



NTT

Security Holdings

パリオリンピックを狙ったサイバー攻撃

NTTセキュリティ・ジャパン

OSINTモニタリングチーム

2024年8月6日

概要

- 世界的な注目を浴びるパリオリンピックを狙ったサイバー攻撃が行われることは多くのセキュリティ研究者等によって予測されてきた。実際に7月26日にパリオリンピックが開催されると、前後して、様々なサイバー攻撃が発生している。
- 攻撃は大きく分けて三つの動機に基づいている。
 - ロシアがオリンピックに参加できないことへの抗議
 - イスラエルがオリンピックに参加していることへの抗議
 - 開会式のパフォーマンスへの抗議

パリオリンピックへの参加状況

- パリオリンピックは、204の国・地域と難民選手団が参加している。ウクライナ、イスラエル、パレスチナから選手団が参加しているが、ロシアは参加していない。
- IOCによる、戦争に対する制裁が2022年2月から継続中であるため、今大会への国としてのロシアおよびベラルーシの参加は認められていない。
 - 国旗や国歌等の使用禁止等が定められている「個人中立アスリート」（AIN）としての個人参加は認めている。
 - AINは、サッカー等の団体競技には適用されない。

出典：

<https://olympics.com/ioc/news/strict-eligibility-conditions-in-place-as-ioc-eb-approves-individual-neutral-athletes-ains-for-the-olympic-games-paris-2024>

<https://www.yomiuri.co.jp/olympic/2024/20240727-OYT1T50074/>

ロシアがオリンピックに参加できないことへの抗議活動

親ロシアのハッカーグループがパリオリンピックを標的と宣言



Security Holdings

- オリンピック開催を翌月に控えた6月23日、親ロシア派のハッカーグループがパリオリンピックを標的とすることをテレグラムにて宣言した。
- 宣言から3時間後、グループはフランスの国際映画祭のWebサイトにDDoS攻撃を実行したことを示唆する投稿を行った。

右：パリオリンピックを標的と宣言する投稿

メッセージ和訳：

ロシアのハッカーたちはオリンピックに参加することに同意した。
ニュートラルな立場で。
フランスのサイトに対する「DDoS攻撃」という新しいスポーツで。

親愛なるサイバー戦士の皆さん！

今日という日をフランスに捧げましょう！
2024年のオリンピック出場に向けて、トレーニングは最終段階に入っています！

マクロン氏が約束し、本日開催される汚染されたセーヌ川での水泳 ※ を機に、私たちはマクロン氏の活動に不満を抱くパリ市民の抗議活動を支援し、更に多くの下水を川に流すことを手伝います。

マクロン氏に、彼のオリンピックがあらゆる意味でどれほどくだらないものであるかを見せてやろう！

セーリングを楽しんでください、エマニュエル（マクロン）！

※ この日にパリ市長がセーヌ川で泳ぐ予定であったが、5月の大雨による川の増水および議会選挙のため、延期された。



パリオリンピックスポンサーへのDDoS攻撃予告



- 現地時間7月26日にパリオリンピックが始まった。7月29日、同グループは大会への批判とともに、オリンピックのスポンサーへの大規模なDDoS攻撃を予告する投稿を行った。

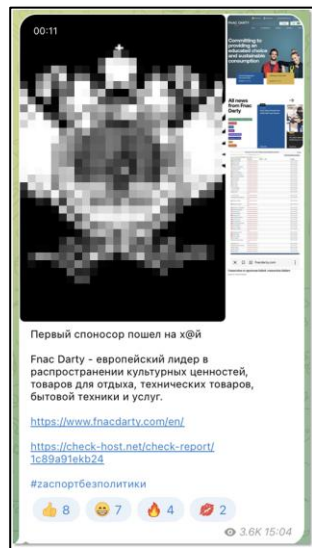


このイベントに参加することはなく、ロシアのメディアで放送する必要もありません。むしろ、オリンピックのスポンサーに対してDDoS攻撃を行うべきです。最新のアナウンスや投稿については、私たちのTelegramチャンネルを確認してください。

