中国のセキュリティ サービス企業 i-Soon のデータが漏えい、既知の中国 APT 攻撃キャンペーンとのリンク見つかる

概要

2024 年 2 月 16 日、中国の IT セキュリティ サービス会社 i-Soon (別名 Anxun Information Technology) に属する可能性のある社内通信、セールス関連資料、製品マニュアルを含むデータが何者かによって GitHub にアップロードされました。漏えいした資料は、ある営利団体が、中国とつながりのある脅威アクターを支援するサイバー スパイ ツールをどのように開発・サポートしたかを示すもののようです。漏えいデータの初期調査の一環として、Unit 42 は、データ漏えい内の情報と以前の中国とつながりのある持続的標的型攻撃 (APT) キャンペーンとのリンクを発見しました。Unit 42 は、この漏えいが本物であることを高い確度で評価しています。

たとえば、この漏えいに含まれていたある文書は、i-Soon が Treadstone マルウェア コントローラー ソフトウェアを販売していたことを示しているようです。このソフトウェアは 2019 年に Elemental Taurus (別名 APT41) に帰属されており、米国の大陪審は成都404の従業員 3 名を起訴 [PDF] しています。

Unit 42 は、漏えいしたデータの分析を通じ、アクターが所有するインフラと、中国の脅威アクターについての過去の報告と関連する潜在的マルウェアを特定しました。漏えいしたデータ範囲を考えると、本稿では初期分析と重要な調査結果を取り上げ、さらなるレポートは将来的に提供することになりそうです。(漏えいデータが投稿された元の GitHub リポジトリは現在、利用規約違反を理由に GitHub スタッフによって削除されていますが、リサーチャーは最初に共有された内容の研究を続ける予定です。)

漏えいデータに関する弊社の現在の理解に基づき、弊社のお客様は、パロアルトネットワークスのセキュリティ製品を通じ、本稿で言及する中国の脅威アクターが使用するツールや手法からより適切に保護されています。

関連する Unit 42 **のトピック**	GitHub, China

技術分析

GitHub リポジトリ上のテキストは、i-Soon がインド、タイ、ベトナム、韓国の政府のほか、政府間組織である NATO を標的にしていると主張しています。これらの主張を検証するため、私たちは漏えいデータの分析を続けています。

当該 GitHub リポジトリには、オンライン チャットの会話、スクリーンショット、おそらくは被害者ものと思われるデータ、セールスやサポートに関連する文書が混在しています。テキストによる会話は 2018 年 11 月から 2023 年 1 月までのもので、37 名分の一意なユーザー名が含まれています。

会話の範囲は、一般的な会話や職場の問題から、ターゲット、ソフトウェアの脆弱性、顧客についての話まで多岐にわたります。

図 1 は、i-Soon のメンバー間で観測されたテキスト コミュニケーションをグラフ化したもので、従業員間の関係と従業員間のメッセージの量を示しています。(特定のユーザー名と名前は伏せています。)

