NTT Security Holdings

OpSafeWinter と保険会社へのサイバー攻撃

NTTセキュリティ・ジャパン
OSINTモニタリングチーム
2023年1月13日

エグゼクティブサマリー

- 2022年12月、渋谷区は美竹公園にて不法な占用を続ける路上生活者に対して行政代執行を行った。
- 年が明けて1月3日、本件に抗議して、アノニマスが渋谷区のWebサイトに対し OpSafeWinter の作戦名の元に DDoS 攻撃を実施したと発表。数日間、渋谷区のWebサイトの表示が不安定になった。
- 続いて、アノニマスは国内の奥多摩町等の複数のWebサイトに攻撃を行い、閲覧不能な状態に追い込んだ。
- 1月8日、サイバー犯罪を繰り返しているアクターが、生命保険会社のチューリッヒとアフラックから窃取した日本人顧客の個人情報を、ハッカー掲示板にて暴露した。
- その後、アノニマスがこのデータを別のサイトに転載し、OpSafeWinter の名の元に Twitter に投稿し拡散させた。

渋谷区の美竹公園路上生活者立ち退き問題と #OpSafeWinter

渋谷区の美竹公園路上生活者立ち退き問題について

- 渋谷区立美竹公園では、路上生活者による不法な占用が続いていた。
- 美竹公園の再開発を進める渋谷区は2022年10月、美竹公園の利用の停止を決定。12月には美竹公園の立ち入りを禁止し、立ち退かない路上生活者らに対し行政代執行を開始した。
  - 渋谷区は、事前に立ち退きを依頼。それに合わせ、路上生活者らの生活や社会復帰を支援（※）している。
  - 支援団体は、公園からの強制立ち退きに抗議。また、区の支援についても不十分であると反論している。


渋谷区 Shibuya City

準備工事の着手に向けた仮囲いの追加設置工事の実施について（経緯詳細）

更新日：令和4年12月14日

お知らせ

区立神宮通公園（北側）の終日利用禁止について（令和4年12月14日付け）

【問い合わせ：ステップアップ事業に関すること】まちづくり第三課（電話：03-3463-2628）
【問い合わせ：公園に関すること】公園課（電話：03-3463-2888）

令和4年9月に基本協定を締結した「都市再生ステップアップ・プロジェクト（渋谷地区）渋谷一丁目地区共同開発事業」は、東京都と渋谷区が共同し、民間の資金及び経営能力の活用により相互に隣接する都有地と区有地の一体的な活用の実現を図るものです。
この地区の有効活用についてはかねてから地域住民から切望されており、地元アンケート結果等を踏まえつつ地域課題を解決するため、都立児童会館の文化を継承する創造文化教育に資する施設、旧区立渋谷小学校体育館の地域開放機能を引き継ぐ多目的ホール、都心の憩いの場として多様な人々が集まるインクルーシブな都市公園の再整備などを行ないます。当該施設は地域住民のための避難所や帰宅困難者の受入施設としても活用してまいります。
このような背景から、渋谷区はこの事業を推進する自治体としての重要な責務を負っており、美竹公園において準備工事を実施する必要があることから、本年10月25日に美竹公園を利用禁止とし、仮囲いを設置いたしました。

また、渋谷区では、これまで長期化・高齢化した路上生活者を対象にした、住まいの確保を優先し地域生活への移行を支援するハウジングファースト事業（注）や、就労し自立を目指す路上生活者への支援として、都区共同で実施している路上生活者対策事業を行なっています。
美竹公園においても、継続したお声かけを行なってきており、仮囲い設置の際には、福祉事務所を通じて3名にシェルターを案内し、2名がアパー

美竹公園の再開発着手にあたっての渋谷区の説明

※渋谷区の支援：公園に寝泊まりさせるのではなく、社会復帰を支援することが自治体の責務との考え
- 渋谷区独自の施策として、アパート等住まいを提供のうえ、食事の提供など生活支援を通して、地域社会での生活へとつなげる「ハウジングファースト事業」を提供
- 東京都と共同で、就労して自立を目指す路上生活者への支援事業を展開

