190 Exploit public facing application

アクターは、リモートアクセスのログインおよびアイデンティティ管理製品における、RCE、権限昇格及び認証バイパスの脆弱性を悪用してネットワークへの初期アクセスを行った可能性がある。

次の理由により、この初期アクセスの方法が使用された可能性が最も高いと考えられる。

- 同サーバは、初期アクセスが行われた時点でこれらのCVEに対して脆弱であった。
- 既知のアクターのインフラから当該脆弱性の悪用の企図があった。
- 最初に認識された内部の悪意ある活動は、脆弱性の悪用の試行直後に発生した。

Execution

T1059.004 Command and Scripting Interpreter: Unix Shell

前述の脆弱性の悪用に成功した当該アクターは、影響を受けた機器上で利用可能なUnixシェルでコマンドを実行できた可能性がある。
当該アクターによって実行されたコマンドの全詳細は同機器によるログが記録されていなかったため、提供することができない。

Persistence

T1505.003 Server Software Component: Web Shell

アクターは、影響を受けた機器にいくつかのウェブシェルを展開した。複数の異なるアクターがウェブシェルを展開した可能性があるが、当該ウェブシェルを用いて攻撃を行ったアクターはごく少数だった。
ウェブシェルは、侵害された機器上で、同アクターによる任意コマンドの実行を可能にしたと考えられる。

Privilege escalation

T1068 Exploitation for Privilege Escalation

入手可能な痕跡では、当該アクターによって獲得された権限のレベルは明らかになっていない。しかし、ウェブシェルを用いることにより、アクターは、少なくとも侵害された機器上のウェブサーバと同レベルの権限を獲得していたと考えられる。
アクターは、侵害された機器上に存在していたとみられる脆弱性により、管理者権限を獲得することができたと考えられる。

Credential access

T1056.003 Input Capture: Web Portal Capture

侵害された機器上の痕跡は、アクターが、正規のものと思われる数百のユーザー名とパスワードのペアを平文でキャプチャしたことを示した。これらの情報は、認証情報をファイルに出力する正規の認証プロセスに何らかの変更を加えてキャプチャされた可能性がある。

T1111 Multi-Factor Authentication Interception

アクターは、正規のログインに対応するMFAトークンの値もキャプチャした。MFAトークンの値は、当該値をファイルに出力する正規の認証プロセスに変更を加えてキャプチャされた可能性がある。
MFAトークンのセキュリティを確保するための固有の値を保存する「秘密サーバ」に対する侵害の痕跡はない。

T1040 Network Sniffing

アクターは侵害された機器上のHTTPトラフィックをキャプチャすることによりJWTをキャプチャしたとみられる。侵害された機器上でtcpdumpユーティリティが実行された痕跡があり、アクターはこれを用いてJWTをキャプチャした可能性がある。

T1539 Steal Web Session Cookie

上述のように、アクターはWebセッションのCookieに類似したJWTをキャプチャした。これらは、同アクターがさらなるアクセスを確立するために再利用された可能性がある。

Discovery

T1046 Network Service Discovery

同一ネットワークセグメントの他の機器をスキャンするために、侵害された機器上でネットワークをスキャンするnmapユーティリティが実行された痕跡がある。これは、横展開の機会を提供する他の到達可能なネットワークサービスを検出するためにアクターが用いた可能性がある。

Collection

入手可能な痕跡からは、当該アクターがどのようにデータを収集したのか、侵害された機器又は他のシステムから具体的に何を収集したのかは明らかになっていない。
しかし、前述のように、アクターが、キャプチャされた認証情報（T1003）、MFAトークンの値（T1111）、JWT等の侵害された機器上の全てのファイルにアクセスした可能性がある。

Command and control

T1071.001 Application Layer Protocol: Web Protocols

アクターは、ウェブシェルを用いてコマンドの実行及び制御を行った。ウェブシェルコマンドは同機器上のウェブサーバを用いHTTPS経由で送信されたとみられる（T1572）。

T1001.003 Data Obfuscation: Protocol Impersonation

アクターは、正規のトラフィックに紛れるように設計された攻撃の開始点として、侵害された端末を利用した。

検知と緩和のための推奨事項

ASD・ACSCは、ASDの「エッセンシャルエイト（Essential Eight）」及び関連するサイバーセキュリティインシデントの緩和戦略の実施を強く推奨している。以下にAPT40の侵入の検知及び防止のためにとられるべきネットワークセキュリティ上の措置に対する推奨事項を示す。そのあと表1に4つの重要なTTPに対する具体的な緩和策についてまとめる。

