# LG Electronics allegedly hit by Maze ransomware attack

By Ionut Ilascu

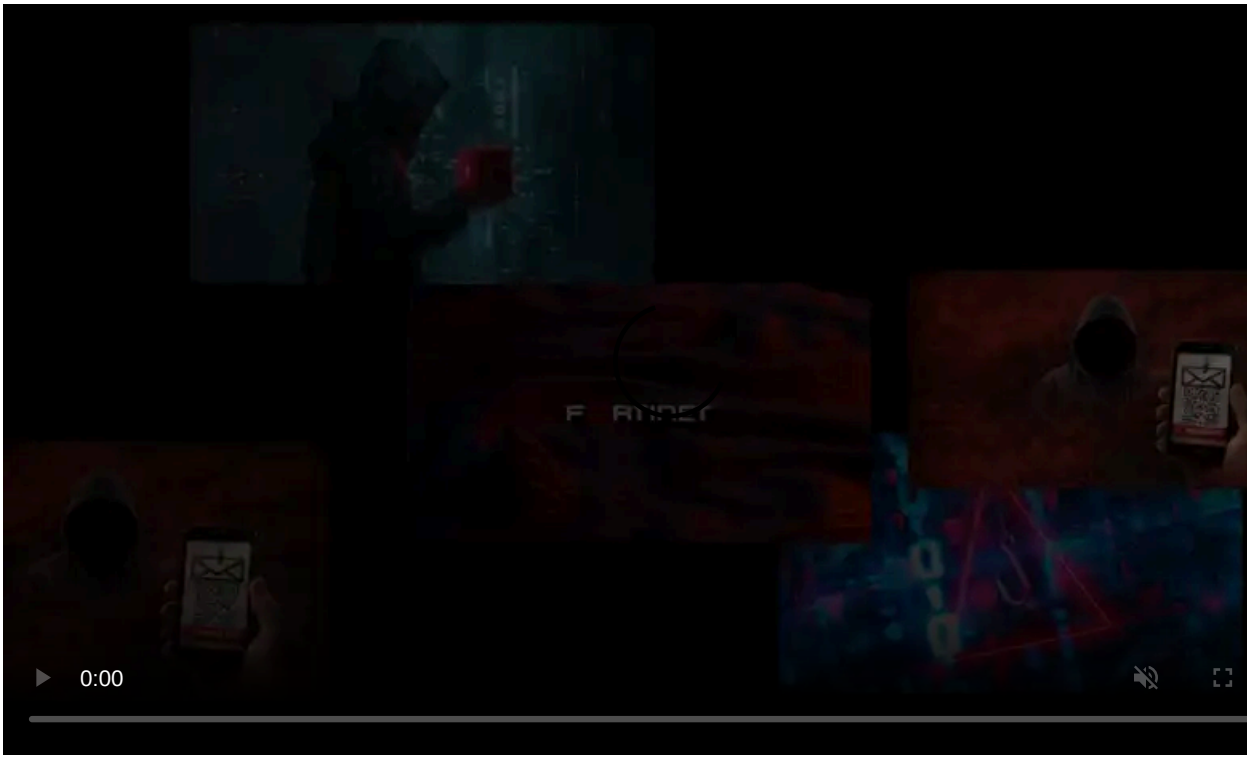
Published: 2020-06-25 · Archived: 2026-04-06 02:57:31 UTC