出典：
https://www.city.shibuya.tokyo.jp/kankyo/machi/shibuya_eki/stepup_pj_junbi_kouji.html
https://www.security-next.com/142651

#OpSafeWinter（安全な冬作戦）

- 2023年1月1日、渋谷区による路上生活者の立ち退き政策を非難する主張に共感するツイートを、アノニマスのメンバーであるYourAnonRiots が行った。
- 以降、本件に関連する投稿を行う場合、アノニマスは#OpSafeWinter（安全な冬作戦）というハッシュタグを付けるようになった。
  - アノニマスはオペレーション（作戦）の遂行時、「#Op～」のように、Opが付いた作戦名のハッシュタグを使用する
- YourAnonRiots は日本在住のアクターと見られ、過去に日本に関連するオペレーションに関して、主導的な役割を果たしていた。
- 同アクターが主導したオペレーションおよび攻撃の被害に遭った組織には下記が含まれる：
  - #OpMyanmar [ミャンマー国軍による市民への弾圧に抗議]：鴻池組、ミャンマー日本商工会議所等
  - #OpBoycottOlympics [東京オリンピックのボイコットを訴える]： Coltテクノロジーサービス等
  - #OpFukushima [福島第一原子力発電所の処理水の海洋放出に抗議]：経済協力開発機構原子力機関等

左：#OpSafeWinter のハッシュタグを付けた YourAnonRiots のツイート
右： YourAnonRiots がミャンマー日本商工会議所及び鴻池組のWebサイトをダウンさせたと主張するツイート

#OpSafeWinter（安全な冬作戦）

- 他のアノニマスメンバーも YourAnonRiots に同調するツイートを発信した。
- 翌2日、Parrattarna というメンバーは、 YourAnonRiots と同様に#OpSafeWinter のハッシュタグを付け、渋谷区を非難する投稿を行った。
- 同メンバーはクルド人である可能性が考えられる。
- 「我々は黙っていないであろう」といった、今後の攻撃を示唆するような投稿も行った。

渋谷区の対応を非難する Parrattarna のツイート

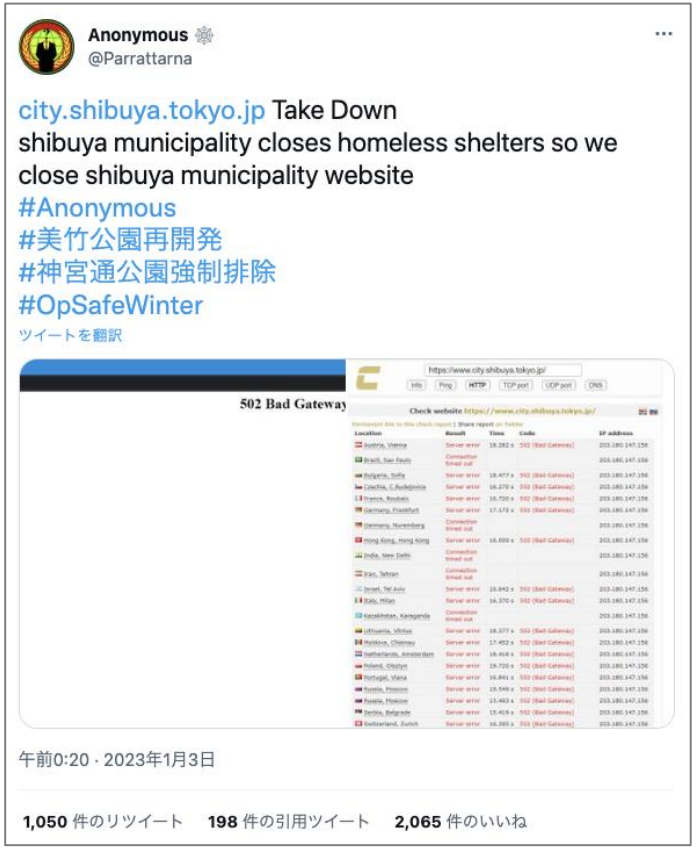
訳：「渋谷区、およびホームレスを追い出したことに責任を負うべき全ての人々に言う：我々は黙っていないであろう」

