サイバーセキュリティレポート

2024.11

NTT セキュリティ・ジャパン株式会社
プロフェッショナルサービス部　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 2024 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『Docusign の API 悪用による新たなフィッシング攻撃』

- 11 月 5 日、オンライン電子署名サービス Docusign の API を悪用したフィッシング攻撃が急増しているとして、サイバーセキュリティ企業 Wallarm がブログ記事で警告した。
- 攻撃者は、Docusign の有料プランを契約し、正規のユーザーアカウントとして有名ブランドに巧妙に似せた請求書を複数の宛先に大量送信し、本物の請求書と誤認した受信者に支払いをさせることで金銭を得ていた。
- Docusign 以外の正規プラットフォームでも同様の攻撃が実行される恐れがあるため、API を介したメッセージを受信する側の組織では、プラットフォームが悪用されることを念頭に置いて、社内での承認プロセスをより厳格化する等の対策が求められる。

第 2 章『北朝鮮ハッカー Jumpy Pisces が金銭目的でランサムウェア攻撃に関与』

- Play ランサムウェアの被害調査から、同グループと北朝鮮の国家支援を受けているハッカーグループ Jumpy Pisces が協力関係にあることが分かった。
- Jumpy Pisces と Play グループの関係性ははっきりとはしないが、Jumpy Pisces は、侵入に使用するためのアクセス権を Play グループに販売するイニシャルアクセスブローカーであった可能性が考えられる。
- Jumpy Pisces は、ランサムウェアグループを隠れ蓑として利用し身代金を得ることで、国際社会から北朝鮮への直接の制裁を回避し利益を得ようとしていたと考えられる。

第 3 章『脆弱なドメイン管理を狙う Sitting Ducks 攻撃』

- ドメインの所有権はそのままだが DNS の設定の権限を乗っ取られてしまう Sitting Ducks 攻撃が、複数のサイバー犯罪グループにより長年行われていること明らかになった。調査によれば標的になりうるドメインは約 80 万件以上存在し、その多くがドメインの権利の保持のために登録されているドメインとみられている。
- ドメインの権威 DNS に関する設定に問題が有り、かつ、ドメインレジストラと異なる DNS プロバイダーを利用しその DNS プロバイダーが攻撃に脆弱であると、ドメインが乗っ取られると考えられている。実際に、有名企業の乗っ取られたドメインがフィッシングに悪用されるといった被害が確認されている。
- Sitting Ducks 攻撃の防止のために、攻撃に脆弱なドメインの Lame delegation 状態の予防や確認が重要である。

1. Docusign の API 悪用による新たなフィッシング攻撃

1.1. 概要

11 月 5 日、オンライン電子署名サービス Docusign の API (Application Programming Interface [システム間でデータをやり取りするためのインターフェイス]) を悪用したフィッシング攻撃が急増しているとして、サイバーセキュリティ企業 Wallarm がブログ記事[1]で警告した。攻撃者は API の悪用により、知名度のある会社からの請求と誤認させる請求書を複数の宛先に大量送信し、正当な請求書と誤認した受信者に支払いをさせることで金銭を得ていた。

1.2. Docusign とは

Docusign は、米国 Docusign 社が提供する、オンライン上で電子署名を行うための有料クラウドサービスである。書類の送付、署名、承認といった契約手続きの一連のプロセスをオンラインで完結することができ、世界 180 か国以上で 150 万社を超える企業に利用されている[2]。

契約ユーザーには、外部システムと連携して自動的に請求書を一括送信するなどの各種機能が、API として提供されている[3]。

1.3. Docusign の API 悪用手口

今回発覚した Docusign の API を悪用した事例では、攻撃者は Docusign の有料プランを契約し、正規のユーザーアカウントを取得していた。そして、そのアカウントを使用して、以下の 3 段階の攻撃ステップを踏むことで、金銭を得ていた。

