NTT Security Holdings

ハクティビスト新時代
2023年 ハクティビストの活動のまとめ

NTTセキュリティ・ジャパン
OSINTモニタリングチーム
2024年1月30日

エグゼクティブサマリー

- 2023年の日本では、ハクティビストによる5つの攻撃キャンペーンが確認された。
  - 渋谷区の路上生活者に対する立ち退き行政代執行への抗議
  - ウクライナ支援に対する抗議
  - 入管法改正に対する抗議
  - 福島原発処理水の海洋放出に対する抗議
  - イスラエルとハマスの軍事衝突に関連する抗議
- 2023年の活動では福島原発処理水の海洋放出が半数近くを占めたが、残りの過半は遠方の地政学的な衝突に関連している。
- ハクティビストの活動は近年停滞していたが、急激に復活している。また、アノニマス中心の活動から変化を見せている。
- 攻撃の中心はDDoSであるが、Webサイトの改ざんが増えている。また、イスラエル・パレスチナ周辺では制御系システムへの攻撃が増えており、注意が必要である。
- サイバー犯罪に加担するグループやサイバー犯罪者がハクティビストに加担する活動、国家からの支援が疑われるハッカーグループの出現など、他のハッカーカテゴリーとの境界があいまいになっている。

2023年に観測された日本を狙ったハクティビストの５つの攻撃キャンペーン

路上生活者に対する立ち退き行政代執行への抗議 #OpSafeWinter

- 再開発事業を進めていた東京都渋谷区は2022年12月、 区立美竹公園からの立ち退きに応じない路上生活者らに対し行政代執行を実施し、この措置に対してアノニマスは抗議活動を始めた。
- 2023年1月３日から９日にかけて複数のアノニマスが、日本組織やそのサイトに対してDDoS攻撃等（少なくとも計11件）を行った。

渋谷区公式サイトをダウンさせたことを主張するアノニマスの投稿

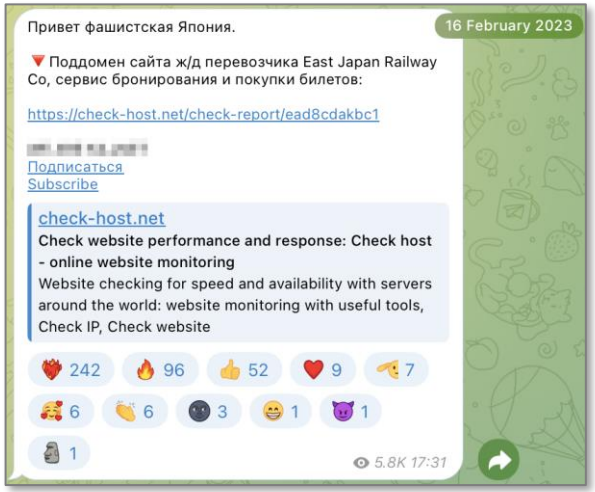
個人情報を含むデータベースを公開したことを示唆するアノニマスの投稿

ウクライナ支援に対する抗議

- ロシアのウクライナ侵攻に関連して、ウクライナを支援する日本に抗議する目的で、親ロシアのハクティビストグループが2022年9月に、日本の組織に対してDDoS攻撃を開始した。2023年も継続して攻撃が確認された。
- 2月から6月にかけて、2つのグループが石油連盟やJR東日本等に対して、計22件のDDoS攻撃を実行したことを主張した。

