

Detection of a Crypto-Mining Malware Attack at a Water Utility

THE DETECTION PROCESS

The industrial network described herein was attacked by crypto-mining malware belonged to a water utility. As it was used primarily for serving a cloud-based OT analytics system and for remote maintenance, the water utility's network needed to be connected to the internet.

The process of detecting and eliminating malware on the utility's SCADA network started with connecting iSID to the network. iSID is Radiflow's multi-engine platform for monitoring SCADA networks. It includes six engines for detecting known vulnerabilities, topology anomalies and asset management.

On January 21st, 2018, Radiflow's iSID Intrusion Detection System was connected to the network, using a Radiflow Smart-Probe. The Smart-Probe enables deploying iSID at a central location and sending a mirrored network traffic stream through using a secure IP tunnel, through diodes, to iSID.

Later that day, the first events began to come in from iSID's engines:

1. The first event was on anomaly on http, sent to IP address 163.172.251.49, at Jan 21, 2018, 18:48.
2. A day later, more events were detected on new links to external IP addresses, all on port 80. This created a major network topology change, which triggered multiple alerts.
3. Throughout that day, iSID monitored the controller for configuration changes and commands sent. No attempts to change the controller configuration, nor sending commands, were found in this case.

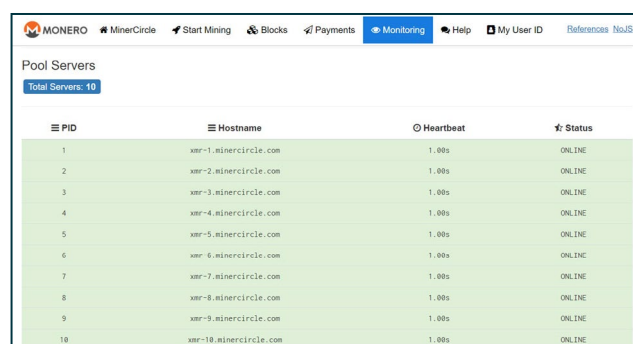
Once the initial events were reported, Radiflow's research team began to further analyze the detailed network information.

Looking up the destination IP address (using Virus Total) did not lead to any malicious site. While (securely) visiting this IP address, we found that it belonged to a "MinerCircle Monero Pool" (<http://xmr-4.minercircle.com>)

A visit to Monero's mining site revealed that there are several other mining pools:

One of the most useful features of iSID, as pertains to this case, is the ability to quickly add new activity signatures and backwards-scan them. We loaded iSID with two signatures:

1. A list of all IP addresses related to miner pools.
2. A proprietary "general" signature developed by Radiflow for miners' payloads. This signature ensures that iSID will detect the miner even if the pools' IP addresses change.



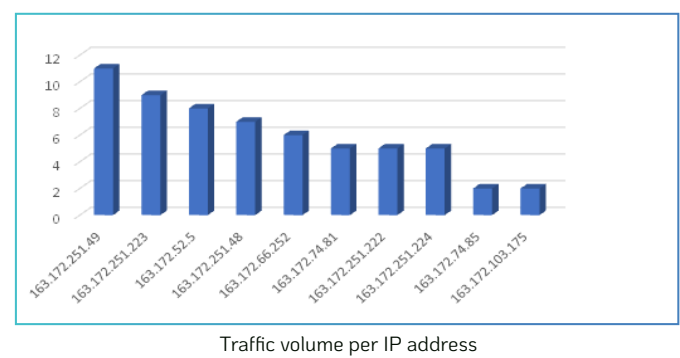
PID	Hostname	Heartbeat	Status
1	xmr-1.minercircle.com	1.00s	ONLINE
2	xmr-2.minercircle.com	1.00s	ONLINE
3	xmr-3.minercircle.com	1.00s	ONLINE
4	xmr-4.minercircle.com	1.00s	ONLINE
5	xmr-5.minercircle.com	1.00s	ONLINE
6	xmr-6.minercircle.com	1.00s	ONLINE
7	xmr-7.minercircle.com	1.00s	ONLINE
8	xmr-8.minercircle.com	1.00s	ONLINE
9	xmr-9.minercircle.com	1.00s	ONLINE
10	xmr-10.minercircle.com	1.00s	ONLINE

One of the most useful features of iSID, as pertains to this case, is the ability to quickly add new activity signatures and backwards-scan them. We loaded iSID with two signatures:

1. A list of all IP addresses related to miner pools.
2. A proprietary "general" signature developed by Radiflow for miners' payloads. This signature ensures that iSID will detect the miner even if the pools' IP addresses change.

Case Study: Detection of a Crypto-Mining Malware Attack at a Water Utility

Based on activity signatures, iSID confirmed several IP addresses related to miners:



Port	Src IP	Dst IP	First Seen
80	IP1	163.172.251.49	Jan 21, 2018 18:48
80	IP1	163.172.52.5	Jan 21, 2018 18:48
80	IP1	163.172.103.175	Jan 22, 2018 1:04
80	IP1	163.172.251.224	Jan 22, 2018 1:04
80	IP2	163.172.52.5	Jan 22, 2018 14:11
80	IP2	163.172.74.81	Jan 22, 2018 14:11
80	IP3	163.172.251.223	Jan 22, 2018 14:41

Samples of communication time and first time seen for each IP address. (source IP addresses were masked to protect the customer information.)

Once detected by Radiflow, the water utility operator was informed about the miner malware and the infected servers.

In the course of devising a recovery scheme for the utility, we deliberated whether it would be possible to update the anti-virus software on the infected servers.

Eventually, the mitigation plan included updating the AV on some servers where it was possible, as well as tightening the firewall configuration. The updated AV detected the CoinMiner malware, as expected.

During the recovery process, iSID continued to monitor the network and collect forensics data, including pcap files and payloads sent during the malicious communications.

EFFECTS ON THE SCADA NETWORK

CoinMiners present several risks to SCADA networks. The mining procedure is extremely CPU-intensive, leaving much less processing power for the operational software. This caused the operational monitoring software to react slowly, akin to using degraded hardware.

About Radiflow

Radiflow develops unique OT cybersecurity tools to protect and ensure organizations' digital resilience. The company closely collaborates with Managed Security Service Providers to oversee the discovery and management of all relevant data security points. Founded in 2009, Radiflow has offices and partners in Europe, USA and APAC. Its field-proven solutions are installed at over 6000 sites around the globe.

Thus, a server infected by a miner malware creates a problematic situation, since SCADA vendors enforce specific hardware requirements for their software, and provide assurances only for those hardware specifications (but not for degraded hardware.)

In this case the hardware platform indeed met the SCADA vendor's hardware requirements; however the miner malware had degraded the actual resources left for the operational SCADA software, increasing the risk for operational faults.

Another effect is the increased amount of traffic sent over the internet. In this case, about 40% of the traffic was classified as related to mining operations – causing overall bandwidth consumption to increase by 60% (!) For limited-bandwidth networks, this poses the risk of creating a bottleneck in the facility's operational data-streams.

CONCLUSION: BEST PRACTICES IN PROTECTING OT AGAINST CRYPTO-MINING (AND OTHER) MALWARE

1. If your system needs to be connected to the internet, it is best to use a well-configured firewall.
2. It is recommended to implement a Defense-in-Depth architecture for monitoring your internal SCADA network using an industrial IDS.
3. Specific to the described detection, the following IDS features were found useful:
 - Network topology anomaly detection
 - Protocol anomaly detection
 - Flexibility to add signatures of malicious activity, and backwards-analysis of the data
 - Forensics capabilities, including mechanisms for monitoring communication patterns and network traffic recording