Black Basta Ransomware DNS Investigation Led to OneNote and Courier Impersonation

Table of Contents

Executive Report

Among the most active and rapidly spreading ransomware in 2022 was Black Basta. It was first detected in April 2022 and victimized nearly 100 organizations in North America, Europe, and Asia by September that same year. As a ransomware-as-a-service (RaaS) malware, Black Basta employs double extortion to force victims to pay the ransom. Aside from data encryption, the threat actors exfiltrated the victims' data and threatened to release it if they wouldn't pay.

ExtraHop expert Josh Snow recently demonstrated how to detect Black Basta ransomware, inspiring WhoisXML API researchers to investigate and expand the threat's indicators of compromise (IoCs). From 5 domains and 51 IP addresses tagged as IoCs, we found the following:

- 980 domains sharing the IoCs' name servers and WHOIS ownership details
- 18 domains hosted on the IP addresses tagged as IoCs
- Possible connections to malware distribution campaigns disguised as courier websites and OneNote documents
- 14% of the courier-related domains sharing a malicious domain's name servers were also flagged as malicious

Threat Investigation: Providing Context to the IoCs

We began by uncovering patterns and common characteristics among the domains and IP addresses tagged as Black Basta ransomware IoCs.

Based on WHOIS history lookup results, we determined that all five domain IoCs from SentinelOne had redacted WHOIS records—three of them used WhoisSecure as their privacy protection provider. Most of the domains indicated OwnRegistrar, Inc. as their registrar and

used the same name server provider (Cloudflare). Their registration dates were also similar, with four created sometime in June 2022. We tabulated these commonalities below.

WHOIS Data Point	Common WHOIS Record IoCs
Registrant contact detail	WhoisSecure
Name servers	• *****[.]ns[.]cloudflare[.]com | *****hine[.]ns[.]cloudflare[.]com • ****[.]ns[.]cloudflare[.]com | ****[.]ns[.]cloudflare[.]com • *****[.]njalla[.]no |*****[.]njalla[.]in | *****[.]njalla[.]fo
Registrar	OwnRegistrar, Inc.
Creation date	June 2022

The rest of the IoCs were IP addresses listed by SentinelOne and Trend Micro, which we subjected to a bulk IP geolocation lookup that revealed the following:

- 30 of the 51 IP addresses tagged as IoCs had active resolutions as of this writing.
- The top IP geolocation countries were the Netherlands, Germany, Romania, and the U.K.
- The top ISPs were Bunea Telecom SRL; Panamaserver.com; The Constant Company, LLC; and Stark Industries Solutions Ltd.

IoC Expansion: Mapping Out WHOIS and IP Connections

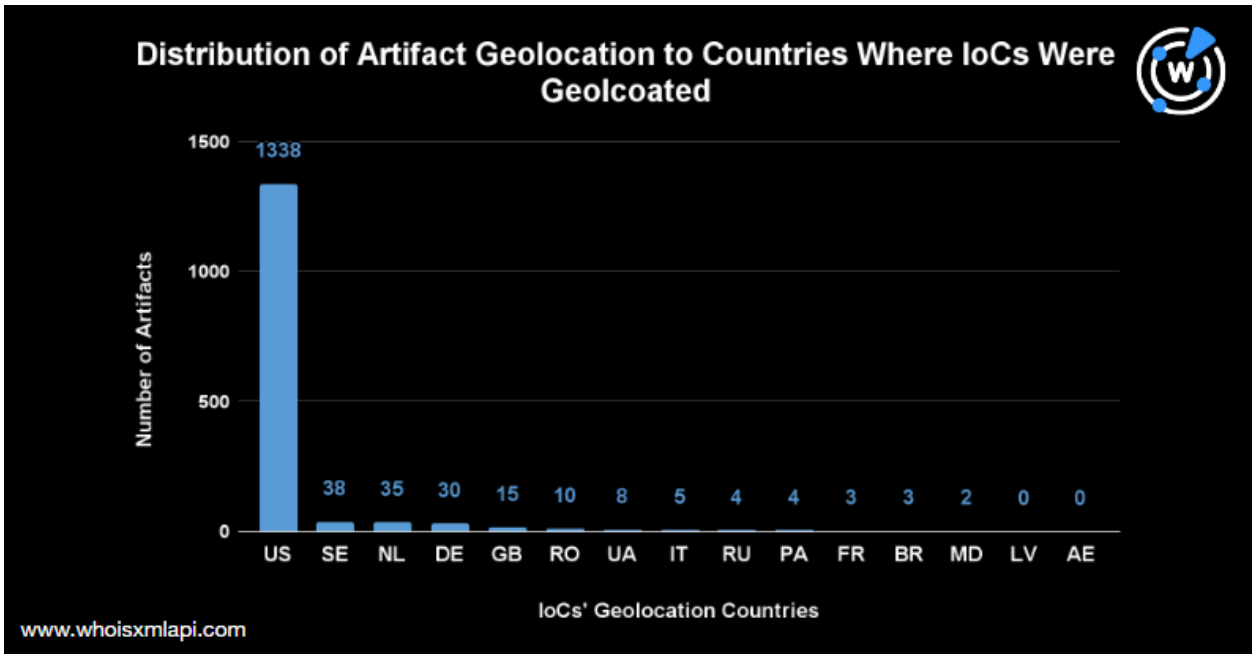
We used the contextual information above to find connected domains that could be considered Black Basta ransomware artifacts.

