サイバーセキュリティレポート

2023.04

NTT セキュリティ・ジャパン株式会社
コンサルティングサービス部　OSINT モニタリングチーム

目次

【当レポートについて】

当レポートでは 2023 年 4 月中に生じた様々な情報セキュリティに関する事件、事象、またそれらを取り巻く環境の変化の中から特に重要と考えられるトピック 3 点を選び、まとめたものである。各トピックの要旨は以下のとおりである。

第 1 章『FBI、各国との共同捜査による Genesis Market の解体を発表』

- 4 月 5 日、米司法省は、ユーザーの PC をマルウェアに感染させ、感染した PC で使われている認証情報等へのアクセス権を第三者に販売していた「Genesis Market」を解体させたと発表した。
- ランサムウェアグループ等のサイバー犯罪者が、攻撃対象のネットワークへの侵入口を確保する等の為に、初期アクセス・ブローカーとして Genesis Market を利用していた。
- Genesis Market 閉鎖後も同様のマーケットが存在し続けているため、業務用の PC がマルウェアに感染して社内システムへの侵入口とならないよう、ウイルス対策ソフトの導入やアップデート等の基本的な対策を怠らず実施する必要がある。

第 2 章『リーク文書「Vulkan files」とその波紋』

- ロシアの IT コンサルタント会社である NTC Vulkan が、ロシア政府傘下の情報機関にサイバー攻撃や情報工作を支援するためのツールを提供していたことが、「Vulkan files」と命名されたリーク文書により明らかになった。
- 文書には、Vulkan がロシアの情報機関や APT グループのために、脆弱性を探すサイバー攻撃ツールや、SNS 等を介した情報工作を行うためのツール、またサイバー攻撃を実施する工作員を訓練するためのツールを開発したことが記されていた。
- ロシア政府の狙う、サイバー攻撃や情報工作を軍事行動と並行して行うハイブリッド戦争の準備の一端を、Vulkan files は明らかにした。

第 3 章『FBI がジュースジャッキング（Juice-Jacking）攻撃について警告』

- 4 月 6 日、米連邦捜査局（FBI）デンバー支局は Twitter で、空港やホテルに設置されている USB 充電ポートに細工する、ジュースジャッキング（Juice-Jacking）攻撃に対する注意喚起を呼びかけた。
- 攻撃者は、USB 充電ポートにチップを埋め込む等の細工を行う。充電のためにスマホやタブレット端末を接続すると、データを盗まれたり、マルウェアや監視ソフトウェアを勝手にインストールされたりする恐れがある。
- ジュースジャッキング攻撃を回避するためには、USB 充電ポートの利用を避ける。または、充電専用の USB ケーブルを携帯して使用することが推奨される。

1. FBI、各国との共同捜査による Genesis Market の解体を発表

1.1. 概要

4 月 5 日、米司法省は、サイバー攻撃によって窃取された認証情報を販売していた「Genesis Market」を解体させたと発表した[1]。この捜査は FBI とユーロポールらの共同で行われ、同マーケットのユーザーが 119 名逮捕された。現在、同マーケットにアクセスすると、捜査に協力した各国の法執行機関のロゴ等と共に「このサイトは押収された」と表示されている。

図 1 押収後に表示される Genesis Market の画面

1.2. Genesis Market と過去の事件

【Genesis Market とは】

Genesis Market は、ロシアの脅威アクターと思われる管理者によって 2018 年 3 月に開設された[2]。既存のユーザーから招待コードを入手しなければ同マーケットにアクセスできない仕組みであったため、ハッカーたちの間では招待コードは価値があるものとみなされ、ハッカーフォーラム等で売買されることもあった。

図 2 Genesis Market の招待コードの購入を持ちかける投稿（一部加工）

[1] 出典：U.S. Department of Justice『Criminal Marketplace Disrupted in International Cyber Operation』
https://www.justice.gov/opa/pr/criminal-marketplace-disrupted-international-cyber-operation

[2] 出典：KELA『サイバー犯罪マーケット「Genesis」のサプライチェーン』
https://ke-la.com/ja/exploring-the-genesis-supply-chain-for-fun-and-profit/

同マーケットは独自にマルウェアを開発しており、マルウェア添付メール等から感染させた PC を「**ボット**」と呼び、ボットが収集する情報へのアクセス権を販売していた。これを購入すると、対象の PC から収集された Cookie、ログイン情報、フォームへの自動入力データ、ブラウザの種類や OS といったブラウザーフィンガープリント[3]等の情報を**リアルタイムで入手できる**。

単純なログイン情報の販売と異なる点としては、**マルウェアの感染者が漏洩に気づきパスワードを変更しても変更後のパスワードを即座に入手できる点**[4,5]、また、**認証後の Cookie が入手できれば多要素認証も回避できる点**[6]が挙げられる。特に企業の従業員が利用する PC のボットは、攻撃対象とする企業ネットワーク内への侵入と内部展開への足掛かりとして有用であるため、ランサムウェアグループ等のサイバー犯罪者によって購入されていた。このような侵入口を提供するサービスは、近年の分業化されたサイバー犯罪のエコシステムの中で「初期アクセス・ブローカー（Initial Access Broker）」と位置づけられ、重要な役割を担っている。

