TSMC denies LockBit hack as ransomware gang demands $70 million

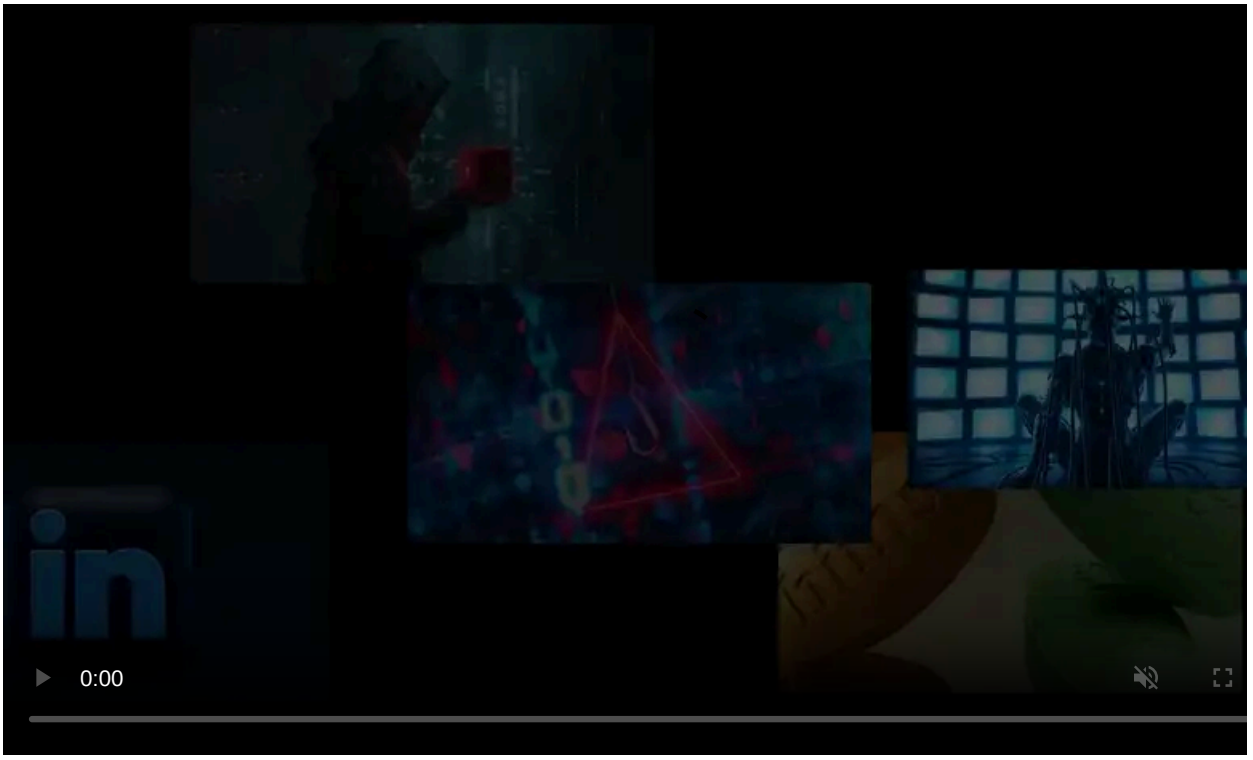
By Bill Toulas

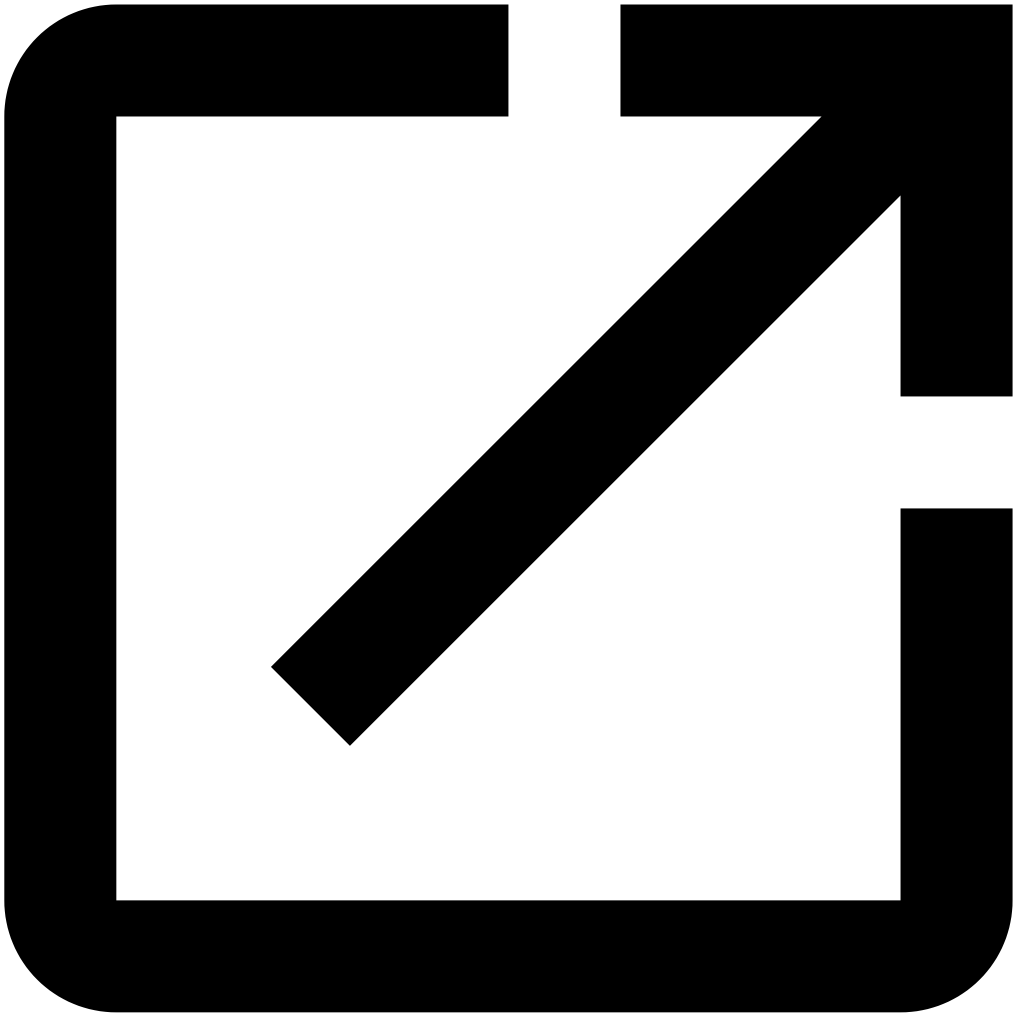
Published: 2023-06-30 · Archived: 2026-04-05 17:12:51 UTC

Chipmaking giant TSMC (Taiwan Semiconductor Manufacturing Company) denied being hacked after the LockBit ransomware gang demanded $70 million not to release stolen data.

TSMC is one of the world's largest semiconductor manufacturers, with its products used in a wide variety of devices, including smartphones, high performance computing, IoT devices, automotive, and digital consumer electronics.

On Wednesday, a threat actor known as Bassterlord, who is affiliated with LockBit, began to live tweet what appeared to be a ransomware attack on TSMC, sharing screenshots with information related to the company.


