サイバーセキュリティレポート

2023.02

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

【当レポートについて】

当レポートでは 2023 年 2 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『ロシア系ハクティビスト、日本企業へも DDoS 攻撃』

- 対ロシア制裁を行う各国に DDoS 攻撃を行っているハクティビスト「NoName」が、2022 年 2 月に入ってから日本の政府機関や企業に対して DDoS 攻撃を行った。
- 日本政府による対ロ制裁への復讐と称し攻撃成果を宣伝しており、実際に一時的に石油連盟等の web サイトに繋がりにくくなるといった影響が発生した。
- 対ロ制裁に関連する業界や、過去の攻撃実績から狙われることが想定される重要インフラに関わる企業は、日本政府の対ロシア制裁の動向を把握して、ハクティビストによる攻撃のタイミングを警戒する必要がある。CDN 等の DDoS 対策を導入し、弱点を無くすことが被害防止において重要である。

第 2 章『Google の広告プラットフォームを利用したサイバー犯罪が増加』

- 2 月 9 日、セキュリティ会社の Sucuri は、WordPress を利用しているサイトを攻撃し、偽の短縮 URL 等を利用して Web サイトの訪問者を不正な広告サイトに誘導するキャンペーンを観測したと発表した。
- 他にも Google の検索結果に表示される広告を悪用した攻撃の増加も観測されており、Google の広告プラットフォームが様々な形でサイバー犯罪に利用されている実態が明らかとなった。
- Google の検索結果だからといって無条件に信用するのではなく、遷移先の URL を確認する、セキュリティソフト等で警告がでたページにはアクセスしない、不審を感じたサイトでは情報の入力やダウンロードをしない、といった基本的な注意点を守り、利用する必要がある。

第 3 章『中国ハッカーグループ「シャオチーイン」、韓国組織にサイバー攻撃を実行』

- 2023 年の年明けに、中国語話者のハッカーグループとみられるシャオチーインが 2,000 以上の韓国の組織をサイバー攻撃の標的とすることを宣言。実際に複数の組織においてサイトの改ざんや接続障害等の被害が発生した。
- 中国では愛国心に基づく動機から、過去には多くのハッカーが日本を含む外国に対してサイバー攻撃等を行っていたが、中国政府による厳しい監視の下、近年はそのようなハッカーの活動が停滞していた。
- 国際的な匿名ハッカーフォーラムでの中国の大規模データ漏洩の暴露や、世界情勢に乗じてハッカーグループが活動する様子は、中国のハッカーにとって刺激となったことが窺える。Telegram や海外の匿名掲示板等を利用することで、中国語話者の匿名ハッカーが集結できる状況が現れている。

1. ロシア系ハクティビスト、日本企業へも DDoS 攻撃

1.1. 概要

2023 年 2 月に入ってから、ロシアを支持するハクティビスト「NoName」が日本の政府機関や企業へ DDoS 攻撃をたびたび行い、石油連盟や JR 東日本等で web サイトが表示されにくくなる被害が出た（図 1）。このグループはウクライナ侵攻直後の 2022 年 3 月頃から活動しており、ロシアに経済制裁を課している各国を狙って DDoS 攻撃を繰り返している。[1]

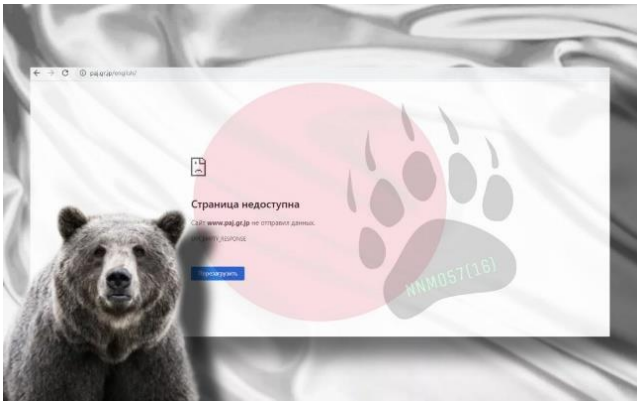

図 1「NoName」による
石油連盟への攻撃成功の発表画面

1.2. NoName の活動

【各国へと DDoS 攻撃】[2]

2022 年 2 月のウクライナ侵攻に前後して、親ロシアのハクティビストによる各国へのサイバー攻撃が活発になった。9 月に日本政府に DDoS 攻撃を行い話題となった KILLNET（キルネット）や Anonymous RUSSIA はその代表例であり、NoName も同様のグループである。

ウクライナをはじめ、米国、バルト三国、フィンランド、スウェーデン、ノルウェー、デンマーク、ドイツ、イタリア等の、ウクライナに連帯する各国を幅広く狙い、政府機関や金融機関、重要インフラ企業等に対し DDoS 攻撃を行っている。おおむね週替わりで標的とする国を変えているが、EU の首脳会議の開催に合わせ開催国を重点的に攻撃するといった、国際情勢にタイミングを合わせた狙い方もしている。

開戦直後の 2022 年 3 月頃から活動している。2022 年 6 月に、ロシアの飛び地領土のカリーニングラードへの輸送を、経由地であるリトアニアが制裁のために阻止した。この直後にリトアニアの輸送インフラ企業を標的とした DDoS 攻撃を実行したことから、NoName は注目されるようになった。また、1 月にはチェコでの大統領選挙の妨害を狙い、候補者の Web サイトを DDoS 攻撃の標的とした[3]。

