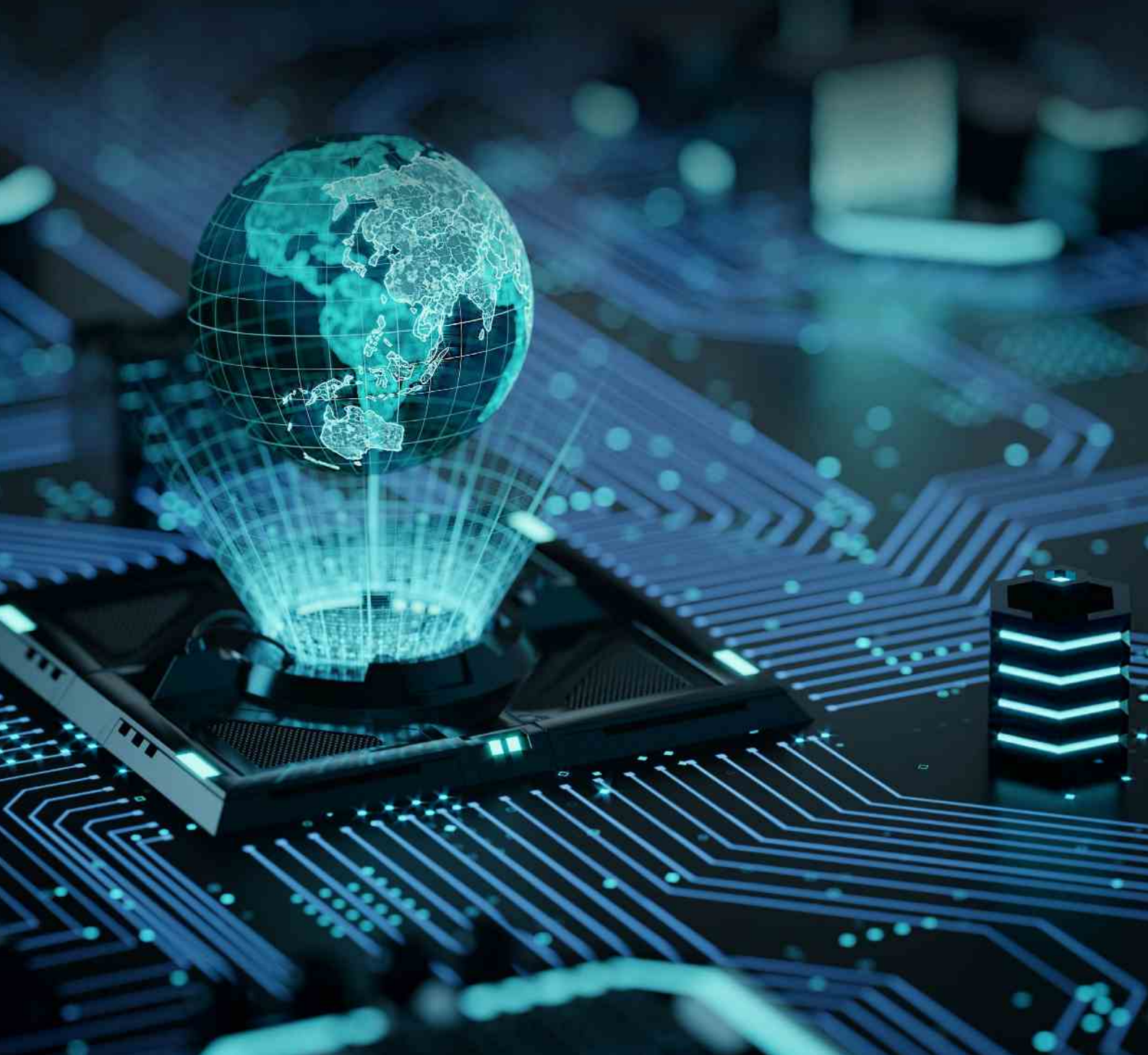




# SEMICONDUCTOR INDUSTRY THREAT LANDSCAPE

Challenges, notable events, and future predictions for the  
Cyber Threat Landscape of the Semiconductor industry



# CONTENTS

---

**4** AN OVERVIEW OF THE SEMICONDUCTOR INDUSTRY

---

**7** RECENT GEOPOLITICAL EVENTS WITH A SIGNIFICANT IMPACT ON THE SEMICONDUCTOR INDUSTRY

---

**8** MAJOR THREATS TO SEMICONDUCTOR INDUSTRY & ITS SUPPLY CHAIN

- RANSOMWARE AND EXTORTION GROUPS
  - INITIAL ACCESS BROKERS AND THEIR ROLE IN SELLING CRITICAL INFRA ACCESS IN UNDERGROUND MARKETS
  - DATA BREACHES/LEAKS IN THE SEMICONDUCTOR INDUSTRY
  - OT & IOT EXPOSURE AND IMPACTS
  - INSIDER THREATS TO THE SEMICONDUCTOR INDUSTRY
- 

**26** CONCLUSION

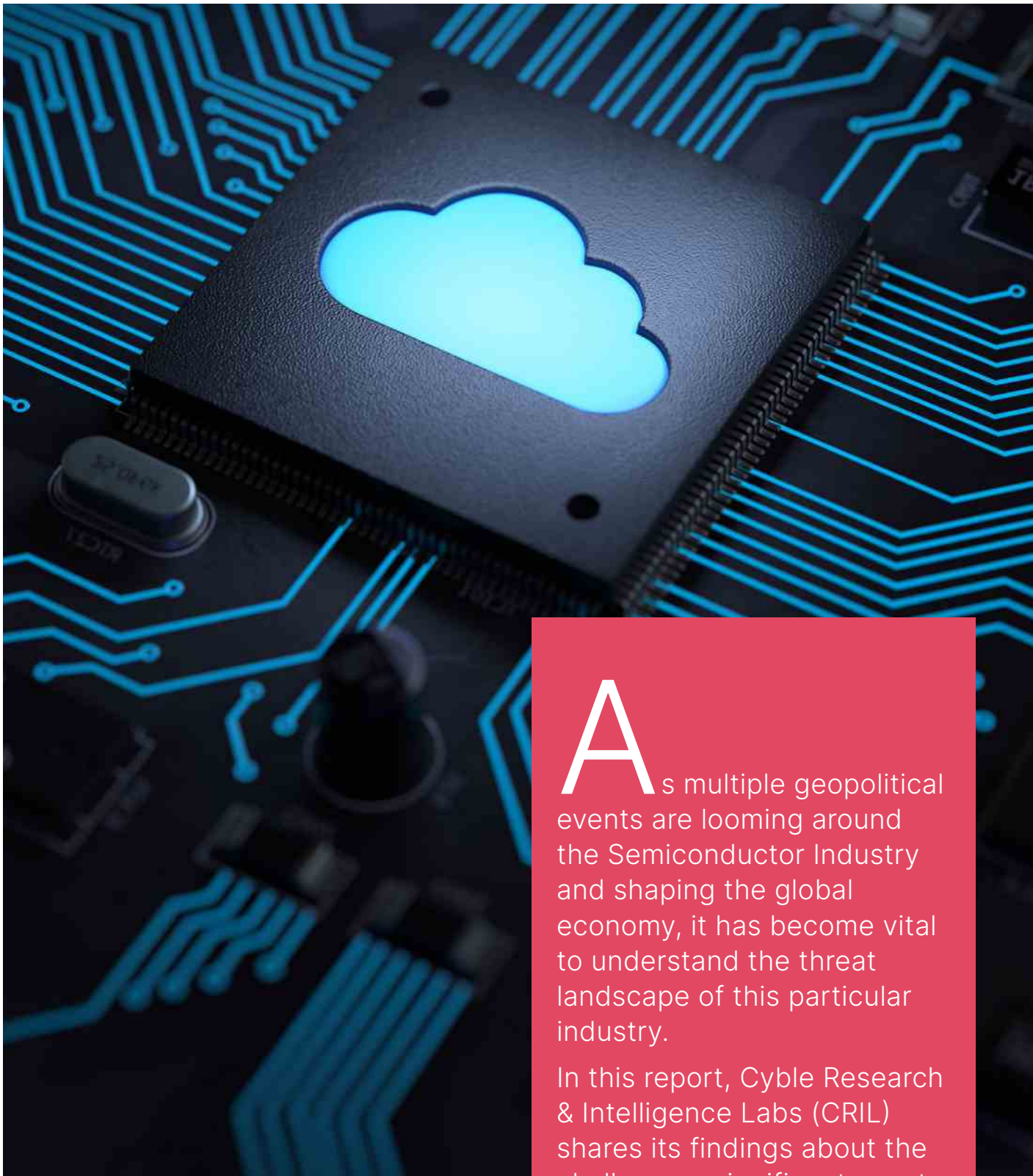
---

**27** RECOMMENDATIONS

---

**28** ABOUT US

---



**A**s multiple geopolitical events are looming around the Semiconductor Industry and shaping the global economy, it has become vital to understand the threat landscape of this particular industry.