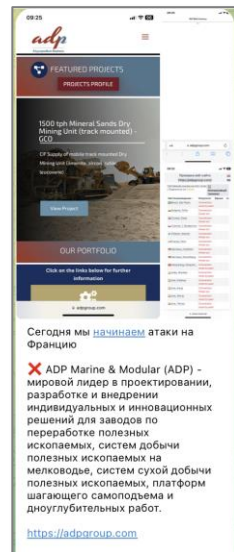
パリオリンピックスポンサーへのDDoS攻撃を予告する投稿

親ロシアのハクティビストによるサイバー攻撃

- 同日、同グループはスポンサーへの攻撃予告の後に Fnac Darty 社(オフィシャルサポーター)へのDDoS攻撃を示唆する投稿を行った。
- 続けて、同じく別の親ロシア系ハッカーグループ がフランスへの攻撃を宣言。オフィシャルパートナーの Groupe ADP (ADP Marine & Modular) 社への DDoS攻撃を示唆する投稿を行った。
- その後も、オフィシャルパートナー : ArcelorMittal社、オフィシャルサポーター : Aquatigue Show社およびArena社への攻撃を主張した。



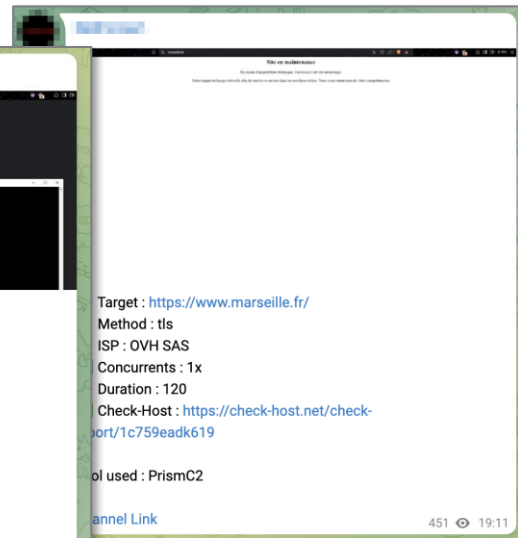
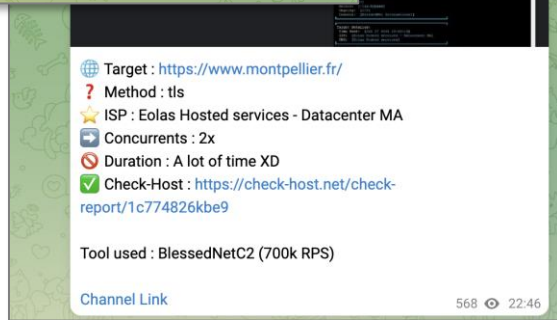
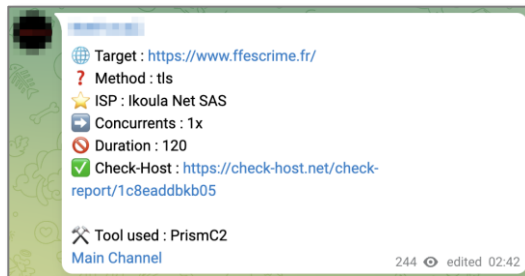
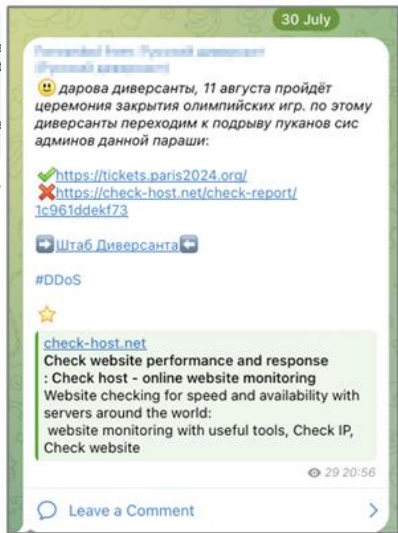
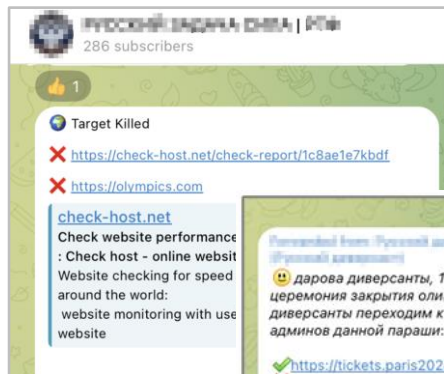
Fnac Dartyへの攻撃を示唆する投稿



