サイバーセキュリティレポート

2024.08

NTT セキュリティ・ジャパン株式会社
コンサルティングサービス部　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 8 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『北朝鮮 IT 技術者が仮想通貨プロジェクトにて、月 30 万ドル以上を稼ぐ』

- 身分を偽った 21 名の北朝鮮 IT 技術者が複数の仮想通貨プロジェクトに雇われていることを、仮想通貨の取引履歴を調査している ZachXBT という人物が突き止めた。
- 21 名の仮想通貨口座を合計すると、月に約 30～50 万ドルの入金があり、その一部は FBI から指名手配されている人物と関連する口座に送金されていた。大量破壊兵器や弾道ミサイルを開発する資金源になっていると見られる。
- 仮想通貨プロジェクトに IT 技術者を送り込むことは、労働の対価として仮想通貨による定期収入を得られることやプロジェクトから短期間で仮想通貨を窃取できる可能性を考慮すると、北朝鮮が資金を調達する／増加させるための効率的な手段になっていると言える。

第 2 章『DDoS 攻撃代行サービス利用の容疑者、国際共同捜査で逮捕』

- DDoS 攻撃を、海外の代行サービスを利用して行ったとして、警察庁サイバー特別捜査部は、8 月 6 日に電子計算機損壊等業務妨害容疑で男を逮捕した。
- 特別な知識がなくても、攻撃先を指定するだけで誰でも利用できる DDoS 攻撃の有料代行サービスがあり、今回は「Bootyou」というサービスが利用されていた。
- DDoS 攻撃では、インターネットに公開されている第三者のサーバーを悪用して攻撃用の通信を増幅させる、「増幅攻撃」がよく用いられることが知られている。自社の公開サーバーで、DNS、SNMP、NTP など増幅攻撃に利用されるサービスを使う場合は、適切な設定を行い、知らない間に犯罪行為に加担、あるいはそのような行為を助長することのないように心がけたい。

第 3 章『パリオリンピックに関連したサイバー攻撃』

- パリ 2024 オリンピック大会の開催前から開催中にかけ、ハクティビストによる DDoS 攻撃から、サイバー犯罪者による詐欺、大会関連施設を巻き込んだランサム攻撃まで、様々なサイバー攻撃がみられた。
- 閉会から間もない 8 月 13 日、フランス当局は大会期間中に 140 件以上のサイバー攻撃が確認されたが運営に支障が出ることは無かったとの見解を発表した。
- 大会の運営に支障をきたすような攻撃は確認されなかったものの、開催に便乗して主張を広めようとするような活動が目立った今大会の経験は、今後の大規模な国際イベントの参考になると思われる。

1. 北朝鮮 IT 技術者が仮想通貨プロジェクトにて、月 30 万ドル以上を稼ぐ

1.1. 概要

8 月 15 日、ZachXBT と名乗るリサーチャーが、名前や国籍／所在地、経歴などの身分を偽った北朝鮮 IT 技術者 21 名が複数の仮想通貨プロジェクトに雇われていると発表した[1]。その中で、技術者たちが月に合計約 30～50 万ドル相当の仮想通貨による給与を得ていたことを明らかにした。

図 1 北朝鮮 IT 技術者が使用した偽造 ID[1]

1.2. 仮想通貨プロジェクトに雇用された北朝鮮 IT 技術者の発見

8 月初旬に、ある仮想通貨プロジェクトにおいて、開発していたプログラムに悪質なコードが組み込まれ、プロジェクトが所持していた 130 万ドル相当の仮想通貨が盗まれる事件が発生した。プロジェクトには、複数の北朝鮮 IT 技術者が、そうとは気づかれないまま雇われていた。

この事件について、ZachXBT が調査の手助けを求められた。ZachXBT は、ブロックチェーンに記録された仮想通貨の取引履歴を調査し、匿名で情報発信を行っている人物である。ZachXBT が様々な仮想通貨プロジェクトについても調査したところ、計 21 名の北朝鮮 IT 労働者が 25 以上のプロジェクトに雇用されていることを発見した。

彼ら 21 名は、名前や国籍／所在地を偽り、履歴書や GitHub アカウントの活動履歴に華麗な経歴を記載していた。彼らは人材派遣会社による紹介や、先に雇われた者が他者にポストを紹介するといった方法により、プロジェクトに入り込んでいた。

