APTアクターの分類“中毒” —Lazarus のサブグループ分類に見るアトリビューションの実務的課題— - JPCERT/CC Eyes

佐々木 勇人（Hayato Sasaki）

2025/01/20

APTアクターの分類“中毒” —Lazarus のサブグループ分類に見るアトリビューションの実務的課題—

Lazarus

-
- メール

はじめに

「Lazarus」[1]は一つの攻撃グループを指す名称ではなく、実際には多数のサブグループの集合を指しています。もともとは一つのグループ、あるいは（今から見れば）ごく限られた規模の集団による活動を示すものだったところ、その後、活動体の規模が拡大し、複数のユニットに規模が拡大／枝分かれしたのではないかと筆者は推測していますが、この規模拡大に対して、旧来の「Lazarus」という呼称が当てはまらなくなってきたと考えるのが現実的です。

「この攻撃は○○（※Lazarusのサブグループ名）ではなくて、××のものだ」といった、Lazarusのサブグループレベルの粒度での特定／アトリビューションの話題を出すと、多くの方が怪訝な顔になるか無表情になりますが、後述のとおり、一見個人の“こだわり”、ややもすると“趣味”に見える考察が国全体の攻撃対処に極めて重要である点を解説したいと思います。

Lazarus系統のサブグループ群の特徴

Lazarus系統の攻撃活動／グループを示す単語は膨大にあり、時間の経過とともに増えていきます。また、Lazarusに限った話ではないですが、同じ（サブ）グループでもセキュリティベンダー間で呼称が異なっていたり、同様に、同一のマルウェアでもそれぞれ違う呼称を使うケースが散見されたりするため、極めて全体像を把握しにくいものとなっています。また、分析レポート公表時の書きぶりとして「攻撃グループ名（またはサブグループ名）」

を中心に据えるのか、「攻撃キャンペーン名」とするのか発表者毎にバラバラであるため、この混乱により一層の拍車をかけています。あるレポートではタイトルなどで「攻撃キャンペーン名」として登場したにもかかわず、時間の経過とともに、その名称が「攻撃グループ名」として他のレポート等で引用されるようになってしまうなどの混乱が散見されます。
※下記は筆者が整理したものですので、「これはキャンペーン名じゃない」等のご指摘／情報提供あれば是非よろしくお願いします。

攻撃活動全体を示す用語： Hidden Cobra、TraderTraitor
個別（または断続的な）攻撃キャンペーン[2]を示す用語： Operation Dreamjob、Operation In(ter)ception、AppleJeus、Dangerous Password、CryptoCore、SnatchCrypto、Contagious Interview、Operation Jtrack ※Dangerous Password、CryptoCoreについては、当初は攻撃グループ名として登場しましたが、その後攻撃キャンペーン名としても使われるケースが散見されます
攻撃グループ（サブグループ）を示す用語： TEMP.Hermit、Selective Pisces、Diamond Sleet、Zinc、UNC577、Black Artemis、Labyrinth Chollima、NICKEL ACADEMY APT38、Bluenoroff、Stardust chollima、CryptoMimic、Leery Turtle、Sapphire Sleet、TA444、BlackAlicanto Jade Sleet、UNC4899、Slaw Pisces Gleaming Pisces、Citrine Sleet Andariel、Stonefly、Onyx Sleet、Jumpy Pisces、Silent Chiollima Moonstone Sleet ※Lazarusのサブグループでない可能性もあります
かつては一つの攻撃グループを指し、現在はその後継／関連グループや派生したサブグループ群等を指す用語： Lazarus、Bluenoroff、APT38、Andariel

筆者はこれまでもさまざまな場にて、脅威側への対抗オペレーションのために攻撃グループのプロファイリング／アトリビューションの精度が重要である点を主張[3]してきました。この主張に対しては、「大きな区分で十分で、細々したサブグループの粒度まではそこまで必要ないのでは？」という指摘が想定されます。確かに、Lazarusのサブグループのいくつかは攻撃対象／目的やTTPが重複しているため、例えば暗号資産を狙うCitrine Sleet/UNC4736であろうが、Sapphire Sleet/CryptoMimicであろうが、Moostone Sleetであろうが、対処方針は大きく変わらないと考えることもできます。

なぜサブグループ単位でアクターを特定しなければならないかについては後述しますが、筆者が特にLazarusのサブグループ群への対処において、明確なサブグループ特定が必要と主張する背景として、アクターのグルーピングを困難にさせる、Lazarusのサブグループ群固有の以下の2点の特徴／傾向を挙げることができます。

