HITACHI

Hitachi Systems Security Journal

VOL.11

株式会社 日立システムズ

Hitachi Systems Security Journal VOL.11

TABLE OF CONTENTS

●はじめに

本文書は、株式会社日立システムズ の公開資料です。バックナンバーは以下の Web サイトで確認できます。
https://www.hitachi-systems.com/report/specialist/index.html

ATMを遠隔操作するマルウェア「NGATE」進化するAndroidマルウェアの脅威を分析

ルーカス ステファンコ インタビュー

2024 年 11 月、CODE BLUE 2024 にて、ESET のルーカス・ステファンコ氏による Android マルウェア「NGate」に関する講演が行われた。このマルウェアは Web アプリとしてユーザーにインストールされ、フィッシングと組み合わせることで、攻撃者が遠隔から ATM を操作できるという新たな脅威である。インタビューでは、NGate の概要や被害状況、そして今後想定されるリスクなどについて話を伺った。

取材・文 = 吉澤 亨史／通訳 = エル・ケンタロウ／撮影 = 卯月 梨沙／編集 = 斉藤 健一

「NGATE」
遠隔から ATM を操作する、その手口とは？

吉澤（以下、Y）：本日は、とても興味深いセッションをありがとうございました。さっそくですが、今回の講演テーマである「NGATE」についてお話をうかがっていきたいと思います。まず、NGATE はどのような経緯で発見されたのか、教えていただけますか。

ルーカス・ステファンコ（以下、L）：最初に NGATE を発見したのは、ヤコブでした。2023 年 11 月のことです。

Y 今回、一緒に発表される予定だった ESET の方ですね。

L そうです。彼は今回来日できませんでしたが、ESET で顧客のブランドに対する脅威を監視するインテリジェンス・サービスの部署に所属していました。顧客は主に金融機関で、彼は検知された脅威に関する報告書の作成と報告を行うチームの一員でした。また、被害を受けた組織からも情報を提供していただき、それらを踏まえてより包括的なレポートを作成していました。そうした情報をつなぎ合わせていく中で、点と点が線となり、NGATE マルウェアの全体像が徐々に明らかになってきたのです。

Y NGATE による実際の被害は、どの程度の規模だったのでしょうか。

L ESET として正式な数字は開示していないため、具体的な件数はお話しできませんが、おそらく中規模程度の被害があったと考えています。これは、NGATE の最後のキャンペーンだけでなく、それ以前のすべての攻撃を含めた被害件数です。確実な数字としては、チェコ警察が被害件数 3 件、被害総額 6000 ユーロ（約 10 万円）と発表しています。実際には、さらに多くの被害があった可能性もありますが、証拠が残っていないため確認できていません。

Y 攻撃の流れとしては、まずユーザーのスマートフォンに、PWA（Progressive Web Apps）を含む偽のテキストメッセージが送られる。つまり、フィッシングから始まるということでしたね。

L PWA とは、アプリストアを介さずに Web サイトや Web アプリをデバイスにインストールできる仕組みです。ただし、iOS では基本的に App Store を経由しないとインストールできないため、正規のアプリストア以外からもインストールが可能な Android デバイスが主な攻撃対象となります。ユーザーが偽のテキストメッセージ内のリンクをクリックしてしまうと、Web アプリがインストールされ、そこから認証情報が盗まれてしまうのです。

Y ユーザーが Web アプリをインストールしたことを攻撃者が検知すると、今度は銀行の行員を装ってユーザーに電話をかけてくる、という流れでした。

L「インシデントが発生したため、あなたの銀行口座を保護する必要があります」と伝えるわけです。この電話は、最初のフィッシングテキストメッセージと連動しています。その後、攻撃者は PIN

●ルーカス・ステファンコ（Lukas Stefanko）

エンジニアリングの強いバックグラウンドを持ち、Android マルウェアの研究とセキュリティに注力している経験豊富なリサーチャー。現在は、ESET でマルウェア・アナリストを務める。13 年以上のマルウェア研究の経験を持ち、Android マルウェアの検出メカニズムの改善に取り組んでいる。近年では、モバイルの脅威やアプリの脆弱性に対する一般の認識を高めるために大きな進展を遂げている。CODE BLUE をはじめ、RSA、Virus Bulletin、Confidence、DefCamp、BountyCon、AVAR、CARO Workshop、Infoshare、Ekoparty、Copenhagen CyberCrime など、数々のセキュリティカンファレンスに登壇している。

CODE BLUE 2024 での登壇の様子。公式サイトでは講演の動画とスライドが公開されている
https://archive.codeblue.jp/2024/results/results/#result-22

コードの変更を促し、さらに「確認が必要だ」として、もう一度テキストメッセージを送信してきます。

Y そのメッセージ内のリンクをクリックしてしまうと、NGATE がインストールされてしまうわけですね。アプリが起動すると、銀行のフィッシングサイトが表示され、ユーザーはログインを求められます。さらに、PIN 変更のためとして現在の PIN コードを入力させられ、それらの情報が盗まれてしまう、という仕組みになっていました。

