サイバーセキュリティレポート

2023.11

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

【1 ページサマリー】

当レポートでは 2023 年 11 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『ランサムウェアグループが被害組織を米国証券取引委員会に告発』

- ランサムウェアグループ ALPHV が、自身が攻撃した被害組織を重要インシデントの情報開示義務に違反したとして、米国証券取引委員会（証取委）に告発した。
- ランサムウェアグループが被害組織を証取委に告発したことが明らかになった事例は、今回が初めてとみられている。
- ALPHV が行った告発の意図は不明であるが、交渉がうまくいかなかったために嫌がらせや、新しい脅迫手法を模索している可能性等が考えられる。

第 2 章『オンラインサービスで作成した短縮 URL で不正なサイトに誘導される』

- 11 月 9 日、スーパーマーケットを展開する株式会社いなげやは、ポスターやチラシに掲載した QR コードをスマートフォンなどで読み取った際、アクセス先のサイトでクレジットカード情報が抜き取られる被害があったことを発表した。
- 本件では、QR コード化されていた URL は短縮 URL サービスで短縮したものだった。短縮 URL サービスで表示される広告から不正なサイトに誘導されたことが、被害に繋がったとみられている。
- 本件の発生以前から政府機関では、攻撃に遭った場合等の問題を踏まえ、短縮 URL サービスによる短縮の禁止をルールに盛り込むよう定めていた。これに倣い、他の組織においても「原則禁止」と定めることが望ましいと考える。

第 3 章『マイクロソフトの開発ツール「VS Code」、設定漏れでパスワードが公開される危険性』

- マイクロソフト社の開発ツール「VS Code」でファイル転送を行う「SFTP プラグイン」の設定を誤ると、SFTP 等の接続に利用されるパスワードを含むファイルがアップロードされ、インターネット上に公開される。
- ハッカーの間では VS Code の SFTP プラグインの情報を収集できるツールが取引されており、実際に攻撃に悪用された事例もある。
- 安全な設定を確実に行うよう注意していても、ミスを完全に防ぐことは困難である。このようなミスを検知できる仕組みやシステムを用意し、多重にチェックできる体制を整えたい。

1. ランサムウェアグループが被害組織を米国証券取引委員会に告発

1.1. 概要

11 月 15 日、ランサムウェアグループ ALPHV は、自身が攻撃した米企業 MeridianLink 社を、重要インシデントの情報開示義務に違反したとして、米国証券取引委員会（以下、証取委）に告発したと明かした。

ランサムウェアグループが被害組織を証取委へ告発したことが公になった事例は、今回が初めてとみられている[1]。

1.2. ALPHV によるランサムウェア攻撃

【ALPHV と MeridianLink 社】

攻撃を行った ALPHV は、2021 年 11 月に活動が確認されたランサムウェアグループで、BlackCat の別名でも知られている[2]。ターゲット組織のネットワークにあるファイルを暗号化／窃取し、身代金が支払われなければ、それらのファイルを復号せず、窃取したファイルは公開するといった脅迫を行う[3]。

2023 年上半期の ALPHV の被害組織数は 205 件、全ランサムウェアグループの中で LockBit3.0 に続き 2 番目に多いものであった（被害組織数は当社調べ）。最近では日本企業のセイコーグループ株式会社が 7 月に[4]、また、日本航空電子工業株式会社が 11 月に[5]、ALPHV の被害にあっており、両社共に窃取されたファイルが ALPHV の暴露サイトで公開された。

今回の事件で被害に遭った MeridianLink 社は、金融機関向けにクラウドベースのソフトウェアソリューションを提供する米国の企業であり[6]、ニューヨーク証券取引所に株式を上場している[7]。

【MeridianLink 社に対する攻撃】

11 月 7 日、ALPHV は暗号化はしなかったものの、MeridianLink 社からファイルの窃取を実行した[1]。

攻撃から約 1 週間経った 11 月 15 日、ALPHV は MeridianLink 社に対する攻撃を行ったことを、自身が運営する暴露サイトへの投稿で明らかにした。この投稿には、「24 時間以内に MeridianLink 社から連絡がない場合、顧客データを公開する」という脅迫文が記載されていた（投稿は既に削除済み）。

---

[1] 出典：DataBreaches.net『AlphV files an SEC complaint against MeridianLink for not disclosing a breach to the SEC (2)』
https://www.databreaches.net/alphv-files-an-sec-complaint-against-meridianlink-for-not-disclosing-a-breach-to-the-sec/

[2] 出典：Bleeping Computer『ALPHV BlackCat - This year's most sophisticated ransomware』
https://www.bleepingcomputer.com/news/security/alphv-blackcat-this-years-most-sophisticated-ransomware/

[3] 出典：Medium『ALPHV/BlackCat: Who, What, Where, Why, How』
https://warnerchad.medium.com/alphv-blackcat-who-what-where-why-how-6290395473f0

[4] 出典：Bleeping Computer『Japanese watchmaker Seiko breached by BlackCat ransomware gang』
https://www.bleepingcomputer.com/news/security/japanese-watchmaker-seiko-breached-by-blackcat-ransomware-gang/

[5] 出典：SecurityWeek『Japan Aviation Electronics Targeted in Ransomware Attack』
https://www.securityweek.com/japan-aviation-electronics-targeted-in-ransomware-attack/

[6] 出典：MeridianLink Inc『INVESTOR RELATIONS』
https://ir.meridianlink.com/overview/

[7] 出典：MeridianLink Inc『MeridianLink Announces Upsizing and Pricing of Initial Public Offering』
https://www.meridianlink.com/blog/press-release-meridianlink-announces-upsizing-and-pricing-of-initial-public-offering/

