MANDIANT

脅威インテリジェンス
レポート

APT43：北朝鮮のハッカー・グループがスパイ活動の資金調達にサイバー犯罪を利用

エグゼクティブ・サマリー

- APT43は、北朝鮮政権の国益を支持する活発なサイバー・オペレーターです。このグループは、中程度に高度な技術的な能力と、攻撃的なソーシャル・エンジニアリング戦術を組み合わせ、朝鮮半島の地政学的問題を重点的に扱う、韓国と米国の政府機関、学術機関、シンクタンクを特に標的としています。
- Mandiantでは、APT43はエスピオナージ活動に加え、サイバー犯罪から資金を得ることによって、戦略的インテリジェンスの収集という第一の目的をサポートしていると見ています。
- 同グループは、偽装したペルソナや詐欺的なペルソナを多数作り出し、ソーシャル・エンジニアリングで使用しています。また、偽の身元情報を作成し、活動を展開するためのツールやインフラの購入に利用しています。
- APT43は、他の北朝鮮のスパイ工作員と複数の活動で連携しており、APT43が北朝鮮政府のサイバー組織において、主要な役割を担っていることを示しています。

脅威の詳細

Mandiantでは、APT43は中程度の技術洗練度を有するサイバー・オペレーターであり、北朝鮮政府の国益を支持するものであると強く確信しています。APT43による活動には、北朝鮮政府の地政学的利益に整合する戦略的な情報収集、エスピオナージ活動をサポートするための認証情報の窃取とソーシャル・エンジニアリング、オペレーション資金獲得のための金銭目的のサイバー犯罪が含まれます。APT43は2018年から追跡されており、その情報収集の優先順位は、北朝鮮の主要な対外情報機関である朝鮮人民軍偵察総局の任務と整合しています。APT43は外交政策と核安全保障の問題に焦点を当てており、これは北朝鮮の戦略的野心と核に関する野心を裏付けるものと言えます。しかし、このグループは2021年のほとんどの時期を通して、パンデミック対策の支援など、健康関連の分野に重点を置いており、このことは、グループが北朝鮮政府の優先事項の変化に対応していることを示します。

- APT43と関連付けられる活動で公に報告されているものは、「Kimsuky」または「Thallium」として報告されることが多く、認証情報の窃取とエスピオナージ活動を含んでいます。これは、進行中の地政学的動向について北朝鮮上層部に情報を提供することを目的としている可能性が高いと見られます。
- APT43の攻撃で最も頻繁に観察されるものは、ソーシャル・エンジニアリング戦術の一環として実行される、偽装したドメインやメールアドレスを用いたスピア・フィッシング活動です。正規サイトを装ったドメインは、認証情報の窃取活動に使用されています。
- APT43がゼロデイ脆弱性を悪用した事例は確認されていません。
- APT43はテンポの速い活動を維持し、フィッシング活動と認証情報の窃取活動を活発に行い、北朝鮮のサイバー・エコシステムの他の要素との連携を示しています。
- 標的とされる主な地域は韓国、米国、日本、欧州であり、特に狙われている業界は以下のとおりです。
  - 政府機関
  - 地理的政策や核政策に重点を置いた教育機関／研究機関／シンクタンク
  - ビジネス・サービス
  - 製造業

グループによる全体的な標的範囲は広範ですが、活動の最終目的の中心は、北朝鮮の兵器開発を可能にすることだと考えられます。これらの活動には、国際交渉、制裁政策、他国の対外関係や国内政治などについての情報収集など、北朝鮮の核に関する野心に影響するものが含まれています。

標的の変化

APT43と関連付けられる活動は北朝鮮の国益と密接に整合しており、金正恩および世界的に孤立した北朝鮮の支配層に影響を与える地政学的発展と強い相関関係があります。Mandiantが追跡を始めてから、APT43は継続して、朝鮮半島に影響する安全保障問題に関心を寄せる韓国および米国の組織に対して、エスピオナージ活動を行ってきました。

- 2020年10月より前は、APT43は主に、韓国と米国にある政府機関、外交機関、朝鮮半島に影響する外交政策や安全保障問題に関心を寄せるシンクタンク関連の組織を標的としていました。
- 2020年10月から2021年10月にかけて、APT43の活動のかなりの部分が、医療関連分野や製薬会社を標的としていました。これは、北朝鮮における新型コロナウイルス感染症への対応を支援するためであったと考えられます。狙った情報が北朝鮮政権にどの程度のメリットをもたらしたかは不明ですが、世界的なコロナ禍において、グループが北朝鮮の他のサイバー攻撃者と連携し、この活動にかなりのリソースを割いて優先事項としていたことを示す兆候があります。
- この期間を通じて、韓国、米国、欧州、日本を標的とするAPT43のエスピオナージ活動が継続していました。
- 注目すべき点として、観察されたAPT43活動は、展開するマルウェアの違いなど、標的に応じてわずかな違いがありました。たとえば、コロナ禍における韓国を標的としたAPT43活動では、VENOMBITE（ローダー）、SWEETDROP（ドロッパー）、BITTERSWEET（バックドア）の使用が特徴的でした。

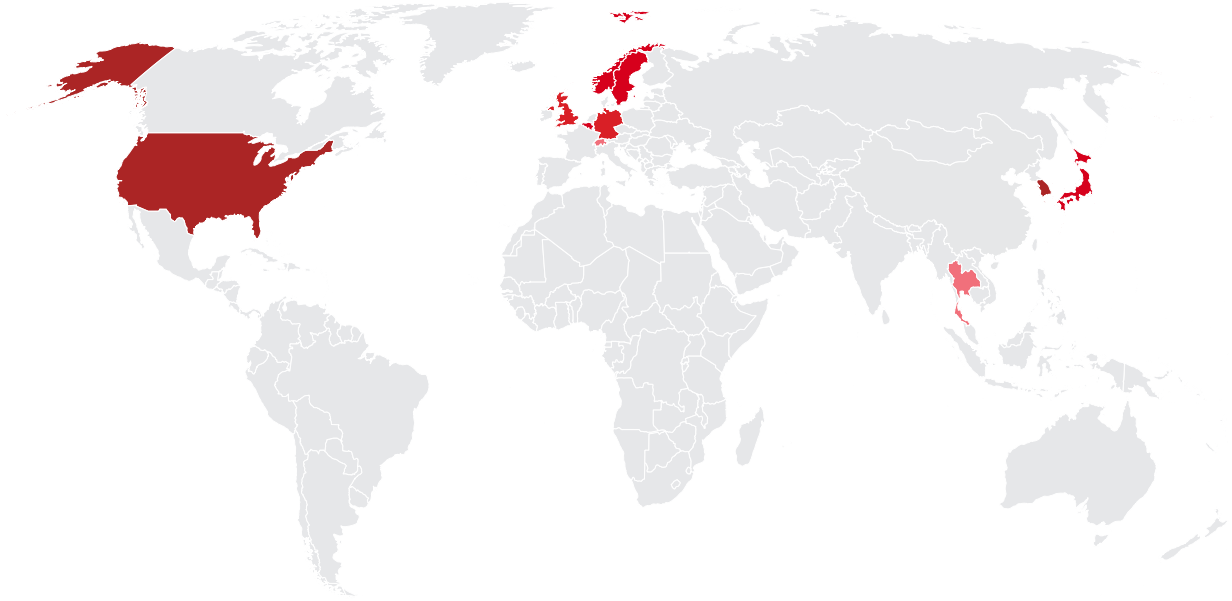

図1：APT43の標的となっている国（濃い赤は、観察された活動の頻度が高いことを示す）

- 市民団体／非営利団体
- 教育機関
- 政府機関
- メディア／エンターテインメント
- 建設／材料
- 防衛／航空宇宙
- 通信
- ハイテク
- 製薬
- コンサルティング／専門サービス