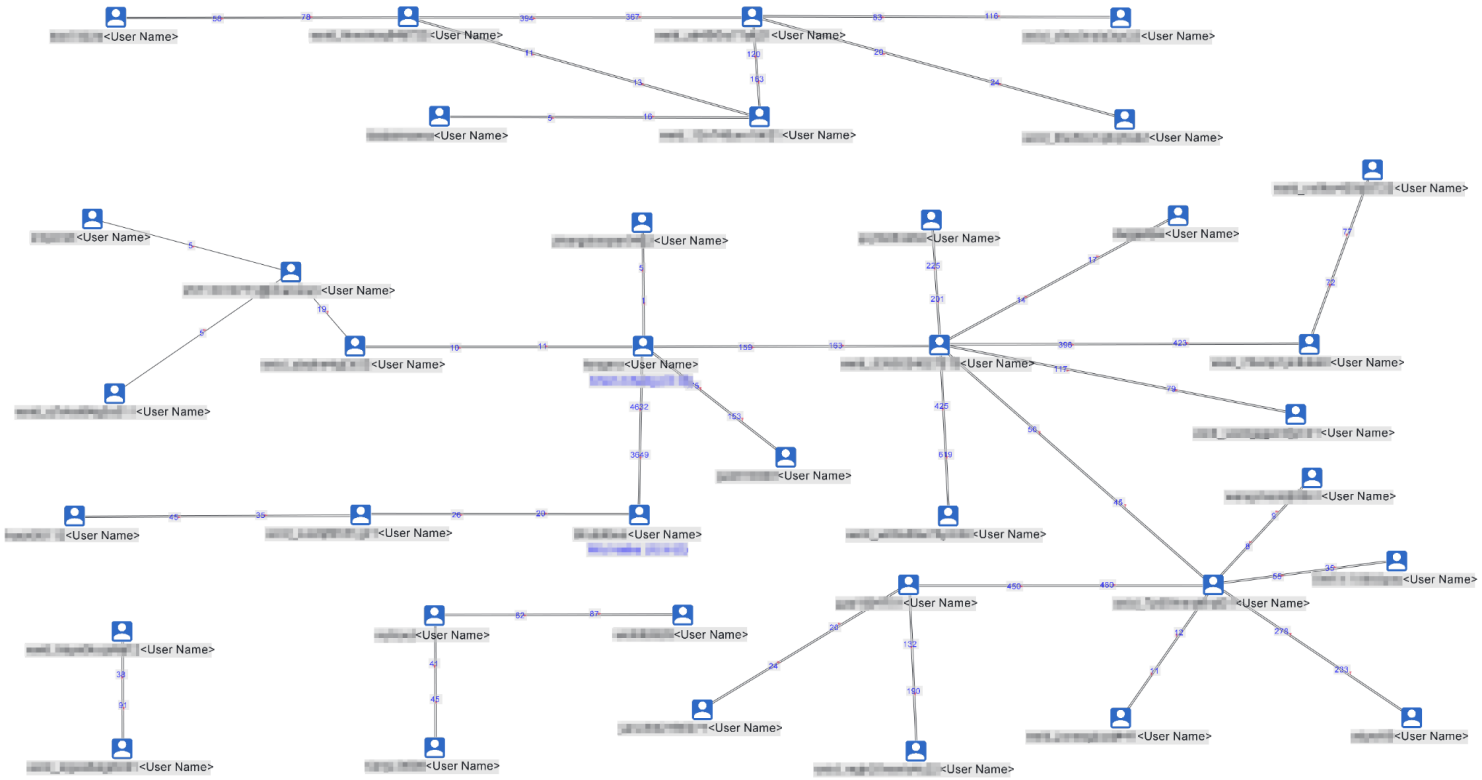

図 1. i-Soon の漏えいしたオンライン チャットを視覚化したもの (特定のユーザー名は伏せてあります)

以前の脅威インテリジェンス レポートとのリンク

Unit 42は、漏えいした i-Soon のテキスト メッセージの会話から、中国系 APT (Advanced Persistent Threat 持続的標的型攻撃) グループに帰属済みの、過去に報告のある 2 つのキャンペーンとのリンクを発見しました。

キャンペーン 1: 2022 年のサプライチェーン攻撃

2022 年 9 月、Trend Micro が、カナダのソフトウェア会社 Comm100 に対するサプライチェーン攻撃を報じました。攻撃者は、公式 Web サイトでホストされている Comm100 のチャットベースの顧客エンゲージメント アプリケーションのインストーラーをトロイの木馬化していました。i-Soon の漏えいデータを調べたところ、i-Soon がこの攻撃に関与していたという指標が見つかりました。

表 1 には、i-Soon の 2 人のメンバー間の会話の抜粋が含まれています。ここでは IP アドレス 8.218.67[.]52 が i-Soon のサーバーだとされています。

日付	From	To	メッセージ	翻訳
2022-06-13 7:39:19	wxid_c9xxxxxxxxx	wxid_zbxxxxxxxxxx	网那网网人pc的通道	[揚州のある個人または組織が] ある特定の個人に属する PC チャネルへのアクセスを要求またはリクエストしたいと考えています。
2022-06-13 7:39:21	wxid_c9xxxxxxxxx	wxid_zbxxxxxxxxxx	[捂网	[当惑または迷惑をかけてごめんなさいという意味を示唆する絵文字]

2022-06-13 7:39:23	wxid_c9xxxxxxxxx	wxid_zbxxxxxxxxxx	囡能囡	今すぐ付与できますか?
2022-06-13 7:40:26	wxid_zbxxxxxxxxx	wxid_c9xxxxxxxxxx	【彩宝贝】 【代理】 8.218.67[.]52:27011 【TCP隧道】 8.218.67[.]52:17011 【囡】 admin 【密囚】 88888888	【 ギャンブルまたは宝くじのサイト】 【プロキシ】 8.218.67[.]52:27011 【TCP トンネル】 8.218.67[.]52:17011 【アカウント】 admin 【パスワード】 88888888

