



NTT

Security Holdings

Killnetによる日本へのサイバー攻撃（更新版）

NTTセキュリティ・ジャパン

OSINTモニタリングチーム

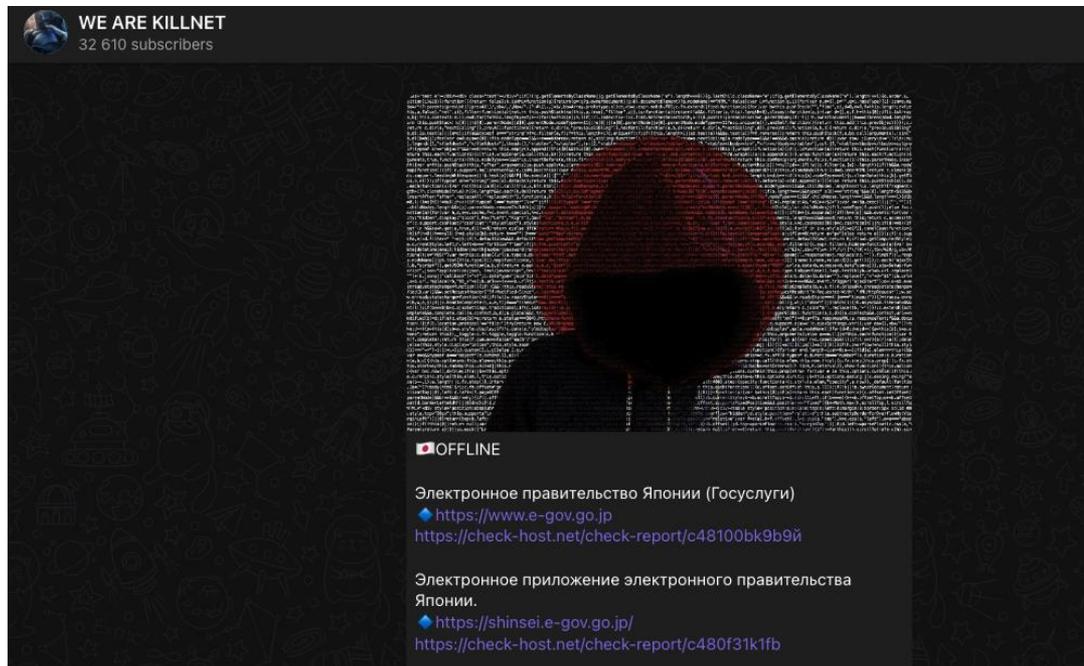
2022年9月14日



2022年9月6日、ロシアを支援するハクティヴィスト Killnet が日本政府機関を含む複数のサイトに対して、サイバー攻撃を行った。本資料は本攻撃について弊社OSINTモニタリングチームによって観測された情報をまとめたものである。

Killnetの攻撃 ～政府関連①～

- ロシアを支援するハッカー集団「Killnet」が9月6日午後4時34分頃、SNSにて日本政府運営の行政情報の総合窓口サイト「e-Gov」等のURLを投稿し、オフラインにしたとサイバー攻撃を示唆した。
- これらのサイトにアクセスできない状況がしばらく続いた。



Killnetによる日本へのサイバー攻撃を示唆する投稿

Killnetの攻撃 ～政府関連②～

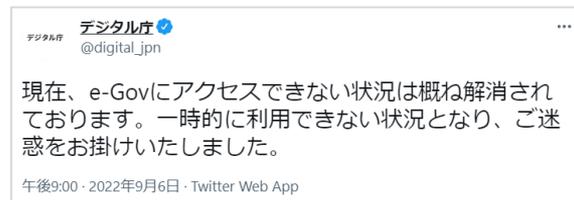
- Killnetが攻撃を示唆したのはe-GovとeLTAXの4つのURL
 - ・ e-GOV www.e-gov.go.jp / shinsei.e-gov.go.jp
 - ・ eLTAX www.eltax.lta.go.jp / www.portal.eltax.lta.go.jp
- e-Govは6日午後9時頃までに復旧。
- eLTAXは8日朝までに復旧。