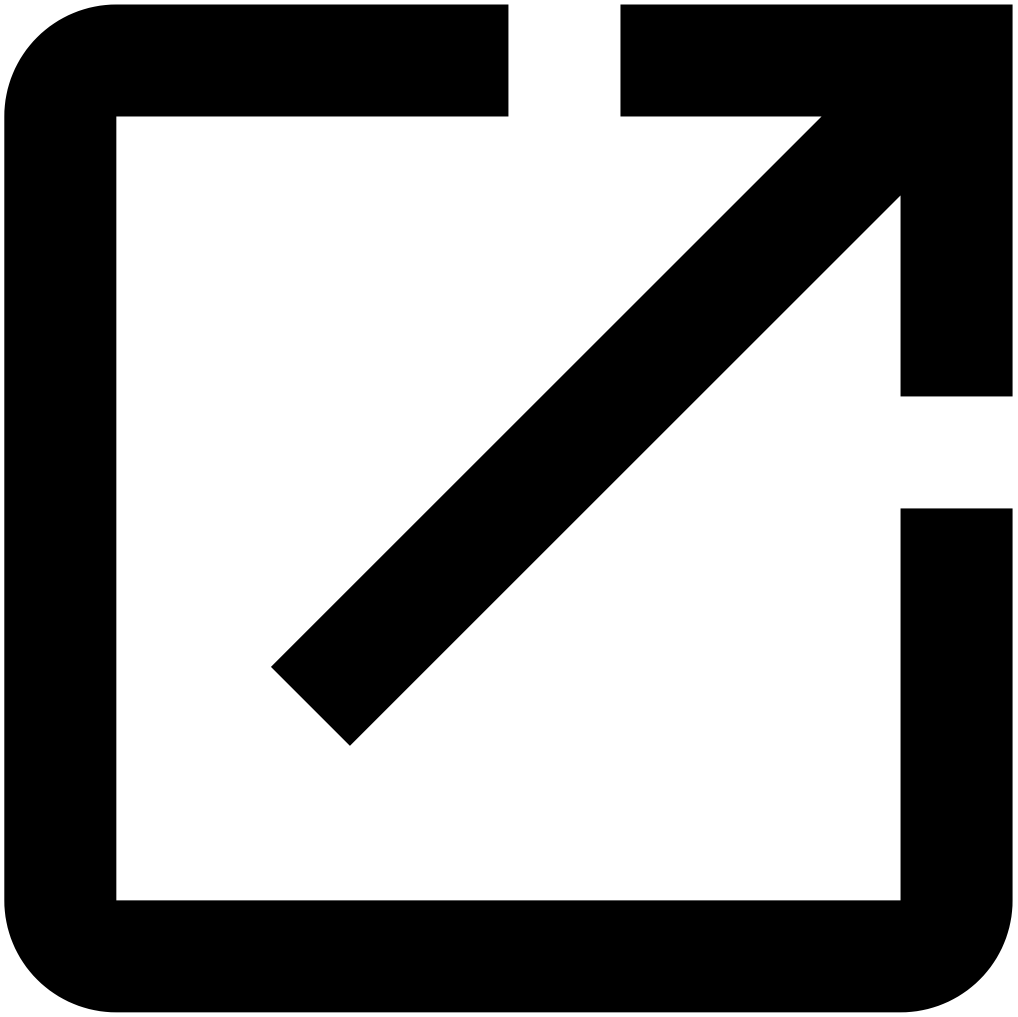
Maze ransomware operators have claimed on their website that they breached and locked the network of the South Korean multinational LG Electronics.

The details of the attack have not been released but the hackers stated that they have stolen from the company proprietary information for projects that involve big U.S. Companies.

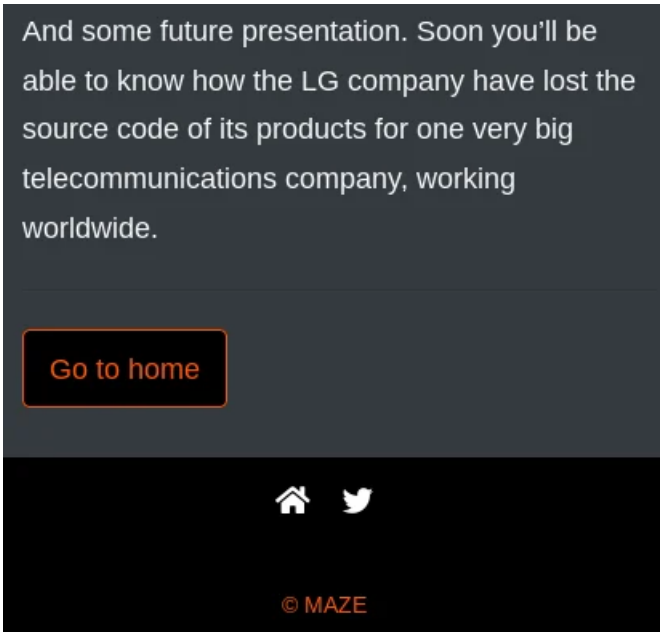
### Proprietary code stolen

This ransomware operator, like many others, publishes information on their victims when their ransom demands are not accepted or contact with the breached entity halts.


0:00



In a "press release" posted their data leak site on Monday, the threat actors announced that they would provide information on an alleged LG Electronics breach and the source code they stole.



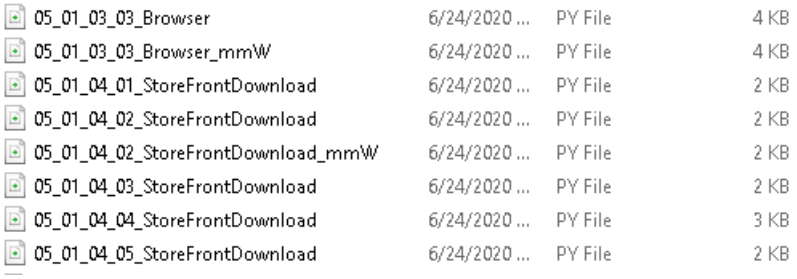

Yesterday, Maze told BleepingComputer that they had breached LG electronics and stole 40GB of source code from the manufacturer.

"Also, we would like to announce that in case of not contacting us today we will share information about attack on Lg. We downloaded 40GB of Python source codes from Lg. Developments for a biggest companies in US, we will share part of source code on Lg later" - Maze ransomware

When asked how many devices were encrypted, the Maze operators told BleepingComputer that this "information currently is private and will be provided only to Lg negotiators."

In a new entry on their data leak site today, though, they published alleged proofs of their attack on LG.

This includes a screenshot of a file listing from a Python code repository.

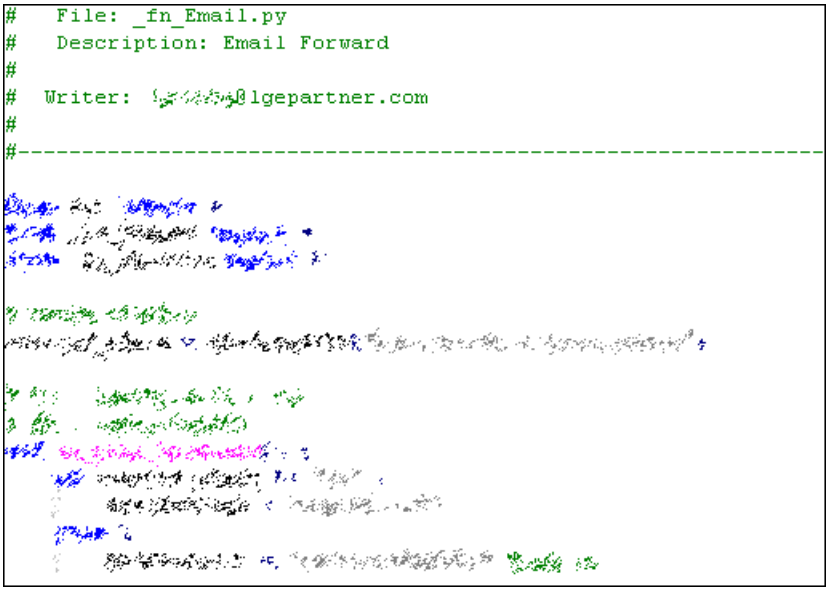



Another screenshot published by Maze shows a split archive for a .KDZ file, which is the format for official stock firmware code from LG.

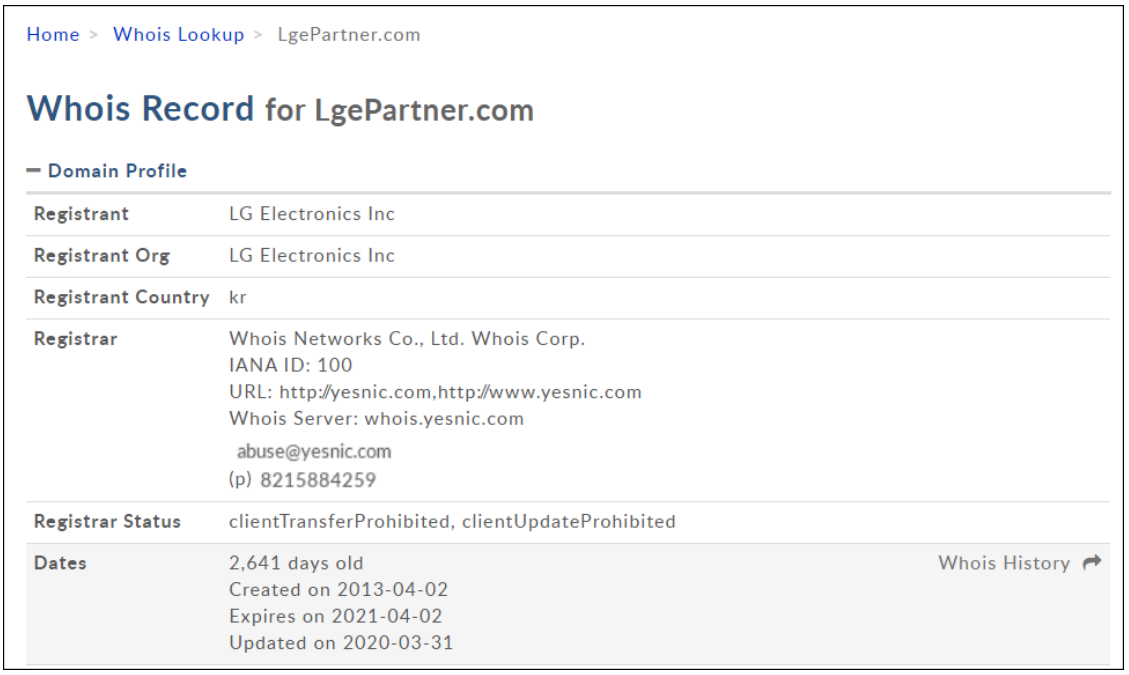
It appears from the image below that the firmware was developed for AT&T. The mobile carrier currently lists 41 phones and four tablets from LG on its device support page.

| | | | |
|---|---|---|---|
| G85020c_00_ATT_US_OP_0422.kdz | 6/24/2020 ... | KDZ File | 0 KB |
| G85020c_00_ATT_US_OP_0422_158757414... | 6/24/2020 ... | WinRAR ar... | 716,800 KB |
| G85020c_00_ATT_US_OP_0422_158757414... | 6/24/2020 ... | 002 File | 716,800 KB |
| G85020c_00_ATT_US_OP_0422_158757414... | 6/24/2020 ... | 003 File | 716,800 KB |
| G85020c_00_ATT_US_OP_0422_158757414... | 6/24/2020 ... | 004 File | 716,800 KB |
| G85020c_00_ATT_US_OP_0422_158757414... | 6/24/2020 ... | 005 File | 716,800 KB |
| G85020c_00_ATT_US_OP_0422_158757414... | 6/24/2020 ... | 006 File | 521,988 KB |
| LG_358864100010740_20200424153311 | 6/24/2020 ... | XML File | 1 KB |

A third screenshot from the attackers shows a snippet of Python code for an email forwarding project.




This source code indicates that the owner is from the domain lgepartner.com, which is owned by LG Electronics.




Since yesterday morning, BleepingComputer has reached out to multiple LG Electronics email addresses with a request to comment on this alleged attack but the company had not answered by publishing time.

When sending an email to one email address listed publicly for general media inquiries and corporate communications we received an automated reply informing that the message could be delivered because the user does not exist.

There is no information on how Maze was able to breach LG Electronics' network but initial access methods used by the actor include connecting via an exposed remote desktop connection and pivoting to valuable hosts via compromised Domain Administrator accounts.

Some companies that fell victim to a Maze ransomware attack also had vulnerable systems reachable over the public internet.

Regardless of how they got in, Maze has made a reputation of publishing stolen files if they don't reach an agreement with their victims for a ransom payment.

**Update [June 25, 08:56 EDT]**: Article updated with quote from Maze ransomware operators.



---

Source: https://www.bleepingcomputer.com/news/security/lg-electronics-allegedly-hit-by-maze-ransomware-attack/