注目を集める ASEAN 諸国: 中国 APT グループによる標的化

概要

過去 90 日にわたり、Unit 42 のリサーチャーは、東南アジア諸国連合 (ASEAN) に加盟する組織および加盟国に対してサイバースパイ活動を行っている 2 つの中国の持続的標的型攻撃 (APT) グループを特定しました。

- 1 つめの APT グループである Stately Taurus は、ミャンマー、フィリピン、日本、シンガポールの組織を標的にしたものと思われる 2 つのマルウェア パッケージを作成しました。これらのキャンペーンのタイミングは、2024 年の 3 月 4 日から 3 月 6 日にかけて開催された、豪 ASEAN 特別首脳会議と一致していました。
- 2 つめの中国の APT グループは、ある ASEAN 加盟組織を侵害しました。この APT グループはここ数カ月、カンボジア、ラオス、シンガポールを含む東南アジアのさまざまな政府機関を標的にしていました。

Stately Taurus (別名 Mustang Panda、BRONZE PRESIDENT、Red Delta、LuminousMoth、Earth Preta、Camaro Dragon) は少なくとも 2012 年から活動しています。私たちは同グループを「サイバースパイ活動を日常的に行っている中国の持続的標的型攻撃 (APT) グループ」と評価しています。このグループはこれまで北米やヨーロッパ、アジアの政府機関や非営利団体、宗教団体、そのほかの非政府組織を標的にしてきました。

私たちは最近、前述の ASEAN 加盟組織から、2 つめの中国 APT グループに紐づく悪意のあるインフラへのネットワーク トラフィックを特定しました。このことは、同組織の環境が侵害されたことを示しています。ASEAN

加盟組織は、同地域内での外交関係や経済的決定に関する機密情報を扱う役割を担っていることから、スパイ活動の魅力的な標的となっています。

パロアルトネットワークスのお客様は、DNS Security や Advanced URL Filtering に加え、WildFire を統合した Prisma Cloud Defender エージェントにより、この悪意のあるインフラからのより適切な保護を受けています。

侵害の懸念があり弊社にインシデントレスポンスに関するご相談をなさりたい場合は、こちら の問い合わせフォームからご連絡いただくか、infojapan@paloaltonetworks.com まで電子メールにてお問い合わせください (ご相談は弊社製品のお客様には限定されません)。

関連する Unit 42 のトピック	**China**, **APT**, **APAC**

Stately Taurus のアクティビティ

2024 年 3 月の豪 ASEAN 特別首脳会議の開催中、Unit 42 のリサーチャーは、アジア諸国を標的としていると見られる Stately Taurus のマルウェア パッケージを 2 つ特定しました。脅威アクターは、豪 ASEAN 特別首脳会議 (2024 年 3 月 4 ～ 6 日開催) に合わせて 2024 年 3 月 4 ～ 5 日にこれらのパッケージ用のマルウェアを作成しました。

パッケージ 1: Talking_Points_for_China.zip

攻撃者は、2024 年 3 月 4 日に最初のパッケージを ZIP アーカイブとして作成しました。フィリピン、日本、シンガポールに拠点を置く複数の組織が、同パッケージをその翌日に目にしていました (彼らが共同データベースにアップロードしたサンプルがその証左となっている)。`Talking_Points_for_China.zip` アーカイブの内容を展開すると、図 1 に示すように、2 つのファイルが表示されます。

画像 1 は、ZIP ファイル Talking_Points_for_China の内容のスクリーンショットです。これには、KeyS
Image not found or type unknown
図 1. `Talking_Points_for_China.zip`

この `Talking_Points_for_China.exe` という実行可能ファイルは実際には、署名済みキーロギング対策プログラム、`KeyScrambler.exe` (開発元は QFX Software Corporation) の名前を変更したものです。なお、脅威アクターが悪意をもって正規製品を悪用・転用するのは珍しいことではなく、悪用された

正規製品の側になにか問題や悪意があるということは意味しません。

このバイナリーを実行すると、悪意のある DLL の `KeyScramblerIE.dll` をサイドロードしてディレクトリー `C:\Users\Public\Libraries\SmileTV\KeyScramblerIE.dll` にコピーし、このディレクトリーと同じ場所の autorun レジストリー キーを作成して永続化を確立します。

