Hive Pro

# THREAT ADVISORY

## RangnarLocker Ransomware hits Critical Infrastructure Compromising 50+ Organizations

**TA2022053**

**Threat Level** RED

**Published Date –** Mar 09, 2022

The Federal Bureau of Investigation (FBI) has released an alert on Ragnarlocker campaign that has affected nearly 52 organizations encompassing 10 critical infrastructure sectors, including entities in significant manufacturing, energy, financial services, government, and information technology. RagnarLocker ransomware operators work as part of a ransomware family, frequently changing obfuscation strategies to avoid detection and security.

The ransomware incorporates VMProtect, UPX, and unique packaging techniques, and it is often installed on hacked computers within a special virtual machine. It also makes use of the Windows API GetLocaleInfoW to determine the system's location and stops the process if the computer is in certain countries. RagnarLocker scans compromised machines for current infections in order to prevent data corruption, identifies tied hard drives, iterates through all running processes and stops those linked with remote administration, and thereafter attempts to delete all Volume Shadow copies in order to prevent data recovery. Following that, the ransomware encrypts any material of interest – avoiding encrypting files in particular folders – and then leaves a.txt ransom note instructing the victim on how to pay the ransom.

Organizations can mitigate the risk using the following methods:

- Use multi-factor authentication and strong passwords for remote access services, as well.
- Maintain patched and up-to-date systems, devices, and apps.
- Keep an eye on cyberthreat reporting for the publishing of compromised VPN login credentials, and update passwords and settings as needed.

The Mitre TTPs commonly used by APT41 are::
TA0001: Initial Access
TA0007: Discovery
TA0040: Impact
TA0009: Collection
TA0005: Defense Evasion
TA0003: Persistence
TA0011: Command and Control
TA0042: Resource Development
TA0002: Execution
TA0008: Lateral Movement
TA0006: Credential Access
TA0029: Privilege Escalation
T1059.003: Command and Scripting Interpreter: Windows Command Shell
T1543.003: Create or Modify System Process: Windows Service
T1486: Data Encrypted for Impact
T1564.006: Hide Artifacts: Run Virtual Instance
T1562.001: Impair Defenses: Disable or Modify Tools
T1490: Inhibit System Recovery
T1120: Peripheral Device Discovery
T1489: Service Stop
T1218.007: Signed Binary Proxy Execution: Msiexec
.010: Signed Binary Proxy Execution: Regsvr32
.011: Signed Binary Proxy Execution: Rundll32
T1614: System Location Discovery

## Indicators of Compromise (IoCs)

| Type | Value |
|---|---|
| IPs | 185[.]138[.]164[.]18,<br>185[.]172[.]129[.]215,<br>45[.]144[.]29[.]2,<br>23[.]106[.]122[.]192,<br>45[.]90[.]59[.]131,<br>149[.]28[.]200[.]140,<br>193[.]42[.]36[.]53,<br>45[.]63[.]89[.]250,<br>190[.]211[.]254[.]181,<br>142[.]44[.]236[.]38,<br>37[.]120[.]238[.]107,<br>26 13:12:56,<br>95[.]216[.]196[.]181,<br>162[.]55[.]38[.]44,<br>116[.]203[.]132[.]32,<br>49[.]12[.]212[.]231,<br>193[.]42[.]39[.]10,<br>193[.]111[.]153[.]24,<br>178[.]32[.]222[.]98,<br>23[.]227[.]202[.]72,<br>159[.]89[.]163,<br>50[.]201[.]185[.]11,<br>47[.]35[.]60[.]92,<br>108[.]26[.]193[.]165,<br>108[.]56[.]142[.]135,<br>198[.]12[.]81[.]56,<br>198[.]12[.]127[.]199,<br>45[.]91[.]93[.]75 |
| Bitcoin Addresses | 19kcqKevFZhiX7NFLa5wAw4JBjWLcpwp3e,<br>1CG8RAqNaJCrmEdVLK7mm2mTuuK28dkzCU,<br>151Ls8urp6e2D1oXjEQAkvqogSn3TS8pp6 |

## References

https://www.ic3.gov/Media/News/2022/220307.pdf
https://www.securityweek.com/fbi-warns-ragnarlocker-ransomware-attacks-critical-infrastructure