石油連盟への DDoS攻撃を示唆する投稿

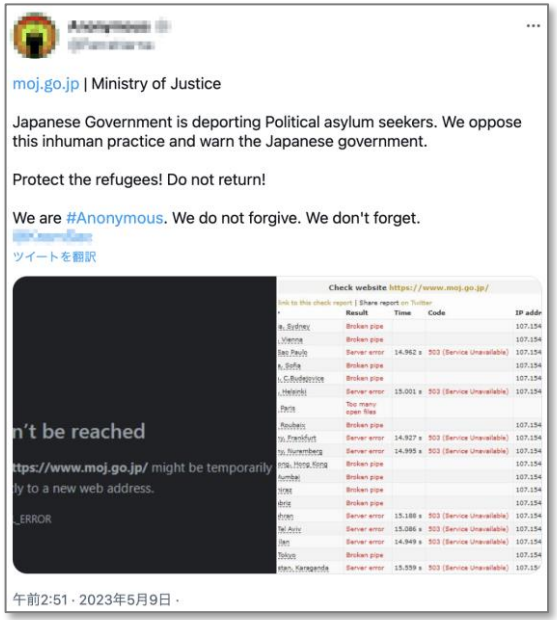
石油連盟による被害発表



JR東日本へのDDoS攻撃を示唆する投稿

入管法改正に対する抗議

- 2023年春、外国人の強制送還の規制の見直しを含む「出入国管理及び難民認定法」(入管法) の改正案が衆参各議院で審議が行われた。アノニマスは本案に抗議して、活動を行った。
- 5月9日、本改正案が衆議院で可決される直前、アノニマスは法務省サイトをダウンさせたことを示唆する投稿を2回行った。



法務省サイトをダウンさせたことを示唆する投稿

今回の攻撃の報道を伝える投稿

福島原発処理水の海洋放出に対する抗議
#OpFukushima

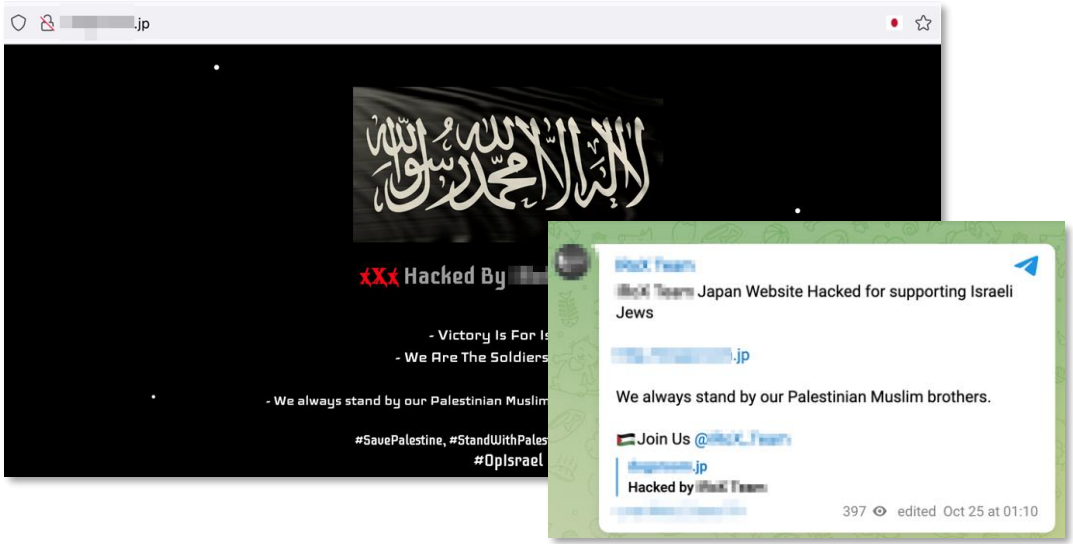
- 福島原発処理水の海洋放出に反対するアノニマスが、官民の日本の組織等に対し抗議活動を行った。
- 日本政府が具体的な海洋放出時期の見通しを示した2023年1月から放出が実施された８月まで、SNSにて攻撃を示唆／主張する投稿が少なくとも64件確認された。攻撃手法はDDoS の他、MySQLサーバーに関連するもの、ネットワークカメラへの不正アクセス、大量のサイト改ざん等であった。