[1] 出典：X『@zachxbt』
https://x.com/zachxbt/status/1824047425822310580

Fake Name	Payment address	Fake Location	Github	Email
Jason Kwon	0x4b94ba1528636a699dab486a217d39bb7ce21d75 0x1075e62bfacbb44e31d7a5719e55c7d16fe7d35d 0x7969b188f7dc6bf80d68f224ac3454dafe6f6d5d 0xa771609C5C56048f146d2C794c87DB946bfF27Cf 0x90cf352dDAF171d41A6DEd1d54cEDA4005047c93 0x72c70980ACddE7a5C9437050E73E7d07fBf21D25	Canada	https://archive.ph/J347l https://archive.ph/WIu3i	0xm00neth@gmail.com
Willie Lee	0x97e36fAE76cD7ef7cC1213927A9A4E10a61CdD8d	California, US	https://archive.ph/SjJfK	willie.lee226@gmail.com
Naoki Murano	0x6188a9e76794e7cb337b8E5a2B91808Ce34Fc6D1 0x85e0504fcd7981baa68774431099c5e2dcf074dd	Tokyo, Japan	https://archive.ph/96QVA	naokimurano@outlook.com
Sano	0xef2a0324cfaa0100db9def8ef31c6e23bc4f9258	-	https://archive.ph/KMoXG	-
Jun Kai	0x8aa07899eb940f40e514b8effdb3b6af5d1cf7bb	Singapore	https://github.com/junkai121	junkai121@outlook.com
Kei Nakano	0xff22be4f00b937dade564bd9659e265f92afa620 0x452f205c6c3872691fbce7ce8438370466d55f76 0x21e5d5a6e40b32cff77cfe77dca034d6d410131d	Tokyo, Japan	https://archive.ph/mo0QZ https://archive.ph/fhKTT	keinakano415@gmail.com
David Adachi	0x210888f2624d01f9cbc71de5bf4caf5b6dc9fa7f	Fukuoka, Japan	https://archive.ph/80EYH	davidadachi56@gmail.com
Gabriel Yiu	0xd80614feb54d49cf46cc861fc549fae0a05b3f7e	-	https://archive.ph/oGlCc	-
Joshua Palmer	0x06f90983cd2215379e440fc525e441d6a5fc3fba 5Jfb3n8eW4JyQrKJktMNBFXnC1zx2YHjRSkzRrTT5QHh 0xa6afe0290fb6f2f7ced0a2753de57f9fa7c9c9dd 0xfa802d9b33ed74baff62b189875c2b2d192874eb 0x7654e18ff3495675606c008a39b6264da5d0e8a7	Michigan, US	https://github.com/call-by https://archive.ph/grqjk	joshupgig@gmail.com smart.solidity@gmail.com
Andy Hoog	0x1043efee936903951b88db23551873bb67292e95	-	https://archive.ph/7IbnH	andyhoogup@gmail.com
Jordan Lopez	0x92cd7363c5b1853bc8fe6b5ae269836fc508ca73	Texas, US	https://archive.ph/tFeQG	cloudrider.m92@gmail.com
Quinn Lee	0x9de5d3158b0b83e9211c7444c94ce0c53763f574 0xf9adac8658e08893fb4e91c1062e471eb11cb6c7	-	https://archive.ph/KLBYw	letteldream@gmail.com
Ryuhei "Rio" Matsuda	0xa71b641a498e33bb13548a01eca5e20e083e637b 0x6fb678b2dd9d2ff50ee9ecf774251dcceb7a2da8	-	https://archive.ph/V5GsZ	ryuheimat3@gmail.com
Chris Yu	ESSfP3aAcW6Z59ozut9Jkqy9btaX5YTHt25b3Vhs2hsf 0x1043efee936903951b88db23551873bb67292e95 0x3b9A870c24905256dE10863cb360F4B93C7cC60f 0xc2b2a9c05740EEb7ee7BA7eB3AB11EC8bebCB1D1	Malaysia	https://archive.ph/x0LMf	atroboj@gmail.com
Bong Chee "Alex" Shen	GrXoxqM2a6QFKSBdZ9RLWJCBVTFvuuH8eCjjsLbjhpiR 0xD9054F484ed98a7Dd632EB9c09644616db3deA8C 0x2EFe21F4FeF7e737C0a3491C93be7D696038b6f5 0x65b4Ba828f85Ac429d6a02dB1304065A819A53f4 0x164729E00e8D0f871189160f36dee4398cAde1F2 0x06f90983cd2215379e440fc525e441d6a5fc3fba	Malaysia	https://github.com/devneser	alexzh.dev@gmail.com
James Lee	0xb9451049310053b29e5dd98c54bff37a5e38819c	Texas, US	https://archive.ph/rf3TU	james117lee@gmail.com
0xl2	0x0c0e8ef4b62a4a2a1b5031911e272362530c1a9a 0xfd1b05e51653339c850c8a18c9ac11aed9105f2a	-	https://archive.ph/KolKd	0xl2@proton.me
Wubone	0x0db9e27060b7f8258448aa31c36e7c0937fd5fd7	-	-	-
Peter Xiao	0x5d8335834bfdf4c746e277e5100d7c778c807356	-	https://github.com/assasinooz77	-
Russell Hieu	0x97467ea9bef1c925e9d8e2e65932d066869b7f13 0xFf6d86807b3387e10dDE52697C3BD7f59b6A145f	Vietnam	https://archive.ph/vgsFX https://github.com/0xdoccer	russellhieu@outlook.com
Pemba Gulu	0xfb5d591e8216f5d0964286f09b1f61114c16aab0	Singapore	https://archive.ph/nVlz9	pemba.sherpa5232@gmail.com pemba.gelu5232@gmail.com