In this report, Cyble Research & Intelligence Labs (CRIL) shares its findings about the challenges, significant events, and cyber incidents shaping the semiconductor industry.

This report emphasizes our sensitive findings from the Dark Web and cybercrime forums.



# AN OVERVIEW OF THE SEMICONDUCTOR INDUSTRY

---

Semiconductors are the foundation of all modern technology, and advances in various fields, such as robotics, computing, communication, transportation, military equipment, healthcare, smart energy, etc., are heavily reliant on semiconductors.

While we have observed the Billion-Dollar semiconductor industry fluctuate in terms of demands and pricing, this industry remains crucial for nations looking to **strengthen their economy** and adopt the **latest technological advancements** and **military hardware**.

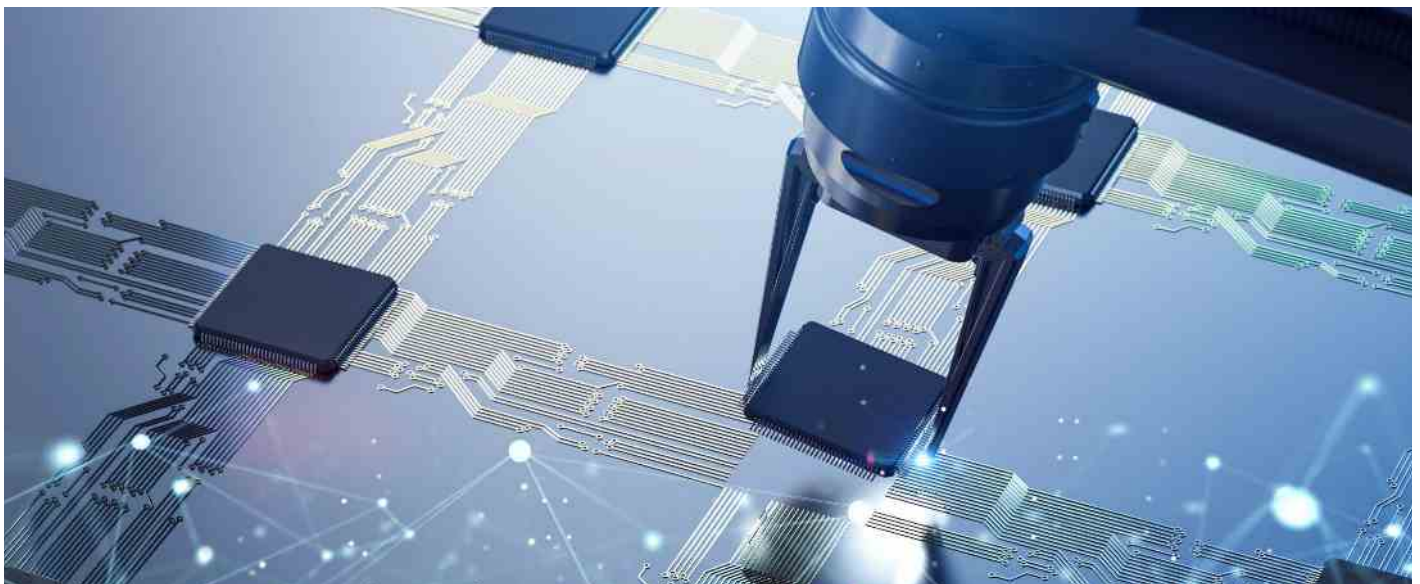
## CHALLENGES IN THE SEMICONDUCTOR INDUSTRY

The ongoing trade conflicts, COVID-19 pandemic, global sanctions, a military conflict in Ukraine, new legislature being enforced, etc., have increased the dependency and volatility of the Semiconductor industry to nations worldwide.

This has proportionally impacted national and international industry players involved with Semiconductors as well, as they are the primary target for most cyberattacks.

The primary reason behind the recent shortage in the semiconductor industry can be attributed to the domino effect caused by the COVID-19 pandemic and the following contributing factors:

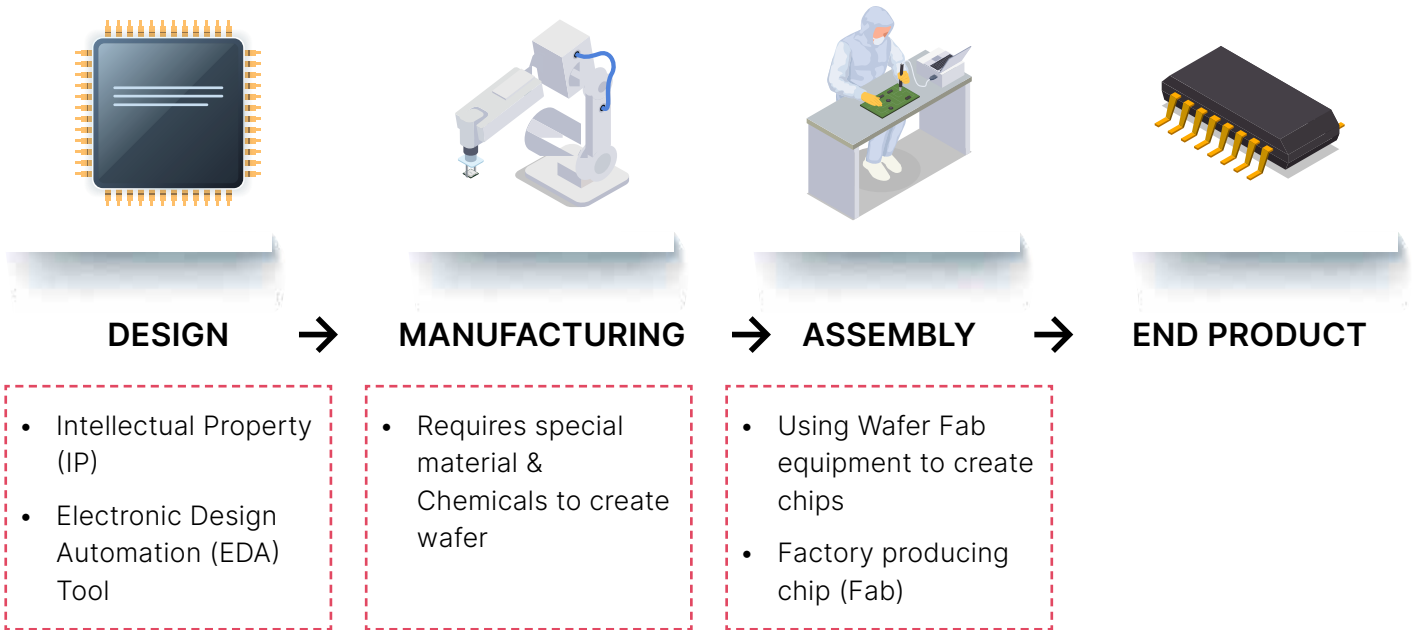
1. Asia-based corporations dealing in the production of Semiconductors have had to stop or slow down their production due to the pandemic
2. Demand fluctuation within Semiconductor Market
3. Rising Inflation
4. Geopolitical Uncertainties and global volatility
5. Logistical challenges due to the COVID-19 pandemic and turbulence in the South China Sea
6. Rapid adoption of Industrial 4.0 Technology



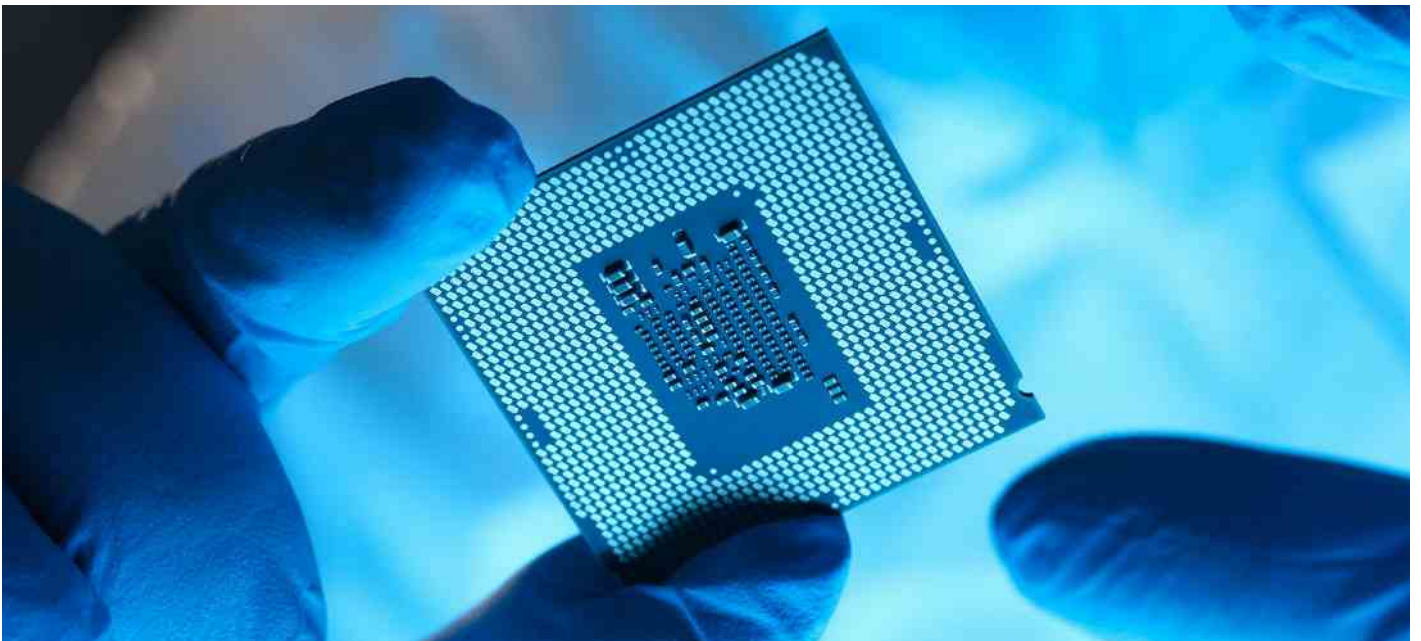
# AN OVERVIEW OF THE SEMICONDUCTOR INDUSTRY

## SEMICONDUCTOR INDUSTRY SEGMENTS

Semiconductor production is a highly complex process that is dependent on various stakeholders collaborating to gain the desired output. The diagram below broadly shows the main segments of the Semiconductor industry ecosystem.