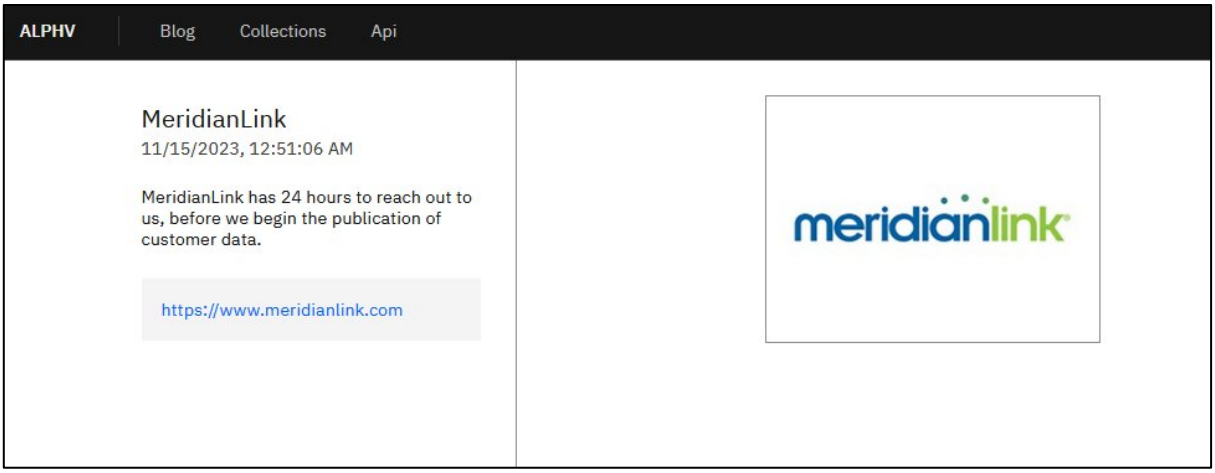


図 1 ALPHV が MeridianLink 社について行った投稿

1.3. ALPHV による証取委への告発

【証取委への告発】

上記の投稿と同日、ALPHV はさらに、MeridianLink 社が重要インシデントの情報開示義務に違反しているとして、証取委に告発したと投稿した。そこには、「証取委に最近採用された規則により、株式公開企業は重大なサイバーセキュリティインシデントを 4 営業日以内に速やかに開示することが義務付けられている。しかし、MeridianLink 社は 1 週間前に発生した侵害についてこの義務を果たしていない。従って、必要な開示の提出を怠ったとして証取委に告発した」と記載されていた。