図 2 北朝鮮 IT 技術者 21 名の偽名や仮想通貨アドレスなどの一覧 [1]

1.3. 北朝鮮 IT 技術者に支払われた仮想通貨の流れ

このように身分を偽って仕事に就いた北朝鮮 IT 技術者は、仮想通貨での給与支払いを要求することが多いとされる[2]。

北朝鮮 IT 技術者 21 名が利用していた複数の仮想通貨口座には、仮想通貨プロジェクトから 2024 年 7 月～8 月の 1 か月で合わせて 37 万 5000 ドル相当の仮想通貨の入金があった[3]。また、2023 年 7 月～2024 年 6 月の間には、総額 550 万ドル相当の仮想通貨の入金があり、それらの一部は北朝鮮人 Sim Hyon-Sop と関連する仮想通貨口座に振り込まれていた[4] 。

Sim Hyon-Sop は、北朝鮮の対外貿易銀行である KKBC（KOREA KWANGSON BANKING CORPORATION）の副代表を務め、北朝鮮関係者が国外で働いて得たもしくは窃取した外貨や仮想通貨を北朝鮮国内

[2] 出典：U.S. Department of the Treasury『Treasury Targets Actors Facilitating Illicit DPRK Financial Activity in Support of Weapons Programs
https://home.treasury.gov/news/press-releases/jy1435

[3] 出典：X『@zachxbt』
https://x.com/zachxbt/status/1824047452108067221

[4] 出典：X『@zachxbt』
https://x.com/zachxbt/status/1824047465827602550

に送金する業務に関わっていた人物である。それら外貨や仮想通貨は大量破壊兵器や弾道ミサイルの開発の資金源となっていることから、彼は OFAC（米国財務省外国資産管理室）により制裁対象に指定されており[2]、また FBI からは指名手配されている[5]。

図 3 FBI が公開する Sim Hyon-Sop の手配書 [5]

1.4. まとめ

仮想通貨プロジェクトを含め、身分を偽り働く北朝鮮 IT 技術者は北朝鮮国内外で数千人に上り、北朝鮮は年間数億ドルの利益を得ている[6]。また、北朝鮮のハッカー達は仮想通貨企業にサイバー攻撃を行い、2017～2023 年の 6 年間で総額 30 億ドルを窃取している[7]。

仮想通貨プロジェクトは、匿名性の高い仮想通貨を怪しまれることなく手に入れたい北朝鮮国家にとって都合がよい。北朝鮮 IT 技術者らの労働によって定期的に仮想通貨収入を得られることや、彼らがプロジェクトから短期間で仮想通貨を窃取できる可能性を考慮すると、北朝鮮国家にとって、仮想通貨プロジェクトに IT 技術者を送り込むことは、資金を調達する／増加させるための大きな手段になっていると言える。

---

[5] 出典：FBI『Most Wanted-Counterintelligence-"SIM HYON-SOP"』
https://www.fbi.gov/wanted/counterintelligence/sim-hyon-sop

[6] 出典：U.S. Department of the Treasury『GUIDANCE ON THE DEMOCRATIC PEOPLE'S REPUBLIC OF KOREA INFORMATION TECHNOLOGY WORKERS』
https://ofac.treasury.gov/media/923126/download?inline

[7] 出典：BleepingComputer『North Korea's state hackers stole $3 billion in crypto since 2017』
https://www.bleepingcomputer.com/news/security/north-koreas-state-hackers-stole-3-billion-in-crypto-since-2017/

