RSAConference2019
Asia Pacific & Japan
Singapore | 16–18 July | Marina Bay Sands

BETTER.

SESSION ID: GPS-W01

Using Honeypots to Determine Who Is Targeting SCADA and Control Systems

Andrew Woodward

Executive Dean
School of Science
Edith Cowan University
Perth, Western Australia

RSAConference2019
Asia Pacific & Japan

This is the research of -
Craig Valli, and Glenn Murray

Security Research Institute, Edith Cowan University, Perth,
Western Australia

Critical Infrastructure Protocols

- Commonly referred to as SCADA, although this is only one type of control system, these devices use a variety of protocols to communicate between master and slave, or server and node etc
- The family of ICS / SCADA protocols have increased over the past 40 years to include
  - Modbus
  - DNP3
  - Siemens S7
  - IEC 60870-5-104
- There are also a variety of other protocols used including serial, IP, BACNET
- As technology expanded and the requirement to support remote operations increased, the SCADA protocols were layered on Ethernet and TCP/IP protocol stacks and systems, exposing the SCADA network, with no built-in security, to the Internet and malicious actors within.
- Collectively these systems, networks and protocols controlling critical infrastructure are referred to as operational technology, or OT, as opposed to information technology (IT)

Honeypots

- Are something that bears like? ;)
- No, are a network tool used for gathering intelligence and / or delaying or deceiving an attacker
- The ECUSRI honeypot program has been expanded and deployed primarily to identify malfeasance and malicious behaviours against ICS/OT/SCADA networks.
- Primary motivation to provide a primary means of gathering attack intelligence from various actors who are enumerating and attacking OT systems
- Intel used to investigate the *modus operandi* of various actors and utilise findings to produce automated responses to attacking entities.
- The shared data also informed the community about malfeasant actors within the OT security space.

Materials and Methods

- The primary honeypot used is *conpot*, a low interaction SCADA honeypot.
- Conpots provide emulation of the Modbus protocol, BACnet protocol, IPMI protocol, hypertext transfer protocol (HTTP), Simple Network Management Protocol (SNMP) and the integration of a Programable Logic Controller (PLC) through the S7Comm protocol.
- 12 conpot instances where deployed across 6 Virtual Private Servers (VPS) providers which were geographically dispersed across the globe from the 1st January 2018 to the 30th January 2018.
- The default conpot setup emulates a Siemens SIMATIC S7-200 PLC, plant ID "Mouser Factory" associated to a "Technodrome".
- As this default is easily fingerprinted, the default parameters were changed. To not give away the identity of the conpots these details will not be made available here (sorry!)

Results

Table 1 Conpot Protocol and Associated Open Ports as deployed to collect data for operational technology networks

Protocol	Port
Modbus	TCP 502
Siemens S7	TCP 102
HTTP	TCP 80
IPMI	TCP 623
BACnet	UDP 47808
SNMP	TCP 161

Materials and Methods

- It should be noted that hosts scada001-003 (Honeynet1), scada010-012 (Honeynet2) and scada030-032 (Honeynet3) respectively were each on the same /24 at the same geographic location but all three honeynets were at different locations.
- The host scada020 is not on the same as scada021 and scada022, with these two likewise on the same /24 at same geographical VPS service.
- Taking this into consideration the data analysis will look at patterns detected in network groups Honeynet1(scada001-003), Honeynet2(scada010-12) and Honeynet3(scada030-32).

Results

- In total there were 40163 interactions recorded across the 12 conpot based honeypots.
- There were four identified protocols, namely Bacnet, Modbus, s7comm and http.
- It should be noted that the majority of interactions on http were scanners looking for weakness in http services.
- Most recorded interactions were seeking open interfaces to SQL databases looking for phpMyAdmin or similar style administrative interfaces common to SQL database engines. i.e. these scans were likely not seeking to exploit OT networks, but IT networks
- There were significant variances observed in terms of the protocols and traffic type detected between the hosts.