【Telegram で成果発表】

NoName は、Telegram 上に公開グループを設置している。2022 年 3 月 11 日にグループを作成して以来フォロワーが増え、参加者は現在 32,000 人を超える。このグループでは主にロシア語で、ロシアに制裁する各国を嘲笑する主張が展開されている。NoName による DDoS 攻撃が成功すると、熊をコラージュした画像を貼るのが恒例となっている。

---

[1] 出典：The Cyber Express『NoName Hits Japanese Organizations After Country Imposes Latest Sanctions on Russia』
https://thecyberexpress.com/pro-russian-hacker-noname-japanese-companies/

[2] 出典：アバスト『アバスト、親ロシア派ハッカー集団「NoName057(16)」によるウクライナや支援国への DDoS 攻撃を確認』
https://press.avast.com/ja-jp/pro-russian-hacker-group-targeting-sites-in-ukraine-and-supporting-countries-with-ddos-attacks

[3] 出典：Check Point Software『Russia Affiliated NoName057(16) Hacktivist Group Puts 2023 Czech Presidential Election on the Spot』
https://blog.checkpoint.com/2023/01/19/russia-affiliated-noname05716-hacktivist-group-puts-2023-czech-presidential-election-on-the-spot/

Telegram のグループ内には、DDosia Projects と呼ばれる NoName が用意した DDoS ツールを使って攻撃を実行する、約 1,400 人の草の根の協力者達がいる。NoName は攻撃実績に応じてランキングを発表し、賞金を与えている[4]。

NoName は、Telegram で成功と発表している攻撃事例より実際には多く攻撃を仕掛けており、また、一度攻撃に成功したサイトを繰り返し攻撃している。セキュリティ会社の avast は、攻撃成功率は 40%程[5]と分析している。

【自己顕示性】

NoName は、攻撃を受ける側の反応を気にし、観察している。被害組織が Web サイトの不調を発表すると攻撃成功の証拠と喜び、Telegram で共有している。また、Twitter 等の SNS で自グループの名前を検索しているとみられ、NoName の攻撃を非難する主張を見つけると、スクリーンショットに揶揄や冷笑のコメントを付けて、Telegram で晒している。（図 2）

SNS で NoName の正式名称を挙げて反応すると、彼らを喜ばせたり逆上させたりして攻撃をエスカレートさせる恐れがあるため、注意が必要である。

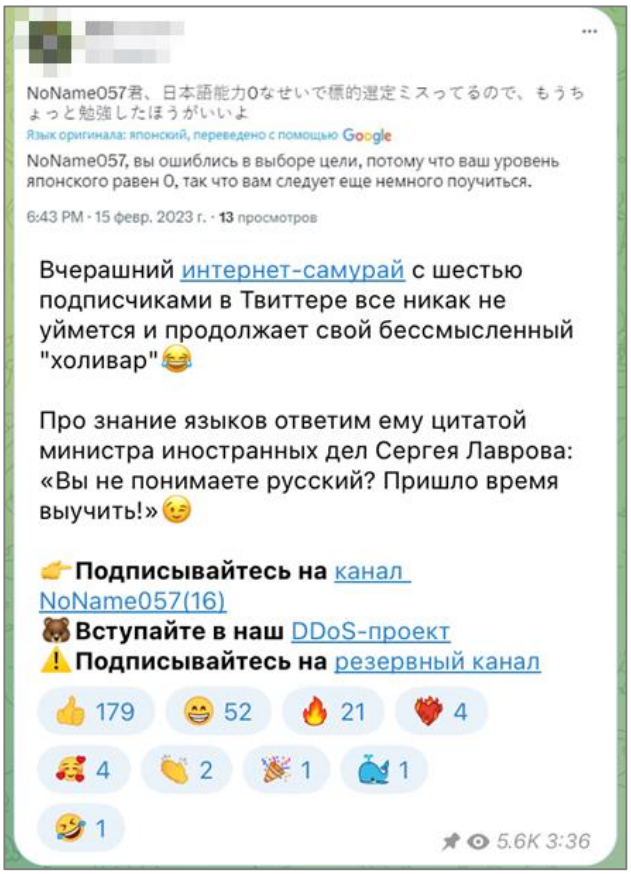

図 2 NoName を揶揄する日本語のツイートを晒して、無駄な議論をしたがる Twitter サムライと嘲笑

1.3. 日本を狙った NoName

2023 年 2 月 13 日、NoName は Telegram で、日本に対する攻撃を開始したと宣言した。理由として、2 月 6 日に日本政府が発表した原油の禁輸措置等[6]のロシアへの制裁や、対ロシア防衛強化、ウクライナへの経済支援への報復であると主張した。（図 3）

攻撃は約 1 週間続き、経済産業省、石油連盟、建設機器メーカー、鉄道事業者、電機メーカー、金融グループ、ゲーム会社の Web サイトへの攻撃に成功したと NoName は宣伝した。しかし翌週には NoName は標的国をエストニア、ラトビア、スウェーデンに切り替え、日本の組織への攻撃成果を発表しなくなった。

その翌週の 2 月 28 日に、日本政府がロシア連邦関係者に対する資産凍結等の追加制裁を発表すると、3 月 1 日に NoName は再び、以前に攻撃に成功した日本の組織を狙い DDoS 攻撃を行った。

[4] 出典：Check Point Software『Russia Affiliated NoName057(16) Hacktivist Group Puts 2023 Czech Presidential Election on the Spot』
https://blog.checkpoint.com/2023/01/19/russia-affiliated-noname05716-hacktivist-group-puts-2023-czech-presidential-election-on-the-spot/