特徴：複数のサブグループ間でTTPの重複がある

これまでも多くのセキュリティベンダー／アナリストが考察しているとおり[4]、複数のサブグループ間で初期侵害手法や攻撃インフラ、マルウェアに重複が見られます。
先日、JPCERT/CC Eyesで解説[5]のとおり、Linkedinを初期侵害に用いる攻撃キャンペーンがこれまでに複数確認されているほか、後述のとおり、同じ攻撃手法を採用する活動が増える傾向もあります。

特徴：従来のサブグループ編成に捕らわれないタスクフォース的グループ等が出現している

2021年から2023年2月にかけて、「Bureau325」と呼称される新たなAPTアクターに関するレポートや報道[6]が登場しました。Bureau325のTTPは既知のLazarus系統の複数のサブグループと共通しているだけでなく、Kimsukyが用いていたマルウェアも使用していることが判明しており、既存のグループ編成に捕らわれない、タスクフォース的なグループ／活動ではないかと想定[7]されています。
また、2023年3月にMandiantが「APT43」に関するレポートを公表[8]しましたが、このアクターの攻撃活動は従前、Kimsuky／Thalliumの活動として報告されることが多かったところ、Mandiantの分析チームは新たにグルーピングし直し、「APT43」と区分しています。
APT43についても（サブ）グループを超えたツール等の共通点が見つかっており、Bureau325と同様の傾向である旨、レポートで指摘されています。

なぜサブグループ単位で特定しなければならないのか

APTアクターの特定というと、実行犯の特定やその背後関係、特定国家への責任帰属といった、いわゆる「アトリビューション」問題が注目されがちです。Lazarusのサブグループ特定にそこまで人々の関心がない理由も、「アトリビューション」問題という背景があるからと筆者は考えます[9]。
いわゆる「アトリビューション」だけでなく、バーチャルな区分でしかない「サブグループ」の特定になぜそこまでの精度が必要なのか、以下の理由から考察します。

理由１：注意喚起等による中長期的な被害予防効果をより確実にするため

例えば、先日のJPCERT/CC Eyesで紹介したようなSNS経由の攻撃については、従前、暗号資産関連会社や防衛・航空産業がメインターゲットであったため、こうした業界に重点的に注意喚起等を行うことが可能でした。SNS経由でエンジニア個人を狙うものですが、基本的に標的組織の従業員を狙うため、当該標的分野の各組織に注意喚起やインディケータ情報等の共有を行うことで対処可能でした。
他方で、2023年後半以降に捕捉されるようになったサブグループ（や関連グループ）や攻撃キャンペーンでは、その多くで暗号資産関連の分野を狙う傾向が共通するものの、企業の機微情報をも狙うものやランサムウェア攻撃も併用するもの（Moonstone Sleet）、IT労働者による不正な外貨収入等を狙うもの（WageMole攻撃キャンペーン）など、目的／標的分野／対象者・組織が複合的になりつつあります。

サブグループ毎の標的分野や目的をより高い精度で捕捉できるようになれば、注意喚起のような情報伝達力の弱い方法ではなく、個別分野／組織へのピンポイントの情報提供が可能になります。特定分野や特定製品の脆弱性を悪用する攻撃に関する注意喚起を行った場合、同じアクターが多分野を狙っていたり、あるいは違う製品の脆弱性を初期侵入に悪用したりしていると、「自分たちがターゲットではない／自組織が使う製品はターゲットになっていない」と解釈され、こうした対象層の組織に注意喚起効果が発生しない場合があります。

理由２：対抗措置／対抗オペレーションのため

今後、国全体としてAPTアクターによる攻撃活動に対処していくにあたり、長期的にアクター個別の活動を捕捉し、これらLazarusのサブグループ群の背後にある政府機関等がどのような活動意図を持っているのか[10]、正確な脅威分析を行うにあたっても、サブグループの正確な捕捉が重要です。
サブグループの背後にいるのは、編制、規則、指揮命令形態を伴う「組織」であり、さまざまな対抗手段の「効果」はそれぞれ異なるはずです。
また、対抗オペレーションの効果だけでなく、取り得る対抗措置の手段によっては、国際法との関係で問題になる可能性[11]もあり、相手方の行為と実行者、背景主体との関係を正確に捕捉することは極めて重要です。