Results

Table 2 Breakdown by protocol of interactions of all traffic collected by the conpot honeypot network (n = 40163)

	Conpot device number											
Protocol	001	002	003	010	011	012	020	021	022	030	031	032
Bacnet	12	23	21	10	8	3	28	18	10	10	10	9
% of traffic	0.60	0.25	0.22	0.73	0.46	1.60	0.40	0.70	0.29	1.88	0.53	1.42
Modbus	76	6445	6660	957	1075	14	3194	35	1122	30	1347	132
% of traffic	3.79	70.44	68.49	69.70	61.92	7.49	46.19	1.36	32.58	5.62	71.04	20.85
s7comm	242	493	522	198	358	53	490	217	245	129	180	156
% of traffic	12.08	5.39	5.37	14.42	20.62	28.34	7.09	8.45	7.11	24.16	9.49	24.64
http	1666	2182	2513	208	295	117	3203	2297	2067	362	356	336
% of traffic	83.13	23.85	25.84	15.15	16.99	62.57	46.32	89.48	60.02	67.79	18.78	53.08
Total	1996	9143	9716	1373	1736	187	6915	2567	3444	531	1893	633

Results

- **Bacnet**
  - This protocol saw the lowest level of interactions across all the honeypots. The spread across Honeynet1 (56) groupings scada001(12), scada002(23) and scada003(21) was not significant.
  - This protocol demonstrated a homogeneity not seen in the next three protocol groups. The bulk of the interactions were from three scanning service providers at SSP-1 (42), SSP-2 (20) and SSP-3 (7) totalling 69 or 42.6% of all interactions.
- **Modbus**
  - This was the highest interaction level of any observed protocol with 21087 unique events.
- **S7comm**
  - This protocol recorded the second lowest level of interactions in the honeynet with a range of 53 (scada012) through to 522 (scada003).
- **http**
  - scada002 and scada003 received 9143 and 9724 respectively with scada001 at 1666

Results

Table 3 - Top 20 attacking hosts by attack number

	Host	Attacks		Host	Attacks
1	A1	4676	11	A52	616
2	A2	4593	12	A55	604
3	A13	2009	13	A73	315
4	A14	1700	14	A74	315
5	A18	1529	15	A75	315
6	A30	1294	16	A76	315
7	A42	874	17	A77	315
8	A45	838	18	A78	314
9	A47	754	19	A79	313
10	A48	746	20	A80	310

Discussion

- One of the largest by number attacks or intrusion into systems were those of the "scanning" services providers (SSP) community from protagonists such as Shodan, Census and others.
- From identified IPs belonging to these SSP's 8 of the top 20 were such services accounting for 17385 (78.392%) interactions.
- Identifiable ISP based accounts were 2178 (9.821%) and the remainder were UNKNOWN interactions accounting for 2614 (11.787%).
- Further investigation into traffic that is directed at OT centric protocols (eg Bacnet, Modbus and S7comm) found 13001 interactions with 12098 (93.07%) of these being directed at the conpots by cyber security providers (binaryedge.ninja) or security scanning providers (Shodan) the so called "good guys" actively probing and attacking OT infrastructure.

Discussion

- Interrogation ranged from simple singular portscans to identify open ports, through to intense interrogation of the honeypot involving in-depth probing and interrogation of the presented protocol, the fake device or both.
- Furthermore discovery of these machines had potential unforeseen consequences
  - If the SSP identified the honeypot as an OT device then it may increase the level of visitation by cyber criminals
  - the exposure of the honeypot as an actual conpot honeypot to the wider community
- Attacks were classified based on the discrete behaviour type and persistence of the attack, and the magnitude of the interaction (Table 4)

Table 4 Attack matrix describing type of attack and intensity

	Low	Medium	High	Very High	Extreme
DE **Detail Extraction**	Simple low-level scan using a known generic tool	Scan using specialised configuration of a known generic tool	A simple scan using a targeted ICS based exploit tool	A modified scan using a targeted ICS based exploit tool	High intensity scan with custom or “unknown unknown” tool
AM **Attack Magnitude**	A slow considered scan	A standard speed scan i.e. coming down at line speed of a single attacker	A high speed/urgency scan e.g. nmap -T4	An insane scan level e.g. nmap -T5 from single entity	Massed or co-ordinated multipoint attacks
PI **Protocol Interrogation**	Minimal or no interrogation	Focuses on a single function call or extraction of protocol feature single host	Targeting multiple functions/features for extraction single host	Targeting multiple functions/features for extraction multiple hosts	Targeting multiple/full functions/features for extraction multiple hosts
AP **Attack Persistence**	Once off	3-5 revisits over the 30 days	Periodic or episodic scanning or attacks e.g. cron or timed	Daily attacks =< 24	Multiple attacks/probes > 100 per day
AC **Attack Consequence**	Negligible Performance Impact	Some degradation but still able to function	Degrades to level of intermittent faults	Frequent faulting of device impacts production values	Device halted

