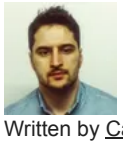
# Ransomware gang publishes tens of GBs of internal data from LG and Xerox

zdnet.com/article/ransomware-gang-publishes-tens-of-gbs-of-internal-data-from-lg-and-xerox/


Home Innovation Security

Maze gang publishes internal data from LG and Xerox after failed extortion attempt.



Written by Catalin Cimpanu, Contributor on Aug. 3, 2020

- 
- 
- 
- 
- 


Image: LG, Simone Hutsch, ZDNet

## Executive guide

## Ransomware: One of the biggest menaces on the web

Everything you need to know about ransomware: how it started, why it's booming, how to protect against it, and what to do if your PC's infected.

Read now

The operators of the Maze ransomware have published today tens of GB of internal data from the networks of enterprise business giants LG and Xerox following two failed extortion attempts.

The hackers leaked 50.2 GB they claim to have stolen from LG's internal network, and 25.8 GB of Xerox data.

While LG issued a generic statement to *ZDNet* in June, neither company wanted to talk about the incident in great depth today.

Both of today's leaks have been teased since late June when the operators of the Maze ransomware created entries for each of the two companies on their "leak portal."

The Maze gang is primarily known for its eponymous ransomware string and usually operates by breaching corporate networks, stealing sensitive files first, encrypting data second, and demanding a ransom to decrypt files.

If a victim refuses to pay the fee to decrypt their files and decides to restore from backups, the Maze gang creates an entry on a "leak website" and threatens to publish the victim's sensitive data in a second form ransom/extortion attempt.

The victim is then given a few weeks to think over its decision, and if victims don't give in during this second extortion attempt, the Maze gang will publish files on its portal.

LG and Xerox are at this last stage, after apparently refusing to meet the Maze gang's demands.

## LG incident and data

*ZDNet* has been tracking both incidents since they've been initially announced on the Maze website in late June.

Based on screenshots shared by the Maze gang last month and by file samples downloaded and reviewed by *ZDNet* today, the data appears to contain source code for the cloused-source firmware of various LG products, such as phones and laptops.


Image: ZDNet

In an email in June, the Maze gang told *ZDNet* that they did not execute their ransomware on LG's network, but they merely stole the company's proprietary data and chose to skip to the second phase of their extortion attempts.

"We decided not to execute [the] Maze [ransomware] because their clients are socially significant and we do not want to create disruption for their operations, so we only have exfiltrated the data," the Maze gang told *ZDNet* via a contact form on their leak site.

When reached out for comment in June, the LG security team told *ZDNet* they would look into the incident and report any intrusion to authorities. In a follow-up email sent today, after the Maze gang published more than 50 GB of the company's files, the security team deflected our request for comment towards its communications team. When we reached out to the communications team, our email bounced, similar to what happened in June.

### Xerox incident and data

But while we have somewhat of an idea of what happened with the Maze attack on LG, things are a lot murkier when it comes to Xerox.

The company has not returned requests for comment sent in June and today.

It is unclear what internal systems the Maze gang encrypted, or if files were stolen and ransomed without encryption, similar to the LG incident.

Based on a cursory review of data leaked online today, it appears that the Maze gang has stolen data related to customer support operations. At the time of writing, we found information related to Xerox employees; however, we have not yet found files holding data on Xerox customers -- although, this is a large trove of information and reviewing all of it will take time.


Image: ZDNet

### Citrix point of entry?

In an interview with threat intelligence company Bad Packets in June, Troy Mursch, the company's co-founder, told *ZDNet* that both companies ran Citrix ADC servers that at one point or another were left unpatched and vulnerable online -- according to his company's internet scans.

The servers were vulnerable to the CVE-2019-19781 vulnerability, which Mursch described as "Maze's favorite vector of compromise."

Ironically, on the same day that the Maze gang leaked LG files on its leak portal, threat intelligence firm Shadow Intelligence told *ZDNet* in an email that another hacker was selling access to LG America's research and development (R&D) center on a hacking forum.

The asking price was between $10,000 and $13,000, according to screenshots shared with *ZDNet*.


Image: Shadow Intelligence (supplied)