ALPHV はさらに、証取委サイトの Web フォームに記入した告発内容のスクリーンショットも公開した（投稿は既に削除済み）。

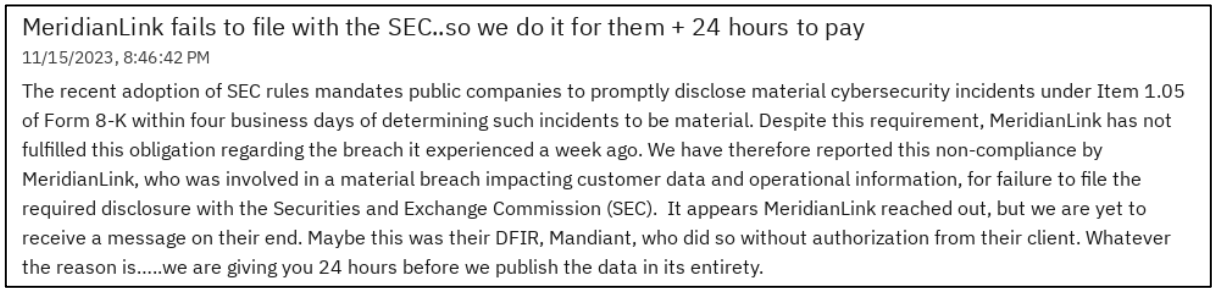


図 2 ALPHV が証取委に MeridianLink 社を告発したとする投稿

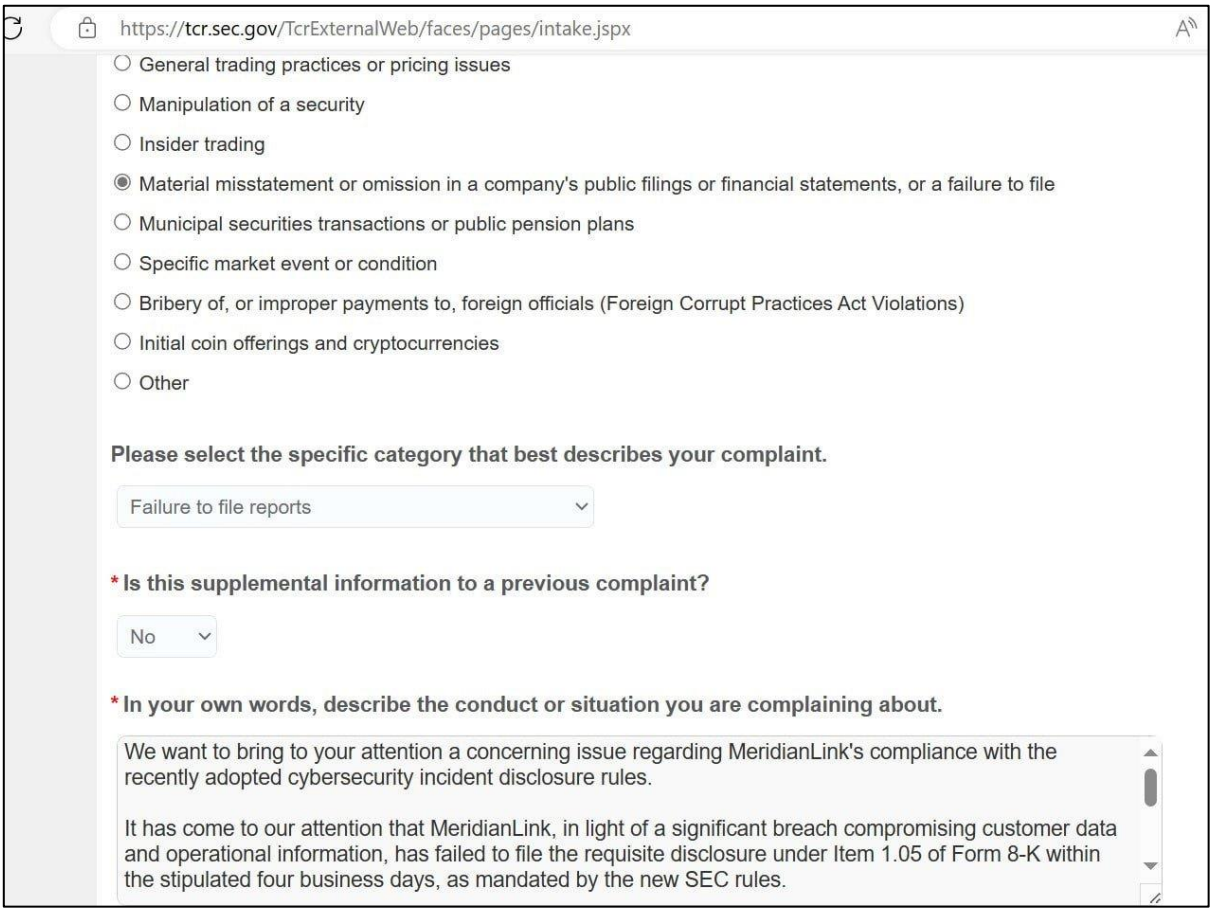


図 3 ALPHV が証取委サイトの Web フォームに記入した告発内容のスクリーンショット

【MeridianLink 社の対応】

ALPHV が言う 4 営業日以内の開示義務に関連して MeridianLink 社は、「証取委の新しい開示規則は 12 月 15 日まで発効されないと考えている」と、取材に答えている [1]。

証取委が今年 7 月に発行したプレスリリースには、新しい開示規則は早くても 12 月 18 日に開始されると記載されており [8]、日付に相違はあるものの、MeridianLink 社が主張する通り、証取委の新しい規則はまだ発効されていなかった。

[8] 出典：U.S. Securities and Exchange Commission『SEC Adopts Rules on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure by Public Companies』
https://www.sec.gov/news/press-release/2023-139

SEC Adopts Rules on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure by Public Companies

FOR IMMEDIATE RELEASE
2023-139

Washington D.C., July 26, 2023 — The Securities and Exchange Commission today adopted rules requiring registrants to disclose material cybersecurity incidents they experience and to disclose on an annual basis material information regarding their cybersecurity risk management, strategy, and governance. The Commission also adopted rules requiring foreign private issuers to make comparable disclosures.

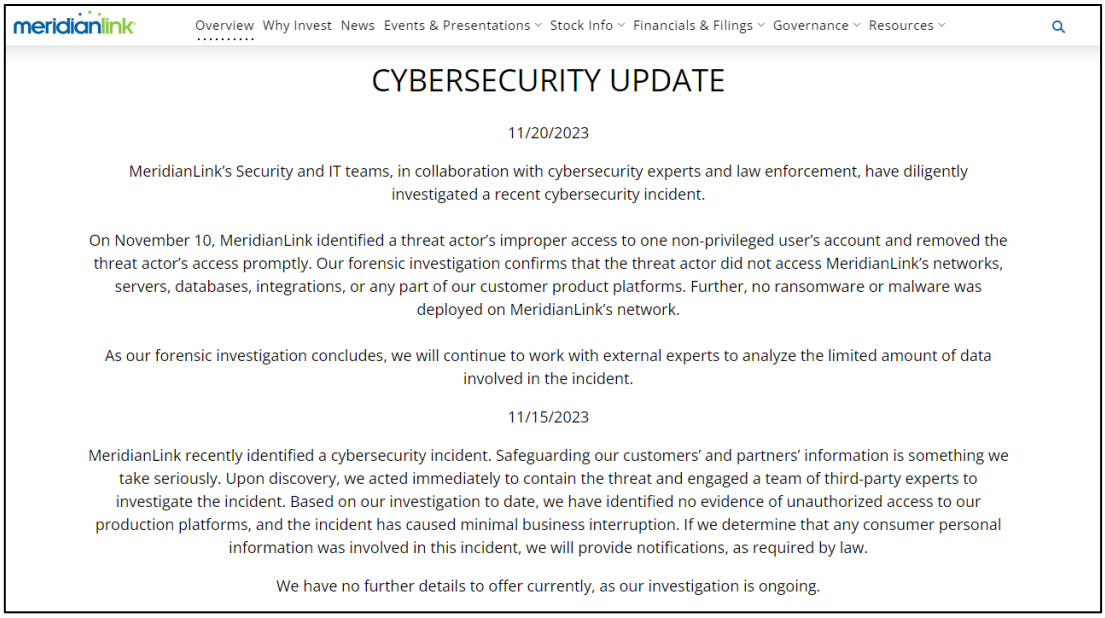
"Whether a company loses a factory in a fire — or millions of files in a cybersecurity incident — it may be material to investors," said SEC Chair Gary Gensler. "Currently, many public companies provide cybersecurity disclosure to investors. I think companies and investors alike, however, would benefit if this disclosure were made in a more consistent, comparable, and decision-useful way. Through helping to ensure that companies disclose material cybersecurity information, today's rules

図 4 証取委が 7 月に発行したプレスリリース

なお、MeridianLink 社は 11 月 15 日と 11 月 20 日に、今回の攻撃についてのプレスリリースを発表している。[6]

ALPHV による攻撃の暴露と脅迫があった 15 日の初報では、現在調査中であり、もし個人情報漏洩等の法令に関わる被害があった場合は公的機関に通知するつもりであることを公表している。

また、20 日の第 2 報では、非特権ユーザーへの不正アクセスはあったが、社内のネットワークやデータへのアクセス、ランサムウェアなどマルウェアの感染は無かったことを含め、調査状況の進捗を伝えた。



meridianlink Overview Why Invest News Events & Presentations Stock Info Financials & Filings Governance Resources

CYBERSECURITY UPDATE

11/20/2023

MeridianLink's Security and IT teams, in collaboration with cybersecurity experts and law enforcement, have diligently investigated a recent cybersecurity incident.

On November 10, MeridianLink identified a threat actor's improper access to one non-privileged user's account and removed the threat actor's access promptly. Our forensic investigation confirms that the threat actor did not access MeridianLink's networks, servers, databases, integrations, or any part of our customer product platforms. Further, no ransomware or malware was deployed on MeridianLink's network.

As our forensic investigation concludes, we will continue to work with external experts to analyze the limited amount of data involved in the incident.

11/15/2023

MeridianLink recently identified a cybersecurity incident. Safeguarding our customers' and partners' information is something we take seriously. Upon discovery, we acted immediately to contain the threat and engaged a team of third-party experts to investigate the incident. Based on our investigation to date, we have identified no evidence of unauthorized access to our production platforms, and the incident has caused minimal business interruption. If we determine that any consumer personal information was involved in this incident, we will provide notifications, as required by law.

We have no further details to offer currently, as our investigation is ongoing.

