Crypto-Jacking

Key Benefits

- ✔ Learns the unique 'patterns of life' for each device and user in an organization
- ✔ Analyzes a wide range of metrics to detect anomalous behavior without reliance on static rules or signatures
- ✔ Responds autonomously to threats, stopping illegal activity in seconds

137.9 TWh
consumed by Bitcoin per year.
University of Cambridge

Threat Landscape: Crypto-Jacking

Crypto-jacking is unique among cyber-threats in that it targets processing power rather than aiming to steal or undermine private data. Although files may not be at risk, crypto-jacking drains resources and can cause serious reputational and financial harm. Aside from slower systems and sky-high energy bills, it is very difficult for security teams to know if an environment is being used for illegal crypto-mining. Attackers can thus spend months, even years, using a company's processing unit without being detected.

Blockchain Basics

Since bitcoin was launched in 2009 by Satoshi Nakamoto, cryptocurrencies have surged in number and value. Cryptocurrency is created when a computer manages to complete a specific mathematical problem, namely finding a 64-digit 'cryptographic hash'. This creates a new 'block' which verifies the transaction, and in return for this, miners are rewarded with digital coins. This process, known as crypto-mining, requires a vast amount of computational power.

The Rise of Illegal Crypto-Mining

Cyber-criminals have profited from the increasing popularity of cryptocurrency by exploiting the CPUs of target companies. Hackers can break into vast company systems and consume their processing power for crypto-mining. In this way, companies suffer all the operational costs while the hackers enjoy sole access to the final monetary harvest.

While not as lucrative in the short-term as other methods, for instance deploying ransomware, crypto-jacking is far less risky and can be more profitable in the long run. Attackers frequently rely on anonymous alternative cryptocurrencies, such as Ethereum and Monero, predicting that they'll be able to spend months inside a system before detection.

Worryingly, threat actors often target critical infrastructure companies because their systems tend to use large amounts of computing power. Harnessing the combined power of IoT devices can prove fruitful, as can 'high-powered mining' attacks aimed at companies which store their data in the cloud. The exponential rise of cloud and IoT adoption brought about by the onset of the pandemic has made organizations worldwide more vulnerable to this type of attack.

How Cyber-Criminals Install Crypto-Mining Malware

Besides hijacking cloud services, by brute-forcing user credentials or through misconfigurations, cyber-criminals can use two main attack vectors to infect a system with crypto-mining malware:

- A victim unwittingly downloads an executable code which spreads crypto-mining script. This happens in several ways, most commonly by clicking on a malicious link or opening an attachment in a phishing email.
- A victim visits a website or clicks on an advertisement which contains malicious JavaScript code. The code script then executes automatically on the browser and begins mining for cryptocurrency in the background.

The crypto-mining script itself can be bought on the Dark Web for less than 50 US dollars. Once installed, it is extremely difficult for legacy security tools to identify. In such attacks, the computer system will often be pushed to maximum capacity, which makes it impractical to troubleshoot devices and inspect the network.

> "Crypto-mining malware has the ability to hamper and even crash an organization's digital environment, if unstopped."
>
> Justin Fier, Director of Cyber Intelligence & Analytics, Darktrace

year-on-year increase in crypto-jacking in March 2020.

ENISA

The Crypto-Jacking Process

Darktrace Immune System: Autonomous Cyber Defense

How Self-Learning AI Disrupts Illegal Crypto-Mining

Darktrace is uniquely placed to detect and defend against crypto-jacking attacks. Cyber AI learns 'normal' for each organization and does not rely on signatures or lists, meaning it can detect never-before-seen threats in their earliest stages.

Modeled on the human immune system, Darktrace's Enterprise Immune System learns the digital DNA of an organization, understanding 'self' in order to identify anomalous behavior and respond to the full range of cyber-threats. With Antigena, Darktrace's Autonomous Response capability, the AI actions a targeted response in seconds, stopping crypto-jacking attempts before mining software is installed.

Crypto-jacking is notoriously difficult to detect because it runs quietly in the background, making very little noise across the digital ecosystem. It is ineffectual to create rules as the messages are short and easily blend in with legitimate communication. As a result, detecting subtle anomalies like beaconing activity and anomalous energy consumption are crucial in discovering a crypto-mining campaign.