Reverse WHOIS searches for the IoCs resulted in the discovery of 980 artifacts, more than 50% of which were added between 1 January and 15 March 2023 and currently shared one of the IoCs' name servers and registrant countries.

Another IoC's name server lookup yielded only 60 connected domains, revealing the possibility that its infrastructure is not publicly shared and is potentially malicious. The same could be said for the IP addresses tagged as IoCs. Despite running 51 IP addresses on Reverse IP Lookup, we only uncovered 18 connected domains.

A bulk IP geolocation lookup for all the artifacts also yielded interesting results. Out of almost 1,000 domains, 64% had active resolutions, 19 of which were hosted on the IP addresses tagged as IoCs, telling us that some malicious properties remained active.

Furthermore, about 95% of the resolutions were geolocated in countries where the IoCs were also geolocated. These are plotted in the following chart.



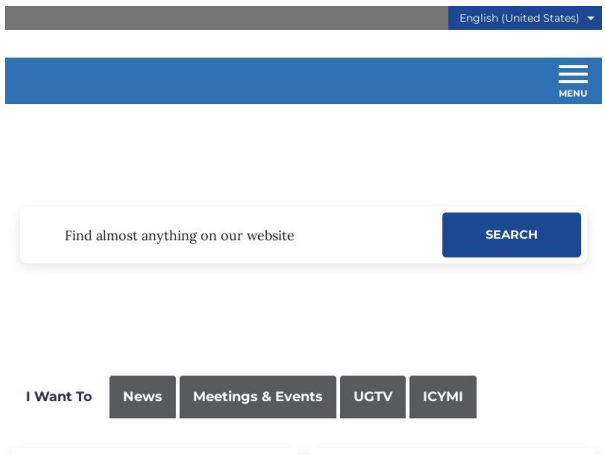
Artifact Investigation: Finding Related Threats

We then sought to find out how the connected domains were used. A bulk malware check led to the discovery of 13 malicious artifacts, the most notable of which is a domain mimicking OneNote. Previous security investigations tied Black Basta to Qbot, a malware family recently seen distributed through fake OneNote documents.

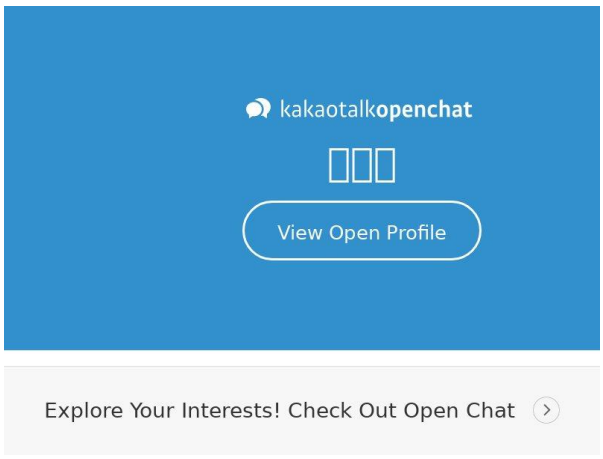
Other malicious domains imitated postal and courier services. One domain seemingly targeted the Australian Post, while others contained the strings ***post*** and ***parcel***. While these courier-related malicious domains no longer resolved, we found an unflagged artifact that continued to host a parcel-tracking website.

