UNISPHERE SOLUTIONS
info@unisphere.co.nz
www.unisphere.co.nz

CYBER GUIDANCE ISSUE 0003

RANSOMWARE DOUBLE THREAT

DATE ISSUED: 24th June 2020

IMPACT	LOW	MEDIUM	**HIGH**
EASE OF EXPLOIT	**LOW**	MEDIUM	HIGH

OVERVIEW

Ransomware has seen a resurgence with the Covid-19 outbreak and the notorious REVil group also known as Sodinokibi and Nefilim group have been at the head of a number of recent Trans-Tasman and global high-profile attacks.

BREAKDOWN

Known Victims: Lion Breweries, Toll, Fisher & Paykel

Active and aggressive ransomware groups are using double tactics by demanding high ransoms in cryptocurrency, accompanied by extortion and threats to publish and auction proprietary and sensitive information on the Darkweb or Ebay if the ransom is unpaid. Common tactics to gain network access to exfiltrate data and encrypt systems include; phishing, breaching network appliances, exploitation of RDP and usually leverage privilege escalation.

REMEDIATION STEPS

- Ensure your organization has up to date Business Continuity and Disaster Recovery Plans
- Check your backup reports and routinely test restore procedures
- Create archive backups and ensure they are updated at regular intervals using varied backup types and have at least one copy stored offsite and offline
- Provide information and training to all employees regarding social engineering and phishing, how to spot an attack and what to do if an attack is suspected.
- Check network device security, access control permissions and open ports and monitor for abnormal activity
- Implement security-in-depth/defense-in-depth multilayered protections

REFERENCES

Stuff: https://www.stuff.co.nz/business/121856473/calls-grow-for-government-action-after-lion-receives-us800000-ransomware-demand
Security Brief: https://securitybrief.co.nz/story/check-point-discovers-new-double-extortion-ransomeware-tactic
Trend Micro: https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/nefilim-ransomware-threatens-to-expose-stolen-data
Bank Info Security NZ https://www.bankinfosecurity.com/nephilim-ransomware-gang-tied-to-citrix-gateway-hacks-a-14480