図2：APT43が直接の標的にした産業

サイバー活動：

APT43は多くの場合、カスタマイズしたスピア・フィッシング・メールを利用して、標的とする情報へのアクセスを取得します。ただし、この攻撃グループは、戦略的インテリジェンスの収集をサポートするために他のさまざまな活動にも関与しています。これには、認証情報を収集するための偽装ウェブサイトの使用や、資金を調達するためのサイバー犯罪の実行が含まれます。

- この攻撃グループは、特に核の安全保障と核不拡散に関して、定期的におとり文書を更新し、特定の対象者に合わせてカスタマイズしています。
- APT43は、標的とする分野（安全保障や防衛など）における主要関係者になりすますなど、説得力のあるペルソナを作成することや、窃取した個人情報（PII）を活用してアカウントの作成やドメインの登録を行うことに長けています。
- APT43は、関連性の高いおとり文書と偽装したメール・アドレスを使用します。
  - APT43はまた、侵害した個人から窃取した連絡先リストを活用して、スピア・フィッシング攻撃に追加する標的を特定しています。
- APT43は、北朝鮮のチュチェ（主体）思想と整合する形で運用インフラを購入するのに十分な額の暗号通貨の窃取と資金洗浄を行い、逼迫する北朝鮮政府の財政を支援しています。

エスピオナージ

APT43の第一の目的はサイバー・エスピオナージであると考えられます。得られたデータから、このグループの他の活動は、戦略的インテリジェンスの収集をサポートするために実行されていることが示されています。

- このグループは主に、米軍および米国政府が策定および保管している情報、防衛産業基盤（DIB）、核安全保障政策と核不拡散に関係する米国内の学術機関やシンクタンクによる研究結果や安全保障政策に関心を持っています。
- APT43は、韓国の同様の業界、特にグローバル政策と地域政策を扱う非営利団体や大学に関心を示しています。また、北朝鮮への輸出が制限されている物品に関する情報が得られる可能性のある、製造業などの企業にも関心を示しています。これには、燃料、機械、金属、輸送車両、兵器が含まれます。
- APT43は、記者やシンクタンクのアナリストを装い、標的とする人物と信頼関係を築き、情報を収集します（図3）。公開された報告にも裏付けられているように、このグループは学術機関関係者を信頼させて、戦略的分析をスパイ攻撃者に直接提供させています。

日付：2022 年 10 月 14 日（金）03:13:48 -0400
件名：ご意見をお聞かせください
送信者：<redacted>@voanews[.]live

拝啓
突然のメール失礼いたします。<redacted> の <redacted> と申します。
10 月 4 日、新たな世界秩序の中、従来の戦略を用いて、北朝鮮が強力なミサイルを発射しました。日本に対して北朝鮮がミサイルを発射したのは 2017 年以来となります。当時の米国大統領はトランプ氏であり、金正恩氏は米国政府との対立を激化させようとしていたと見られています。

この件に関していくつかお伺いします。
1) 10 月中旬の中国共産党大会の開催直後に、北朝鮮は再び核ミサイル実験を実施すると思われますか？
2) 北朝鮮の脅威に対して、より冷静なアプローチが必要となると思われますか？
3) 日本は防衛予算の増加や積極的な防衛政策へと動くと思われますか？
5 日以内にご回答をいただければ幸いです。
お手数ではございますが、ご協力いただけますようお願いいたします。

何卒宜しくお願いいたします。
<redacted>

図3：APT43がジャーナリストを装って標的との信頼関係を築こうとしているメールの例

- APT43に関連する技術的な指標は、2022年の韓国大統領選挙を前に、政策転換の可能性を探るため、このグループが韓国の政治団体を標的としたという、韓国語の報告を一部裏付けています。

非サイバー活動を含む他の北朝鮮の活動についても、APT43が内部監視を行っていることを示す兆候があります。APT43は、自らの攻撃活動の内部にいる者を含め、エスピオナージ担当者を侵害しています。しかし、これが自己監視を目的とした意図的なものか、それとも偶発的なものであり、オペレーションのセキュリティの低さを示すものであるのかは不明です。

認証情報の収集

APT43は、認証情報の収集活動を行い、学術、製造、国家安全保障の各分野に属する組織の財務データ、個人情報、顧客データを直接侵害しています。その活動は、特に韓国において顕著です。具体的には、標的とする国で人気のある検索エンジン、Webプラットフォーム、暗号通貨取引所を装ったドメインを登録しています。入手した認証情報は、APT43の目標を進展させる活動をサポートするために使用すると見られます。

- 収集された認証情報データは、オンラインのペルソナを作成し、正規のサービスを偽装したサイトなど、サイバー・エスピオナージ活動のためのインフラを構築するために使用されています（図4）。

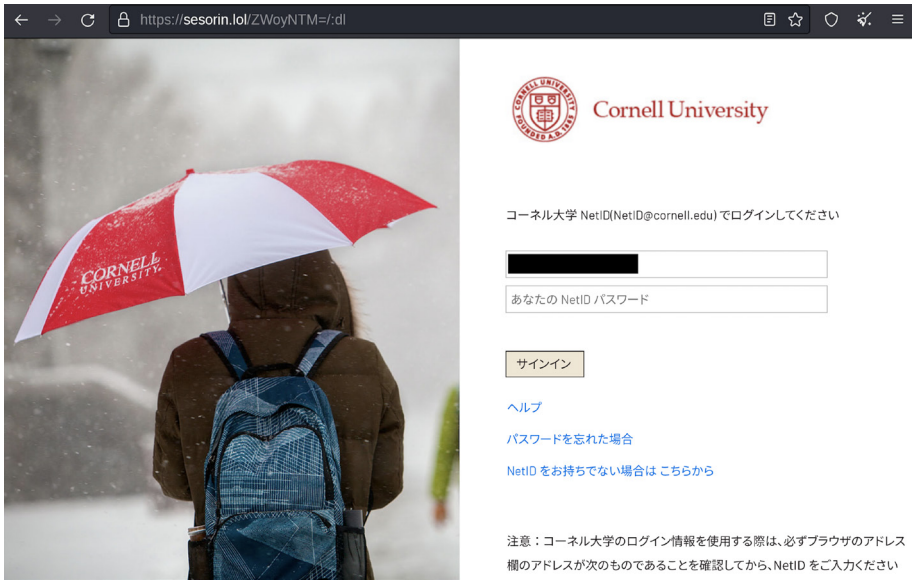

図4：APT43の管理下にあるsesorin.lol（コーネル大学サイトのなりすまし）の認証情報収集サイト

- このグループは、侵害済みインフラと攻撃者自身が所有するインフラの両方を活用し、マルウェアをホストしてターゲットに配信し、認証情報を収集しています。
  - 2018年には、侵害済みWebサイトをネットワーク・インフラの一部として利用し、PASSMARKマルウェアとLATEOPマルウェアを配信しました。