Discussion

- **Persistent Probing**

- We blocked known attack IPs using a firewall to stop probing from the SSP which should have resulted in a reduction in activity reaching the conpot. It did not.
- It followed that as IPs were blocked, previously unobserved IPs were employed to continue scanning activities for that SSP. Upon investigation these “new” IPs were other servers or services utilised by the originating SSP.
- This practice/behaviour/activity moves beyond scanning of IP addresses and moves to a behaviour that is neither benign nor harmless
- We will not enter into legal debate here, but it has been presented as a problem that our law colleagues are now researching an opinion on. Leaving legal argumentation aside this is a significant escalation beyond harmless scanning.

Persistent probing

- What is not well understood by many IT security professionals is the relative fragilities within OT systems when subjected to loads that easily will exceed the limited computational capabilities of many legacy OT devices, that can have catastrophic outcomes.

- It's just a scan…

- In OT systems a scan from modern laptops with relative high-speed internet connections can cause an OT device to fail completely.
- We say relative high speed as some of the interfaces must down translate to serial speeds sometimes as low as 2400 baud.
- The speed of modern networks does not have the latency expected in older networks which even early Ethernet at 10Mbit per second is now slower than speed of modern broadband
- Large traffic volumes can easily overwhelm the ability of the device to store and process the incoming data, primarily due to the age of the devices, and their corresponding relatively low processing power and memory capacity.

Discussion

- Where is the line and when is it crossed?
- Behaviour ranged from simple scans to sophisticated attempts to penetrate and manipulate an OT device.
- In particular is the use of coil reads on a PLC. A common ModBUS interrogation tool was used and clearly identified. Its purpose is simply to sequentially request reads from 0 through to 255. Some intelligent attackers are using randomisation of reads. However, in the end the outcome is the same - a complete enumeration of the device.
- In addition to this a ModBUS protocol specific probe which is 43/14. This probe under normal operation is meant to facilitate significant enumeration and expression of a device configuration to trusted users on the system.

Discussion

- It is important to remember that ModBUS was designed for *in-situ* access to what was initially closed loop network systems.
- This allows for a comprehensive and sometimes complete enumeration of the device, there is no argument that this is directly used in determining this part of the devices state and we posit intent of the interrogating entity.
- The other protocol being used to communicate with the Conpot was S7Comm or more properly Siemens S7 protocol.
  - This level of interaction again indicates it is well past a simple scan.
  - The type of interactions sent were intended to interrogate the devices at a higher level of detail.

Conclusions

- The research has uncovered sophisticated and expanded probing of systems, meaning that default deployment of a conpot system will see it rapidly identified as a honeypot and is something that should not be done by serious researchers or intelligence gatherers.
- More effort needs to go into device and also protocol emulation to represent a device in a believable industrial configuration or context.
- Dynamic exclusion of known known security scanning service providers hosts also needs to occur. We suggest that a blacklist of SSPs IPs be developed and used by honeynet developers to mask detection and also reduce unnecessary data being collected.
- The project is ongoing and we now have significant datasets of over 6 months that we are starting to analyse.

Apply - Actions

- If you operate control systems:
  - Look at your logs – are you seeing this type of traffic? Is it impacting your network?
  - Consider blocking IP address of known “security” scanners
- Investigate whether a honeypot can add value to your network
  - Intel gathering?
  - Decoy?
  - Detection aid? (As part of a true defence in depth strategy - 3DR)
- Report it
  - Some of this scanning activity can be illegal!
  - Contact relevant agency in your jurisdiction – CERT or law enforcement to seek opinion on reporting this activity if it is impacting you

Thank you