L 攻撃者は、同時に NFC トラフィックも取得することができます。ただし、NGATE はネイティブアプリであるため、通常であれば Web ブラウザーが警告を表示しますし、出所不明のアプリであることから、インストールにはユーザーの明示的な許可が必要です。こうしたハードルをすべてクリアして NGATE がインストールされると、攻撃者はユーザーの認証情報を入手できるようになります。さらに、NGATE はユーザーに対して追加の認証を求める機能も備えています。

Y ユーザーのスマートフォンに非接触型のカード情報が登録されていれば、それを使って認証が行われます。その際、NGATE による NFC リレーアタックによって、攻撃者は自分のスマートフォンを介して ATM を遠隔操作できるようになる、ということですね。

L NGATE の大きな特徴は、2 つの C&C サーバー（コマンド＆コントロールサーバー）を使っている点です。一方は、NFC リレーアタックやデータの取得・保存を担うもので、もう一方は JavaScript ベースのインターフェイスを備えており、攻撃者が Web ブラウザー経由でフィッシングサイトからさまざまな操作を行えるようになっています。このインターフェイスを通じて、デバイス情報の取得や NFC 機能の有効化といった制御が可能になるのです。

Y NGATE は単体のマルウェアというよりも、複数の手法を組み合わせた一連の攻撃だというお話でした。

L NGATE マルウェア自体は新しいものですが、その攻撃手法はソーシャルエンジニアリング、フィッシング、そして NFC リレー攻撃といった、古くからある技術の組み合わせによって成り立っています。また、仮に NGATE による攻撃が失敗したとしても、攻撃者はフィッシングを通じて銀行の認証情報をすでに入手しているため、不正送金を行うことは可能なのです。

Y 複数の警告やユーザーの許可が必要であっても、実際には引っかかってしまうケースが少なくないのでしょうか。

L 特に、PWA や WebAPK といった新しい技術を悪用した初の攻撃が、先月ポーランドの CIRT で確認されました。こうした状況を踏まえると、従来のフィッシング攻撃では、どこかの段階でユーザーが違和感を覚えるポイントがありました。しかし、PWA や WebAPK を利用した新たな攻撃では、画面に何も警告が表示されず、ユーザーが違和感を持たないままアプリがインストールされてしまう。そういった手口が今後現れる可能性があります。

従来の手口がフィッシングと融合して新たな脅威に

Y そもそも、自分のスマートフォンに入っているアプリをきちんと整理できていない人は、私も含めて多いのではないでしょうか。そうした状況では、たとえ何か怪しさを感じたとしても、そのまま放置してしまいそうです。また、先ほどのお話

にあった「古くからある技術の組み合わせで構成されている」という点も、とても興味深いと感じました。

L 私は日々、さまざまな攻撃情報に目を通していますが、その中で新しい攻撃手法を見かけたとしても、それが本当に新しいものかどうか、自分だけで判断するのは難しいこともあります。ただ、やはり以前からある攻撃手法が繰り返し使われているケースは多いと感じます。

Y NGATE 以外にも、最近確認された新たな攻撃手法はありますか？

L しいて挙げるとすれば、何らかの形で悪意のあるコードがユーザーの端末上で実行され、その結果として NFT などの非暗号化資産が、ウォレットや取引所（Exchange）を経由して流出してしまうケースを、最近よく見かけるようになりました。銀行のアプリなどでアカウントが乗っ取られ、不正送金されるケースも、同様の手口で行われることがあります。

Y 銀行などの金融系アプリが乗っ取られてしまうと、金融機関側からはユーザーによる正規の操作にしか見えないでしょうね。例えば、過去の取引履歴とかけ離れた大金が海外に送金されるようなケースであれば、異常として検知される可能性はあると思います。しかし、それ以外の場合は、詐欺や犯罪行為として検知するのは難しそうですね。

L ユーザーが気づかないうちに、何度も送金されてしまう事例は少なくありません。

Y 講演の映像では、犯人のスマートフォンと被害者のスマートフォンを並べて置いていましたが、双方の距離には物理的な制限があるのでしょうか？

L 実際の通信はインターネット経由で行われるため、端末やサーバーのどちらかが地球の反対側にあっても、特に問題はありません。講演では、被害の状況をわかりやすく伝えるために、あえてスマートフォンを隣同士に並べて配置しました。

Y なるほど、わかりやすくするためだったのですね。ということは、リモートからでも被害を受ける可能性があるということですね。CODE BLUE 事務局による講演前のインタビュー※では、「ATM のそばをウロウロしていたため、周囲から不審な目で見られた」とありましたが、それは頻繁に検証を行っていたということでしょうか？

L 攻撃に再現性があるかどうかを確認するため、ダウンタウンの比較的人通りの多い街中を歩きながら、5 台ほどの ATM で実験を行っていました。とはいえ、「実験中に誰かに撮影されて警察に通報されたらどうしよう…」という不安もありました。もしそこで捕まってしまったら、私が「悪者」になってしまいますからね。

