THE FIRST **5 THINGS** TO DO (OR NOT DO)

When You're the Victim of a Ransomware Attack

If you think your organization has been the victim of a ransomware attack, immediate action is required. Taking the right steps as soon as you think an attack is underway can have a positive impact on the cost to your organization (cost and reputation). Follow these five tips below to mitigate the impact of a ransomware attack.

$761,106

Average cost of a ransomware attack considering downtime, people time, ransom paid, network cost, lost opportunity, etc. (Sophos 2020 Report)

1 DO isolate network traffic to mitigate the risk of continued adversary activity

Once you determine there is an active ransomware attack, you need to stop the spread and prevent the attacker from maintaining their foothold on network connectivity. You can accomplish this by building "islands". Network connections should be blocked at the following locations:

- External firewall (to prevent any and all internet traffic and to keep the attackers out)
- Business-critical servers
- Any asset with indications of ransomware
- On-premise backup solutions

2 DO NOT turn off servers until you are certain they have not been affected by ransomware

The applications attackers use are often stored in the computer's live memory. This is valuable forensic information that can be used to determine the most effective countermeasures against an attack. Restarting or rebooting assets clears the live memory, wiping out this valuable data. Servers should stay on, but must be isolated (see Step 1).

3 DO verify the state of business-critical system backups and make an offline copy of these backups

Attackers have invested time, and they want to get paid. They will often target backup solutions and, if found, delete them, to prevent the victim from rebuilding critical assets. An offline copy of the backups reduces the likelihood that all quality backups will be destroyed by ongoing ransomware efforts.

4 DO contact legal counsel and inform them of the situation

Every state has laws around breach disclosure that stipulate what you need to do if your organization has been the victim of an attack. It's important to consult legal counsel with experience in cyber law to help you determine whether or not public disclosure of the event is required by law.

5 DO NOT try to "clean up" the ransomware without professional assistance

While it may be tempting to try and clean up a ransomware attack on your own, this can increase your chances of falling victim to a future attack. Once an adversary is inside your network, they can turn 1 back door into 5. Attackers also share information about successful attacks with fellow hackers. Proper hunting and remediation is key to future protection.

If you suspect an attack, call our emergency hotline right away: 612-399-9680

BLUE TEAM ALPHA

Emergency | 612-399-9680 | 911@blueteamalpha.com
Email | sales@blueteamalpha.com
Web | blueteamalpha.com