2. DDoS 攻撃代行サービス利用の容疑者、国際共同捜査で逮捕

2.1. 概要

DDoS 攻撃（複数のコンピューターから標的のサーバーに対して大量のデータを送りつけ、システムに過剰な負荷を与えること）を、海外の代行サービスを利用して行ったとして、8 月 6 日、警察庁サイバー特別捜査部は、電子計算機損壊等業務妨害容疑で男を逮捕した。本件は、国際共同捜査をきっかけに国内の容疑者を逮捕するに至ったケースであり、これは警察庁によると、2022 年にサイバー特捜部の前身組織（サイバー特別捜査隊）が設置されて以来、初めてのことであった[8]。

2.2. 攻撃について

本件において逮捕されたのは、大分市の配管工の二十代の男[9]。2022 年 3 月 17 日、海外の DDoS 攻撃代行サービスのサイト「Bootyou」（現在は閉鎖）を利用して、東京都内の出版社のサーバーに対して DDoS 攻撃を 2 度にわたり行い、計約 1 時間半もの間 Web サイトを閲覧できない状態にしたとされる[10]。

同容疑者は、「サイバー攻撃が簡単に成功するセキュリティの弱そうな中小企業を狙った」「大企業は狙わなかった」「ストレス発散でやった」と供述している。他にも、学校などの教育機関や食品製造会社に対しても攻撃を繰り返していた疑いがあり、容疑者は DDoS 攻撃を行ったことについて「弁解することはない」と認めている[11, 12]。

2.3. DDoS 攻撃代行サービス

DDoS 攻撃においては、特別な知識がなくても攻撃先を指定するだけで誰でも簡単かつ安価で利用できる代行サービス（Booter/Stresser とも呼ばれる）が存在する。プログラミングに関する専門知識はないという前述の容疑者も、Bootyou をインターネットで見つけ、攻撃に利用していた。同サービスは、月額 4.99 ドルから 99.99 ドルで DDoS 攻撃を請け負っており、同容疑者は月額 1000 円程度の契約をしていた[13]。

---

[8] 出典：朝日新聞 DIGITAL『出版社に DDoS 攻撃容疑で逮捕　海外サービス利用、国際捜査で発覚』
https://www.asahi.com/articles/ASS861HW2S86UTIL010M.html

[9] 出典：朝日新聞 DIGITAL『出版社に DDoS 攻撃容疑で逮捕　海外サービス利用、国際捜査で発覚』
https://www.asahi.com/articles/ASS861HW2S86UTIL010M.html

[10] 出典：読売新聞オンライン『出版社にＤＤｏＳ攻撃容疑、２５歳の配管工「ストレス発散だった」…海外の代行業者を利用』
https://www.yomiuri.co.jp/national/20240806-OYT1T50213/

[11] 出典：Rocket Boys『サイバー攻撃 代行 サービスを利用して DDos 攻撃 大分の男性を逮捕』
https://rocket-boys.co.jp/7093/

[12] 出典：朝日新聞 DIGITAL『出版社に DDoS 攻撃容疑で逮捕　海外サービス利用、国際捜査で発覚』
https://www.asahi.com/articles/ASS861HW2S86UTIL010M.html

[13] 出典：読売新聞オンライン『出版社にＤＤｏＳ攻撃容疑、２５歳の配管工「ストレス発散だった」…海外の代行業者を利用』
https://www.yomiuri.co.jp/national/20240806-OYT1T50213/

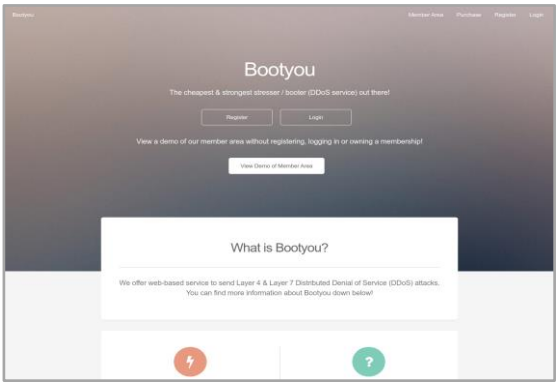

図 4「Bootyou」のサイト(Web アーカイブより)

図 5 閉鎖されたページ(現在)