検知

上記で特定されたファイルの一部は、C:\Users\Public*又はC:\Windows\ Temp*といった場所に置かれていた。これらの場所は、通常、全ユーザーに書き込み権限がある場所、すなわちWindowsに登録された全てのユーザーアカウントからアクセスできるディレクトリ及びサブディレクトリであるため、データの書き込みを行うのに都合がよい場所であると考えられる。多くの場合、書き込み後、全てのユーザーが当該ファイルにアクセスできるため、横展開、防衛策の回避、低い権限での実行、及び情報摂取の準備の機会をもたらす。

以下のSigmaルールは、疑わしい場所からのプロセス実行を悪意ある活動の指標として検知する。全ての場合において、悪意ある活動及び属性を確認するためのさらなる調査を行う必要がある。

Title: World Writable Execution - Temp

ID: d2fa2d71-fbd0-4778-9449-e13ca7d7505c

Description: Detect process execution from C:\Windows\Temp

Background:

This rule looks specifically for execution out of C:\Windows\Temp*. Temp is more broadly used by benign applications and thus a lower confidence malicious indicator than execution out of other world writable subdirectories in C:\Windows.

Removing applications executed by the SYSTEM or NETWORK SERVICE users substantially reduces the quantity of benign activity selected by this rule

This means that the rule may miss malicious executions at a higher privilege level but it is recommended to use other rules to determine if a user is attempting to elevate privileges to SYSTEM

Investigation:

1. Examine information directly associated with this file execution, such as the user context, execution integrity level, immediate follow-on activity and images loaded by the file.
2. Investigate contextual process, network, file and other supporting data on the host to help make an assessment as to whether the activity is malicious.
3. If necessary attempt to collect a copy of the file for reverse engineering to determine whether it is legitimate.

References:

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

Author: ASD's ACSC

Date: 2024/06/19

Status: experimental

Tags:

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

Log Source:

category: process_creation

product: Windows

Detection:

```
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:
    User:
    - '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)

False Positives:

- Allowlist auditing applications have been observed running executables from Temp
- Temp will legitimately contain an array of setup applications and launchers, so it will be worth considering how prevalent this behaviour is on a monitored network (and whether or not it can be allowlisted) before deploying this rule

Level: low

Title: World Writable Execution - Non-Temp System Subdirectory

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

Description: Detect process execution from a world writable location in a subdirectory of the Windows OS install location.

Background:

This rule looks specifically for execution out of world writable directories within C:\ and particularly C:\Windows*, with the exception of C:\Windows\Temp (which is more broadly used by benign applications and thus a lower confidence malicious indicator).

AppData folders are excluded if a file is run as SYSTEM - this is a benign way in which many temporary application files are executed.

After completing an initial network baseline and identifying known benign executions from these locations, this rule should rarely fire.

Investigation:

1. Examine information directly associated with this file execution, such as the user context, execution integrity level, immediate follow-on activity and images loaded by the file.
2. Investigate contextual process, network, file and other supporting data on the host to help make an assessment as to whether the activity is malicious.
3. If necessary attempt to collect a copy of the file for reverse engineering to determine whether it is legitimate.

References:

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

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

Author: ASD's ACSC

Date: 2024/06/19

Status: experimental

Tags:

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

Log source:

category: process_creation

product: Windows

Detection:

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\\'

User: 'SYSTEM'

condition: writable_path and not appdata

False positives:

Allowlist auditing applications have been observed running executables from these directories.

It is plausible that scripts and administrative tools used in the monitored environment(s) may be located in one of these directories and should be addressed on a case-by-case basis.

Level: high

Title: World Writable Execution - Users

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

Description: Detect process execution from C:\Users\Public* and other world writable folders within Users.

Background:

AppData folders are excluded if a file is run as SYSTEM - this is a benign way in which many temporary application files are executed.

Investigation:

1. Examine information directly associated with this file execution, such as the user context, execution integrity level, immediate follow-on activity and images loaded by the file.
2. Investigate contextual process, network, file and other supporting data on the host to help make an assessment as to whether the activity is malicious.
3. If necessary attempt to collect a copy of the file for reverse engineering to determine whether it is legitimate.

References:

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

Author: ASD's ACSC

Date: 2024/06/19

Status: experimental

Tags:

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

Log source:

category: process_creation

product: Windows

Detection:

users:

Image|contains:

