Black BastaランサムウェアのDNS調査でOneNoteと宅配便のなりすましを発見

目次

要旨

2022年に最も急速に拡散したランサムウェアの一つは、Black Bastaでした。2022年4月に初めて検出され、同年9月までに北米、欧州、アジアの約100の組織が被害に遭いました。Ransomware-as-a-Service（RaaS）マルウェアであるBlack Bastaは、身代金を取るために被害者に二重の恐喝を用います。すなわち、データの暗号化のみならず被害者のデータ抜き取りも行い、身代金を支払わなければデータを公開すると脅すのです。

ExtraHopのエキスパートであるJosh Snowは最近、Black Bastaの検出方法を披露しました。これをきっかけに、WhoisXML APIでは、Black Bastaのセキュリティ侵害インジケーター（IoC）（5つのドメイン名と51個のIPアドレス）をもとに調査の網を広げました。その結果、以下を新たに発見しました。

- ネームサーバーおよびWHOISの登録者情報がIoCと共通していた980個のドメイン名
- IoCとされたIPアドレスでホストしていた18個のドメイン名
- 宅配便のウェブサイトやOneNoteドキュメントを装ったマルウェア配布キャンペーンと関連している可能性
- 悪意あるドメイン名と同じネームサーバーを使用していた宅配便関連ドメイン名の14%も、悪意あるドメイン名としてすでにフラグが立っていた

IoCに文脈を与える

当社はまず、Black BastaのIoCとしてタグ付けされたドメイン名やIPアドレスと共通の特徴を明らかにすることから始めました。

WHOIS history lookupで調べた結果、SentinelOneが特定した5つのドメインIoCは全て、WHOIS

レコードの一部を非公開にしていました。また、そのうち3つは、WhoisSecureというプライバシー保護業者を使っていました。また、ほとんどはOwnRegistrar, Inc.というレジストラを介して登録されたドメイン名で、かつ使用していたネームサーバー事業者はCloudflareでした。さらに、それらのドメイン名の登録日はほぼ同じで、2022年6月のある時点で登録されたものが4つありました。これらの共通点を以下に整理しました。

WHOISデータポイント	Common WHOIS Record IoCs
登録者の連絡先情報	WhoisSecure
ネームサーバー	• *****[.]ns[.]cloudflare[.]com | *****hine[.]ns[.]cloudflare[.]com • ****[.]ns[.]cloudflare[.]com | ****[.]ns[.]cloudflare[.]com • *****[.]njalla[.]no |*****[.]njalla[.]in | *****[.]njalla[.]fo
レジストラ	OwnRegistrar, Inc.
登録年月	June 2022

残りのIoCはSentinelOneとTrend Microがリストアップ したIPアドレスです。それらをbulk IP geolocation lookupにかけたところ、以下が判明しました。

- IoCとされた51個のIPアドレスのうち30個は、本稿執筆時点で名前解決が有効
- IPジオロケーションの上位国は、オランダ、ドイツ、ルーマニア、英国
- 上位ISPは、Bunea Telecom SRL、Panamaserver.com、The Constant Company, LLC、Stark Industries Solutions Ltd.