図 5 MeridianLink 社が発行したプレスリリース

1.4. まとめ

ランサムウェアグループは従来、被害組織の端末やサーバー上のファイルを暗号化し、そのファイルの復号と引き換えに金銭（身代金）を要求していた。

しかしここ数年は、前述の脅迫に加え、窃取したファイルの公開、EU の GDPR（一般データ保護規則）など規則違反の公表、株主やユーザーといった利害関係者やマスコミへの公表、DDoS（分散サービス拒否）攻撃の実行、窃取したファイルをオークションでの販売など、ランサムウェアグループは被害組織に対しさらなる脅迫を試みている。

ALPHV は今回、「証取委に情報開示義務違反を告発されたくなかったら引き換えに身代金を払え」という脅迫ではなく、証取委に情報開示義務違反を告発したという発表を行ったのであり、被害企業にプレッシャーを与え身代金を支払うよう仕向けているようには見られない。ALPHV が公表していないため今回の行動の意図は不明であるが、交渉がうまくいかなかったために嫌がらせや、新しい脅迫手法を模索している可能性等が考えられる。

2. オンラインサービスで作成した短縮 URL で不正なサイトに誘導される

2.1. 概要

南関東でスーパーマーケットを展開する株式会社いなげやは 11 月 9 日、ネットスーパーの入会案内のためのポスターやチラシに掲載した QR コードを顧客がスマートフォンなどで読み取った際、アクセス先のサイトでクレジットカード情報が抜き取られる被害があったことを発表した。QR コードにはオンラインのサービスで作成された短縮 URL が使用されていた。

いなげやは、同スーパー以外の不審なサイトがアクセス先で表示された場合はすぐに画面を閉じ、クレジットカード番号を入力してしまった場合はカード会社へ連絡するよう顧客に呼び掛けた（図 6）[9]。

図 6 いなげやによる注意喚起（ITmedia News より。現在は削除済み）

[9] 出典：ITmedia News『「いなげや」QR コードから不正サイトに誘導、カード情報抜き取られる被害』
https://www.itmedia.co.jp/news/articles/2311/10/news120.html

2.2. 短縮 URL を含む QR コードについて

【長い URL について】[10]

検索サイトなどで URL をコピーすると、非常に長いことがある。これは、WEB アプリケーションが検索キーワード等の検索条件のパラメータ（クエリ文字列）を、基本の URL に追加しているためである。パラメータはページ間や WEB アプリケーションとの情報の受け渡し等に便利であるため、多くの Web サイトで利用されている。

例：https://www.google.com/search?q=NTT%E3%82%BB%E3%82%AD%E3%83%A5%E3%83%AA%E3%83%86%E3%82%A3%E3%82%B8%E3%83%A3%E3%83%91%E3%83%B3&lr=lang_ja&hl=ja&tbs=qdr%3Ay%2Clr%3Alang_1ja

WEB サイトでは様々なパラメータを付与するため、とても長い URL が生成される。長い URL は扱いにくく、見た目も悪いというデメリットがある。

【短縮 URL について】[11]

SNS などで「t.co」といったドメインを含む、10 文字程度の短い URL を目にすることがあるが、これらは基本的に専用のツールサービスを使って作成された短縮 URL である。

短縮 URL は長い WEB アドレスを短くすることで文字数を減らし、より利便性が高く分かりやすい体裁にすることができる。そのため、短縮 URL は、長い URL が自動改行で切れてしまうメールや、文字数制限があり長い URL を入力できない Twitter 等の SNS で特に人気を博した。（なお現在、X [旧・Twitter]では、URL は自動的に短縮 URL「t.co」に変換される）

短縮 URL サービスの中には、単に URL を短縮するだけでなく、クリック数、ユーザー数、アクセス方法など、追跡したい統計情報を確認するための機能を含めることが可能なものもある。

【短縮 URL の仕組み】[12]

アクセス先として指定したい URL（正規の URL）を短縮 URL サービスに登録すると、自動的に短縮された URL が生成され、その際、登録した本サービスのデータベースに正規の URL と紐づいて保存される。これにより、短縮 URL にアクセスすると正規の URL に転送される。

[10] 出典：IT 用語辞典 e-Words『URL パラメータ（リクエストパラメータ / GET パラメータ）とは』
https://e-words.jp/w/URL%E3%83%91%E3%83%A9%E3%83%A1%E3%83%BC%E3%82%BF.html

[11] 出典：NaviPlus『短縮 URL の基礎知識：仕組み、使用例、事例紹介』
https://www.naviplus.co.jp/bitly/info_url_shortening_101_how_it_works_use_cases_and_examples.html

[12] 出典：一般社団法人日本スマートフォンセキュリティ協会 『スマートフォン・サイバー攻撃対策ガイド「短縮 URL ＆ ダイナミック DNS の悪用」』
https://www.jssec.org/column/20220901.html

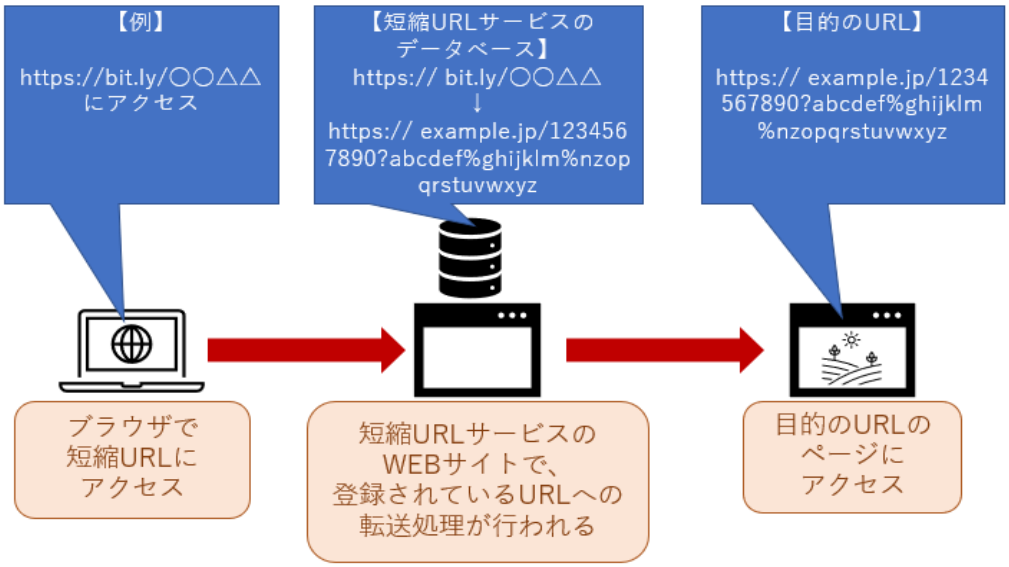


図 7 短縮 URL の仕組み

【短縮 URL を用いた QR コードの作成**】**[13, 14]

