Crypto-mining on a DNS server

darktrace.com/en/blog/crypto-mining-on-a-dns-server/

Oakley Cox, Principal ICS Analyst | Tuesday June 22, 2021

The rise of crypto-currencies has fuelled cyber-crime in various ways. Bitcoin has facilitated a range of criminal activities from money laundering to ransomware payments since its release in 2009, leading to a spike in ransomware attacks which has been growing ever since.

More directly, cyber-criminals often hack into company servers and exploit their processing power to mine cryptocurrency, without the organization’s knowledge. This blog will explore a real-life attack where an Internet-facing server was compromised and started mining Monero coins.

Mining cryptocurrency on an Internet-facing server

At a small private company in the APAC region, an Internet-facing DNS server began to receive multiple incoming RDP connections. They all came from rare destinations which had never been seen on the network. Many were sent from external sources with the RDP cookie, ‘hello’, indicating a brute-force attack.

Figure 1: Timeline of the attack

Hours later, the device was seen connecting out to a known endpoint associated with crypto-mining.

As both RDP and SMB ports on the device were open to the Internet, anomalous SMB connections were seen as well shortly following the crypto-mining connections.

Open ports, open sesame

Internet-facing servers are subject to many external threats, especially if sensitive ports are exposed. In this case, the attacker was able to gain a foothold through the DNS server because both the RDP and SMB ports could receive connections. It is important therefore to close communication to all external points which do not strictly need to be open.

Crypto-jacking continues to be a viable way for attackers to expend company resources in order to speed up their mining operations. Especially with the popularity of cryptocurrencies at the moment, we have observed a significant uptick in these types of threat.

The connections to the mining pool were identified by Darktrace’s AI without relying on any known IoCs. Instead, Cyber AI recognized the anomalous nature of the external endpoints, which were statistically rare for the server’s ‘pattern of life’.

If the threat had not been detected, the attacker would have continued to abuse the server resources, resulting in latency issues for important processes. The server could also have been subject to further malicious activity such as DDoS or ransomware.

Figure 2: A similar incident showing an increase in model breaches around the time of compromise on June 8

Protecting a company’s gems

Crypto-mining is notoriously difficult to detect and can go on for months unnoticed. And it can form just one phase of an attacker’s full plan to infiltrate a network — alongside moving laterally and compromising additional devices. Open ports and siloed defenses pave the way for an attacker to break into a system with little resistance.

Organizations need a mechanism for detecting unusual and sinister behavior once the threat is inside. To this end, Darktrace’s evolving understanding of ‘normal’ across users, devices, and peer groups enables it to detect the subtle signs of latent threats. And with Autonomous Response, it responds at machine speed, neutralizing the threat before it has had the chance to spread.

In this case, with Darktrace’s SOC team, the client was immediately made aware of the activity and promptly took the device offline. A Proactive Threat Notification was sent as soon as the attacker had commenced mining. Darktrace analysts then worked through the issue with the customer until the crisis had been resolved.

Darktrace’s AI detects and responds to threats no matter where they come from – RDP account compromise, misconfigured Internet-facing server, or sophisticated Hafnium-style zero day. Furthermore, it provides much-needed visibility over the enterprise, identifying and highlighting Internet-facing devices and any issues they may pose.

Thanks to Darktrace analyst Taylor Breland for his insights on the above threat find.

Learn more about illegal crypto-mining

IoCs:

IoC	Comment
185.202.1[.]123 80.82.77[.]85 95.217.62[.]100 213.152.161[.]234	Anomalous RDP connections from externally rare endpoints
71.66.5[.]150 210.86.230[.]202 188.113.154[.]189 201.22.59[.]203 180.232.127[.]166	Anomalous SMB connections from external rare endpoints
139.99.125[.]38 Pool-hk.supportxmr.com	Monero mining endpoints

Darktrace model detections:

- Device / Anomalous RDP Followed By Multiple Model Breaches
- Compromise / Monero Mining
- Compromise / High Priority Crypto Currency Mining *(Enhanced Model Breach/PTN)*
- Device / Anomalous SMB Followed By Multiple Model Breaches
- Compliance / Crypto Currency Mining Activity
- Anomalous Server Activity / Anomalous External Activity from Critical Network Device
- Compliance / Incoming Remote Desktop
- Compliance / Internet Facing RDP Server

MITRE ATT&CK techniques observed:

Initial Access	T1133 – External Remote Services T1078 – Valid Accounts
Persistence	T1133 – External Remote Services
Impact	T1496 – Resource Hijacking

Oakley Cox

Oakley Cox is Analyst Technical Director for the Asia-Pacific region, and oversees the defense of critical infrastructure and industrial control systems, helping to ensure that Darktrace’s AI stays one step ahead of attackers. Oakley is GIAC certified in Response and Industrial Defense (GRID), and helps customers integrate Darktrace with both existing and new SOC and Incident Response teams. He also has a Doctorate (PhD) from the University of Oxford.