標的が変化したことは、収集要件の戦術の変化を反映している可能性があります。

- 2021年末、APT43は宗教団体、大学、非政府組織（NGO）に対する認証情報の収集活動を再開しました。これらの活動は北朝鮮と韓国や日本のカウンターパートとの間の「トラック2」の外交チャネルを標的にしていたことを示す兆候があります。注目すべき点として、この活動は、新型コロナウイルス感染症関連の組織に一時的に焦点を合わせた後で、エスピオナージの標的に焦点を置いたメインの活動に戻ったことを意味します。
- 2022年初め、Mandiant Intelligenceは、韓国を中心に、学術機関、ジャーナリスト、政治家、ブロガー、その他の民間人を対象とした複数の認証情報収集活動が実施されたことを観察しています。
- 2022年中ごろまでに、認証情報の窃取活動は、韓国問題、人権、学術、宗教、暗号通貨と関連のある、韓国のブロガーやソーシャル・メディア・ユーザーへと標的を移しています。

暗号通貨の標的化

APT43は、暗号通貨と暗号通貨関連サービスを標的としてきました。APT38のように、北朝鮮政府のための資金調達が主な目的と見られる他の北朝鮮のグループとは異なり、APT43は、自分たちの活動を維持するために、そうした攻撃活動を行っている可能性が高いと見られます。

- Mandiantでは、APT43が暗号通貨サービスを利用して、窃取した資金のロンダリングを行っていることを特定しています。関連する活動として、支払い方法、エイリアス、購入に使用したアドレス（図5）が特定されており、ハッシュ・レンタルとクラウド・マイニング・サービスを利用して、窃取した暗号通貨をロンダリングし、クリーンな暗号通貨に換えている可能性が高いと見られます。

B 様

あなたの Namecheap アカウントに、Bitcoin のお支払い $120.00 が追加されたことをお知らせします。
このアカウント残高を Namecheap.com での商品の購入や更新にお使いいただけます。

ユーザー名：BRoyal1990
取引 ID：82073030
取引参照番号：GKRwiyWiTTUXreqpvxNv4A
金額：$120.00

この取引の詳細は、弊社の「資金追加履歴」ページ (https://manage.www.namecheap.com/myaccount/reports/funds-report.asp) でご覧いただけます。

ご質問は弊社サポート担当 (http://www.namecheap.com/support) までご連絡ください。

今後ともよろしくお願いいたします。

Namecheap.com サポート

図5：窃取したBitcoinを使用して、APT43がNamecheapサービスを購入している可能性が高い

  - ハッシュ・レンタルやクラウド・マイニングのサービスは、有料でハッシュ・パワーを提供します。ハッシュ・パワーは、バイヤーの本来の支払いに対してブロックチェーン・ベースの関連付けを一切行わずに、バイヤーの指定したウォレットに暗号通貨をマイニングするために使用されます。
  - インフラやハードウェアの購入にはいくつかの支払い方法が使用されており、ここには過去の攻撃活動で入手した可能性が高いPayPal、American Expressカード、Bitcoinが含まれています。
- APT43は不正なAndroidアプリを使って、暗号通貨ローンを探している中国のユーザーを標的にしたようです。このアプリと関連ドメインが、おそらく認証情報を収集しました（図6を参照）。

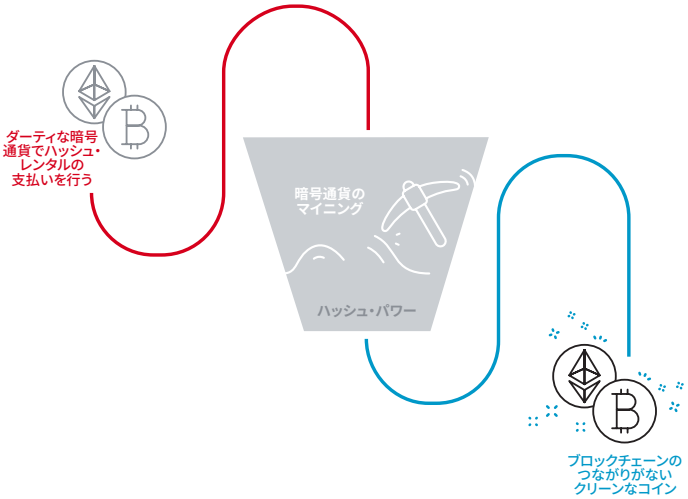

図6：APT43が使用している、ハッシュ・レンタル・サービス経由での暗号通貨のロンダリング

- これまでサイバー・エスピオナージに重点を置いてきたグループも含め、北朝鮮のグループの間で金銭目的の活動が多く見られることは、自己資金調達が広く義務付けられており、リソースを追加しなくても活動を維持できることが期待されていることを示しています。

素性

Mandiantでは、APT43が北朝鮮政府の広範な地政学的目的を支援するために活動する、国家の支援を背景としたサイバー攻撃者であると強く確信しています。

- このグループの主な活動は、北朝鮮の最大のライバル国である韓国に関する情報収集ですが、その標的は北朝鮮の国益の変化と一致しています。
  - さらには、米国による韓国への支援も、APT43の主要な標的となっています。
- APT43は、北朝鮮の既知の攻撃グループとインフラやツールを共有しています。このことは、グループの役割と目的が国家の支援を背景とした広範なサイバー組織と整合していることを示します。

具体的には、APT43が北朝鮮の主要な対外情報機関である朝鮮人民軍偵察総局（RGB）に関連付けられると、Mandiantはある程度の確信を持って見ています。

- APT43の要素が、他のRGB関連のサイバー・エスピオナージ攻撃者、具体的にはTEMP.Hermit（例：UNC1758）と協力していることが特定されています。これについては次のセクションで詳しく述べます。

他のエスピオナージ攻撃グループとのつながり

APT43の活動は時に、北朝鮮の他のサイバー・エスピオナージ攻撃グループの活動と共通点が見られます。しかし、Mandiantはこれらのグループは異なるものであると見ており、共通点は一時的な協力や限定的なリソースの共有の結果である可能性が高いと考えています。このような共通点は主に、北朝鮮の単一のクラスターが従来使用していたマルウェア・ファミリーが、新たな攻撃者によって使用されるという形で現れます。

