ICS THREAT FEED

Honeypot feeds

CIM's proprietary honeynet system is the most important source of its collections. Through it CIM provides first-hand information about attacks on both general IT infrastructure and the most common ICS protocols.

Honeypot networks operate on three distinct layers:

1. **Surface layer:** Its purpose is to capture open network scans and botnet attacks. The information obtained is the attacking IP and any payloads (e.g. username, password).

2. **Application layer:** In the case of real, prepared attackers, they find services in the honeynet that emulate real applications (e.g. Apache), the vulnerabilities of which can be exploited by known exploits

3. **Advanced layer:** Emulates live, complex applications that do not have known vulnerabilities. They are only sensitive to very complex attacks or zero-day exploits.

Emulated general protocols:

- ***HTTP / HTTPS:*** TTP information about the attacker is obtained through an emulated web application. If the attacker manages to get through the login interface, the application records all the actions of the actor (so-called Session-logging). The collected data is correlated with the IoC database of already registered vulnerabilities so that the attack method can be identified. If the system does not find a match, it registers it as a possible zero-day attack and submits it to the analyst for further investigation. Less complex attacks are also registered, providing information about possible botnets.
- ***Telnet:*** Simple telnet service with authentication. It primarily provides information about threat actors.
- ***FTP:*** A full-fledged file server to which an attacker can upload documents. After uploading a new file, the system automatically scans it with multiple antivirus programs and subjects it to dynamic analysis in the Cyber Intel Matrix Malware Lab.
- ***SSH:*** A shell with a reduced instruction set that logs commands issued by an attacker. Once collected, the system places it in context based on IoC rules.
- ***SNMP:*** Emulates a corporate network through which the attacker's attack target and methods can be identified.

In addition to general purpose honeypots, CIM also emulates industrial services. They respond as full-fledged devices, so they log all protocol-specific commands.

ICS THREAT FEED

Emulated ICS protocols:

Based on the experience gained during the analysis of industrial controllers, the CIM honeypot system is designed to communicate using ICS protocols on relevant ports. The most commonly used standards have been implemented first:

- **DNP3**
- **Modbus**
- **S7comm**
- **EC 60870-5-104**
- **OPC**

CIM's emulators log all packages that fit the standard, using preconfigured rules to analyze the execution scenarios that could result in a real system. This allows CIM to select (detect) any malicious commands.

Due to the explosive spread of smart homes, CIM has incorporated protocols governing the communication of IoT devices as well. Services include the MQTT protocol implementation in CIM honeynet systems.