2022-06-13 7:40:34	wxid_c9xxxxxxxxx	wxid_zbxxxxxxxxxx	⊠⊠	はいはい
2022-06-13 7:40:37	wxid_c9xxxxxxxxx	wxid_zbxxxxxxxxxx	我日	[卑語]
2022-06-13 7:40:54	wxid_c9xxxxxxxxx	wxid_zbxxxxxxxxxx	⊠服⊠在香港的	このサーバーは香港にあります
2022-06-13 7:41:06	wxid_zbxxxxxxxxx	wxid_c9xxxxxxxxx	你不管	心配する必要はありません

2022-06-13 7:41:07	wxid_c9xxxxxxxxx	wxid_zbxxxxxxxxxx	domain_access_result(1).csv	
2022-06-13 7:41:11	wxid_c9xxxxxxxxx	wxid_zbxxxxxxxxxx	☒	はい
2022-06-13 7:41:14	wxid_zbxxxxxxxxx	wxid_c9xxxxxxxxxx	☒服器是我☒	このサーバーは私たちのものです

1. IP 8.218.67[.]52 i-Soon

上記の会話が行われた数日後の 2022 年 6 月 17 日、この IP アドレス 8.218.67[.]52 は SHA256 db4497090a94d0189aa3c3f4fcee30d5381453ec5aa38962e2ca971074b74e8b をもつ、ある Linux ELF ファイルをホストしました。このファイルは hxxp[://]8.218.67[.]52/js/xxx.jpg という URL から提供されていました。このファイルは実行されるとドメイン unix.s3amazonbucket[.]com (正規の Amazon ドメインではない) への接続を試行します。

Trend Micro のレポートでは別のサブドメイン s3amazonbucket[.]com (analyaze.s3amazonbucket[.]com) についても言及していますが、このサブドメインは、トロイの木馬化されたインストーラーのコマンド & コントロール (C2) サーバーとして使われていました。

s3amazonbucket[.]com というドメインは i-Soon の制御下にあった可能性が高いことから、Unit 42 は、i-Soon 内のハッカーのグループが、Comm100 に対するサプライ チェーン攻撃に関与していたたことを中程度の確度で評価しています。

キャンペーン 2: 2019 年の Poison Carp 攻撃

2019 年 9 月に、複数の iOS と Android のエクスプロイトを介してチベット人グループを標的としていた攻撃者について、Citizen Lab が報じました。Citizen Lab は、POISON CARP の名前で追跡されている中国の脅威グループにこの攻撃を帰属させています。同レポートで言及されているドメインは、私たちが今回のデータ漏えい内で見つけた IP アドレスと結びつくものでした。

この IPアドレス 74.120.172[.]10 は、2020 年 9 月 22 日から 2024 年 2 月 20 日までの間は mailteso[.]online というドメインに、2021 年 8 月 7 日から 2022 年 7 月 12 日までの間は、mailnotes[.]online というドメインに結びついていました。

表 2 は、IP アドレス 74.120.172[.]10 に関する i-Soon 従業員間の会話の概要を示したものです。

日付	From	To	メッセージ	翻訳

2023-01-09 02:28:14	wxid_hlxxxxxxxx	wxid_12xxxxxxxx	等一下 平台有点⊠⊠	待ってください、プラットフォームに問題があります
2023-01-09 02:28:18	wxid_12xxxxxxxx	wxid_hlxxxxxxxx	好的	OK
2023-01-09 02:36:19	wxid_hlxxxxxxxx	wxid_12xxxxxxxx	hxxps[://]74.120.172[.]10:10092/home	

2023- 01-09 02:36: 25	wxid_ hlxxx xxxxx xxxx	wxid_ 12xxx xxxxx xxxx	access OrFRXV LZtestUser lzqzmp@123	
2023- 01-09 02:43: 51	wxid_ 12xxx xxxxx xxxx	wxid_ hlxxx xxxxx xxxx	演示□屏□一个	デモビデオを送信します
2023- 01-09 02:44: 06	wxid_ 12xxx xxxxx xxxx	wxid_ hlxxx xxxxx xxxx	□个□料都不用□ 了	この情報を伝える必要はありません