理由３：攻撃者側への「メッセージ」

多くの脅威アナリストがサブグループの特定に注力するようになってきているのは、前述の理由１のように対抗戦術的な理由もありますが、「サブグループ」というものがバーチャルな区分でなく、実際の実行者たちの活動や組織的背景、リソースを反映しているからと考えてもいるからです。
パブリックアトリビューションや分析レポートの公表といった「情報開示」によって脅威側の活動そのものに影響を与えられるケースは限定的[12]ですが、少なくとも、攻撃者が導入した新たな戦術の成功率を下げたり、“陳腐化”させることによって影響を与えたりすることは可能です。APTアクターがどこまで「我々」側の情報開示を気にしているのか、ほとんど検証されておらず未知の世界ですが、少なくとも、パブリックアトリビューションといった脅威側にけん制等の影響を与える目的の情報開示を行うのであれば、影響を与えたい対象者（実行者、実行組織）に情報を伝えるための正確なサブグループ特定・明示は最低条件となるでしょう。

そして、何よりも、正確なサブグループ特定の開示というのは、防御側／対処側の能力を示すことになるという点を忘れてはなりません。

ケーススタディ：SNSによるコンタクトや悪意あるnpmパッケージのDLを行う戦術が重複するサブグループ

先日のJPCERT/CC Eyesで解説のとおり、LinkedinなどのSNSを使ってエンジニア個人にコンタクトし、PyPIやGithub経由で悪意あるPythonパッケージやnpmパッケージ等をダウンロードさせる初期侵害手法は複数のサブグループで共通して用いられるようになりました。
以下は同様／類似の手口を使う複数のサブグループの活動を時系列で整理したものです。