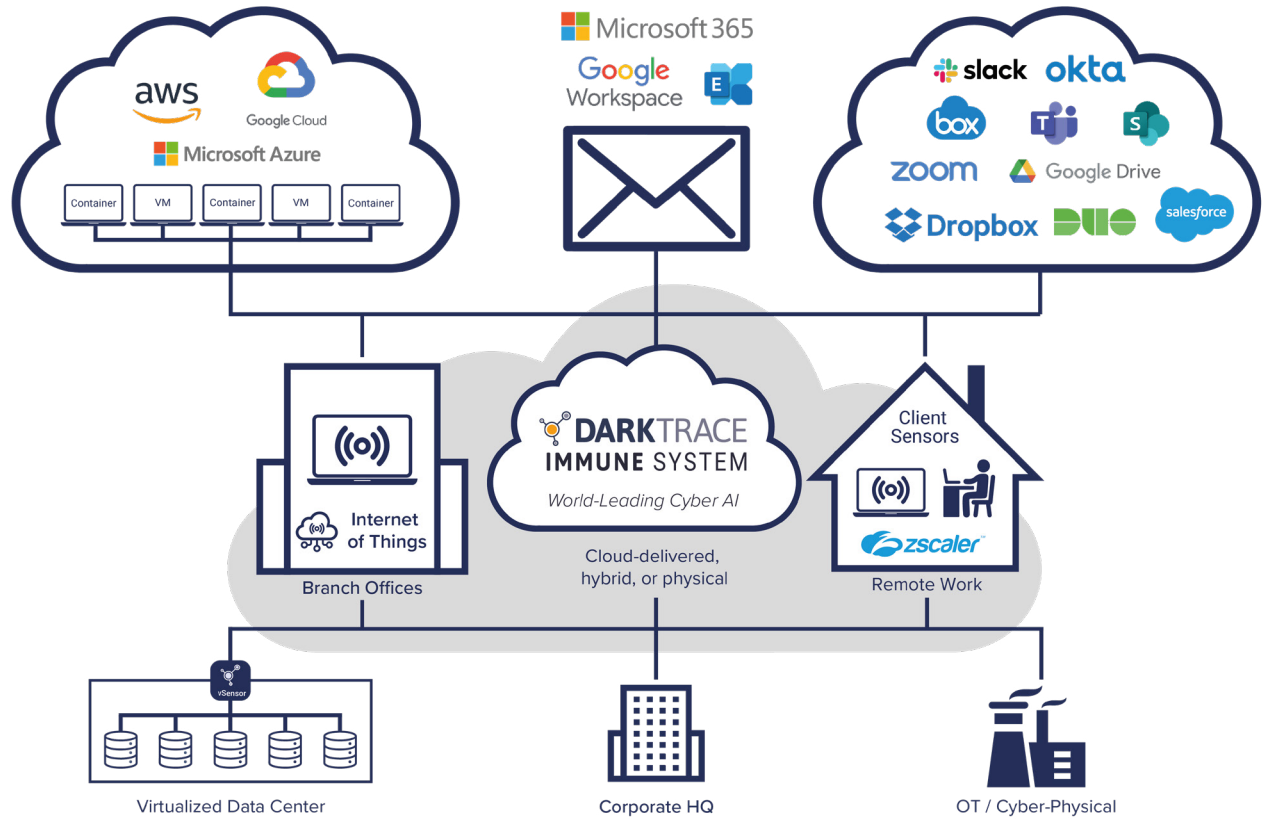

Figure 1: Darktrace's AI offers an enterprise-wide solution to cyber defense

A Forward-Looking Approach

Malicious actors often rely on encrypted connections to hide command and control (C2) communication and crypto-mining. Darktrace Cyber AI uses JA3 analysis and JA3 rarity which provides an extra layer of information on encrypted connections, helping to detect encrypted C2 beaconing among the noise of other encrypted traffic. Darktrace's rarity scores means it can detect TLS by identifying unusual domains, rather than relying solely on exactly what content is being sent to and from those domains.

Many signature-based security tools tend to look for an individual indicator of 'bad', a single Indicator of Compromise (IoC), whether it be information in an endpoint TLS certificate or a known malicious IP. However, Darktrace detects crypto-mining by identifying anomalous behavior across the digital ecosystem, taking into account a range of different metrics such as rare endpoints, self-signed TLS certificates, and anomalous connectivity.

By analyzing the metadata around a connection and developing an understanding of what 'normal' looks like, Cyber AI can detect unusual device behavior and thus intercept crypto-jacking in its earliest stages, distinguishing it from companies which use their own servers to mine cryptocurrency.

Darktrace analyzes close to 300 protocols with Deep Packet Inspection, monitoring all traffic rather than just sampling it. This allows the AI to identify every type of crypto-mining protocol, including Minergate. As cryptocurrency works peer to peer, criminals can't come out with a new protocol, making it easy for Cyber AI to detect these unique patterns.

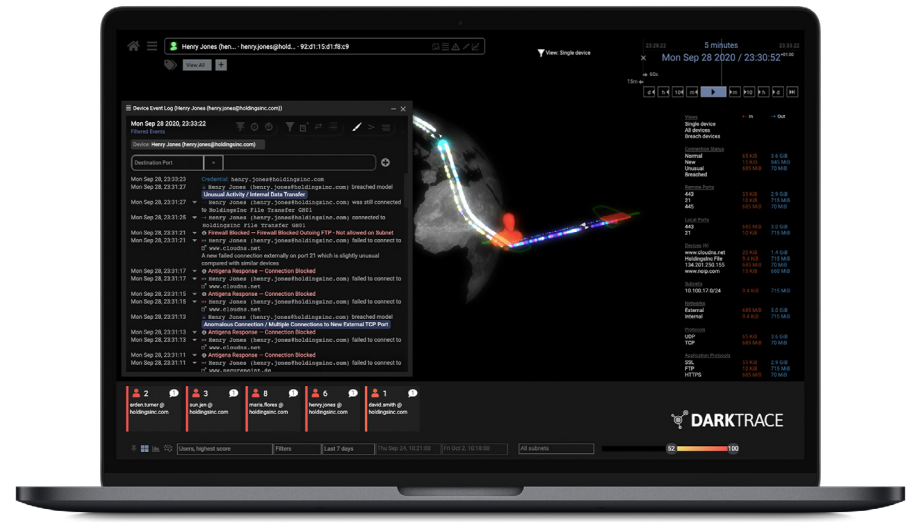

Figure 2: Across the world, Darktrace Antigena autonomously stops a cyber-attack every second

"The 24/7 visibility Darktrace has provided us with is invaluable and has transformed our understanding of our systems and the activity within."

Mark Harris, Head of Information Technology, Pool Re

Threat Finds: Illegal Crypto-Mining in Action

Crypto-Mining Campaign on a Biometric Scanner in an Empty Office

Darktrace detected a crypto-mining campaign occurring at a manufacturing firm while their physical office was closed due to COVID-19 restrictions. Hackers had compromised a corporate server which controlled the company's biometric door access and were intending to use its processing power to mine for cryptocurrency.

Darktrace first detected anomalous behavior when the server downloaded a suspicious executable file, Securitcy.111, from a new external IP that had never been seen on the system. Following this file download, the server began to repeatedly connect to external endpoints using self-signed TLS certificates.

Despite a lack of threat intelligence on the external source of the file download, the crypto-mining connections were immediately identified by Darktrace as suspicious due to their use of self-signed TLS certificates, alongside the statistical rarity of the endpoints for the business.

In addition, the new user agent was generic, commonly associated with legitimate and malicious processes alike. This use of user agents means that C2 communication is less likely to be detected by the traditional security stack; however, its unusual use was immediately flagged and investigated by Cyber AI.

