Hive Pro

THREAT ADVISORY

Rook: New Ransomware in the market scavenges code from Babuk

TA202161

Threat Level RED

Publish Date – Dec 26, 2021

Security researchers found a new ransomware dubbed as Rook that reuses the code from Babuk which was released earlier. It was initially seen on VirusTotal on November 26th and pwned its first victim, a Kazkh financial organization from whom Rook stole 1128GB of data on November 30th.

Rook ransomware invades a victim's system through a third-party framework, such as Cobalt Strike, or through a phishing email. Individual samples are typically UPX-packed, but other packers/crypters, such as VMProtect, have been also observed. When executed, it attempts to terminate processes associated with security tools or anything else that could interfere with encryption. Because no persistence mechanisms have been discovered, Rook will encrypt the files, append the ".Rook" extension, and then delete itself from the compromised system.

Rook has been linked to Babuk due to the following reasons:

- The same API calls are used to retrieve the name and status of each running service, as well as the same functions are used to terminate them.
- The list of stopped processes and Windows services is the same for both ransomwares.
- Both checks to see if the sample is operating on 64-bit OS before deleting the disk shadow from the victim's machine.
- Both uses Windows Restart Manager API to assist with process termination, including processes associated with Microsoft Office programs and the popular gaming platform Steam
- Uses similar code for enumeration of local drives.

Organizations should educate employees about phishing to avoid getting targeted by ransomwares such as Rook, Babuk etc.

The TTPs used by **Rook** include:
TA0001 - Initial Access
T1566 - Phishing
TA0002 - Execution
T1059 – Command and Scripting Interpreter
TA0005 - Defense Evasion
T1027 - Obfuscated Files or Information
T1027.002 – Obfuscated Files or Information: Software Packing
T1562 - Impair Defenses
TA0007 - Discovery
T1007 – System Service Discovery
T1082 – System Information Discovery
TA0011 - Command and Control
T1090 - Proxy
TA0010 – Exfiltration
TA0040 - Impact
T1490 – Inhibit System Recovery

Indicators of Compromise(IoCs)

Type	Value
MD5	bec9b3480934ce3d30c25e1272f60d02, 6d87be9212a1a0e92e58e1ed94c589f9, 4f7adc32ec67c1a55853ef828fe58707
SHA1	36de7997949ac3b9b456023fb072b9a8cd84ade8, 19ce538b2597da454abf835cff676c28b8eb66f7, 104d9e31e34ba8517f701552594f1fc167550964
SHA256	f87be226e26e873275bde549539f70210ffe5e3a129448ae807a319cbdcf7789, c2d46d256b8f9490c9599eea11ecef19fde7d4fdd2dea93604cee3cea8e172ac, 96f7df1c984c1753289600f7f373f3a98a4f09f82acc1be8ecfd5790763a355b

References

https://www.sentinelone.com/labs/new-rook-ransomware-feeds-off-the-code-of-babuk/
https://otx.alienvault.com/pulse/61c986f940126b3db3bf70e4/
https://www.bleepingcomputer.com/news/security/rook-ransomware-is-yet-another-spawn-of-the-leaked-babuk-code/