左記の投稿から数分後の Parrattarna のツイート

アノニマスによるDDoS攻撃

アノニマスによるDDoS攻撃

- Parrattarna は翌3日 0時20分に、渋谷区のWebサイト「city.shibuya.tokyo.jp」をダウンさせたとツイートした。
- DDoS攻撃を実行したとみられ、この投稿には、DDoS攻撃成功の証拠となるスクリーンショットも添えられていた。
- 渋谷区への報復としてDDoS攻撃を行った旨の主張が記されていた。

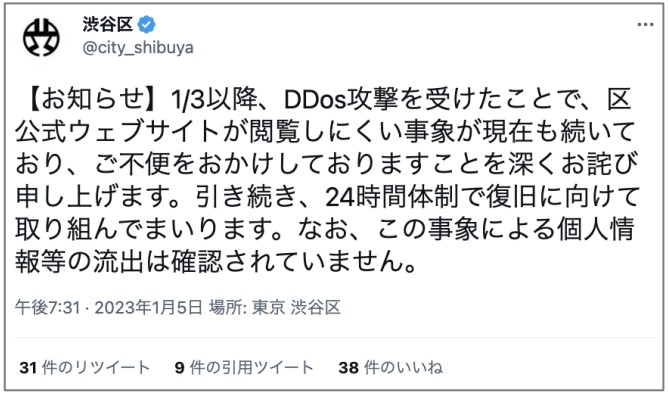


Parrattarna によるサイトダウン報告のツイート
訳：渋谷区がホームレスのシェルターを閉鎖したのだから、我々は渋谷区のサイトを閉鎖する

アノニマスによる攻撃の被害状況

- アノニマスの攻撃により、実際に1月3日未明から、渋谷区公式サイトが閲覧しづらい状態となった。
- 渋谷区は同日から4日にかけ、この事象はアノニマスが実行するDDoS攻撃によって引き起こされたこと、更に5日にはこの状態が未だに続いていることを発表した。

1/4付の渋谷区による発表（公式サイト）



1/5付の渋谷区による発表（Twitter）

出典：
https://www.city.shibuya.tokyo.jp/kusei/koho/website_syougai.html
https://twitter.com/city_shibuya/status/1610947126904918016

継続する日本のサイトへの攻撃

- 渋谷区のWebサイトに対する攻撃の1時間後には team_insane_pk と名乗るアノニマスが、下記のように東京都奥多摩町を含む複数の日本のサイトを表示不可能にしたと主張した。
  - town.okutama.tokyo.jp
  - setagaya.tokyo.jp
  - olympic.tokyo.jp
- この人物も、Parrattarna と同様に、渋谷区に対する報復の意図を示している。
- 自身をパキスタンのハッカーグループであると述べている。

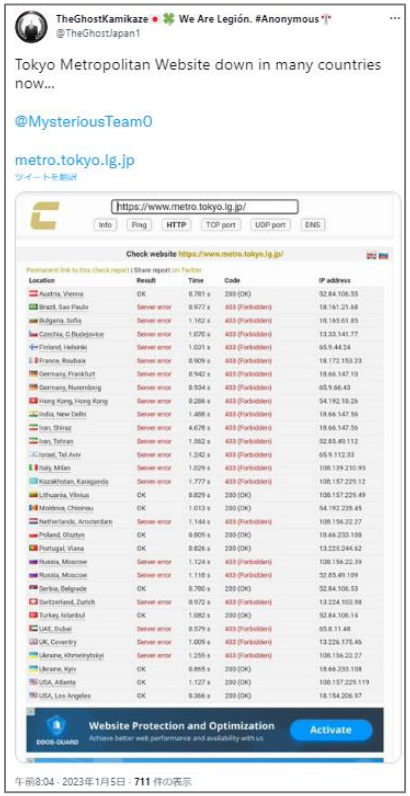
team_insane_pk のツイート
右図の4件と合わせ、「たくさんの日本のサイトが表示不可能となった」とツイート