Y チェコのダウンタウンですか？

L スロバキアです。私はスロバキア出身なので、地元の ATM を使って実験を行いました。

Y 日本でも一時期、車のキーの電波を中継して車を盗むリレーアタックが流行しましたが、NGATE の場合はインターネット経由で中継されるということですね。

L 車のキーに対する攻撃は、電波が届く範囲という物理的な制約がありますが、今回の攻撃はインターネット経由で行われるため、距離は一切関係ありません。

Y ただし、そのような攻撃を行うには、事前にフィッシングによってカード情報などを入手しておく必要があるということですね。

L 現金を引き出すには PIN コードが必要なので、まずはそれを入手するためにフィッシングを仕掛ける、というわけです。

Y 犯罪者の逮捕以降、現在のところ NGATE の活動は確認されていないとのことでしたが、何らかの兆候もまったく見られていない状況でしょうか？

L 2024 年 3 月以降、NGATE マルウェアの活動は確認されていません。ちょうどその時期に犯罪者が逮捕されており、その逮捕が活動停止のきっかけになった可能性は高いと考えています。

スマートフォンへの攻撃は今後も続く

Y 今回のこの事例は、今後どのように発展していく可能性があるとお考えですか？

※ **講演関連資料** https://note.com/code_blue/n/ncfcdeb7551d3

NGATE は、遠隔から ATM を操作するという特徴を持っているが、その実態はソーシャルエンジニアリングやフィッシング、NFC リレーといった従来の攻撃を組み合わせたものだと、ステファンコ氏は語る

L 今後も、同様の攻撃は継続して発生すると考えています。というのも、この攻撃は非常にシンプルでありながら、2024 年になっても依然として効果を発揮しているからです。これは驚くべきことであり、同時に非常に不安でもあります。さらに、実際に使用されたツールのソースコードは GitHub 上で公開されており、現在も更新が続けられています。私たちは定量的な監視を行っていますが、このソースコードをベースに新たな疑わしい Android アプリが登場する可能性は十分にあると見ています。

Y 具体的には、どのような攻撃が想定されるのでしょうか？

L 考えられる攻撃パターンは大きく 2 通りあります。1 つは、リモートマネジメントソフトを経由して、攻撃者がスマートフォンをリモート端末として実際に操作するケースです。もう 1 つは、さらに厄介な完全自動化型の攻撃です。攻撃者はアプリの動作を把握しているため、送金処理を自動化することが可能です。この場合、アプリを起動し、自動的に送金を実行し、完了後にアプリを閉じるという一連の操作が、わずか数秒で完了してしまいます。こうした自動化された攻撃は、最近になって実際に見かけるようになっています。

Y そのようなアプリは、例えば iOS であればサンドボックス機能があるため、権限のない不正な動作を行うのは難しいと思います。一方で、Android であれば、そうした動作が可能になる余地があるかもしれませんね。

L iOS でも Android でも、基本的に OS はサンドボックス化されており、この点に大きな違いはありません。ではなぜ、こうした攻撃が可能になるのかというと、Android では悪意のあるマルウェアが正規の機能、例えば操作が困難なユーザー向けに用意されたアクセシビリティ機能を悪用するからです。これらの機能には、他のアプリへのアクセス権限があり、攻撃者はその特性を巧妙に利用しています。

Y 現在のスマートフォンは、クレジットカードの代わりとして使えるほか、さまざまな決済機能も備えています。そのため、スマートフォンが乗っ取られた場合のリスクは非常に大きいですね。

L スマートフォンが日常的に使われ、誰もが無意識にテーブルの上などに置いていることを考えると、攻撃の可能性は非常に高いと言えます。もちろん、ユーザーが悪意のあるアプリをインストールしてしまうことが前提条件にはなりますが、その条件さえクリアしてしまえば、リプレイ攻撃を何度でも繰り返すことが可能になります。

セキュリティエンジニアとしてのこれまでとこれから

Y ルーカスさんがセキュリティの分野に取り組むようになったきっかけは、どのようなことだったのでしょうか？

L もともと、セキュリティの観点から「物事がどのように動いているのか」に強い興味がありました。最初はペネトレーションテストからキャリアをスタートさせ、その後、本来取り組みたかったリバースエンジニアリングにも関わるようになりました。それが、私にとってサイバーセキュリティの世界に足を踏み入れる最初のステップでした。その後は、脅威インテリジェンスなどの分野にも関わるようになっていきました。

Y 現在は ESET でマルウェア解析や Android のセキュリティに取り組んでいらっしゃいますが、その分野に関心を持ち、研究しようと思われたきっ

かけは何だったのでしょうか？

L 最初は、Windows デスクトップを狙うマルウェアの解析やリバースエンジニアリングに仕事として取り組んでいました。その後の約 2 年間は、モバイル、特に Android アプリの開発に専念していました。しかし、今から約 11 年前に Android マルウェアが急増し始めたことをきっかけに、「これまでのリバースエンジニアリングのスキルがモバイル分野でも活かせる」と感じ、以降はモバイルを中心に活動するようになりました。

