Dark Angels Ransomware

Date: 28th April 2024 | Severity: High

Summary

The Dark Angels ransomware group has been active since at least May 2022. The Dark Angels ransomware strain seems to be a rebrand of Babuk and can target both Windows and Linux operating systems.

Attack Vectors

Dark Angels gains initial access through malspam messages that distribute RATs, which then lead to the deployment of a SOCK5 backdoor to maintain persistence. Then, the threat actors scan the compromised network to obtain weak access points and valid credentials for lateral movement. Dark Angels access NAS instances and other enterprise assets using weak and common passwords and exfiltrate sensitive data before encrypting the system. The threat actors were observed lingering in the system for five months before initiating the encryption.

- Another API makes a connection to the service control manager and gives the ransomware access to the service control manager database.
- It enumerates the services that run on the victim's machine (e.g. VSS, SQL, and Memtas) and terminates the ones that might interfere with the encryption process.
- To prevent system recovery, the Dark Angels ransomware deletes volume shadow copies and all items from the Recycle Bin.
- The encrypted files are appended with the .crypt or .crypted extension. Some files, such as EXE, DLL, and BABYK, are excluded from encryption.
- Finally, a ransom note (How_To_Restore_Your_Files.txt) with negotiation instructions is dropped in the encrypted folders.

Indicator of compromise

INDICATOR TYPE	INDICATORS
Domains	• login.myob[.]live • p66slxmtum2ox4jpayco6ai3qfehd5urgrs4oximjzklxcol264driqd[.]onion • qspjx67hi3heumrubqotn26cwimb6vjegiwgvrnpa6zefae2nqs6xqad[.]onion • lyoevnzm3ewiq6jeyyuob2wfou7gh47yotuucsrwlf6ju3xrw43wacad[.]onion • myob[.]live • login.myob[.]link

URLs	• http[:]//p66slxmtum2ox4jpayco6ai3qfehd5urgrs4oximjzklxcol264driqd.onion/index.html • http[:]//wemo2ysyeq6km2nqhcrz63dkdhez3j25yw2nvn7xba2z4h7v7gyrfgid.onion • http[:]//qspjx67hi3heumrubqotn26cwimb6vjegiwgvrnpa6zefae2nqs6xqad.onion/page/6297aa368 ec25
File Hashes	• 7c2e9232127385989ba4d7847de2968595024e83 • 38e05d599877bf18855ad4d178bcd76718cfad1505328d0444363d1f592b0838 • 5411d7905bef69cb16d44f52fc46aa32fd922c80 • fe8b6b7c3c86df0ee47a3cb04a68891fd5e91f3bfb13482112dd9042e8baebdf • f668f74d8808f5658153ff3e6aee8653b6324ada70a4aa2034dfa20d96875836 • e931e3191524a0f4bb264408969c3e4f • a874076693aff0f34d4248396a2dd777 • 529e24c81ede5dfcedcc4fbc7d0030f985c67af1 • 06187023d399f3f57ca16a3a8fb9bb1bdb721603 • 5cc2306e9e0aa8d1cb095791febf89b3 • 3b56cea72e8140a7044336933cf382d98dd95c732e5937a0a61e0e7296762c7b • 709b7e8edb6cc65189739921078b54f0646d38358f9a8993c343b97f3493a4d9 • ad5122a5ef7ecdd89d936cb8cc4e2bd5 • 1758a8db8485f7e70432c07a9e3d5c0bb5743889 • ebd310cb5f63b364c4ce3ca24db5d654132b87728babae4dc3fb675266148fe9 • a034f79273e3f61d34eeadf38f12dee2 • 7247f33113710e5d9bd036f4c7ac2d847b0bf2ac2769cd8246a10f09d0a41bab • 903c04976fa6e6721c596354f383a4d4272c6730b29eee00b0ec599265963e74 • 65ccbd63fbe96ea8830396c575926af476c06352bb88f9c22f90de7bb85366a3 • 4e9d4afc901fa1766e48327f3c9642c893831af310bc18ccf876d44ea4efbf1d • 435781ab608ff908123d9f4758132fa45d459956755d27027a52b8c9e61f9589 • 9c8feeab65f71344713d63f4879e247aba49dce4 • c860bf644bd5e3d6f4cae67848c4fc769184ae652fcb41cac670042b185d217a • 33f612338b6b5e6b4fe8cbb17208795c • 8ff189783dc0646513c791421df723187b614f6dbfafad16763e3c369c5dfa2a • 1b426f43c91ff3858ed91dfb621cf537 • fb57abf08a85f1d7ca0a6fdcd76b04ccf964a5b05f2f784492083994773e4590 • 9785231ebf3d00216aa979f8c705e2513568802e • 93cb0fa81ed42d4c44fac49dd0354d0b • 4a2ee1666e2e9c40d372853e2203a7f2336b6e03
IPs	• 89.38.225[.]166

Recommendation

- Use anti-malware software or other security tools capable of detecting and blocking known ransomware variants. These tools may use signatures, heuristics, or machine learning algorithms, to identify and block suspicious files or activities.
- Monitor network traffic and look for indicators of compromise, such as unusual network traffic patterns or communication with known command-and-control servers.
- Conduct regular security audits and assessments to identify network and system vulnerabilities and ensure that all security controls are in place and functioning properly.
- Educate and train employees on cybersecurity best practices, including identifying and reporting suspicious emails or other threats.
- Implement a robust backup and recovery plan to ensure that the organization has a copy of its data and can restore it in case of an attack.

NOTE: The recommended settings/controls should be implemented after due shall be tested on Pre-Prod or test environment before implementing. diligence and impact analysis.

Reference Links

- https://www.pcrisk.com/removal-guides/23738-dark-angels-team-ransomware
- https://medium.com/@scottbolen/threat-intelligence-report-dark-angels-ransomware-group- ef3cacf83f10