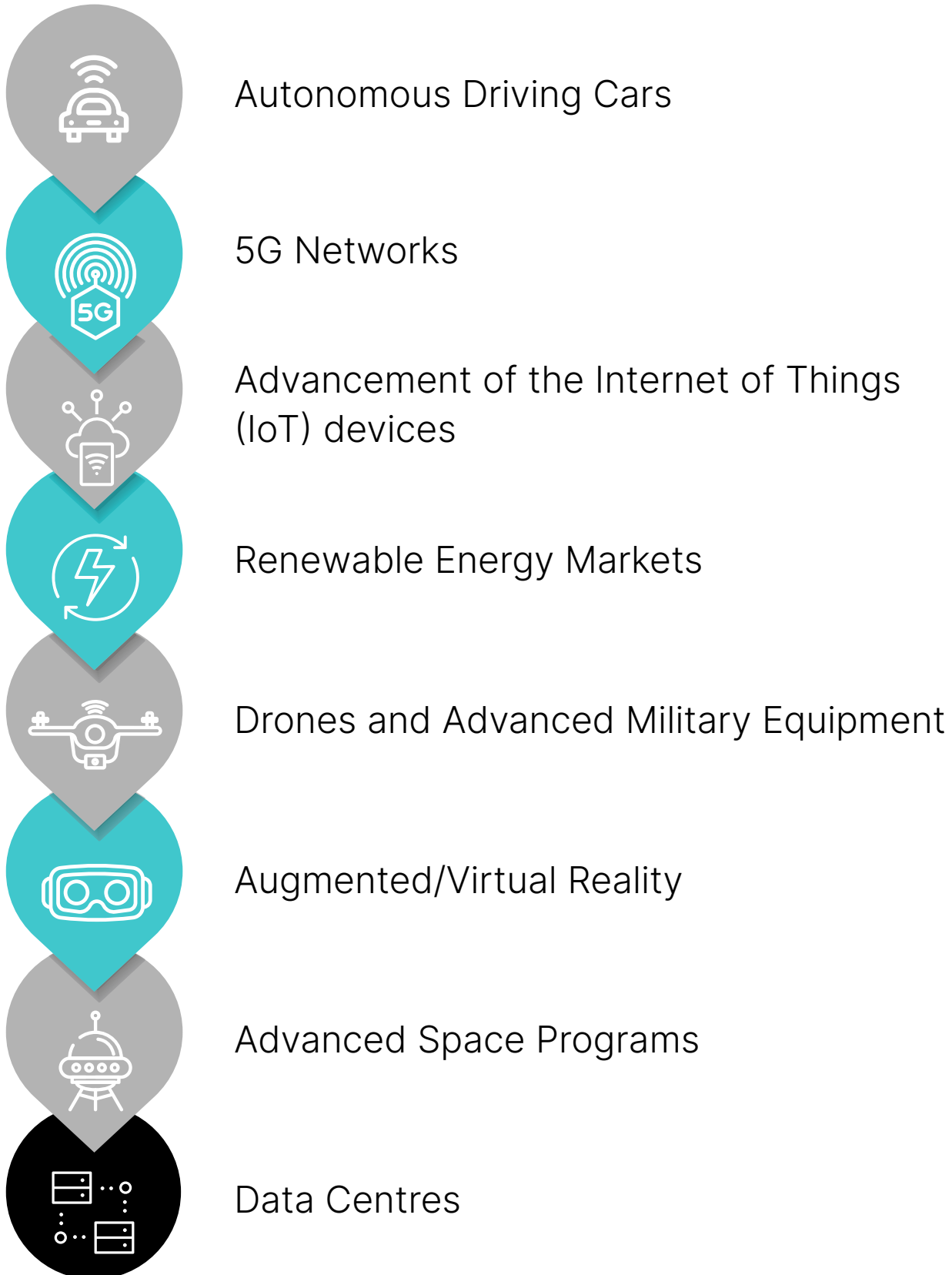
Apart from the segments mentioned above, multiple other processes and organizations are stitched together to produce semiconductors, for example, Integrated Device Manufacturers (IDMS), Fabless manufacturing, Outsourced Semiconductor Assembly and Test (OSAT), etc.



# AN OVERVIEW OF THE SEMICONDUCTOR INDUSTRY

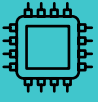
---

## KEY EMERGING TECHNOLOGIES RELIANT ON THE SEMICONDUCTOR INDUSTRY

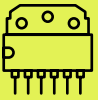


# RECENT GEOPOLITICAL EVENTS WITH A SIGNIFICANT IMPACT ON THE SEMICONDUCTOR INDUSTRY

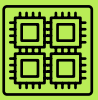
---



Global dependency on [Taiwan Semiconductor Manufacturing Company \(TSMC\)](#) and [Samsung Semiconductor](#) for the mass production of advanced Semiconductor Lithography.



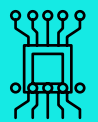
U.S. House Speaker Nancy Pelosi's visit with TSMC chairman Mark Liu during her Taiwan tour in early August 2022. The visit incited [massive cyberattacks](#) in Taiwan Region.



Biden signing the "Chips and Science Act 2022" - "This [Executive Order](#) reflects the Biden-Harris Administration's commitment to quickly increase production of semiconductors, strengthen research and design leadership, and grow a diverse semiconductor workforce to give the country a competitive edge on the world stage."



The role of Quadrilateral Security Dialogue (QSD), commonly known as the QUAD in "[Semiconductor Supply Chain Initiative](#)" is to reform supply chains, global demands, and security issues in the Semiconductor industry.



Volcan Investments Ltd. and Foxconn semiconductor manufacturing [setup](#) in India.



Micron to [invest](#) up to \$100 Billion over the next two decades in a semiconductor factory in New York.



An unknown individual has allegedly [leaked](#) the source code for Intel's Alder Lake BIOS onto 4chan. Shortly afterward, a duplicate copy was posted to GitHub as well. Security researchers warn that the contents could make it easier to find vulnerabilities in the code.



TSMC, Samsung and Intel are expanding there semiconductor manufacturing and research facilities in regions like Arizona, Texas, Germany etc.

# MAJOR THREATS TO SEMICONDUCTOR INDUSTRY & ITS SUPPLY CHAIN

The threat landscape of the Semiconductor industry is becoming highly volatile, with new vulnerabilities emerging daily. As the industry has matured with time, the chips have become even more advanced and complex to produce.