IoCリストの拡張：WHOISとIPアドレスの関連性を読み解く

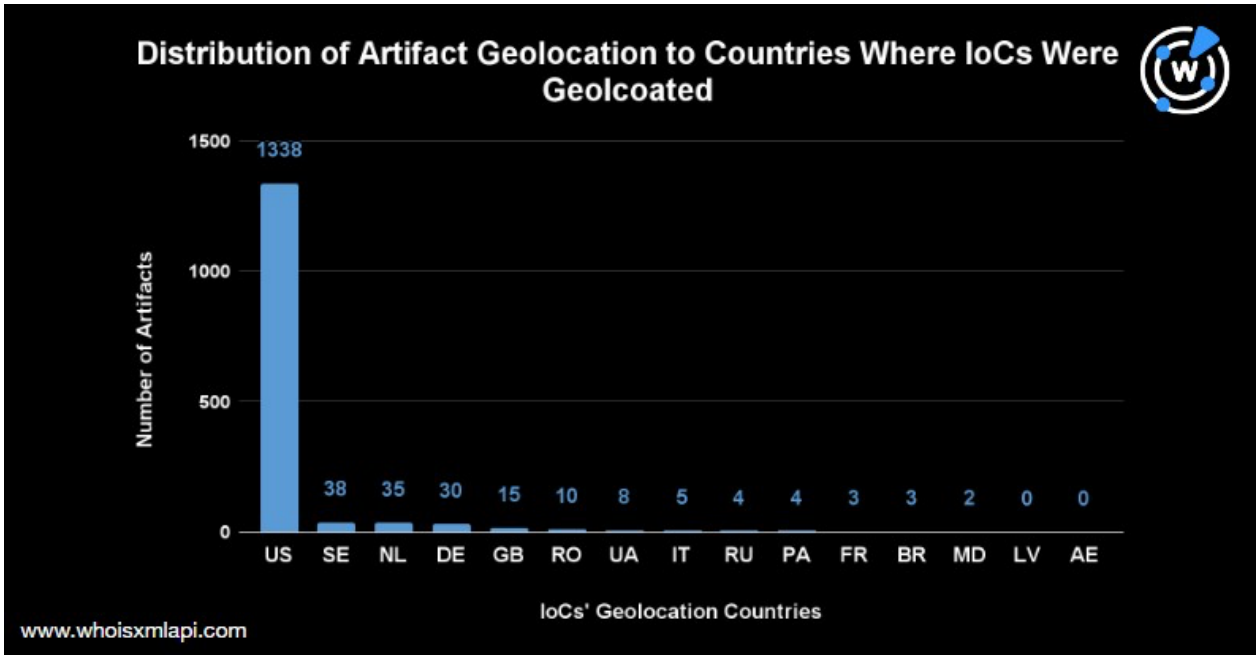
次に、上記の文脈情報を用いて、Black Bastaのアーティファクトと考えられる関連ドメイン名を探し出しました。

Reverse WHOIS searchesでIoCを逆引きしたところ、980個のアーティファクトが見つかりました。そのうち50%超は2023年1月1日から3月15日までの間に登録されたもので、現在はネームサーバーと登録者の国が1つのIoCと共通しています。

また、別のIoCのネームサーバーを調べたところ、関連性のあるドメイン名は60個しかありませんでした。したがって、そのインフラは一般に共有されておらず、悪意があるかもしれません。同じことが、IoCとしてタグ付けされたIPアドレスにも言えます。51個のIPアドレスをReverse IP Lookupで検索しましたが、関連するドメイン名は18個しか発見できませんでした。

全てのアーティファクトをbulk IP geolocation lookupで一括検索したところ、1,000個近いドメイン名のうち64%は名前解決が有効で、うち19個はIoCとされたIPアドレスでホストしていることがわかりました。つまり、一部の悪意あるプロパティは有効なままでした。