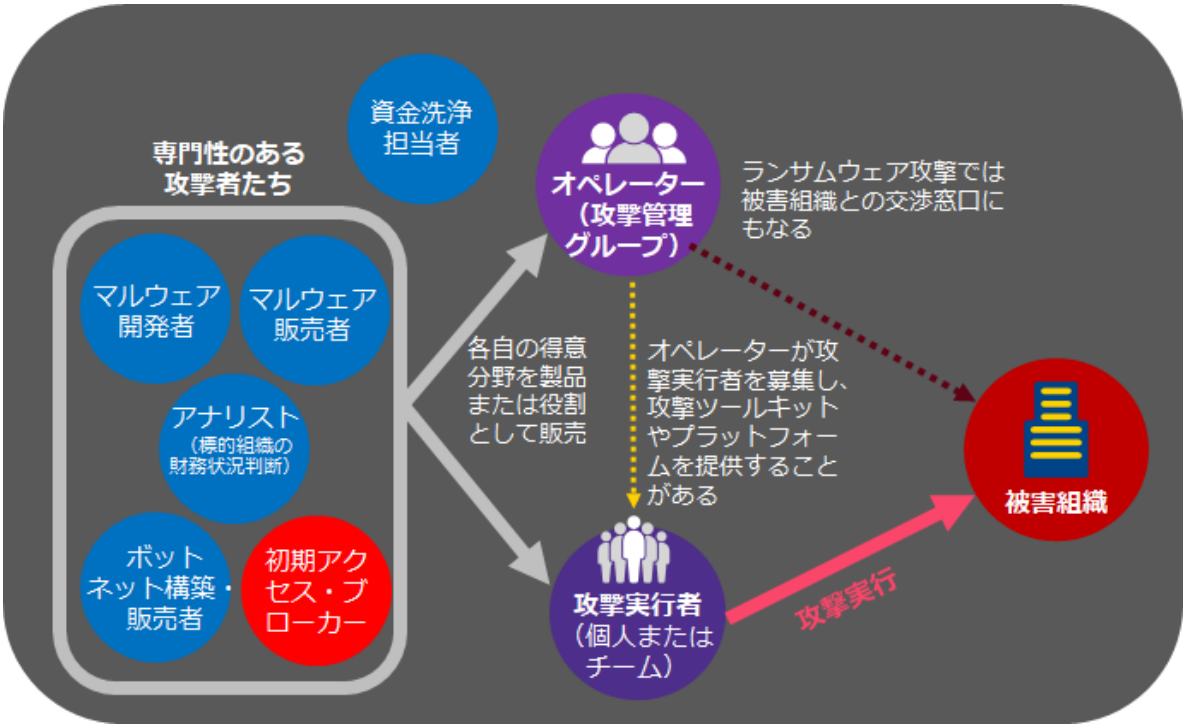

図 3 サイバー犯罪における分業体制の模式図

【事例：エレクトロニック・アーツへの攻撃での悪用】

Genesis Market で販売されたボットが攻撃に利用された事例として、2021 年 6 月に発生した、ゲーム会社のエレクトロ

[3] 出典：日経 XTREND『ユーザーを特定する「ブラウザーフィンガープリント」技術とは』
https://xtrend.nikkei.com/atcl/contents/technology/00005/00013/

[4] 出典：EUROPOL『Takedown of notorious hacker marketplace selling your identity to criminals』
https://www.europol.europa.eu/media-press/newsroom/news/takedown-of-notorious-hacker-marketplace-selling-your-identity-to-criminals

[5] 出典：SOPHOS『認証情報が売買される招待制マーケットプレイス「Genesis」』
https://news.sophos.com/ja-jp/2022/08/04/genesis-brings-polish-to-stolen-credential-marketplaces-jp/

[6] 出典：SOCRadar『5 Things You Should Know About the Genesis Marketplace』
https://socradar.io/5-things-you-should-know-about-genesis-marketplace/

ニック・アーツ（Electronic Arts）での事件が知られている[7]。

きっかけとなったのは、攻撃者が Genesis Market にてわずか 10 ドルで購入した、同社社員のボット化していた PC へのアクセス権だった[8]。攻撃者はボットから入手した Cookie を利用して同社の Slack グループへのログインに成功した。

さらに攻撃者は Slack を踏み台にして、同社の社内ネットワークへの侵入を目論む。Slack 上で同社社員になりすまして IT サポート担当者に連絡し、多要素認証のトークンを騙し取ることにより社内ネットワークへのログインに成功した。侵入した攻撃者は、保存されていた大量のゲームのソースコードと内部ツールを窃取し、マーケットで販売した。


Electronic Arts

ゲーム　さらに体験　情報　提言　リソース

2021年7月14日

6月に、最近発生したネットワークへの侵入事件に関して報告しました（下記の声明文を参照してください）。今週、ハッカーとされる人物たちから脅威を受け、一部のファイルが一般に公開されました。我々は公開されたファイルを分析しましたが、現時点ではプレイヤーの皆様のプライバシーを侵害する恐れのあるデータは含まれておらず、当社のゲームおよびビジネス、そしてプレイヤーに対して重大なリスクがあると信じる理由はありません。今後も現在進行中の犯罪捜査の一環として、連邦法執行機関との協力を続けます。

2020年6月11日

EAネットワークがハッキングされるというケースが発生したため、一部盗まれたゲームのソースコードや関連ツールに関して現在調査中です。プレイヤー側のデータへのアクセスはなかったため、皆様のプライバシーが脅かされたとは考えていません。我々は事件後に速やかにセキュリティの改善策を講じており、また本件によって当社のゲームまたはビジネスに影響が及ぶことはないと想定しています。現在、犯罪捜査の一環として、法執行当局やその他の専門家たちと積極的に協力しています。

図 4 事件に関してエレクトロニック・アーツ社が発表した声明文[9]