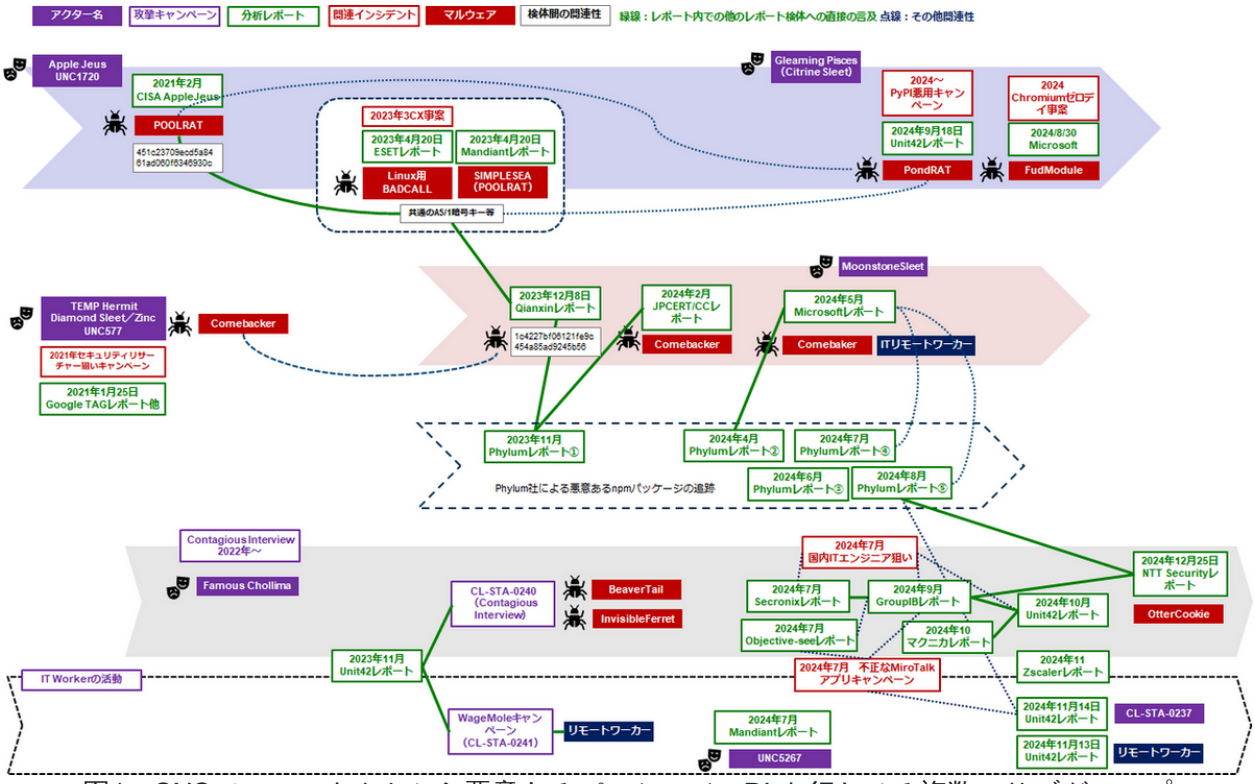


図1：SNSでのコンタクトから悪意あるパッケージのDLを行わせる複数のサブグループ

Moonstone Sleet

標的分野／目的：暗号資産窃取、ランサムウェア攻撃、防衛産業等の機微情報、IT労働者による不正な収入

2024年2月にJPCERT/CC EyesにてPyPI経由で不正なPythonパッケージをダウンロードさせる事象について公表[13]しました。この攻撃活動では最終的にComebackerを用いると分析しましたが、同様の検体については2023年12月にQianxinがレポート[14]しており、また、その後2024年5月にはMicrosoftがMoonstone Sleetというサブグループ名で追跡している旨を公表[15]しています。
TTPが類似している、（後述の）Contagious Interviewを行うサブグループとは、Microsoftは「直接的な重複はない」との見解[16]を示しています。
ComeBackerはTEMP.Hermit（※Mandiant呼称。過去にはUNC577とも区分）／Diamond Sleet（Microsoft呼称。過去にはZincと呼称）による2021年のセキュリティ研究者を狙った攻撃キャンペーン[17]で見つかっていますが、攻撃グループ間の関連性についてはまた情報が乏しい状況です。

Gleaming Pisces（Citrine Sleet）

過去に分類されていたグループとの関係：Apple Jeusのアクター（UNC1720）
標的分野：暗号資産関連事業者、個人

Moonstone Sleetと同じく、PyPIを使った初期侵害を行っているサブグループとして、Gleaming Pisces（Unit42呼称）／Citrine Sleet（Microsoft呼称）があります。2024年のPyPI悪用の攻撃キャンペーン[18]で使われていたPondRAT（Unit42呼称）は2021年2月に米CISAがAppleJeus攻撃キャンペーンについて注意喚起をした際に公表[19]したPoolRAT（Unit42呼称）に起源を持ち、PoolRATは2023年3月に3cxが侵害されたサプライチェーン攻撃でも見つかっています。[20]
これらのRATは共通のA5/1暗号化キーが用いられており、同じキーは先述のQianxinがレポートしたComebacker類似の検体でも見つかっています。Comebackerについては上記の通りですが、ほかにも、TEMP.Hermit／Diamond Sleetが用いていたとされるFudModuleもCitrine Sleetの攻撃で確認されており、こうした重複について、Microsoftは「Diamond SleetとCitrine Sleetとの間にはインフラ、マルウェアの重複がある」と指摘[21]しています。

Contagious Intervew（攻撃キャンペーン名）

標的分野：暗号資産窃取、IT労働者による不正な収入（※Wagemoleは別キャンペーンであるが関連性が指摘されている）

2024年10月にマクニカ[22]が、また、2024年12月にNTTセキュリティ[23]がそれぞれレポートした、ITエンジニアに求人関係のインタビュー依頼を装ってコンタクトする攻撃活動です。この攻撃活動は2023年11月にUnit42がはじめてレポート[24]したもので、Unit42によれば2022年から活動しているとされています。。
この攻撃キャンペーンについては、CrowdStrikeが区分するところの、FAMAOUS CHOLLIMAが実行したとされていますが、FAMOUS CHOLLIMAがLazarusのサブグループ群の一つなのか、あるいは異なる系統のグループなのか、現時点では判然としていません。
また、この活動は、「ITワーカー」[25]と呼ばれる、北朝鮮国籍のIT技術者のなりすましによる、海外IT企業での不正労働（外貨獲得）活動にも関係しているとされる「Wagemole」や「CL-STA-0237」（※Unit42呼称）の活動とも関係性が見つかっています[26]
なお、前述のとおり、MicrosoftはMoonstone Sleetの活動とContagious Interviewについては別の活動と現時点では区分していますが、両活動で使われた不正なnpmパッケージについては、共通してPhylum社が継続的に追跡し、多くのレポートを公開[27]しています。

参考：現時点での各サブグループ間の関係性の整理

本稿では、主にSNS経由でのコンタクトの後、不正なnpmパッケージ等をダウンロードさせる初期侵害手法が共通する、MoonstoneSleetの活動、Contagious Interview攻撃キャンペーン、Gleaming Pisces（Citrine Sleet）の活動について解説・比較しましたが、これ以外の

Lazarus関連のサブグループの活動や時間経過に伴う区分／セキュリティベンダー毎の呼称名の変遷について以下のように整理しています。

今後も新たなサブグループの登場や、セキュリティアナリストによる再区分[28]が発生すると思われ、情報が次々と変わっていくことが想定されます。こうした情報を機動的に捕捉・整理できる仕組みづくりについても今後挑戦していきたいと思います。