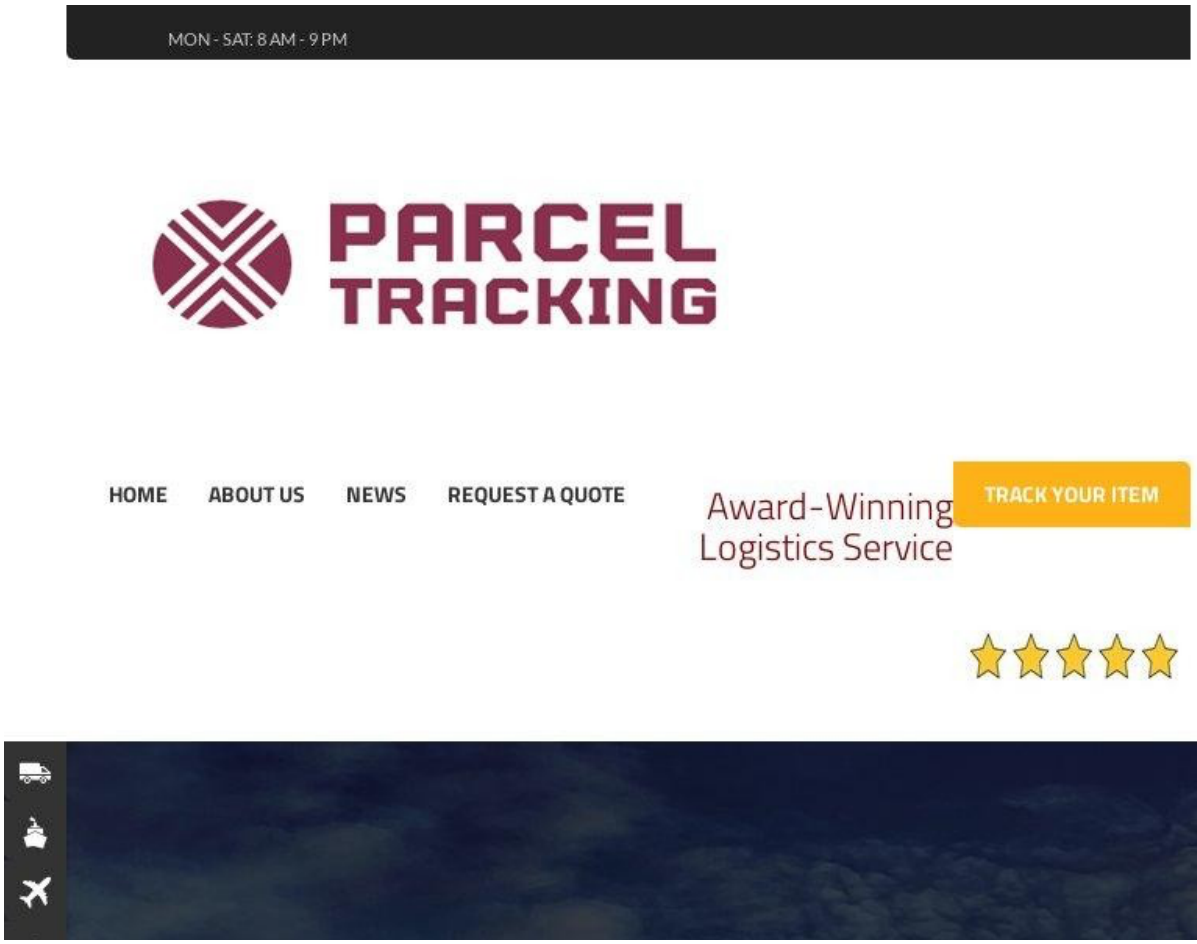
さらに、名前解決の95%はIoCの地理的位置と同じ場所にありました。下のグラフの通りです。



アーティファクトの調査：関連する脅威を発見

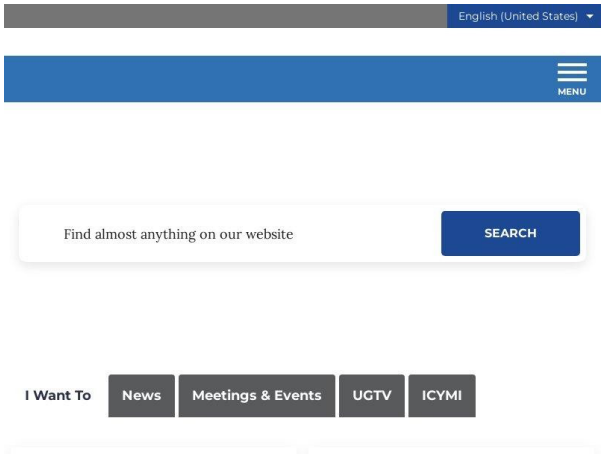
続いて、関連性のあるドメイン名がどのように利用されているのかを探りました。マルウェアの一括チェックにより13個の悪意あるアーティファクトが発見されましたが、その中で最も注目すべきはOneNoteを模倣したドメイン名です。これまでのセキュリティ調査で、Black BastaはQbotと結び付いていることがわかっています。Qbotは、偽のOneNoteドキュメントを介した配布が最近確認されたマルウェアファミリーです。

また、郵便や宅配便を模倣した悪意あるドメイン名もありました。あるドメイン名はAustralian Postを標的としているように見え、別のドメイン名は***post***や***parcel***といった文字列を含んでいました。それらのドメイン名は名前解決しなくなっていましたが、その一方で、宅配便追跡サイトをホストし続けるフラグのないアーティファクトが1つ見つかりました。

