NTT Security Holdings

【続報】イスラエルとハマスの軍事衝突における ハッカーグループの活動と日本への波及

NTTセキュリティ・ジャパン
OSINTモニタリングチーム

2023年11月2日
最終更新日：2023年12月22日

国連決議に関連すると考えられる攻撃の宣言

国連決議に関連すると考えられる攻撃の宣言

- 10月30日、パキスタンに関連するハッカーグループがSNSにて、日本を含む20か国に対してサイバー攻撃の開始を宣言した。
- これらの攻撃対象は、10月27日にヨルダンが国連総会に提出して賛成多数で議決した休戦案に対し、反対や棄権をした国々にほぼ一致する。

20か国への攻撃の宣言（日本は最後に記載）

	国名	27日ヨルダン案への賛否
1	オーストリア	反対
2	クロアチア	反対
3	チェコ	反対
4	フィジー	反対
5	グアテマラ	反対
6	ハンガリー	反対
7	イスラエル	反対
8	マーシャル諸島	反対
9	ミクロネシア	反対
10	ナウル	反対
11	パプアニューギニア	反対
12	パラグアイ	反対
13	トンガ	反対
14	アメリカ	反対
15	フランス	賛成
16	イギリス	棄権
17	インド	棄権
18	カナダ	棄権
19	イタリア	棄権
20	日本	棄権

**サイバー攻撃を宣言された20か国と
ヨルダン提出の休戦案への賛否**

注：賛成していたフランスは攻撃対象に含まれている。

10月18日に安保理で否決されたロシア提出の停戦案に反対したことや、本アクターが個別に攻撃対象としている経済協力開発機構原子力機関の本部がパリにあることなどが理由として考えられる。

日本への攻撃を宣言

- 同アクターは攻撃対象とした国々を中心に、次々と攻撃を実施したと主張。
- その後、日本時間の11月1日13時頃に突如、**「まず日本から攻撃を始める」**と投稿。
- 攻撃理由は、イスラエルによって作られたサイバーセキュリティシステムを日本の多くの企業や政府関係組織で利用しているから、と投稿している。

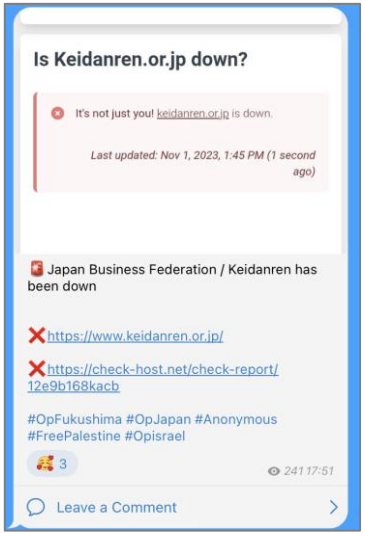
日本への攻撃の宣言

日本への攻撃

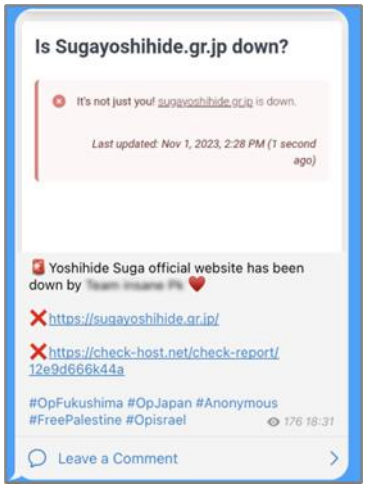
日本への攻撃①

- 日本への攻撃を宣言した数時間後、同アクターは日本のサイトへの攻撃を主張する投稿を開始した。
- 同アクターは以下の日本の11サイトへの攻撃に関する投稿を、日本時間の17時頃から20時頃にかけて次々と行った：NTTPCコミュニケーションズ、自民党、経団連、衆議院議員 菅義偉、衆議院議員 茂木としみつ、ミャンマー日本商工会議所、鴻池組、東京スカイツリー、東京都、J-POWER（電源開発株式会社）、日本原子力学会