Y 現在は主に Android のマルウェアを研究されているとのことですが、今後はどのようなテーマや分野の研究に取り組んでいきたいとお考えですか？

L 今後も引き続き、Android マルウェアの研究に取り組んでいきたいと考えています。その中には、犯罪行為に関わるものはもちろん、APT のようなサイバースパイ活動に近いものも含まれます。これまで Android とマルウェアの研究に長く携わってきて、とても面白く、やりがいを感じてきましたし、これからもこの分野を深めていきたいと思っています。

Y IoT 機器にも Android OS が搭載されるケースが増えていますよね。例えば、多くのスマートテレビでは Android が動作していますが、実際にはセキュリティアップデートやシステムアップデートがきちんと行われているケースは、まだまだ少ないのが現状です。

L そうした機器は、ボットネットの格好の標的になります。また、スマートライトのような身近な家電製品も、Android で動作するものが増えており、その多くはモバイルアプリとの連携を前提としています。今後、こうしたデバイスはそれぞれ独自に進化していくと思います。IoT についてももっと深く調べたいと思っていますが、どうしても時間には限りがあります。それでも今後も、モバイルと Android に関する脅威の体系を引き続き追いかけていきたいと考えています。

Y 最後に、CODE BLUE と日本についての印象をぜひお聞かせください。

L 今回が初めての CODE BLUE、そして初めての日本でした。これほど多くの人が集まる大規模なカンファレンスだとは思っていなかったので、とても感動しましたし、内容も非常に興味深く充実していました。個人的には、もう少しモバイルに関する研究発表が増えると嬉しいですが、全体としてとても貴重な経験になりました。

Y お疲れのところ、貴重なお話をありがとうございました。

社会のさまざまな動向を把握し、リスクの変化に対応したセキュリティ体制を構築

Hitachi Systems CSI（Cyber Security Intelligence）Watch 2025.06

文＝日立システムズ

パスワードからの脱却に向けた認証基盤の段階的移行

【概要】：近年、オンラインサービスの利用増加に伴い、認証情報の漏えいが深刻化している。多くのユーザーがパスワードを使い回すため、漏えい時には複数サイトでの変更が必要となる。一部のWebブラウザーは再設定を促す機能を実装するが、根本的な解決にはならない。パスワード依存の認証では被害を防げないため、パスワードレス認証が注目されている。本稿では、その課題と対策としてのパスワードレス認証への移行を解説する。

【内容】：Google Chromeなど一部のWebブラウザーでは、認証情報の漏えいを検知すると、ユーザーがワンクリックで新しいパスワードを再設定できる機能の実装が進められている。この機能は、漏えいによるセキュリティインシデントを防ぐ対策として期待されている。非営利団体W3C（World Wide Web Consortium）の「A Well-Known URL for Changing Passwords」仕様に基づき、Webサイト直下にパスワード変更ページへの導線を設置することが定められている。

この仕様が注目される背景には、漏えいしたパスワードリストを用いた攻撃の常態化や、同一パスワードを複数サイトで使い回すユーザーの多さがある。漏えいに早期に気づいても、同じパスワードを使うすべてのサービスでの変更が必要で、手間や漏れが被害拡大につながっていた。このように、従来どおりユーザー任せで変更を促すだけでは限界があり、2016年ごろからパスワードの自動変更が議論されてきた。

仕様自体はシンプルだが、Webサイト運用者には注意点がある。設計面では、パスワード変更ページに多要素認証やCAPTCHAなど人の操作が必要な要素があると自動化が難しくなるため、新たに設計するか既存の設計を見直す必要がある。運用面では、自動化によるアクセス集中に備えた負荷対策が重要だ。例えば、SMSによる多要素認証は送信ごとの従量課金でコスト増のリスクがある。これを防ぐには、送信数制限やアラート整備など、コスト管理と通知の仕組みを整えておく必要がある。また、この仕組みは一時的な緩和策にすぎない。パスワードに依存する限り、漏えいやフィッシングのリスクは避けられず、根本的な解決にはパスキーのようなパスワードレス認証への移行が求められる。

パスキーは、端末内に保存された秘密鍵で署名し、Webサーバーには公開鍵のみを保持させる仕組みである。認証情報が直接やりとりされないため、リスクを原理的に排除できる。ユーザーは生体認証や端末のPINコードで認証を完了でき、利便性にも優れる。米国NISTは公開鍵認証を強固な手段として推奨しており、米政府や金融機関での導入が進んでいる。日本でもデジタル庁が本人確認手法ガイドラインの見直しの中で、パスワードレス認証の活用を検討するなど、制度面での後押しが始まっている。

一方、パスキーにも課題がある。端末紛失時の鍵の復旧、企業での鍵のライフサイクル管理、レガシー環境や一部Webブラウザーの未対応、生体情報の法的扱いなどが移行の障壁となる。こうした現実を踏まえると、自組織のロードマップでは、高リスク領域から優先的にパスキーを導入し、他の領域には自動パスワード変更を適用してリスクを緩和する方針が現実的だ。自動パスワード変更を過渡的な防御策としつつ、将来的なパスワードレス環境への移行を目指すことが重要である。そのためには、自動化の恩恵とコストを正しく見積もり、パスワード脱却を見据えた移行計画を検討する必要がある。