1.3.「オペレーション クッキーモンスター」

今回の捜査は、FBI とオランダ警察が主導し、ユーロポールやドイツ、イギリス、オーストラリアといった 45 の国・地域の法執行機関の協力で行われた。作戦名は「オペレーション クッキーモンスター」と付けられた[10,11,12]。

捜査の結果、Genesis Market のユーザー119 名が逮捕され、同マーケットが利用していた 11 のドメイン名が押収され

[7] 出典：Vice『Hackers Steal Wealth of Data from Game Giant EA』
https://www.vice.com/en/article/wx5xpx/hackers-steal-data-electronic-arts-ea-fifa-source-code

[8] 出典：Vice『How Hackers Used Slack to Break into EA Games』
https://www.vice.com/en/article/7kvkqb/how-ea-games-was-hacked-slack

[9] 出典：Electronic Arts『先日発生したネットワークへの不法侵入に関する声明文』
https://www.ea.com/ja-jp/news/ea-statement-on-june-11-security-incident

[10] 出典：Bleeping Computer『FBI seizes stolen credentials market Genesis in Operation Cookie Monster』
https://www.bleepingcomputer.com/news/security/fbi-seizes-stolen-credentials-market-genesis-in-operation-cookie-monster/

[11] 出典：REUTERS『'Operation Cookie Monster': International police action seizes dark web market』
https://www.reuters.com/world/uk/operation-cookie-monster-international-police-action-seizes-dark-web-market-2023-04-05/

[12] 出典：U.S. Department of Justice『Genesis Market Disrupted in International Cyber Operation』
https://www.justice.gov/usao-edwi/pr/genesis-market-disrupted-international-cyber-operation

た。現在、これらの押収されたドメイン名を用いた URL でアクセスすると、「このサイトは押収された」と表示され、サイトは利用できなくなっている（図 1）。

しかし、同マーケットの管理者は特定されておらず、未だ逮捕されていない。また、「.onion」の付く別のドメインを利用するダークウェブ上のサイトには現在でもアクセスでき、同マーケットのシステムは稼働している模様である[13]。これについては、捜査を継続している法執行機関がハッカーの情報を収集するおとりとして残しているという説もある。

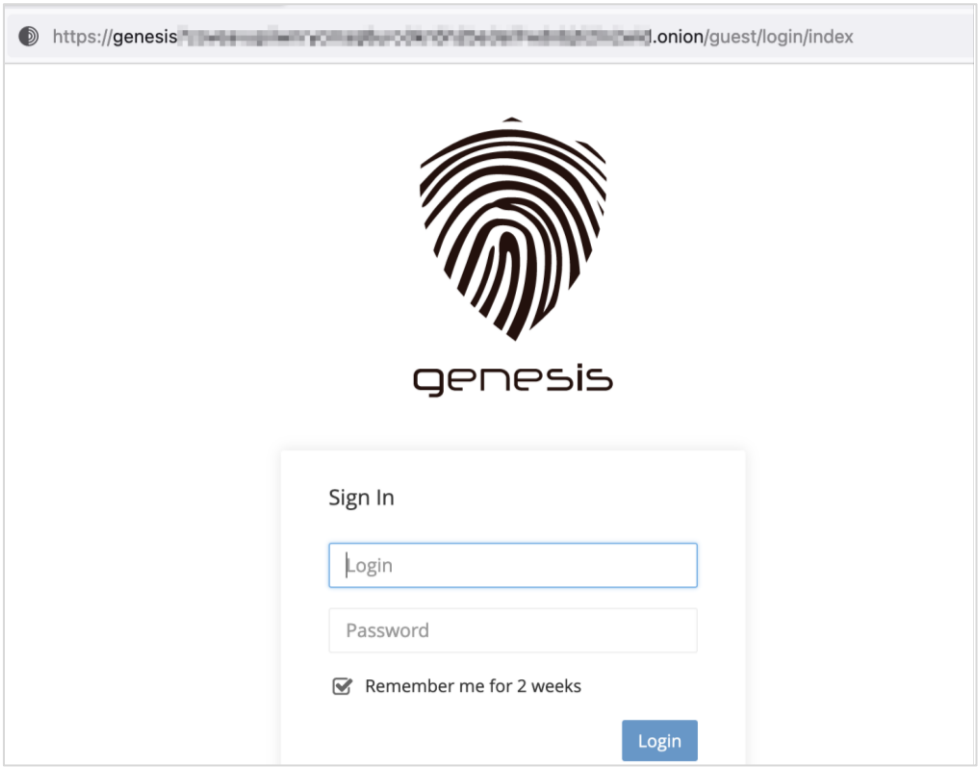

図 5 ダークウェブ上の Genesis Market の Web サイト（5 月 15 日時点）

1.4. まとめ

2018 年から長期に渡り初期アクセス・ブローカーとしてサイバー犯罪に加担してきた Genesis Market が摘発され、多くのユーザーが逮捕された。これは国際的な捜査協力の大きな成果ではあるが、類似したサービスを提供するマーケットは他にも確認されていることから[14]、引き続き警戒が求められる。

Genesis Market や類似サービスのマルウェアに感染すると、企業に大きなダメージを与える攻撃のきっかけとなるため、不審なファイルや URL を開かない、ウイルス対策ソフトの導入やアップデートを行うといった基本的な対策を怠らず実施する必要がある。

[13] 出典：HACKREAD『Genesis Market's Clearnet domain seized; Dark Web site still online』 https://www.hackread.com/dark-web-genesis-market-domain-seized/

