# Understanding of Crypto-jacking Attacks

## **Introduction:** Explanation of cryptojacking and its relevance

In the evolving landscape of cyber threats, cryptojacking emerges as a silent yet pervasive hazard. Cryptojacking is a clandestine form of cybercrime where hackers exploit an individual's or organization's computing power to mine cryptocurrency without consent. Unlike other forms of cyber attacks, which overtly seek to steal data or disrupt systems, cryptojacking quietly leeches resources, often going unnoticed by the untrained eye. As cryptocurrencies continue to gain value and prominence, the incentive for cybercriminals to engage in crypto-jacking has surged, making understanding and awareness of this cyber threat more relevant than ever

## **Identification:** Key indicators that a system may have been compromised

Recognizing the signs of a system compromise is essential for timely and effective response. Here are the key indicators that may suggest a system has been breached:

**Unusual System Performance**

- Slower than normal operation or frequent crashes.
- Unexplained lack of storage space or sudden spikes in network traffic.
- Overheating of devices due to overutilization of processing power.

**File Anomalies**

- Unfamiliar files or software appear on the system.
- Modified file timestamps that do not correlate with known updates or changes.
- Files that suddenly encrypt or become inaccessible without explanation.

**Account Irregularities**

- Unexpected user account lockouts.
- New, unknown user accounts appear on the system.
- Unauthorized changes in user permissions or access levels.

**Security Software Tampering**

- Antivirus software or firewalls are disabled without user action.
- Security logs that show unauthorized access attempts or are inexplicably cleared.
- Alerts from security software about blocked intrusion attempts.

**Suspicious Network Activities**

- Detection of traffic to and from unknown or risky IP addresses.
- Unrecognized active connections in the network resource list.
- Unexpectedly high data usage that could indicate data exfiltration or command and control communication.

**Program and System Anomalies**

- Programs starting, closing, or operating without any user input.
- Tasks running in the background that are not initiated by the user or system updates.

**Unexplained User Account Activities**

- New user accounts showing up without having been created by authorized personnel.
- Unauthorized access attempts to existing accounts or multiple failed login attempts.

**Storage and Resource Discrepancies**

- A sudden lack of available storage space, which could indicate the presence of large, unauthorized files or software.
- Unexplained network traffic or unusual outbound communication, suggesting data exfiltration

Prompt recognition of these indicators can be the difference between a contained incident and a widespread cybersecurity breach. Regular monitoring and immediate investigation of these signs are vital for maintaining system integrity and security.

# **Immediate Actions:** Step-by-step first response actions once crypto-jacking is detected

When cryptojacking is suspected or detected, immediate action is required to mitigate the threat. Follow these steps to respond effectively:

**Isolate the Affected Systems**

- Disconnect the compromised device from the network to prevent further spread.
- If possible, isolate the affected segment of the network while maintaining minimal operational impact.

**Initiate a Security Scan**

- Perform a thorough scan using updated antivirus and anti-malware software to identify and remove the cryptojacking malware.
- Use specialized cryptojacking detection tools if available.

**Change Access Credentials**

- Immediately change passwords for all user accounts, especially those with administrative privileges.
- Update credentials for any affected service or application.

**Update and Patch Systems**

- Ensure that all systems are updated with the latest security patches to close any vulnerabilities exploited by the attackers.
- Upgrade security software and install patches provided by vendors in response to the crypto-jacking threat.

**Monitor for Anomalies**

- Keep a close watch on system performance and network traffic for further anomalies that could indicate additional issues.
- Set up system alerts for unusual activity that could suggest a reinfection or secondary attack vector.

**Report the Incident**

- Inform your organization's IT or cybersecurity team immediately.
- Report the incident to relevant authorities, such as national cybercrime units or industry-specific regulatory bodies, if applicable.

**Review and Strengthen Security Measures**

- Conduct a security review to identify how the breach occurred and to prevent similar incidents.
- Implement stricter security policies and consider using cloud-based security solutions for enhanced monitoring and protection.

**Educate and Inform Staff**

- Provide information to all staff members about the incident and educate them on how to recognize and prevent cryptojacking.
- Reinforce the importance of not clicking on suspicious links and reporting any unusual computer performance issues.

**Document Everything**

- Keep a detailed record of the incident, actions taken, and any findings during the investigation.
- Documentation can aid in future prevention efforts and may be required for compliance with data protection regulations.

**Seek Professional Help if Needed**

- If the scope of the attack is beyond the internal capabilities, consider hiring external cybersecurity experts.
- Professional cybersecurity services can provide deeper insights and more sophisticated countermeasures against cryptojacking.

Prompt and decisive action is key to mitigating the damage caused by cryptojacking and preventing its recurrence. Regularly updating and following a cybersecurity incident response plan will help to ensure preparedness for such threats.

**This project was funded by the European Union's Internal Security Fund - Police Programme under Grant Agreement No 101038738**