Thanks for the memories... now pay up or else: Maze ransomware crew claims to have hacked SK hynix, leaks '5% of stolen files'

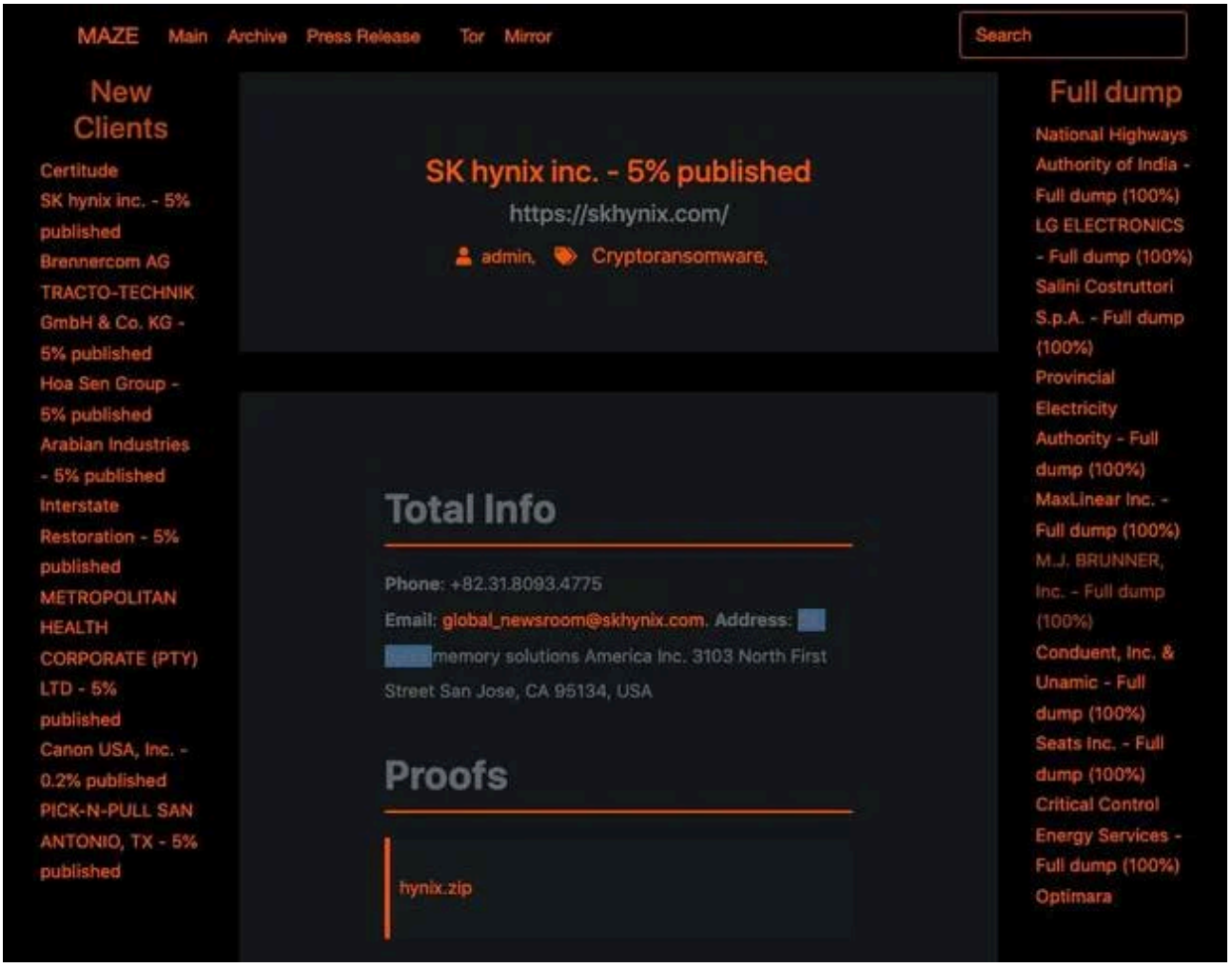
By Shaun Nichols

Published: 2020-08-20 · Archived: 2026-04-05 14:19:04 UTC

The Maze hacker gang claims it has infected computer memory maker SK hynix with ransomware and leaked some of the files it stole.

The South Korean semiconductor giant could not be reached for comment. For what it's worth, the Maze crew doesn't tend to need to fib about these sort of things. When it claims to have infiltrated a victim – and it has pwned a great deal of organizations lately – it usually publicly shares data stolen from the compromised network as proof.

And such is the case with SK hynix. Here's a screenshot of the Maze crew's website announcing the infiltration of the manufacturer's network, and the exfiltration of its internal data:



A screen-grab of the announcement ... Click to enlarge. Credit: *Reg source*.

A 570MB ZIP archive is provided as a download from the Maze site. It is supposedly just five per cent of the total amount siphoned from SK hynix, which suggests as much as 11GB was stolen by the gang after breaking into the corp's networks and before scrambling its files to hold them to ransom.

According to one person who has viewed the archive's contents, it appears to contain confidential NAND flash supply agreements with Apple, and a mix of personal and corporate files, though nothing dated more recently than a couple of years ago.

SK Hynix is one of the largest suppliers of RAM and flash memory in the world. Their clients include the likes of Apple and IBM. A crippling ransomware attack on its internal network can therefore have knock-on effects for its customers.

For those unfamiliar, Maze offers something of a new take on the old ransomware racket. Whereas traditional extortionware operators simply encrypt their victims' file systems, and then ask a fee to unscramble the data, the Maze miscreants take things a step further and promise to publicly leak all the stolen information if the company doesn't pay up.

Those that fail to meet the ransom demands have their corporate secrets handed out to the public. It's a pretty shady tactic, though one that has proven very effective for the hackers. The approach helped Maze get a name for itself as a crew to be feared.

The ransomware crew likes to make a show of distributing the data of companies that don't pay up. Their previous victims include IT service provider Cognizant, Texas-based VT Aerospace, and semiconductor giant MaxLinear. In June, it extorted a New York architecture firm when it intended to go after a Canadian standards body. ®

A hat-tip to the Register reader who alerted us to the SK hynix update on the Maze website.