Docusign のユーザーコミュニティーでは、同様の攻撃に関する投稿が多数あり[4, 5]、攻撃は少なくとも数か月継続していたと見られる。

攻撃ステップ 1/3

攻撃者はまず、正規のユーザーに提供される文書テンプレートの編集機能を利用して、知名度のある会社を騙って電子署名を求める請求書を作成した。図 1 は、アンチウイルスソフトウェアで有名な Norton 社を騙った請求書で、一連の攻撃で実際に使用されたものである。

この偽の請求書に記載されていた金額は、本物の請求額と誤認させるために、実際の製品価格と同等になるように抑えられ

---

[1] 出典：Wallarm『Attackers Abuse DocuSign API to Send Authentic-Looking Invoices At Scale』
https://lab.wallarm.com/attackers-abuse-docusign-api-to-send-authentic-looking-invoices-at-scale/

[2] 出典：Docusign『About Docusign』
https://www.docusign.com/company

[3] 出典：Docusign『API Categories』
https://developers.docusign.com/docs/esign-rest-api/reference/

[4] 出典：Docusign Community『Phishing Emails from Docusign.net Domain』
https://community.docusign.com/esignature-111/phishing-emails-from-docusign-net-domain-4174

[5] 出典：Docusign Community『Phishing Scam - Norton』
https://community.docusign.com/esignature-111/phishing-scam-norton-4623