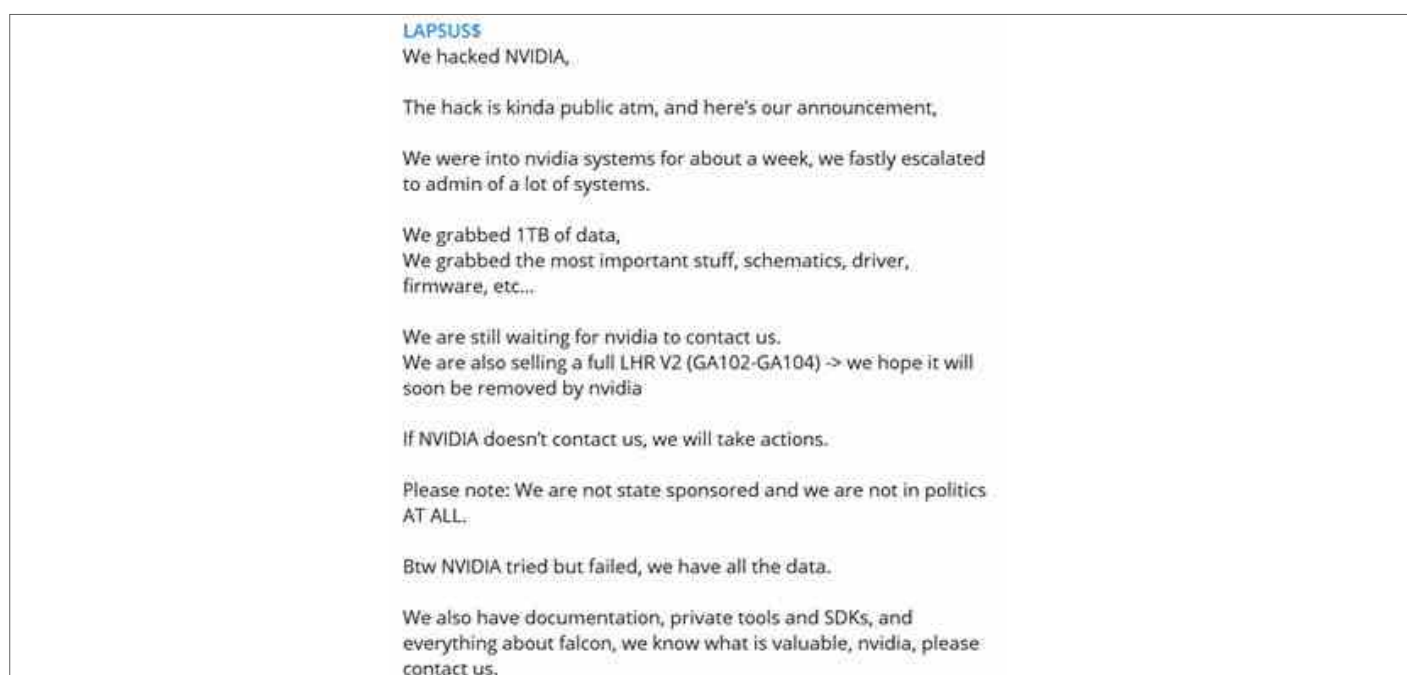
Nowadays, there are multiple organizations and stakeholders involved production, assembly, and distribution of the chips. This has benefited the national economy in some ways, as having multiple parties involved has complicated the supply chain and provided a **broader attack surface** to the attackers.

In 2022, we noticed several ransomware attacks on organizations in the Semiconductor Industry, indicating that Threat Actors (TAs) are actively targeting the industry. It is also essential to understand that every successful cyber-attack on assets related to this industry can create specific scenarios which might impact **Critical National Operations**.

## RANSOMWARE AND EXTORTION GROUPS

Victim Organization	<b>NVIDIA</b>
Data Extortion Group	<b>Lapsus\$</b>
Timeline	<b>February</b>

In February 2022, the Lapsus\$ group claimed that they had breached NVIDIA and were in their systems for about a week. As shown in the figure below, the group claimed to have stolen 1TB of data from the victim organization. The group also claimed to possess confidential data, schematics, drivers, firmware, private tools, SDKs, etc.

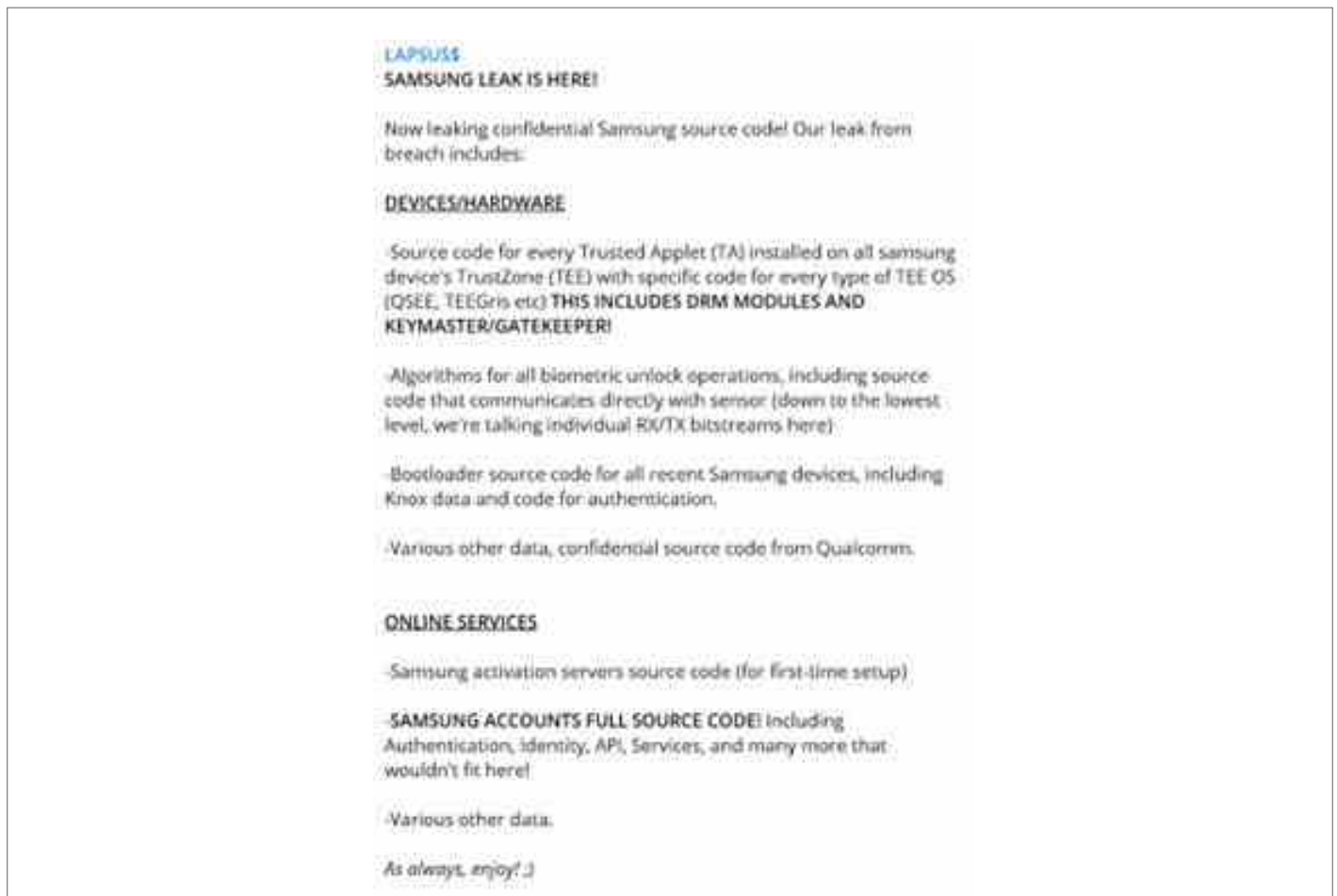




# MAJOR THREATS TO SEMICONDUCTOR INDUSTRY & ITS SUPPLY CHAIN

Victim Organization	Samsung
Data Extortion Group	Lapsus\$
Timeline	March

In March 2022, the Lapsus\$ group claimed to have breached Samsung, and the sample data's availability was advertised on their Telegram channel. Among the data exfiltrated was the source code for every Trusted Applet installed in Samsung's TrustZone, Algorithms for biometric unlock operations (including source code that communicates directly with the sensor), confidential data, source code from Qualcomm and Samsung activation servers, etc.



# MAJOR THREATS TO SEMICONDUCTOR INDUSTRY & ITS SUPPLY CHAIN

---

Victim Organization	Ignitarium
Data Extortion Group	Lockbit
Timeline	March

Ignitarium is a semiconductor manufacturing industry specializing in IC design, FPGA design, Embedded Software, AI/ML, and Robotics. Lockbit 2.0 ransomware group claimed to have access to the company's source code in March 2022.



# MAJOR THREATS TO SEMICONDUCTOR INDUSTRY & ITS SUPPLY CHAIN

Victim Organization	AMD
Data Extortion Group	RansomHouse
Timeline	May

Advanced Micro Devices (AMD), Inc. is one of the leading organizations dealing in cutting-edge semiconductor products. AMD's primary products include microprocessors, motherboard chipsets, embedded processors, graphics processors, and FPGAs for servers, workstations, personal computers, and embedded system applications.

As the Threat Actors (TAs) posted in May 2022, RansomHouse claimed to have exfiltrated 450 GB of data, and the sample data they shared contained numerous compromised devices.

An important point to be noted in this leak was that the TA mocked AMD for having **poor security posture** and using passwords like "password," "123456", "123qwe-" etc., which can be easily brute-forced (as shown below).

**Advanced Micro Devices, Inc**

Advanced Micro Devices, Inc. is an American multinational semiconductor company based in Santa Clara, California, that develops computer processors and related technologies for business and consumer markets. Traded as: NASDAQ: amd, AMD, Nasdaq 100 component, S&P 500 component

**Data leaked**  
05/01/2022

**Downloaded**  
more than 450Gb

**Website**  
<https://www.amd.com/>

**Revenue**  
\$15.4 billion

**Employees**  
22500

**Status: EVIDENCE**  
27/06/2022

**Evidence packs:**  
Download

**Password:**  
no password

An era of high-end technology, progress and top security...there's so much in these words for the crowds. But it seems those are still just beautiful words when even technology giants like AMD use simple passwords like "password", "P@ssw0rd", "123456", "123qwe", "P@ssw0rd", "amd22", "123456", and "12345qwert" to protect their networks from intrusions. It is a shame those are real passwords used by AMD employees, but a bigger shame to AMD Security Department which gets significant financing according to the documents we got our our hands on - all thanks to these passwords.