福島市への攻撃を示唆する投稿

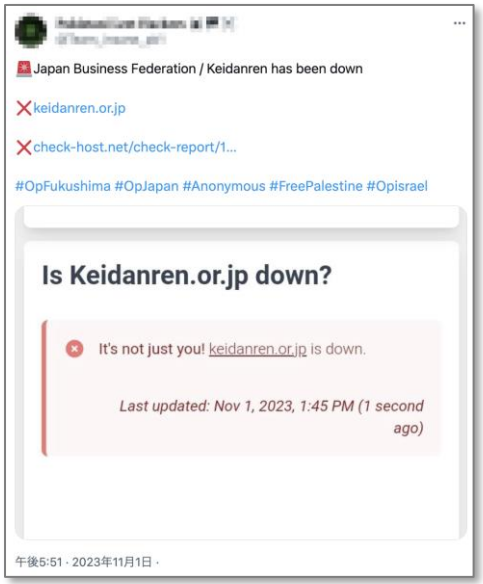
改ざんされたルーターのログイン画面

イスラエルとハマスの軍事衝突に関連する抗議

- ロシアが国連安保理に提出したイスラエル・ハマスの停戦案に対し、 10月７日、日本は米英仏と共に反対を表明。これに関して、親パレスチナのハッカーグループが日本に対して抗議活動を開始した。
- 10月25日から12月5日までの間、日本の事業者のサイトの改ざんや、外務省、経団連、衆議院議員等のサイトに対するDDoS攻撃の実行を示唆／主張する投稿が少なくとも計27件、確認されている。



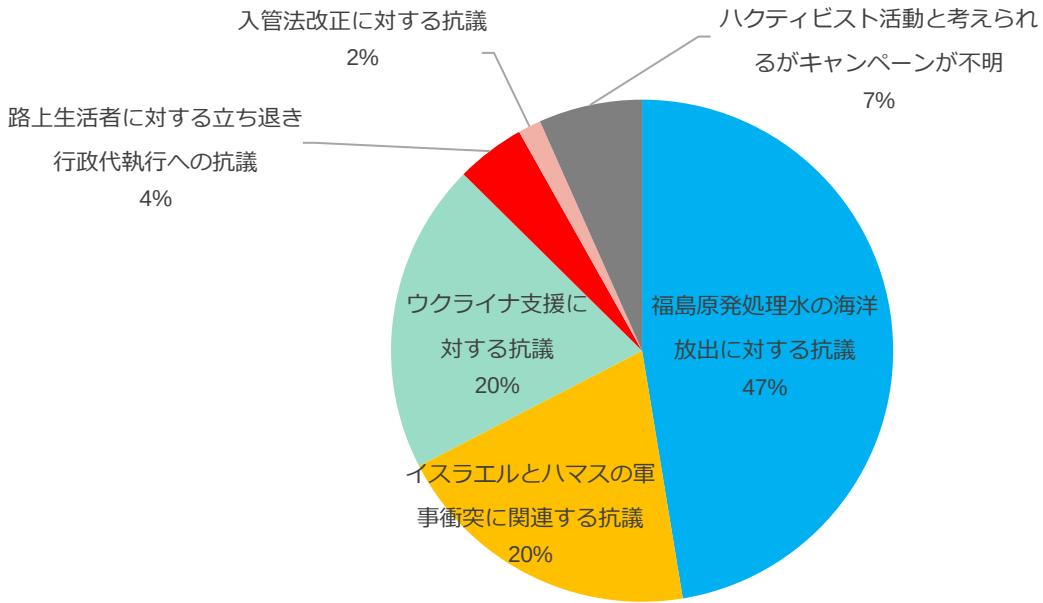
改ざんされた日本の事業者のサイト、および犯行を主張する攻撃者の投稿



経団連へのDDoS攻撃を示唆する投稿

2023年の活動の内訳

- 2023年にハクティビストが日本の組織やサイトへの攻撃を主張/示唆するSNSでの投稿は135件確認された。
- 福島原発処理水の海洋放出に関する投稿が半数近くを占めたが、残りの多くは遠方の地政学的な衝突に関連している。