- APT43が用いるマルウェアは当初、コロナ禍において、TEMP.Hermitのものと疑われるクラスター（一般に「Lazarus」と呼ばれることが多い）に関連していると見られていました。APT43とTEMP.Hermitのクラスターとの間にはある程度の共有リソースが観察されますが、Mandiantでは、これらのつながりは一時的なものであると評価しています（図7）。
  - 具体的には、このような活動には、新型コロナウイルス感染症への対応に関与する世界的組織を標的とした活動が含まれていました。これらの活動の一部では、APT43のサブセットがほぼ確実に他のRGB関連の組織と密接に協力していました。これには、既存のマルウェア・ツールの共有、当初は拡大タスクに使用された新たなツールの開発、医療研究および関連組織に対する持続的な活動の実行が含まれます。
    - これらの活動に使用するために、ダウンローダーPENCILDOWNなどのAPT43マルウェアから派生した別のツールには、PENDOWN、VENOMBITE、EGGHATCH（すべてダウンローダー、図7参照）があります。
    - これらのツールは、APT43の中心的なツールであるLOGCABINやLATEOPなどと併用されていました。
    - HANGMAN.V2はHANGMANバックドアから派生したもので、通常はTEMP.Hermitに関連付けられますが、HANGMAN.V2のようなマルウェア亜種をAPT43が使用していることは、2020年の協力活動においてある程度の伝播があったことを示しています。
- 明らかにグループを超えているこのような活動は、「Bureau 325」として公表され、「Cerium」として報告された活動とも合致しています。
- 他にも、APT43と同じツールを一部利用している未分類のクラスターが特定されています。たとえば、あるクラスターはPENCILDOWNを使用し、Androidのモバイル・ウォレット・アプリを侵害して暗号通貨を窃取していました。
- 逆に、別の例においては、暗号通貨を標的とするUNC1069と強い関連があるツール、LONEJOGGERをAPT43が展開していることが観察されています。
  - UNC1069は北朝鮮のサイバー犯罪攻撃であると疑われていますが、APT38との関連の確信度は高くありません。

オープンソースでは、公開レポートに「Kimsuky」活動についての別の活動が含まれることがあります。しかし、Mandiantではこれらのグループ、特にKONNIなどのマルウェア・ファミリーと関連ツールのCABRIDEおよびPLANEPATCHを利用するグループについては、別々に追跡しています。これらの活動クラスターはAPT43と共通点がありますが、関連性は弱く、別々のグループであると考えています。

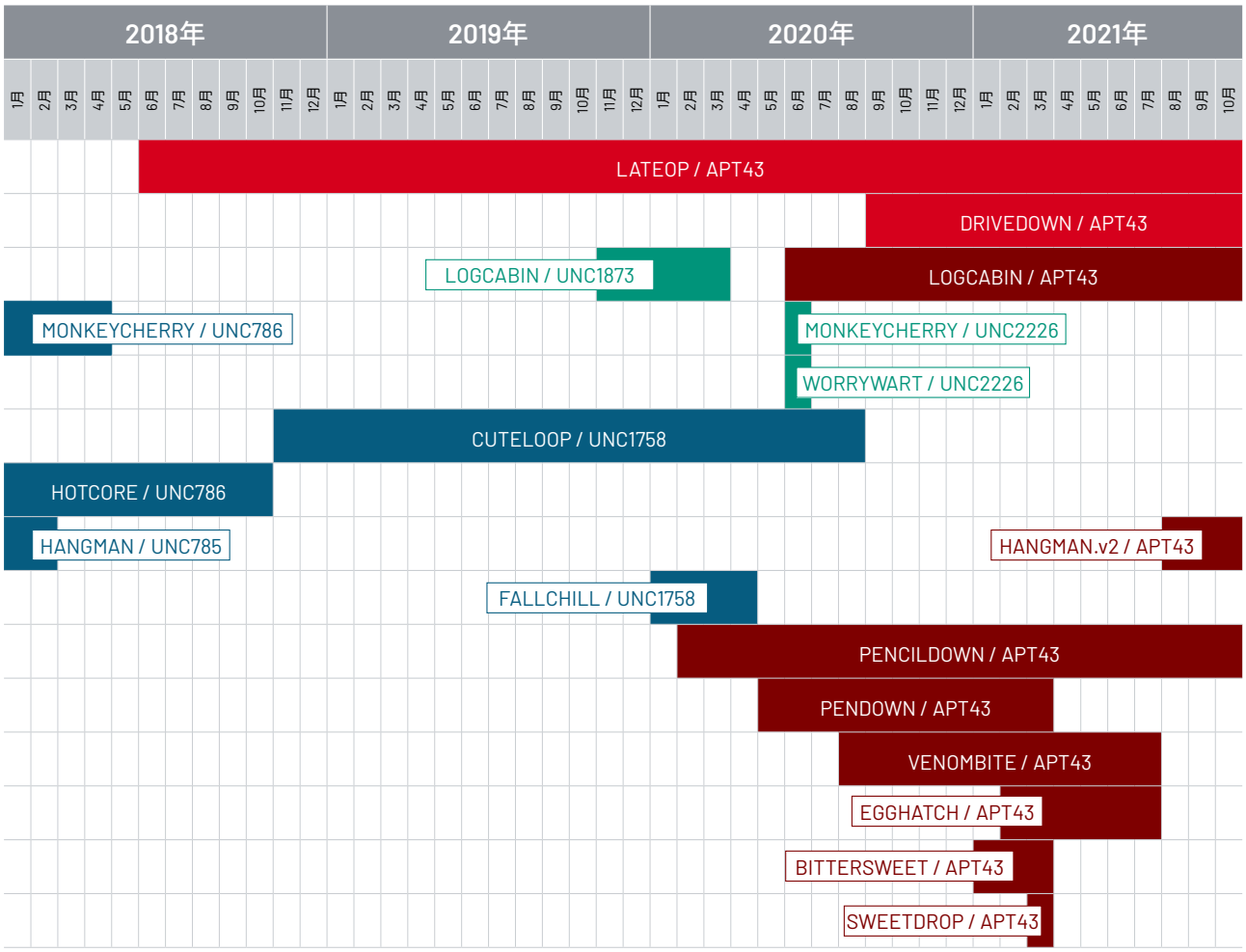

図7：マルウェアの展開に基づく、APT43、TEMP.Hermit、北朝鮮のその他の追跡対象クラスターの収束

マルウェア

APT43は、非公開マルウェアと一般に入手可能なツールの両方を含む、比較的広範なツールキットを利用しています。APT43について報告しているオープンソースの多くは、LATEOP（一般に「BabyShark」として知られる）を使用するグループを追跡していますが、Mandiantでは、このオペレーションのマルウェア・ライブラリが時と共に着実に進化、拡大していることを観察しています。ツールの一部は、以前のツールからコードを大量に借用し（図8）、これに改良を加え、機能を追加しています。

- このグループは、gh0st RAT、QUASARRAT、AMADEYといった一般に入手可能なマルウェアを展開していますが、その活動は、VisualBasicスクリプトに基づくバックドアであるLATEOPと関連付けられることでよく知られています。
- APT43は、手持ちのツールからさまざまな亜種を開発し、複数のプラットフォームを標的にできるようにしています。たとえば、Windowsベースのダウンローダーであ るPENCILDOWNのAndroid用の亜種が特定されています。