DNSサーバーを攻撃したことを示唆するツイート

継続する日本のサイトへの攻撃

- 5日には、別のアノニマスである MysteriousTeam0 が、公益財団法人アーツカウンシル東京のWebサイトを表示不能にしたと主張した。
- 同アクターは自身を「バングラデシュのサイバー戦士たち」であると表現している。
- また同日には、TheGhostJapan1 と名乗るアノニマスが、東京都庁のWebサイトを攻撃したことを報告した。
- これらのメンバーはこれまでにも、他のアノニマスのオペレーションで攻撃に関与していることが確認されている。

MysteriousTeam0 のツイート



TheGhostJapan1 のツイート

チューリッヒ/アフラックの顧客個人情報暴露

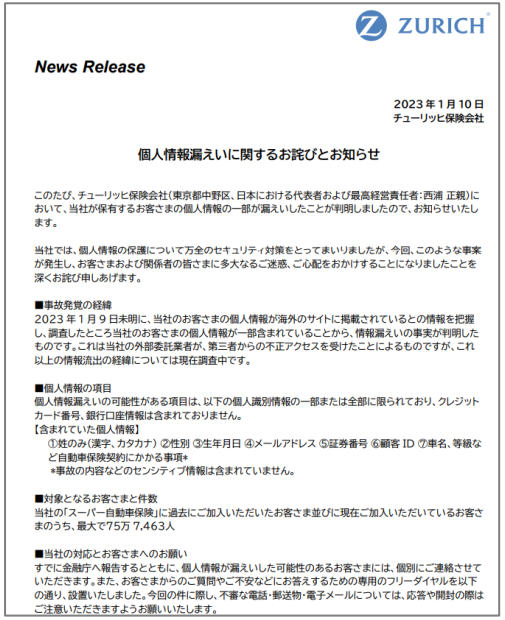
チューリッヒ保険の情報暴露

- 1月9日、アノニマスの team_insane_pk が#OpSafeWinter のハッシュタグと共に、チューリッヒ保険日本法人の個人情報を暴露した。
- 260万ユーザーのデータベースと称するリンクが、同アクターのツイートに記載されていた。

team_insane_pk のツイート

日本の保険企業2社の被害公表

- 1月10日、チューリッヒ保険日本法人およびアフラック生命保険日本法人は、個人情報の流出があったことを公表した。
- 7日以降に、両社が業務を委託していた同一の米企業が不正アクセスを受け、個人データが盗み出されていた。
- 実際に対象となった顧客数はアノニマスの主張とは異なり (※)、チューリッヒは最大で75万人と発表している。またアフラックが発表した人数は132万人であった。



ZURICH

News Release

2023年1月10日
チューリッヒ保険会社

個人情報漏えいに関するお詫びとお知らせ

このたび、チューリッヒ保険会社(東京都中野区、日本における代表者および最高経営責任者:西浦 正親)において、当社が保有するお客さまの個人情報の一部が漏えいしたことが判明しましたので、お知らせいたします。

当社では、個人情報の保護について万全のセキュリティ対策をとってまいりましたが、今回、このような事案が発生し、お客さまおよび関係者の皆さまに多大なるご迷惑、ご心配をおかけすることになりましたことを深くお詫び申しあげます。