[5] 出典：アバスト『アバスト、親ロシア派ハッカー集団「NoName057(16)」によるウクライナや支援国への DDoS 攻撃を確認』
https://press.avast.com/ja-jp/pro-russian-hacker-group-targeting-sites-in-ukraine-and-supporting-countries-with-ddos-attacks

[6] 出典：経済産業省『対ロシア等制裁関連』
https://www.meti.go.jp/policy/external_economy/trade_control/01_seido/04_seisai/crimea.html

図 3 日本への攻撃の開始を宣言する Telegram 投稿

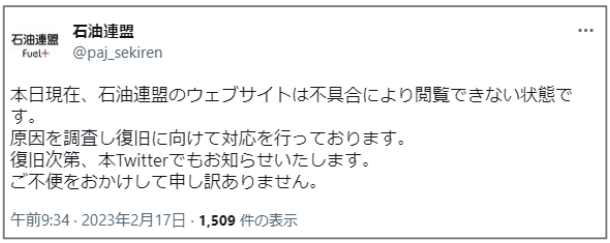

図 4 石油連盟の被害発表：2 月 17 日

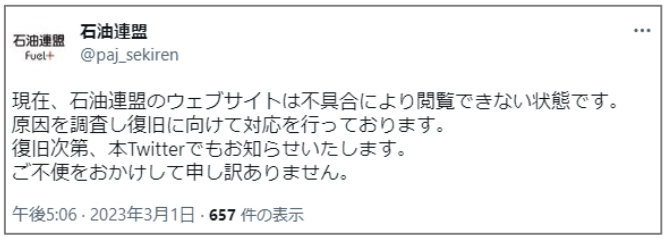

図 5 石油連盟の被害発表：3 月 1 日

被害事例①：石油連盟

NoName の主張から、石油連盟は原油の禁輸措置に関連して攻撃対象に選ばれたとみられる。NoName が DDoS 攻撃を行った時期の 2 月 17 日と 3 月 1 日にサイトが表示されにくくなっていることを発表しており（図 4、図 5）[7]、攻撃の影響とみられる。

[7] 出典：Twitter『石油連盟』
https://twitter.com/paj_sekiren/status/1626379596508860419
https://twitter.com/paj_sekiren/status/1630841911748730880

被害事例②：JR 東日本

JR 東日本は、コンテンツ配信システムである CDN を利用していて DDoS 攻撃への耐性があったが、2 月 16 日の攻撃では、旅行等の情報サイトのシステムが一時停止に追い込まれた[8]。狙われたサイトのサブドメインに「origin2-」という単語が含まれていることから（図 6）、CDN の裏側にあるオリジンサーバーを探し出されて攻撃を受けたと考えられる。

図 6 DDoS 攻撃で狙われ、表示されなくなったとみられる JR 東日本のサイト

1.4. まとめ

NoName は、日本政府の対ロ制裁に反応して日本への DDoS 攻撃を行うパターンが見られるため、対ロ制裁の内容に関連する業界や、過去の攻撃実績から狙われることが想定される重要インフラに関わる企業は、攻撃対象になる恐れがある。重要なネットワークは CDN で強化するといった DDoS 対策の導入が効果的である。

また、攻撃者は保護がされていない部分を探し出して狙ってくるため、オリジンサーバーへのアクセスを CDN に制限して保護する、一度被害に遭った web サイトは再び狙われる恐れがあるので直ちに強化するといった、攻撃される弱点を無くすことも重要である。

[8] 出典：Twitter『JR 東日本(公式)』
https://twitter.com/JREast_official/status/1626037432197218306

2. Google の広告プラットフォームを利用したサイバー犯罪が増加

2.1. 概要

2 月 9 日、セキュリティ会社の Sucuri は、WordPress を利用しているサイトを攻撃し、偽の短縮 URL 等を利用して Web サイトの訪問者を不正な広告サイトに誘導するキャンペーンを観測したと発表した[9]。攻撃者はこの攻撃によって、不正に広告の閲覧数やクリック数を稼ぎ、「Google Adsense」の広告収益を得ている。このキャンペーンは 2022 年 9 月に始まり、これまでに 1 万件以上のサイトで感染が確認されている。

他にも Google の検索結果に表示される広告を悪用した攻撃の増加も観測されており、Google の広告プラットフォームが様々な形でサイバー犯罪に利用されている実態が明らかとなった。

2.2. Google Adsense と Sucuri によって観測された攻撃

【Google Adsense とは】

ウェブサイトの所有者が広告収入を得ようとする場合、広告主の企業と直接契約するのではなく、広告の配信や閲覧数のカウント等を行う仲介業者と契約し、自分のサイトに広告を掲載し報酬を受け取るのが一般的である[10]。「Google AdSense」は、Google がそういった仲介業者の役割を果たす広告プラットフォームである[11,12]。

図 7 Google AdSense の仕組み [12]

Google Adsense では、ウェブサイトに掲載されているコンテンツ内容や訪問者の情報に基づいて、関連する広告が自動

[9] 出典：Sucuri『Bogus URL Shorteners Redirect Thousands of Hacked Sites in AdSense Fraud Campaign』
https://blog.sucuri.net/2023/02/bogus-url-shorteners-redirect-thousands-of-hacked-sites-in-adsense-fraud-campaign.html

[10] 出典：Xserver『【ブログで収益化！】広告収入を得る仕組みと定番サービス 3 つを紹介』
https://www.xserver.ne.jp/blog/how-to-monetize-and-popular-ad-services/