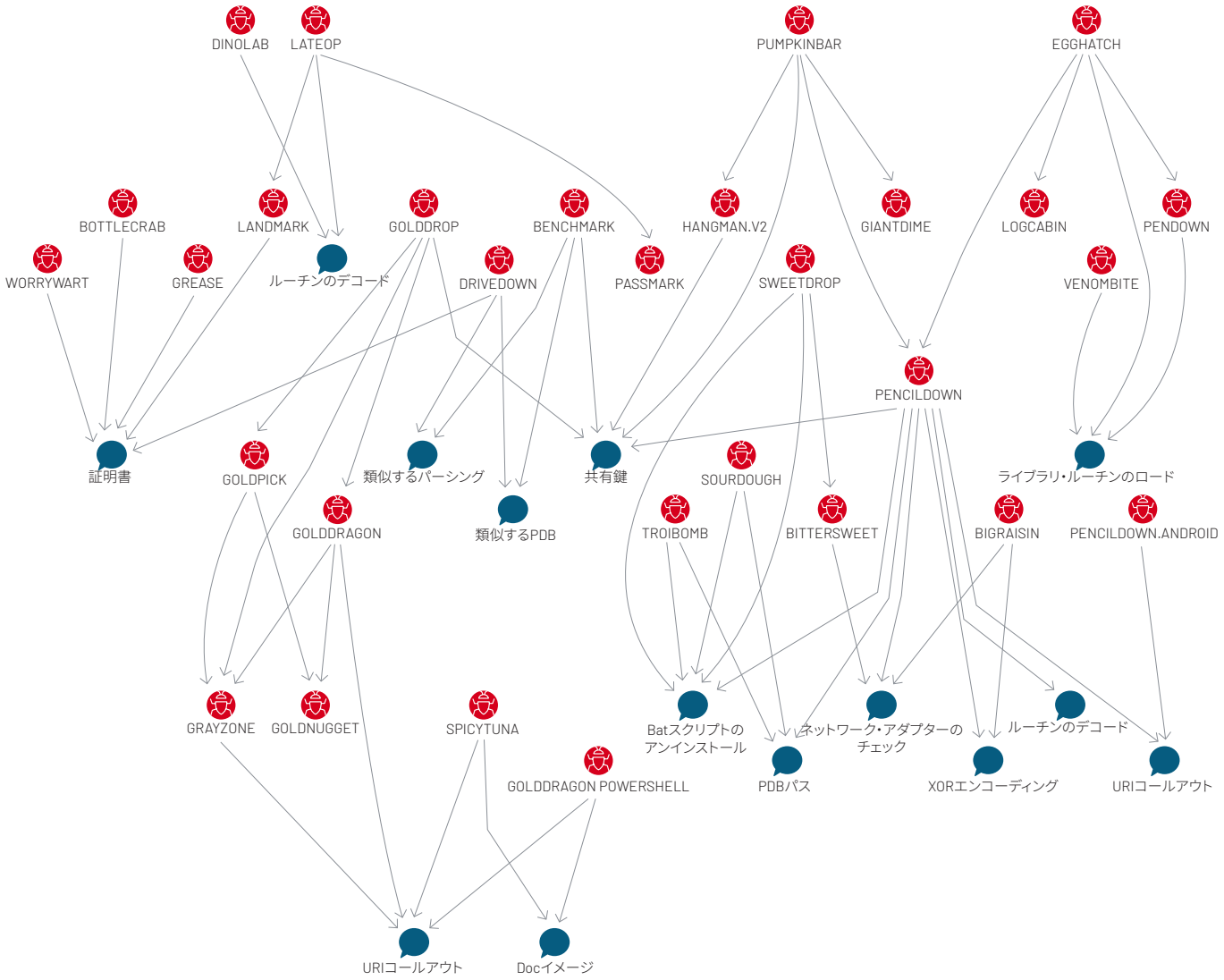

図8：APT43が使用するツールのコード・ファミリーの共通点

今後の展望

北朝鮮の国家的優先事項が大きく変化しない限り、APT43は北朝鮮の国益をサポートするエスピオナージ活動や金銭目的の活動を今後も活発に実行していくと予想されます。北朝鮮はサイバー機能への依存を高めていると見られ、APT43の継続的かつ執拗なオペレーション開発の状況は、同国がAPT43のようなグループに持続的に資金を提供し、依存していることを反映しています。

APT43が急激かつ一時的に医療機関および製薬関連企業に標的を移したことからも、APT43が北朝鮮上層部の要求に密接に対応していることを示しています。APT43の中心的なタスクは、政府、軍、外交機関に対するスピア・フィッシングや認証情報の収集ですが、APT43は、政権を支える必要性から金銭目的のサイバー犯罪を実行するなど、スポンサーの意向に合わせて最終的に標的やTTP（戦術、技術、手順）を変更しています。

技術解説：アタック・ライフサイクル

図9：APT43のアタック・ライフサイクル

技術解説：MITRE ATT&CK

Initial Access	
T1566	Phishing
T1566.001	Spearphishing Attachment
T1566.002	Spearphishing Link

Resource Development	
T1583.003	Virtual Private Server
T1584	Compromise Infrastructure
T1588.003	Code Signing Certificates
T1588.004	Digital Certificates
T1608.003	Install Digital Certificate
T1608.005	Link Target

Execution	
T1047	Windows Management Instrumentation
T1053.005	Scheduled Task
T1059	Command and Scripting Interpreter
T1059.00:	PowerShell
T1059.003	Windows Command Shell
T1059.005	Visual Basic
T1059.007	JavaScript
T1129	Shared Modules
T1203	Exploitation for Client Execution
T1204.001	Malicious Link
T1204.002	Malicious File
T1569.002	Service Execution

Command and Control	
T1071.001	Web Protocols
T1071.004	DNS
T1090.003	Multi-hop Proxy
T1095	Non-Application Layer Protocol
T1102	Web Service
T1102.002	Bidirectional Communication
T1105	Ingress Tool Transfer
T1132.001	Standard Encoding
T1573.002	Asymmetric Cryptography

Discovery	
T1007	System Service Discovery
T1010	Application Window Discovery
T1012	Query Registry
T1016	System Network Configuration Discovery
T1033	System Owner/User Discovery
T1057	Process Discovery
T1082	System Information Discovery
T1083	File and Directory Discovery
T1087	Account Discovery
T1518	Software Discovery
T1614.001	System Language Discovery

Collection	
T1056.001	Keylogging
T1113	Screen Capture
T1115	Clipboard Data
T1213	Data from Information Repositories
T1560	Archive Collected Data
T1560.001	Archive via Utility

Persistence	
T1137	Office Application Startup
T1505.00	Web Shell
T1543.003	Windows Service
T1547.001:	Registry Run Keys / Startup Folder
T1547.004	Winlogon Helper DLL
T1547.009	Shortcut Modification

Defense Evasion	
T1027	Obfuscated Files or Information
T1027.001	Binary Padding
T1027.002	Software Packing
T1027.005	Indicator Removal from Tools
T1027.009	Embedded Payloads
T1036	Masquerading
T1036.001	Invalid Code Signature
T1036.007	Double File Extension
T1055	Process Injection
T1055.001	Dynamic-link Library Injection
T1055.003	Thread Execution Hijacking
T1070.004	File Deletion
T1070.006	Timestomp
T1112	Modify Registry
T1134	Access Token Manipulation
T1140	Deobfuscate/Decode Files or Information
T1218.005	Mshta
T1497	Virtualization/Sandbox Evasion
T1497.001	System Checks
T1548.002:	Bypass User Account Control
T1553.002	Code Signing
T1564.003	Hidden Window
T1564.007	VBA Stomping
T1620:	Reflective Code Loading
T1622	Debugger Evasion

