LockBit Green and phishing that targets organizations

securelist.com/crimeware-report-lockbit-switchsymb/110068/

Authors

Expert GReAT

Introduction

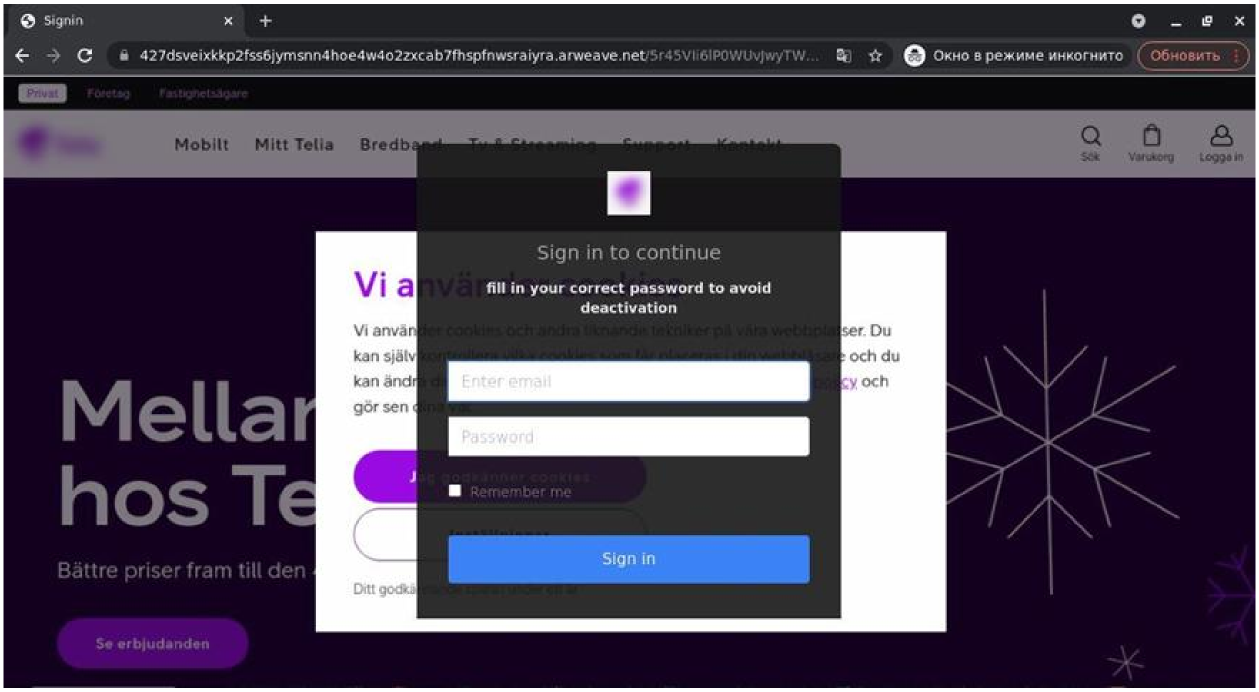
In recent months, we published private reports on a broad range of subjects. We wrote about malware targeting Brazil, about CEO fraud attempts, Andariel, LockBit and others. For this post, we selected three private reports, namely those related to LockBit and phishing campaigns targeting businesses, and prepared excerpts from these. If you have questions or need more information about our crimeware reporting service, contact crimewareintel@kaspersky.com.

Phishing and a kit

Recently we stumbled upon a Business Email Compromise (BEC) case, active since at least Q3 2022. The attackers target German-speaking companies in the DACH region. As in many other BEC cases, they register a domain name that is similar to that used by the attacked organization and typically differs in one or two letters. For reasons unknown, the Reply-to field contains a different email address from the From field. The Reply-to email address does not mimic the target-organization’s domain.

In contrast to BEC campaigns that are targeted and require significant effort from the criminals, ordinary phishing campaigns are relatively simple. This creates opportunities for automation, of which the SwitchSymb phishing kit is one example.

At the end of this past January, we observed a spike in phishing email from a campaign targeting business users, which we have closely monitored. We noticed that the message contained a link to an “email confirmation form”. If one clicked on the link, they found themselves on a page looking very similar to that of the recipient’s domain. The phishing kit was designed to serve multiple campaigns at a time while running one instance on the web server. This was easily demonstrated by modifying the page URL, specifically the reference to the targeted user in it^ the layout of the phishing page would change.


427dsveixkkp2fss6jymsnn4hoe4w4o2zxcab7fhspfnwsraiyra.arweave.net/5r45VIi6lP0WUvJwyTW...

Sign in to continue

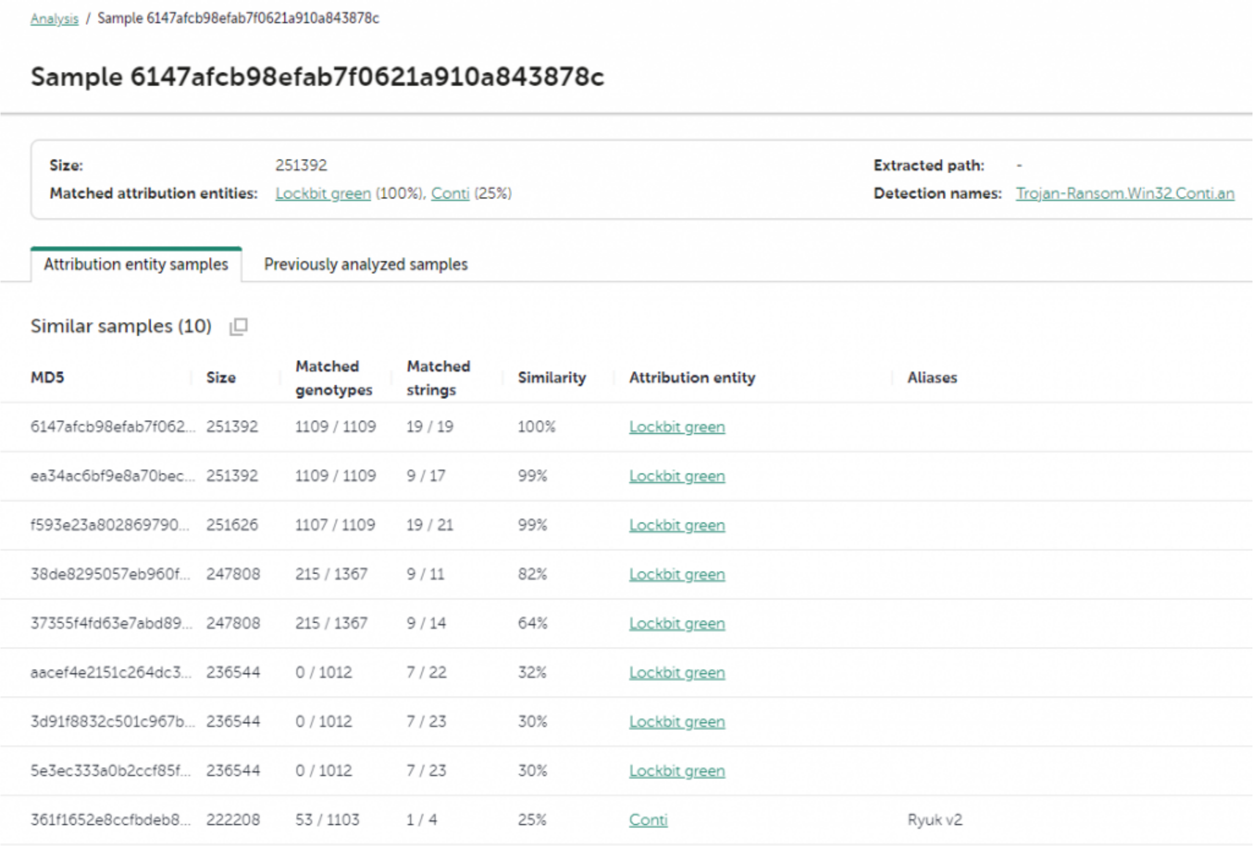
fill in your correct password to avoid deactivation

An example of a SwitchSymb-generated phishing page

LockBit Green

LockBit is one of the most prolific ransomware groups currently active, targeting businesses all over the world. Over time, they have adopted code from other ransomware gangs, such as BlackMatter and DarkSide, making it easier for potential affiliates to operate the ransomware.

Starting in this past February, we have detected a new variant, named “LockBit Green”, which borrows code from the now-defunct Conti gang. According to the Kaspersky Threat Attribution Engine (KTAE), LockBit incorporates 25% of Conti code.



Analysis / Sample 6147afcb98efab7f0621a910a843878c

Sample 6147afcb98efab7f0621a910a843878c

Size:	251392	Extracted path:	-
Matched attribution entities:	Lockbit green (100%), Conti (25%)	Detection names:	Trojan-Ransom.Win32.Conti.an

Similar samples (10)

MD5	Size	Matched genotypes	Matched strings	Similarity	Attribution entity	Aliases
6147afcb98efab7f062...	251392	1109 / 1109	19 / 19	100%	Lockbit green	
ea34ac6bf9e8a70bec...	251392	1109 / 1109	9 / 17	99%	Lockbit green	
f593e23a802869790...	251626	1107 / 1109	19 / 21	99%	Lockbit green	
38de8295057eb960f...	247808	215 / 1367	9 / 11	82%	Lockbit green	
37355f4fd63e7abd89...	247808	215 / 1367	9 / 14	64%	Lockbit green	
aacef4e2151c264dc3...	236544	0 / 1012	7 / 22	32%	Lockbit green	
3d91f8832c501c967b...	236544	0 / 1012	7 / 23	30%	Lockbit green	
5e3ec333a0b2ccf85f...	236544	0 / 1012	7 / 23	30%	Lockbit green	
361f1652e8ccfbdeb8...	222208	53 / 1103	1 / 4	25%	Conti	Ryuk v2

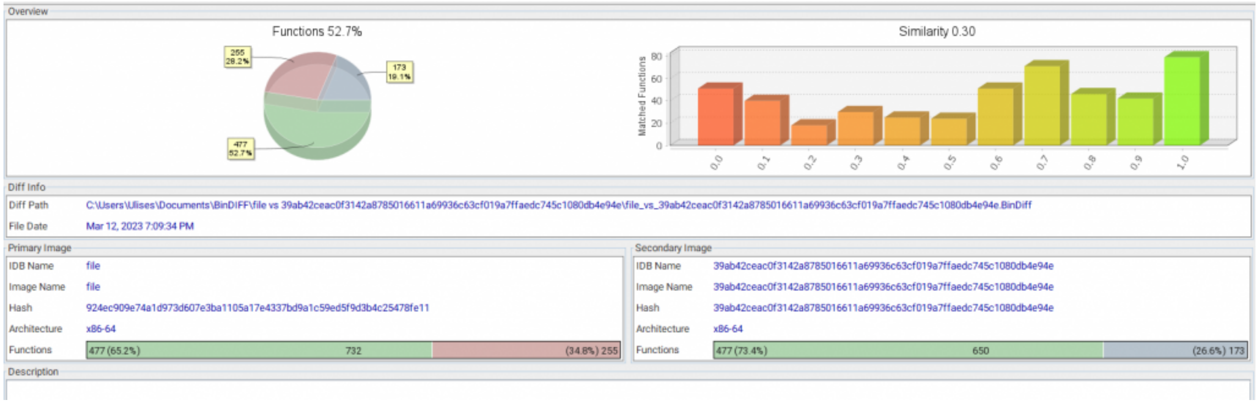
KTAE shows similarities between LockBit Green and Conti

Three pieces of adopted code really stand out: the ransomware note, the command line options and the encryption scheme. Adopting the ransom note makes the least sense. We could not think of a good reason for doing so, but nevertheless, LockBit did it. In terms of command line options, the group added those from Conti to make them available in Lockbit. All the command line options available in Lockbit Green are:

Flag	Functionality
-p folder	Encrypt the selected folder using a single thread
-m local	Encrypt all available drives within multiple threads, each of them
-m net	Encrypt all network shares within multiple threads, each of them
-m all	Encrypt all available drives and Network shares within multiple threads, each of them
-m backups	Flag not available to use on the detected versions but coded inside the ransomware
-size chunk	Functionality to encrypt only part of the files
-log file.log	Possibility to log every action performed by the ransomware

-nomutex	Skip mutex creation

Finally, LockBit adopted the encryption scheme from Conti. The group now usesa custom ChaCha8 implementation to encrypt files with a randomly generated key and nonce that are saved/encrypted with a hard-coded public RSA key.



Diff Info

Diff Path	C:\Users\Ulises\Documents\BinDIFF\file vs 39ab42ceac0f3142a8785016611a69936c63cf019a7ffaedc745c1080db4e94e\file_vs_39ab42ceac0f3142a8785016611a69936c63cf019a7ffaedc745c1080db4e94e.BinDiff
File Date	Mar 12, 2023 7:09:34 PM

Primary Image

IDB Name	file
Image Name	file
Hash	924ec909e74a1d973d607e3ba1105a17e4337bd9a1c59ed5f9d3b4c25478fe11
Architecture	x86-64
Functions	477 (65.2%) 732 (34.8%) 255

Secondary Image

IDB Name	39ab42ceac0f3142a8785016611a69936c63cf019a7ffaedc745c1080db4e94e
Image Name	39ab42ceac0f3142a8785016611a69936c63cf019a7ffaedc745c1080db4e94e
Hash	39ab42ceac0f3142a8785016611a69936c63cf019a7ffaedc745c1080db4e94e
Architecture	x86-64
Functions	477 (73.4%) 650 (26.6%) 173

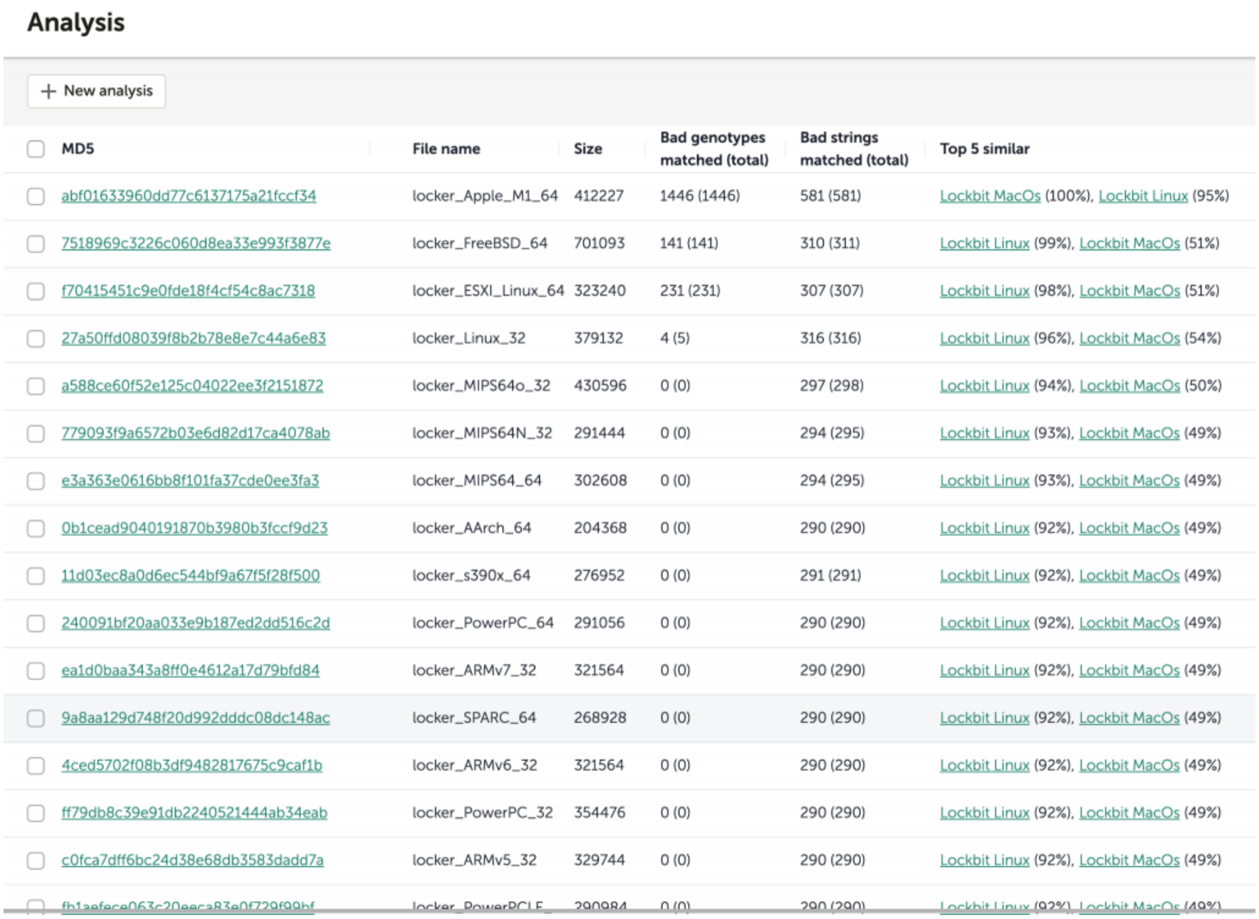
Description

Binary diffing across the two families

Multi-platform LockBit

We recently stumbled on a ZIP file, uploaded to a multiscanner, that contained LockBit samples for multiple architectures, such as Apple M1, ARM v6, ARM v7, FreeBSD and many others. The next question would obviously be, “What about codebase similarity?”.

For this, we used the KTAE: simply throwing in the downloaded ZIP file was enough to see that all the samples were derived from the LockBit Linux/ESXi version, which we wrote about in an earlier private report.