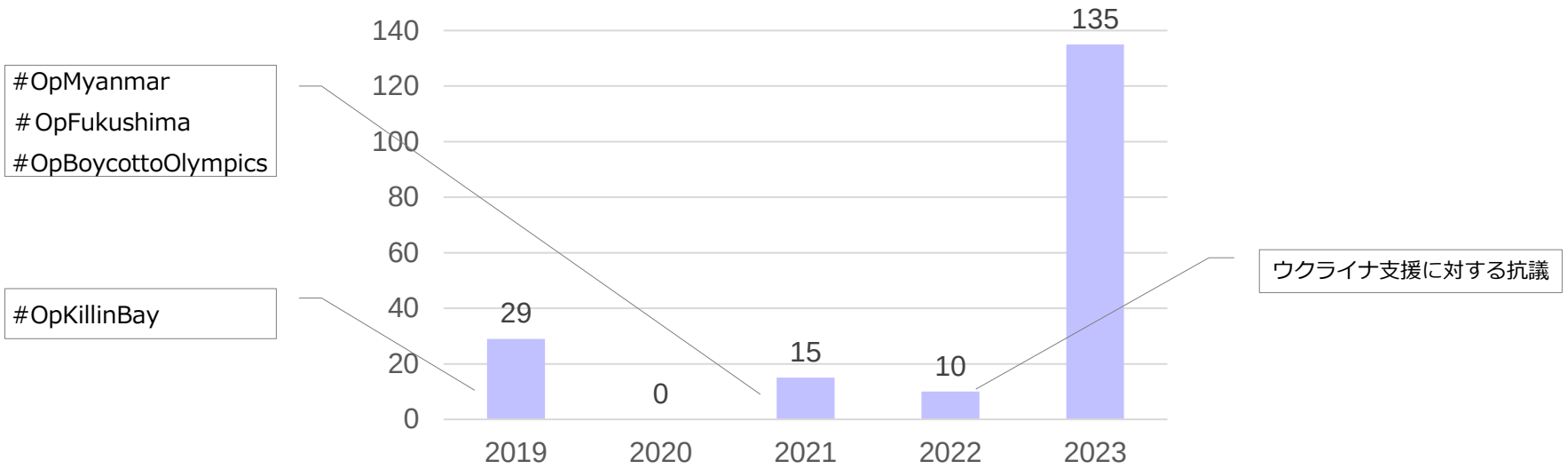


SNSでのハクティビストによる日本（関係）の組織やサイトへの攻撃主張／示唆の投稿件数の攻撃キャンペーン別の内訳（2023年）

過去５年間で確認された活動の推移

過去５年間で確認された日本での活動の推移

- 2010年代後半から、ハクティビストの活動は世界的に停滞しており、日本でもサイバー攻撃は散発的な状況が続いていた。
- 2023年は近年見ないほど、盛んな活動が観測され、ハクティビストの復活が印象付けられた1年であった。