Booter/Stresser サービスは、ダークウェブフォーラム、チャットプラットフォーム、YouTube などで宣伝されている。ターゲットに対して送信するトラフィックの量、攻撃の期間、同時攻撃の件数等に応じて様々なプランがあり、ユーザーは 1 か月あたり数ドルから数百ドル程度のサブスクリプションを登録する。支払いはオンライン決済サービス PayPal や Google Wallet、暗号通貨等で行う[14]。

2.4. 国際共同捜査

Booter/Stresser サービスの提供者は、ユーザーが自身の管理するサーバーに負荷テストを行う為のサービスとの立場をとっている。ユーザー側での利用方法については責任を負わないと主張し、利用規約にも攻撃に利用しないことを同意させる項目が含まれている[15]。

しかし、実際は犯罪に繋がる広範な悪用がほとんどで、欧州警察機構（ユーロポール）の他、米国、英国、オランダ、ドイツ、ポーランド各国の捜査機関は DDoS 攻撃代行サービスを提供する者を問題視していた。そして、これらのサービスを閉鎖するため、2018 年に「Operation PowerOFF」という作戦を立ち上げて以来、共同捜査を進めてきた[16]。この作戦により 2022 年 12 月までに海外の 50 程の代行サービスのサイトを機能停止にし、管理者 7 人を逮捕した[17]。Bootyou も同作戦にて 2022 年に閉鎖されてから押収データの解析が行われてきた。

警察庁は、2023 年 9 月にこの作戦に参加。ユーロポールから受けた情報提供が、今回の国内での逮捕につながったという[18]。

[14] 出典：Krebs on Security『Six Charged in Mass Takedown of DDoS-for-Hire Sites』
https://krebsonsecurity.com/2022/12/six-charged-in-mass-takedown-of-ddos-for-hire-sites/

[15] 出典：Krebs on Security『Six Charged in Mass Takedown of DDoS-for-Hire Sites』
https://krebsonsecurity.com/2022/12/six-charged-in-mass-takedown-of-ddos-for-hire-sites/

[16] 出典：DATAFORT『Operation PowerOFF: Inside the Takedown of a Vast Cybercrime Network』
https://datafort.com/operation-poweroff-inside-the-takedown-of-a-vast-cybercrime-network/

[17] 出典：朝日新聞 DIGITAL『出版社に DDoS 攻撃容疑で逮捕　海外サービス利用、国際捜査で発覚』
https://www.asahi.com/articles/ASS861HW2S86UTIL010M.html

[18] 出典：朝日新聞 DIGITAL『出版社に DDoS 攻撃容疑で逮捕　海外サービス利用、国際捜査で発覚』
https://www.asahi.com/articles/ASS861HW2S86UTIL010M.html

2.5. まとめ

このような DDoS 攻撃代行サービスの摘発は西側先進諸国で続いているが、同様のサービスは発展途上国やロシア語圏にも多く存在しており、マーケット全体を抑え込むにはまだまだ遠い状況である。

また、DDoS 攻撃では、インターネットに公開されている第三者のサーバーを悪用して攻撃用の通信を増幅させる、「増幅攻撃」がよく用いられることが知られている。インターネットに公開している自社のサーバーで、DNS、SNMP、NTP など増幅攻撃に利用されるサービスを使う場合は、適切な設定を行い、知らない間に犯罪行為に加担、あるいはそのような行為を助長することのないように心がけたい。

3. パリオリンピックに関連したサイバー攻撃

3.1. 概要

7 月 26 日から 8 月 11 日、パリオリンピック大会が開催された。大会の開催前や開催期間中には、関連した様々なサイバー攻撃や便乗したサイバー犯罪等が確認された。

閉会後にフランス当局は、最終的に 140 件以上のサイバー攻撃が確認されたが大会の運営に支障が出ることは無かったと発表している[19]。

3.2. オリンピックに関連したハクティビストの活動

【ハクティビストによる攻撃の背景】

大会の開催に前後して、自らの主義主張をオリンピックに絡めてアピールしようとするハクティビストの活動が観測された。これらハクティビストとしては主に、親ロシア系、親パレスチナ系が挙げられる。

背景として、パリオリンピック大会における参加国・参加禁止国の問題が有る。同大会には 204 の国・地域と難民選手団が参加し、ウクライナ、イスラエル、パレスチナからも選手団が参加した。だが、ロシアおよびベラルーシは、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国としての参加は認められなかった。