[14] 出典：ReliaQuest『The Technology Adoption Lifecycle of Genesis Market』 https://www.reliaquest.com/blog/the-technology-adoption-lifecycle-of-genesis-market/

2. リーク文書「Vulkan files」とその波紋

2.1. 概要 [15]

ロシアのサイバー戦争への取り組みの一端を明かす機密文書が報道された。モスクワの IT コンサルタント会社である NTC Vulkan 社（以下、Vulkan と呼称）の社内文書であることから「Vulkan files」と呼ばれている。ロシアのウクライナ侵攻に反対する同社の内部告発者が西側の報道機関に提供し、明るみになった。

Vulkan files の分析から、ロシア政府によるサイバー攻撃と情報工作をサポートする大規模なツールの開発が確認された。また、ツールの開発元である Vulkan と、これまで様々なサイバー攻撃への関与が確認されてきたロシア政府系のハッキンググループとの関連も文書の中にみられた。

2.2. リーク文書「Vulkan files」 [16]

【モスクワの IT コンサル会社、Vulkan】

Vulkan は、モスクワに居を構える情報セキュリティが専門の IT コンサルティング会社である（図 6）。社名はロシア語で火山を意味する。ロシアの元陸軍軍人の Anton Markov が 2010 年に設立した。大手銀行の Sberbank、国営航空会社のアエロフロート、ロシア鉄道といったロシアの大企業が顧客となっている。

設立者のコネクションから、軍・情報機関と Vulkan に人的交流がみられる事、また従業員の多くは、ロシアの治安機関の影響下にあるモスクワのバウマン大学の卒業生である事等から、ロシアの国家と関係が深い軍産複合体の一部と、Vulkan は位置付けられている。

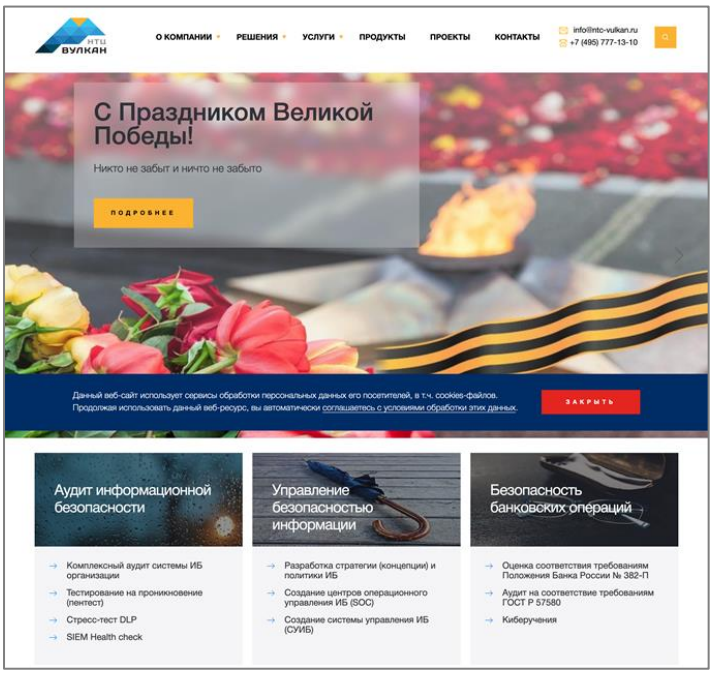

図 6 Vulkan のホームページ

【Vulkan からの内部告発】

2022 年 2 月、ロシアがウクライナへと侵攻を開始した。Vulkan 社内のある人物はウクライナでロシアが起こした様々な非道な行いとそのようなロシア政府に協力する Vulkan に怒りを感じ、密かにドイツのジャーナリストと接触した。そして、Vulkan がロシアの政府機関に提供していたサイバー攻撃ツールについての数千ページに及ぶ機密文書「Vulkan files」を、ドイツの報道調査グループに提供した。内部告発者は「密室で何が起こっているのかを明らかにするためにこの情報を活

[15] 出典：The Guardian『'Vulkan files' leak reveals Putin's global and domestic cyberwarfare tactics』
https://www.theguardian.com/technology/2023/mar/30/vulkan-files-leak-reveals-putins-global-and-domestic-cyberwarfare-tactics

[16] 出典：The Guardian『'Vulkan files' leak reveals Putin's global and domestic cyberwarfare tactics』
https://www.theguardian.com/technology/2023/mar/30/vulkan-files-leak-reveals-putins-global-and-domestic-cyberwarfare-tactics

用することを望む」[17]と述べている。

グループは、DER SPIEGEL 紙をはじめ協定を結んでいる複数の報道機関に Vulkan files を共有した。欧米の情報機関も加えた専門家らによる精査の結果、本物の可能性が高いと判断されたため、2023 年 3 月 30 日に DER SPIEGEL 紙等から Vulkan files についての調査報道記事が発表された。

【Vulkan files の中身】

Vulkan files は 2016 年から 2021 年までの 5,000 ページを超えるデータであり、電子メール、内部文書、プロジェクト計画書、予算書、契約書類を含む（図 7）。分析から、ロシアの情報機関のために Vulkan がツールを開発・提供するという協力関係が明らかになった。関係が判明した情報機関には、軍事情報機関の GRU、ロシア国内を監視する情報機関の FSB、対外工作や経済工作の SVR がある。文書内には米国の地図やスイスの原子力発電所の図もみられ、標的をヨーロッパと米国に想定していることをうかがわせる。