2023-01-09 02:44:09	wxid_12xxxxxxxx	wxid_hlxxxxxxxx	[□□]	【ニヤニヤ笑う絵文字】
2023-01-09 02:44:20	wxid_hlxxxxxxxx	wxid_12xxxxxxxx	□是微□的□用版	これは Microsoft の [ツールの] 試用版です
2023-01-09 02:44:33	wxid_12xxxxxxxx	wxid_hlxxxxxxxx	恩，我看到了	見ました

2023-01-09 02:44:51	wxid_12xxxxxxxx	wxid_hlxxxxxxxx	微□的演示□□有	[この Microsoft Windows ツールの] デモビデオはありますか?
2023-01-09 02:44:58	wxid_hlxxxxxxxx	wxid_12xxxxxxxx	我□下	聞いてみます
2023-01-09 02:48:54	wxid_hlxxxxxxxx	wxid_12xxxxxxxx	.7z	Microsoft Mail Secret Platform .7z

2023-01-09 02:52:01	wxid_12xxxxxxxx	wxid_hlxxxxxxxx	是不是你[illegible] 啊	なにかビデオに問題がありますか ?
2023-01-09 02:52:03	wxid_12xxxxxxxx	wxid_hlxxxxxxxx	我打不开	開けられません
2023-01-09 02:55:53	wxid_hlxxxxxxxx	wxid_12xxxxxxxx	[illegible]?	はい?

2023-01-09 02:55:56	wxid_hlxxxxxxxx	wxid_12xxxxxxxx	解□就行了呀	とにかく展開してください
2023-01-09 02:56:36	wxid_12xxxxxxxx	wxid_hlxxxxxxxx	估□是我没看□屏的	動画は見なかったと思う
2023-01-09 03:01:26	wxid_12xxxxxxxx	wxid_hlxxxxxxxx	□有安卓的□控	Android RAT も

2023-01-09 03:02:07	wxid_hlxxxxxxxx	wxid_12xxxxxxxx	安卓稍等一下 有点⊠⊠	ちょっと待って、Android のやつになにか問題があります
2023-01-09 03:02:26	wxid_12xxxxxxxx	wxid_hlxxxxxxxx	好	OK

2. IP 74.120.172[.]10 i-Soon

Citizen Lab による報告の当時、`mailnotes[.]online` は IPアドレス `207.246.101[.]169` に結びついていました。またこの IP アドレスはこれと同じ時期、ドメイン `gmail.isooncloud[.]com` に結びついていました。

既知の中国の侵入セットとのリンク

今回のデータ漏えいには、さまざまなソフトウェア
ツールのマニュアルやホワイトペーパーが含まれています。とくに重要なのは、これらのツールには、過去に中国系 APT
グループに帰属されたソフトウェアが含まれているということです。

i-Soon がこれらのツールの開発者だったのか、リセラーだったのか、単なるエンド
ユーザーだったのかは現時点ではわかりません。しかし、今回漏えいした文書は、中国に帰属されている複数の脅威アクターのグループが、同一の、おそらくは商用化されたマルウェア ツール
セットを、頻繁に使用しているという以前の報告を裏付けるものとなっています。

ドキュメントの 1 つには、「Anxun Information Technology Co., Ltd.」と翻訳されるフッターが含まれています。これは、i-Soon が販売するさまざまなソフトウェア ツールの製品マニュアルのようです。これらのツールには、Windows、Mac、iOS、Android、Linux 用のリモート コントロール管理システムが含まれています。

図 2 に示した Linux 用のリモート
コントロール管理ソフトウェアは注目に値します。なぜなら、同ツールの機能説明用に文書内で提供されているこのスクリーンショットのマルウェア コントロール パネル名は「Treadstone」となっているからです。2019 年の米国大陪審による成都404の従業員 3 名の起訴では、直接 Treadstone に言及しています。