QR コードはセルと呼ばれる四角い黒白の点で構成されており、データ量が増えるとそのセル数が増えて画像が大きくなっていく。QR コードの読み取り精度は、QR コードリーダーとなるスマートフォンや携帯電話のカメラやアプリケーションの性能に依存しており、以前の、性能の低い携帯カメラが主流の頃は、データ量が多い QR コードをうまく読み取れないことがあった。読み取り精度を上げるため、QR コードの提供側では慣習的に短縮 URL サービスを利用して、データ量（URL の文字数）を減らし、より小さくシンプルな QR コードを作るようになった。

■短縮 URL の例

＊正規 URL（短縮前：107 文字）

https://b.qrqrq.com/about-long-qrcode/test/test/test/test/test/test/more-long/more-long/more-long/more-long

↓

＊短縮 URL（短縮後：28 文字）

https://r.qrqrq.com/7DVxtAPS

図 8 特定の URL にアクセスするための 正規 URL（短縮処理前）と短縮 URL（短縮処理後）[15]

図 9 左記の正規/短縮 URL による QR コードのセルの比較[16]

[13] 出典：株式会社デンソーウェーブ『QR コードの情報量とバージョン』
https://www.qrcode.com/about/version.html

[14] 出典：株式会社イケル『QR コードの作り方｜色の変え方や、細かすぎて読み取れない場合の対処法もご紹介します』
https://ikel.co.jp/column/2441.html

[15] 出典：アララ株式会社『短縮 URL を用いた QR コードの作成方法』
https://b.qrqrq.com/2018/06/07/qrcode-shorten_url/

[16] 出典：アララ株式会社『短縮 URL を用いた QR コードの作成方法』
https://b.qrqrq.com/2018/06/07/qrcode-shorten_url/

2.3. いなげやの事件と短縮 URL

今回のいなげやのケースは、業務委託先が作成したチラシやポスターに、無料の短縮 URL サービス「オンラインツール(onl.jp)」で生成された QR コードを掲載していた。onl.jp では、QR コードを介してスマートフォンなどから読み取った短縮 URL をクリックすると、正規の URL へリダイレクトする前に処理中であることを知らせるページが表示され、そこには広告スペースが設けられていた。スペース内の広告は onl.jp が広告収入を得るために掲載したものと思われ、内容は毎回異なっていたとみられる。いなげやの例では、クリックを誘発するような「OK」と書かれたボタンの広告が表示されていて、そのボタンをクリックすると正規の URL とは別のサイトが表示された。そこからさらに進み、促されるままにクレジットカード番号を入力して、情報を抜き取られるといった事態が発生したと考えられる[17]。

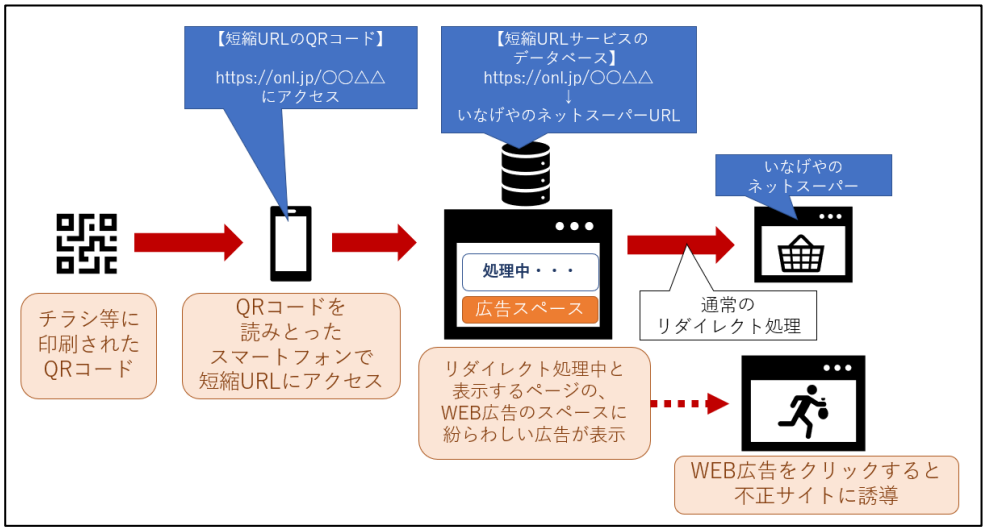


図 10 QR コードの読み込み後に広告が表示されるケースの流れ（一例）

図 11 短縮 URL サービスで標示された広告（左）と誘導先の不正サイト（中、右）の例
（赤枠をクリックすると不正サイト内での操作が進んでしまう）[18]

[17] 出典：Security NEXT『QR コード生成サイトの利用に注意 - 思わぬ動作でトラブルに』
https://www.security-next.com/151238

[18] 出典：ITmedia News『「いなげや」QR コードから不正サイトに誘導、カード情報抜き取られる被害』
https://www.itmedia.co.jp/news/articles/2311/10/news120.html

【同時期の類似事例】

同様の短縮 URL サービスでの被害事例は、オートバックスセブンが 10 月に送付したダイレクトメールに含まれる QR コードでも発生した。短縮 URL の作成はいなげやと同じサービスを使用したとみられ、コードを読み込むと予定していない広告ページが表示された[19]。ちなみに、これらの問題を受け「オンラインツール（onl.jp）」の短縮 URL サービスは、11 月 17 日付でサービスを停止した。

2.4. 短縮 URL の問題

短縮 URL はツールのドメインと無作為の英数字で構成されており、リンク先とのつながりを示す情報がないため、ユーザーはどこにアクセスさせられるのか判断できない。この特性から、短縮 URL はフィッシング詐欺やワンクリック詐欺、マルウェアのダウンロードなど悪質なサイトに誘導する手口として頻繁に利用されている[20]。