0:00

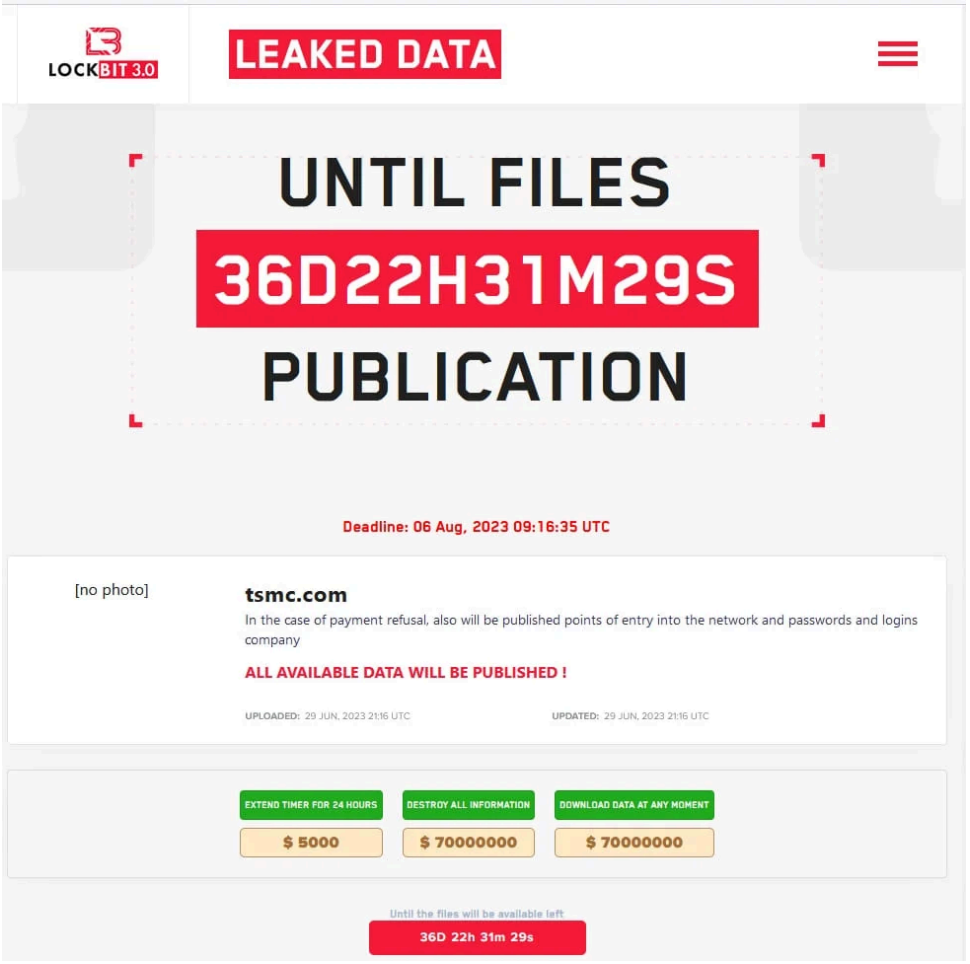


Visit Advertiser websiteGO TO PAGE

These screenshots indicated that the threat actor had significant access to systems allegedly belonging to TSMC, displaying email addresses, access to applications, and credentials for various internal systems.

While this Twitter thread has since been deleted, the LockBit ransomware gang created a new entry for TSMC yesterday on their data leak site, demanding $70 million or they would leak stolen data, including credentials for their systems.

"In the case of payment refusal, also will be published points of entry into the network and passwords and logins company," reads the LockBit data leak entry for TSMC.



LockBit's threat to TSMC *(BleepingComputer)*

TSMC denies it was hacked

A TSMC spokesperson told BleepingComputer that they were not breached, but rather the systems of one of their IT hardware suppliers, Kinmax Technology, were hacked.

"TSMC has recently been aware that one of our IT hardware suppliers experienced a cybersecurity incident which led to the leak of information pertinent to server initial setup and configuration," stated the spokesperson.

"At TSMC, every hardware component undergoes a series of extensive checks and adjustments, including security configurations, before being installed into TSMC's system."

"Upon review, this incident has not affected TSMC's business operations, nor did it compromise any TSMC's customer information."

Apart from validating that its systems had not been impacted in any way, TSMC states that it also stopped working with the breached supplier until the situation cleared up.