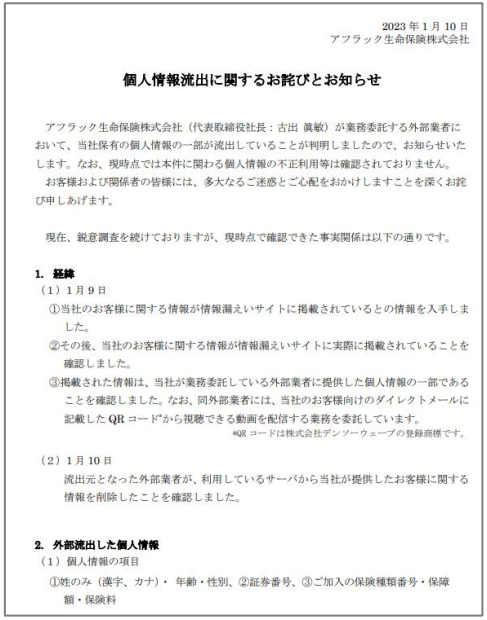
■事故発覚の経緯
2023年1月9日未明に、当社のお客さまの個人情報が海外のサイトに掲載されているとの情報を把握し、調査したところ当社のお客さまの個人情報が一部含まれていることから、情報漏えいの事実が判明したものです。これは当社の外部委託業者が、第三者からの不正アクセスを受けたことによるものですが、これ以上の情報流出の経緯については現在調査中です。

■個人情報の項目
個人情報漏えいの可能性がある項目は、以下の個人識別情報の一部または全部に限られており、クレジットカード番号、銀行口座情報は含まれておりません。
【含まれていた個人情報】
①姓のみ(漢字、カタカナ) ②性別 ③生年月日 ④メールアドレス ⑤証券番号 ⑥顧客 ID ⑦車名、等級など自動車保険契約にかかる事項*
*事故の内容などのセンシティブ情報は含まれていません。

■対象となるお客さまと件数
当社の「スーパー自動車保険」に過去にご加入いただいたお客さま並びに現在ご加入いただいているお客さまのうち、最大で75万 7,463人

■当社の対応とお客さまへのお願い
すでに金融庁へ報告するとともに、個人情報が漏えいした可能性のあるお客さまには、個別にご連絡させていただきます。また、お客さまからのご質問やご不安などにお答えするための専用のフリーダイヤルを以下の通り、設置いたしました。今回の件に際し、不審な電話・郵送物・電子メールについては、応答や開封の際はご注意いただきますようお願いいたします。

チューリッヒから漏洩した可能性のある情報：
①姓のみ（漢字、カタカナ）
②性別
③生年月日
④メールアドレス
⑤証券番号
⑥顧客 ID
⑦車名、等級など自動車保険契約にかかる事項



2023年1月10日
アフラック生命保険株式会社

個人情報流出に関するお詫びとお知らせ

アフラック生命保険株式会社（代表取締役社長：古出 眞敏）が業務委託する外部業者において、当社保有の個人情報の一部が流出していることが判明しましたので、お知らせいたします。なお、現時点では本件に関わる個人情報の不正利用等は確認されておりません。
お客様および関係者の皆様には、多大なるご迷惑とご心配をおかけしますことを深くお詫び申しあげます。

現在、鋭意調査を続けておりますが、現時点で確認できた事実関係は以下の通りです。

1. 経緯
（1）1月9日
①当社のお客様に関する情報が情報漏えいサイトに掲載されているとの情報を入手しました。
②その後、当社のお客様に関する情報が情報漏えいサイトに実際に掲載されていることを確認しました。
③掲載された情報は、当社が業務委託している外部業者に提供した個人情報の一部であることを確認しました。なお、同外部業者には、当社のお客様向けのダイレクトメールに記載した QR コードから視聴できる動画を配信する業務を委託しています。
*QR コードは株式会社デンソーウェーブの登録商標です。