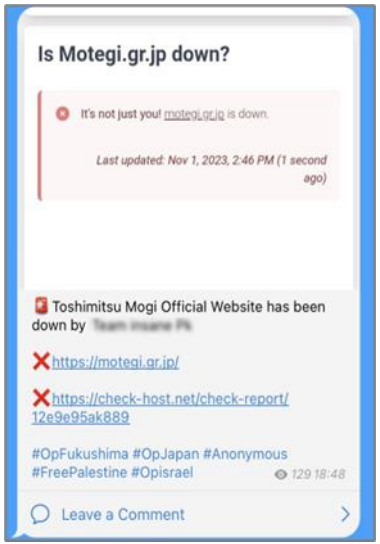
自民党のWebサイトへの攻撃を主張する投稿



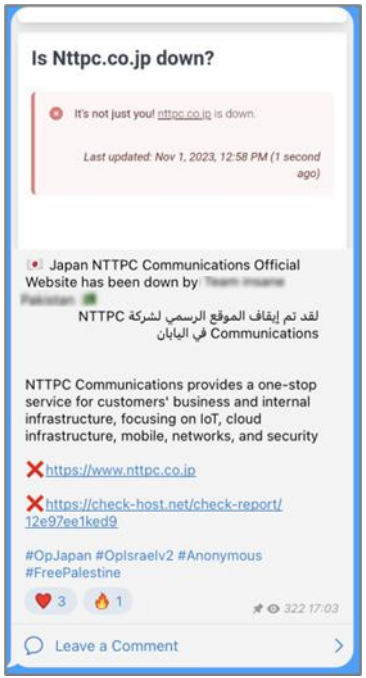
経団連のWebサイトへの攻撃を主張する投稿



衆議院議員 菅義偉のWebサイトへの攻撃を主張する投稿



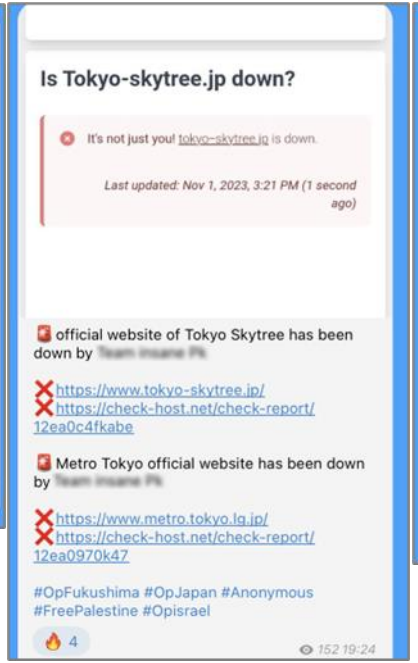
衆議院議員 茂木としみつ のWebサイトへの攻撃を主張する投稿

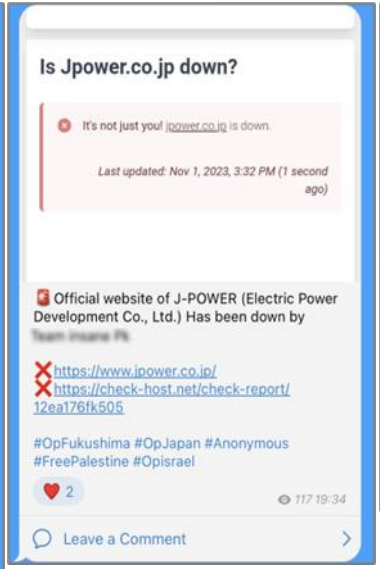


NTTPCコミュニケーションズのWebサイトへの攻撃を主張する投稿

日本への攻撃②

- 攻撃手法はDDoSと考えられ、同時間帯に対象サイトのうちのいくつかが閲覧できない状態であったことを、弊社でも確認している。
- これらのサイトの多くは、福島原発海洋放出に反対するアノニマスの攻撃キャンペーンで2021年4月に公開された攻撃対象リストに記載されていた。同アクターが主張するイスラエル製のサイバーセキュリティシステムの利用とは無関係のようにみえる。