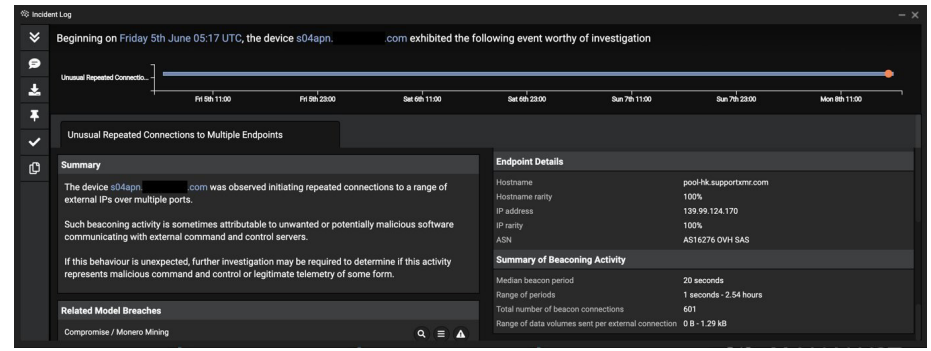

Figure 3: Darktrace's Cyber AI Analyst investigates and reports on cyber-threats, reducing time to triage by 92%

"The AI alerts us to threats we would never have known about. For us, deploying Darktrace wasn't an option; it was a necessity in staying ahead of today's advanced and unpredictable threats."

Paul Haugan, Director of Innovation and Technology, City of Auburn

Bitcoin Mining Campaign Leverages Citrix Netscaler Vulnerabilities

Darktrace detected at least 80 different customers all being targeted by the same CVE-2019-19781 vulnerability — affecting the Citrix ADC (Citrix Application Delivery Controller) and Citrix Gateway solution for public cloud.

1. Darktrace's detection capabilities highlighted the steps taken by exploited Citrix Netscaler devices executing shell commands.
2. These devices began by receiving HTTP POST requests to URIs that are vulnerable to directory traversal attacks, for example /vpn/.../vpns/cfg/smb.conf.
3. These POST requests were followed by high confidence alerts created by Darktrace. The alerts were very similar, regardless of the target, as the attack behavior was the same.
4. Code execution was triggered, leading to the download of shell scripts and other malware with the end goal of running crypto-mining malware.

In one example, compromised devices were observed downloading an executable file from Ukraine (http://217.12.221[.]12/netscalerd) containing an ELF:BitCoinMiner Malware. This triggered crypto-mining and C2 beaconing alerts.

Darktrace Antigena responded immediately, eliminating the incoming threat by blocking miner file downloads and activity for a day, while still allowing regular business activity to continue. This offered the customer ample time to react to the anomalous activity while Darktrace halted the malware's spread to other devices.

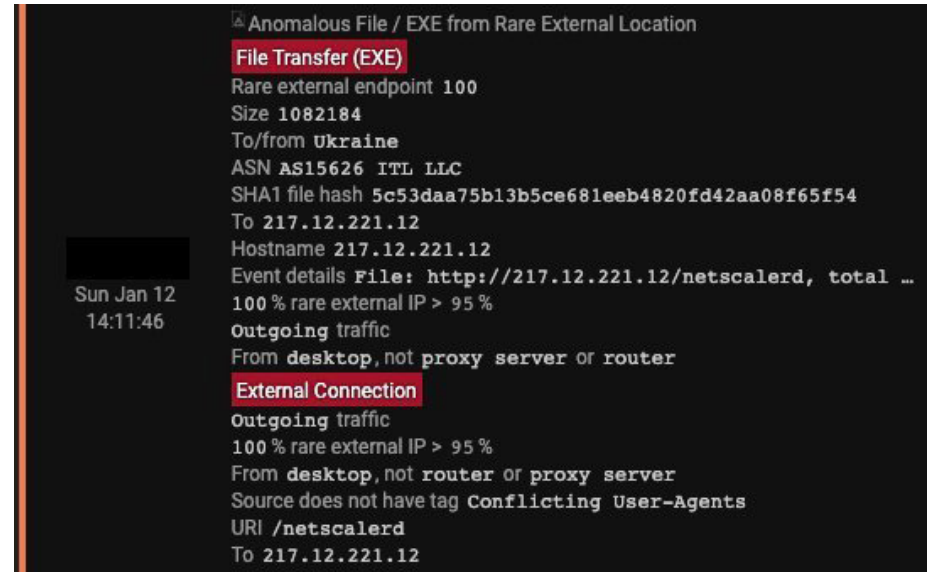

Figure 4: The Anomalous File / EXE from Rare External Location alert triggered by C2 traffic

> "By leveraging Cyber AI, the Bitcoin malware using the Citrix vulnerabilities was instantly contained – before any damage could be done to the customer."
>
> Max Heinemeyer, Director of Threat Hunting, Darktrace

Uncovering a Cryptocurrency Farm in a Warehouse

Last year, Darktrace detected anomalous crypto-mining activity within an organization's digital infrastructure. Upon investigation, Darktrace traced the anomalous activity to one of the company's warehouses, where they found what appeared to be unassuming cardboard boxes sitting on a shelf. Opening these boxes revealed a cryptocurrency 'farm' in disguise, running off the company's computing power.