このコードは次に、私たちが PubLoad マルウェアであるものと評価しているシェルコードを復号します。続けてこのマルウェアは、`103.27.109[.]157:443` への接続を確立しようとします。

このパッケージには、CSIRT-CTI による投稿の「Campaign #4 – Talking Points for China.zip」というセクションで説明されているサンプルとの強い重複が見られます。それらの類似点として、次のようなものがあります。

- アーカイブのファイル名
- ペイロードを開始するマジック バイト (`17 03 03`)
- QFX Software Corporation の署名付きバイナリーの使用
- PubLoad マルウェアの実行特性

パッケージ 2: Note PSO.scr

脅威アクターは 2 つめのパッケージを 2024 年 3 月 5 日にスクリーンセーバーの実行可能ファイル (拡張子 SCR) として作成していました。同日、ミャンマーのある組織がこのファイルを目にしていました (マルウェア リポジトリーへのアップロードがその証左となっている)。`Note PSO.scr` というファイル名からしてこの「PSO」はおそらくミャンマー軍の階級のひとつである「Personal Staff Officer」という称号を指しているのではないかと考えられます。

私たちは、Stately Taurus がこの悪意のあるパッケージについて、その戦術・技術・手順 (TTP) を切り替えたようすを観測しています。今回 Stately Taurus は、いつものファイル アーカイブ形式 (ZIP、RAR、ISO) を配布手段として選ばず、初期感染にスクリーンセーバー (SCR) のファイル拡張子を持つ実行可能ファイルを採用していました。このアプローチにより、IP アドレス `123.253.32[.]71` から悪意のあるコードがダウンロードされることになりました。

この SCR ファイルを開くと、脅威アクターはネットワーク接続を確立し、無害な実行可能ファイル `WindowsUpdate.exe` と悪意のある DLL の `EACore.dll` をダウンロードしようとします。これらのファイルは次の場所でホストされていました。

- hxxp[:]//123.253.32[.]71/WindowsUpdate.exe
- hxxp[:]//123.253.32[.]71/EACore.dll

脅威アクターは名前が WindowsUpdate.exe
に変更された無害なプログラムを使います。ただしこのファイルは実際には評判の高いビデオ ゲーム会社 Electronic Arts, Inc.
が署名した、古いバージョンの EACoreServer.exe
です。脅威アクターは信頼できるプログラムに見せかけるためにこうした名前の変更を行います。その裏では正規 EACore.dll
ファイルを上書きするために名前を変更した悪意のある DLL
ファイルをサイドローディングしています。このマルウェアは次に、コマンド & コントロール (C2) のために 146.70.149[.]36
にある www[.]openservername[.]com への接続を確立しようとします。

2 つめの中国 APT グループのアクティビティ

私たちは最近、ASEAN 加盟組織と中国 APT グループの C2
インフラとの間でのネットワーク接続を特定しました。このことは、同組織の環境が侵害されたことを示しています。私たちはまた、同様のアクティビティが ASEAN 加盟国の複数の政府機関から発信されたことも観測しています。ASEAN
加盟組織は、同地域内での外交関係や経済的決定に関する機密情報を扱う役割を担っていることから、スパイ活動の魅力的な標的となっています。

C2 インフラ

表 1 は、C2 に使われる既知の標的組織に面したインフラの概要を示しています。

IP アドレス	宛先ポート	ドメイン
65.20.103[.]231	80, 81	
139.59.46[.]88	80, 443, 8443, 8080, 9443	
193.149.129[.]93	8443	ai.nerdnooks[.]com
192.153.57[.]98	8080	web.daydreamdew[.]net

アクティビティのタイムライン: 2 つめの中国 APT グループ

Unit 42 のリサーチャーは、2024 年 1 月から 2 月にかけての脅威アクターのアクティビティを特定しました。また、図 2 に示すように、旧正月と中国が定めた 2024 年 2 月 18 日の「中国特殊工作日 (Special Working Day)」に合わせて、明確な小休止も観測されました。

