Protection for IP Cameras

PFP CYBERSECURITY

Background

Adversaries have weaponized supply chain from chips, boards, devices and many more. IP cameras pose a security concern to any company or consumer who sources their technology from areas where hacking is more common, such as China, Russia, Turkey, and others, as they carry out implant-based attacks that infiltrate any part of the supply chain. The vulnerabilities in the IP cameras allowed for hackers' infiltration and weaponization of DDoS attacks, providing the hacker a large number of entry points to fuel the attack, allowing them to reach an unprecedented size.

"IP CAMERAS POSE A SECURITY CONCERN TO ANY COMPANY OR CONSUMER WHO SOURCES THEIR TECHNOLOGY FROM AREAS WHERE HACKING IS MORE COMMON SUCH AS CHINA, RUSSIA, TURKEY."

Figure 1: US Company sold Chinese cameras as made in USA

Supply Chain Risks The US government has made an unprecedented move on the video surveillance supply chain, charging a US company, Aventura for "having conspired with PRC [China] manufacturers", "by falsely claiming that AVENTURA manufactured its own products" and claiming some to be made in the USA. While Huawei is blocked in U.S., but its chips power security cameras everywhere, this situation won't change until new alternative chips for IP cameras are available. It does not help when US Congress rolls back proposal to restrict use of Chinese chips. Dependence of Chinese manufacturing is broad and won't improve to the level it must be in a short time. An adversary inserts vulnerabilities in hardware or software in order to manipulate those systems at the developer, assembly, or designer's location. Such vulnerabilities can be activated at a later point in time without direct access by the attacker. Most COTS electronics used in DoD systems are fabricated overseas and could be tampered (Figure 2).

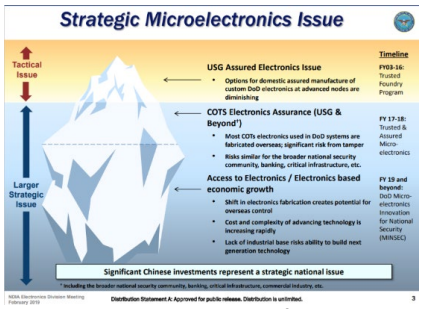

Figure 2: COTS electronics fabricated overseas is a big risk

Operational Risks The vulnerabilities in millions of IP cameras allowed the infamous Mirai internet of things botnet' infiltration and weaponization of DDoS attacks, providing the hacker a large number of entry points to fuel the attack, allowing them to reach an unprecedented size. MIRAI is spiking in growth while changing up its tactics, techniques and procedures since, to target more and more enterprise-level hardware, It's a state of affairs that presents a greater concern than ever before given the ongoing migration to the cloud era, researchers said. Beside being used to launch attacks, IP cameras could also be used to break out of air-gapped networks, by using the infrared (IR) LEDs inside surveillance cameras in buildings for communicating with drive-by adversaries (Figure 4).

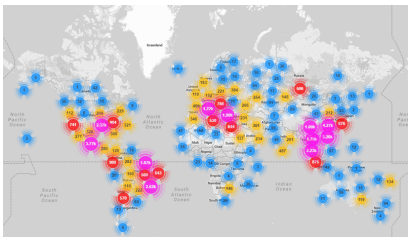

Figure 3: Millions of IP cameras Vulnerable in the Mirai Attacks

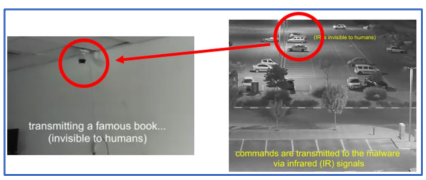

Figure 4 Leakage over air gap using the infra-red LED in the camera

Policies The MITRE CAPEC (Common Attack Pattern Enumeration and Classification) lists supply chain attack as one of the 6 domains of attack, could come from manufacturing, distribution, etc. GSA Subpart 504.70 - Cyber-Supply Chain Risk Management, Effective 2022-4-1, directs agencies to implement supply chain risk management principles to protect against the insertion of counterfeits, tampering, malware, poor manufacturing, etc.