Impact	
T1489	Service Stop
T1529	System Shutdown/Reboot

Exfiltration	
T1020	Automated Exfiltration

Credential Access:	
T1110	Brute Force
T1555.003	Credentials from Web Browsers

技術解説：APT43が使用したマルウェア

マルウェア・ファミリー	機能	入手可能性	説明
AMADEY	ダウンローダー	公開	AMADEYはCで書かれたダウンローダーで、HTTP経由でペイロードを取得します。ダウンロードしたペイロードがディスクに書き込まれ、実行されます。
BENCHMARK	ドロッパー	非公開	BENCHMARKはC/C++で書かれたドロッパーで、ファイル名を読み込み、ハードコードされたパスからBase64エンコードされたペイロードを抽出し、ペイロードをデコードして、ディスクにドロップします。
BIGRAISIN	バックドア	非公開	BIGRAISINはC/C++ Windowsベースのバックドアです。ダウンロードされたコマンドの実行、ダウンロードされたファイルの実行、ファイルの削除を行うことができます。
BITTERSWEET	ダウンローダー	非公開	BITTERSWEETはC/C++ Windowsダウンローダーです。基本的なシステム情報を収集してから、次のステージをディスクにダウンロードして実行します。
BRAVEPRINCE	ダウンローダー	公開	BRAVEPRINCEはC/C++ダウンローダーです。Daumメール・サービスを使用して、収集したシステム情報をアップロードし、ファイルをダウンロードします。
COINTOSS COINTOSS.XLM	ダウンローダー	非公開	COINTOSSはC/C++ダウンローダーです。Windows Management Instrumentationコマンドライン（WMIC）ユーティリティを使用して、FTP経由でペイロードをダウンロードします。その後、COINTOSSは自らをアンインストールするバッチ・スクリプトを作成して実行します。
DINOLAB	ビルダー	非公開	DINOLABはC/C++ビルダーです。ファイルの暗号化および復号化、VBSスクリプトの難読化、ファイルの感染に使用します。
DRIVEDOWN	ダウンローダー	非公開	DRIVEDOWNはC/C++ Windowsダウンローダーで、埋め込みスクリプトの実行と、OneDriveからのステージのダウンロードを行うことができます。
EGGHATCH	ダウンローダー	非公開	EGGHATCHはC/C++ Windowsダウンローダーです。mshta.exeを使ってスクリプトのダウンロードと実行を行います。
FASTFIRE	バックドア	非公開	FASTFIREは不正なAPKで、サーバーに接続して、侵害されたデバイスの詳細をC&Cに送り返します。
GhOst RAT	バックドア	公開	GhOstはC++で書かれたバックドアで、TCPまたはUDP上でカスタム・バイナリ・プロトコル経由で通信を行います。一般的に、各メッセージの最初にあるパケット・シグネチャを特徴とし、これはサンプルによって異なります。
GOLDDRAGON GOLDDRAGON. POWERSHELL	ダウンローダー	非公開	GOLDDRAGONはCで書かれたダウンローダーで、HTTP経由でリモート・サーバーからペイロードを取得します。ダウンロードされたペイロードがディスクに書き込まれ、実行されます。GOLDDRAGONはさらに、ハングルのワードプロセッサ文書からペイロードを抽出し、これをスタートアップ・ディレクトリに書き込みます。その結果、現在のユーザーがログインする際に新たなファイルが実行されます。
GOLDDROP	ドロッパー	非公開	GOLDDROPはC/C++ Windowsドロッパーです。リソース・ファイルを復号し、ファイル・システムに保存し、これを別のプロセスに注入します。
GOLDSMELT	ユーティリティ	非公開	GOLDSMELTはC/C++ユーティリティで、rundll32.exeプロセスを終了させ、ログに使用されている可能性が高いファイルを削除します。
GRAYZONE	バックドア	非公開	GRAYZONEはC/C++ Windowsバックドアで、システム情報の収集、キーストロークのロギング、C&Cサーバーからの追加ステージのダウンロードを行うことができます。
HANGMAN.V2	バックドア	非公開	HANGMAN.V2はバックドアHANGMANの亜種です。HANGMAN.V2はHANGMANと非常に似ていますが、ネットワーク通信にHTTPを使用し、C&Cサーバーに渡すデータのフォーマット形式が異なります。
Invoke-Mimikatz	認証情報の窃取	公開	Invoke-MimikatzはPowerShellスクリプトで、Mimikatz認証情報窃取DLLを反映的にメモリにロードします。
JURASSICSHELL	ユーティリティ	非公開	JURASSICSHELLはPHPファイル管理Webシェルで、攻撃者がファイルのダウンロードとアップロードを行うことができます。

マルウェア・ファミリー	機能	入手可能性	説明
LANDMARK LANDMARK.NET	起動ツール	非公開	LANDMARKはC/C++ Windows起動ツールで、ディスクにdesktop.r5uとして保存されているファイルのロードと実行を行います。
LATEOP LATEOP.V2	データ・マイナー	非公開	LATEOPはデータ・マイニングVisualBasicスクリプトで、標的とするシステムのさまざまな特徴を列挙し、任意のVisualBasicコンテンツを追加で実行できます。LATEOPの展開では、PASSMARK認証情報窃取ペイロードのダウンロードと実行を伴うことがあります。一方、LATEOP.v2の展開は、BENCHMARKに起因する感染から生じることがあります。
LOGCABIN	バックドア	非公開	LOGCABINは、複数のステージを伴う、ファイルのないモジュール型バックドアです。ステージはいくつかのVisualBasicおよびPowerShellのスクリプトからなり、そのスクリプトがダウンロードされ、実行されます。LOGCABINは詳細なシステム情報を収集し、これをC&Cに送信してから、別のコマンドを実行します。
LONEJOGGER	ダウンローダー	非公開	LONEJOGGERはダウンローダー／ドロッパーで、暗号通貨サービス（取引所や投資会社など）を標的としていることが観察されています。.lnkショートカットを使用して、ガードレール付きHTMLアプリケーション・ペイロードをダウンロードします。
METASPLOIT	フレームワーク	公開	METASPLOITはペネトレーション・テスト・フレームワークで、脆弱性テスト、ネットワーク列挙、ペイロードの生成と実行、防御回避といった特徴があります。
PASSMARK	フレームワーク	公開	PASSMARK は、Web ブラウザーや電子メール アプリケーションからユーザー名とパスワードを盗む資格情報ハーベスターです。 PASSMARK は、ツール PassView から派生した可能性があります。
PENCILDOWN PENCILDOWN.ANDROID	ダウンローダー	非公開	PENCILDOWNはC/C++ Windowsベースのダウンローダーです。PENCILDOWNは基本的なシステム情報を収集し、これをC&Cサーバーに送信してから、次のステージを受信します。その後、応答のフラッグに基づいて、次のステージがメモリにロードされるか、直接実行されます。
PENDOWN	ダウンローダー	非公開	PENDOWNはC++で書かれたダウンローダーで、HTTP経由でペイロードを取得します。ダウンロードされたファイルはディスクに保存され、実行されます。
PUMPKINBAR	ドロッパー	非公開	PUMPKINBARはC/C++ドロッパーです。PUMPKINBARはそれ自体の中に、エンコードされ、埋め込まれた複数のペイロードを含めることができます。各ペイロードをデコードする鍵は、PUMPKINBAR実行可能ファイルの末尾に添付されています。ペイロードはディスクにドロップされ、実行されます。
QUASARRAT	バックドア	公開	QUASARRATは一般に公開されているWindowsバックドアです。Webサイトを開き、ファイルのダウンロード、アップロード、実行が可能です。QUASARRATはシステム情報を取得し、リモート・デスクトップまたはシェルとして機能し、またWebカメラをリモートで動作させることができます。このバックドアは、一般的に利用されているブラウザやFTPクライアントから、キーストロークのロギングやパスワードの窃取を行うこともできます。QUASARRATは元はxRATと呼ばれていましたが、2015年8月に開発者が名前を変更しました。
SLIMCURL	ダウンローダー	非公開	SLIMCURLはC/C++ダウンローダーです。Base64エンコードされたGoogle Driveのリンクとして次のステージを含みます。次のステージはcURLを使用してダウンロードされます。
SOURDOUGH	バックドア	非公開	SOURDOUGHはCで書かれたバックドアで、HTTPを経由して通信を行います。キーロギング、スクリーンショットのキャプチャ、ファイル転送、ファイル実行、ディレクトリ列挙を行うことができます。
SPICYTUNA	ダウンローダー	非公開	SPICYTUNAはVBAダウンローダーです。基本的なシステム情報を収集し、追加のステージのダウンロードと実行が可能です。