# MAJOR THREATS TO SEMICONDUCTOR INDUSTRY & ITS SUPPLY CHAIN

Victim Organization	ETRON Technology Inc.
Data Extortion Group	Cuba Ransomware Group
Timeline	June

Etron Technology Inc. is a world-renowned fabless ICS design and product company. The company specializes in producing and researching buffer memory, logic chip designs, electronic applications, and system-on-chips.

Etron has also developed the world's first wafer-level chip-scale micro package and 256MB RPC DRAM for computing devices. As per the post on the Cuba Ransomware site, the TAs could exfiltrate financial documents, balance sheets, tax documents, source codes, etc., as shown below.

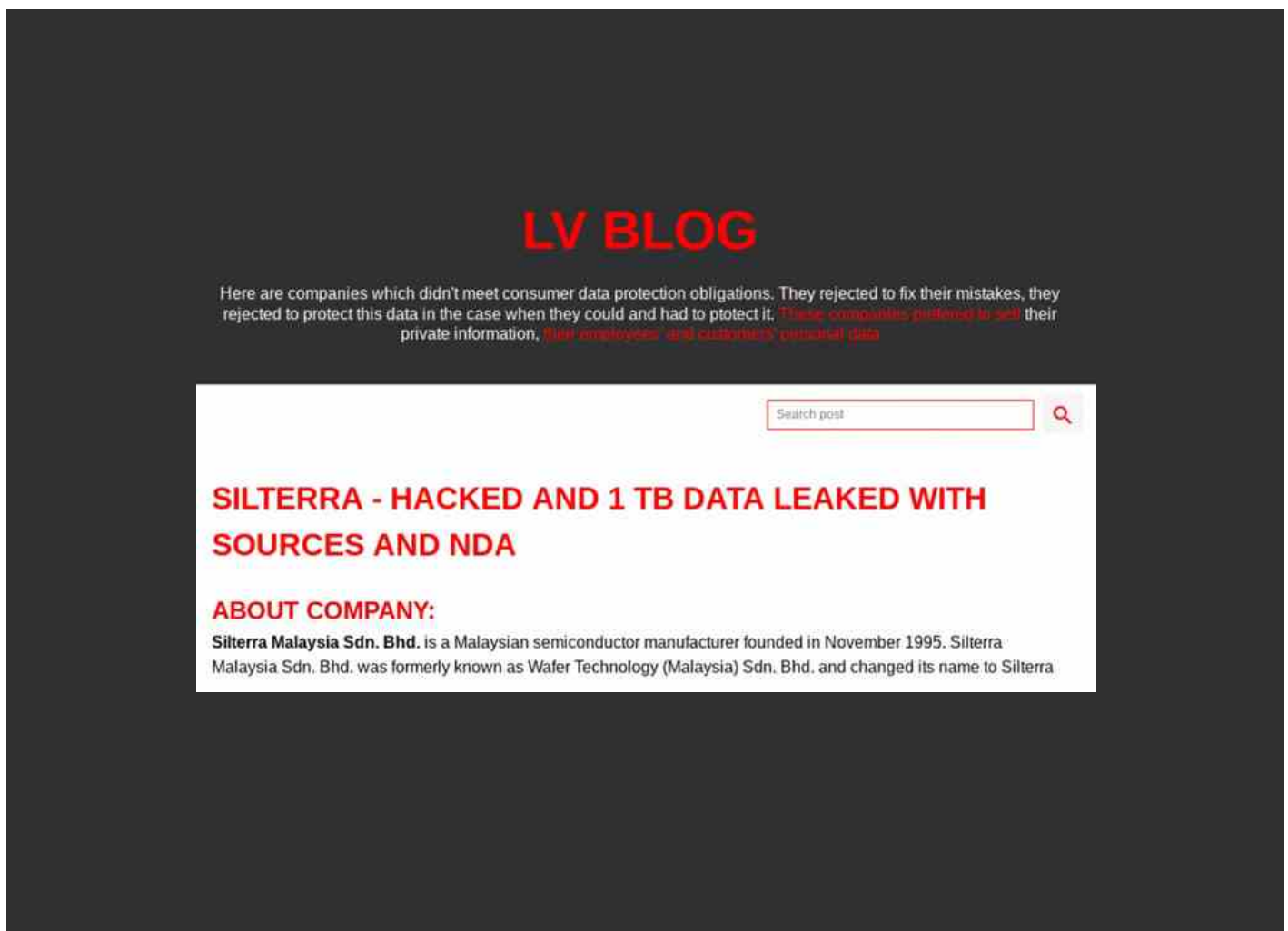




# MAJOR THREATS TO SEMICONDUCTOR INDUSTRY & ITS SUPPLY CHAIN

Victim Organization	SilTerra Malaysia Sdn. Bhd
Data Extortion Group	LV Ransomware Group
Timeline	June

SilTerra Malaysia Sdn. Bhd is a Malaysia-based semiconductor manufacturer formerly known as Wafer Technology (Malaysia) Sdn. Bhd. As per the post on LV Ransomware's website, the TAs were able to exfiltrate 1 TB worth of compromised data, including business planning documents, financial data, employee data, insurance information, client data, etc., all of which were available for download.



# MAJOR THREATS TO SEMICONDUCTOR INDUSTRY & ITS SUPPLY CHAIN

Victim Organization	Diodes Inc.
Data Extortion Group	Lockbit
Timeline	July

Diodes Inc. serves the consumer electronics, computing, communications, industrial, and automotive markets. Diodes Incorporated is a global manufacturer and supplier of application-specific standard products within the discrete, logic, analog, and mixed-signal semiconductor markets.

In July 2022, the LockBit ransomware group claimed to have Diodes' data, including all datasheets, X-ray photos, instructions, engineer comments, production costs and wafer fabrication schemes, companies' confidential data, bank documents, contracts, etc. (as shown below).

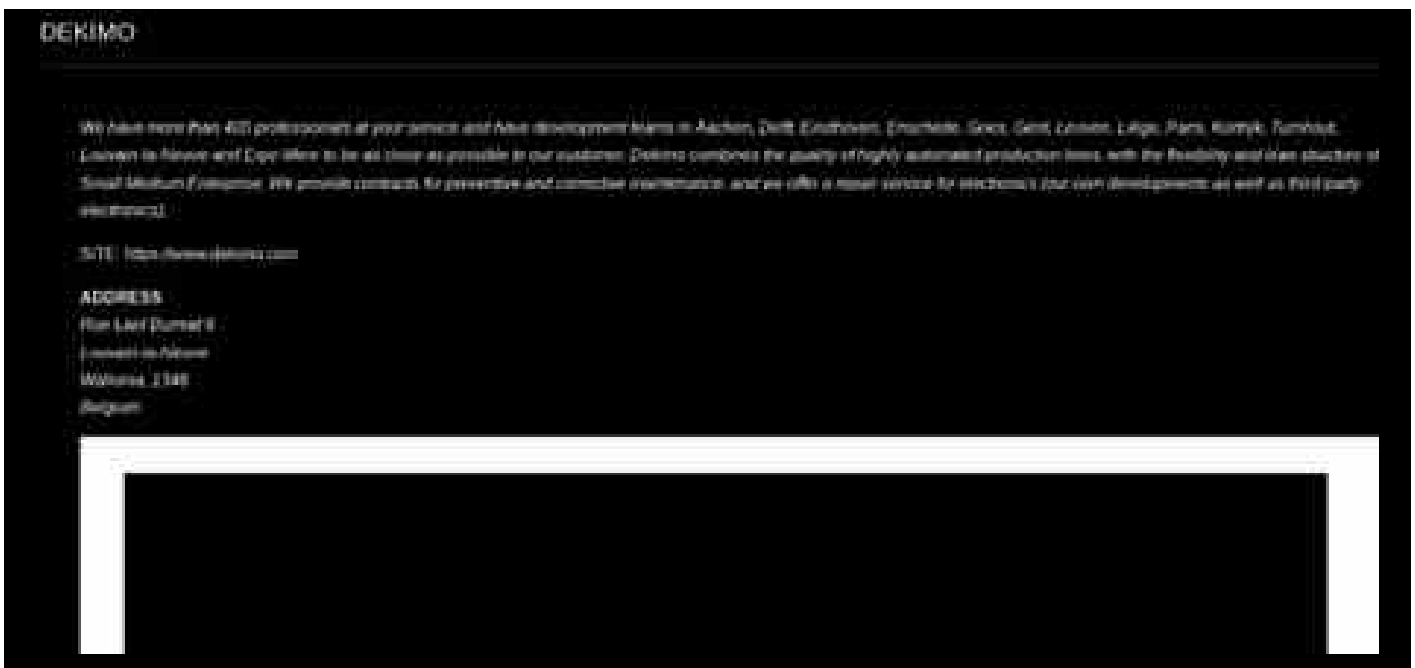


# MAJOR THREATS TO SEMICONDUCTOR INDUSTRY & ITS SUPPLY CHAIN

Victim Organization	Dekimo
Data Extortion Group	Black Basta
Timeline	July

Dekimo is a supplier of software and hardware engineering and are part of semiconductor supply chain. Dekimo offers the following services, amongst many others:

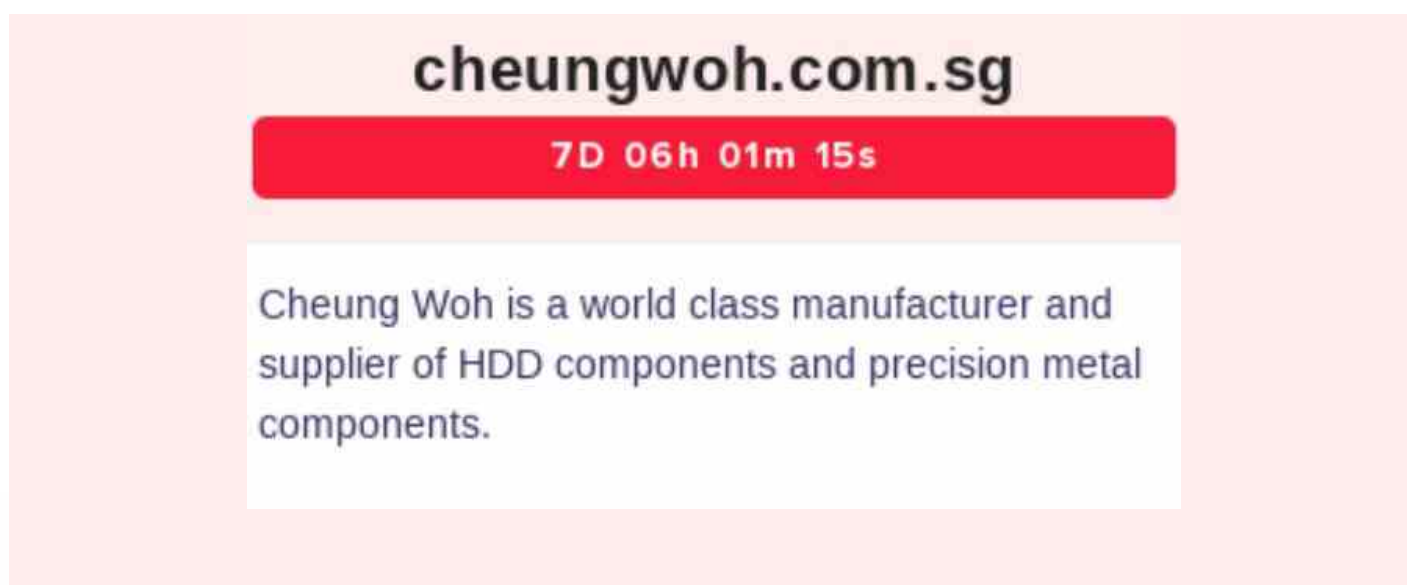
- Development of electronics & software
- Consultancy & flexible staffing in electronics & software
- PCB design/layout and EMC measurements
- Series production and assembly of PCBAs
- Mechatronics solutions



# MAJOR THREATS TO SEMICONDUCTOR INDUSTRY & ITS SUPPLY CHAIN

Victim Organization	Cheung Woh Technologies Ltd.
Data Extortion Group	Lockbit
Timeline	July

[Cheung Woh](#) provides high-precision engineering products to the HDD, communications, electronics, semiconductor, and automotive industries. The Lockbit ransomware group allegedly compromised them in July 2022.





# MAJOR THREATS TO SEMICONDUCTOR INDUSTRY & ITS SUPPLY CHAIN

Victim Organization	Semikron
Data Extortion Group	LV Ransomware Group
Timeline	August

Semikron is a power semiconductor component manufacturer based out of Germany. Semikron manufactures integrated circuits, discrete semiconductors, transistors, diodes, thyristor power modules, power assemblies, and systems for markets. These include industrial drives, wind and solar energy, hybrid and electric cars, the rail sector, and power supplies.

As per the post on the LV Ransomware website, the TAs were able to exfiltrate 2 TB data, including:

- NDAs
- Drawings
- Employee Data
- Contracts
- Finance Data
- Investment Data
- Customer Database

**SEMIKRON - EXTREMELY LOW LEVEL OF CYBERSECURITY. 2 TB OF CORPORATE DATA STOLEN**

publication at 04.08.22 19:03 GMT

**Information on the Cyber Incident at SEMIKRON**

SEMIKRON **does not** cares very much about a trustful and transparent cooperation with its customers and partners. Therefore, we would like to inform you that the SEMIKRON Group has become a victim of a cyber attack by a professional hacker group **LV**.

**ABOUT COMPANY:**

Semikron is a German-based independent manufacturer of power semiconductor components. The company was founded in 1951 by Dr. Friedrich Josef Martin in Nuremberg. In 2019, the company has a staff of more than 3.000 people in 24 subsidiaries with production sites in Germany, Brazil, China, France, India, Italy, Slovakia and the USA.


**ABOUT DATA THAT WE HAVE:**

- NDA
- Drawings
- Employee data
- Contracts
- Finance data
- Investment data
- Customers database

# MAJOR THREATS TO SEMICONDUCTOR INDUSTRY & ITS SUPPLY CHAIN

Victim Organization	Peak International Limited
Data Extortion Group	Lockbit
Timeline	September

Peak International Limited supplies precision-engineered packaging products for the storage, transportation, and automation handling of semiconductor devices and other electronic components. The company's products are designed to interface with automated handling equipment used in the production and testing of semiconductor and electronic products.



**peakinternational.com**  
peak.com.hk

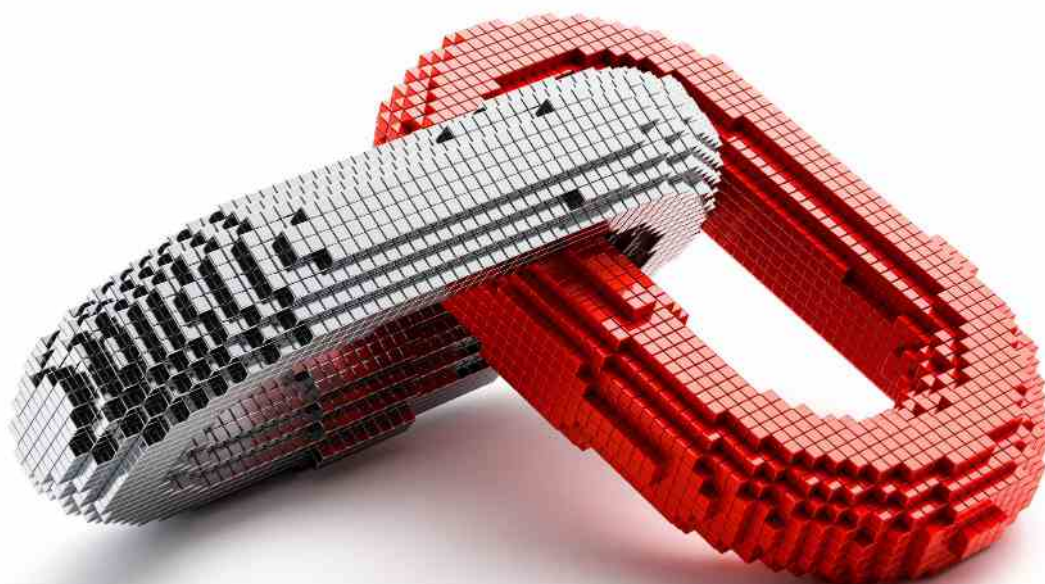
Peak is an industry leader in engineered plastics and packaging for high value-add products in industries such as semiconductors, precision mechanical components, and solutions for the laboratory, and consumer markets. With offices in Hong Kong, manufacturing facilities in Shenzhen (PRC), and distribution centers worldwide, Peak brings unprecedented economics together with superior design and service to deliver complete solutions to our customers.

Peak's products are already in use by some of the world's largest companies in their high-speed, automated manufacturing processes that require dimensional stability and precision tolerances. Peak has a wide array of standard packaging products, large manufacturing capacity, tooling and design expertise, and a worldwide footprint to support even the toughest JIT requirements.

Peak's worldwide SemiCycle?division is a leading recycler of used plastics. Additionally, Peak is equipped to utilize specially formulated plastics to reduce weight, carbon footprint, and evolving industry requirements for the elimination of PVC-based plastics in many applications.

Founded in 1987, Peak is a stable, reliable plastics and packaging partner supplying the Global 2000 in a wide range of and industries. Peak has been recognized by industry with numerous supplier awards and is ISO-9002, QS-9000 and ISO-14001 certified.