［情報源］https://thehackernews.com/2025/05/google-chrome-can-now-auto-change.html

セキュリティツールを実践的に紹介する連載企画

Let's try Web サイト簡易調査

2. ブラックリスト / SandBox 利用編

文＝日立システムズ

1. はじめに

本稿は、各種セキュリティツールなどを実践的に紹介する連載企画です。前号より「Web サイト簡易調査」と題して、フィッシングサイト、改ざんされたサイトなど、直接アクセスすることが危険な Web サイトの調査方法について紹介します（下図参照）。
「Web サイト簡易調査」は、以下の 2 部により構成されます。

1. **Web アーカイブ利用編**
   過去にキャプチャーされた Web サイトの情報を活用して、Web サイトの危険性や類似のコンテンツなどを調査します。
2. **ブラックリスト / SandBox 編**
   入力した URL の Web サイトに潜む危険性を確認するサービスを利用して Web サイトを調査します。

前号では、Web アーカイブの 1 つである urlscan.io を用いた調査を紹介しました。今回は VirusTotal、Gred を用いた調査を紹介します。

なお、本稿の安全性には留意していますが、安全を保証するものではありません。OA 端末で実施するのではなく、分離された回線内および機器を利用することを推奨します。

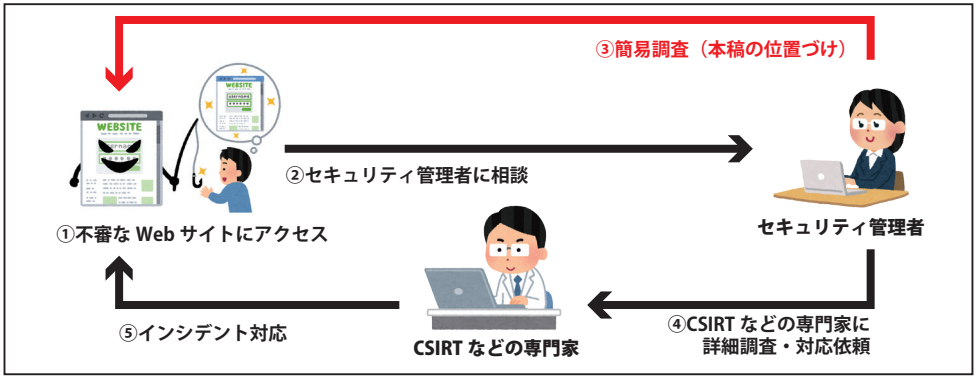


図 不審な Web サイトに対する簡易調査

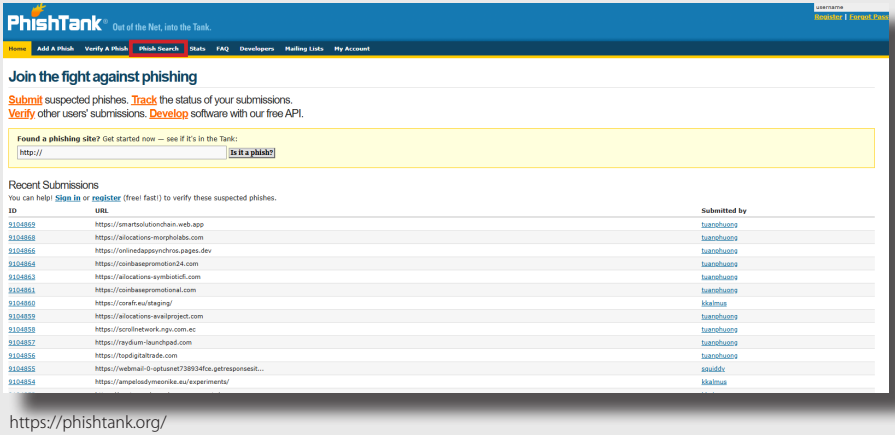
2. 事前準備

今回は、過去に確認されているフィッシングサイトの内容を確認します。フィッシングサイトは、悪意ある Web サイトです。安全な調査環境を準備して、調査をすべきです。調査環境例については、本誌 Vol. 63「Let's try OSINT 体験 1. 環境準備編」でも紹介しています。そちらも参照してください。

3. 悪性 URL の準備

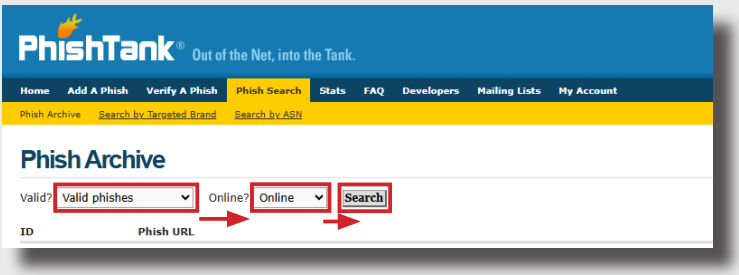
3.1 フィッシングサイト URL の準備

調査にあたって、最新の悪性ドメイン（URL）を確認していきます。
フィッシングサイト URL を得る方法はいくつかありますが、今回は「PhishTank」を利用します。
「PhishTank」は、誰でもフィッシングデータを送信、検証、追跡、共有できる無料のコミュニティサイトです。
以下の URL より、「PhishTank」にアクセスしてください。
アクセスできましたら、上部の「Phish Search」をクリックしてください。