ミャンマー日本商工会議所のWebサイトへの攻撃を主張する投稿

鴻池組のWebサイトへの攻撃を主張する投稿

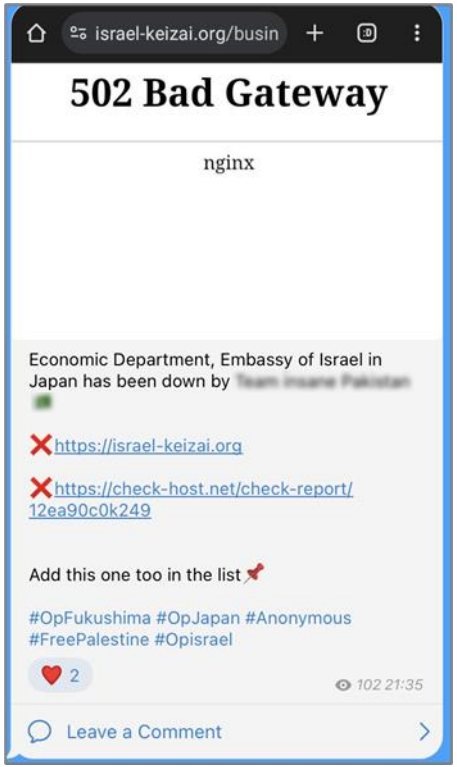
東京スカイツリー、東京都のWebサイトへの攻撃を主張する投稿

J-POWER（電源開発株式会社）のWebサイトへの攻撃を主張する投稿

日本原子力学会のWebサイトへの攻撃を主張する投稿

イスラエル大使館 経済部への攻撃

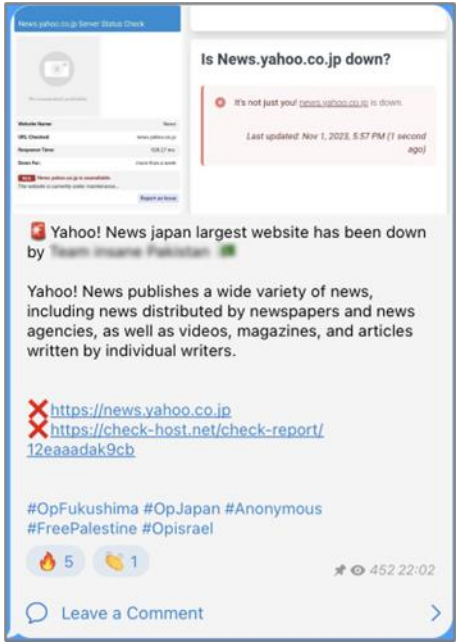
■ 日本の組織への攻撃後、さらにイスラエル大使館 経済部のWebサイトへの攻撃を示す投稿を行った。