ていた。

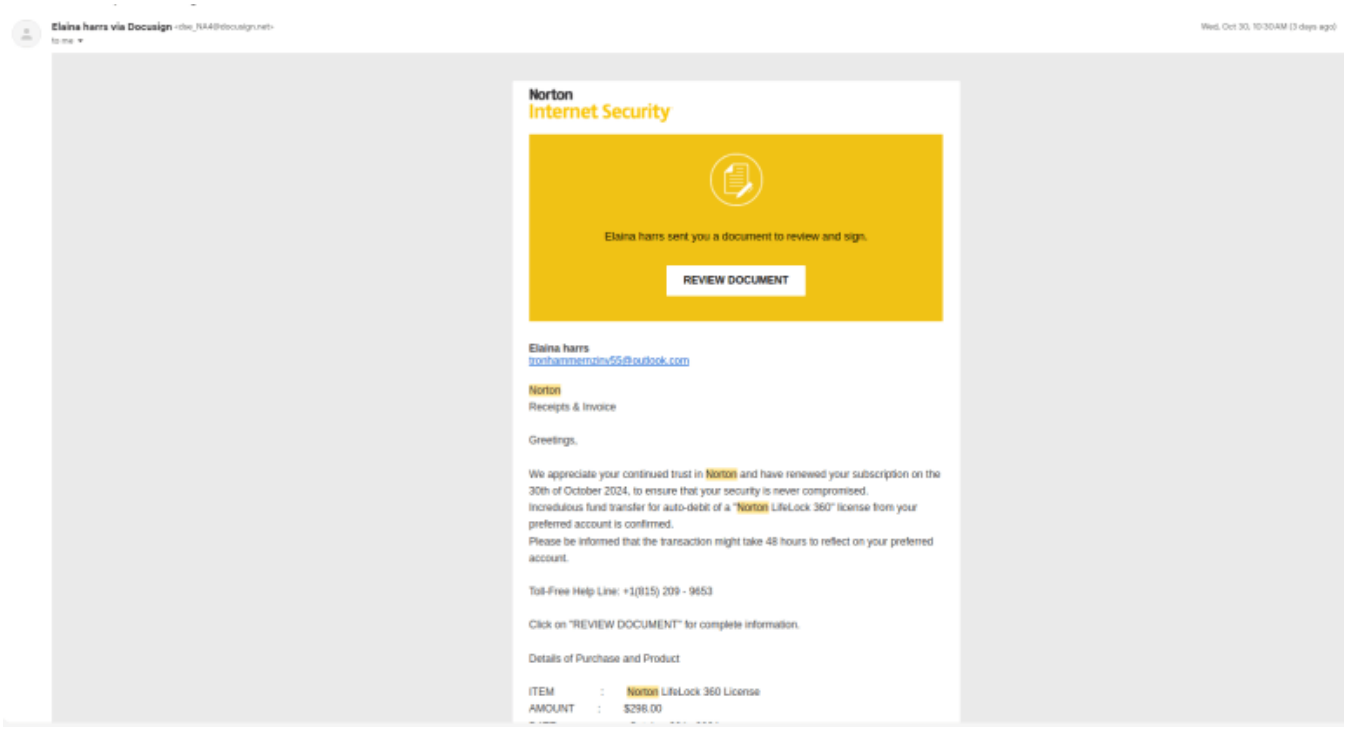

図 1 攻撃に使用された Docusign 経由で送付された請求書

攻撃ステップ 2/3

続いて、攻撃者は Docusign の API を使用して、偽の請求書を大量送信した。これらの偽の請求書は、Docusign のプラットフォームからの正当なメッセージとして送付されてくるため、迷惑メールフィルターなどで防ぐことはできない。日常的に Docusign からの請求書を受信する人物であれば、他の正規の請求書と区別できず、購入の実績がないにもかかわらず請求書に署名してしまった可能性がある。

攻撃ステップ 3/3

署名された偽の請求書を手に入れた攻撃者は Docusign を介して、署名者が所属する組織の財務部門に対して支払いを請求することができる。署名者と財務部門の担当者は別の人間であることが多く、Docusign という正当なプラットフォームからの支払い請求のため、双方で製品購入の事実を確認することなく、支払いが行われたとみられる。

1.4. API 悪用に対する Docusign の対応

11 月 6 日、Docusign は攻撃に関して注意喚起[6]を発表した。詐欺や違法行為に関連する疑わしい行動を迅速に調査

[6] 出典：Docusign Trust Center『Alert: Phishing Campaign Observed, November 6, 2024』
https://www.docusign.com/trust/alerts/alert-phishing-campaign-observed-november-6-2024

し、停止できるように複数のレイヤーでシステムを監視しているとコメントしている[7]。 具体的な対策を公表することで、攻撃者が対策を回避した別の手法を用いる可能性があるため、詳細は明らかにしていない。

また、同様の攻撃に気付いた場合は、Docusign の不正報告機能を使用したり、ウェブポータルから報告したりするようユーザーに呼び掛けている。

1.5. まとめ

今回発覚した Docusign の API を悪用したフィッシング攻撃は、広く利用されている信頼性の高いプラットフォームの仕組みを介してメッセージを送信することで、受信者に本物の請求書と誤認させることが特徴である。

API への攻撃は急増し[8]、日々被害が報告されており[9][10]、今後も様々な手口で API が悪用されることが予想される。API を介したメッセージを受信する側の組織では、プラットフォームが悪用されることを念頭に置いて、社内での承認プロセスをより厳格化する等の対策が求められる。

[7] 出典：BleepingComputer『DocuSign's Envelopes API abused to send realistic fake invoices』
https://www.bleepingcomputer.com/news/security/docusigns-envelopes-api-abused-to-send-realistic-fake-invoices/

[8] 出典：Check Point Blog『A Shadowed Menace: The Escalation of Web API Cyber Attacks in 2024』
https://blog.checkpoint.com/research/a-shadowed-menace-the-escalation-of-web-api-cyber-attacks-in-2024/

[9] 出典：BleepingComputer『Dell API abused to steal 49 million customer records in data breach』
https://www.bleepingcomputer.com/news/security/dell-api-abused-to-steal-49-million-customer-records-in-data-breach/

[10] 出典：BleepingComputer『Hackers abused API to verify millions of Authy MFA phone numbers』
https://www.bleepingcomputer.com/news/security/hackers-abused-api-to-verify-millions-of-authy-mfa-phone-numbers/

2. 北朝鮮ハッカー Jumpy Pisces が金銭目的でランサムウェア攻撃に関与

2.1. 概要

10 月、北朝鮮の国家支援を受けているハッカーグループ「Jumpy Pisces」（ジャンピー パイシーズ）が、Play ランサムウェアグループ（以下、Play グループ）と協力関係にあることが分かった。Play ランサムウェアの被害組織の調査にて、Play ランサムウェアの感染の前に Jumpy Pisces が侵入していたことが分かり、両グループの関与が判明した。Jumpy Pisces は、侵害したネットワークのアクセス権を販売するイニシャルアクセスブローカーとして機能していた可能性がある。Jumpy Pisces が金銭的な動機に基づいて既存のランサムウェアを使用したことが確認されたのはこれが初めてである[11]。