```
    - ':\\Users\\All Users\\'
    - ':\\Users\\Contacts\\'
    - ':\\Users\\Default\\'
    - ':\\Users\\Public\\'
    - ':\\Users\\Searches\\'
  appdata:
    Image|contains: '\\AppData\\'
    User: 'SYSTEM'
  condition: users and not appdata
```

False positives:

- It is plausible that scripts and administrative tools used in the monitored environment(s) may be located in Public or a subdirectory and should be addressed on a case-by-case basis.

Level: medium

緩和措置

ログ記録

ASD・ACSCの調査において、調査の取り組みの有効性と速度を低下させる共通の問題は、ウェブサーバのリクエストログ、Windowsのイベントログ、及びインターネットのプロキシログを含む多数の領域における包括的な履歴ログ情報の欠如である。

ASD・ACSCでは、「Windowsイベントのログ記録及び転送」（「Windowsイベントのログ記録リポジトリ」の設定ファイル及びスクリプトを含む）及び情報セキュリティマニュアルの「システム監視のためのガイドライン」に記載されているガイダンスを確認の上実施し、集約的なログを取り入れ、ログを適切な期間保管することを推奨している。

パッチ管理

ウェブサーバ、ウェブアプリケーション及びリモートアクセスゲートウェイを含む、インターネット接続された全ての機器及びサービスには、遅延なくパッチを適用すること。当該プロセスを自動化し、促進するために、集約化されたパッチ管理システムの提供を検討すること。ASD・ACSCでは、ISMのシステム管理のためのガイドライン（特に「システムのパッチ適用」の該当するコントロール）を必要に応じて実施することを推奨している。

アクターが使用した攻撃のほとんどは既知で、パッチ又は緩和措置が提供されていた。組織は、インターネットに接続している機器には、48時間以内に確実にセキュリティパッチや緩和措置を適用し、可能であれば、ソフトウェアやOSは最新バージョンを使用する。

ネットワークの分離

ネットワークの分離は、攻撃者による組織の機密データの検出及びアクセスをより困難にすることができる。ネットワークを分割し、要求がない限りコンピュータ間のトラフィックを拒否することで、横展開を制限またはブロックすること。Active Directoryや他の認証サーバといった重要なサーバは、限られた数のプロキシーサーバ又は「踏み台サーバ」からのみ管理されるようにするべきである。当該サーバは綿密に監視してセキュリティを強化し、接続できるユーザー及び機器を限定するべきである。

横展開が妨げられていることが特定された事例にかかわらず、追加のネットワークの分離によって、アクターがアクセスし抽出できたデータの量はさらに制限できたと考えられる。

追加の緩和措置

署名組織は、APT40及びその他のアクターによる以下のTTPの使用に対抗するための以下の緩和措置も推奨している。

- 使用されていない又は不要なネットワークサービス・ポート・プロトコルを無効にする。
- 十分に調整されたウェブアプリケーションファイアウォール（WAF）を使用してウェブサーバ及びアプリケーションを保護する。
- 管理者権限を必要最小権限とし、サーバ、ファイル共有及びその他のリソースへのアクセスを制限する。
- 多要素認証（MFA）及びマネージドサービスアカウントを使用し、認証情報の解読と再利用をより困難にする。以下を含めたインターネット上に公開された全てのリモートアクセスサービスにはMFAを適用するべきである。
  - ウェブ及びクラウドベースのEメール
  - コラボレーションプラットフォーム
  - VPN接続
  - リモートデスクトップサービス
- サポート切れの機器を交換する。

表 1　緩和戦略／技術

TTP	8つの重要な緩和戦略	ISMコントロール
Initial Access T1190 Exploitation of Public-Facing Application	• アプリケーションにパッチをあてる • OSにパッチをあてる • 多要素認証 • アプリケーションの管理	ISM-0140 ISM-1698 ISM-1701 ISM-1921 ISM-1876 ISM-1877 ISM-1905
Execution T1059 Command and Scripting Interpreter	• アプリケーションの管理 • Microsoft Officeのマクロを制限 • 管理者権限を制限	ISM-0140 ISM-1490 ISM-1622 ISM-1623 ISM-1657 ISM-1890
Persistence T1505.003 Server Software Component: Web Shell	• アプリケーションの管理 • 管理者権限を制限	ISM-0140 ISM-1246 ISM-1746 ISM-1249 ISM-1250 ISM-1490 ISM-1657 ISM-1871
Initial Access / Privilege Escalation / Persistence T1078 Valid Accounts	• OSにパッチをあてる • 多要素認証 • 管理者権限を制限 • アプリケーションの管理 • ユーザーアプリケーションの堅牢化	ISM-0140 ISM-0859 ISM-1546 ISM-1504 ISM-1679

一般的な検知及び緩和措置の推奨事項の詳細については、本アドバイザリーの後半のMITRE ATT&CKの概要で示されている各技術を公開しているMITRE ATT&CKの技術ウェブサイトの緩和措置及び検知セクションを参照すること。

免責事項

本報告書の情報は、情報提供のみを目的として「そのままの状態」で提供されている。署名組織は、本資料に関連する全ての事業体、製品、又はサービスを含むいかなる商業事業体、製品、企業、サービスも支持していない。サービスマーク、商標、メーカー又はその他の方法による特定の商業事業体、製品、プロセス、又はサービスについての言及は、署名組織による支持、推奨、又は奨励を構成又は暗示するものではない。

本資料はTLP:CLEARである。開示は制限されない。情報の提供元は、情報が悪用されるリスクが最小限または予見できない場合に、適用される規則と公開手順に従ってTLP:CLEARを使用できる。標準の著作権規則に従い、TLP:CLEAR情報の配布は制限されない。トラフィックライトプロトコル（TLP）の詳細については、cisa.gov/tlpを参照すること。

