RANSOMWARE ATTACK

IMMEDIATE ACTIONS LIST

IF YOU ARE EXPERIENCING A RANSOMWARE ATTACK, YOU SHOULD TAKE THE FOLLOWING IMMEDIATE ACTIONS...

- Disconnect the infected devices' Network Interface Cards (NIC) from the network.
- Disconnect network Internet connectivity (including wireless).
- Separate backups from the network and write protect where possible.
- If you have cloud backups, log in from a location other than your company systems and change the credentials.
- Disconnect switches to prevent continued, or the beginning of, lateral infections.
- DO NOT shut down a device that is known to be in the process of encryption. You may corrupt the OS or other applications and make recovery using the keys impossible.
- DO NOT communicate on the network, company related email, IP phones, Teams, Slack, etc., as the threat actors are often listening to, and/or reading your communications. Additionally, you cannot take back anything said to employees, partners, etc., in writing or verbally.
- DO NOT communicate with the threat actor until you have the support you need. This can create issues and start a timer. Having the right negotiator can have a massive impact on the results, so don't rush to settle.
- Consult a lawyer known as breach council before messaging anyone not a decision-making executive or staff/service providers critical to your recovery. Ransomware is as much a legal issue as it is a technical emergency.
- Finally, we recommend you reach out to us from a phone not associated with your firm. We are available 24x7, 365 days a year, and can immediately begin to guide you through the proper response.

Call us at (877) 662-6624

www.alvaka.net

ALVAKA