2.2. Jumpy Pisces について

北朝鮮の著名なハッカーグループ Lazarus のサブグループであると考えられている Jumpy Pisces は、スパイ活動を担っている朝鮮人民軍偵察総局（RGB）に所属しており、サイバースパイ活動や北朝鮮への資金提供を目的とした攻撃に従事している[12, 13]。また、ランサムウェア攻撃にも以前から関与しており、カスタム開発されたランサムウェア「Maui」で医療機関を標的とした攻撃を行ったとして、米国司法省から起訴されている[14]。同ランサムウェアは日本、ロシア、ベトナム、インドを標的とした 2022 年の攻撃でも使用された[15]。

2.3. Play グループについて

今回、Jumpy Pisces との協力関係にあるとされる Play グループは、2022 年半ばに存在が確認された[16]。このグループが使用する Play ランサムウェアは、今年の 12 月までに 600 以上の組織に被害を与えたとみられる（当社調べ）。同グループは、身代金が支払われなければ、自身が暗号化したデータを復号せず、さらには窃取したデータを公開するといった、被害組織への多重恐喝も行う。攻撃の対象は、政府や金融、病院、製造業、非営利組織等、幅広い[17]。

---

[11] 出典：Palo Alto Networks『Jumpy Pisces Engages in Play Ransomware』
https://unit42.paloaltonetworks.com/north-korean-threat-group-play-ransomware/

[12] 出典：Palo Alto Networks『パロアルトネットワークス Unit 42 が追跡している脅威アクター グループの一覧』
https://unit42.paloaltonetworks.jp/threat-actor-groups-tracked-by-palo-alto-networks-unit-42/

[13] 出典：The Hacker News『North Korean Group Collaborates with Play Ransomware in Significant Cyber Attack』
https://thehackernews.com/2024/10/north-korean-group-collaborates-with.html

[14] 出典：U.S. Department of JUSTICE『North Korean Government Hacker Charged for Involvement in Ransomware Attacks Targeting U.S. Hospitals and Health Care Providers』
https://www.justice.gov/opa/pr/north-korean-government-hacker-charged-involvement-ransomware-attacks-targeting-us-hospitals

[15] 出典：BleepingComputer『North Korean govt hackers linked to Play ransomware attack』
https://www.bleepingcomputer.com/news/security/north-korean-govt-hackers-linked-to-play-ransomware-attack/

[16] 出典：Palo Alto Networks『Jumpy Pisces Engages in Play Ransomware』
https://unit42.paloaltonetworks.com/north-korean-threat-group-play-ransomware/

[17] 出典：Palo Alto Networks『パロアルトネットワークス Unit 42 が追跡している脅威アクター グループの一覧』
https://unit42.paloaltonetworks.jp/threat-actor-groups-tracked-by-palo-alto-networks-unit-42/

同グループは 2022 年 8 月にアルゼンチンのコルドバ司法当局を標的にしたことで注目を集めた[18]。また、今年 12 月には日本の飲料メーカーである株式会社伊藤園へサイバー攻撃を行い、不正アクセスと情報窃取を行ったことを示す声明を出している。

これまで、Play グループはランサムウェアを自ら開発および使用してきたが、最近、ランサムウェアをビジネスとして他のハッカーに提供するサービスモデルである RaaS（Ransomware-as-a-Service）に移行した可能性が指摘されている。ただ、同グループは自身のデータリークサイト（窃取したデータを暴露するサイト）で、「RaaS の提供はしていない」と否定している[19]。