MITRE ATT&CK - 着目すべきAPT40のトレードクラフト

Reconnaissance（TA0043）	
Search Victim-Owned Websites （T1594）	Gather Victim Identity Information: Credentials （T1589.001）
Active Scanning: Vulnerability Scanning （T1595.002）	Gather Victim Host Information （T1592）
Search Open Websites/Domains: Search Engines （T1593.002）	Gather Victim Network Information: Domain Properties （T1590.001）
Gather Victim Identity Information: Email Addresses （T1589.002）	

Resource Development（TA0042）	
Acquire Infrastructure: Domains （T1583.001）	Acquire Infrastructure （T1583）
Acquire Infrastructure: DNS Server （T1583.002）	Compromise Accounts （T1586）
Develop Capabilities: Code Signing Certificates （T1587.002）	Compromise Infrastructure （T1584）
Develop Capabilities: Digital Certificates （T1587.003）	Develop Capabilities: Malware （T1587.001）
Obtain Capabilities: Code Signing Certificates （T1588.003）	Establish Accounts: Cloud Accounts （T1585.003）
Compromise Infrastructure: Network Devices （T1584.008）	Obtain Capabilities: Digital Certificates （T1588.004）

Initial Access（TA0001）	
Valid Accounts （T1078）	Phishing （T1566）
Valid Accounts: Default Accounts （T1078.001）	Phishing: Spearphishing Attachment （T1566.001）
Valid Accounts: Domain Accounts （T1078.002）	Phishing: Spearphishing Link （T1566.002）
External Remote Services （T1133）	Exploit Public-Facing Application （T1190）
Drive-by Compromise （T1189）	

Execution（TA0002）	
Windows Management Instrumentation （T1047）	Command and Scripting Interpreter: Python （T1059.006）
Scheduled Task/Job: At （T1053.002）	Command and Scripting Interpreter: JavaScript （T1059.007）
Scheduled Task/Job: Scheduled Task （T1053.005）	Native API （T1106）
Command and Scripting Interpreter （T1059）	Inter-Process Communication （T1559）
Command and Scripting Interpreter: Windows Command Shell （T1059.003）	System Services: Service Execution （T1569.002）
Command and Scripting Interpreter: PowerShell （T1059.001）	Exploitation for Client Execution （T1203）
Command and Scripting Interpreter: Visual Basic （T1059.005）	User Execution: Malicious File （T1204.002）
Command and Scripting Interpreter: Unix Shell （T1059.004）	Command and Scripting Interpreter: Apple Script （T1059.002）
Scheduled Task/Job: Cron （T1053.003）	Software Deployment Tools （T1072）

Persistence（TA0003）	
Valid Accounts （T1078）	Server Software Component: Web Shell （T1505.003）
Office Application Startup: Office Template Macros （T1137.001）	Create or Modify System Process: Windows Service （T1543.003）
Scheduled Task/Job: At （T1053.002）	Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder （T1547.001）
Scheduled Task/Job: Scheduled Task （T1053.005）	Boot or Logon Autostart Execution: Shortcut Modification （T1547.009）
External Remote Services （T1133）	Hijack Execution Flow: DLL Search Order Hijacking （T1574.001）
Scheduled Task/Job: Cron （T1053.003）	Hijack Execution Flow: DLL Side-Loading （T1574.002）
Account Manipulation （T1098）	Valid Accounts: Cloud Accounts （T1078.004）
Valid Accounts: Domain Accounts （T1078.002）	

Privilege Escalation（TA0004）	
Scheduled Task/Job: At（T1053.002）	Create or Modify System Process: Windows Service（T1543.003）