Vulkan files からは、開発されたツールが実際の攻撃に使用されたかまでは明らかになっていない。一方で、ツールの実用性や完成度等から、ウクライナ侵攻前後に確認されたサイバー攻撃での使用の可能性が疑われている。

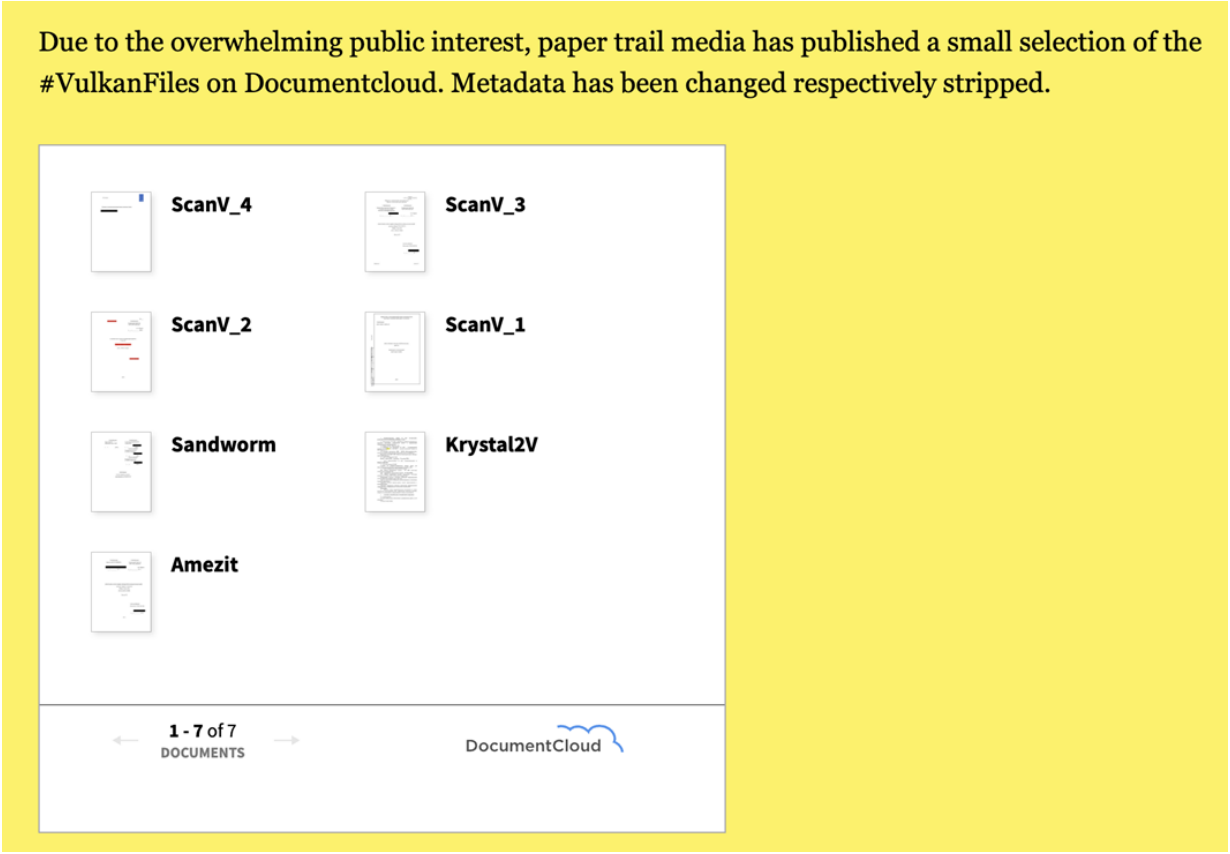

図 7 Vulkan files のデータ
（ドイツの報道調査グループ「paper trail media」のサイトで一部のデータが公開されている）[18]

[17] 出典：paper trail media『Vulkan Files』
https://www.papertrailmedia.de/investigations/vulkan-files/

[18] 出典：paper trail media『Vulkan Files』
https://www.papertrailmedia.de/investigations/vulkan-files/

2.3. Vulkan files に記されていたツール

Vulkan files から、以下の 3 件のサイバー攻撃や情報工作のツールの開発プロジェクトに、Vulkan が関与していることが確認された。[19] [20] [21]

【Scan-V：脆弱なシステムを探索するツール】

「Scan-V」は世界中の攻撃候補となるシステムをスキャンし脆弱性情報等を収集するツールである。Vulkan files には、収集したデータを収納するデータベースの構築方法に関する、包括的なドキュメントが含まれている。

情報機関の GRU と連携して開発したことが Vulkan files に含まれる情報の範囲では分かっているが、実際に GRU が Scan-V の購入や配備に至ったかまでは不明である。一方で Vulkan files に Scan-V のサブシステムとして記載されているツールが、2012 年頃に検知した世界的なサイバー攻撃「MiniDuke」で使用されていたと Google のセキュリティチームは分析しており、この時の成功を受けて Scan-V 本体の開発プロジェクトが促進されたと考察 [22]している。

【Amesit：情報工作支援ツール】

「Amesit」は、インターネット上での情報工作を準備から実施まで一貫して支援する、フレームワーク型のツールである。大規模なツールであるため開発には複数社が参加し、幹事社を務める Vulkan の社員が度々FSB 本部を訪問して仕様をヒアリングしていた。

