Detection of a Crypto-Mining Malware Attack at a Water Utility, Using Radiflow's iSID

Synopsis:

Cyber-mining malware enables crypto-currency miners to use some of the processing power of an infected computer for mining cyber-currency. This case study describes the process of detecting and eliminating the malware on SCADA servers operated by a water utility.

The process utilized Radiflow's iSID for analyzing network traffic captured by Radiflow Smart Probes.

Once iSID detected abnormal activity it was able to indicate the port and destination IP address used for the attack, which were used to update the utility's anti-virus and firewall rules and prevent the recurrence of such attacks.

The Detection Process

In the case described in this paper, the network 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.

Continued...

WHY RADIFLOW?

Radiflow is a recognized leader in industrial cybersecurity, offering dedicated solutions designed to meet the unique requirements of industrial infrastructures:

EXPERIENCE

Over 10 years' experience discovering and analyzing advanced persistent threats and targeted attacks, including attacks on critical and industrial infrastructure

UNIQUE METHODOLOGY

Radiflow offers a unique passive monitoring methodology to detect industrial attack vectors that can cause downtime.

EXPERTISE

Dedicated team of industrial cybersecurity experts who understand the colliding worlds of automation and security.

END-TO-END PORTFOLIO

Radiflow offers a holistic portfolio of services and technologies, including secure gateways, Industrial IDS and many more.

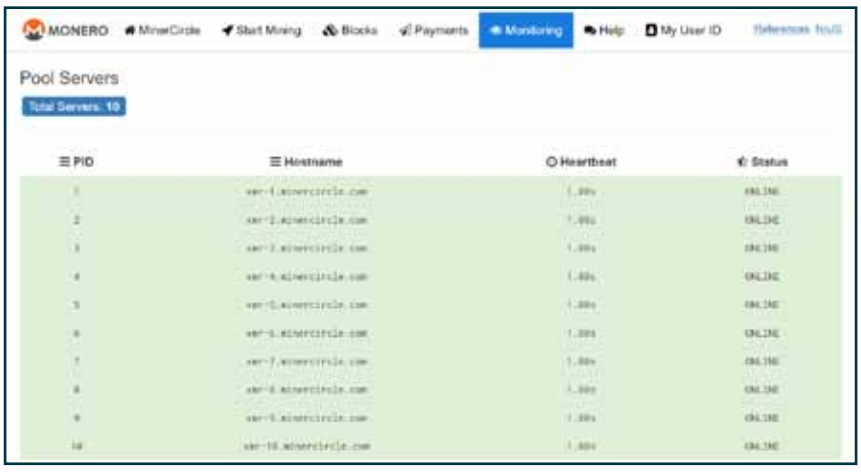
Later that day, the first events began to come in from iSID's engines:

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.

What is crypto-mining, and why are SCADA Servers attacked?

Just like minerals, crypto-currencies need to be "crypto-mined," using resource-intensive software to validate Blockchain (a layered framework for secure, distributed ledgering) transactions. For their efforts, miners are awarded new units of cryptocurrency.

As the price of crypto-currency rose crypto-mining has become more lucrative; however with more people mining virtual currencies, the process of generating hashes, or keys, for Blockchain validation, has become far more complex.

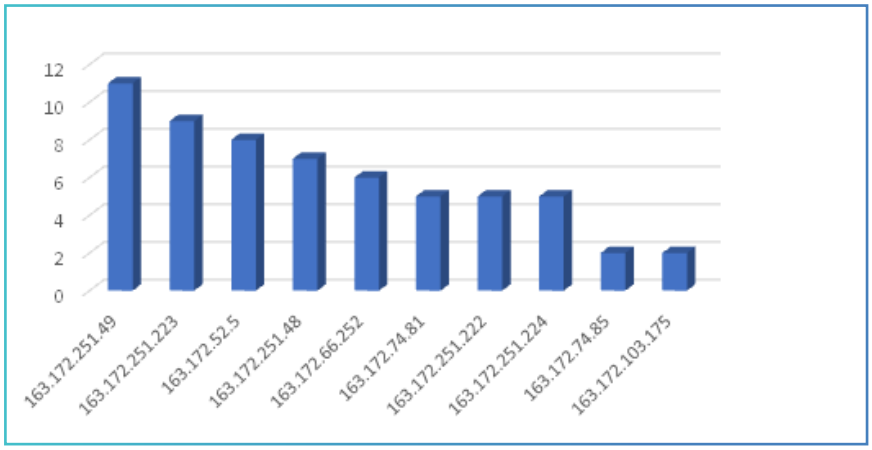
The high gains in crypto-mining created the incentive to use malware that hijacks the processing power of infected computers for mining. It is estimated that over 20% of all enterprises have been affected by crypto-mining malware.

High-powered internet-connected computers, such as SCADA servers, are prime candidates for crypto-mining malware attacks. SCADA servers are typically very powerful; they are accessible remotely by design; and many lack adequate protection, on both the individual server and the network levels.

To make things worse, SCADA servers are typically unmanned, meaning that a crypto-mining malware attack would go unnoticed for a long time.

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

- 163.172.103.175
- 163.172.251.222
- 163.172.251.223
- 163.172.251.224
- 163.172.251.48
- 163.172.251.49
- 163.172.52.5
- 163.172.66.252
- 163.172.74.81
- 163.172.74.85



Traffic volume per IP address

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 about 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.

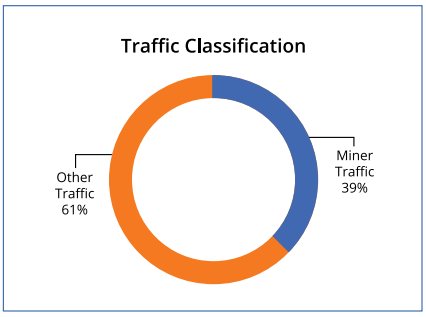
During the recovery process, iSID continued to monitor the network and collect forensics data, including pcap files and payloads sent during the malicious communications.

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.

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 SCADA servers 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 monitoring communication patterns and network traffic recording

Radiflow is a leading provider of cybersecurity solutions for critical infrastructure's ICS/SCADA networks. Radiflow's security toolset validates the behavior of both M2M applications and H2M (Human to Machine) sessions in distributed operational networks. Radiflow's security solutions are available both as in-line gateways for remote sites and as a non-intrusive IDS (Intrusion Detection System) that can be deployed per-site or centrally.

Radiflow's solutions are sold either integrated within a global automation vendor's end-to-end solution, or by local channel partners, as a standalone security solution.

US and Canada:
Tel: +1 (302) 547-6839
sales_NA@radiflow.com

EMEA:
Tel: +972 (77) 501-2702
sales@radiflow.com

UK:
Tel: +44 (0) 800 2461963
sales_UK@radiflow.com

radiflow
Secure Your Assets