Scheduled Task/Job: Scheduled Task（T1053.005）	Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder（T1547.001）
Process Injection: Thread Execution Hijacking（T1055.003）	Boot or Logon Autostart Execution: Shortcut Modification（T1547.009）
Process Injection: Process Hollowing（T1055.012）	Hijack Execution Flow: DLL Search Order Hijacking（T1574.001）
Valid Accounts: Domain Accounts（T1078.002）	Exploitation for Privilege Escalation（T1068）
Access Token Manipulation: Token Impersonation/Theft（T1134.001）	Event Triggered Execution: Unix Shell Configuration Modification（T1546.004）
Process Injection: Dynamic-link Library Injection（T1055.001）	Valid Accounts: Domain Accounts（T1078.002）
Valid Accounts: Local Accounts（T1078.003）	

Defence Evasion（TA0005）	
Rootkit（T1014）	Indirect Command Execution（T1202）
Obfuscated Files or Information（T1027）	System Binary Proxy Execution: Mshta（T1218.005）
Obfuscated Files or Information: Software Packing（T1027.002）	System Binary Proxy Execution: Regsvr32（T1218.010）
Obfuscated Files or Information: Steganography（T1027.003）	Subvert Trust Controls: Code Signing（T1553.002）
Obfuscated Files or Information: Compile After Delivery（T1027.004）	File and Directory Permissions Modifications: Linux and Mac File and Directory Permissions Modification（T1222.002）
Masquerading: Match Legitimate Name or Location（T1036.005）	Virtualisation/Sandbox Evasion: System Checks（T1497.001）
Process Injection: Thread Execution Hijacking（T1055.003）	Masquerading（T1036）
Reflective Code Loading（T1620）	Impair Defences: Disable or Modify System Firewall（T1562.004）
Process Injection: Process Hollowing（T1055.012）	Hide Artifacts: Hidden Files and Directories（T1564.001）
Indicator Removal: File Deletion（T1070.004）	Hide Artifacts: Hidden Window（T1564.003）
Indicator Removal: Timestomp（T1070.006）	Hijack Execution Flow: DLL Search Order Hijacking（T1574.001）
Indicator Removal: Clear Windows Event Logs（T1070.001）	Hijack Execution Flow: DLL Side-Loading（T1574.002）
Modify Registry（T1112）	Web Service（T1102）
Deobfuscate/Decode Files or Information（T1140）	Masquerading: Masquerade Task or Service（T1036.004）
Impair Defenses（T1562）	

Credential Access（TA0006）	
OS Credential Dumping: LSASS Memory（T1003.001）	Unsecured Credentials: Credentials in Files（T1552.001）
OS Credential Dumping: NTDS（T1003.003）	Brute Force: Password Guessing（T1110.001）
Network Sniffing（T1040）	Forced Authentication（T1187）
Credentials from Password Stores: Keychain（T1555.001）	Steal or Forge Kerberos Tickets: Kerberoasting（T1558.003）
Input Capture: Keylogging（T1056.001）	Multi-Factor Authentication Interception（T1111）
Steal Web Session Cookie（T1539）	Steal Application Access Token（T1528）
Exploitation for Credential Access（T1212）	Brute Force: Password Cracking（T1110.002）
Input Capture: Web Portal Capture（T1056.003）	OS Credential Dumping: DCSync（T1003.006）
Credentials from Password Stores（T1555）	Credentials from Password Stores: Credentials from Web Browsers（T1555.003）

Discovery（TA0007）	
System Service Discovery（T1007）	System Information Discovery（T1082）