Analysis

☐	MD5	File name	Size	Bad genotypes matched (total)	Bad strings matched (total)	Top 5 similar
☐	abf01633960dd77c6137175a21fccf34	locker_Apple_M1_64	412227	1446 (1446)	581 (581)	Lockbit MacOs (100%), Lockbit Linux (95%)
☐	7518969c3226c060d8ea33e993f3877e	locker_FreeBSD_64	701093	141 (141)	310 (311)	Lockbit Linux (99%), Lockbit MacOs (51%)
☐	f70415451c9e0fde18f4cf54c8ac7318	locker_ESXI_Linux_64	323240	231 (231)	307 (307)	Lockbit Linux (98%), Lockbit MacOs (51%)
☐	27a50ffd08039f8b2b78e8e7c44a6e83	locker_Linux_32	379132	4 (5)	316 (316)	Lockbit Linux (96%), Lockbit MacOs (54%)
☐	a588ce60f52e125c04022ee3f2151872	locker_MIPS64o_32	430596	0 (0)	297 (298)	Lockbit Linux (94%), Lockbit MacOs (50%)
☐	779093f9a6572b03e6d82d17ca4078ab	locker_MIPS64N_32	291444	0 (0)	294 (295)	Lockbit Linux (93%), Lockbit MacOs (49%)
☐	e3a363e0616bb8f101fa37cde0ee3fa3	locker_MIPS64_64	302608	0 (0)	294 (295)	Lockbit Linux (93%), Lockbit MacOs (49%)
☐	0b1cead9040191870b3980b3fccf9d23	locker_AArch_64	204368	0 (0)	290 (290)	Lockbit Linux (92%), Lockbit MacOs (49%)
☐	11d03ec8a0d6ec544bf9a67f5f28f500	locker_s390x_64	276952	0 (0)	291 (291)	Lockbit Linux (92%), Lockbit MacOs (49%)
☐	240091bf20aa033e9b187ed2dd516c2d	locker_PowerPC_64	291056	0 (0)	290 (290)	Lockbit Linux (92%), Lockbit MacOs (49%)
☐	ea1d0baa343a8ff0e4612a17d79bfd84	locker_ARMv7_32	321564	0 (0)	290 (290)	Lockbit Linux (92%), Lockbit MacOs (49%)
☐	9a8aa129d748f20d992dddc08dc148ac	locker_SPARC_64	268928	0 (0)	290 (290)	Lockbit Linux (92%), Lockbit MacOs (49%)
☐	4ced5702f08b3df9482817675c9caf1b	locker_ARMv6_32	321564	0 (0)	290 (290)	Lockbit Linux (92%), Lockbit MacOs (49%)
☐	ff79db8c39e91db2240521444ab34eab	locker_PowerPC_32	354476	0 (0)	290 (290)	Lockbit Linux (92%), Lockbit MacOs (49%)
☐	c0fca7dff6bc24d38e68db3583dadd7a	locker_ARMv5_32	329744	0 (0)	290 (290)	Lockbit Linux (92%), Lockbit MacOs (49%)
☐	fb1aeface063c20eeca83e0f729f99bf	locker_PowerPCLE_	290984	0 (0)	290 (290)	Lockbit Linux (92%), Lockbit MacOs (49%)

Source code shared with LockBit Linux

Further analysis of the samples led us to believe that LockBit were in the process of testing their ransomware on various architectures, instead of deploying it in the wild. For instance, the macOS sample was unsigned, so it could not be executed as is. Also, the string encryption method was simple: one byte XOR.

Nevertheless, our findings suggest that LockBit will target more platforms in the wild in the (near) future.

Conclusion

The world of cybercrime is huge, consisting of many players and gangs that are fluid in terms of composition. Groups adopt other groups’ code, and affiliates — which can be considered cybercrime groups in their own right — switch between different types of malware. Groups work on upgrades to their malware, adding features and providing support for multiple, previously unsupported, platforms, a trend that existed for some time now.

When an incident occurs, it is important to find out who has targeted you. This helps to limit the scope of incident response and could help to prevent further damage. The KTAE attributes code to cybercrime groups and highlights features shared by different malware families. This information can also help in taking proactive countermeasures to prevent incidents from happening in the future.

Finally, criminals often resort to old tricks, such as phishing, which, nevertheless, remain highly effective. Being aware of the latest trends can prevent threats like BEC from materializing.

Intelligence reports can help you to stay protected against these threats. If you want to keep up to date on the latest TTPs used by criminals or have questions about our private reports, contact crimewareintel@kaspersky.com.

- Apple MacOS
- crimeware
- Cybercrime
- LockBit
- Malware
- Malware Descriptions
- Phishing
- Phishing kits
- Ransomware
- Spear phishing

Authors

Expert GReAT

LockBit Green and phishing that targets organizations

Your email address will not be published. Required fields are marked *