マルウェア・ファミリー	機能	入手可能性	説明
SWEETDROP	ドロッパー	非公開	SWEETDROPはC/C++ Windowsドロッパーです。埋め込みバイナリ・リソースをファイル・システムにドロップし、これを実行します。
TROIBOMB	バックドア	非公開	TROIBOMBはC/C++ Windowsバックドアで、システム情報の収集と、C&Cサーバーからのコマンドの実行が可能です。
VENOMBITE	ダウンローダー	非公開	VENOMBITEはC/C++ Windowsダウンローダーで、PENDOWNから進化したものです。同じカスタムのエンコーディング・ルーチンを使用しますが、ネットワーク機能は埋め込み実行可能ファイルに移されています。ダウンロードされたファイルはメモリにロードされ、実行されます。

技術解説：APT43の侵害指標の例

マルウェア・ファミリー	MD5のサンプル	SHA1	SHA256
AMADEY	982fc9ded34c854 69269eacb1cb4ef26	e205ed81ccb99641dcc 6c2799d32ef0584fa2175	557ff6c87c81a2d2348bd8d667ea8412a1a 0a055f5e1ae91701c2954ca8a3fdb
BENCHMARK	de9a8c26049699d bbd5d334a8566d38d	47a32bc992e5d4613b3 658b025ab913b0679232c	43c2d5122af50363c29879501776d907ea a568fa142d935f6c80e823d18223f5
BIGRAISIN	144bd7fd423edc3 965cb0161a8b82ab2	1087efbd004f65d226bf 20a52f1dc0b3e756ff9e	2b78d5228737a38fa940e9ab19601747c68 ed28e488696694648e3d70e53eb5a
BITTERSWEET	cd83a51bec0396f 4a0fd563ca9c929d7	f3b047e6eb3964deb04 7767fad52851c5601483f	fb7fb6dbaf568b568cd5e60ab537a42d59 82949a5e577db53cc707012c7f20e3
BRAVEPRINCE	33df74cbb60920d 63fe677c6f90b63f9	539acd9145befd7e670f e826c248766f46f0d041	94aa827a514d7aa70c404ec326edaaad4b 2b738ffaea5a66c0c9f246738df579
	ebaf83302dc78d9 6d5993830430bd169	bc6cb78e20cb2028514 9d55563f6fdcf4aaafa58	5cbc07895d099ce39a3142025c557b7fac 41d79914535ab7ffc2094809f12a4b
COINTOS	b846fa8bc3a55fa 0490a807186a8ece9	c0c6b99796d732fa534 02ff49fd241612a340229	855656bfecc359a1816437223c4a133359e 73ecf45acda667610fbe7875ab3c8
COINTOSS.XLM	f92a75b98249fa61 cf62e8b63cb68fae	e5b312155289cdc6a80 a041821fc82d2cca80bcd	d0971d098b0f8cf2187feeed3ce049930f 19ec3379b141ec6a2f2871b1e90ff7
DRIVEDOWN	1dcd5afeccfe204 0895686eefa0a9629	40826e2064b59b8b7b3 e514b9ef2c1479ac3b038	07aed9fa864556753de0a664d22854167a 3d898820bc92be46b1977c68b12b34
	5fe4da6a1d82561a1 9711e564adc7589	e79527f7307c1dda62c4 2487163616b3e58d5028	8d0bafca8a8e8f3e4544f1822bc4bb08ce aa3c7192c9a92006b1eb500771ab53
EGGHATCH	e8da7fcdf0ca67b 76f9a7967e240d223	b0c2312852d750c4bce b552def6985b8b800d3f3	9dac6553b89645ac8d9e0a3dc877d1264 1e6d05fb52e8de6ae5533b2bdf0abc9
FASTFIRE	2bf26702c6ecbd4 6f68138cdcd45c034	1b9a4c0a5615a4f96a04 1d771646c1a407b17577	38d1d8c3c4ec5ea17c3719af285247cb1d8 879c7cf967e1be1197e60d42c01c5
Gh0st RAT	2d330c354c14b39 368876392d56fb18c	a1f72c890d0b920f4f4c b2d59df6fa40734de90d	f86d05c1d7853c06fc5561f8df19b53506b 724a83bb29c69b39f004a0f7f82d8
GOLDDRAGON	15ec5c7125e6c74f 740d6fc3376c130d	fb09b89803da071b7b7e b23244771c54d979a873	4a1c43258fe0e3b75afc4e020b904910c9 4d9ba08fc1e3f3a99d188b56675211
GOLDDRAGON.POWERSHELL	2a5562de1d3e734 d9328a1c78b43c2e5	4b0d0ebb0c676efe855 bed796221dd475a39ba40	203ea478fa4d2d5ef513cad8b51617e0c9f 7571bf3a3becf9c267a0d590c6d72
GOLDDROP	0cc0aa5877cec91 09b7a5a0e3a250c72	1d49d462a11a00d8ac96 08e49f055961bf79980d	1324acd1f720055e7941b39949116dfe72ce 2e7792e70128f69e228eb48b0821
	2c530adb84111436 6ce6177ce964a5e6	5b69e3e5f4f49cf8b635 a57a8c92e17a4f130d50	873b8fb97b4b0c6d7992f6af1565329578 8526def41f337c651dc64e8e4aeebd
GOLDSMELT	c066b81c4b8b070 3f81f8bc6fb432992	2508f5ff0c28356c0c3f 8e6cae7b750d53495bca	63b4bd01f80d43576c279adf69a5582129 e81cc4adbd036759095816437 65ea8
GRAYZONE	1d30dfa5d8f21d14 65409b207115ded6	942fd7b4ef1ccf7032a4 0acad975c7b5905c3c77	ed0161f2a3337af5e27a84bea85fb4abe35 654f5de22bcb8a503d537952b1e8a