"After the incident, TSMC has immediately terminated its data exchange with this concerned supplier in accordance with the Company's security protocols and standard operating procedures. TSMC remains committed to enhancing the security awareness among its suppliers and making sure they comply with security standards," continued TSMC.

Finally, the semiconductor company told BleepingComputer that the investigation of the cybersecurity incident continues and also involves a law enforcement agency.

Kinmax, the impacted supplier, has published a statement today explaining that it became aware of a compromise of a specific testing environment in its network on June 29, 2023.

The company discovered that the intruders managed to exfiltrate some data from the accessed system, mainly concerning system installation and configuration guidance for customers.

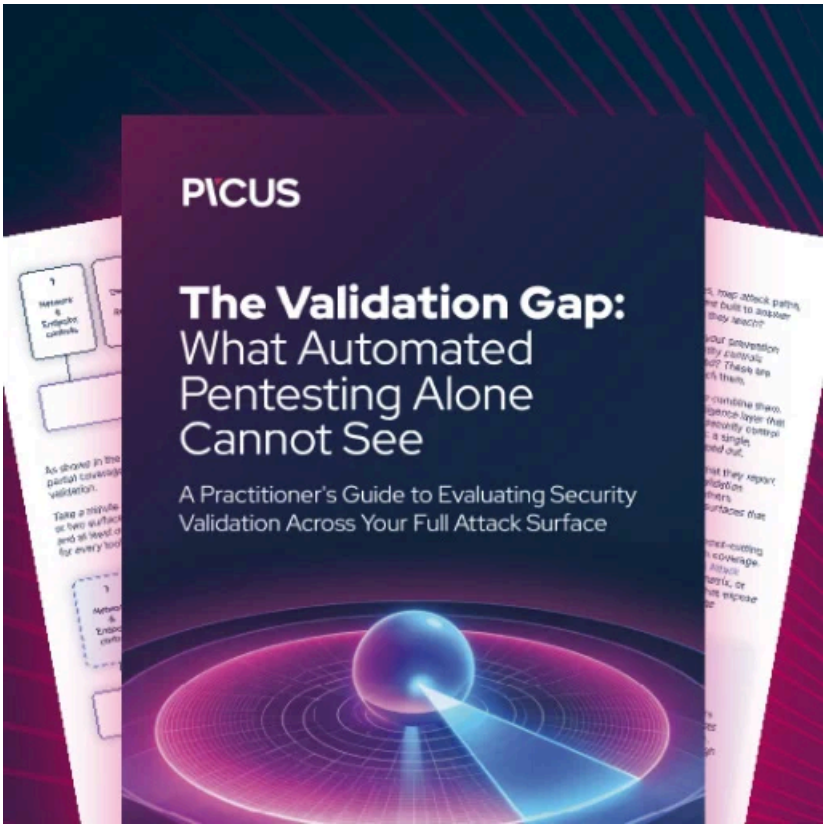
"In the morning of June 29, 2023, the Company discovered that our internal specific testing environment was attacked, and some information was leaked," reads the Kinmax statement.

"The leaked content mainly consisted of system installation preparation that the Company provided to our customers as default configurations."

Kinmax is not the corporate giant that TSMC is, so LockBit's demands for a $70 million ransom payment will likely be ignored.

While there appears to be a mixup as to who was comprimised in this attack, the $70 million ransom demand is one of the largest seen to date.

Other large ransom demands include a $50 million ransom for Acer, $50 million in an attack on CNA, $70 million in the Kaseya supply chain attack, and $240 million in an attack on MediaMarkt.



Automated Pentesting Covers Only 1 of 6 Surfaces.

Automated pentesting proves the path exists. BAS proves whether your controls stop it. Most teams run one without the other.

This whitepaper maps six validation surfaces, shows where coverage ends, and provides practitioners with three diagnostic questions for any tool evaluation.

Source: https://www.bleepingcomputer.com/news/security/tsmc-denies-lockbit-hack-as-ransomware-gang-demands-70-million/