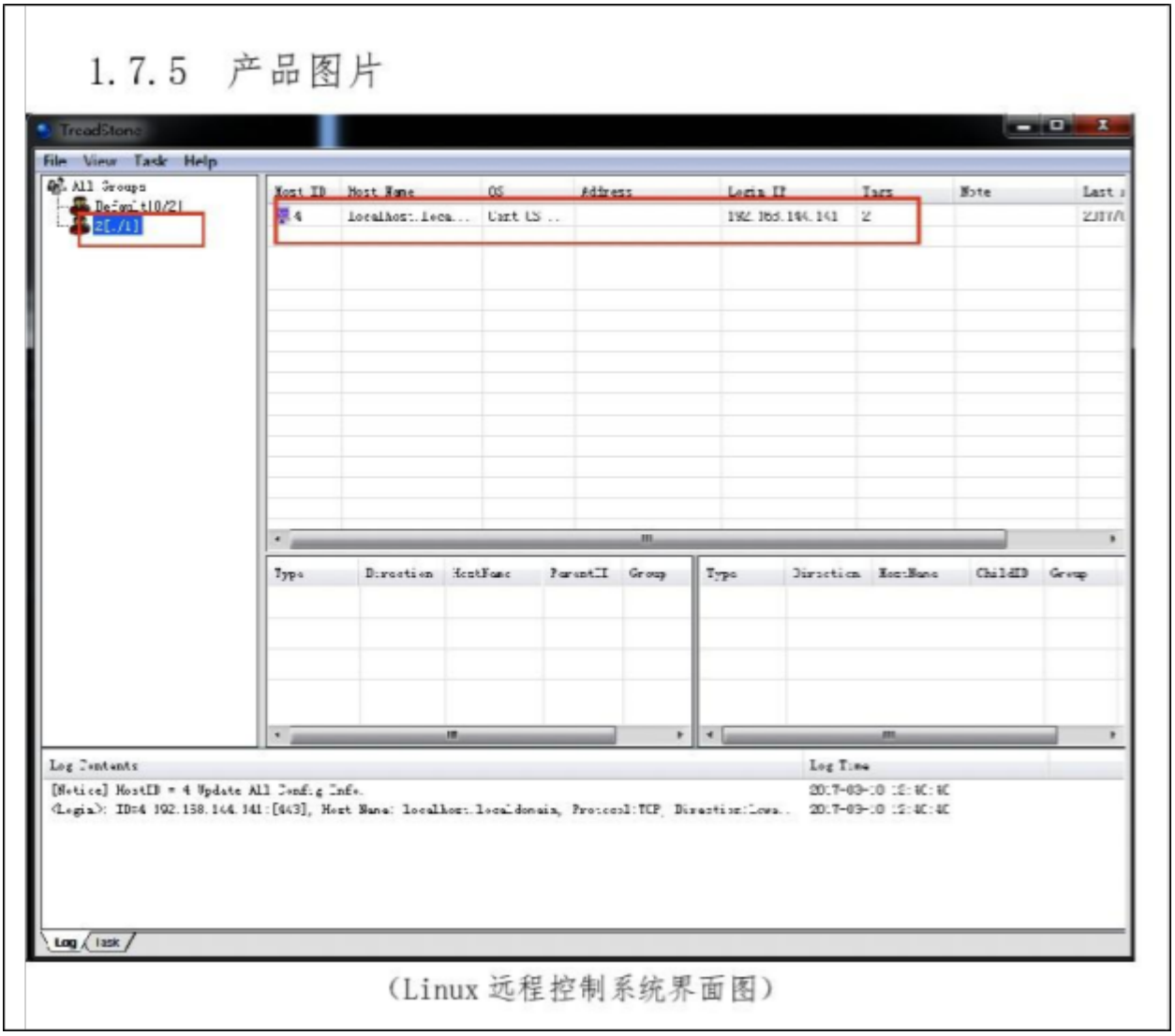

図 2. 漏えいした製品マニュアルからの Treadstone Linux マルウェア コントロール パネルのスクリーンショット

起訴状では、Treadstone マルウェア コントローラー ソフトウェアは「当時、少数のハッカー グループのみが使用していた Winnti マルウェアと連携するように設計されていた」とされています。成都404 がソフトウェア開発契約をめぐる紛争で i-Soon に対する訴訟を起こしたという 2023 年 10 月の報告からすると、i-Soon が Treadstone パネルを開発した可能性があります。

既知の中国製 APT ツールに関連するもう 1 つの文書は、Windows リモート コントロール管理システムに関するホワイトペーパーです。このドキュメントは、システムとネットワークのアーキテクチャ、製品の機能について説明しています。ツールの管理について説明しているページには、管理者パネルとおぼしきもののスクリーンショットが掲載されています (図 3 参照)。