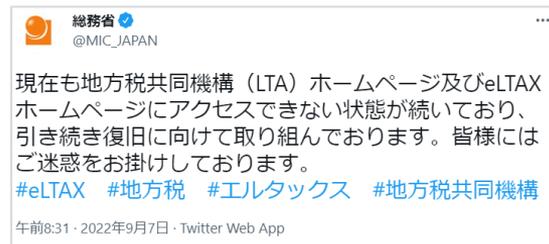
Killnetが示したe-Gov攻撃の証跡



Killnetが示したeLTAX攻撃の証跡

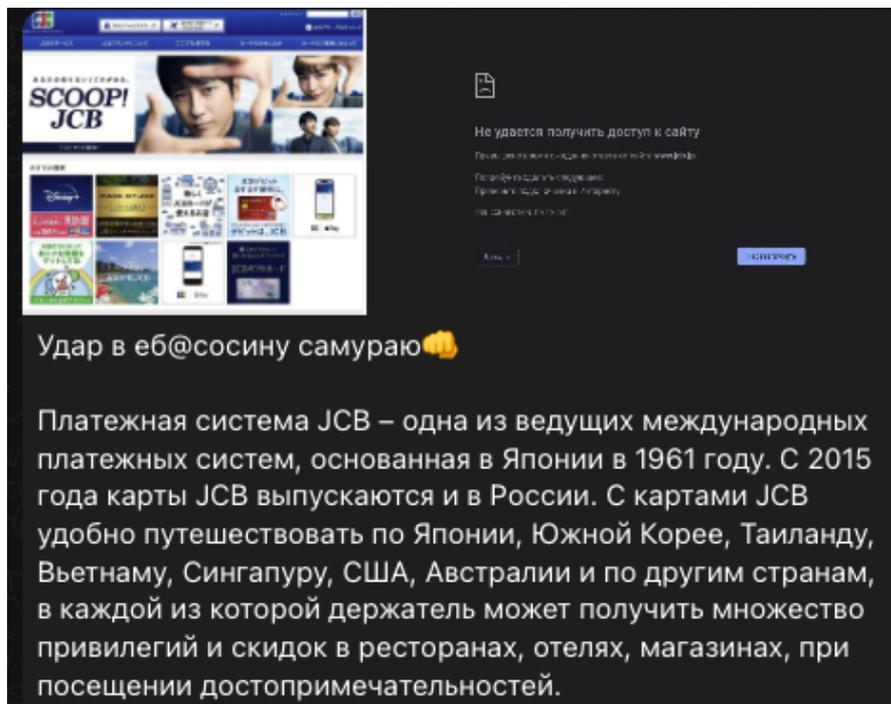


e-Govへの接続ができないことを伝える総務省のツイート



eLTAXへの接続ができないことを伝える総務省のツイート

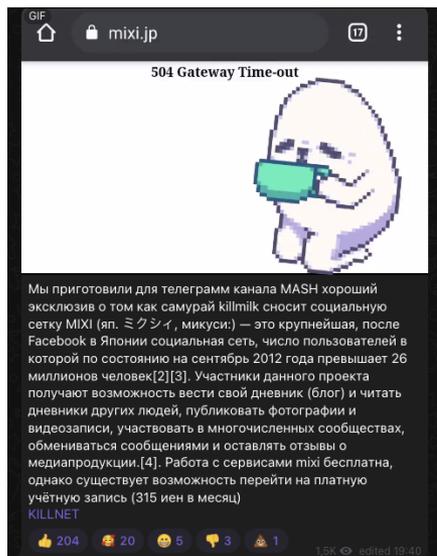
- 続けて、午後5時17分ごろには「汚いサムライに蹴りをいれる」という説明文と、JCBの公式Webサイト（www.jcb.jp）にサイバー攻撃を仕掛けたと思われる画像を投稿。



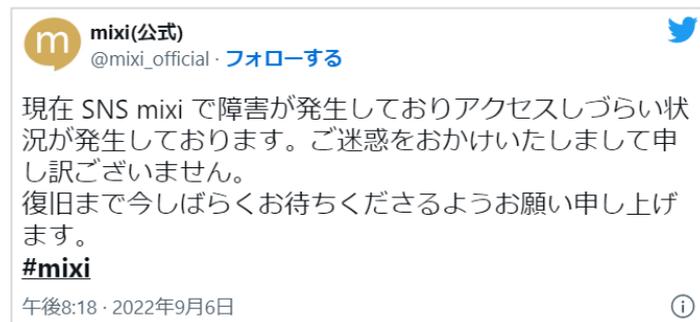
JCBへのサイバー攻撃を示唆する投稿

Killnetの攻撃 ～ミクシィ～

- 午後5時48分 攻撃候補のリクエストを8万を超えるグループメンバーに呼び掛けた。
- これに応じてKillnetのメンバーが多数のサイトをチャットに投稿した。
(次ページに投稿された代表的なサイトを記載)
- 午後7時28分 メンバーが示したサイトの一つであるミクシィを攻撃したことを示唆する投稿を行った。