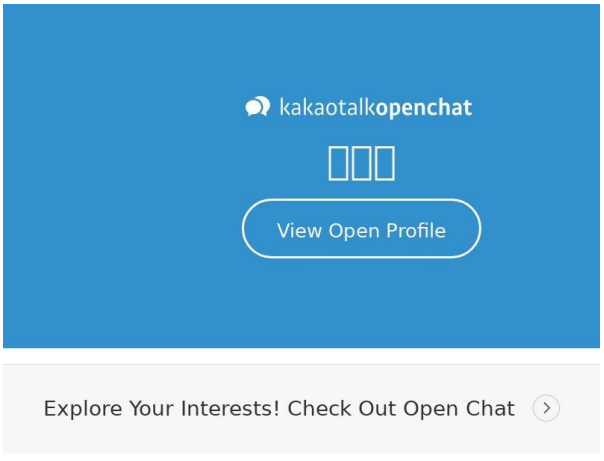


*parceltracking[.]express*のスクリーンショット

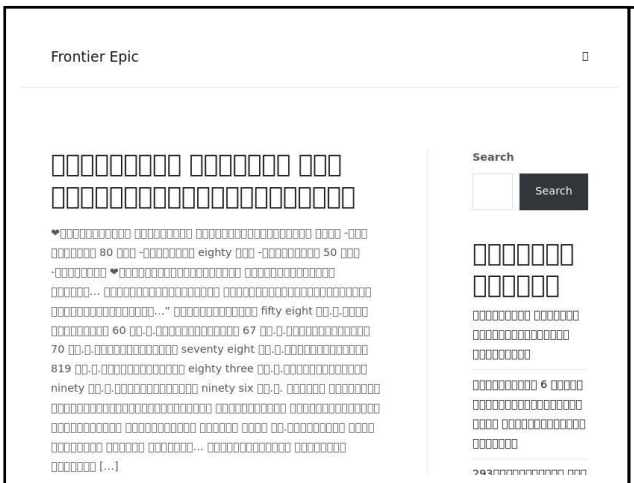
悪意あるドメイン名の中には、有効なコンテンツをホストしているものもありました。以下はその例です。



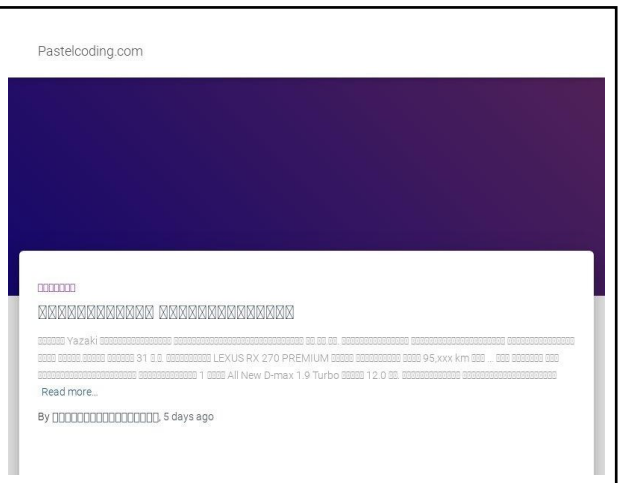
*wycokckgov[.]org*のスクリーンショット



*hts[.]guru*のスクリーンショット



frontierepic[.]comのスクリーンショット



pastelcoding[.]comのスクリーンショット

偽の宅配便を探る

Black Bastaの脅威アクターは、フィッシングやスピアフィッシングを利用して被害者のシステムに最初にアクセスし、特にQbotの手法を真似て、マルウェアをOneNoteドキュメントに偽装したことが確認されています。

OneNoteを介したマルウェア配布は、別の脅威レポートで最近取り上げました。そこで、今回は宅配便をテーマにした悪意あるドメイン名や不審なドメイン名を掘り下げていきます。

Checkparcel[.]org（悪意ありとのフラグが立ったアーティファクト）とparceltracking[.]express（フラグがないアーティファクト）は同じネームサーバーを共有していました。そこで、検索キーワードに***post***と***parcel***を含めて逆WHOIS検索を実行しました。その結果259個のドメイン名が見つかり、そのうち14%は悪意があるドメイン名と報告されました。

フラグが立ったドメイン名のほとんどは、以下のような北米、欧州、アジアの郵便・宅配便サービスを対象としたサイバースクワッティングドメインでした。

- Australian Post
- Canada Post
- Chronopost
- Postage Depot
- Posten Norge
- U.S. Postal Service (USPS)

—

Black Bastaはエンドポイントでの検知と対応（EDR）のソリューションを停止させる可能性があるため、そのIoCの検出がサイバーセキュリティ業界で喫緊の課題となっています。それらのIoCは、より広範囲の悪意あるインフラの一部となっている可能性があります。したがって、IoCリストを拡張してさらに多くのアーティファクトを発見することで、脅威アクターによって作成はされたもののまだ展開には至っていないウェブプロパティから組織を守ることができます。

今回当社が行った調査で1,200超にのぼる未報告のアーティファクトが見つかりましたが、そのうち数十個はすでに悪意あるキャンペーンでの使用が確認されており、さらに疑わしいものでした。

同様の調査をご希望のお客様、または本調査のデーター式をご希望のお客様は、こちらまでお気軽にお問い合わせください.