[11] 出典：Google『Google AdSense』
https://adsense.google.com/intl/ja_jp/start/

[12] 出典：Google『AdSense の仕組み』
https://support.google.com/adsense/answer/6242051

的に選ばれて表示される。広告を掲載するためのスクリプトを改編することや、広告を含むページに暴力的・性的・違法なもの等を含むコンテンツを掲載すること、広告をクリックするようにユーザーを誘導したり、誤解を招くように広告を配置したりすることは禁じられている。以上のような Google のポリシーに違反した場合には、収益を没収される可能性がある。

【報告された攻撃】

2022 年 9 月から、WordPress を利用しているサイトを標的としたマルウェアキャンペーンが観測された[13]。攻撃者はプラグインの脆弱性を利用する等何らかの方法で WordPress サイトに不正アクセスをして、マルウェアを感染させる。マルウェアは、WordPress で生成される Web ページにスクリプトを埋め込む。この Web ページにアクセスした訪問者は、いくつかのサイトをリダイレクトを繰り返して経由し、偽の Q&A サイトに誘導させられる。

埋め込まれたスクリプトは難読化されていて、リダイレクト先が簡単に分析できないようになっていた。リダイレクト先には「bit.ly」等の著名なリダイレクトサービスを模したドメインが利用されていた。経由するサイトのホスティングには、ロシアの「DDoS-Guard」のサービスを CDN として利用することで、本体のサーバー（オリジンサーバー）を外部からわかりづらくするといった巧妙な隠ぺい工作が取られていた。

誘導先の偽の Q&A サイトには Google AdSense の広告が含まれていることから、広告表示数を増やして収益を得ることを狙っていると推測される。

図 8 攻撃で用いられた bit.ly に似せた偽のＵＲＬ例

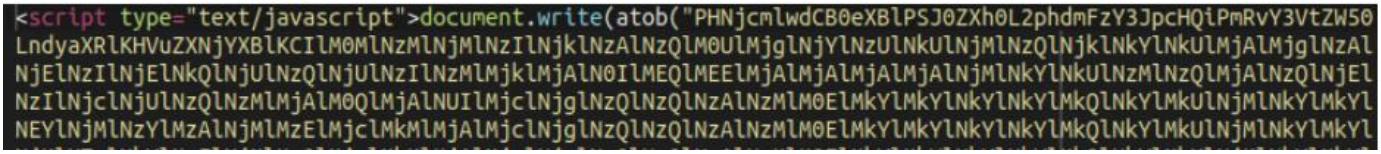

図 9 攻撃を受けた Web ページに挿入された難読化されたスクリプト

2.3. Google の広告を悪用したその他の攻撃

Sucuri のレポートは Google から広告収入を得ようとする攻撃であったが、Google の広告は他の方法でも犯罪に利用されている。

2022 年 10 月[14]と 12 月[15]と続けて、JR 東日本の「えきねっと」を模倣した偽サイトが、正規の JR のサイトよりも検索結果で上位に表示されるようになっていた。Google の検索結果画面では、検索結果よりも広告枠が上位に表示されることを悪用していた。偽サイトには ID とパスワードの入力欄が設けられており、認証情報を詐取するための偽サイトであったと考えられる。

---

[13] 出典：Sucuri『Massive ois[.]is Black Hat Redirect Malware Campaign』
https://blog.sucuri.net/2022/11/massive-ois-is-black-hat-redirect-malware-campaign.html

[14] 出典：産経新聞『グーグルで「えきねっと」検索→偽サイトへ　ＪＲ東が削除依頼』
https://www.sankei.com/article/20221019-JW6B4XO2PBOQLLBNJSWKAHCXIU/

[15] 出典：ITmedia NEWS『Google で「えきねっと」検索するとトップに偽サイト　現在は非表示　JR 東の対応は』
https://www.itmedia.co.jp/news/articles/2212/14/news169.html

また、著名なソフトウェアを検索したユーザーを狙い、「えきねっと」と同様に正規サイトよりも上位に偽サイトの広告を表示させ、訪れたユーザーにマルウェア入りのソフトウェアをダウンロードさせる「マルバタイジング」攻撃も 1 月以降急増している[16]。以前は、「Microsoft Teams」や「Adobe Acrobat」のような業務で利用されるソフトウェアの配布サイトになりすますケースが多かったが、最近では、そういった業務用のソフトウェアに限らず、著名なものを幅広くなりすましの対象とするようになってきており、どういったソフトウェアが危険かという予想も困難になってきている。

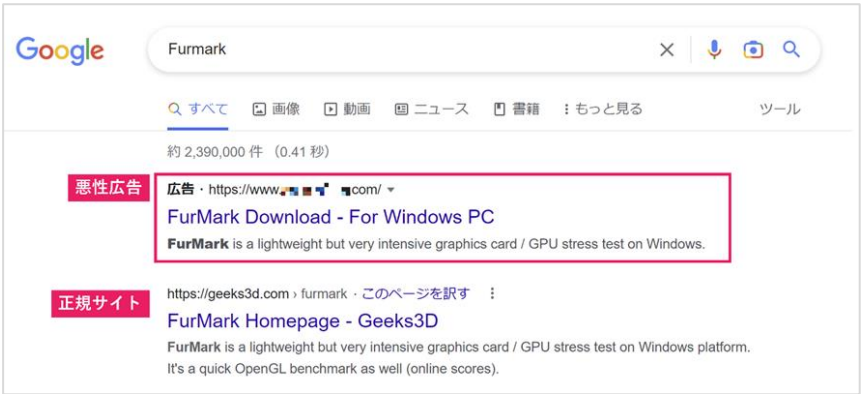

図 10 Google の検索結果に表示される、偽のソフトウェアの配布サイトの広告例 [16]