Our-of-Band Monitoring PFP (Power Fingerprinting) enables out-of-band screening and verification of electronics from chips to systems, at scale. All electronic devices generate un-intended emanations which are unique to each device due to variations in manufacturing processes, and specific firmware configuration. PFP uses Machine Learning to create a baseline and detect changes. PFP detects emanation anomalies and can be trained to generate signatures to detect specific attacks to provide protection over the whole life cycle.

Figure 4: Principle of the PFP integrity assessment platform

Trusted Supply Chain and Continuous Monitoring from Chips to Systems

PFP can detect deviations in hardware and firmware from approved configurations, such as counterfeits, cameras with Huawei chips, tampered firmware, presence of MIRAI botnet, Trojans, etc. Since it can detect live attacks in machine time during operation, it could detect and interrupt kill chain. Figure 5 shows a process for supply chain security and continuous monitoring during operation from chips to systems for Commercially-Off-The-Shelf (COTS) information and communications technology (ICT) products. This process can also be applied to many other products such as sensors, networks, cloud infrastructure, etc.

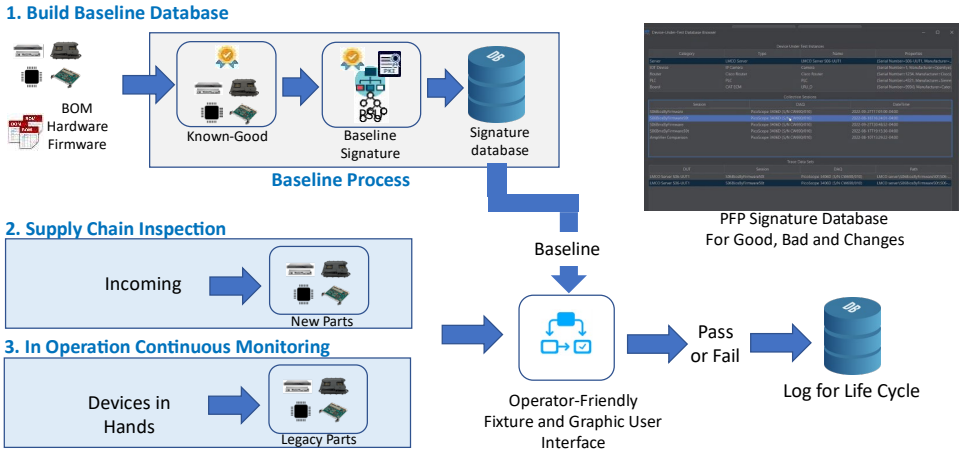

Figure 5. Concept of operation for trusted supply chain

A Run-Time Example Hackers can exploit the vulnerabilities in IP cameras as a gateway into an isolated network, accessing other devices in the network, delivering malware to the programmable logic controller, or PLC, on an isolated network, then erasing their traces on the router and the camera. The event lasts about 3 minutes.

Using PFP, the operators can detect attack on each device when it happens, report and issue alarms in machine time, and can trigger remediation or recovery operation for cyber resilience.

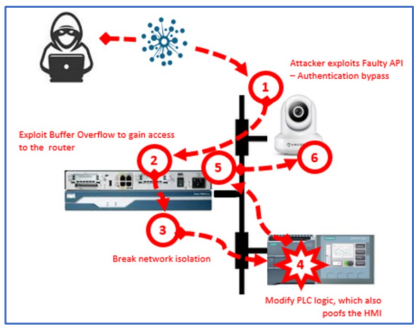

Figure 3: Example enterprise networks with IP camera, network and OT equipment

Contact Information

PFP Cybersecurity (aka Power Fingerprinting Inc)
1577 Spring Hill Rd, Suite 405, Vienna, VA 22182

Steven Chen - schen@pfpcyber.com
https://pfpcyber.com