Brief History of ICS-Tailored Attacks

10 Attacks from 2000-2022

mamdouhmuhammad

mamdouh.de

Maroochy Shire Sewage Attack (2000)

Threat Actor (Who): A disgruntled insider (Vitek Boden), a former contractor for Maroochy Water Services. After failing to get a job with the utility, he decided to sabotage the system in revenge.

Threat Vector (How): Boden used a laptop and radio transmitter stolen from his employer to remotely send unauthorized control signals to the sewage SCADA network. Over at least 46 separate occasions, he drove around intercepting and transmitting radio commands to pumping stations.

Threat Target (What): The target was Maroochy Shire Council's sewage pumping control system in Queensland, Australia.

By altering pump operations and disabling alarms, Boden's attacks caused pumps to malfunction and overflow. An estimated 800,000 liters of raw sewage spilled into local parks, rivers, and even the grounds of a hotel, killing marine life and creating noxious conditions.
(The attacker was eventually caught and convicted.)

SQL Slammer Worm (2003)

Threat Actor (Who): SQL Slammer was an Internet worm rather than a directed human attacker. Its creator remains unknown. The worm spread indiscriminately worldwide in January 2003, exploiting a buffer overflow in Microsoft SQL Server. It was not specifically aimed at industrial systems, but its effects reached them.

Threat Vector (How): The worm propagated rapidly through networks by scanning for vulnerable MS-SQL servers. At Ohio's Davis-Besse nuclear power plant, Slammer penetrated via an unsecured connection: it entered through an outside contractor's network and traversed a T1 line into the plant's internal network, bypassing the firewall. Because a critical server hadn't been patched, the worm infected it and flooded the plant network with traffic.

Threat Target (What): The immediate impact was on the plant's Safety Parameter Display System (SPDS) – a monitoring system for reactor safety. The Slammer infection overwhelmed the network and disabled the SPDS for nearly five hours, leaving operators without the computerized safety display. (Fortunately, the reactor was offline at the time and a backup analog system remained available. No physical damage occurred, but the incident highlighted the vulnerability of ICS networks to collateral infection from global malware.)

Stuxnet (2010)

Threat Actor (Who): A nation-state cyber operation that was considered a “cyber-weapon” developed under the secret Operation Olympic Games. Its development involved significant resources and intelligence about Iran’s nuclear facilities.

Threat Vector (How): Stuxnet was a highly sophisticated worm with multiple zero-day exploits. It was introduced via an infected USB flash drive into the secure, air-gapped network of Iran’s Natanz uranium enrichment facility. Once inside, it spread through Windows systems and sought out Siemens Step7 PLC software. The malware was tailored to alter the control logic on specific Siemens programmable logic controllers (PLCs) used for gas centrifuges. By masquerading as legitimate control signals and hiding its tracks, Stuxnet silently sabotaged the centrifuge operation.

Threat Target (What): The target was Iran’s gas centrifuges used to enrich uranium, controlled by Siemens PLCs at Natanz. Stuxnet caused the centrifuges to spin at irregular speeds, ultimately tearing themselves apart. It’s reported to have destroyed about 1,000 centrifuges, roughly one-fifth of Iran’s capacity, setting back the nuclear program. This attack, discovered in 2010, was the first known case of malware causing physical destruction of industrial equipment.

Shamoon (in Arabic شمعون) (2016 & 2012)

Threat Actor (Who): A suspected Iranian state-linked group, which in 2012 identified itself as the “Cutting Sword of Justice.” U.S. intelligence later attributed the 2012 Shamoon attack to Iran. The malware reappeared in 2016 (sometimes called “Shamoon 2”), likely by the same or affiliated actors, again targeting Gulf state organizations.

Threat Vector (How): Shamoon (also known as DistTrack) is a destructive wiper malware. In 2012, attackers infiltrated the network of Saudi Aramco – possibly via a phishing email or an infected USB device (exact initial access remains unclear publicly). Once inside, Shamoon stole administrative credentials, spread through Windows workstations, and then wiped the hard drives of infected computers, overwriting data with a political image. The malware also had a logic bomb to trigger the wipe at a specific time. In 2016, a new wave of Shamoon attacks similarly used phishing and malware to breach networks of Saudi government agencies and companies (e.g. General Authority of Civil Aviation (GACA)) before deploying the wiper.

Threat Target (What): Shamoon’s 2012 attack hit Saudi Aramco, the world’s largest oil company, erasing data on approximately 35,000 corporate computers (about 75% of Aramco’s PCs). The wipe rendered the machines unusable, forcing Aramco to replace drives and disrupting its business operations for weeks. Less than two weeks later, Qatar’s RasGas was also affected. In late 2016, Shamoon attacks struck Saudi government offices and critical organizations, wiping servers and PCs; for example, Saudi’s General Authority of Civil Aviation had operations disrupted for several days. These Shamoon incidents did not directly manipulate ICS hardware, but by crippling the corporate IT infrastructure of oil & gas organizations, they indirectly impacted industrial operations and highlighted the potential for state-sponsored cyber retaliation.