ミクシィへの攻撃を示唆する投稿



接続できないことを伝えるmixiのツイート

Killnetメンバーによって候補として挙げられたサイト (主要なサイトのみの抜粋)



東京大学 www.u-tokyo.ac.jp
日本航空 www.jal.com
ANA www.ana.co.jp
Peach www.flypeach.com
首相官邸 www.kantei.go.jp
SBI Holdings www.sbigroup.co.jp
外務省 www.mofa.go.jp
JR東海 jr-central.co.jp
第一生命 www.dai-ichi-life.co.jp
KDDI www.kddi.com
みずほフィナンシャルグループ www.mizuho-fg.co.jp
三井住友フィナンシャルグループ www.smfg.co.jp
SoftBankGroup group.softbank
日本郵政 www.japanpost.jp
三菱UFJフィナンシャルグループ www.mufig.jp
NTTグループ group.ntt
みずほフィナンシャルグループ www.mizuhogroup.com
ソニー sony.com
トレンドマイクロ www.trendmicro.com
ハイパーダイヤ www.hyperdia.com
Explore Japan m.jrpass.com
講談社 www.kodansha.co.jp
アニマックス www.animax.co.jp
NHK www.nhk.or.jp
フジテレビ www.fujitv.co.jp

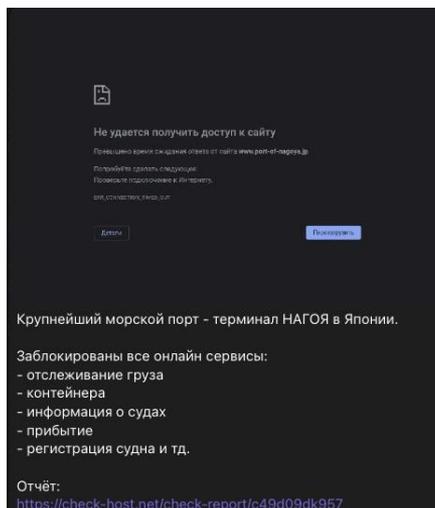
小学館 www.shogakukan.co.jp
集英社 www.shueisha.co.jp
双葉社 www.futabasha.co.jp
トムスエンタテインメント www.tms-e.co.jp
東宝 www.toho.co.jp
コナミ www.konami.com
ヤフー news.yahoo.co.jp
NTTレゾナント www.goo.ne.jp
野村証券 www.nomura.com
衆議院 www.shugiin.go.jp
自由民主党 www.jimin.jp
宮内庁 www.kunaicho.go.jp
警察庁 www.npa.go.jp
TRON Forum www.tron.org
広島市 city.hiroshima.jp
長崎市 city.nagasaki.lg.jp
さやの湯処 www.sayanoyudokoro.co.jp
小田急リゾート www.hakoneyuryo.jp
鬼怒川温泉ホテル www.kinugawaonsenhotel.com
財務省 www.mof.go.jp
NTT docomo www.docomo.ne.jp
Line mobile.line.me
フォビジャパン www.huobi.co.jp
ビットフライヤー bitflyer.com
北野天満宮 www.kitanotenmangu.or.jp