Groupe ADPへの
攻撃を示唆する投稿

その他の親ロシアのハッカーグループの攻撃

- その他の複数の親ロシアのハッカーグループも、オリンピック関係組織やフランスの地方自治体等へのDDoS攻撃を行ったことを主張している。

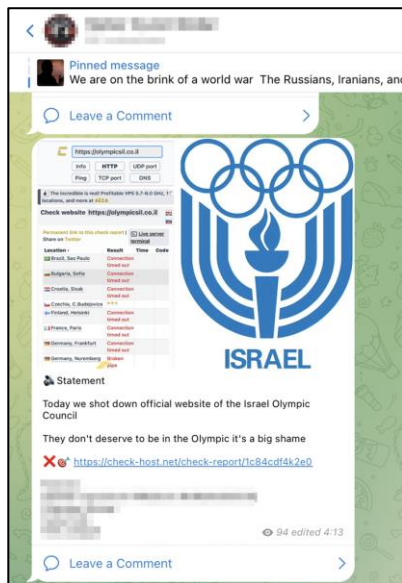


フランスフェンシング連盟、モンペリエ市、マルセイユ市への攻撃を主張する投稿

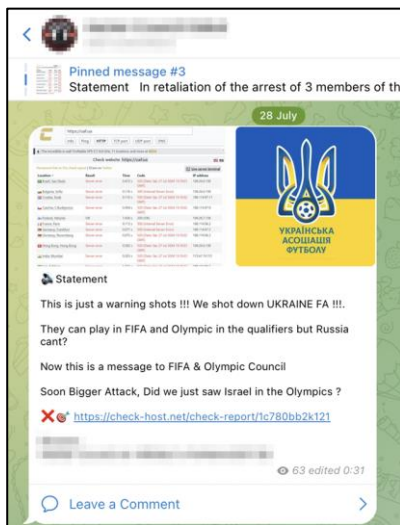
オリンピック公式サイトおよびチケット販売サイトへの攻撃を主張する投稿

イスラエルのオリンピック関連組織への攻撃

- 親ロシアのハクティビストが、イスラエルのオリンピック関連組織へのDDoS攻撃を行ったことを主張している。
- ロシアが参加できないパリオリンピックにイスラエルが参加していることへの抗議を、攻撃の理由としている。



イスラエルのオリンピック評議会への
攻撃を示唆する投稿



ウクライナサッカー協会への
攻撃を示唆する投稿



ロシアとイスラエルの差について
「ダブルスタンダード」と表現している投稿

イスラエルがオリンピックへ参加していることへの抗議活動

- ある親パレスチナのハッカーグループは開会式の映像配信をハイジャックし、イスラエルの入場シーンの代わりにガザでの残虐行為を放映させたと主張している。
- 別のグループは、大会出場選手の個人情報等の暴露を繰り返し行っている。情報の一部はイスラエルのスポーツ評議会から窃取した機密情報と考えられている。



ハッカーグループの公式チャンネルに投稿された動画より

街頭の大型ビジョンに映し出された、開会式を撮影したと考えられる映像で、イタリア選手団に続いてイスラエル選手団の入場シーンが表示されると、ハッカーグループのロゴに切り替わったように見える。その後イスラエルを非難する映像が続く