また、短縮 URL を提供する民間事業者のサービスは永続的なものではないため、サービスが消滅するとリダイレクト先がなくなり、正規の URL への接続ができなくなる。さらに放棄された短縮 URL のドメイン名が悪意ある者に取得されるというリスクもある。実際に別のサービスに再利用され、アクセスすると情報窃取や広告収入を狙った不正なサイトが表示されるケースがある。

短縮 URL は便利ではあるが、目的のサイトにアクセスさせるために他の事業者のサイトを経由することを強いることがそもそもの問題で、安易に利用することはユーザーの安全性を脅かすことになる可能性がある。

【政府機関での使用が禁止されている短縮 URL】[21, 22, 23]

短縮 URL の危険性については 10 年程前から既に認識されていた。例えば、日本政府では、内閣サイバーセキュリティセンター（NISC）の定める「府省庁対策基準策定のためのガイドライン」にて、平成 26（2014）年版以来、最新の令和 5（2023）年度版においても、短縮 URL は原則使用しないことを明記している。当ガイドラインは政府機関等のサイバーセキュリティに関する統一的な枠組みで、各政府機関はこれを最低限のベースラインとして自組織の対策のルールを定めることになっている。

政府機関においては、 WEB サイトといったコンテンツを告知する場合は、利用者を確実に誘導できるように対策すること、また告知する URL の有効性を保つことが遵守事項となっている。同ガイドラインでは、短縮 URL のような民間事業者のサービスをアクセス経路に挟むことは、長期的に見て、遵守事項で求める安全性や有効性の継続的な確保が期待できないとの考えを示している。

---

[19] 出典：ITmedelia News『原因は「短縮 URL」か？ QR コードから不正サイトへ誘導される事例が相次ぐ オートバックスセブン、学習院大学も』
https://www.itmedia.co.jp/news/articles/2311/15/news194.html

[20] 出典：総務省『国民のためのサイバーセキュリティサイト』
https://www.soumu.go.jp/main_sosiki/cybersecurity/kokumin/enduser/enduser_security02_05.html

[21] 出典：内閣サイバーセキュリティセンター『府省庁対策基準策定のためのガイドライン』
https://www.nisc.go.jp/pdf/policy/general/guide26.pdf

[22] 出典：内閣サイバーセキュリティセンター『政府機関等の対策基準策定のためのガイドライン（令和 5 年度版）』
https://www.nisc.go.jp/pdf/policy/general/guider5.pdf

[23] 出典：内閣サイバーセキュリティセンター『政府機関等のサイバーセキュリティ対策のための統一基準群』
https://www.nisc.go.jp/policy/group/general/kijun.html

同ガイドラインにおける原則は、民間企業でもセキュリティ対策水準を上げるための参考とすることができる。

短縮 URL の危険性は他の国でも認知されており、イギリス政府も「使用すべきでない」との姿勢である[24]。また、米国連邦政府も、以前、政府公式の短縮 URL サービスである「Go.USA.gov」を提供していたが 2019 年に廃止している。廃止にあたって米国政府は、ユーザーにとっての短縮 URL の必要性の低さ、不正サイトへのリダイレクトに使われる可能性、実際にアクセスするサイトと異なるドメインを経由することによる混乱の懸念を理由に挙げている[25, 26]。

2.5. まとめ

現在でも短縮 URL の使用を見かけることは多いが、セキュリティ上様々な問題があることが指摘されており、ユーザーをサイトに誘導する際に使用することは避けたほうがよい。組織においては社内ルール等で短縮 URL サービスによる短縮を原則禁止とし、周知徹底することが望ましい。

WEB サイトへの誘導といった一般的に行われる行為でも、安全性や有効性を確保して提供できるか、使用するサービス等により、誘導する者にはユーザーに対する責任が問われる。短縮 URL サービスに起因した本件は、そのことを改めて認識させたといえる。

[24] 出典：Government Communication Service (UK)『Link shorteners: the long and short of why you shouldn't use them』 https://gcs.civilservice.gov.uk/blog/link-shorteners-the-long-and-short-of-why-you-shouldnt-use-them/

[25] 出典：Digital.gov『Gov URL Shorteners and How to Use Them』 https://digital.gov/2013/12/20/gov-url-shorteners-and-how-to-use-them/

[26] 出典：USAGov『Sunsetting Go.USA.gov: Frequently Asked Questions』 https://blog.usa.gov/sunsetting-go.usa.gov-frequently-asked-questions

3. マイクロソフトの開発ツール「VS Code」、設定漏れでパスワードが公開される危険性

3.1. 概要

マイクロソフト社の開発ツール「Visual Studio Code」（以下、VS Code と表記）でファイル転送を行う「SFTP プラグイン」の設定を誤り、SFTP 等の接続に使用するパスワードを含むファイルがアップロードされ、インターネット上に公開されている事例を多数確認した。また、この問題に関して、攻撃者についての調査を行ったところ、攻撃者達が管理不十分な VS Code の開発環境を狙った情報収集や攻撃を行っていることも明らかになった。

3.2. VS Code とは

VS Code はマイクロソフト社の提供する開発ツールである。C#や Java、HTML、JavaScript、Python 等、多くのプログラミング言語に対応している。アプリケーションや Web サイトの開発者が、プログラミングのコードを記述するために利用している。