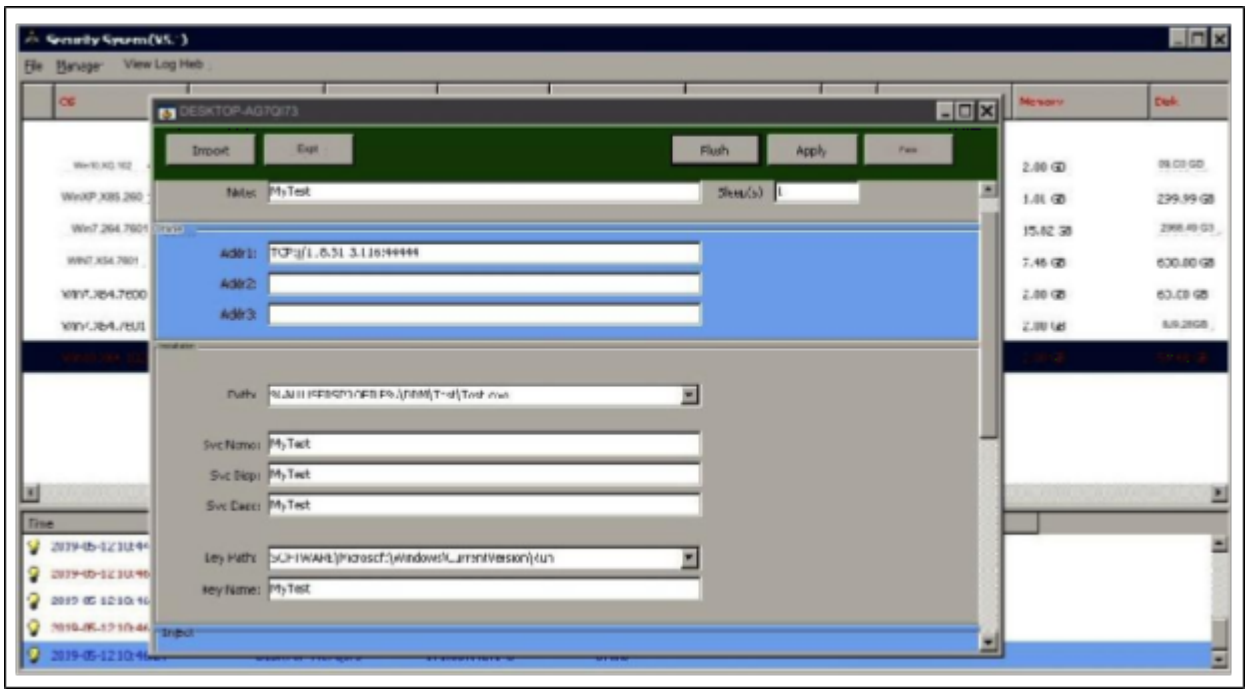

図 3. 既知の中国製 APT ツールと関連している Windows リモート
コントロール管理システムの管理者パネル

このスクリーンショットには、構成済みのパブリック IP アドレス/ポートとして `TCP[://]118.31.3[.]116:44444` が表示されています。SentinelLabs はこの IP アドレスが 2021 年 8 月に ShadowPad の C2 サーバーとして使用されていたと報告し、同アドレスを Winnti グループに帰属させています。Winnti グループに対するこの 2 つめのリンクは、i-Soon が既知の Winnti ツール セット開発に関与していたという証拠をさらに追加するものとなっています。

結論

今回のデータ漏えいは、これまで米国政府の起訴や報告書を通じてしか明らかにされてこなかった中国の民間部門のハッキング産業に関し、特異な洞察を提供するものとなっています。また、グループ間での同一ツール セットの共有・再販方法がどのようなものであるかなど、中国の脅威アクターの能力に関してさらに理解を深めてくれるものでもあります。こうしたツールの拡散は、防御側や脅威インテリジェンス アナリストによる帰属特定をさらに困難なものにします。

Unit 42 は漏えいデータの分析を継続し、共有すべき情報が見つかりしだい、本稿を定期的に更新します。

漏えいデータに関する弊社の現在の理解に基づき、弊社のお客様は、パロアルトネットワークスのセキュリティ製品を通じ、本稿で言及する中国の脅威アクターが使用するツールや手法からより適切に保護されています。本稿で取り上げたキャンペーンに関連する悪意のある IP アドレスは Advanced URL Filtering によってブロックされます。

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。

追加リソース

- Probing Weaponized Chat Applications Abused in Supply-Chain Attacks – Trend Micro
- Missing Link: Tibetan Groups Targeted with 1-Click Mobile Exploits – The Citizen Lab, Munk School of Global Affairs and Policy, University of Toronto
- ShadowPad | A Masterpiece of Privately Sold Malware in Chinese Espionage – SentinelLabs, SentinelOne

2024-02-28 08:38 JST 2024-02-27 08:03 PST 2 3