Application Window Discovery（T1010）	Account Discovery: Local Account（T1087.001）
Query Registry（T1012）	System Information Discovery, Technique T1082 - Enterprise | MITRE ATT&CK®
File and Directory Discovery（T1083）	System Time Discovery（T1124）
Network Service Discovery（T1046）	System Owner/User Discovery（T1033）
Remote System Discovery（T1018）	Domain Trust Discovery（T1482）
Account Discovery: Email Account（T1087.003）	Account Discovery: Domain Account（T1087.002）
System Network Connections Discovery（T1049）	Virtualisation/Sandbox Evasion: System Checks（T1497.001）
Process Discovery（T1057）	Software Discovery（T1518）
Permission Groups Discovery: Domain Groups（T1069.002）	Network Share Discovery, Technique T1135 - Enterprise | MITRE ATT&CK®
System Network Configuration Discovery: Internet Connection Discovery（T1016.001）	

Lateral Movement（TA0008）	
Remote Services: Remote Desktop Protocol（T1021.001）	Remote Services（T1021）
Remote Services: SMB/Windows Admin Shares（T1021.002）	Use Alternate Authentication Material: Pass the Ticket（T1550.003）
Remote Services: Windows Remote Management（T1021.006）	Lateral Tool Transfer（T1570）

Collection（TA0009）	
Data from Local System（T1005）	Archive Collected Data: Archive via Library（T1560.002）
Data from Network Shared Drive（T1039）	Email Collection: Remote Email Collection（T1114.002）
Input Capture: Keylogging（T1056.001）	Clipboard Data（T1115）
Automated Collection（T1119）	Data from Information Repositories（T1213）
Input Capture: Web Portal Capture（T1056.003）	Data Staged: Remote Data Staging（T1074.002）
Data Staged: Local Data Staging（T1074.001）	Archive Collected Data（T1560）
Email Collection（T1114）	

Exfiltration（TA0010）	
Exfiltration Over C2 Channel（T1041）	Exfiltration Over Alternative Protocol: Exfiltration Over Asymmetric Encrypted Non-C2 Protocol（T1048.002）
Exfiltration Over Alternative Protocol（T1048）	Exfiltration Over Web Service: Exfiltration to Cloud Storage（T1567.002）

Command and Control（TA0011）	
Data Obfuscation: Protocol Impersonation（T1001.003）	Web Service: Dead Drop Resolver（T1102.001）
Commonly Used Port（T1043）	Web Service: One-way Communication（T1102.003）
Application Layer Protocol: Web Protocols（T1071.001）	Ingress Tool Transfer（T1105）
Application Layer Protocol: File Transfer Protocols（T1071.002）	Proxy: Internal Proxy（T1090.001）
Proxy: External Proxy（T1090.002）	Non-Standard Port（T1571）
Proxy: Multi-hop Proxy（T1090.003）	Protocol Tunnelling（T1572）
Web Service: Bidirectional Communication（T1102.002）	Encrypted Channel（T1573）
Encrypted Channel: Asymmetric Cryptography（T1573.002）	Ingress Tool Transfer（T1105）
Proxy, Technique T1090 - Enterprise | MITRE ATT&CK®	

Impact（TA0040）	
Service Stop（T1489）	Disk Wipe（T1561）
System Shutdown/Reboot（T1529）	Resource Hijacking（T1496）

メモ

お断り
本ガイドに含まれる資料は一般的性質のものであり、法律に基づく助言と見なされるべきではなく、又、特定の状況又は緊急時に依拠されるべきではない。重要事項については、独立した適切な専門家に個々の状況に関する助言を求めること。

コモンウェルスは、本ガイドに含まれる情報への依拠に起因する損害、損失、又は費用について、いかなる責任も負わない。

詳細又はサイバーセキュリティインシデントの報告の連絡先：

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

Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre