Severity

High

Analysis Summary

In August 2021, Quantum Ransomware was identified for the first time. One of the first access vectors used by the threat actors is the IcedID virus, which uses Cobalt Strike for remote access and leads to data theft and encryption using Quantum Locker. Using phishing emails with an ISO file attached, IcedID gained initial access to the target's PC. To get beyond email security restrictions, IcedID and ISO archive are a fantastic combination. Cobalt Strike was injected two hours after the infection had begun. Threat actors eventually employed WMI and PsExec to encrypt machines and deploy the Quantum ransomware payload. The attack was completed in less than four hours, which is extremely impressive.

Impact

- Unauthorized Access
- Data Exfiltration
- File Encryption

Indicators Of Compromise

MD5

- 2cbb3497bfa28d9966c1feeae96d452d

SHA-256

- 85c3b718090144dadeb8035ac287d46b9d3458f9de409229217d42a475f42868

SHA-1

- 9ef94c7d3fedc71bb3ed1abf542dfc7ec692883d

Remediation

- Block all threat indicators at your respective controls.
- Search for IOCs in your environment.