East Midlands Special Operations Unit

COVID-19 CYBER AND FRAUD PROTECT MESSAGES

Thursday 09 July 2020

This advice has been collated by EMSOU and is intended for wider distribution within the East Midlands Region to raise awareness among businesses and the public.

Advice and information is changing daily as we navigate our way through the COVID-19 pandemic, so please ensure you only take information from reputable sources.

If you require any further information, assistance or guidance please contact the

EMSOU Protect Team EMSOU Protect Team **or your local Force protect team.**

Today's topic is: Cryptocurrency and Cryptojacking

Cryptocurrency is digital money that can be used to pay for goods and services. Bitcoin, Monero and Ethereum are examples of cryptocurrencies, but there are many others.

Unlike other legal tender, cryptocurrency is not controlled by the banks. Instead it uses complex mathematical algorithms (encryption and blockchain technology) to verify and secure every transaction made. Each transaction is recorded across multiple servers so that multiple records are synchronised and maintained to protect the integrity of each cryptocurrency account.

Cryptomining:

It is possible to earn cryptocurrency by downloading software that solves the complex mathematical problems that validate other people's transactions. Every solved equation earns a small reward, paid out in cryptocurrency.

Solving these mathematical calculations requires a massive amount of processing power and will exhaust the resources of most computers that attempt them. Instead, a malicious actor will steal the processing power of other people's systems by covertly installing the cryptomining software and syphoning off any earnings. This is known as **cryptojacking.**

Adversaries will also distribute the malware through weaponized mobile apps; infecting vulnerable websites and hijacking Wi-Fi hotspots.

What systems and devices are at risk from cryptojacking:

Any connected device with a processor is susceptible. Common targets include:

- Cloud vendors
- Mobile devices
- Networked computers
- IoT devices such as printers, smart TVs and gaming consoles.

East Midlands Special Operations Unit

Symptoms of a cryptojacking attack:

- Degraded system and network performance because bandwidth and processing resources are being monopolised.
- Increased power consumption, system crashes, and physical damage from component failure due – usually due the extreme temperatures this type of processing necessitates.
- Financial loss due to system downtime, increased power consumption as well as sanitization and recovery efforts.

How to protect against cryptojacking:

- **Maintain antivirus software:** Detects and removes unwanted programs.
- **Keep software and operating systems up to date**: So known vulnerabilities cannot be exploited.
- **Use strong passwords:** Change default passwords to prevent unauthorised access.
- **Check system privileges:** Only administrative accounts should be able to make system changes.
- **Apply application whitelisting**: Prevent unknown executables from launching and remove unused software, to reduce the attack surface of a system.
- **Download files using only trusted sites:** Check site reviews where possible.
- **Benchmark CPU, running services and other system resources:** So abnormal loads and processes can be quickly detected.
- **Validate input**: On internet-facing web servers and web applications to mitigate injection attacks. On web browsers, disable JavaScript execution.
- **Install a firewall**. Which will monitor for malicious inbound traffic and unnecessary outbound traffic. Configure firewalls using vendor guidance and industry best practice.
- **Create and monitor blacklists**: Using threat intelligence to identify websites that distribute malware or are leveraged for command and control. Block these sites using the IP address and prevent devices from being able to access them.

Reporting

Please report all Fraud and Cybercrime to Action Fraud by calling 0300 123 2040 or online.

Forward suspicious emails to report@phishing.gov.uk.

Report SMS scams by forwarding the original message to 7726 (spells SPAM on the keypad).