これに対し、ロシアは制裁の発動以来、強い反発を示し続けてきた。また、パレスチナは参加国であるイスラエルに出場禁止の制裁を行うよう、IOC に求めていた。

【偽情報を広める動画】

図 6 Telegram に投稿されていた、
偽のドキュメンタリー映画「Olympics has fallen」の宣伝画像

開幕の 1 年以上前から、パリオリンピック大会に関連した偽情報が出回っていた。IOC を批判することでロシアの正当性を

[19] 出典：France 24『France reports over 140 cyberattacks linked to Olympics』
https://www.france24.com/en/live-news/20240814-france-reports-over-140-cyberattacks-linked-to-olympics

広めるのが目的と考えられている。代表的なものが偽のドキュメンタリー映画「Olympics has fallen」（図 6）である[20]。2023 年初めに YouTube で公開されたこの動画は IOC の腐敗を告発する内容で、Netflix 制作と詐称し、俳優のトム・クルーズのディープフェイク音声が使われていた。動画はすぐに削除されたが、削除後も Telegram 等の SNS を通じ、たびたび拡散された。これ以外にも、様々なオリンピックや IOC を毀損する偽の動画が拡散された。

事態を重く見た IOC は 2023 年 11 月に「Olympics has fallen」について、内容を否定し、組織的な偽情報キャンペーンの一部である旨の声明[21]を出した。そして、SNS で見かけたこのようなコンテンツを、事実確認する前に記事にする報道関係者がみられたことから、そのような動画を見かけた際には報道する前に IOC に連絡を取り、流布されている情報の信憑性を確認するよう報道関係者に要請した。

【大会前後のハクティビストの活動】[22]

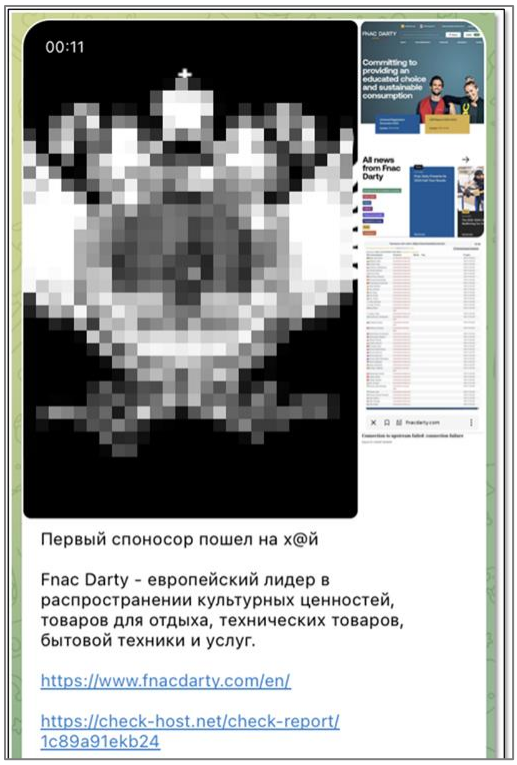

図 7 親ロシアのハクティビストによる、オリンピックオフィシャルパートナーへの DDoS 攻撃を示唆する投稿

図 8 親パレスチナのハクティビストによる、イスラエルの水泳協会への DDoS 攻撃を示唆する投稿

大会開催直前から開催期間中にわたり、親ロシア、親パレスチナの各ハクティビストによって、オリンピック関連の組織や民間企業に対し、サイバー攻撃が度々行われた。

[20] 出典：The New York Times『I.O.C. Says It Was Target of Elaborate 'Fake News' Campaign』 https://www.nytimes.com/2023/11/09/world/europe/ioc-fake-news.html

[21] 出典：IOC『IOC statement on fake news campaigns targeting the IOC』 https://olympics.com/ioc/news/ioc-statement-on-fake-news-campaigns-targeting-the-ioc

[22] 出典：NTT セキュリティ・ジャパン『パリオリンピックを狙ったサイバー攻撃』 https://jp.security.ntt/resources/cyber_security_report/adhoc_CSR_20240806.pdf

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や関連組織に対して DDoS 攻撃を行った（図 7）。親パレスチナのハッカーグループは、イスラエル選手の個人情報等の暴露や、イスラエルのスポーツ団体への DDoS 攻撃を行った（図 8）。

ほか、物議を呼んだ開会式のパフォーマンスについて、イスラム系のハッカーグループが抗議のサイバー攻撃を行った。預言者としてイスラム教でも崇敬されるイエスが侮辱されたことへの抗議に、フランスの Web サイトを改ざんする等の活動を行ったと主張している。

