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

CYBER GUIDANCE ISSUE 00207

CONTI RANSOMWARE DESTROYS BACKUPS

DATE ISSUED: 4th October 2021

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

OVERVIEW

A new feature from the Conti Ransomware gang makes it the new leader in backup destruction with the novel tactics used to annihilate your backups – especially if they are performed using Veeam recovery software.

BREAKDOWN

Both Advanced Intelligence and Palo Alto Networks have commented that the ransomware gang has become a standout in their ruthlessness and ability to seek and destroy an organisations backups during a ransomware attack. The group specialises in double extortion (Cyber Guidance 003) has been active for over a year now and have been known to target many verticals and business types focussing on those who have a serious need to restore their data, including the likes of Ireland's department of health in May 2021. By building their expertise in destroying backups, the Conti gang increase the likelihood of their victim paying the ransom as they are unable to restore their systems by other means. Conti attacks are typically initiated with the Cobalt Strike Beacon followed by deployment of another legitimate tool Atera (a remote management agent) giving them a foothold in the network. They use Ngrok to expose local server ports to the Internet and establish a tunnel for data exfiltration. This is then followed by privilege escalation and granting themselves access to the Veeam backups. They then weaponize Rclone to search for the backups and compromise them.

REMEDIATION STEPS

- Educate and train employees in identifying social engineering phishing and other malicious emails. Provide them with guidance on what to do and how to report them within your organisation
- Disable user's ability to run executable files and commands
- Track externally exposed endpoints as Conti sometimes use corporate VPN as their infiltration method
- Implement network hierarchy controls with network segmentation and decentralisation to prevent lateral movement.
- Use network monitoring discovery and alerting tools to expose anomalous behaviours and capture events such as the Rclone data exfiltration command line interface activities.
- Harden your Veeam backup access by layer controls such as special security protocols, restricted access, updating passwords and any other security controls possible.

REFERENCES & RESOURCES

Advanced Intelligence https://www.advintel.io/post/backup-removal-solutions-from-conti-ransomware-with-love
Palo Alto https://unit42.paloaltonetworks.com/conti-ransomware-gang/
Threatpost https://threatpost.com/conti-ransomware-backups/175114/