- 午後10時13分 名古屋港へ攻撃を示す投稿を行った。

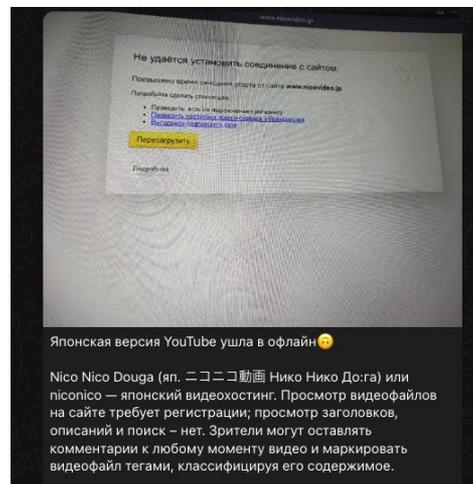
攻撃が成功したことを示す証拠も投稿された。

- 午前0時00分 ニコニコ動画への攻撃を示す投稿を行った。

攻撃の証拠はロシア等の特定の地域からのアクセスができなかったことを示しているが日本のユーザへの影響については確認できていない。

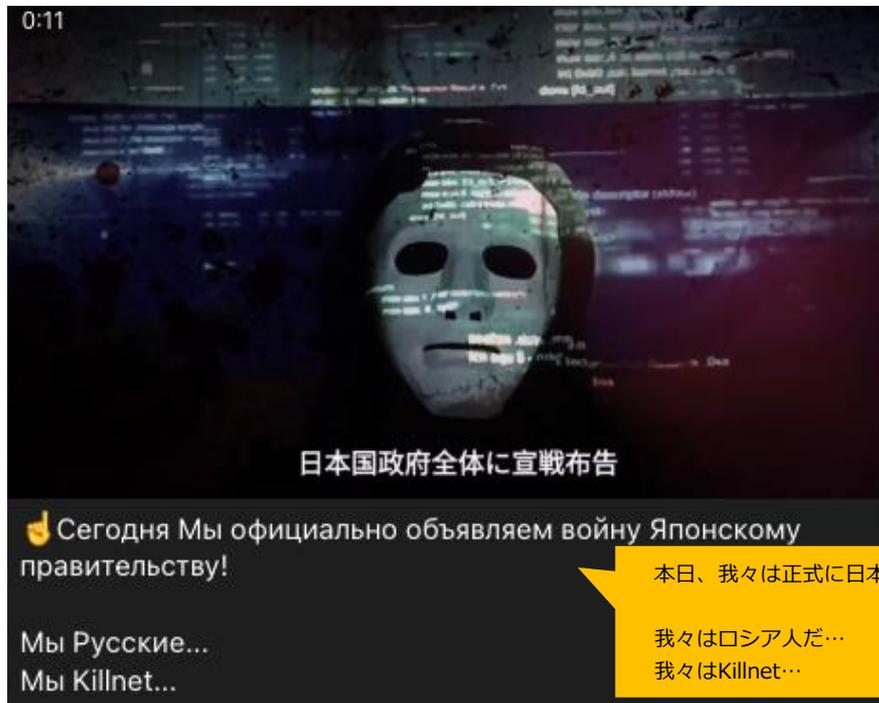


名古屋港への攻撃を示唆する投稿



ニコニコ動画への攻撃を示唆する投稿

- 7日午後6時29分頃、「日本政府全体に宣戦布告」という日本語字幕付きの動画を投稿した。



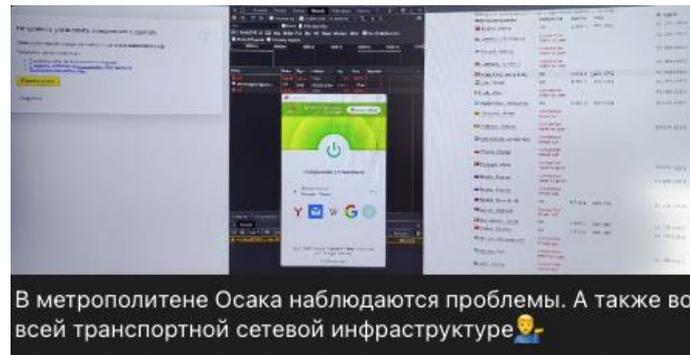
Killnetによる日本政府への宣戦布告

Killnetの攻撃 ～東京メトロと大阪メトロ～

- 9月7日午後7時頃、東京メトロに対して攻撃を示す投稿を行った。
攻撃が成功したことを示す証跡も投稿された。
- 続いて午後9時48分、大阪メトロに対して攻撃を示す投稿を行った。
攻撃が成功したことを示す証跡も投稿された。