図 2 Play グループのデータリークサイト

「Play グループは RaaS を提供したことがない」と記載されている（赤枠）

2.4. Jumpy Pisces の攻撃と Play グループの関係について

2024 年 9 月、Play ランサムウェアが関係するインシデントの調査で、Jumpy Pisces のものと推定される痕跡が発見された。ランサム攻撃にあたり、5 月から 9 月にかけて被害組織への侵入があったが、これを行っていたのが Jumpy Pisces であったとみられる。同グループは標的への最初のアクセスに成功した後、マルウェアをネットワーク内の他のホストにもコピーして拡散し、自身がリモートアクセスできる状態を維持できるようにした。そして 9 月上旬には、何者かによって Play ランサムウェアを使ったデータの暗号化が実行されたと考えられている[20]。

[18] 出典：Palo Alto Networks『パロアルトネットワークス Unit 42 が追跡している脅威アクター グループの一覧』
https://unit42.paloaltonetworks.jp/threat-actor-groups-tracked-by-palo-alto-networks-unit-42/

[19] 出典：The Hacker News『North Korean Group Collaborates with Play Ransomware in Significant Cyber Attack』
https://thehackernews.com/2024/10/north-korean-group-collaborates-with.html

[20] 出典：Palo Alto Networks『Jumpy Pisces Engages in Play Ransomware』
https://unit42.paloaltonetworks.com/north-korean-threat-group-play-ransomware/

図 3　Play ランサムウェアを使用した Jumpy Pisces による攻撃（Unit42 のレポートより）[21]

Jumpy Pisces と Play グループが、標的のシステムに同じアカウントを用いて侵入していたことから、両者の間には協力関係があると考えられる[22]。ただ、今回の Play ランサムウェアの感染を狙った一連の攻撃にあたり、Jumpy Pisces が Play グループのアフィリエイト（攻撃実行役）になっていたかは不明である。先述の、RaaS システムを提供していないという Play グループの主張が真実であれば、Jumpy Pisces は、最初の侵入で使用するためのアクセス権を Play グループに販売したイニシャルアクセスブローカーとしてのみ機能していた可能性も考えられる。

2.5. まとめ

ランサム攻撃では分業体制がよく取られている。一般的に身代金が支払われると、これを受け取った者から分業に参加した各者に分け前が配分される。Jumpy Pisces は協力関係にある Play グループを、身代金による利益を得るための隠れ蓑に利用している可能性がある。この隠密活動は、国際社会からの北朝鮮に対する制裁を回避しつつ金銭を得ることが狙いと考えられる。

このように効率的に資金を獲得するための手段として、北朝鮮の国家支援を受けているハッカーグループがより広範なランサム攻撃キャンペーンに参加する可能性が懸念される。ロシアやイランの国家支援を受けるハッカーグループでも同様の傾向が見られ[23]、今後の動向が注目される。

[21] 出典：Palo Alto Networks『Jumpy Pisces Engages in Play Ransomware』
https://unit42.paloaltonetworks.com/north-korean-threat-group-play-ransomware/

[22] 出典：Palo Alto Networks『Jumpy Pisces Engages in Play Ransomware』
https://unit42.paloaltonetworks.com/north-korean-threat-group-play-ransomware/

[23] 出典：The Record『Nearly 400 US healthcare institutions hit with ransomware over last year, Microsoft says』
https://therecord.media/ransomware-healthcare-microsoft-last-year

3. 脆弱なドメイン管理を狙う Sitting Ducks 攻撃

3.1. 概要

ドメインの設定不備を突いて DNS 設定の権限を乗っ取る「Sitting Ducks」と呼ばれる攻撃に関して、セキュリティ会社の Infoblox が 7 月と 11 月にレポートした[24, 25, 26]。以前に一部の研究者が発見していたが、セキュリティ業界でもほとんど知られていなかった攻撃手法である。このレポートにおける最新の調査では、ここ数年被害が増えつつあり、脆弱なドメインがインターネット上に約 80 万件存在し、そのうち約 7 万件が既に Sitting Ducks 攻撃で乗っ取られていたことが明らかになった。乗っ取られたドメインの多くは、ブランド保護等のために予防的に取得したり、使い終えたりした等、ドメインの権利の保持のために登録されたものとみられている。