German Steel Mill Attack (2014)

Threat Actor (Who): An unknown advanced threat group, likely state-sponsored, with deep knowledge of industrial control systems. The attackers were noted to have “very pronounced” expertise in both general IT security and specific industrial processes. (The incident was reported by Germany’s Federal Office for Information Security (BSI), but the perpetrators were not publicly identified.)

Threat Vector (How): The attack began with a spear-phishing campaign against the steel plant’s corporate network. Employees were tricked into opening malicious attachments or links, giving the attackers a foothold. From there, the adversaries pivoted into the plant’s production network, gradually compromising a multitude of systems including industrial control components. They manipulated the plant’s control systems, causing various subsystems to fail. Notably, the attackers leveraged their specialized ICS knowledge to override or disrupt safety interlocks.

Threat Target (What): The target was a blast furnace at an unnamed steel mill in Germany. The cyber intruders ultimately caused a situation where operators could not properly shut down the blast furnace. The furnace was left in an uncontrolled state, resulting in “massive damage” to the equipment. This was one of the first publicly known instances of a cyber attack causing direct physical destruction in an industrial plant (comparable in significance to Stuxnet). Fortunately, reports did not indicate any injuries, but the financial and production losses were presumably large.

Ukraine Power Grid Attack (BlackEnergy, 2015)

Threat Actor (Who): A Russian military-linked hacker group known as Sandworm (or "Telebots"), identified by Ukrainian and Western investigators as responsible for this attack. The attack on Ukraine's power grid in December 2015 took place amid the ongoing conflict in eastern Ukraine, and is considered a state-sponsored operation by Russia.

Threat Vector (How): The attackers spent months in preparation. They first penetrated the IT networks of three regional electricity distribution companies using spear-phishing emails with malicious Microsoft Office documents. These emails delivered the BlackEnergy3 malware (a trojan toolkit) into the corporate network. From there, the attackers moved into the operational networks. On December 23, 2015, they remotely took control of the SCADA systems used by grid operators. The attackers opened dozens of circuit breakers across multiple substations nearly simultaneously, using the legitimate control interfaces but under unauthorized access. They also sabotaged the infrastructure: malicious firmware was deployed to substation equipment, phone lines were jammed (denial-of-service to call centers), and disk-wiping malware (KillDisk) was activated on computers to erase files and render systems inoperable.

Threat Target (What): The targets were three power distribution companies in Ukraine (serving Ivano-Frankivsk, Chernivtsi, and Kyiv regions). The coordinated attack opened about 30 substations and cut power to approximately 225,000 customers in the middle of winter. The lights went out for 1 to 6 hours for those customers until manual operations could restore power. This incident was the first confirmed cyberattack on a power grid, marking a grim milestone in ICS security. Recovery was aided by having manual operations as a fallback, but the companies had to painstakingly rebuild computer systems and improve network security afterward.

Industroyer (CrashOverride, 2016)

Threat Actor (Who): The Sandworm group (Russia) is also believed to be behind this December 17, 2016 attack on Ukraine's power grid. Coming one year after the 2015 blackout, the 2016 attack showed the attackers' continued intent to disrupt Ukrainian critical infrastructure. Security experts assess this operation as a planned "large-scale test" of a new grid-attack malware.

Threat Vector (How): The attackers developed a specialized piece of malware known as Industroyer (or CrashOverride). After infiltrating the electric transmission company's network (via means not publicly detailed, possibly using backdoors or phishing from prior campaigns), they deployed Industroyer within the substation control systems. Uniquely, Industroyer was designed to directly communicate with power grid equipment using standard electric utility protocols (such as IEC 60870-5-104 and IEC 61850). In effect, the malware acted like a rogue grid operator: it sent commands to circuit breakers to open them and disable power, without needing human supervision. The malware also had a wiper component to erase itself and disable systems after executing the attack.

Threat Target (What): The target was part of Ukraine's high-voltage transmission substation infrastructure near Kyiv. The Industroyer attack succeeded in cutting off about a fifth of Kyiv's power for roughly one hour. While brief, this was the second cyber-induced blackout in Ukraine and the first ever caused by tailor-made grid malware. Industroyer is notable as the first malware created specifically to disrupt electric power grids. Its existence demonstrated a new level of threat to ICS, though in this case the impact was limited in duration. (Investigators believe the 2016 attack may have been a proof-of-concept by the attackers, as it occurred late at night and affected a smaller area than the 2015 incident.)