Amesit を使用する情報工作員はまず、ロシア国内・国外の言論の広がりを把握するため、SNS や携帯電話の通話等の監視・傍受・収集を実施する。次に、状況に合わせた情報工作を検討し、使用するコンテンツを作成する。コンテンツは、さまざまな形式のテキスト、画像、ビデオ、音声データで展開可能である。そして、コンテンツを SNS、ブログ、SMS、電子メールなど、複数のベクトルに跨ってばら撒く。Vulkan files にある資料は、Amesit は SNS での情報工作を支援するため約 100 個もの偽の SNS アカウントを管理する機能、またアカウントの偽装元を特定する調査を回避する機能を有すると説明している。

Amesit による情報工作の影響範囲は、ロシア周辺地域に限定する場合にも、ロシア国外でグローバルに展開する場合にも、どちらにも使えるようになっていると考えられている [23]。

【Krystal-2B：サイバー工作訓練ツール】

「Krystal-2B」は、サイバー攻撃を実施する工作員に向けたトレーニング用ツールである。最大 30 人が同時に訓練に参加できる。

鉄道、航空、海上の重要インフラの制御系システムを狙った演習、またロシアの軍事インフラの脆弱性を調べる演習と、攻守

---

[19] 出典：Mandiant『Contracts Identify Cyber Operations Projects from Russian Company NTC Vulkan』
https://www.mandiant.com/resources/blog/cyber-operations-russian-vulkan

[20] 出典：DER SPIEGEL『The "Vulkan Files": A Look Inside Putin's Secret Plans for Cyber-Warfare』
https://www.spiegel.de/international/world/the-vulkan-files-a-look-inside-putin-s-secret-plans-for-cyber-warfare-a-4324e76f-cb20-4312-96c8-1101c5655236

[21] 出典：The Washington Post『The Vulkan Files: Secret trove offers rare look into Russian cyberwar ambitions』
https://www.washingtonpost.com/national-security/2023/03/30/russian-cyberwarfare-documents-vulkan-files/

[22] 出典：DER SPIEGEL『The "Vulkan Files": A Look Inside Putin's Secret Plans for Cyber-Warfare』
https://www.spiegel.de/international/world/the-vulkan-files-a-look-inside-putin-s-secret-plans-for-cyber-warfare-a-4324e76f-cb20-4312-96c8-1101c5655236

[23] 出典：The Guardian『'Vulkan files' leak reveals Putin's global and domestic cyberwarfare tactics』
https://www.theguardian.com/technology/2023/mar/30/vulkan-files-leak-reveals-putins-global-and-domestic-cyberwarfare-tactics

の両方の演習をサポートできるよう設計されているとみられている。

【Amesit の訓練に使われた Krystal-2B】

Vulkan files にあるサイバー工作訓練ツールの Krystal-2B を使用した演習計画では、情報工作支援ツールの Amesit を使用することが記されている。また、演習を通じて航空、海上、鉄道の運用を制御するシステムを含む、現実世界のインフラストラクチャを混乱させる能力を鍛えると明確に述べている [24]。これらの記述から、Amesit の機能の多さは、情報工作だけに留まらず公共インフラ攻撃支援の機能にも及んでいると考えられている。

2.4. Vulkan とロシア関連 APT グループの接点

Vulkan files からは、Vulkan とロシアの APT グループとの接点も発見されている。GRU のサイバー部隊と推定されている Sandworm グループ[25]は、2015 年のウクライナの送電システムへのサイバー攻撃や、2017 年の NotPetya マルウェアの感染拡大、2018 年の韓国・平昌冬季オリンピックに対する「オリンピック デストロイヤー攻撃」等のサイバー攻撃の主犯であると、英米の政府機関が非難している[26]。Vulkan files では、Sandworm グループが Scan-V の構築支援を Vulkan に許可した書類が確認されている。

他にも Scan-V 開発において、関連したサイバー攻撃「MiniDuke」は SVR に属する Cozybear グループ[27]が実行したとの推定から、Vulkan は Cozybear グループとも接点があるとみられている [28]。

2.5. まとめ

Vulkan files はロシアのサイバー戦争の驚くべき実情を明らかにした。2010 年代からロシア政府はハイブリッド戦争を想定し、サイバー攻撃を戦略に組み込もうとしていた。情報工作ツールである Amesit と訓練ツールの Krystal-2B の組み合わせは、ロシア政府が公共インフラへのサイバー攻撃実行中に情報工作を展開することに高い価値を置いている証と、推察[29]されている。

Vulkan files は 2021 年までの情報であり、それ以降に起きたウクライナ侵攻でのサイバー攻撃の実態は、直接には記されていない。しかし、侵攻に前後して Vulkan files にあるツールの機能にみられるような情報工作や重要インフラへの攻撃、さらにミサイルや軍隊による攻撃が同時進行するハイブリッド戦が、ウクライナに対し盛んに行われた。ウクライナ侵攻に至る取り組みの一端を、Vulkan files は明らかにしたといえる。

---

[24] 出典：Mandiant『Contracts Identify Cyber Operations Projects from Russian Company NTC Vulkan』
https://www.mandiant.com/resources/blog/cyber-operations-russian-vulkan

[25] 出典：MITRE ATT&CK『Sandworm Team』
https://attack.mitre.org/groups/G0034/

[26] 出典：U.S. Department of Justice『Six Russian GRU Officers Charged in Connection with Worldwide Deployment of Destructive Malware and Other Disruptive Actions in Cyberspace』
https://www.justice.gov/opa/pr/six-russian-gru-officers-charged-connection-worldwide-deployment-destructive-malware-and