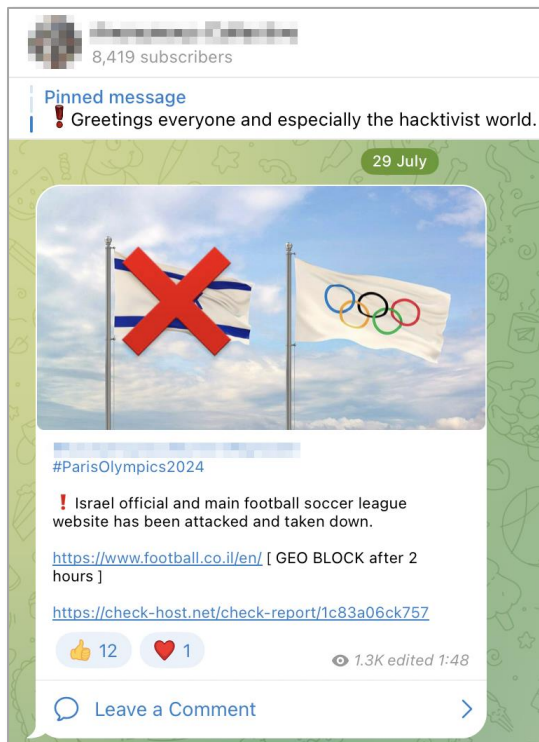
イスラエルの選手の個人情報を暴露する投稿

親パレスチナのハッカーグループによる抗議活動②



Security Holdings

- 別の親パレスチナのハッカーグループは、イスラエルのサッカーリーグと水泳協会のサイトへの攻撃を示唆する投稿を行った。



イスラエルのサッカーリーグのWebサイトへの攻撃を示唆する投稿

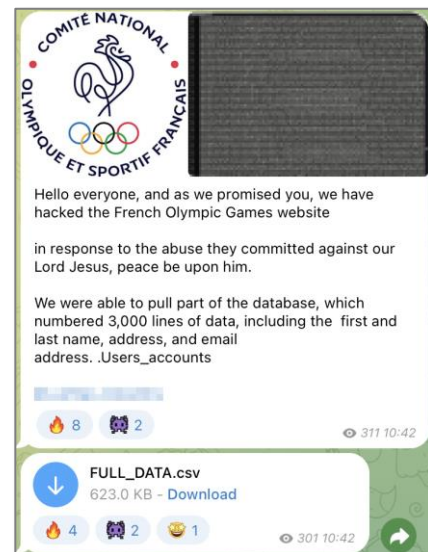


イスラエルの水泳協会のWebサイトへの攻撃を示唆する投稿

開会式のパフォーマンスに対する抗議活動

開会式のパフォーマンスに対する抗議活動

- あるイスラム系のハッカーグループが7月28日からフランスのWebサイトの改ざん、情報窃取などのサイバー攻撃を繰り返し行った。
- パリオリンピック開会式のパフォーマンスにおいてイスラム教で預言者とされるイエスが侮辱されたと述べている。



フランスのWebサイトをハッキングしたとの投稿[7月28日] (左)、および改ざんしたサイトの例 (右)

フランス国立オリンピック・スポーツ委員会のWebサイトをハッキングし、データベースの一部を取り出したと主張する投稿 (7月31日)

まとめ

- DDoSによるサービス妨害、Webサイトの改ざん、情報窃取と暴露など多くのサイバー攻撃が行われているが、幸いにも現在までのところ大会の運営に影響を与えるような大きな被害は確認されていない。
- 国際的なイベントであるオリンピックは自らの主張を広めたいハッカーグループにとって格好の場であり、今後も攻撃が繰り返されると考えられる。
- 攻撃範囲はオリンピック関連組織、フランスおよびイスラエルの国内に留まっているが、親ロシアのハッカーグループはオリンピックのスポンサーを攻撃すると宣言し、攻撃を繰り返しており、日本を含むスポンサー企業への攻撃が行われることが懸念される。



NTT

Security Holdings