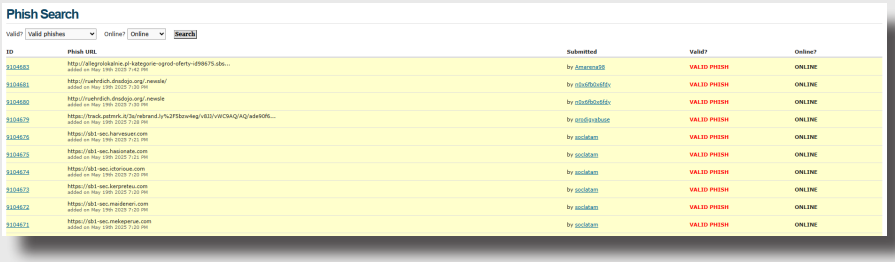


https://phishtank.org/

次に、Valid? を「Valid phishes」、Online? を「Online」を選択し、Search ボタンを押下してください。



「Valid phishes」とは、有効なフィッシングサイトと確認されているもので、「Online」とは現在もフィッシングサイトが稼働中である (と推定される) 状態を示します。
検索の結果、下の図のとおり、多くのフィッシングサイトの情報を得ることができました。



上記、検索結果より、URL をいくつかメモしてください。最新の URL を対象とするため、本稿では URL を明記していません。

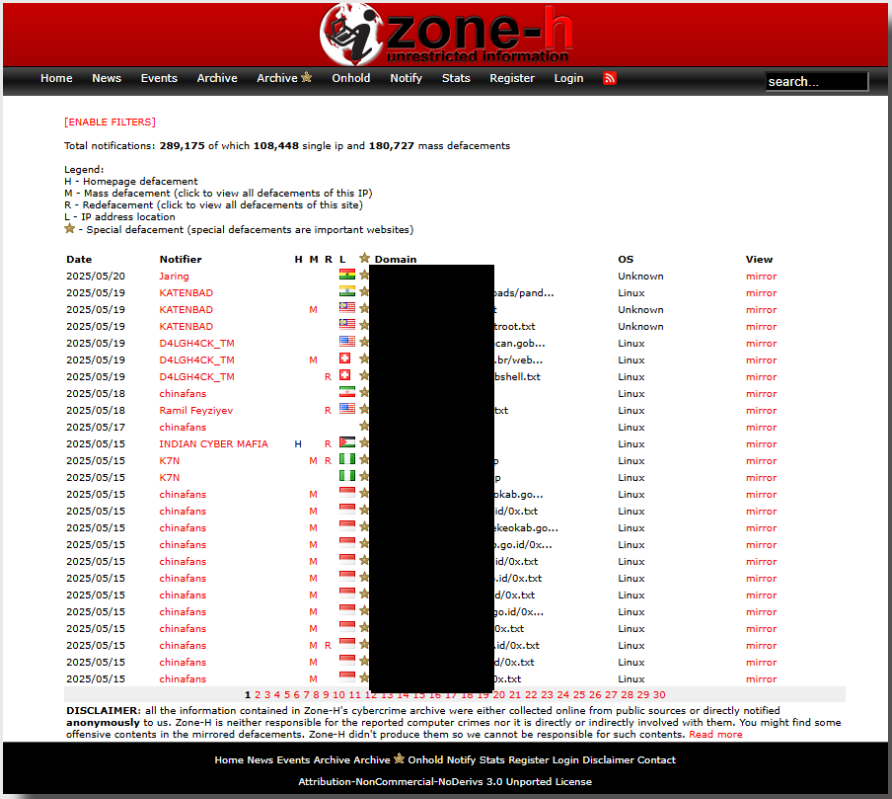
なお、PhishTank では、「Search by Tardgeted Brand」を選択することで、「SMBC」や「Rakuten」など、日本国内においても著名なブランドを騙ったフィッシングサイトも検索可能です。

3.2 改ざん Web サイト URL の準備

改ざんサイト URL を得る方法はいくつかありますが、今回は「Zone-h」を利用します。「Zone-H」は、セキュリティニュースサイトです。改ざんのアーカイブ情報も保持しています。
次ページの URL より、「Zone-H」にアクセスし、URL をいくつかメモしてください。最新の URL を対象とするため、本稿では URL を明記していません。