[27] 出典：MITRE ATT&CK『APT29』
https://attack.mitre.org/groups/G0016/

[28] 出典：DER SPIEGEL『The "Vulkan Files": A Look Inside Putin's Secret Plans for Cyber-Warfare』
https://www.spiegel.de/international/world/the-vulkan-files-a-look-inside-putin-s-secret-plans-for-cyber-warfare-a-4324e76f-cb20-4312-96c8-1101c5655236

[29] 出典：Mandiant『Contracts Identify Cyber Operations Projects from Russian Company NTC Vulkan』
https://www.mandiant.com/resources/blog/cyber-operations-russian-vulkan

3. FBI がジュースジャッキング（Juice-Jacking）攻撃について警告

3.1. FBI による注意喚起

4 月 6 日、米連邦捜査局（FBI）のデンバー支局は、空港等に設置されている USB 充電ポートに細工した上で、それに接続した端末に対してマルウェアをインストールする等の攻撃を行う、「ジュースジャッキング（Juice-Jacking）攻撃」に注意する呼びかけを、Twitter に投稿した（図 8）[30]。

FBI デンバー支局によると、FBI は定期的にパートナー組織と連携して注意喚起や公共サービスの通知を行っている[31] [32]。

図 8 FBI デンバー支局のツイート

和訳：空港やホテル、ショッピングセンターにある無料の充電ステーションの利用を避けてください。アクターらは、公共の USB ポートを使って端末にマルウェアや監視ソフトを取り込む方法を既に見つけ出しています。自分の充電器と USB コードを携行し、コンセントを使いましょう。

[30] 出典：Twitter『@FBIDenver』
https://twitter.com/FBIDenver/status/1643947117650538498

[31] 出典：SLATE『Actually, Charging Your Phone in a Public USB Port Is Fine』
https://slate.com/technology/2023/04/free-public-phone-chargers-fbi-warning-bad-actors-threat-bogus-debunked.html

[32] 出典：Federal Communications Commission『What is 'Juice Jacking' and Tips to Avoid It』
https://www.fcc.gov/juice-jacking-tips-to-avoid-it

3.2.「ジュースジャッキング（Juice-Jacking）攻撃」とは

【増加する USB 充電ポート】[33]

これまでは、長期の出張／旅行の際にスマホやタブレット端末を充電する場合、自身で充電器やモバイルバッテリーを持ち歩くことが一般的であった。しかし近年は、施設のグレードや国/地域にもよるが、空港やホテル、カフェなどで、スマホやタブレット端末の充電が誰でも無料でできる USB 充電ポートの設置が増加しつつあり、USB ケーブルを一本携行するだけで、旅先の様々な場所で気軽に充電することができる。

出力の問題から USB 充電ポートでは PC に充電することはできないが、今後、PC に対応した USB 充電ポートも発売されるため[34]、スマホやタブレット等だけでなく PC の充電も一般化していくと考えられる。

図 9 羽田空港に設置されている USB 充電ポート[35]

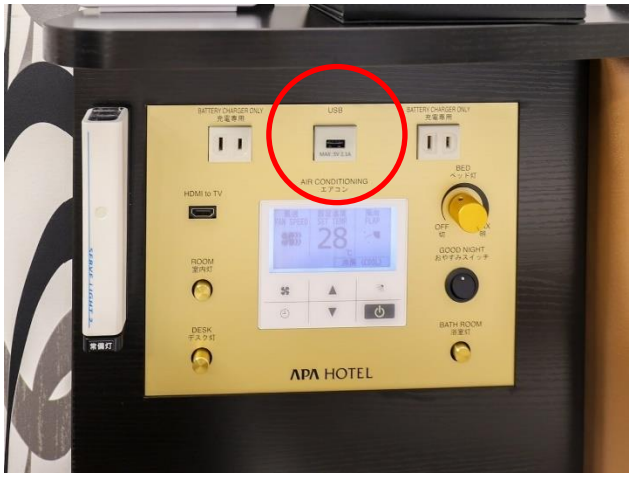

図 10 ホテルのベッド脇の USB 充電ポート[36]
（明示のため赤丸を追加）

【攻撃手法】

攻撃者は、公共の場で提供されている USB 充電ポートの中に小型チップを埋め込む等の細工を施す。何も知らないユーザーがこのポートに接続してしまうと、充電中にデータの窃取が行われる他、監視ソフトウェアやマルウェアをインストールされる可能性がある。このような USB 充電ポートに罠を張るサイバー攻撃を**「ジュースジャッキング攻撃」**と呼ぶ。

普段セキュリティを意識しているユーザーであれば、PC 等に自分のあずかり知らない USB メモリを接続する事に対しては抵抗感が大きい。これに比べると、スマホやタブレット端末を USB 充電ポートに接続することは多くのユーザーが行っており、抵抗感は小さい。これは、USB メモリと異なり、USB 充電ポートに接続しても、充電と同時にデータ通信も行われるとは想定しづら

[33] 出典：Forbes『How 'Juice Jackers' Plant Malware On Your Phone At Airports And Hotels』
https://www.forbes.com/sites/suzannerowankelleher/2023/04/20/juice-jacking-malware-phone-airports-hotels/

[34] 出典：PC Watch『パナソニック、業界初の最大 60W PD 対応 USB コンセント』
https://pc.watch.impress.co.jp/docs/news/1500589.html

[35] 出典：PR TIMES『羽田空港の充電設備を機能強化 / 蓄電池を内蔵し、停電時にも充電が可能に』
https://prtimes.jp/main/html/rd/p/000000006.000058641.html

