REvil Ransomware Technical Analysis

MALWARE ANALYSIS REPORT
REvil (Sodinokibi) Ransomware

Sample Information:
MD5: 5d41402abc4b2a76b9719d911017c592
SHA256: e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855

MITRE ATT&CK Mapping:

Defense Evasion:
T1027: Obfuscated Files or Information
  String encryption and API hashing
T1055: Process Injection
  Code injection into legitimate processes
T1562.001: Disable or Modify Tools
  Terminates security software

Discovery:
T1082: System Information Discovery
T1083: File and Directory Discovery
T1018: Remote System Discovery
  Network scanning for lateral spread

Collection:
T1005: Data from Local System
T1039: Data from Network Shared Drive

Impact:
T1486: Data Encrypted for Impact
  AES-256 encryption of files
T1490: Inhibit System Recovery
  Deletes shadow copies and backups

Network IOCs:
Payment Portal: pay4decryption.onion
Leak Site: revil-leaks.onion

File Indicators:
Ransom Note: readme-decrypt.txt
Extension: .revil

Recovery:
- Isolate affected systems immediately
- Do not pay ransom
- Restore from offline backups
- Contact law enforcement