SNSでのハクティビストによる日本（関係）の組織やサイトへの攻撃主張／示唆の投稿件数の推移

ハクティビスト新時代
～復活と変化～

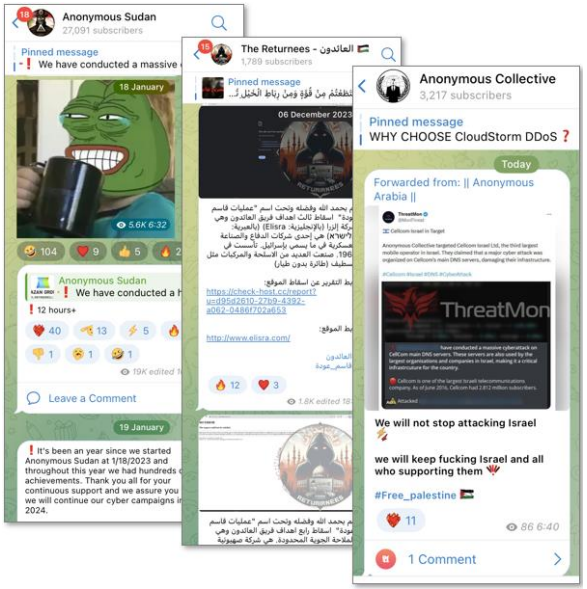
2022年からの変化

- 2021年までのハクティビストの国際的な活動はアノニマスが主流。
- 欧米出身者が多いアノニマスでは、西欧的な普遍的な価値観（人権問題、環境問題、動物愛護）に基づくキャンペーンが共感を得やすかった。
- アノニマスは2010年代前半は活動が活発であったが、逮捕者の続出や内部分裂により、2010年代後半に衰退していた。
- 2022年2月末のロシアのウクライナ侵攻後、再びハクティビストの活動が盛んになっていた。
- ウクライナ侵攻に対するアノニマスのロシアへの攻撃キャンペーンが世界的に報道され、注目を集めたことが契機と考えられる。
- イスラム教国、発展途上国からの攻撃キャンペーンへの参加が増えており、地政学的・宗教的な国際連携が著しく増大。
- 2022年以降、アノニマスも増えているが、アノニマスを名乗らないハクティビストはそれ以上に増えており、混在した状況で各キャンペーンが行われており、全体の様相に大きな変化が起きている。

ハクティビスト新時代
情報発信プラットフォームの変遷とその影響

- 以前はハクティビストが利用するSNSはX（旧Twitter）が定番であったが、多くのハッカーグループがXを利用せず、法執行機関から追跡が困難なプラットフォームとして定評のあるTelegramを利用するようになった。
- 従来のハクティビストはXを使って個人で活動しているケース多かったが、Telegramでは、チャンネルやグループといった枠組みを作ることができ、グループで活動を行うケースが増えている。

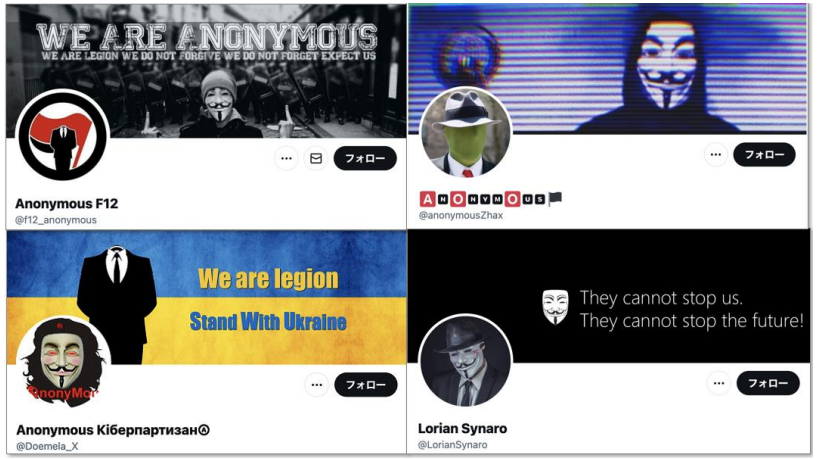
ハクティビスト個人のものとみられる X アカウントのプロフィールページの例：「サイバー活動家」と自称したり、自身の信念、社会問題解決の意思などを表したりしている



Telegramでの投稿例:
人気のあるグループには多数のメンバーが参加しており、コミュニティを形成している

ハクティビスト新時代
カルチャーの変化（アノニマスカルチャーの後退等）

- アノニマス固有の表現や言い回し（We are legion. We do not forgive. We do not forget. Expect us! 等）の利用が減っている。
- プロフィール画像では、以前はガイフォークスのマスクを利用したものが多かったが、グループのロゴを利用するものが増えている。
- 以前は少なかった、グループ名や個人名に出身国/居住国を含めるケースが増えている。

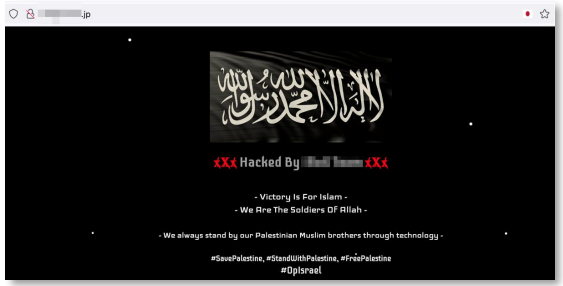


Xでガイフォークスや独特の言い回しを使用するアノニマスのプロフィールページ（部分）の例

Telegramチャンネルで表示されるグループのロゴの例
一部には国名も見られる

ハクティビスト新時代
攻撃の変化①　Webサイトの改ざんの増加

- 多くの攻撃はDDoSによるWebサイトへのサービス妨害であるが、国内外で改ざんの被害が増えている。
- 改ざんされたページの記載方法（ロゴやチームメンバーを連名で記載、政治的主張を記載する）等が、イスラム教国を中心に以前から存在する改ざんハッカー文化を踏襲している。
- 福島原発処理水の海洋放出への抗議では、約1400台のルータのログイン画面が改ざんされた。