乗っ取ったドメインを悪用するサイバー犯罪グループが複数存在し、有名企業のドメインがフィッシングに悪用されるといった被害が確認されている。

3.2. Sitting Ducks 攻撃の成立条件

Sitting Ducks 攻撃によってドメインの乗っ取りが成立するには、次の条件が揃う必要がある。

まず、ドメインのネームサーバーが Lame delegation になっている事が挙げられる。Lame delegation は、委任先を変更したにもかかわらず、委任元ゾーンで指定している NS レコードを変更していない、または委任先ネームサーバー名に誤りがある等の場合に発生する[27]。

さらに、ドメイン所有者がネームサーバーの委任先を、ドメインを登録したドメインレジストラから異なる DNS プロバイダーへと変更して利用しており、その DNS プロバイダーがドメインの所有者の確認を十分に行っておらず攻撃者の成りすまし対策ができていない場合、攻撃が成功すると考えられている[28]。

Sitting Ducks 攻撃ではドメインの所有権はそのままである。攻撃者はドメインの所有者が気付かないうちに DNS 設定を変更することにより、ドメインの名前解決先を攻撃者の用意したフィッシングサイトに紐づける等、ドメインを悪用する。

乗っ取られるドメインは、ブランド保護等のために予防的に登録されているドメインや、WEB サイト等に利用されていない休眠状態のドメインが多い。悪用例として上記のようなフィッシングサイトの他にも、休眠状態のドメインが Sitting Ducks 攻撃に遭い、爆破予告メールの送信に使われていたといったケースも確認されている[29]。

---

[24] 出典：Infoblox『Who Knew? Domain Hijacking is So Easy』
https://blogs.infoblox.com/threat-intelligence/who-knew-domain-hijacking-is-so-easy/

[25] 出典：Infoblox『DNS Predators Hijack Domains to Supply their Attack Infrastructure』
https://blogs.infoblox.com/threat-intelligence/dns-predators-hijack-domains-to-supply-their-attack-infrastructure

[26] 出典：The Hacker News『Experts Uncover 70,000 Hijacked Domains in Widespread 'Sitting Ducks' Attack Scheme』
https://thehackernews.com/2024/11/experts-uncover-70000-hijacked-domains.html

[27] 出典：JPNIC『インターネット 10 分講座：lame delegation』
https://www.nic.ad.jp/ja/newsletter/No36/0800.html

[28] 出典：Eclypsium『Ducks Now Sitting (DNS): Internet Infrastructure Insecurity』
https://eclypsium.com/blog/ducks-now-sitting-dns-internet-infrastructure-insecurity/

[29] 出典：Krebs on Security『Bomb Threat, Sextortion Spammers Abused Weakness at GoDaddy.com』
https://krebsonsecurity.com/2019/01/bomb-threat-sextortion-spammers-abused-weakness-at-godaddy-com/

3.3. Sitting Ducks の攻撃者たち

Sitting Ducks 攻撃についての被害調査[30]で、インターネット上には脆弱なドメインが約 80 万件存在し、そのうち約 7 万件が既に乗っ取られていたことが明らかになっている。被害を受けたドメインの所有者は、米国のミズーリ州政府、法律事務所、医療機関から大企業、中小企業と様々である。

2019 年頃からは、Sitting Ducks 攻撃を行うサイバー犯罪グループが複数現れている。例えば、Vacant Viper と命名されているグループは、2019 年 12 月以降、毎年推定 2,500 件のドメインを乗っ取っている。Vacant Viper はスパムメールの送信、フィッシングサイトの設置、マルウェアの配信や C2 サーバーの設置等に、乗っ取ったドメインを用いている。また、Horrid Hawk と命名されているグループは投資詐欺サイトの設置に Sitting Ducks 攻撃で乗っ取ったドメインを使用している。このグループは世界 30 か国以上をターゲットにし、Facebook 広告等から投資詐欺サイトに誘導していた。