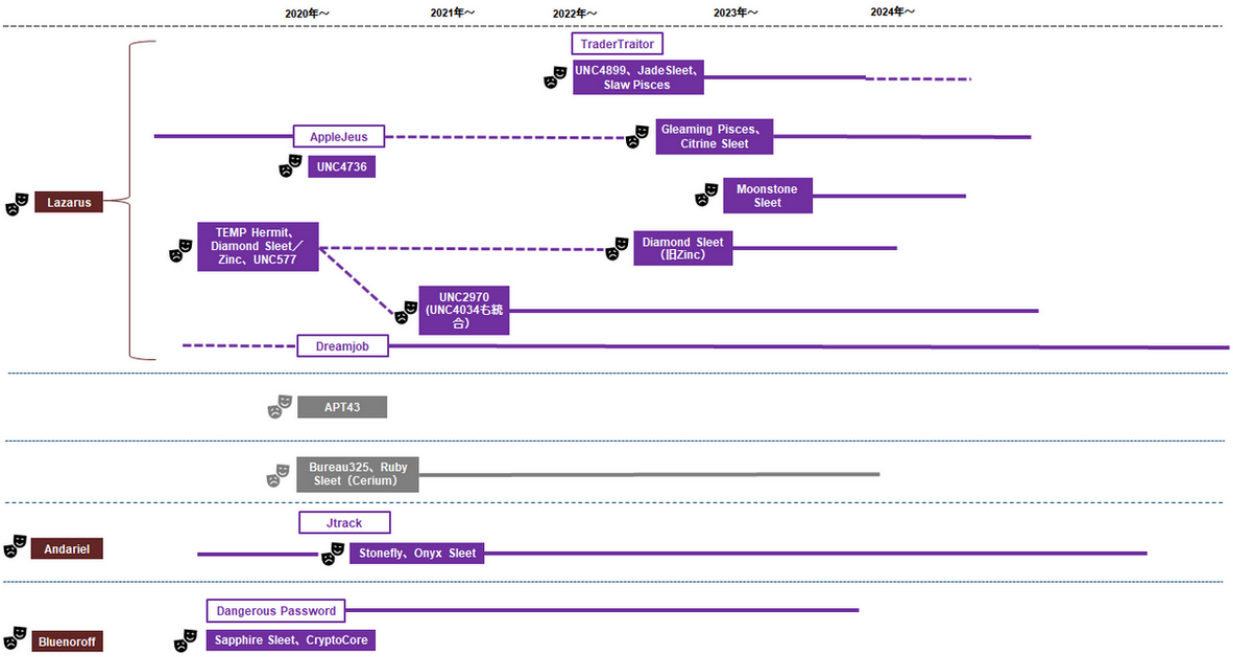


図2：Lazarusの各サブグループの変遷

さいごに

「アトリビューション」には、国際法や刑事手続き上厳密な意味での「アトリビューション」とセキュリティ業界が慣行的に用いてきた「アトリビューション」の2つの「アトリビューション」概念が存在します。筆者は前者を「“ハード”なアトリビューション」と呼称しており、実際に関与した人物・組織の特定や責任帰属までを射程とするもの、後者を「“ソフトな”アトリビューション」と呼称し、「アクター／攻撃グループ」といったバーチャルなグルーピング、プロファイリングまでを射程とするものと（勝手に）区分しています。“ハード”なアトリビューションとしては不十分な証拠粒度のものであったとしても、的確な注意喚起／対策情報の展開に資する“ソフトな”アトリビューションがあり、その反対に、技術的にタイムリーな対応には間に合わなくても長期的な対抗措置等に必要な“ハード”なアトリビューションもあります。

アトリビューションを巡るさまざまな技術的／非技術的問題をここで取り上げるには紙幅が足りませんが、今後、「情報の開示」が重要な論点になると筆者は考えています。
アトリビューション結果を開示することは、民間側にとっては、アナリストの成果であり、また、営利企業としての専門企業のPRになる重要なものです。製品・サービスの能力という可視化しづらいものに比べて、「これだけのことを解き明かした」と理解しやすい（ソフトな）アトリビューションレポートはセキュリティ市場の健全性維持のためにも重要です。

他方で、行政側にとってもアトリビューションは“成果”です。パブリックアトリビューションの効果の有無を巡る議論[29]はさておき、行政がなぜ被害情報を集めるのか「可視化」される貴重な機会であり、また、先述のとおり、国としての能力を相手方に見せる機会でもあります。
いずれの立場であれ、成果を出すことが優先されてしまい、技術的に不確かなアトリビューション結果が開示されることは本稿でここまで述べたとおり、多くのデメリットをもたらします。また、情報開示の効果も検証されなければなりません。