[36] 出典：アパホテル『【公式】アパホテル〈浅草 新御徒町駅前〉』
https://www.apahotel.com/hotel/syutoken/tokyo/shin-okachimachi-ekimae/gallery/

いためと考えられる。

【デモンストレーション】

ジュースジャッキング攻撃というアイディアが最初に紹介されたのは、2011 年。DEFCON という国際的なセキュリティ会議の開催期間中に行われたデモンストレーションにおいてであった[37]。DEFCON は、毎年ラスベガスで開催されており、多くのハッカーやセキュリティ専門家、研究者、政府関係者等が参加している[38]。

この発表以降、複数のハッカーやサイバー研究者がジュースジャッキング攻撃を成功させるために、端末において実施しているセキュリティ対策の回避や、普通の USB 充電ポートと見た目が変わらないようにする細工を行うこと等を研究するようになった。2019 年の DEFCON では iPhone の充電ケーブルに細工することで、マルウェアをインストールし遠隔操作を可能にするツールの発表があり、ジュースジャッキング攻撃に利用できると注目された[39]。

【O.MG アダプター】

この DEFCON で発表されたツールは「O.MG アダプター」といい、現在、セキュリティ研究者向けに販売されている。

O.MG アダプターの見た目は単なる USB 変換プラグだが、コネクター部分に小型のチップが埋め込まれている(図 11 [40] 図 12 [41])。この小型チップによって、接続した端末は Wi-Fi のアクセスポイントとなり、攻撃者は端末の利用者に気づかれることなく外部から無線 LAN で端末内にアクセスできるようになる。

USB 充電ポート内に、このようなハッキングのためのケーブルやパーツを組み込むことは容易であり、攻撃者によっては数分で作業を完成させることができるといわれている [33]。

図 11 O.MG アダプター

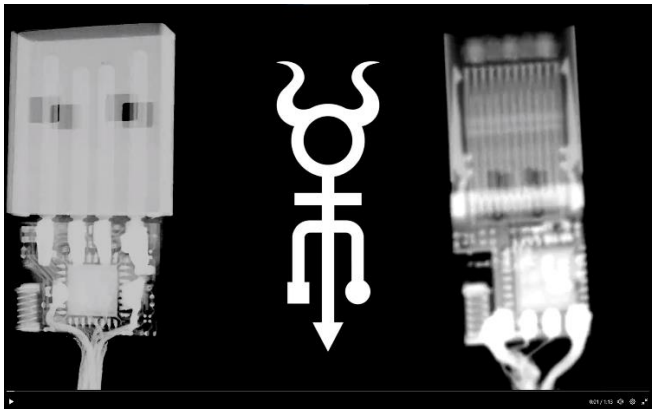

図 12 チップが埋め込まれたコネクター
(O.MG アダプター製作者 Twitter の動画より)

[37] 出典：naked security by SOPHOS『Juicejacking – an emergency phone charge can be a security risk』
https://nakedsecurity.sophos.com/2011/08/19/is-juicejacking-the-new-firesheep/

[38] 出典：GMO サイバーセキュリティ by イエラエ『ハッカーの祭典" DEFCON 26 現地レポート-その 1』
https://gmo-cybersecurity.com/blog/defcon-26_part1/

[39] 出典：Forbes『Why You Should Never Borrow iPhone Cables』
https://www.forbes.com/sites/zakdoffman/2021/05/29/apple-iphone-and-ipad-users-warned-not-to-borrow-other-peoples-cables/

[40] 出典：ラジオライフ.com『変換コネクタ型ハッキングツールがデータを盗む』
https://radiolife.com/internet/virus/61548/

[41] 出典：Twitter『@_MG_』
https://twitter.com/_MG_/status/1565003970535247872

【攻撃への利用への危惧】

2023 年 4 月時点の米連邦通信委員会の発表 [32] にあるように、これまでジュースジャッキング攻撃の事例は知られていない。だが、O.MG アダプターのように、ジュースジャッキングという手法の実用化は進んでいるため、既に攻撃に利用されていても不思議ではない。政府高官等を狙うスパイ行為のような攻撃への使用が危惧される他 [39]、金銭的利益を狙うサイバー犯罪者にも魅力的な攻撃と考えられている [33]。

3.3. ジュースジャッキング攻撃への対策

ジュースジャッキング攻撃の予防として、USB 充電ポートの利用を極力避けることが挙げられる。または、市販されている充電専用の USB ケーブルを携帯して USB 充電ポート接続時に使用すれば、データ通信が行われず攻撃が成立しない。

3.4. まとめ

今回の FBI からの注意喚起により、これまでに危険性を指摘されてきたフリーWi-Fi 同様[42]、公共の場にある USB 充電ポートにおいても、思いも寄らない被害を招く可能性があることが改めて知られるようになった。

USB 充電ポートの設置場所は今後も増えていくことが予想される。外出先で端末を充電する際は、注意を怠らないようにする事が必要である。

以上

[42] 出典：スペクトラム・テクノロジー株式会社『被害事故例（WiFi)』
https://spectrum-tech.co.jp/incident.html

免責事項

本記事の内容は、正確であることに最善を尽くしておりますが、内容を保証するものではなく、本記事の利用に起因して発生したいかなる損害、損失についても補償しませんのでご留意ください。記事内に誤植や内容の誤り、その他ご指摘等、お問い合わせ事項がある場合は、お手数ですが下記までご連絡ください。

お問い合わせ先：NTT セキュリティ・ジャパン株式会社

コンサルティングサービス部　OSINT モニタリングチーム
メールアドレス： WA_Advisorysupport@ntt.com