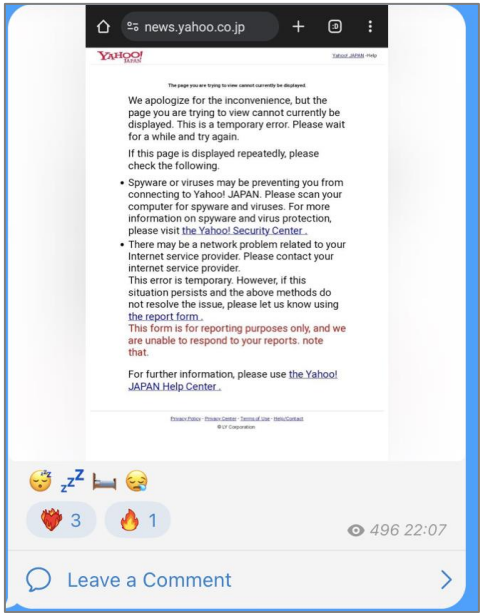
イスラエル大使館 経済部のWebサイトへの攻撃を主張する投稿

Yahoo! ニュースへの攻撃

- さらに日本時間の11月1日22時頃、Yahoo! ニュースのWebサイトへの攻撃を示す投稿を行った。
- 同アクターの示したアクセス可能状況の証跡からすると、日本からのアクセスに問題はなかったものの海外からアクセスできない状況が発生していたと考えられる。



Yahoo! ニュースのWebサイトへの攻撃を主張する投稿



同アクターが投稿した、Yahoo! ニュースで表示されたエラーメッセージ

同アクターが投稿した、日本など一部の国を除いて海外からアクセスできない状況を示す証跡

攻撃対象　一覧表

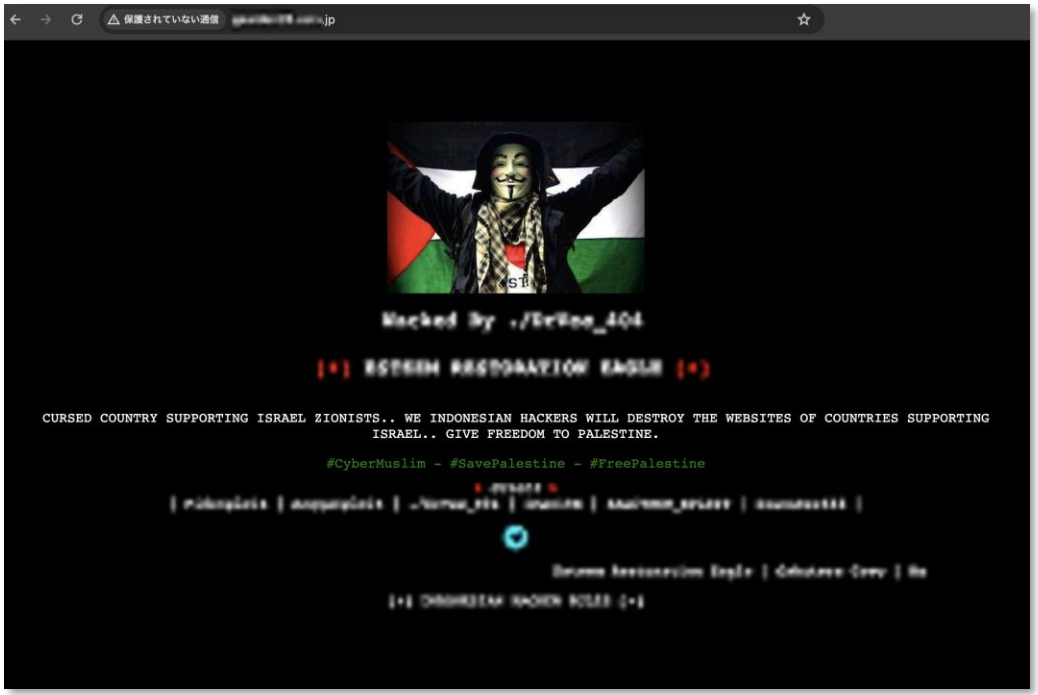
■ 以下は、11月1日に同アクターが攻撃を主張した組織の一覧である。(※2023年11月2日10時時点 確認)