そして、何よりも、アトリビューション結果等を含む、いわゆる「脅威インテリジェンス」情報というものは、情報の発信者自身だけで生み出したものではなく、被害組織や現場対応に当たるアナリスト等が関与する役割が極めて大きいという点を忘れてはなりません。情報開示は脅威側へ影響を与える行為であり、また同時に、注意喚起対象者だけでなく、事案に関わった被害組織、アナリスト、製品ベンダなど、多くの関係者にも影響を与える極めて複雑な行為です。アトリビューション手法自体もまだ発展途上である中、その情報開示はさらに多くの未解決の問題をはらんでいます。これまでも度々「情報開示」を巡る諸問題[30]を取り上げてきましたが、注意喚起や分析レポートと同じく、こうした問題提起に関する情報発信も「出して終わり」ということでなく、継続的にこのテーマに向かい合っていきたいと考えています。

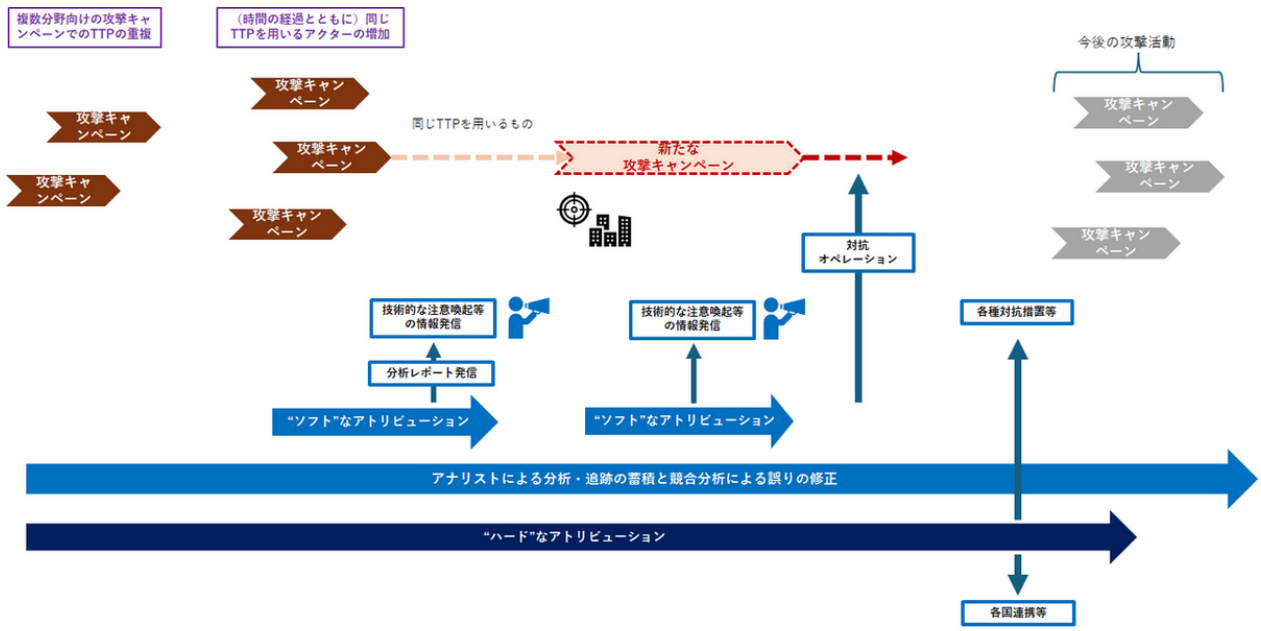


図3：各アトリビューションのタイミング

参考資料等

※件数が多いため、各参考資料等の作成者名・文献名の記載を省略していますので、ご了承ください。

[1]この呼称が初めて登場したのは、2016年にNovetta社主導で多数のセキュリティベンダが参加した共同分析レポート「Operation Blockbuster」でした。当初は「Lazarus Group」と記述されていました。

[2]攻撃キャンペーン：一定期間内において特定の組織／分野に対して特定の攻撃手法／攻撃インフラを用いて行われる攻撃活動（参照：2024年3月「攻撃技術情報の取扱い・活用手引き」（サイバー攻撃による被害に関する情報共有の促進に向けた検討会事務局（経済産業省、JPCERT/CC））

[3]JSAC2023 https://jsac.jpcert.or.jp/archive/2023/pdf/JSAC2023_2_2_sasaki_jp.pdf、JSAC2024 https://jsac.jpcert.or.jp/archive/2024/pdf/JSAC2024_2_6_hayato_sasaki_jp.pdf、防衛研究所NIDSコメンタリー https://www.nids.mod.go.jp/publication/commentary/pdf/commentary346.pdf