TRISIS/TRITON (2017)

Threat Actor (Who): A state-sponsored adversary believed to be linked to Russia. In 2018, FireEye identified the likely source as Russia's Central Scientific Research Institute of Chemistry and Mechanics (CNIIHM), a government research entity, based on the malware's tooling and network activity. This was the first known cyber attack to deliberately target industrial safety systems, raising alarm in the global security community.

Threat Vector (How): The attackers gained access to the target petrochemical plant's networks (possibly via phishing or exploiting an IT vulnerability – details were not made public). Once on the operational network, they focused on the Safety Instrumented System (SIS), which is a fail-safe mechanism for industrial plants. They deployed a sophisticated malware known as "Triton" or "Trisis" onto the SIS engineering workstation, which was running the Schneider Electric Triconex safety PLC software. The malware was able to communicate with and attempt to reprogram the Triconex safety controllers. It even exploited a Windows vulnerability on the engineering station to gain persistent control. The goal was to disable or modify the safety logic – effectively to sabotage the safety layer that protects against dangerous conditions.

Threat Target (What): The target was a petrochemical plant in Saudi Arabia, reportedly the Tasnee petrochemical facility (although officially unnamed, media reports indicate the company Tasnee). Specifically, the attack targeted the Triconex SIS controllers that ensure safe operation of critical processes. In August 2017, the Triton malware attempted to manipulate these safety controllers. Fortunately, the attack failed in a safe way – the SIS detected an anomaly and triggered a plant shutdown. This meant the industrial process was halted safely before any damage occurred. However, investigators noted that had the malware succeeded in disabling safety interlocks, the plant could have been exposed to conditions leading to equipment damage or even a potential industrial accident (e.g. toxic release or explosion). Triton is thus regarded as one of the most dangerous ICS threats, since it directly targets life-critical safety systems.

Colonial Pipeline Ransomware Attack (2021)

Threat Actor (Who): A criminal ransomware gang known as DarkSide. This group, likely operating out of Eastern Europe/Russia, is financially motivated and not state-sponsored. DarkSide had a history of targeting organizations for ransom, and Colonial Pipeline became its most prominent victim.

Threat Vector (How): In spring 2021, DarkSide actors gained entry via a compromised VPN password for Colonial Pipeline's network. The VPN account did not have multi-factor authentication, making it easier for the attackers to use stolen credentials. After breaching the IT network, the hackers moved laterally and deployed their ransomware. They also stole approximately 100 GB of data from Colonial's servers (a "double extortion" tactic). The ransomware payload encrypted critical business systems, including accounting and billing, locking the company out of its own data.

Threat Target (What): The ransomware directly impacted Colonial Pipeline's business (IT) network – no physical control systems were reported harmed. However, the company preemptively shut down its 5,500-mile fuel pipeline (which supplies ~45% of the U.S. East Coast's fuel) for several days to contain the threat. This led to gasoline shortages and panic buying in multiple states, and the U.S. government issued emergency waivers to transport fuel by other means.
Pipeline paid the ransom, about $4.4 million in Bitcoin, to obtain a decryption tool. Although operations resumed after nearly a week (by May 12, 2021), the attack highlighted the vulnerability of critical infrastructure to IT-focused attacks and prompted new federal cybersecurity directives for pipeline operators.

Industroyer2 (2022)

Threat Actor (Who): Sandworm (Russian GRU), the same state-backed group behind previous Ukrainian grid attacks, launched this operation in the midst of the 2022 Russian invasion of Ukraine. Western governments publicly attributed the attempted attack to the Russian state in May 2022, as part of broader cyber aggression against Ukraine.

Threat Vector (How): The adversaries deployed a new variant of the Industroyer malware – dubbed Industroyer2 – tailored to Ukraine's power grid equipment. Alongside Industroyer2, they unleashed multiple strains of wiper malware (called CaddyWiper, OrcShred, etc.) on the victim network. The attack was meticulously scheduled: Industroyer2 was set to send out grid disruption commands at a specific time, and then the wipers would erase systems to hinder recovery. The malware's payload was configured to speak the communication protocols of high-voltage substations, opening breakers and attempting to cause a blackout, just like its 2016
predecessor.

Threat Target (What): The target was a Ukrainian regional electric utility's high-voltage substations. In April 2022, Sandworm operatives tried to trigger a widespread power outage in Ukraine by remote control of those substations . Importantly, this attack was thwarted. Ukraine's CERT (CERT-UA), with help from cybersecurity experts, detected the malicious activity in time. They isolated systems and prevented Industroyer2 from executing its full mission. The attempted grid sabotage was successfully repelled by the defenders, avoiding any major power disruption. This foiled Industroyer2 attack underscores how critical infrastructure remains in the crosshairs during geopolitical conflicts, and how proactive cyber defense can mitigate even highly advanced threats.