上記のように Google の広告を利用しマルウェアに感染させるキャンペーンは、セキュリティ会社の「Guardio」からも報告されており[17]、FBI も検索エンジンの広告を利用した攻撃について注意喚起している[18]。

2.4. まとめ

Google の広告を様々な形で悪用するサイバー犯罪が多く観測されるようになってきた。特に検索結果画面の広告を悪用した情報窃取やマルバタイジング攻撃は、エンドユーザーとしても直接被害を受ける可能性のある危険なものであり、Google の対策が追い付いていない状況が浮き彫りとなっている。フィッシング対策として、SMS やメールでリンクを送らないことが推奨されているが、これは Google をはじめとする検索エンジンの検索結果が信頼できることが前提となっており、その前提が崩れてしまっている。

Google の検索結果だからといって無条件に信用するのではなく、クリックする前に遷移先の URL を確認する、セキュリティソフトやブラウザからの警告が表示されたページにはアクセスしない、不審を感じたサイトでのパスワードや個人情報の入力、ソフトウェアのダウンロードは避ける、といった基本的な注意点を守った上で、利用する必要がある[19,20]。

---

[16] 出典：NTT セキュリティテクニカルブログ『SteelClover による Google 広告経由でマルウェアを配布する攻撃の活発化について』
https://insight-jp.nttsecurity.com/post/102i7af/steelclovergoogle

[17] 出典：TechGenix『MasquerAds — The Latest Malware Campaign That Leverages Google Ads』
https://techgenix.com/masquerads-leveraging-google-ads/

[18] 出典：FBI『Cyber Criminals Impersonating Brands Using Search Engine Advertisement Services to Defraud Users』
https://www.ic3.gov/Media/Y2022/PSA221221

[19] 出典：総務省『事故・被害の事例 ＞ 事例 17：有名サイトからダウンロードしたはずなのに・・・』
https://www.soumu.go.jp/main_sosiki/joho_tsusin/security/enduser/case/17.html

[20] 出典：総務省『ホームページ閲覧における注意点』
https://www.soumu.go.jp/main_sosiki/joho_tsusin/security/enduser/security02/01.html

3. 中国ハッカーグループ「シャオチーイン」、韓国組織にサイバー攻撃を実行

3.1. 概要

2023 年の年明け以降、中国語話者が中心とみられるハッカーグループ「シャオチーイン」（暁騎営：中国語で「夜明けの騎兵隊」の意）が、韓国の学術・研究機関に対し、Web サイトの改ざんや個人情報窃取といったサイバー攻撃を行った。中国には愛国心に動機づけられたハッカーグループが多く存在していたが、近年は活動が停滞していた。

3.2. 韓国の複数の組織に対するサイバー攻撃

【攻撃予告】[21] [22]

1 月 7 日、シャオチーインが、長期的にデータ漏洩を引き起こす作戦を韓国に対して準備中であることを、自身のサイトで発表。旧正月連休初日の 21 日には、2,000 以上の韓国政府機関および 30 社以上のメディアを攻撃すると予告し、内部資料を窃取・公開するとも述べた。
これを受けて、準政府機関である韓国情報保護振興院（KISA）は企業に対し、自社サイトの監視強化や不審な IP アドレスの遮断、また問題発生時には KISA に報告すること等を勧告した。

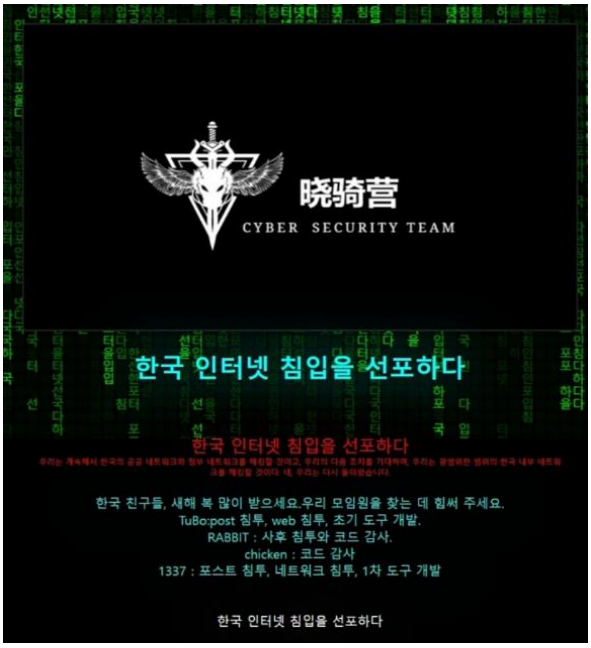

図 11 改ざんされた韓国社会科授業学会ホームページ画面（「韓国のインターネットへの侵入を宣言する」と表示されている）

【攻撃発生】[23] [24] [25] [26]

攻撃予告の前日（20 日）以降、韓国の 12 の学術機関のサイトが、次々とハッキングされた。サイトに接続できない、または改ざんされたページが表示されるという状態が続き、これらのサイトが、KISA のサポートにより完全に復旧したのは 2 月 1 日であった。また韓国の警察庁サイバーテロ捜査隊は、この攻撃に利用された IP