3.3. オリンピックに便乗した詐欺

パリオリンピック大会では、イベントに便乗した偽サイトや偽の映像配信サイト等によるサイバー犯罪がみられた。これらの多くは金銭を騙し取ることを目的としている。これまで他のスポーツイベント等でも確認されており、高揚感のあるイベントに便乗するサイバー犯罪が定番化していると言える。

【大会関連サイトの偽サイト】

サイバー犯罪者によりチケットやグッズ販売の偽サイトが作られ、クレジットカード情報の詐取や偽グッズの販売等の詐欺が行われた。偽サイトの作成では、公式サイトとの誤認を誘うため、大会のロゴの無断使用や、正規サイトのコピーといったことが行われた。さらに、検索の上位に表示されることを狙い、「parisolympics2024[.]store」「shop-olympics[.]shop」といったオリンピック関連のキーワードを使ったドメインを数多く取得して、偽サイトに使用したことが確認されている[23]。

【投資詐欺】

オリンピック関連のブランドを使用した、詐欺的な暗号通貨コインやトークンの販売が、いくつも確認された[24]。投資詐欺とみられ、これまでも FIFA ワールドカップなどの過去の大規模なイベントで同様の詐欺が出現している。

【映像配信サイト詐欺】

SNS では、野球やサッカーのリーグ戦等の競技時間に合わせて、不正な配信サイトへ誘導する投稿が日常的に横行している。パリオリンピック大会期間中も、同様の投稿が多数確認された。投稿に記載された URL をクリックすると、オリンピック公式と偽った Web サイトが表示される（図 9）。興味を持ってサイト内のボタンをクリックするとアカウント登録画面が表示される（図 10）。画面の指示に従ってメールアドレス等のほかクレジットカード情報も入力すると、不正使用の被害に遭うとみられている[25]。

[23] 出典：BforeAI『2024 Paris Olympic Games Infrastructure Attack Report』
https://bfore.ai/2024-paris-olympic-games-infrastructure-attack-report/

[24] 出典：トレンドマイクロ『2024 年パリ・オリンピックに便乗するサイバー犯罪者 ～生成 AI も利用する詐欺の手口とは？～』
https://www.trendmicro.com/ja_jp/jp-security/24/g/ico-scams-leverage-2024-olympics-to-lure-victims-use-ai-for-fake.html

[25] 出典：読売新聞『パリオリンピック映像配信とうたい、カード情報窃取の詐欺サイト…専門家「正規サイトから接続を」』
https://www.yomiuri.co.jp/national/20240731-OYT1T50181/