[4]少し古いですが、マルウェアクラスターのクラスタリングからサブグループの整理と重複について分析したものとして、https://securelist.com/lazarus-threatneedle/100803/、https://vblocalhost.com/uploads/VB2021-Park.pdf

[5]https://blogs.jpcert.or.jp/ja/2025/01/initial_attack_vector.html

[6]https://cloud.google.com/blog/topics/threat-intelligence/mapping-dprk-groups-to-government/?hl=en、“Final report of the Panel of Experts submitted pursuant to resolution 2627 (2022)”, https://www.un.org/securitycouncil/sanctions/1718/panel_experts/reports 他

[7]CISTECジャーナル2023年5月号　JPCERT/CC 佐々木勇人「2022年度国連北朝鮮制裁委報告書から北朝鮮関連のサイバー攻撃動向を読み解く―新たな攻撃グループ登場の背景とその動向について―」

[8]https://cloud.google.com/blog/topics/threat-intelligence/apt43-north-korea-cybercrime-espionage?hl=en

[9]ある国際機関の方と意見交換した際に、筆者がLazarusのサブグループの解説をしたところ、「どのサブグループであろうと、それらの違法行為の（某国政府への）責任帰属ができているから、それで十分ではないか」と指摘されたことがあります。

[10]2023年まで、国連の北朝鮮制裁委員会の専門家パネルの場で、こうした追跡・報告がなされていました。本稿で取り上げるような、さまざまなセキュリティベンダーのレポートとして散らばった情報を集め、グループ別、また、各グループの背後にいると思われる政府機関との整理を踏まえた脅威分析が行われていましたが、報道のとおり、専門家パネルの活動は2023年度で終了してしまっています。

[11]参考文献：中谷和弘、河野桂子、黒崎将広『サイバー攻撃の国際法　タリン・マニュアル2.0の解説（増補版）』、中村和彦『越境サイバー侵害行動と国際法―国家実行から読み解く規律の行方―』ほか

[12]米国におけるパブリックアトリビューションを中心とした懲罰的抑止アプローチの限界とコスト賦課アプローチへの転換経緯等の解説は、防衛研究所NIDSコメンタリー　佐々木勇人、瀬戸崇志『サイバー攻撃対処における攻撃「キャンペーン」概念と「コスト賦課アプ

ローチ」――近年の米国政府当局によるサイバー攻撃活動への対処事例の考察から』参照 https://www.nids.mod.go.jp/publication/commentary/pdf/commentary346.pdf

[13]https://blogs.jpcert.or.jp/ja/2024/02/lazarus_pypi.html

[14]https://ti.qianxin.com/blog/articles/Analysis-of-Suspected-Lazarus-APT-Q-1-Attack-Sample-Targeting-npm-Package-Supply-Chain-EN/

[15]https://www.microsoft.com/en-us/security/blog/2024/05/28/moonstone-sleet-emerges-as-new-north-korean-threat-actor-with-new-bag-of-tricks/

[16]https://thehackernews.com/2024/05/microsoft-uncovers-moonstone-sleet-new.html

[17]https://blog.google/threat-analysis-group/new-campaign-targeting-security-researchers/

[18]https://unit42.paloaltonetworks.com/gleaming-pisces-applejeus-poolrat-and-pondrat/

[19]https://www.cisa.gov/news-events/cybersecurity-advisories/aa21-048a

[20]https://www.welivesecurity.com/2023/04/20/linux-malware-strengthens-links-lazarus-3cx-supply-chain-attack/

[21]https://www.microsoft.com/en-us/security/blog/2024/08/30/north-korean-threat-actor-citrine-sleet-exploiting-chromium-zero-day/

[22]https://security.macnica.co.jp/blog/2024/10/-contagious-interview.html

[23]https://jp.security.ntt/tech_blog/contagious-interview-ottercookie

[24]https://unit42.paloaltonetworks.jp/two-campaigns-by-north-korea-bad-actors-target-job-hunters/

[25]https://ofac.treasury.gov/recent-actions/20220516

[26]https://unit42.paloaltonetworks.com/fake-north-korean-it-worker-activity-cluster/

[27]https://blog.phylum.io/crypto-themed-npm-packages-found-delivering-stealthy-malware/

[28]2023年3月にMandiantが新たに「APT43」と区分し直したことをレポートしましたが、このアクターの活動は従前、KimsukyやThalliumによるものとして報告・区分されることが多かったのですが、長年の追跡により分析し直し、新たに「APT43」と再区分して発表がなされました。 https://cloud.google.com/blog/ja/topics/threat-intelligence/apt43-north-korea-cybercrime-espionage