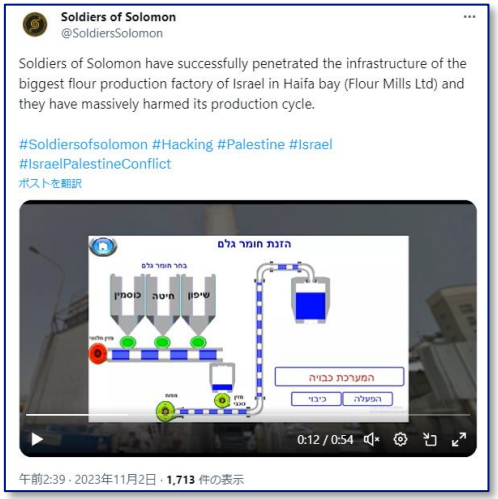


改ざんされたWebページ
チームのロゴ、チームメンバーの連名での記載、政治的主張の記載などの特徴がみられる

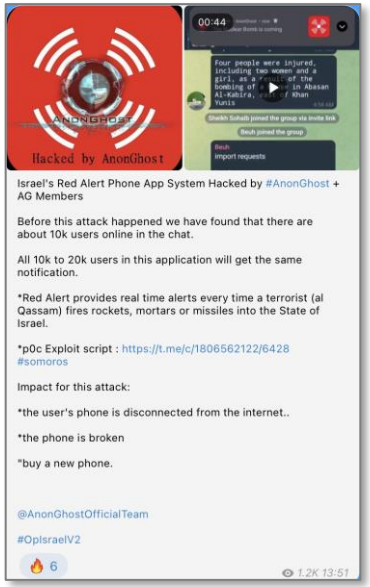
福島原発処理水の海洋放出への抗議のため
に改ざんされたルーターのログイン画面

ハクティビスト新時代
攻撃の変化②　制御系システムを狙った攻撃の増加

- 軍事衝突の当事国周辺（特に、イスラエル・パレスチナ）では制御系システムを狙った攻撃が増えている。
  - イスラエルの電力、水道、小麦粉生産工場、ロケットアラートシステムなどの制御系システムを狙った攻撃が行われた。
  - イラン全土のガソリンスタンドがサイバー攻撃によりサービス停止した。