[21] 出典：Digital Today『중국 해커조직 국내 12 개 기관 사이트 해킹...피해 확산』
https://www.digitaltoday.co.kr/news/articleView.html?idxno=468928
[22] 出典：Digital Today『KISA "중국 해커조직 국내 2000 개 홈페이지 해킹 예고"』
https://www.digitaltoday.co.kr/news/articleView.html?idxno=468881
[23] 出典：디지털데일리『[단독] "한국 인터넷 침입을 선포하다"… 中 해커에 뚫린 대한민국 보안』
https://www.ddaily.co.kr/news/article/?no=255980
[24] 出典：The Korea Times『Korean websites fully restored after Chinese cyberattacks』
https://koreatimes.co.kr/www/nation/2023/02/251_344663.html
[25] 出典：헤럴드경제『경찰, '국내학술단체 해킹'에 인터폴 등 공조 공식 요청…中 협조는 미지수』
http://news.heraldcorp.com/view.php?ud=20230130000167
[26] 出典：산업일보『中 해커조직에 12 개 기관 해킹… "공격 IP 확인"』
https://www.kidd.co.kr/news/231090

アドレス情報に基づき、国際刑事警察機構（インターポール）、米 FBI、更に中国公安部門に対し、国際捜査協力を要請した。

【メッセージの発信】

シャオチーインはこれら一連の攻撃を実行する他、主にメッセージングサービスの Telegram を使用してメッセージを発信していた。その中には、KISA への攻撃予告や、被害組織数は 12 ではなく、実際には韓国教育部門のフォルダに含まれていた 41 組織のデータベースを窃取したという主張、更に韓国政府がそのような大きな被害をごまかして隠そうとしているのではないかとの皮肉等、様々な内容が含まれていた[27]。

【攻撃手法】[28] [29]

1 月に被害に遭った 12 サイトはファイアウォールを構築していなかったり、システム管理がずさんであったりする等、セキュリティ対策に不備があった。シャオチーインは主に、Web アプリケーションの脆弱性を悪用してデータベースを不正に操作する SQL インジェクションの他、サーバーに設置すると任意のコマンドの実行が可能となる Web シェルを利用した攻撃を実行したとの分析が、韓国のセキュリティ企業から示されている。

【2 月の攻撃】

2 月になっても、韓国の財団法人から 4 万件の個人・機密情報を窃取する等、シャオチーインによる攻撃は続いた[30]。また同グループは、新規メンバーの加入条件として、5 件の韓国のサイトをハッキングすることを挙げていたが、これに応えた人物がコンビニチェーンや大学等、5 件のサイトをハッキングし、グループに迎え入れられた[31]。

3.3. シャオチーインとは

シャオチーインは、2022 年 12 月 28 日に実行した、四川省炭鉱監視プラットフォームのハッキングから活動を本格化させている[32] [23]。同グループは、以前、活動していたグループ「タンスネーク」（腾蛇）の後継とみられている。

タンスネークは 2021 年末から活動し、ハッキングで窃取した情報の暴露などを行っていたグループである。2022 年 4 月には、日本のメーリングリストであるとして複数のファイルを公開した。そしてその翌月には、韓国保健省のアクティブディレクトリ

[27] 出典：MBN 뉴스『[단독] 중국 해킹 조직 "피해단체, 12 개 아닌 41 개…한국 정부가 덮고 있나"』
https://m.mbn.co.kr/news/4899057
[28] 出典：Byline Network『홈페이지 얼굴 바꾼 '샤오치잉'발 디페이스 해킹…대처 방안은?』
https://byline.network/2023/01/0130_01/
[29] 出典：매일경제『설 연휴에 中 해커조직 공격 … "한국사회 혼란 노린듯"』
https://www.mk.co.kr/today-paper/view/2023/5369469/
[30] 出典：朝鮮日報 IT Chosun『中해킹조직 '샤오치잉' 韓공격 중단 선언…보안업계 "안심은 금물"』
https://it.chosun.com/site/data/html_dir/2023/02/21/2023022102058.html
[31] 出典：서울경제『[단독] 편의점 CU 홈피도 뚫렸다…中 해커조직 놀이터 된 韓』
https://www.sedaily.com/NewsView/29LREYG01K
[32] 出典：중앙일보『"한국 스타가 날 화나게 했다"…12 개 기관 홈피 뚫은 中 해커』
https://www.joongang.co.kr/article/25135792#home

（AD）サーバーに侵入したと主張（実際には別組織を攻撃）し、サーバーへのアクセス権を販売していた[33]。またタンスネークが韓国政府プラットフォームから窃取したと主張し公開していた情報を、シャオチーインは自身が窃取したデータに含めて2023 年 1 月初旬に公開している[34]。

【なぜ韓国を標的に】[23] [35]

グループは 1 月下旬に Telegram で「我々は中国政府のために働いているのではない。我々のチームは自由なグループであり、訓練場として韓国を利用するつもり。各メンバーは韓国への侵入に参加するだろう」とコメントした。韓国を攻撃した理由としては、（新型コロナウィルスの感染拡大を防ぐ目的で）韓国が中国国民に対して実施している短期ビザ発給制限に対する報復、そして韓国の複数の人気動画配信者にイライラしたことを挙げた。

シャオチーインはその後も、「機嫌が悪くなると、面白半分に韓国語のデータベースを掲載する」といった発言をしていた。ただ新規メンバーを募集するメッセージでは、韓国人に対しても友好的な雰囲気で語りかけている（図 12）。