なお、Zone-H のメニューには、「Archive」のほかに、「Archive ★」と★が付されたメニューがあります。、これは、特別なサイトと位置付けられています。内容を確認すると、gov の文字列が確認できるなど、重要な Web サイトに関する情報がアーカイブされていると考えられます。

https://www.zone-h.org/archive/special=1



https://www.zone-h.org/archive

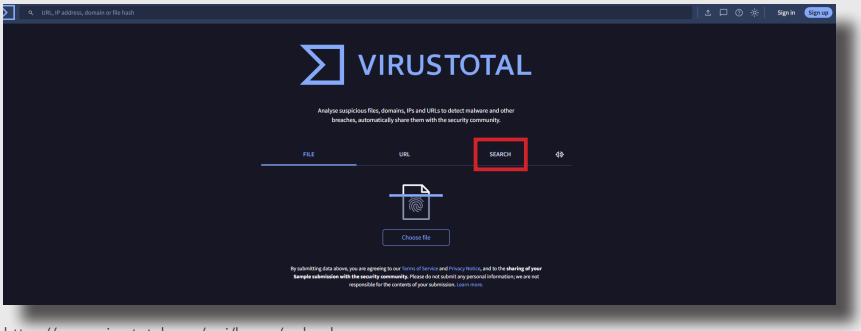
4. ブラックリストなどを使った調査

4.1 Virus Total を使った調査

VirusTotal は、「Google Cloud Security」が運営するファイルや Web サイトのマルウェア検査を行うサービスです。複数のウイルス対策ソフト製品で当該マルウェアの検出状況などを確認できます。

