OT: ICEFALL: Coming soon to a water treatment plant near you. (Or an LNG installation; or a power generation plant; or a major hospital; the list is almost endless.)

I can corrupt, manipulate, control what you see
I am the instigator of your future technology
I know your vices and desires but won't fix 'em for free
— Eyes on Me, Paranoid dj

I agree that ICEFALL does sound like a recent James Bond movie. Moreover, the subject of software vulnerabilities in **Industrial Control Systems/Operational Technology (ICS/OT)**, and the possible tragic outcomes once these vulnerabilities are exploited, also sound like the story line of an espionage thriller; but the threat that ICS/OT vulnerabilities pose can impact just about anyone in our modern world.

ICEFALL, so dubbed by Vedere Labs, refers to "**the name of the second stop on the Everest route, after Base Camp, and given the rising number of OT vulnerability disclosures, we know we have a mountain to climb to secure these devices and protocols**." Specifically, ICEFALL represents 56 distinct vulnerabilities in OT technology by some of the biggest names in the industrial controls industry. Emerson, Honeywell, Motorola are all shown to have critical vulnerabilities in their current industrial control products. **The Feds through CISA have also issued advisories on the same issue discussed herein**.

The harms these vulnerable products can bring about read like any other computer malware we have encountered, but the hackers of ICS/OT act upon a stage far greater than our desktops and smartphones. Where these attacks can have the most negative impacts would be in water treatment plants and small electrical power generating stations, to name two common plants where all regions would have risks. Imagine what happen to your town if the **town's water treatment plant fell victim to any one of these types of attacks common on industrial control system (ICS) installations**. **CSO summarized the findings thusly**:

> "**The products affected by OT:ICEFALL are known to be prevalent in industries that are the backbone of critical infrastructures such as oil and gas, chemical, nuclear, power generation and distribution, manufacturing, water treatment and distribution, mining and building automation.**"

The harmful results on these attacks on control systems is indeed frightening in that we are not talking abut individual computers or private networks. The attacks upon the technology that keeps the wheels of our modern world spinning. Although the attack surface is far greater space in ICS/OT than our PCs, **the fallout from cyberattacks on ICS/OT installations are quite similar to attacks on PCs and smartphones**.

- ✓ **Remote Code Execution (RCE): Allows an attacker to execute arbitrary code on the impacted device**
- ✓ **Denial of service (DoS): Allows an attacker to either take a device completely offline or to prevent access to some function.**
- ✓ **File/firmware/configuration manipulation: Allows an attacker to change important aspects of a device such as files stored within it, the firmware running on it or its specific configurations.**
- ✓ **Compromise of credentials: Allows an attacker to obtain credentials to device functions**
- ✓ **Authentication bypass: Allows an attacker to bypass existing authentication functions and invoke desired functionality on the target device**

The essential problem with securing these critical ICS/OT systems and devices is that the devices were designed and built around a concept now known as "insecure by design." These devices were conceived with the understanding that system changes can be made easily and with little real technological knowledge about the device in question. Another factor in the "insecure by design" designation is many of these devices were designed and manufactured before security was even an afterthought, no more than security concerns were a forethought. Or, as security blogger, Gupta Bless, stated it: "**As the name indicates "insecure design", are those vulnerabilities that exist due to lack of security implementation in an application at the time of development**."

Security firm **Dragos has been monitoring attacks on OT devices**. Their research shows that new hacker groups are entering the fray around ICS/OT, with three new groups and their exploits identified operating in 2021. Dragos year-end 2021 summary of their findings exposed the dangers the exploitation of these vulnerable devices have caused:

> **In 2021, the industrial community attracted high-profile attention. Major cybersecurity incidents struck industrial organizations in a range of sectors, with international headlines detailing everything from a compromise of a water treatment facility with the intent to poison its community to a ransomware attack against a pipeline operator that disrupted gas supplies to the southeastern United States.**

The report went on to declare that "**Ransomware became the number one attack vector in the industrial sector... Dragos assessed that manufacturing accounted for 65% of all ransomware attacks**." Talk about your disruptions of the supply chain!

Exasperating the problems of mitigating against these threats is lackadaisical attitudes about, and just plain ignorance of, these increasingly dire circumstances by plant operators. Dragos made four observations that they derived from engagement with "customers," i.e. plant operators and their employees.

> **✓ 86% of service engagements have a lack of visibility across OT networks —making detections, triage, and response incredibly difficult at scale.**
>
> **✓ 77% of service engagements included a finding about improper network segmentation.**
>
> **✓ 70% of service engagements included a finding of external connections from OEMs, IT networks, or the Internet to the OT network.**
>
> **✓ 44% of service engagements included a finding about shared credentials in OT systems, the most common method of lateral movement & privilege escalation.**

All of these practices violate today's accepted standards of secure computing, and, in fact violate the basic tenets of Zero Trust. It should never be forgotten that the chain wide hacking of Target Stores Point of Sale terminals (cash registers) was initiated when a HVAC vendor — not an employee — logged on to Target's main server from an infected PC in its office to check billing info. **Slate magazine makes the point here** that after 9 years, the compromise of "**Forty million credit and debit cards, 70 million customers' information...We Still Haven't Learned the Major Lesson of the 2013 Target Hack**." Slate authors asks the right question: "**With all this security — an investment of millions of dollars, state-of-the-art security software, hundreds of security personnel, and round-the- clock monitoring—how did Target fail?**" The answer to the question was simple and should have been a wake up call to all American industries. Target's IT security failed because:

> **...the person who let the hackers into Target wasn't even a Target employee and wasn't bent on mischief. The person worked for Fazio Mechanical, a Pennsylvania-based HVAC company, a third-party vendor hired by Target. The Fazio employee fell for a phishing trick and opened an attachment in a fraudulent email the hackers had sent to him. Hidden in the email attachment lurked the Citadel Trojan horse—a malicious software program that took root in Fazio's computers.**

The Target fiasco represents the very definition of a supply chain attack.

The Colonial Pipeline hack in May 2021 should be top of mind when considering ICS/OT attacks. These are the salient facts about "the largest publicly disclosed cyber attack against critical infrastructure in the U.S."

> ✓ **The attack involved multiple stages against Colonial Pipeline IT systems. The pipeline's operational technology systems that actually move oil were not directly compromised during the attack**
>
> ✓ **The attack began when a hacker group identified as DarkSide accessed the Colonial Pipeline network. The attackers stole 100 gigabytes of data within a two-hour window. Following the data theft, the attackers infected the Colonial Pipeline IT network with ransomware that affected many computer systems, including billing and accounting.**

The threat is very real indeed. And we citizens are powerless to do anything about the threat. We can only hope that plant operators read the same material as do engaged readers of The Dispatches From the Front; and that the same operators can at least spell the word "patch."

Here goes P-A-T-C-H.

Sure. Sure you can.

Gerald Reiff

Back to Top

← previous post next post →