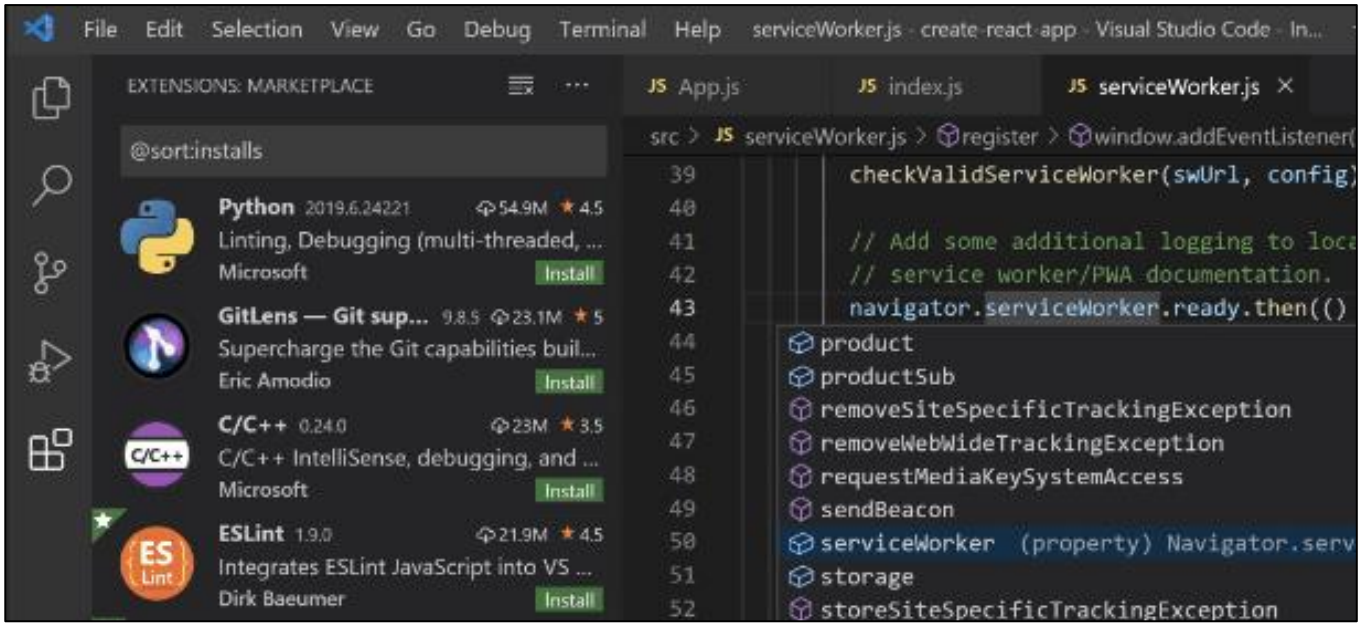


図 12 VS Code の画面例[27]

【SFTP プラグイン】

Web サイトを公開するには、Web サイトのコードを記述し、そのコードを保存したファイルを Web サーバーへ転送する必要がある。VS Code にはコードを記述する機能はあるが、ファイルを転送するには別のソフトウェアを利用する必要がある。そこで VS Code のプラグイン「SFTP」（以下、SFTP プラグイン）を導入すると、VS Code 上で直接、ファイルを転送できるようになる。利便性が上がることから、多くの開発者がこのプラグインを利用している。

[27] 出典：Visual Studio Code『Code Editing. Redefined』
https://code.visualstudio.com/

【適切に設定されていない SFTP プラグインの問題点】

SFTP プラグインは、接続するサーバーの IP アドレスやユーザー名、パスワード等の情報を「.vscode/sftp.json」というファイルに平文で保存している。SFTP プラグインには、アップロードしないファイル／ディレクトリを除外するための設定がある。この設定において、「.vscode/sftp.json」を指定していない場合、ソースコードと共にサーバーに転送され、公開される恐れがある。このファイルを悪意のある第三者が閲覧して認証情報等を取得し、サーバーに接続すれば、Web サイトの改ざんや不正プログラムの設置等の攻撃を実行することが可能となる。また、ターゲット組織が同一のパスワードを他のサービスでも使い回している場合は、さらに広範囲の被害へとつながる恐れがある。

```
{
    "name": "Profile Name",
    "host": "name_of_remote_host",
    "protocol": "ftp",
    "port": 21,
    "secure": true,
    "username": "username",
    "remotePath": "/public_html/project", // <--- This is the pat
    "password": "password",
    "uploadOnSave": false
}
```

図 13 .vscode/sftp.json の記述例[28]（ユーザー名やパスワードも平文で保存）

実際に、この設定漏れによってインターネット上に公開されてしまったと考えられる「.vscode/sftp.json」ファイルが多数存在することを確認した。

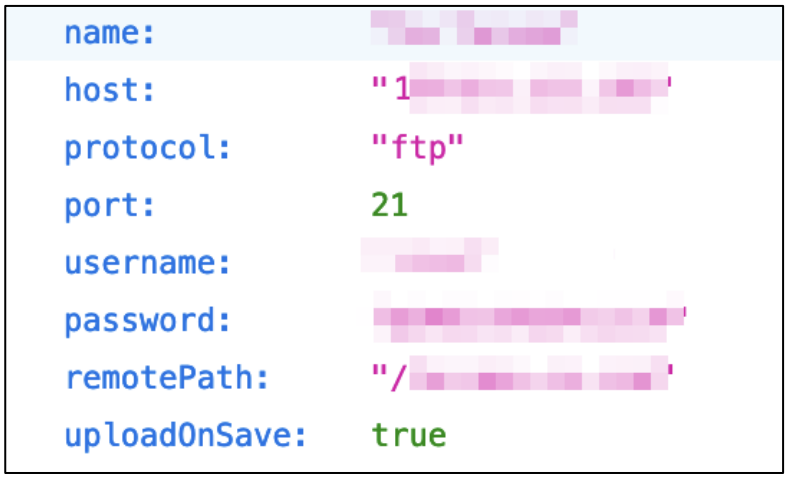


図 14 公開状態の「.vscode/sftp.json」
ユーザー名、パスワードを含むすべての情報が平文であった

[28] 出典：Visual Studio Marketplace『SFTP』
https://marketplace.visualstudio.com/items?itemName=Natizyskunk.sftp

