U UNISPHERE SOLUTIONS

info@unisphere.co.nz
www.unisphere.co.nz

CYBER GUIDANCE ISSUE 00191

LOCKBIT RANSOMWARE NEW FEATURES & RAAS

DATE ISSUED: 30th August 2021

IMPACT	LOW	MEDIUM	[✓ HIGH]
EASE OF EXPLOIT	HARD	[✓ MEDIUM]	EASY

OVERVIEW

LockBit (first appearing in 2019) is being pushed in a new campaign by its developers advertising new features to make the Ransomware-as-a-Service (RaaS) more appealing to potential affiliates.

BREAKDOWN

Since the beginning of July this year, researchers have noted a recent surge of activity for LockBit attacks with the disappearance of REvil and Darkside groups. Its developers are claiming LockBit 2.0 as one of the fastest encryptors available on the ransomware market. LockBit is able to gain network access through leaked or actively stolen account credentials for Remote Desktop Protocol (RDP) or VPN. New features include a Ryuk-stule Wake-on-LAN feature – waking offline devices by sending them packets to assist with lateral movement across a network. Additionally, modelling further Tactic, Techniques and Procedures (TTPs) from other ransomware including using Egregor tactics of hijacking printers to print ransom notes, data exfiltration for double extortion of victims and much more. Ransomware is fast becoming one of the greatest cybersecurity threats of 2021.

REMEDIATION STEPS

- Apply latest security patches and updates.
- Use MFA where possible and disable unnecessary Internet facing services.
- Use good password practices to secure against multiple account compromise.
- Download Unisphere's free Ransomware Defence Strategy Checklist to check how secure you are and start hardening your environment.

REFERENCES & RESOURCES

ZDNet	https://www.zdnet.com/article/this-ransomware-has-returned-with-new-techniques-to-make-attacks-more-effective
Unisphere Solutions	https://www.unisphere.co.nz/articles/hot-topic-ransomware