イスラエルの小麦粉生産工場の生産システムへの攻撃を主張する親パレスチナのハッカーグループの投稿



イスラエルのロケットアラートシステムをハッキングしたと主張する親パレスチナのハッカーグループの投稿

イラン全土のガスポンプを止めたと主張する親イスラエルのハッカーグループの投稿

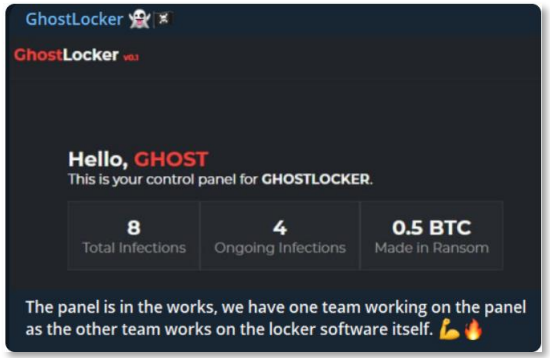
ハクティビスト新時代

他のハッカーカテゴリーとの境界があいまいに①（サイバー犯罪者）

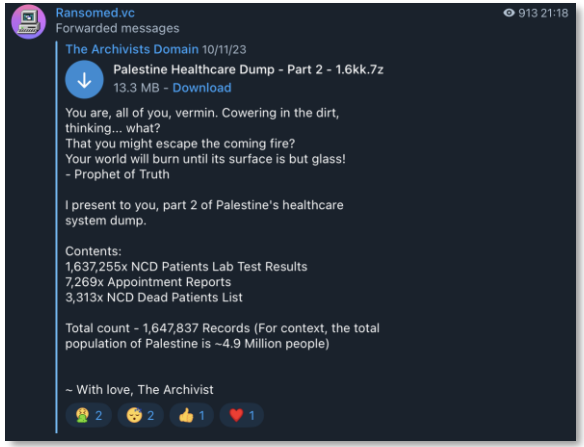
- ハクティビストがサイバー犯罪に加担したり、サイバー犯罪者がハクティビストのキャンペーンに参戦したりする事態が確認された。

➢ ハクティビストとして有名なGhostSecは10月にランサムウェアサービスを開始した。

➢ 同月、ランサムウェアを運営しているRansomed.vcがイスラエル・ハマスの軍事衝突に参戦した。



GhostSecが開始したランサムウェアサービス（GhostLocker）



ランサムウェアグループRansomed.vcがパレスチナの健康保険システムのデータをTelegramに投稿

ハクティビスト新時代

他のハッカーカテゴリーとの境界があいまいに②（国家/国家に準じる組織との関係）

地政学的なキャンペーンでは国家/国家に準じる組織（あるいはAPT）との関係性が疑われる多数のグループが活動を行っていることが指摘されている。ハクティビストを隠れ蓑にして、国家の活動を支援していると考えられる。

- 12月、イスラエルサイバー局はイラン、ヒズボラ、ハマスに所属する15以上のサイバー攻撃グループがイスラエルに対して活動していると報告
- 同月、イスラエル軍事諜報総局と関係があるとみられるグループが実行したサイバー攻撃により、イランのガソリンスタンドの70%がサービス中断を余儀なくされた。

Over 15 cyber attack groups affiliated with Iran, Hezbollah or Hamas are operating against Israel, says National Cyber Directorate

According to a report published by the National Cyber Directorate summarizing the cyber events since the beginning of the war, their main targets include academia, healthcare, water, energy, fuel, transportation and maritime shipping sectors

Omer Kabir 13:11, 25.12.23

ニュース記事：イスラエルサイバー局はイラン、ヒズボラ、ハマスに所属する15以上のサイバー攻撃グループがイスラエルに対して活動していると報告

サイバー攻撃によりサービス中断中のガソリンスタンドで待つ人々（テヘランで）

出典：
https://www.calcalistech.com/ctechnews/article/r1brg1pdp
https://www.reuters.com/world/middle-east/software-problem-disrupts-iranian-gas-stations-fars-2023-12-18/

考察

- 2023年の日本を狙ったハクティビストの活動は近年見ないほど盛んであり、遠く離れたイスラエル・ハマスおよびロシア・ウクライナの衝突に関連するサイバー攻撃が全体の半数近くを占めていた。しかし、日本で現れた影響はこれらのサイバー攻撃の世界的規模から見ると微々たるものであった。このような地政学に関連するハクティビスト活動は世界全体で急激に盛んになっており、活動の主流となっていることは注目に値する。
- 仮に台湾有事等、日本周辺の地政学的な問題が進展した場合でもハクティビストによる国際的なキャンペーンが展開され、様々な国々からハッカーグループがそれぞれの陣営に分かれて参戦することが想定される。
- このようなハッカーグループの中には国家等が関与するグループが含まれる可能性があり、自国に優位な状況に扇動したり、ハクティビストの名を借りて過激なサイバー攻撃を行うことなどが懸念される。
- ハクティビストの内面は大きく変化しており、従来のアノニマス中心の活動とは異なる様相を見せている。
- サイバー攻撃は依然DDoSが中心であるが、Webサイトの改ざんが増えており、更に地政学的な衝突の当事国周辺では、制御系システムを狙った攻撃が確認されており、脅威は増している。
- ハクティビストの活動は新しい時代に突入したと考えられ、攻撃手法や活動形態等が変化しながら、大きく脅威を増している。今後も継続的な観察と注意が必要である。


NTT
Security Holdings