付録：アーティファクトとIoCの例

Black BastaのIoCの例

- courtlincolnglave[.]com
- jardinoks[.]com
- widisusez[.]com
- purestealconstruction[.]com
- groundworkseasy[.]com
- 185[.]217[.]1[.]23
- 159[.]223[.]236[.]110
- 193[.]29[.]13[.]159
- 193[.]29[.]13[.]216
- 193[.]29[.]13[.]170
- 190[.]123[.]44[.]126
- 190[.]123[.]44[.]130
- 185[.]125[.]206[.]218
- 95[.]179[.]161[.]101
- 69[.]46[.]15[.]147
- 87[.]247[.]152[.]249
- 185[.]107[.]80[.]78
- 177[.]54[.]145[.]139
- 109[.]248[.]149[.]137
- 109[.]170[.]6[.]150
- 95[.]211[.]185[.]11
- 176[.]77[.]112[.]74
- 193[.]105[.]7[.]122
- 5[.]62[.]43[.]252
- 45[.]67[.]229[.]148
- 78[.]128[.]112[.]217
- 45[.]153[.]241[.]167
- 209[.]250[.]236[.]75
- 139[.]162[.]191[.]118
- 5[.]196[.]124[.]228
- 185[.]16[.]40[.]67
- 45[.]133[.]216[.]39
- 45[.]87[.]154[.]208
- 213[.]109[.]192[.]116
- 24[.]178[.]196[.]44:2222
- 37[.]186[.]54[.]185:995
- 39[.]44[.]144[.]182:995
- 45[.]63[.]1[.]88:443
- 46[.]176[.]222[.]241:995
- 47[.]23[.]89[.]126:995
- 72[.]12[.]115[.]15:22
- 72[.]76[.]94[.]52:443
- 72[.]252[.]157[.]37:995
- 72[.]252[.]157[.]212:990
- 73[.]67[.]152[.]122:2222
- 75[.]99[.]168[.]46:61201
- 103[.]246[.]242[.]230:443
- 113[.]89[.]5[.]177:995
- 148[.]0[.]57[.]82:443
- 167[.]86[.]165[.]191:443
- 173[.]174[.]216[.]185:443
- 180[.]129[.]20[.]53:995
- 190[.]252[.]242[.]214:443
- 217[.]128[.]122[.]16:2222
- 172[.]105[.]88[.]234:4001
- 23[.]106[.]160[.]188

IoCのIPアドレスまたはネームサーバーを共用していた関連ドメイン名の例

- leatimahtmete[.]tk
- micklyvishealthnappsour[.]ga
- masterskaja-ujuta[.]ru
- dogonion[.]com
- stuarthicks[.]me
- homeatsantiago[.]cl
- thedonsproject[.]xyz
- kmsmbs[.]com
- cleveorenbu[.]cyou
- lookblinds[.]co[.]uk
- plannerchart[.]com
- reelsvector[.]com
- vidmatesnap[.]com
- glutagunarentia[.]tk
- rapidmemopad[.]com
- go3-alaskusa[.]online
- rozsacsaszar[.]com
- lessmegituli[.]tk
- lightbotbuild[.]com
- malhotrahospitals[.]in
- wallstreettext[.]com
- stuffcrafts[.]com
- pastelcoding[.]com
- awesomeever[.]com
- frontierepic[.]com
- formatweekly[.]com
- subslowly[.]com
- softbacktheme[.]com
- shortcutsign[.]com
- sinclone[.]com
- tunerengine[.]com
- singlefacade[.]com
- groundmedium[.]com
- groupsharepoint[.]com
- catchercloud[.]com
- leassonbrowse[.]com
- yocarz[.]in
- ptb5qlyuzusjiwegg3tr4z6mv2vtye3n[.]info
- oroluntaquals[.]tk
- ahqtraders[.]com
- courtbravehills[.]com
- wascre[.]com
- chronicprofits[.]com
- mixesu[.]com
- kobitatu[.]com
- tribimilglisbag[.]tk
- sconexlidef[.]ml
- vingdelitora[.]tk
- palitamili[.]tk
- rubtuperwhe[.]ml
- reicivol[.]tk
- lanpaytop[.]tk
- quitinilimo[.]ml
- listconsingcorbei[.]tk
- urgapacon[.]ga
- sentcribricco[.]tk
- amunenis[.]tk
- ciochoplei[.]tk
- precembuyma[.]tk
- direct-debit-authentication[.]com
- mailnexus[.]org
- rapid77[.]info
- kaizenedge[.]capital
- mymaii[.]org
- binharby[.]org
- variant[.]bet
- mochamail[.]coffee
- aqrabathospital[.]org
- chatgptree[.]org
- beatsource[.]video
- frutor[.]org