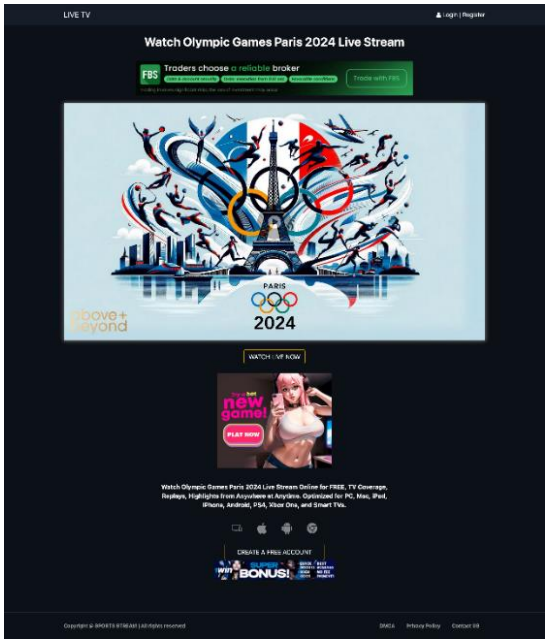

図 9 オリンピック公式と偽った配信サービス

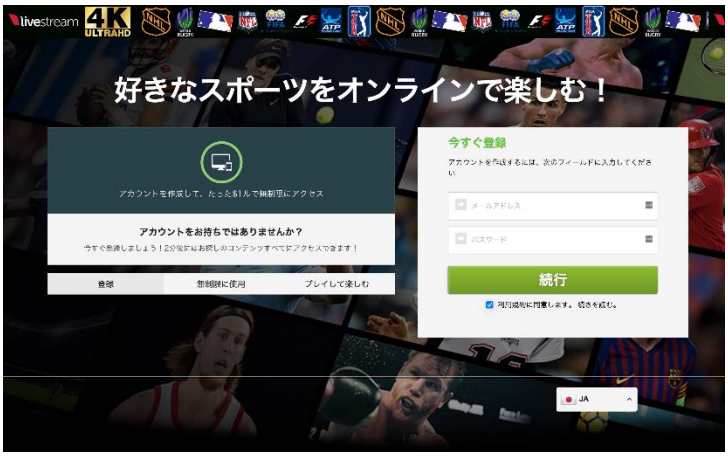

図 10 偽の配信サービスへのアカウント登録を求める画面

3.4. オリンピック会場施設で起きたランサム攻撃

フランスの 36 ある美術館を管理する GrandPalaisRmn（グラン・パレ・フランス国立美術館連合 [以下、国立美術館連合]）は、財務データを集中して扱うシステムが 8 月 3 日頃にサイバー攻撃を受けたと発表[26]した。なお、当組織の重要な活動拠点の一つである美術館のグラン・パレは、フェンシングとテコンドーの会場となっていた。

このサイバー攻撃はランサム攻撃であったと報じられている[27]。データを暗号化した攻撃者は、国立美術館連合に対し財務データを公開すると脅迫し身代金を要求したとされるが、攻撃による情報の外部流出については確認されなかった。被害拡大を防ぐための通信制限により、管理下の美術館にある書店等で一部営業活動に支障が出たが、美術館の運営には影響は無かったと国立美術館連合は発表している。なお、この攻撃による競技への影響、およびオリンピック関係のシステムへの影響についても、確認されなかった[28]。

3.5. フランス当局の振り返り

パリオリンピック大会の組織委員会は大会の準備において、ANSSI（国家情報システム・セキュリティ庁）をはじめとするフランスの政府や軍のサイバーセキュリティ機関と連携し、大会のセキュリティ対策に当たった[29]。まず、サイバー脅威インテリジェンスの強化や重要な IT インフラストラクチャの保護等の戦略を立て、大会開催に関連する約 700 の組織を特定した。そして、そ

[26] 出典：Grand Palais Pressroom『Le GrandPalaisRmn visé par une cyberattaque』 https://presse.rmngp.fr/le-grandpalaisrmn-vise-par-une-cyberattaque/

[27] 出典：Sud Ouest『Cyberattaque contre des musées : Grand Palais, Louvre touchés, rançongiciel… Que sait-on à ce stade?』 https://www.sudouest.fr/economie/cybersecurite/cyberattaque-contre-des-musees-grand-palais-louvre-touches-rancongiciel-que-sait-on-a-ce-stade-20907388.php

[28] 出典：Les Echos『La cyberattaque contre les musées français n'a touché que leurs boutiques』 https://www.lesechos.fr/industrie-services/services-conseils/la-cyberattaque-contre-les-musees-francais-na-touche-que-36-boutiques-2112529

[29] 出典：Infosecurity Magazine『How France is Protecting the 2024 Olympics from Unprecedented Cyber-Attacks』 https://www.infosecurity-magazine.com/news-features/how-france-protecting-the-2024/

れらの組織に技術的/人的な支援を行う等の綿密な準備をした上で、開催に臨んだ。

パリオリンピック大会の閉会直後の 8 月 13 日、ANSSI は大会のセキュリティ対策を支援した結果として、期間中に競技に支障をきたすような攻撃はなかったと発表した[30]。7 月 26 日から 8 月 11 日の間に、140 件以上のサイバー攻撃が報告された。主要なものとしては、影響度の低い「セキュリティイベント」に該当する報告が 119 件、また、攻撃者が情報システムを狙ったことによるインシデントが 22 件と ANSSI は記録している。このことから、期間中発生したサイバーセキュリティに関する事件は、影響度が低いと判定されるものばかりであったと、ANSSI は分析している。

3.6. まとめ

世界の注目を集めたパリオリンピック大会は、厳重なセキュリティ対策により、ほとんど大過なく終えられた。大会の中止を目的とした攻撃ではなく、大会への注目に便乗し、主張を広めたり詐欺で儲けようとしたりすることで目的を達成しようとするサイバー攻撃が目立った。

最新のサイバー脅威に対抗した今回の経験は、今後の大型国際イベントにおける、サイバーセキュリティ対策の参考にされていくと考えられる。

以上

[30] 出典：France 24『France reports over 140 cyberattacks linked to Olympics』
https://www.france24.com/en/live-news/20240814-france-reports-over-140-cyberattacks-linked-to-olympics

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

コンサルティングサービス部　OSINT モニタリングチーム
メールアドレス：nsj-co-osint-monitoring@security.ntt