マルウェア・ファミリー	MD5のサンプル	SHA1	SHA256
HANGMAN.V2	21cffaa7f9bf224ce 75e264bfb16dd0d	862abce03f7f5de0c466 fdbd24ad796578eaa110	a605570555620cea6d6be211520525fc95 a30961661780da4cc4bafe9864f394
Invoke-Mimikatz	20bc53deb7b12145 80e9d9efeaa5e9d7	e74b816f1c6d6347cb40 121e0b50dadd0d8f1f97	908777e581616156576636568 61c212ac2569 6741ef69411021474158fa2b4cf
JURASSICSHELL	9cdda333432f403 b408b9fe717163861	d80be054a569df5f20 1191dcc4fea0dde9622da5	d2f4bf0caed5a442198fcdc43c83c7b27ae 04f341a72b270c9ed40778aa77afe
	ddae18c65d583b4 1a2157d496a4bde61	63e113f0a906af82903 dbfac3e78bdd2d146e738	a4ba1e6ab678a1bdf8bc05bea8310d74392 8a4e2c05bad104e61afdd9cccf9a1
LANDMARK	1ffccf6cb3b74d68 df2b899fd33127a5	a61f009e73ae81a18751e 9aee39f8121a3902280	da22d327124a0ee6a93cd07e85f9804fbc 98eda87824ddcf7c8a63d349e87034
LANDMARK.NET	60efecf4e1b5b2c5 80329e9afa05db15	12c508ace6e8aa42be0 2750d759e720b800bf796	034d29fb89a8f68ba714f1868b2181c4cd5 9d4a2604630ef1554a6ccf3fe6d75
LATEOP LATEOP.V2	0f77143ce98d0b9 f69c802789e3b1713	7da4e8b743478370fa41 fe39a45e3ff2ca2194b3	54a8b8c933633c089f03d07cfbd5cafbf7 6a6d7095f2706d6604e739bb9c950f
LOGCABIN	0b558ee89a7bb32 968ef78104f6b9a28	b7fdb5e5b31adfc5ada0 de1e05b0c069968e5bce	79c0fe1467dada33e0b097dd772c362296 18b7091baa5f10da083f894192a237
LONEJOGGER	139d2561f5c72fab b099a12c16b8960c	2dd269608dd7f4da171d 1a220fe97347162008c7	2c338055e8245057169f1733846e0490bc 4ae117d1dadefe0a3f07a63dc87520
	14a00f517012279a f53118a491253e5c	98040f42103ce3b840d d54bf3490587f141a0bc3	26a98b752fd8e700776f11bad4169a06708 24d5b5b9337f3c8f46fac33bc03e8
METASPLOIT	37e7d679cd4aa78 8ec63f27cb02962ea	7d66c1f36b4b48d99046 1ec44d626793ade6a8d1	b55e9d65a3130f543360a9c488d35475d4 789ee7a32a4e94d02f33c21a172bcb
PASSMARK	b077ba5af1dfbd4a c523923eab56bcd4	4e93797dd3b383050cf 0ee585aa5b5525efb2380	4a08b78d410bc3d9b78dd63b146767f293 dc3f3f6f8092352d2aa2f589e9c772
PENCILDOWN	04d0856afb1aa916 8377d6aa579c5403	f3b774e921eaad9335b9 c057dd49b918c5dae4a6	e637c86ae20a7f36a0ad43618b00c48f47 b5591a03af3fb689a16c45afa43733
PENCILDOWN.ANDROID	4626ed60dfc8dea f75477bc06bd39be7	a9ff1ebb548f5bba600d 38e709ff331749fa9971	2365a48f7d6cf6dcc83195f06ea11b93c95 5c3a491c60b50ba42788917ba22e2
PENDOWN	768c84100d6e318 1a26fa50261129287	6f4b6938ac8fd9591fc3 99219dbaf4347d8b444b	780e7edbfad5f68051c2039036b00b304d 3f828fdbee85d2d09edbcc6d07ea34
PUMPKINBAR	946f787c129bf469 298aa881fb0843f4	d3b233d6d8b11235929e 4a0cbdb12eefdd47d927	32beeda8cffc2ecc689ea2529194cf80695 5879a334ec68176864d1e6c09800c
	c9d70bf37017260 9da848fa785989939	851ba2182b37bc738042 0a986840e16f73947413	ba3c79dbeca0234fa838ae4c95640911555 6f437372aeeb0737206d71caf4a38
QUASARRAT	0085bc8ce16ef176 43909c4799ead02b	25d94c9ab7635ff330da be96780f330f7f2ba775	a9c404e100bfd2716a8f6bfafc07b0bd617 5bedb047d10b94390c79249258272
SLIMCURL	68ce092f1a3d1985 2ea32db8388de5c7	700acc4e48eae84f80f 4dbaf74bf60b79efd49bd	25c2f4703cbaa1ff4dbcfcc16a10b29ef35c cc174b71b21de360d898540889f8
SOURDOUGH	7e609404cc258bb e283bea6ddd7af293	6618e25dd49b68f7b2 b266eb2d787e6f05c964bc	502136707a70b768800640224e48c6340 57dc651892113b62522f0dd2fcf1e87

マルウェア・ファミリー	MD5のサンプル	SHA1	SHA256
SPICYTUNA	0821884168a644f3c27176a52763acc9	1f6c7c9219f6b6ea30cd481968ae1a038789be67	e7fae41c0bd8d3d95253bd75dce99015599ecc404bd8d737cec305fc3e4dd018
	8ca84c206fe8436dcc92bf6c1f7cf168	636f2c20183b45691b742949d49b3d6c218c9cce	7943bf9cc7b2adf50f7f92dd37347381e6d0aef23b34a3cd0a3afcda1d72e16d
SWEETDROP	N/A	N/A	N/A
TROIBOMB	18df13900f118158c33	11f646095495d625e7d	98d4471fe549bb3067a
	df904c662e875	71038578cc838a6d5e111	c2f2d9afd50ed1baaddab41ec4270834989e7f1ade14d
VENOMBITE	107f917a5ddb4d3947233fbc9d47ddc8	75c516dde8415494c288e349d440ce778dede8e3	2d41b04f5d86047dc2353a10595418b0d5239c22112f36eb9d253b2e8b6eb0d0

詳しくは**www.mandiant.jp**をご覧ください。

マンディアント
〒100-0006 東京都千代田区有楽町1丁目1番2号
東京ミッドタウン日比谷 日比谷三井タワー12F
03-4577-4401

japan@mandiant.com

Mandiantについて
Mandiantは、広範なサイバー防御、脅威インテリジェンス、インシデントレスポンス・サービスのリーダーとして知られています。長年にわたり攻撃の最前線で得た豊富な経験を活かし、サイバー脅威に対する防御と対応においてお客様組織を支援します。Mandiantは現在、Google Cloudの一部です。

MANDIANT
Mandiantは現在、Google Cloudの一部です。