組織	URL	福島原発処理水海洋放出に関する攻撃対象リストへの記載
NTTPCコミュニケーションズ	https://www.nttpc.co.jp	—
自民党	https://www.jimin.jp/	有
経団連	https://www.keidanren.or.jp/	有
衆議院議員 菅義偉	https://sugayoshihide.gr.jp/	有
衆議院議員 茂木としみつ	https://motegi.gr.jp/	有
ミャンマー日本商工会議所	https://jccim.org/	有
鴻池組	https://www.konoike.co.jp/	有
外務省	https://www.mofa.go.jp/	有
東京スカイツリー	https://www.tokyo-skytree.jp/	有
東京都	https://www.metro.tokyo.lg.jp/	有
J-POWER（電源開発株式会社）	https://www.jpower.co.jp/	有
日本原子力学会	https://www.aesj.net/en/	有
イスラエル大使館 経済部	https://israel-keizai.org	—
Yahoo! ニュース	https://news.yahoo.co.jp	—

その他の日本に関する攻撃／攻撃予告

その他の日本に対する攻撃／攻撃予告①

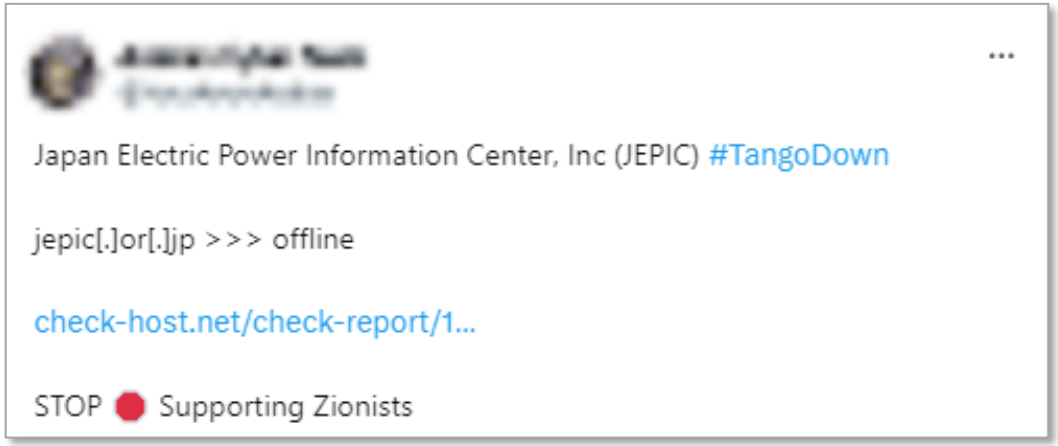
- 10月31日、インドネシア系のハッカーグループが、日本のホスティングサービスを利用していると考えられる２つのサイトを攻撃した。
- パレスチナを支持する文言や画像が表示されるよう、改ざんを行っている。



10月31日に改ざんされたWebサイトの一つ

その他の日本に対する攻撃／攻撃予告②

■ 11月2日、アラビア系のハッカーグループがSNSに、一般社団法人 海外電力調査会（JEPIC）へのDDoS攻撃を示唆する投稿を行った。



JEPICへの攻撃を示唆する投稿

その他の日本に対する攻撃／攻撃予告③

- 11月2日、アラビア系のハッカーグループが投稿を行い、日本の有名企業「YOKAJAWA」（横河電機とみられる）の従業員や科学研究、契約等に関する機密情報を入手したと主張した。
- 共に投稿された動画には、横河電機製のデータ収集機器のWebインターフェイスを操作している様子が表示されている。

横河電機への攻撃を主張する投稿

【参考】https://socradar.io/reflections-of-the-israel-palestine-conflict-on-the-cyber-world/

その他の日本に対する攻撃／攻撃予告④

- 11月4日、パキスタン系のハッカーグループが mail.ace.setagaya.tokyo.jp と town.okutama.tokyo.jp を落としたと宣言。
- 当該サイトにアクセスすると、確かにエラーが表示され、DDoS攻撃が成功しているかのように見える。
- しかし上記のURLの冒頭に「www」を付けると、正規のサイトが正常に表示される。
- エラーが表示されるURLを記載することで、攻撃が成功したように見せかけている可能性が考えられる。

mail.ace.setagaya.tokyo.jp と town.okutama.tokyo.jp への攻撃を示唆する投稿

その他の日本に対する攻撃／攻撃予告⑤

- 11月6日、日本政府がイスラエルを支持しているとして、インドネシア系の２つのハッカーグループが警告を発した。さらに政府のWebサイトについてハッキングを行うことを宣言した。