今回は、前項でメモしたいくつかの URL を VirusTotal を使って調査します。

次ページの URL より、VirusTotal にアクセスしてください。

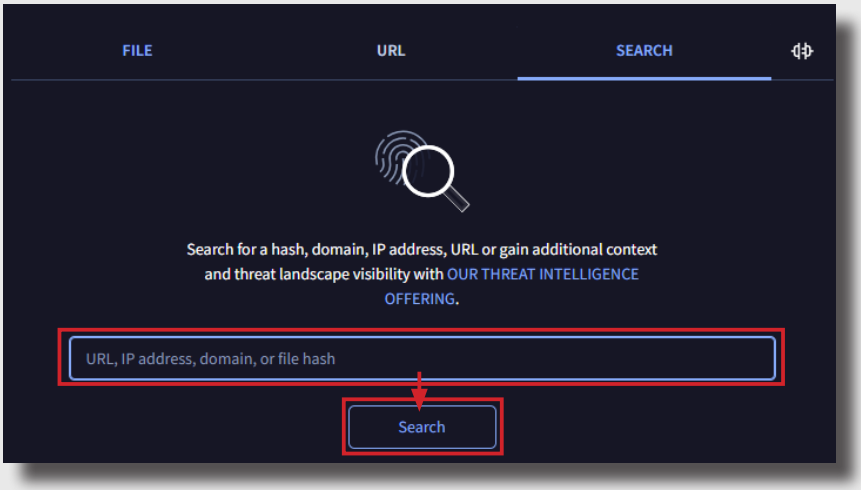


https://www.virustotal.com/gui/home/upload

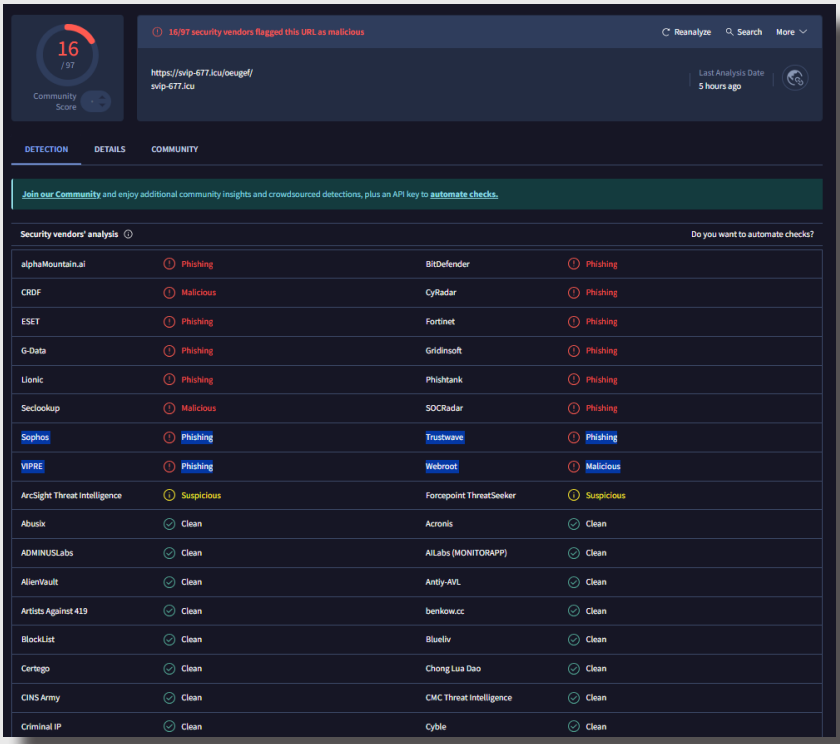
アクセスしたら、「SEARCH」をクリックします。

4.2 Virus Total を使ったフィッシングサイトの調査

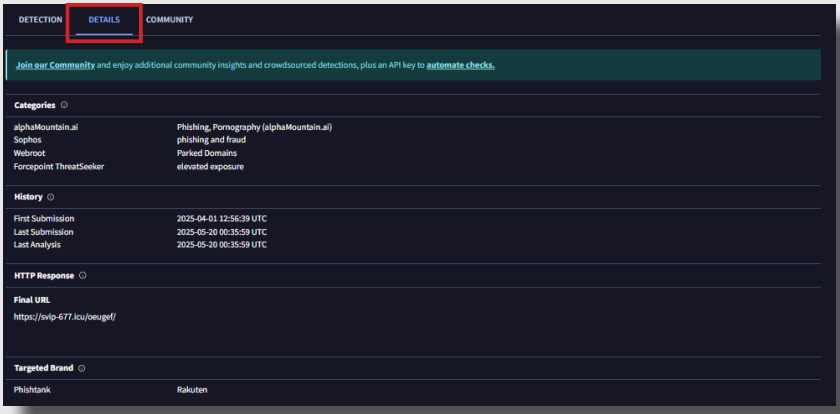
検索窓に前項でメモしたフィッシングサイト URL を入力し「Search ボタン」を押下します。



検索した結果、例えば次のような検索結果を得ることができます（次ページの図を参照）。なお、結果は調査ＵＲＬによって異なります。
図の例では、97 セキュリティベンダー中、16 のセキュリティベンダーが提供する製品が調査 URL を悪性と判断していることが確認できます。



次に、DETAIL タブを確認します。このページでは、各ベンダーの検出したカテゴリや、どのブランドをターゲットにしたフィッシングサイトであるかなどを確認できます。

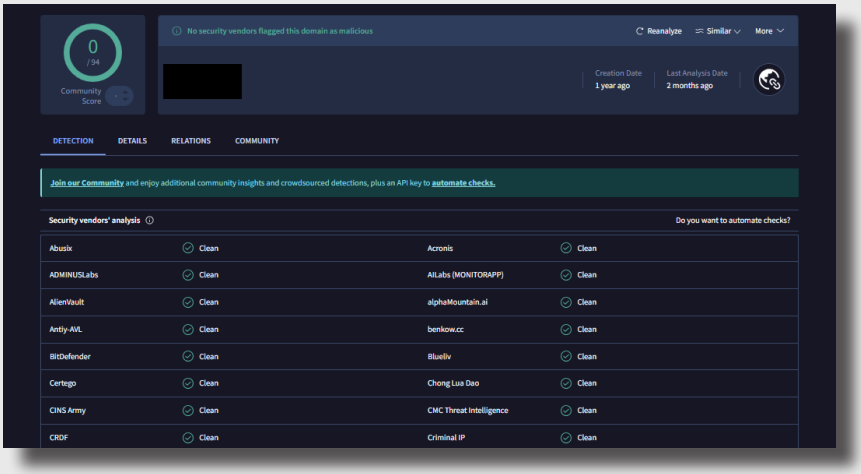


なお、悪性サイトと判断されない場合は、メモした他の URL で試行してください。

4.3 Virus Total を使った改ざん Web サイトの調査

前項でメモした改ざん Web サイト URL は、絶対パスとなります。「VirusTotal」で検索する際は、ドメインで検索が必要なため、ドメインだけ抽出し検索します。

ただし、今回、ほとんどの場合で、悪性ドメインとは判定されないはずです。これは、改ざんされた Web サイトは、あくまでも被害者であり、悪性でないドメインであるためと考えらるからです。



4.4「Gred」を使った調査

「Gred」は、当社（日立システムズ、旧セキュアブレイン社）が提供する Web サイトチェックツールです。

以下の URL より、「Gred」にアクセスしてください

https://check.gred.jp/

4.5「Gred」を使ったフィッシングサイトの調査

検索窓に前項でメモしたフィッシングサイト URL を入力し、「CHECK ボタン」を押下してください。

検索の結果、次のとおり、今回筆者が調査した URL は、フィッシングサイトと判定し、警告が出ていることが確認できます。

「Gred」は、リアルタイムでサイトを確認しにいくため、調査時点で当該フィッシングサイトが存在しない場合は、判断ができない場合があります。この場合、メモした他の URL を施行してください。

なお、あくまでのフィッシングサイトの特徴点などから判断していることから、必ず正確な判断ができるわけではない点にも注意が必要です。

4.6「Gred」を使った改ざん Web サイトの調査

検索窓に前項でメモした改ざん Web サイト URL を入力し、「CHECK ボタン」を押下してください。検索の結果は次ページの図のとおりです。今回筆者が調査した URL は、改ざんされていると判定し、警告が出ていることが確認できます。

なお、今回は、改ざんされているコンテンツが自明でした。改ざんされているかわからないが、調査したい場合は、トップページを指定の上、次の通り、「リンク先のページもチェックする」にチェックを入れることで、リンクが張られている範囲で改ざんを調査することができます。

4. おわりに

「Web サイト簡易調査 ブラックリスト、SandBox 利用編 」では、フィッシングサイト、改ざんされたサイトなど、直接アクセスすることが危険な Web サイトについて、VirusTotal や Gred を用いて、フィッシングサイト、改ざんサイトを例に調査手法を確認しました。

Hitachi Systems Security Journal

株式会社 日立システムズ　本社：〒141-8672　東京都品川区大崎 1-2-1　www.hitachi-systems.com

お問い合わせは

Printed in Japan