- interchange[.]exchange
- enginesupport[.]network
- turningpointmag[.]org
- blocksafari[.]org
- financetips[.]money
- orange-swap[.]finance
- capitalt-trust[.]ltd
- capital-trust[.]ltd
- champaigncountyil[.]org
- ziu[.]red
- wikitorrent[.]org
- piratehive[.]org
- pancakeswapv3[.]finance
- systemguard[.]org
- nitrohex[.]org
- gott[.]haus
- recht[.]haus
- sala[.]bet
- mailaustralia[.]org
- post-fastdelivery[.]org
- tm3[.]blue
- chytry[.]house
- bone[.]tools
- drughub[.]business
- drughub[.]network
- drughub[.]market
- drughub[.]center
- capinvest[.]limited
- sentinelcapital[.]group

2023年3月15日時点の悪意あるアーティファクトの例

- pastelcoding[.]com
- frontierepic[.]com
- hts[.]guru
- checkparcel[.]org
- checkfees[.]org
- mypostaus[.]org
- wycokckgov[.]org
- postli[.]org
- gigafilesnote[.]com
- anyaaplanet[.]xyz
- chilesand[.]com
- dinomobsonke[.]xyz
- staratilas[.]com

Checkparcel[.]orgと同じネームサーバーを使用していた宅配便関連ドメイン名の例

- postparceltracking[.]net
- parceldeliverycdn[.]net
- servicepost-parcel[.]com
- redirectparcel[.]net
- parcelassist-post[.]com
- checkparcel[.]org
- parcelcollect-depot[.]com
- trackingparcelrequest[.]com
- websecureparcel[.]com
- parceltracking[.]express
- parcelrescheduleau[.]com
- processparcelrequest[.]com
- myuspsparcel[.]net
- trackparcelau[.]com
- trackparcel192[.]com
- postdepot-parcel[.]com
- ausparcels[.]org
- parcelreroute[.]com
- parcelsapp001[.]com
- parcelupdateonline[.]com
- parcelredelivery8[.]com
- parceldeliveryredirect[.]com
- parceldeliverybooking[.]com
- parcelmyusps-1[.]com

- expresdhlparcel[.]com
- expressdhlparcel[.]com
- trackparcel[.]app
- bookparceldelivery[.]com
- trackparcel[.]express
- usptrackingparcelz[.]com
- wxwposters[.]com
- csuivi-chronopost-fr[.]com
- postparceltracking[.]net
- garopost[.]com
- repostcrusader[.]com
- statspostback[.]com
- post-fastdelivery[.]org
- postb[.]org
- itemservicepost[.]com
- openpost[.]com
- wooripost[.]com
- ceskapostaonline[.]com
- mypostaustralia[.]org
- exerciserrepost[.]net
- deliveryaupost[.]com
- servicepost-parcel[.]com
- posteingang[.]wtf
- package-depotpost[.]com
- skvela-postava[.]com
- laposte-suivicolis[.]fr

2023年3月16日時点の悪意ある小包関連サイバースクワッティングドメインの例

- postparceltracking[.]net
- parceldeliverycdn[.]net
- servicepost-parcel[.]com
- redirectparcel[.]net
- checkparcel[.]org
- parcelrescheduleau[.]com
- trackparcelau[.]com
- postdepot-parcel[.]com
- ausparcels[.]org
- expresdhlparcel[.]com
- postparceltracking[.]net
- ceskapostaonline[.]com
- deliveryaupost[.]com
- servicearrange-post[.]com
- aupost-reschedule[.]com
- can-delpost[.]com
- chronopost-express-inc[.]com
- cad-poste[.]com
- mypostaus[.]org
- chronopost-votre-suivi[.]com