Chipmaker MaxLinear reports data breach after Maze Ransomware attack

bleepingcomputer.com/news/security/chipmaker-maxlinear-reports-data-breach-after-maze-ransomware-attack/

Sergiu Gatlan

By
Sergiu Gatlan

- June 16, 2020
- 12:47 PM
- 0

U.S. system-on-chip (SOC) maker company MaxLinear disclosed that some of its computing systems were encrypted by Maze Ransomware operators last month, after an initial breach that took place around April 15.

MaxLinear is a New York Stock Exchange-traded company and a provider of RF, analog, and mixed-signal integrated circuits for connected home, industrial, and infrastructure applications.

In April 2020, MaxLinear announced net revenue of $62 million for the first quarter of 2020, and its CEO, Kishore Seendripu, shared plans to "acquire Intel's Home Gateway Platform Division in the third quarter of this year."

Data breach reported after stolen data leaked online

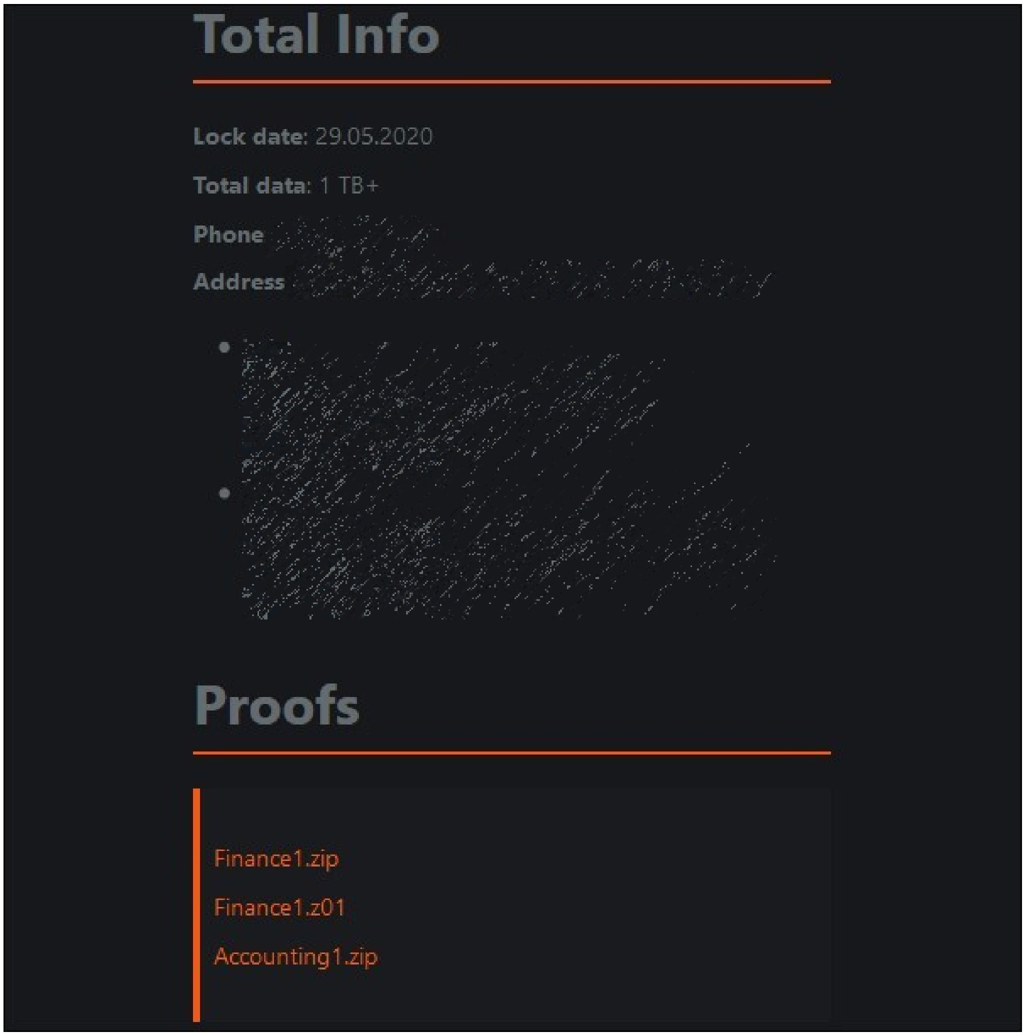
In a data breach notification sent to affected individuals on June 10 and seen by BleepingComputer, MaxLinear states that the attack was discovered on May 24.

"We immediately took all systems offline, retained third-party cybersecurity experts to aid in our investigation, contacted law enforcement, and worked to safely restore systems in a manner that protected the security of information on our systems," the letter reads.

"Our investigation to-date has identified evidence of unauthorized access to our systems from approximately April 15, 2020, until May 24, 2020."

MaxLinear says that it was able to restore some of the systems affected during the attack and its IT staff is still working on bringing back up the rest.

On June 15, Maze Ransomware leaked 10.3GB of accounting and financial information out of the over 1TB of data allegedly stolen before encrypting MaxLinear's systems.



Total Info

Lock date: 29.05.2020

Total data: 1 TB+

Phone [redacted]

Address [redacted]

- [redacted]
- [redacted]

Proofs

Finance1.zip

Finance1.z01

Accounting1.zip

Data leaked by Maze Ransomware

Personal and financial info exposed

The SOC maker says that this leaked information could include personally identifiable (PII) and financial information such as "name, personal and company email address and personal mailing address, employee ID number, driver’s license number, financial account number, Social Security number, date of birth, work location, compensation and benefit information, dependent, and date of employment."

The company also states that the incident has led to an enterprise-wide password reset and that the breach was disclosed to the appropriate law enforcement authorities.

According to documents filed with the U.S. Securities and Exchange Commission (SEC) on June 16, as discovered by Reuters, the attack did not affect shipment, order fulfillment, and production capabilities, and MaxLinear doesn't plan to pay the ransom Maze Ransomware requested to stop leaking the stolen data.

The chipmaker said in the SEC filing that, although the company would incur extra costs due to the forensic investigation and systems remediation following the attack, it does not anticipate "that the incident will materially or adversely affect our operating expenses."

"We carry cybersecurity insurance, subject to applicable deductibles and policy limits," MaxLinear said.

Related Articles:

GitHub: Attackers stole login details of 100K npm user accounts

US Senate: Govt’s ransomware fight hindered by limited reporting

Ransomware attack exposes data of 500,000 Chicago students

US links Thanos and Jigsaw ransomware to 55-year-old doctor

Costa Rica declares national emergency after Conti ransomware attacks