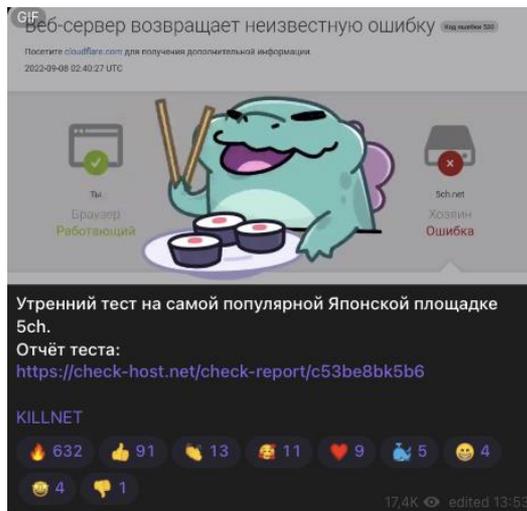
東京メトロへの攻撃を示唆する投稿



大阪メトロへの攻撃を示唆する投稿

Killnetの攻撃 ~5ちゃんねる~

- 9月8日、5ちゃんねるへの攻撃を示す投稿を行った。
攻撃が成功したことを示す証拠も投稿された。



5ちゃんねるへの攻撃を示唆する投稿



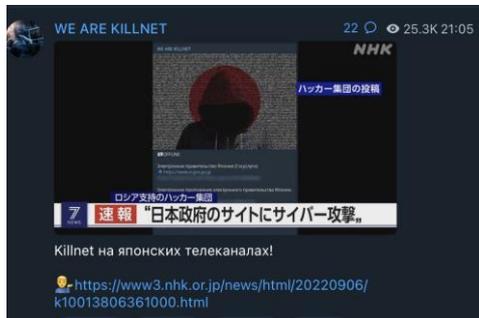
攻撃成功の証拠の投稿

- Killnet は、親ロシア派のハッカーグループで、ウクライナを支持する国々を標的にする。
- 2022年9月現在で8万8千人を超えるメンバーを抱え、親ロシア派としては最大規模を誇る。
- DDoSを使った攻撃を行うことが知られている。また、このグループは他のDDoSより帯域幅をほとんど利用しない slow httpと呼ばれる攻撃手法を多用している。
- ロシアのウクライナへの侵攻以降、ルーマニアの政府組織、イタリア国立政府サイトの Web サイトに対して、DDoS 攻撃を行った。
- 2022年8月1日、米国がウクライナに供給している M142高機動砲兵ロケット システム (HIMARS) やFGM-148(ジャベリン) を製造している米国の軍事会社ロッキード マーチンに対して攻撃開始を宣言、DDoSや従業員の情報漏えい等の攻撃を行った。
- 2022年6月27日に公開されたNHKのインタビューで、日本について「ウクライナを支援している国を攻撃している。」 「日本も例外ではない。現時点では優先順位は低いが、日本がロシアに敵対的であるという事実を忘れてはいない」と答えている。

出典 : <https://www.wired.com/story/russia-hacking-xaknet-killnet/>
<https://www.techcentral.ie/russian-hackers-declare-war-on-10-countries-after-failed-eurovision-ddos-attack/>
<https://economie.hotnews.ro/stiri-telecom-25525633-cine-este-gruparea-hackeri-killnet-care-atacat-site-urile-guvernului-armatei-romaniei.htm>
<https://www.newsweek.com/deadly-cyberwarfare-warning-russian-hacker-killnet-1731949>
<https://www3.nhk.or.jp/news/html/20220627/k10013690121000.html>
<https://www3.nhk.or.jp/news/html/20220627/k10013690121000.html>

その後のKillnetの投稿

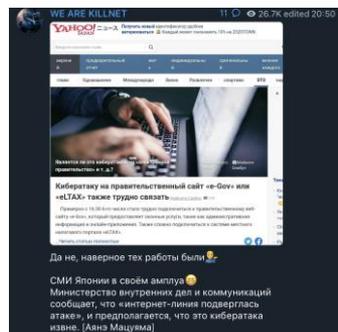
- 以降、日本の報道に取り上げられた様子を「Killnetが日本のテレビに登場」や「サムライがみとめたKillnet」等とコメントをつけて投稿しており、各種メディアにて報道されていることや、twitterで騒ぎになっていることに繰り返し、反応を示している。



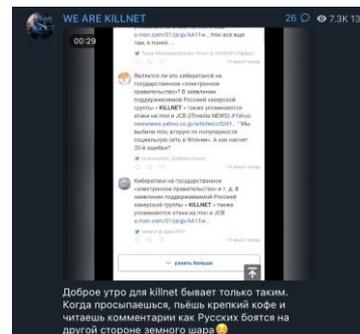
日本のTVでKillnetが放送されていることを伝える投稿



日本への攻撃が中国でニュースになっていることを伝える投稿



ニュースサイトでKillnetが話題になっていることを伝える投稿



TwitterでKillnetが話題になっていることを伝える投稿

「ポストーク2022」との関連性

- ロシア軍は、9月1日から7日までの間、ロシア軍は日本海を含む極東での大規模軍事演習「ポストーク2022」を実施していた。
- 9月6日には、プーチン大統領も視察に訪れた。
- Killnetによる日本を狙った一連の攻撃は、これにタイミングをあわせて行われた可能性がある。



ポストーク2022を視察するプーチン大統領

- 8月6日、新興グループ「HeawsNet」は、「これらの国々に攻撃を行っていく」と述べ、攻撃対象の21の国のリストを投稿した。
- 現在のところ、「HeawsNet」による日本に対しての攻撃は確認されていない。



HeawsNetのテレグラム

ハローワールド！

私たちはDDoS攻撃に関する新しい軍団だ。
我々の使命はウクライナ人に復讐することである。
これらの国に対して攻撃を行う予定だ。

1. アメリカ合衆国
2. オーストラリア
3. アルバニア
4. アンドラ
5. イギリス
- (中略)
21. 日本

- 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注意ください。



NTT

Security Holdings