**ALL AVAILABLE DATA WILL BE PUBLISHED !**



# MAJOR THREATS TO SEMICONDUCTOR INDUSTRY & ITS SUPPLY CHAIN

Victim Organization	Mektec Trading (Shanghai) Co., Ltd.
Data Extortion Group	Lockbit
Timeline	September

The "MEKTEC" group provides flexible printed circuits, precision rubber, and resin parts for electronic devices to varied customers.



# MAJOR THREATS TO SEMICONDUCTOR INDUSTRY & ITS SUPPLY CHAIN

Victim Organization	Phoenix Silicon International Corporation
Data Extortion Group	LV Ransomware Group
Timeline	September

Phoenix Silicon International was established in 1997 and was started by Wafer Reclaim Department. Then, it developed into the [Wafer Thinning](#) Department and Wafer Integration Department. Wafer reclaim is based on a professional stripping process.

It can remove all kinds of films from IC Fab without damaging the characteristics of the wafers, such as photoresistors, oxides, metal films, etc.





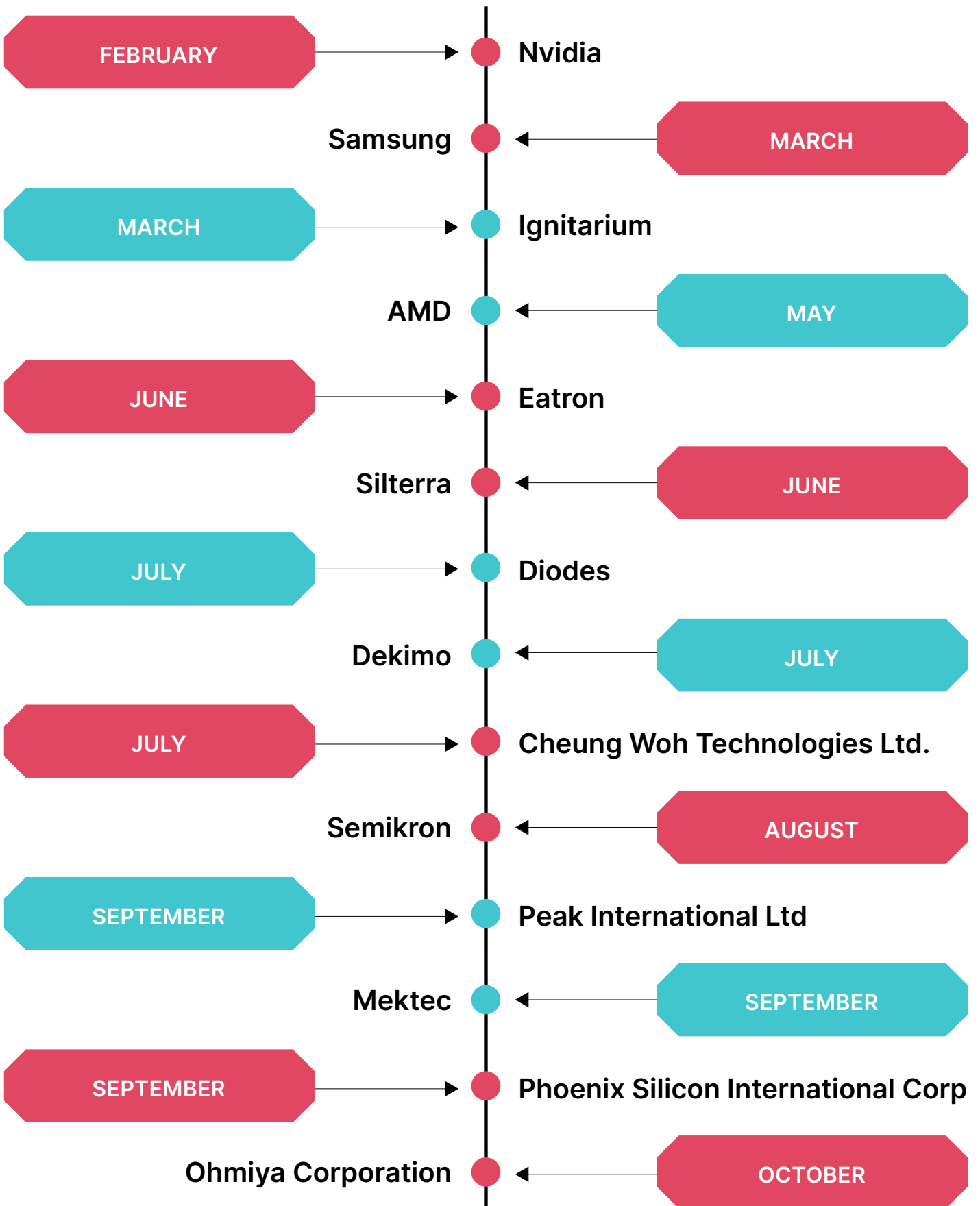
# MAJOR THREATS TO SEMICONDUCTOR INDUSTRY & ITS SUPPLY CHAIN

Victim Organization	Ohmiya Corp
Data Extortion Group	Lockbit
Timeline	October

[Ohmiya Corporation](#) sells industrial chemicals such as surface treatment chemicals, sewerage chemicals, resins, and chemical materials for semiconductor and display use. Ohmiya also sells industrial machinery and electronic parts.



# MAJOR THREATS TO SEMICONDUCTOR INDUSTRY & ITS SUPPLY CHAIN



# MAJOR THREATS TO SEMICONDUCTOR INDUSTRY & ITS SUPPLY CHAIN

## INITIAL ACCESS BROKERS AND THEIR ROLE IN SELLING CRITICAL INFRA ACCESS IN UNDERGROUND MARKETS

**Initial Access Brokers** are financially motivated Threat Actors (TAs) that obtain access to enterprises. They subsequently sell these accesses to Ransomware-as-a-Service (RaaS) operators, APT groups, and other nefarious cyber criminals on cybercrime forums, thus giving them a larger attack surface to target.

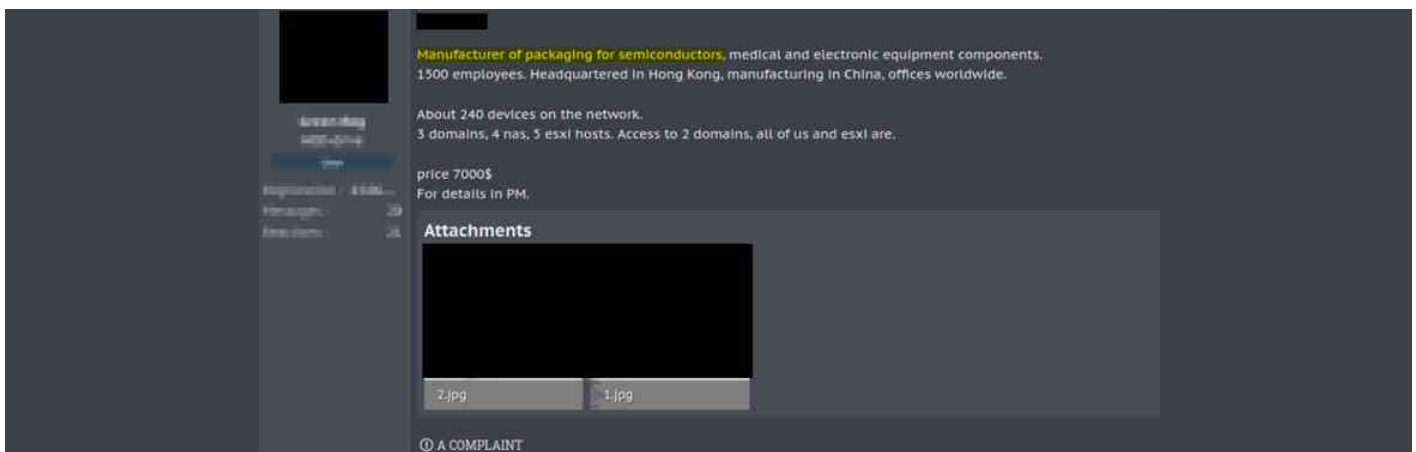
This, in turn, allows them to steal data and deploy ransomware or malware without worrying about leaving footprints in the network during the initial intrusion.

During our routine monitoring, we discovered that one of the TAs was selling Remote Desktop Protocol (RDP) access to an organization dealing in Electronics and Electrical services in Taiwan.

Our preliminary open-source investigation indicated that the impacted organization was possibly a semiconductor manufacturer, but the affected organization's identity remains unconfirmed.



A Threat Actor on a Russian cybercrime forum claimed to provide access to the domains of an organization dealing in the manufacture of packaging for semiconductors and medical and electronic equipment components.