日本政府に対して警告し、ハッキングを宣言する投稿（一部）

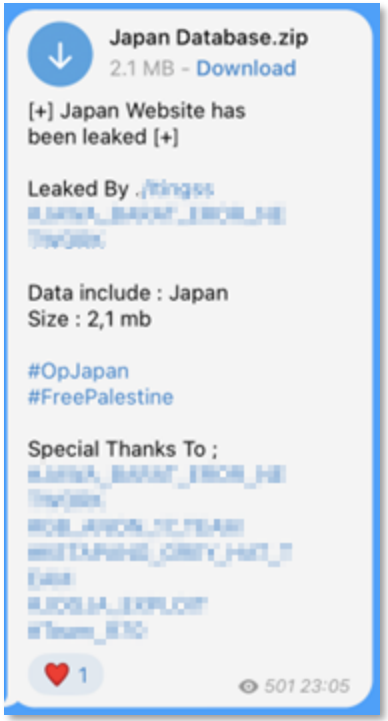
その他の日本に対する攻撃／攻撃予告⑥

- 11月6日、インドネシア系の２つのハッカーグループが理化学研究所のサイト（riken.go.jp）を攻撃し、27GBのデータを盗んだと主張した。
- サンプルデータの一部を投稿しているが、そのデータが本物であるか、また、実際に攻撃を行ったかどうかは不明である。

理化学研究所への攻撃を主張する投稿

その他の日本に対する攻撃／攻撃予告⑦

- 11月7日、インドネシア系のハッカーグループが、日本のWebサイトから漏洩したと主張する17件のファイルを公開した。
- 同グループは漏洩情報と主張しているが、いずれも公開情報と考えられる。



日本のWebサイトからの漏洩データを公開する投稿

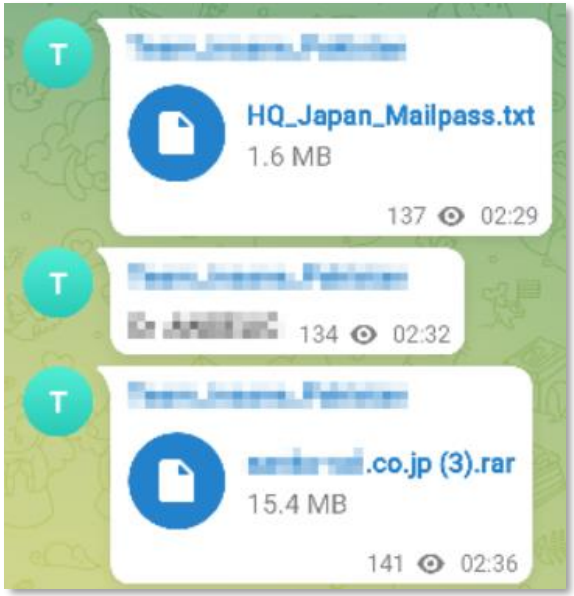
その他の日本に対する攻撃／攻撃予告⑧

■ 11月7日、パキスタン系のハッカーグループが日本最大のカジノ／ギャンブルサイトが落ちたと投稿し、DDoS攻撃を実行したことを示唆した。

カジノ／ギャンブルサイトへの攻撃を示唆する投稿

その他の日本に対する攻撃／攻撃予告⑨

- 11月9日、パキスタン系のハッカーグループが、日本に関する２つのデータを投稿した。
- これはイスラエル・ハマスの衝突以前の8月28日に、インドネシア系と考えられる別のグループが投稿したデータと同一であった。
- 自グループのサイバー攻撃が成功したかのように見せかけている可能性がある。



日本に関する２つのデータの投稿

その他の日本に対する攻撃／攻撃予告⑩

- 11月10日、パレスチナ系のハッカーグループが「日本はイスラエルを支持することに賛成票を投じた。日本が国連で停戦に反対したため、今もパレスチナ人が殺されている」と述べ、約50件の組織や個人を含むターゲットリストを投稿した。


Japan voted in support of Israel. Today Palestinians are getting killed because Japan opposed a ceasefire at the UN.