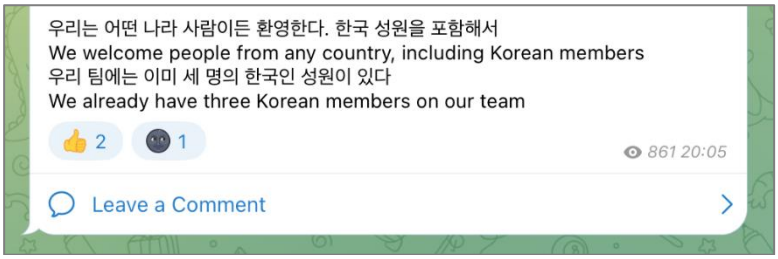

図 12　新規メンバー募集メッセージ（抜粋）

「韓国を含め、あらゆる国からメンバーを歓迎する。当チームには既に 3 名の韓国人がいる」

【その後のシャオチーイン】

シャオチーインは 2 月 1 日、Telegram で「韓国と日本に対する新たな攻撃を来月 28 日に開始する」と述べていた[36]。これは文字通り「3 月 28 日」なのか、それとも実際は「2 月 28 日」を意味していたのか不明であるが、後者の日付に攻撃は発生しなかった。

2 月 19 日、自身のサイトで、「韓国での約 1 か月にわたる作戦を終了した」と宣言。Telegram でも、「韓国はもはやターゲットではない」、「韓国は挑戦し甲斐が無いので、他のネットワークドメインに行く」と発言した。

同グループは別のメッセージングサービスの Signal に活動の拠点を移すことになり、Telegram の使用を 2 月末までに停止した。

---

[33] 出典：Medium『HOTSAUCE | S2W TALON「变脸, Teng Snake (a.k.a. Code Core)」』
https://medium.com/s2wblog/%E5%8F%98%E8%84%B8-teng-snake-a-k-a-code-core-8c35268b4d1a
[34] 出典：디지털데일리『中 해커 "한국 정부가 피해 은폐" 주장, 대대적인 공격 예고했지만…』
https://www.ddaily.co.kr/news/article/?no=256158
[35] 出典：연합뉴스『中해커그룹, 12 개 학회·연구소 해킹…정부기관까지 공격(종합 3 보)』
https://www.yna.co.kr/view/AKR20230125034053017
[36] 出典：데일리시큐『[긴급] 한국 정부·공공기관 해킹 선전포고했던 중국 '샤오치잉' 조직...새로운 공격 예고』
https://www.dailysecu.com/news/articleView.html?idxno=143239

3.4. 中国のハッカーらによる攻撃活動

【中国のハッキング活動】[37] [38] [39] [40]

中国で最初のハッカーグループが出現したのは 1994 年頃といわれる。それ以来、多くのグループは（国家の支援・支持の下で活動する現在の APT グループとは異なり）自身の愛国的な主義主張を広める手段として、サイバー攻撃を行ってきた。

特に 1,200 名以上の中国系インドネシア人が虐殺されたジャカルタ暴動（1998 年）や、翌年の NATO によるベオグラードの在ユーゴスラビア中国大使館の爆撃（NATO は「誤爆」と主張）といった、「反中国」と受け取られる事件が発生したことを契機に、ハッカーらは愛国心の下で活動を活性化させていったと考えられている。この中から、後に緑盟（Green Army）や中国紅客連盟（Honker Union of China）、中国鷹派連盟（China Eagle Union）等の著名なグループに発展したケースもある。それらのグループは中国に敵対するとみなした外国の組織に対し、認証情報の窃取の他、サイトの改ざんや DDoS 攻撃を行い、注目を集めるようになった。

【日本組織への攻撃】[41] [42] [43] [44]

日本の組織も、これまで折に触れて中国のハッカーグループによる攻撃対象となっている。例えば 2011 年、満州事変の発端となった柳条湖事件が発生した 9 月 18 日には、日本政府機関等のサイトに対して改ざんや DDoS 攻撃が行われた。また、2010 年から 2014 年までは、9 月 18 日前後に、中国を送信元とする IP アドレスから日本に対する SQL インジェクション攻撃の増加が観測されていた。

---

[37] 出典：Infosecurity『State of Denial: The Chinese Cyber Threat』
https://www.infosecurity-magazine.com/magazine-features/state-of-denial-the-chinese-cyber-threat/

[38] 出典：日経ビジネス電子版『インドネシアの華人虐殺 930 事件』
https://business.nikkei.com/atcl/seminar/19/00059/082900168/

[39] 出典：Recorded Future『Thieves and Geeks: Russian and Chinese Hacking Communities』
https://www.recordedfuture.com/russian-chinese-hacking-communities

[40] 出典：ReliaQuest『Honker Union: Has the grandfather of Chinese Hacktivism returned?』
https://www.reliaquest.com/blog/honker-union-has-the-grandfather-of-chinese-hacktivism-returned/

[41] 出典：European Union Agency for Cybersecurity『Mariko Miya, Cyber Defense Institute, Inc.「Findings and Lessons Learned From Massive Cyber Attack Emergence Mechanisms in Japan」』
https://www.enisa.europa.eu/events/2nd-enisa-conference/presentations/mariko-miya-cyber-defence-institute-japan-major.pdf

[42] 出典：日本経済新聞『尖閣国有化後のサイバー被害、19 サイト 警察庁まとめ』
https://www.nikkei.com/article/DGXNASDG1904B_Z10C12A9CC1000/

[43] 出典：日本経済新聞『人事院などにサイバー攻撃 中国サイトで呼び掛けか』
https://www.nikkei.com/article/DGXNASFK1901A_Z10C11A9000000/

[44] 出典：IBM セキュリティー・インテリジェンス・ブログ『柳条湖事件が起こった 9 月 18 日前後の攻撃動向について』
https://www.ibm.com/blogs/security/jp-ja/liutiaogou-918-2016/