Screenshot of parceltracking[.]express

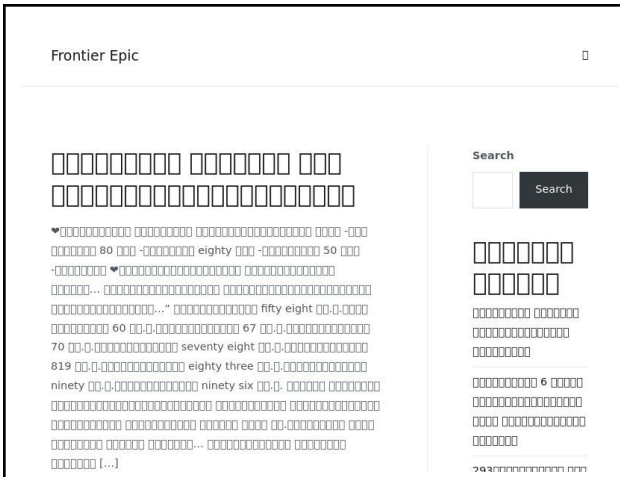
Some of the malicious domains also hosted live content. Below are some examples.



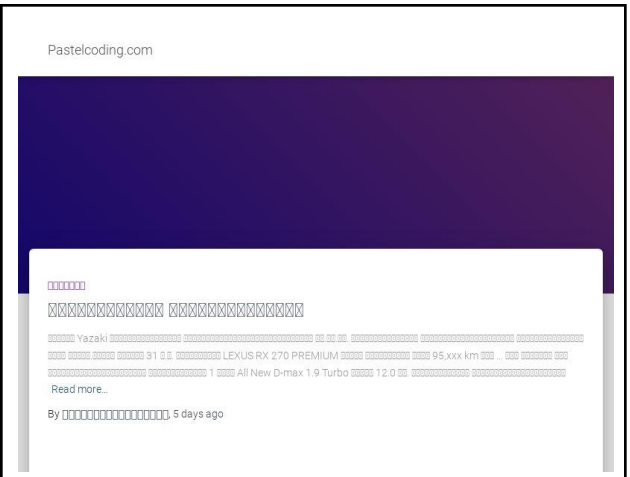
Screenshot of wycokckgov[.]org



Screenshot of hts[.]guru



Screenshot of frontierepic[.]com



Screenshot of pastelcoding[.]com

Exploring Fake Parcels

Black Basta ransomware threat actors were seen using phishing and spearphishing to gain initial access to victim systems, notably mimicking Qbot's technique, particularly disguising malware as OneNote documents.

Since we tackled malware distribution through OneNote in a recent threat report, we dedicate this part to digging deeper into parcel-themed malicious and suspicious domains.

Since checkparcel[.]org (artifact flagged as malicious) and parceltracking[.]express (unflagged artifact) shared the same name servers, we ran a reverse WHOIS search and included the strings ***post*** and ***parcel*** as search terms. We found 259 domains, 14% of which were reported to be malicious.

Most of these flagged domains were cybersquatting properties targeting postal and courier services in North America, Europe, and Asia, including the following:

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

—

Detecting Black Basta ransomware IoCs is an urgent concern for the cybersecurity community, especially since it can shut down endpoint detection and response (EDR) solutions. These IoCs could be part of a more extensive malicious infrastructure, and expanding them to uncover additional artifacts can help protect organizations from web properties that the threat actors may have created but haven't deployed yet.

Our investigation led us to more than 1,200 yet-unreported artifacts, dozens of which had already figured in malicious campaigns, and even more appeared suspicious.

If you wish to perform a similar investigation or get access to the full data behind this research, please don't hesitate to contact us.

Appendix: Sample Artifacts and IoCs

Sample Black Basta IoCs

- 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

Sample Connected Domains Sharing the IoCs' IP Hosts or Name Servers

- 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

Sample Malicious Artifacts as of 15 March 2023

- 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

Sample Courier-Related Domains Sharing the Same Name Servers as checkparcel[.]org

- 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

Sample Malicious Courier Cybersquatting Domains as of 16 March 2023

- 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