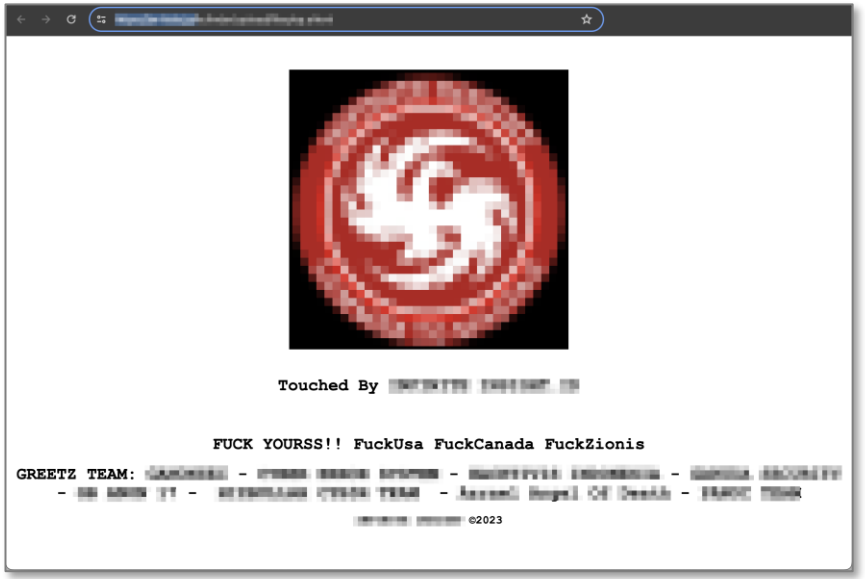
All targets.

投稿したターゲットリスト

その他の日本に対する攻撃／攻撃予告⑪

- 11月10日、インドネシア系のハッカーグループが日本の2件のサイトをハッキングしたと主張する投稿を行った。
- 投稿されたURLにアクセスすると、同グループのロゴマークや攻撃的な文言等が表示されていた。