（2）1月10日
流出元となった外部業者が、利用しているサーバから当社が提供したお客様に関する情報を削除したことを確認しました。

2. 外部流出した個人情報
（1）個人情報の項目
①姓のみ（漢字、カナ）・ 年齢・性別、②証券番号、③ご加入の保険種類番号・保障額・保険料

アフラックから漏洩した情報：
①姓のみ（漢字、カナ）・年齢・性別
②証券番号、
③加入している保険種類番号・保障額・保険料

※ 同一人物による複数の契約情報や、解約者の情報等によって、差分が出ている可能性が考えられる

出典：
https://www.zurich.co.jp/-/media/jpz/zrh/pdf/pr/2023/NewsRelease_20230110_ZurichInsuranceCompanyLtd.pdf
https://www.aflac.co.jp/news_pdf/2023011001.pdf
https://www3.nhk.or.jp/news/html/20230110/k10013946151000.html

チューリッヒ（左）、アフラック（右）のプレスリリース

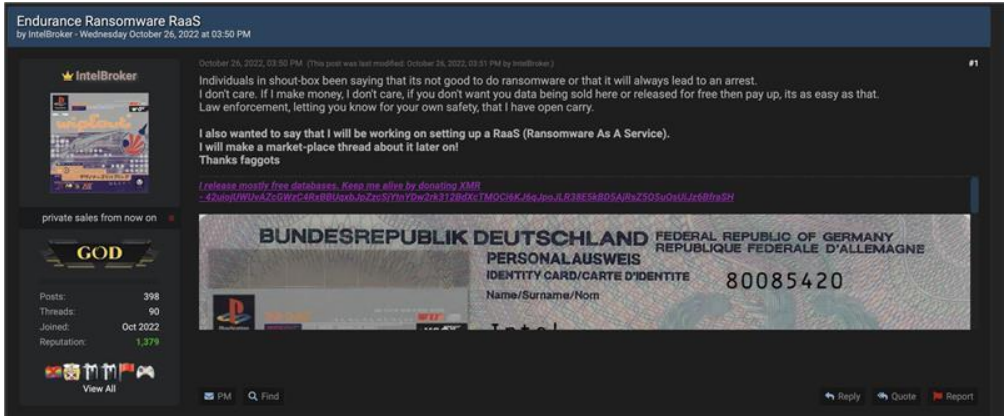
チューリッヒ/アフラックの顧客個人情報暴露

- 1月8日に、IntelBroker と名乗る人物が2023年1月に両社から盗んだと主張する個人データをハッカー掲示板に投稿していた。
- チューリッヒ保険については260万人分、アフラック生命保険については310万人分と述べている。
- アノニマスの team_insane_pk は自身で両社のデータを窃取したのではなく、当掲示板で公開されていたデータを転載した可能性が考えられる。

ハッカー掲示板に投稿されたチューリッヒ、アフラックのデータベースの暴露
サンプルとして一部個人データが掲載されているため、該当部分を加工

IntelBroker について

- IntelBroker はセルビア出身であり、ロシア語圏を含む複数のハッカー掲示板等での、収益を目的としたサイバー犯罪活動が確認できる。
- アノニマスとの関係性については確認できていない。
- これまでに、米国の複数の公的機関やボルボ社等の民間の大企業に対してハッキングを行った実績がある。
- ランサムウェアサービスを立ち上げようとしており、ハッカー仲間を募っている。サービスは未だ開発途中であるが、既に攻撃を行っていることを示す投稿が確認できる。
- チューリッヒ/アフラックの個人情報は、IntelBroker とその仲間たちのハッキングにより窃取されたと考えられる。



IntelBroker によるハッカー掲示板への投稿
自身でランサムウェアを開発中であり、サービス化に向けてハッカー仲間を募っている

まとめ

まとめ

- アノニマスの活動は、内部対立や法執行機関の取り締まり強化等により、2010年代半ば頃からは低迷していた。
- 今回の#OpSafeWinter の活動では、様々なアクターが短期間のうちにサイバー攻撃を実行しており、過去数年にはなかったような勢いがみられる。
- ウクライナ侵攻以降のアノニマスの活動が注目を浴びており、求心力を再び取り戻した可能性が考えられる。
- 今後のアノニマスの活動には、注意を要する。

Security Holdings