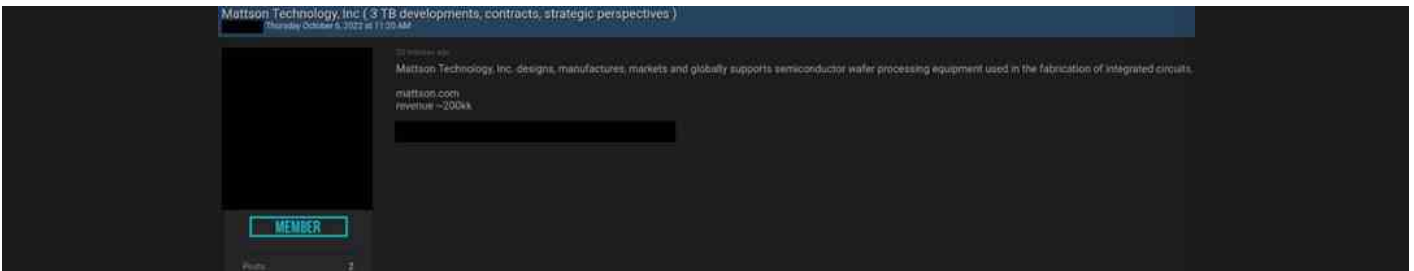


# MAJOR THREATS TO SEMICONDUCTOR INDUSTRY & ITS SUPPLY CHAIN

## DATA BREACHES/LEAKS IN THE SEMICONDUCTOR INDUSTRY

During a routine threat hunting exercise, Cyble Research & Intelligence Labs discovered a Threat Actor claiming to sell 3 TB of compressed data (as shown in the image below) containing folders concerning financial information, employee details, and business information of US-based semiconductor equipment manufacturer Mattson Technology, Inc.

Mattson Technology is a Beijing-based and state-owned E-town International subsidiary that has operations spanning high-tech manufacturing businesses in the semiconductor, aviation, automotive, and telecom sectors.



The resurfaced database of the Malaysian Ministry of International Trade and Industry (MITI) Public Private Industrial Immunization Programme (PIKAS) required companies to register their employee's vaccination status.

The information MITI required companies to submit includes:

- Company name
- Employee name
- National Registration Identity Card/Passport number
- Phone number
- Position

Among the long list of companies that provided PII details of their employees was NXP Semiconductors Malaysia. NXP Semiconductor Malaysia is a modern semiconductor facility for assembling and testing Integrated Circuits (ICs).

NXP provides technology solutions targeting the automotive, industrial, IoT, mobile, and communication infrastructure markets.

The standard format of leaked files can be seen below.

Name	No. I/C or Passport No.	Employee ID	AGE	GENDER	CONTACT NO
[REDACTED]	87 [REDACTED]	[REDACTED]	34	Male	01 [REDACTED]
[REDACTED]	IP [REDACTED]	[REDACTED]	33	Male	01 [REDACTED]
[REDACTED]	78 [REDACTED]	[REDACTED]	43	Male	01 [REDACTED]
[REDACTED]	84 [REDACTED]	[REDACTED]	37	Female	01 [REDACTED]
[REDACTED]	93 [REDACTED]	[REDACTED]	28	Female	01 [REDACTED]
[REDACTED]	73 [REDACTED]	[REDACTED]	48	Male	01 [REDACTED]

# MAJOR THREATS TO SEMICONDUCTOR INDUSTRY & ITS SUPPLY CHAIN

---

## OT & IOT EXPOSURE AND IMPACTS

The various products that end-users utilize day to day, which contain semiconductors, have a very long journey from their origin to end use. This includes their design, manufacturing, assembly, testing, etc.; the process consists of using various Operational Technology (OT) and the Internet of Things (IoT) equipment.

The numerous Equipment, Sensors, Applications, Protocols, etc., used in the semiconductor industry and the organizations connected with it might be vulnerable to exploitation by Threat Actors. With rising internet-facing assets, an organization's risk of exploitation increases proportionally.

There are multiple automations placed in the process of manufacturing semiconductors, which include the usage of Programmable Logic Controllers (PLCs), SCADA systems, Industrial routers, switches, etc.

This equipment has recently been a prime target for TAs due to the impact they can create on the entire supply chain, operations, and physical damage to factories.

Hence, entities in the semiconductor industry should take extra precautions while installing, operating, and monitoring OT and IoT equipment, as they might be under the scope of attackers while launching a targeted attack on the industry.

## INSIDER THREATS TO THE SEMICONDUCTOR INDUSTRY

Insider Threat includes a current or former employee or business associate with access to sensitive information or privileged accounts within an organization's network and intentionally or inadvertently misusing this access. Insiders continue to be a significant issue and a difficulty for firms regarding intellectual property and trade secrets.

If the chip designs get leaked in the public domain or distributed on Darkweb forums, malicious adversaries or competitive entities could gain access to them, compounding the risk of reverse engineering and IP theft.

Insider threats present a complex and dynamic risk affecting the multiple vectors in the supply chain of Semiconductors. Although the globalization of IC design, manufacturing, assembly, and deployment lowers overall costs and facilitates various advantages, it poses substantial concerns to intellectual property privacy and integrity. Malicious design modification and intellectual property theft are the two critical dangers of the worldwide IC supply chain.



# CONCLUSION

---

Cyble believes that with government and state entities supporting start-ups, collaborations, and other schemes to promote domestic production and export of semiconductors, Threat Actors (TAs) will continue actively targeting employees via social engineering campaigns as they try to exploit the human element in an organization's cybersecurity posture.

With companies and nations accelerating and competing in the manufacturing of semiconductors, more minor and more advanced semiconductor chips, insider threat incidents, and data leaks continue to pose a significant cybersecurity risk.

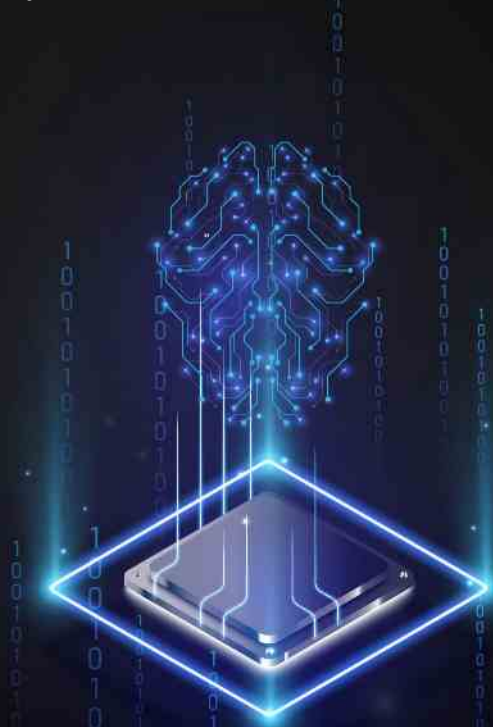
As per *IC insights*, "IC Insights expects foundry giant TSMC to surpass Samsung and take over the top spot in the semiconductor company sales ranking in 3Q22. Intel is expected to move to the third position in the ranking with 3Q22 sales of 26% less than TSMC's.

TSMC was ranked as the third largest semiconductor supplier in the world in 2021 and had sales that were 31% less than Samsung's."

Cyble believes that advanced military equipment, the automotive industry, and the telecommunications sectors will be disproportionately targeted and impacted due to increased cyber-attacks globally. A country's dependency on imported components used within defense and military equipment can play a massive role in geopolitical conflicts and is a national security concern. TAs will thus look to target the various entities in the supply chain.

Increased ransomware attacks will severely impact victim organizations' operations, further disrupting processes in the entities connected with these victim organizations.

Cyble believes that the trade and economy of nations will also be widely affected by the incidents happening in the semiconductor supply chain resulting in delays and shortages of technologies that heavily rely on semiconductors.



# RECOMMENDATIONS

---

1. Ensure physical access controls & network perimeter security placed by the organization are adequate.
2. Implement proper network segmentation to prevent attackers from lateral movement and minimize exposure of critical assets over the internet.
3. Implementing Zero Trust policy within the organization.
4. Keep critical assets behind properly configured and updated firewalls.
5. Utilize Software Bill of Materials (SBOM) to gain further visibility into assets.
6. Keeping software, firmware, and applications updated with the latest patches and mitigations released by official vendors is necessary to prevent attackers from exploiting vulnerabilities.
7. Implementing proper access controls.
8. Organizations should follow a strong password policy at all times.
9. Regular Audits, Vulnerability, and Pentesting exercises are vital in finding security loopholes that attackers may exploit.
10. Continuous monitoring and logging can help in detecting network anomalies early.
11. Implement Multi-Factor Authentication wherever possible.
12. Keep track of advisories and alerts issued by vendors and state authorities.
13. Cyber security awareness training programs for employees within the organization.
14. Enhance Risk Intelligence throughout the organization.
15. Implement secure backup, archiving, and recovery processes.

# ABOUT US

---

Cyble is a global threat intelligence SaaS provider that helps enterprises protect themselves from cybercrimes and exposure in the Darkweb. Its prime focus is to provide organizations with real-time visibility into their digital risk footprint. Backed by Y Combinator as part of the 2021 winter cohort, Cyble has also been recognized by Forbes as one of the top 20 Best Cybersecurity Start-ups to Watch In 2020. Headquartered in Alpharetta, Georgia, and with offices in Australia, Singapore, Dubai and India, Cyble has a global presence.

To learn more about Cyble, visit [www.cyble.com](http://www.cyble.com)