日本の２件のサイトへの攻撃を示唆する投稿

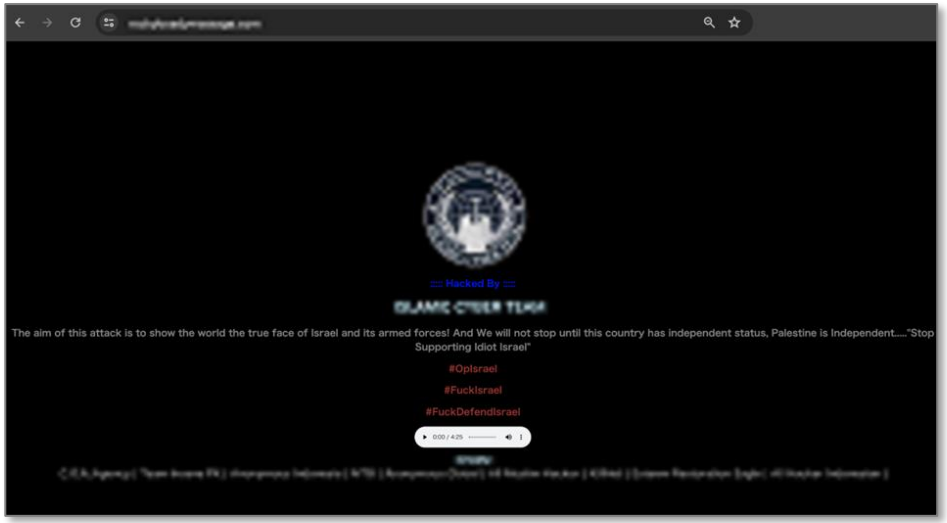


ハッキングされたWebページ

その他の日本に対する攻撃／攻撃予告⑫

- 11月18日、インドネシア系のハッカーグループが、日本のWebサイトをハッキングしたと投稿。
- 現在もサイトはアクセスできない状況であり、アーカイブデータによると日本語のサイトのようであるが、詳細は不明。

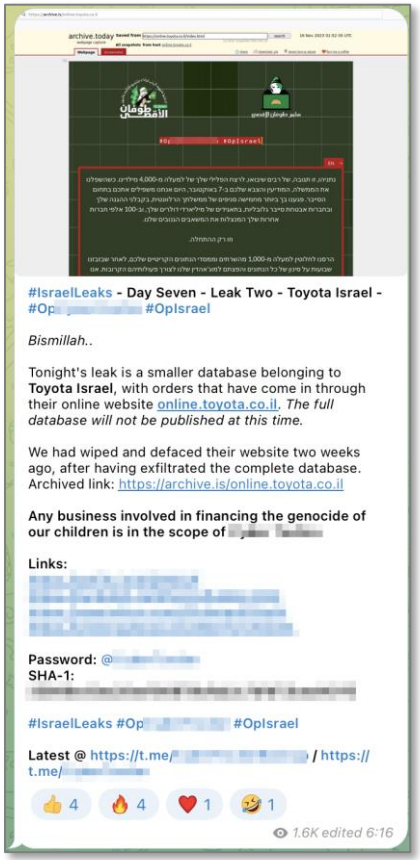
攻撃を主張する投稿



ハッカーグループにより改ざんされたWebサイト

その他の日本に対する攻撃／攻撃予告⑬

- 12月4日、アラビア系のハッカーグループが「トヨタ・イスラエル」のWebサイトのデータを消去し、改ざんを行ったと投稿。
- 窃取したと主張するデータベースの一部の公開を開始した。

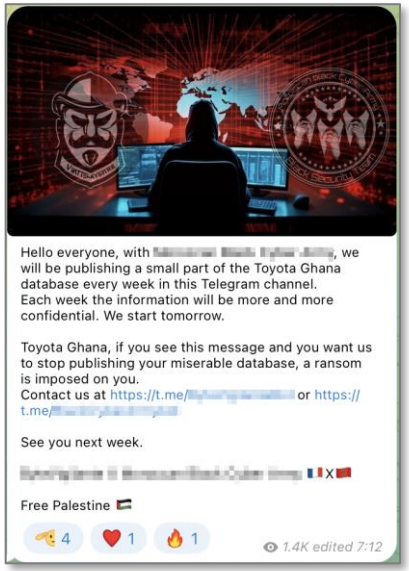


トヨタ・イスラエルへの攻撃を主張する投稿

その他の日本に対する攻撃／攻撃予告⑭

- ガーナがイスラエルと（経済や貿易において）つながっているとして、12月５日、フランス系のハッカーグループとモロッコ系のグループが連名で「トヨタ・ガーナ」のデータベースにハッキングを行ったこと、データのサンプルを公開するつもりであることを投稿した。
- ７日の新たな投稿では、トヨタ・ガーナに対し、データの公開中止と引き換えに身代金を課すと述べ、２グループの連絡先を示した。なお、データの公開は確認されていない。

12月5日　トヨタ・ガーナへの攻撃を主張する投稿



12月7日　トヨタ・ガーナに対し、データの公開中止と引き換えに身代金の支払いを課すと述べる投稿

更新履歴

2023年11月2日　第1版発行

2023年12月22日　第2版発行（P11以降において加筆・修正）


NTT
Security Holdings