Globant confirms hack after Lapsus$ leaks 70GB of stolen data

By Ionut Ilascu

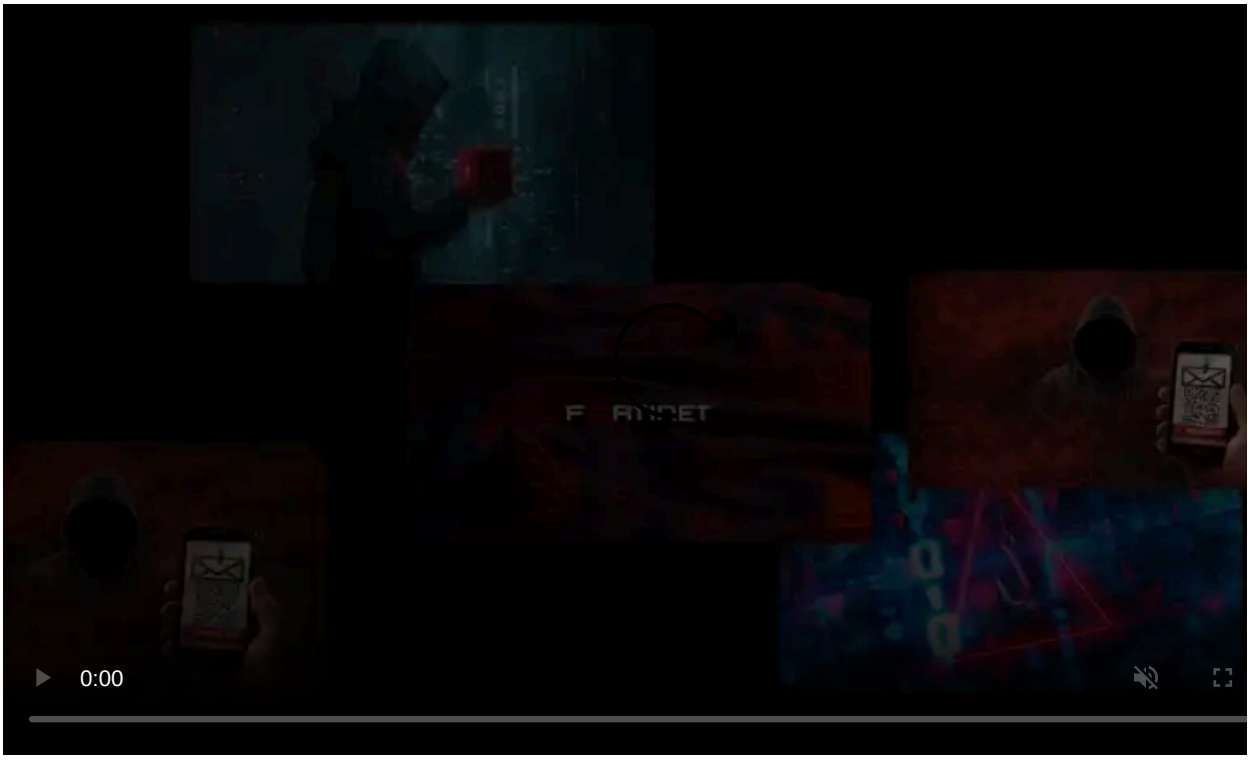
Published: 2022-03-30 · Archived: 2026-04-06 00:07:26 UTC

IT and software consultancy firm Globant has confirmed that they were breached by the Lapsus$ data extortion group, where data consisting of administrator credentials and source code was leaked by the threat actors.

As part of the leak, the hacking group released a 70GB archive of data stolen from Globant, describing it as “some customers source code.”

Source code and private keys

Globant is an IT and software development firm with over 16,000 employees worldwide and $1.2 billion in revenue for 2021.


0:00

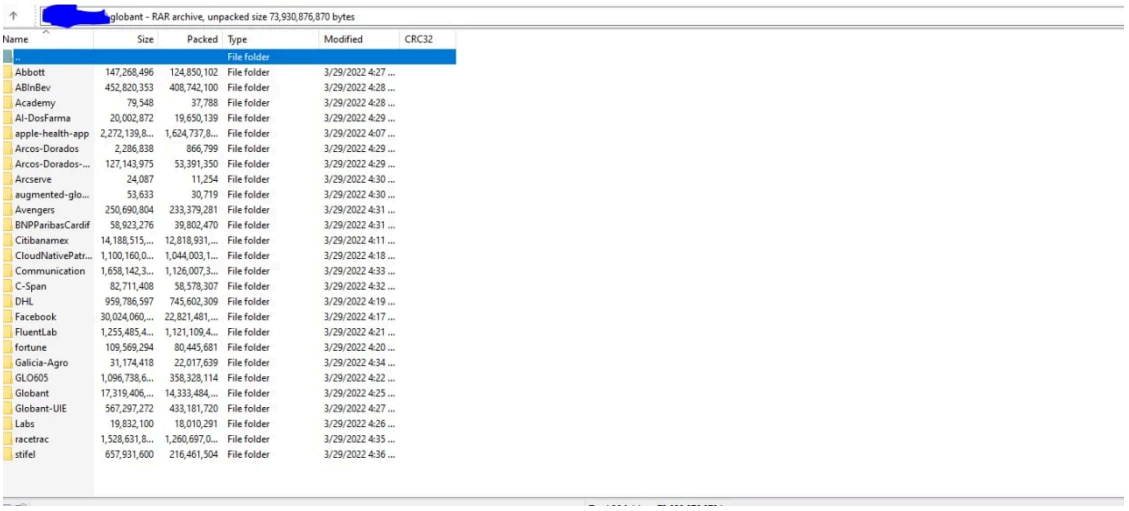
Founded in Buenos Aires, Argentina, Globant is currently headquartered in Luxembourg and boasts a well-known list of customers, including Metropolitan Police, SmileDirectClub, Autodesk, Electronic Arts, Santander, Interbank, Royal Carribbean, and many more.

Following the leak from Lapsus$, Globant issued a press release confirming that some of the company source code has been exposed to an unauthorized party.

“We have recently detected that a limited section of our company's code repository has been subject to unauthorized access” - Globant

Among the data published by Lapsus$, there is a screenshot the group claims to be of an archived directory from Globant, containing folder names that appear to be company customers.

Some of the source code folders listed in the screenshot include, Abbott, apple-health-app, C-span, Fortune, Facebook, DHL, and Arcserve.

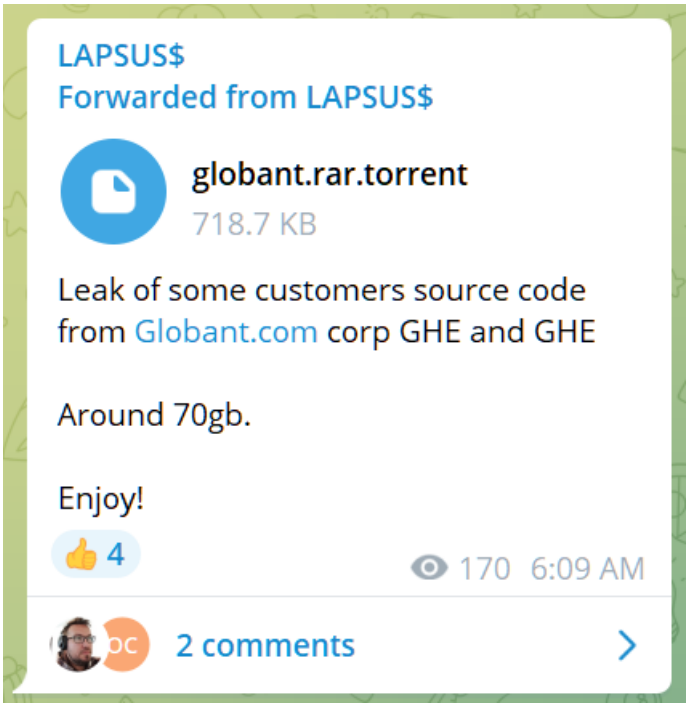

[redacted]globant - RAR archive, unpacked size 73,930,876,870 bytes

Name	Size	Packed	Type	Modified	CRC32
..			File folder		
Abbott	147,268,496	124,850,102	File folder	3/29/2022 4:27 ...	
ABInBev	452,820,353	408,742,100	File folder	3/29/2022 4:28 ...	
Academy	79,548	37,788	File folder	3/29/2022 4:28 ...	
Al-DosFarma	20,002,872	19,650,139	File folder	3/29/2022 4:29 ...	
apple-health-app	2,272,139,8...	1,624,737,8...	File folder	3/29/2022 4:07 ...	
Arcos-Dorados	2,286,838	866,799	File folder	3/29/2022 4:29 ...	
Arcos-Dorados-...	127,143,975	53,391,350	File folder	3/29/2022 4:29 ...	
Arcserve	24,087	11,254	File folder	3/29/2022 4:30 ...	
augmented-glo...	53,633	30,719	File folder	3/29/2022 4:30 ...	
Avengers	250,690,804	233,379,281	File folder	3/29/2022 4:31 ...	
BNPParibasCardif	58,923,276	39,802,470	File folder	3/29/2022 4:31 ...	
Citibanamex	14,188,515,...	12,818,931,...	File folder	3/29/2022 4:11 ...	
CloudNativePatr...	1,100,160,0...	1,044,003,1...	File folder	3/29/2022 4:18 ...	
Communication	1,658,142,3...	1,126,007,3...	File folder	3/29/2022 4:33 ...	
C-Span	82,711,408	58,578,307	File folder	3/29/2022 4:32 ...	
DHL	959,786,597	745,602,309	File folder	3/29/2022 4:19 ...	
Facebook	30,024,060,...	22,821,481,...	File folder	3/29/2022 4:17 ...	
FluentLab	1,255,485,4...	1,121,109,4...	File folder	3/29/2022 4:21 ...	
fortune	109,569,294	80,445,681	File folder	3/29/2022 4:20 ...	
Galicia-Agro	31,174,418	22,017,639	File folder	3/29/2022 4:34 ...	
GLO605	1,096,738,6...	358,328,114	File folder	3/29/2022 4:22 ...	
Globant	17,319,406,...	14,333,484,...	File folder	3/29/2022 4:25 ...	
Globant-UIE	567,297,272	433,181,720	File folder	3/29/2022 4:27 ...	
Labs	19,832,100	18,010,291	File folder	3/29/2022 4:26 ...	
racetrac	1,528,631,8...	1,260,697,0...	File folder	3/29/2022 4:35 ...	
stifel	657,931,600	216,461,504	File folder	3/29/2022 4:36 ...	

The metadata for the entries shows that the folders have been modified on March 29, which could indicate when the data was stolen.

In a follow-up post, Lapsus$ published a set of credentials for what they say give administrator access to various platforms used by Globant for developing, reviewing, and collaborating on customer code (Jira, Confluence, GitHub, Crucible).

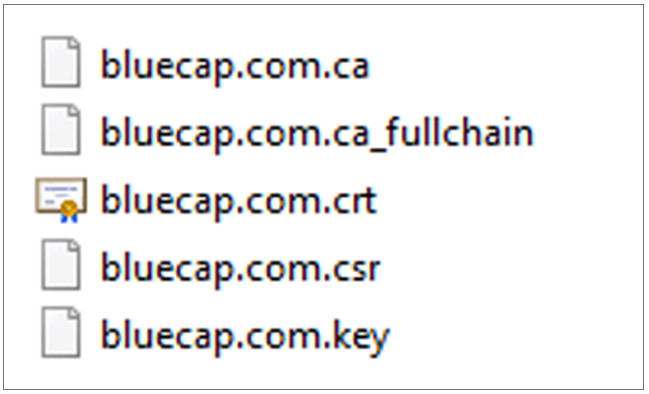
A third post from the gang today shared a torrent file for about 70GB of data stolen from Globant. The company says that the intruder on its systems accessed “certain source code and project-related documentation for a very limited number of clients.”



The damage appears to be significant.

According to threat intelligence company SOS Intelligence, the leaked data contains customer information as well as a code repositories with a large number of private keys (full chain, web server SSL certificates, Globant server, API keys).

One of the repositories is for the Bluecap app for consultancy in the financial sector, that Globant acquired in late 2020.



The cache that Lapsus$ leaked also includes a little over 150 SQL database files for various customer applications, SOS Intelligence says.

"In terms of legitimacy, going just by volume alone it's hard to fabricate that amount of data - however samples of the data have been cross referenced with live systems and other methods that show the leak is legitimate and very significant as far as Globant and Globant's impacted customers are concerned" - SOS Intelligence

Globant said today that its investigation into the incident did not reveal any evidence that the hackers compromised other parts of its infrastructure system.

Lapsus$ on LE radar

The Lapsus$ data extortion group has been constantly making the news due to their attacks on big technological companies, like Microsoft, Nvidia, Samsung, Okta, Ubisoft, many of them resulting in big data leaks.

Despite the big names on their victim list, Lapsus$ is believed to be formed mainly by teenagers exercising their hacking skills driven mainly by making a name on the hacking scene, not by financial motivation.

The group has been on the radar of law enforcement for a while and some individuals, all teens believed to be connected to Lapsus$, have been arrested in the U.K.

The FBI is also investigating the activities of the group and has asked the public for any information leading to identifying Lapsus$ members involved in the compromise of computer networks from U.S.-based companies.

SEEKING INFORMATION

LAPSUS$

Cyber Intrusions of United States-Based Technology Companies
March 21, 2022

DETAILS

The Federal Bureau of Investigation (FBI) is asking the public for assistance in an investigation involving the compromise of computer networks belonging to United States-based technology companies.

On March 21, 2022, individuals from a group identifying themselves as Lapsus$ posted on a social media platform and alleged to have stolen source code from a number of United States-based technology companies. These unidentified individuals took credit for both the theft and dissemination of proprietary data that they claim to have illegally obtained. The FBI is seeking information regarding the identities of the individuals responsible for these cyber intrusions.

If you have any information concerning these individuals, please contact your local FBI office, or the nearest American Embassy or Consulate.

Field Office: San Francisco

However, it is unclear how many active members are in the group and what roles they play.

It is believed that Lapsus$ has affiliates all over the world, as their Telegram chats seem to suggest that some of them speak English, Russian, Turkish, German, and Portuguese.

Source: https://www.bleepingcomputer.com/news/security/globant-confirms-hack-after-lapsus-leaks-70gb-of-stolen-data/