Had Darktrace Antigena been active, any anomalous crypto-mining devices would have been blocked from communicating with the relevant external endpoints, effectively inhibiting mining activity. Antigena can also respond by enforcing the normal 'pattern of life' for the user, device, or environment in question, preventing malicious behavior while allowing normal business activities to continue.

Figure 5: The unassuming cardboard boxes

Figure 6: The cryptocurrency farm

Crypto-Miner Infections on Unpatched Salt Servers

Darktrace detected that a number of customer servers running SaltStack were making external connections to endpoints previously not seen operational within those corporate environments. The connections used the curl or wget utilities to download and execute a hash script, which would install a secondary-stage payload containing a cryptocurrency miner.

The systems were targeted directly utilizing 2020-11651 and CVE-2020-11652 vulnerabilities in the ZeroMQ protocol running on SaltStack. These vulnerabilities allowed direct remote code execution as root on the targeted systems. The downloader script cleaned the target system of pre-existing infections and disabled the known security software, before it iterated through three functions to download the crypto-miner payload.

Following a series of cryptographic checks, the downloaded ELF LSB executable kicked into action, and a plaintext HTTP C2 channel was established, sending basic metadata about the infected host, such as processor architecture, available resources, and whether root execution was achieved. Lastly, the devices began mining for cryptocurrency.

The complete attack lifecycle was investigated and reported on by Darktrace's Cyber AI Analyst, which automatically surfaced some crucial details regarding the C2 communication, including other servers that were seen making similar communication patterns.

```
setenforce 0
echo SELINUX=disabled >/etc/selinux/config
service apparmor stop
systemctl disable apparmor
service aliyun.service stop
systemctl disable aliyun.service
ps aux | grep -v grep | grep 'aegis' | awk '{print $2}' | xargs -I % kill -9 %
ps aux | grep -v grep | grep 'Yun' | awk '{print $2}' | xargs -I % kill -9 %
rm -rf /usr/local/aegis
```

Figure 7: The downloader script

Crypto-Mining in the Healthcare Industry

During a trial with a private medical institution, Darktrace immediately discovered that an AXIOS spectrometer, a medical IoT device for characterizing materials using X-rays, had been compromised. It had breached hundreds of models, many of a potentially serious nature. The device was continuously making outbound SSH connections to rare external IP addresses, transferring over 1 GB of data a week.

Further analysis determined that the compromised medical device was being used to send large volumes of outbound spam mail, resulting in the medical institution's external IP address being blocked by spam filters. Effectively classified as a sender of junk mail, emails from the medical institution risked falling into recipients' trash or not being received at all – anything from appointment updates to the results of cancer scans.

On further investigation, at least one of the HTTP connections was to a server utilized within cryptocurrency exchange and bitcoin activity, which suggested the presence of crypto-mining malware. As soon as Darktrace detected the activity, the institution's security team were alerted and the device was isolated, giving the team precious time to conduct further investigation.

Figure 8: Every device is a potential security risk, even a spectrometer

About Darktrace

Darktrace is a leading autonomous cyber security AI company and the creator of Autonomous Response technology. Its self-learning AI is modeled on the human immune system and used by over 4,700 organizations to protect against threats to the cloud, email, SaaS, traditional networks, IoT devices, endpoints, and industrial systems.

The company has over 1,500 employees and is headquartered in Cambridge, UK. Every second, Darktrace AI fights back against a cyber-threat, before it can cause damage.

For More Information

- Visit darktrace.com
- Book a free trial
- Visit our YouTube channel
- Follow us on Twitter
- Follow us on LinkedIn