**Group Name:** CUBARANSOMWARE ([Attack Graph Response to US-CERT Alert (AA22-335A): #StopRansomware: Cuba Ransomware - AttackIQ](https://www.attackiq.com/2022/12/03/attack-graph-response-to-us-cert-alert-aa22-335a-stopransomware-cuba-ransomware/))

Associated Groups: NORTHKOREANHACKERS Description: CUBARANSOMWARE is a North Korea-based threat group that has been active since at least 2020. The group focuses on targeting the healthcare and financial sectors. ([North Korea Cyber Threat Overview and Advisories | CISA](https://www.cisa.gov/topics/cyber-threats-and-advisories/advanced-persistent-threats/north-korea) **techniques used**

**RomCom: A custom-made ransomware tool used by the group to encrypt files and demand ransom..**

**Phishing: The group uses phishing emails with malicious attachments or links to gain initial access.**

**Exploit Public-Facing Application: The group exploits vulnerabilities in public-facing applications to gain initial access.**

**Living Off the Land: The group uses legitimate system tools to evade detection.**

**RDP: The group uses Remote Desktop Protocol (RDP) to move laterally within the network.**

**Group Association:**CUBARANSOM has been used by CUBARANSOMWARE.

**Tools and software used:**

**Cobalt Strike**: A commercial penetration testing tool used for post-exploitation and lateral movement.

**Empire**: An open-source post-exploitation framework used for lateral movement and privilege escalation.

**Mimikatz**: A tool used for credential harvesting and password extraction.

**PsExec**: A tool used for executing processes on remote systems.

**WinRAR**: A compression tool used to archive and encrypt stolen data.

***Targeted Sectors:****Financial Services, Government Facilities, Healthcare and Public Health, Critical Manufacturing, and Information Technology* [*https://www.attackiq.com/2022/12/03/attack-graph-response-to-us-cert-alert-aa22-335a-stopransomware-cuba-ransomware/*](https://www.attackiq.com/2022/12/03/attack-graph-response-to-us-cert-alert-aa22-335a-stopransomware-cuba-ransomware/)

**Description:** CUBARANSOM is custom ransomware used by CUBARANSOMWARE to encrypt files and demand ransom.

**Platform**: Windows Techniques

• **Data Encrypted for Impact (T1486)**– CUBARANSOM has encrypted files on compromised systems, demanding ransom in exchange for the decryption key.

• Command and Scripting Interpreter: Windows Command Shell (T1059.003) – CUBARANSOM has used the Windows Command Shell to execute malicious commands. [Cuba, Software S0625 | MITRE ATT&CK®](https://attack.mitre.org/software/S0625/)