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

CYBER GUIDANCE ISSUE 00074

MALWARE THAT ASSOCIATES WITH RANSOMWARE

DATE ISSUED: 30th November 2020

IMPACT	LOW	MEDIUM	HIGH
EASE OF EXPLOIT	HARD	MEDIUM	EASY

OVERVIEW

Ransomware used to be most commonly propagated through phishing emails campaigns, but this may no longer be the case. More often than not, recent ransomware attacks have been tied to previously compromised or malware infected systems sold and supplied to ransomware gangs by "initial access brokers"

BREAKDOWN

In partnership with cybercrime organisations, ransomware gangs are able to more easily gain access to corporate networks through Remote Desktop Protocol (RDP) endpoints, network devices and hosts with backdoors and malware infections and carry out their attacks with elevated access privileges supplied by these so called brokers. The cybercriminals sell their gathered information and compromised machines to the gangs in order to facilitate these types of attacks. ZDNet have compiled a list of malware that have known connections to ransomware attacks over the past two years and a full break down can be viewed in their article listed below:

Emotet, Trickbot, BazarLoader, QakBot, SDBBot, Dridex, Zloader, Buer, Phorpiex, and CobaltStrike.

REMEDIATION STEPS

- Ensure your organisation has robust password policies and standards in place that are rigorously enforced
- Ensure all systems are up to date with the latest security patches issued by vendors and suppliers
- Educate users on social engineering attacks, how to detect them and what to do if they are suspicious
- Use up to date endpoint malware protection on all devices to detect and enable a response to any suspicious activity and make sure there is a sound incident response strategy in place.

REFERENCES & RESOURCES

ZDNet: https://www.zdnet.com/article/the-malware-that-usually-installs-ransomware-and-you-need-to-remove-right-away/?ftag=TRE49e8aa0&bhid=29606343124056600886148366084033&mid=13179745&cid=2352480217