2012 年には、尖閣諸島が 9 月 11 日に国有化されたことを受け、中国紅客連盟の掲示板等で、約 300 の日本組織が攻撃対象として挙げられた。うち 11 サイトが実際に閲覧できない状況に陥った他、裁判所を含む 8 つのサイトに対し、中国の国旗等の画像を使用した改ざんが行われた。また中国のチャットサイトでは攻撃に関する書き込みが行われ、参加者数は 4,000 名に達した。

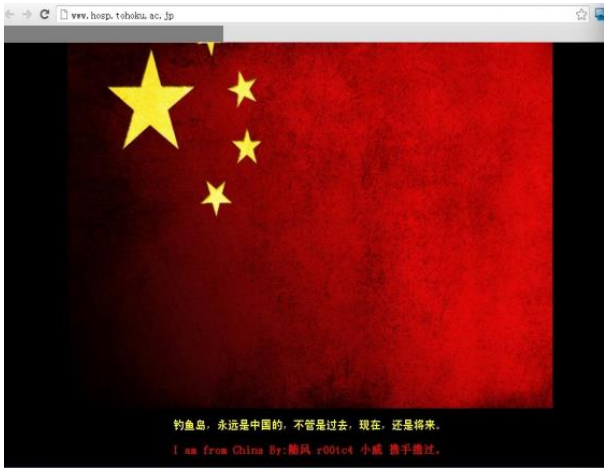

図 13　2012 年 9 月に確認された東北大学病院サイトの改ざん（一部加工）

【ハッカーグループの沈静化】

中国のハッカーらは、国家に対して危険をもたらさない限り、活動が容認されていると言われてきた。このことを背景に、日本の組織に対しても毎年のように、歴史・政治的な問題や記念日にちなんだサイバー攻撃が行われてきたが、2010 年代半ばを過ぎると、同様の攻撃はほとんど観測されなくなった。

2013 年の習近平政権の発足後はインターネット上の検閲・監視が厳しくなっており、ハッカーを内包する匿名文化が育ちにくくなっていたと考えられる[45] [46] [39]。

【ハッカーらの覚醒か】[46] [47] [48] [49] [50]

2022 年 7 月、ChinaDan と名乗る人物が、上海国家警察から漏洩したとする 10 億の中国人の個人情報を含むデータベースを、（シャオチーインも利用する）国際的なハッカーフォーラムで売りに出した。これまで世界で発生した政府系データベースの規模としては最大と見られ、大きな話題となった。その翌月には、新型コロナウィルス感染拡大防止策の一環として上海での使用が義務付けられていた健康コードアプリのユーザー4,850 万人に関するデータを、XJP と名乗る人物が「くまのプーさん」のプロフィール写真と共に、同じハッカーフォーラムで売りに出した。「XJP」は Xi Jinping（習近平）の略でもあり、「くまのプーさん」は中国のネットユーザーらが軽蔑を込めて習氏に付けているあだ名である。

中国政府の検閲・監視体制により、活動が困難になっていったハッカーらにとって、これらの事件が刺激となったことは想像に難くない。実際に、上海国家警察漏洩事件の後、上記のハッカーフォーラムに中国語の書き込みが殺到するようになり、中国のハッカーやその予備軍の間で、海外の匿名のハッキングフォーラムの存在が広く知られるようになったと考えられる。

---

[45] 出典：防衛研究所『ブリーフィング・メモ 2020 年 7 月号　小野圭司「サイバー傭兵の動向」』
http://www.nids.mod.go.jp/publication/briefing/pdf/2020/202007.pdf

[46] 出典：Mercator Institute for China Studies (MERICS)『Chinese public databases leaks reveal growing dissatisfaction with authorities』
https://merics.org/en/opinion/chinese-public-databases-leaks-reveal-growing-dissatisfaction-authorities

[47] 出典：BBC News Japan『中国当局、なぜまたクマのプーさんを検閲？　主席任期延長案で』
https://www.bbc.com/japanese/features-and-analysis-43208840

[48] 出典：HACKREAD『Killnet Claim They've Stolen Employee Data from Lockheed Martin』
https://www.hackread.com/killnet-hackers-hit-lockheed-martin-employee-data/

[49] 出典：Security NEXT『4 省庁 23 サイトで障害、DDoS 攻撃が原因か - 民間サイトでも障害』
https://www.security-next.com/139562

[50] 出典：Twitter『YourAnonTV』
https://twitter.com/YourAnonTV/status/1500557635686486023

また、ロシアのウクライナ侵攻を機に、世界中では多くのサイバー攻撃が発生している。例えば、親ロシア派のハッカーグループ KILLNET は、米ロッキードマーティン社や日本の電子政府窓口「e-Gov」等を攻撃したと主張。一方、人権、政治等についての主張に基づきサイバー攻撃を行う者らのネットワークとして知られるアノニマスは反ロシア派として、ロシアの国営テレビを含む複数の映像サービスをハッキングし、ウクライナの被害状況を放送した。このような、世界情勢に乗じたハッカーグループの激しい活動を目の当たりにして、彼らのように自分達も活動できるということに気付かされた中国のハッカーが、動き始めている可能性がある。

3.5. まとめ

中国の検閲・監視体制は変わっていないが、Telegram や海外の匿名掲示板等を利用することで、中国語話者の匿名ハッカーが集結できる状況が現れている。現在でも中国のハッカーの多くは、政府寄りの姿勢を保っているが、ここでは中国政府の検閲や監視は困難であり、反体制的な活動も広がっていく可能性が考えられる。

以上

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： WA_Advisorysupport@ntt.com