画像 2 は、1 月末から 2 月末にかけて観測された脅威アクターを特定する営業日のタイムラインです。脅
Image not found or type unknown
図 2. 生活パターン: 勤務日

私たちはこれと同様の生活パターンを、中国のゴールデンウイーク (2023 年 9 月と 10 月) 中、同じアクターについて観測していました。

図 3 に示すように、この攻撃者の勤務時間は、UTC +08:00 (中国標準時) に調整された平日 (月曜から金曜) の営業時間に関する以前の観測結果と一致していました。

画像 3 は、中国標準時に調整された生活パターンのヒート マップです。縦軸には、月曜日を先頭にして日
Image not found or type unknown
図 3. 生活パターン: 勤務時間 (+08:00 で時間調整)

結論

Unit 42 は、東南アジア諸国連合 (ASEAN) の加盟組織および加盟国に対して最近サイバースパイ活動を行っていた 2 つの中国 APT グループを特定しました。この種のキャンペーンは、サイバースパイ活動を目的として組織がどのように標的化されるのかを引き続き示すものとなっており、そこでは国家との関連をもつ脅威グループが地域内の地政学的利益にからんだインテリジェンスの収集を行っています。今回の私たちの調査結果をすべての組織に活かしていただき、この種の脅威に対する防御を高めていただくことをお勧めします。

保護と緩和策

パロアルトネットワークスのお客様は、以下の製品を通じて、上記の脅威からさらに強力に保護されています。

- DNS Security と Advanced URL Filtering は本稿のドメインを悪意のあるものとして分類します
- クラウド ベースの脅威検出エンジン WildFire は本稿における Stately Taurus のマルウェア サンプルを悪意のあるものとして分類します
- Prisma Cloud Defender エージェントと WildFire の統合により、本稿に記載した Stately Taurus マルウェア サンプルによる悪意のある実行を Windows ベースの仮想マシン (VM)、コンテナー、サーバーレス クラウド インフラ上で検出・防止できます

侵害の懸念があり弊社にインシデントレスポンスに関するご相談をなさりたい場合は、こちらのフォーム からご連絡いただくか、infojapan@paloaltonetworks.comまでメールにてご連絡いただくか、下記の電話番号までお問い合わせください(ご相談は弊社製品のお客様には限定されません)。

- 北米フリーダイヤル: 866.486.4842 (866.4.UNIT42)
- EMEA: +31.20.299.3130
- APAC: +65.6983.8730
- 日本: (+81) 50-1790-0200

パロアルトネットワークスは、これらの調査結果を Cyber Threat Alliance (CTA: サイバー脅威アライアンス) のメンバーと共有しました。CTA のメンバーはこのインテリジェンスを使って、お客様に保護を迅速に提供し、悪意のあるサイバー攻撃者を体系的に阻害できます。詳細は Cyber Threat Alliance にてご確認ください。

IoC (侵害指標)

Stately Taurus のキャンペーン

マルウェア ハッシュ

- `a16a40d0182a87fc6219693ac66428673832922983bd9e70b455f198e124ba2`
- `316541143187acff1404b98659c6d9c8566107bd652310705214777f03ea10c8`

- 02f4186b532b3e33a5cd6d9a39d9469b8d9c12df7cb45dba6dcab912b03e3cb8
- 5cd4003ccaa479734c7f5a01c8ff95891831a29d857757bbd7fe4294f3c5c126

インフラ:

- 103.27.109[.]157
- 123.253.32[.]71
- 146.70.149[.]36
- www.openservername[.]com

ASEAN 関連のアクティビティ

インフラ:

- ai.nerdnooks[.]com
- web.daydreamdew[.]net
- 65.20.103[.]231
- 139.59.46[.]88
- 193.149.129[.]93
- 192.153.57[.]98

追加リソース

- ライブラリーにひそむ侵入者: DLL ハイジャック探究 – パロアルトネットワークス Unit 42
- Stately Taurus Continued – New Information on Cyberespionage Attacks against Myanmar Military Junta – CSIRT-CTI
- カンボジア政府を狙う中国の APT 攻撃グループ – パロアルトネットワークス Unit 42