[29]いわゆる懲罰的抑止を想定したパブリックアトリビューションや経済制裁措置等による「抑止アプローチ」の成果がほとんどなかったとする論調をベースとした先行研究としては、Michael P. Fischerkeller, Emily O. Goldman, Richard J. Harknett, “Cyber Persistence

Theory: Redefining National Security in Cyberspace”、Robert Chesney and Max Smeets Eds, “Deter, Disrupt, or Deceive Assessing Cyber Conflict as an Intelligence Contest”等

[30]https://blogs.jpcert.or.jp/ja/2022/04/sharing_and_disclosure.html、
https://blogs.jpcert.or.jp/ja/2023/05/cost-and-effectiveness-of-alerts.html、
https://blogs.jpcert.or.jp/ja/2023/08/incident-disclosure-and-coordination.html、
https://blogs.jpcert.or.jp/ja/2023/12/leaks-and-breaking-trust.html

-
- メール

この記事の筆者

佐々木 勇人（Hayato Sasaki）

JPCERT/CC早期警戒グループマネージャー。脅威アナリスト。政策担当部長。注意喚起等の情報発信のほか、インシデント対応や情報共有活動、官民連携活動に従事。サイバーセキュリティ法制学会理事。2024年5月から防衛研究所政策研究部サイバー安全保障研究室 特任研究員。“能動的”に研究を進めています。

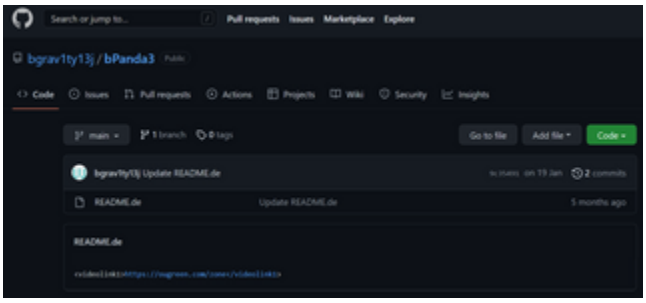
関連記事

- 

  あなたではなく組織の財産を狙うLinkedIn経由のコンタクトにご用心

- 

  PyPIを悪用した攻撃グループLazarusのマルウェア拡散活動

- 

  GitHubからC2サーバーの情報を取得するマルウェアVSingle

- YamaBot

  攻撃グループLazarusが使用するマルウェアYamaBot

- 

```
v7 = mal_check_count(http_strc->URL);
(*(void (__stdcall **)(int, int, int, int *))o_InternetCrackUrlA[0])(http_strc->URL, v7,
if ( v6 == 1 )
{
  wsprintfA(
    &v30,
    "Content-Type: multipart/form-data; boundary=%s\r\n",
    (const char *)http_strc->http_bonday_str);
  if ( !v20 || !v21 )
  {
    if ( v20 )
      wsprintfA(
        &v32,
        "--%s\r\nContent-Disposition: form-data; name=\"%s\"\r\n\r\n%s\r\n\r\n",
        (const char *)http_strc->http_bonday_str,
        (const char *)http_strc->http_name1,
        (const char *)http_strc->http_body_text);
    else
      wsprintfA(
        &v32,
        "--%s\r\n"
        "Content-Disposition: form-data; name=\"%s\"; filename=\"%s\"\r\n"
        "Content-Type: image/bmp\r\n"
        "\r\n",
        (const char *)http_strc->http_bonday_str,
        (const char *)http_strc->http_name,
        (const char *)http_strc->http_filename);
  }
  else
  {
    wsprintfA(
      &v32,
      "--%s\r\n"
      "Content-Disposition: form-data; name=\"%s\"\r\n"
      "\r\n"
      "%s\r\n"
      "--%s\r\n"
      "Content-Disposition: form-data; name=\"%s\"; filename=\"%s\"\r\n"
      "Content-Type: image/bmp\r\n"
      "\r\n",
      (const char *)http_strc->http_bonday_str,
      (const char *)http_strc->http_name1,
      (const char *)http_strc->http_body_text,
      (const char *)http_strc->http_bonday_str,
      (const char *)http_strc->http_name,
      (const char *)http_strc->http_filename);
  }
  wsprintfA(&v33, "\r\n--%s--\r\n", (const char *)http_strc->http_bonday_str);
  v27 = mal_check_count((int)&v32);
  v28 = mal_check_count((int)&v33);
```

日本の組織を狙った攻撃グループLazarusによる攻撃オペレーション

≪ 前へ
トップに戻る
次へ ≫