【レンタルサーバー会社による注意喚起】

9 月、レンタルサーバーサービスの「ロリポップ!」は、利用者に向け、SFTP プラグインの除外設定を確認するよう促す注意喚起を発表した[29]。

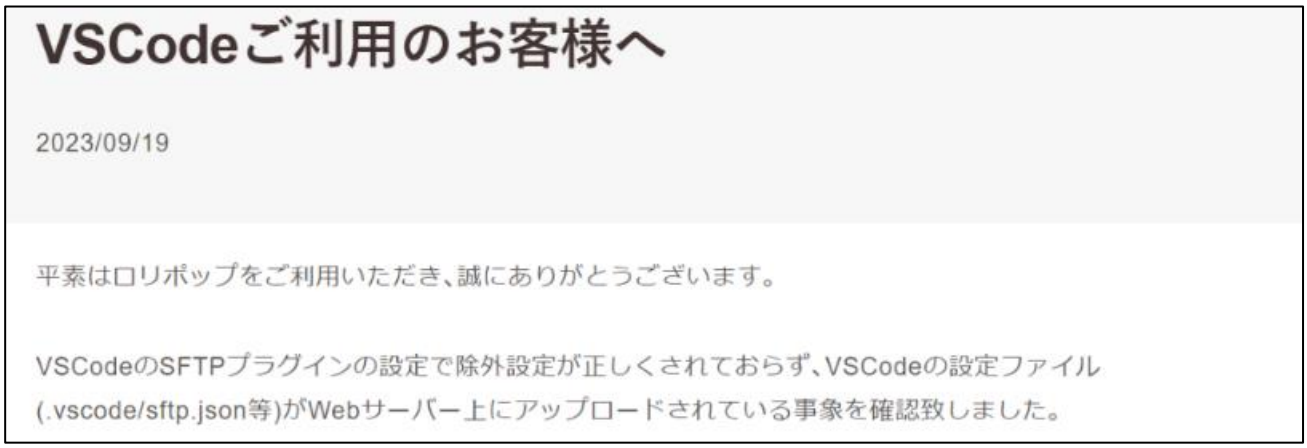


図 15 ロリポップ!による注意喚起

3.3. 攻撃者の動向

攻撃者もこのような SFTP プラグインの問題に関心を持っていることが確認できる。

【情報収集ツールの販売】

Telegram のハッキングに関するチャンネルでは、VS Code SFTP プラグイン情報を収集する攻撃ツールが販売されている。攻撃者は、このようなツールを利用することで、インターネット上に誤って公開されているパスワード情報を効率的に収集し、攻撃に利用していると考えられる。

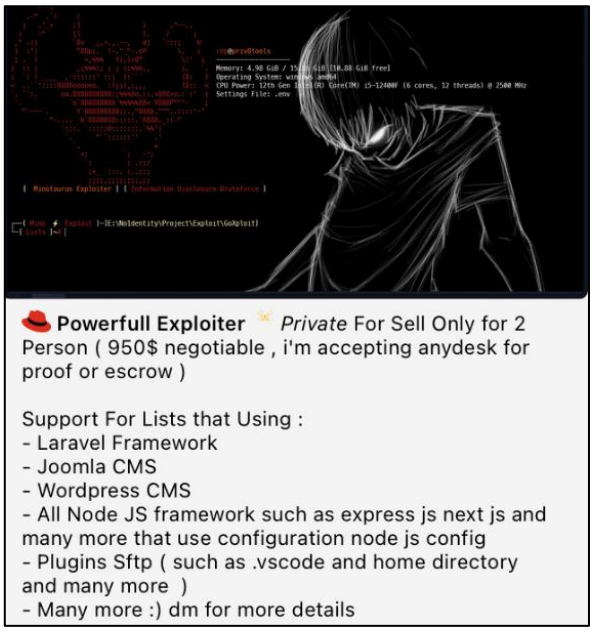


図 16 SFTP プラグインの情報を収集するツールを販売する Telegram の投稿

[29] 出典：ロリポップ！レンタルサーバー『VSCode ご利用のお客様へ』
https://lolipop.jp/info/news/7618/

【攻撃事例】

あるロシア系ハッカーフォーラムに、顧客の Web サーバーが攻撃を受け仮想通貨のコインマイナーが仕掛けられたが、どこに穴があったか調べたいと相談する投稿があった。フォーラムの参加者達の間では、攻撃者はどのようにハッキングしたのかという議論になった。結局、VS Code SFTP プラグインで、前述の除外設定をしていなかったためパスワードが漏洩したことがわかった。

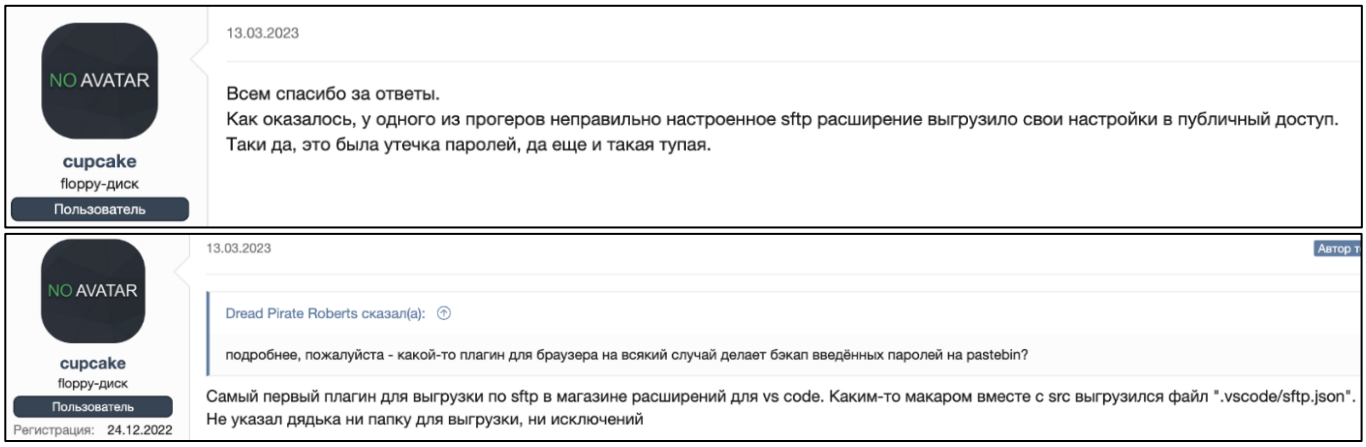


図 17 ハッカーフォーラムの投稿

「（抄訳）SFTP プラグインを導入して、ソースコードと共に .vscode/sftp.json がアップロードされていた。これはパスワードの漏洩を意味している。非常に愚かなことだった。除外の設定をしていなかった。」

3.4. まとめ

VS Code の SFTP プラグインの設定漏れにより、パスワードを含むファイルが公開され、さらに、それを狙った攻撃者の活動が確認できた。管理の目が届きにくい開発ツールのプラグインの設定漏れが原因であるが、攻撃者達はこのような細かなミスまでしたたかに狙っている。安全な設定を確実に行うよう注意していても、ミスを完全に防ぐことは困難である。このようなミスを検知できる仕組みやシステムを用意し、多重にチェックできる体制を整えたい。

以上

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