このような攻撃者たちによるドメインの乗っ取りは、長期間・短期間の両方が確認されている。特に短期間の乗っ取りでは、一部の DNS プロバイダーが提供する無料アカウントサービスを利用することで、無料期間である 30 日から 60 日の間だけ乗っ取るといった手法も確認されている。この期間を過ぎるとすぐに、また別の攻撃者が同じように乗っ取る、といったことが行われている。

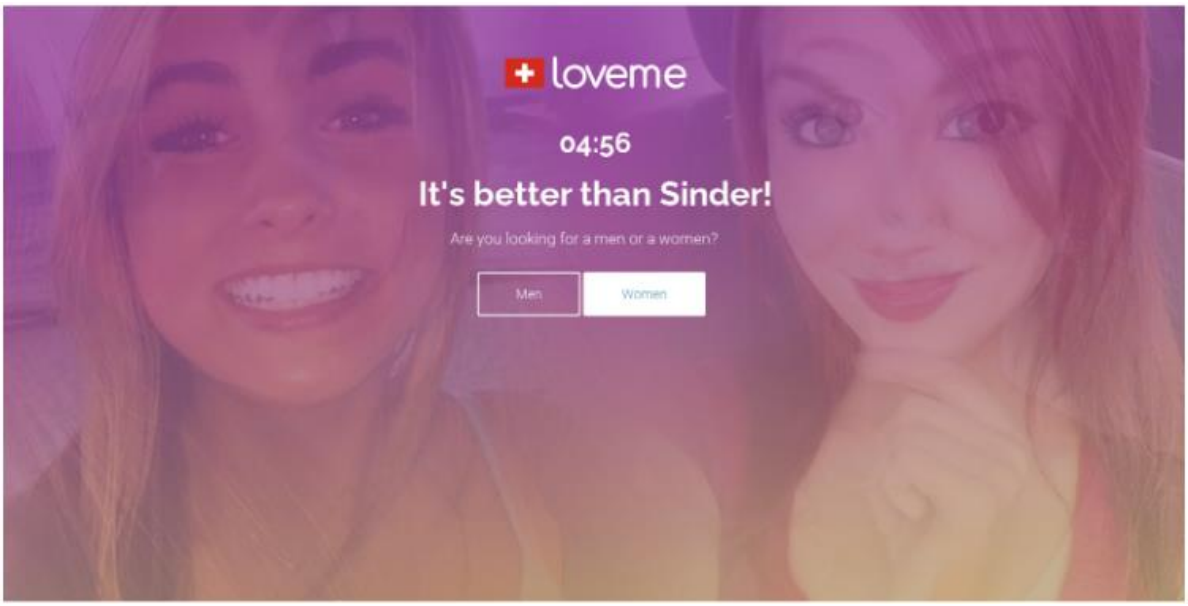

図 4 Sitting Ducks 攻撃による乗っ取り例：
教育機関のドメインの誘導先になっていた出会い系サイト

3.4. まとめ

Sitting Ducks 攻撃でドメインを乗っ取られてフィッシング攻撃や第三者への攻撃への踏み台に悪用された場合、組織の評判の低下等の様々な被害に繋がるため、事前の予防が重要である。ドメインを使わなくなった時の DNS 設定の削除の実

[30] 出典：Infoblox『DNS PREDATORS ATTACK:VIPERS AND HAWKS HIJACK SITTING DUCKS DOMAINS』
https://insights.infoblox.com/resources-research-report/infoblox-research-report-dns-predators-attack-vipers-hawks-hijack-sitting-ducks-domains

施を徹底すること[31]が、対策として有効である。また、予防的に取得したドメインや休眠状態のドメイン等を所有する事業者は Sitting Ducks 攻撃に脆弱な Lame delegation 状態のドメインが無いか等、ドメインの DNS 設定の確認を行う事を推奨する。

以上

[31] 出典：IIJ Engineers Blog『忘れ去られたドメイン名に宿る付喪神』
https://eng-blog.iij.ad.jp/archives/15199

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

プロフェッショナルサービス部　OSINT モニタリングチーム
メールアドレス：nsj-co-osint-monitoring@security.ntt