

8 TIPS

FOR BETTER RANSOMWARE DEFENSES AND RESPONSES

Did you know that ransomware attacks are more than a “smash-and-grab” attempt? These attacks are now getting more sophisticated. Here are eight ways to help defend your data against these growing cyberattacks.

01 IDENTIFY ATTACKERS' ONGOING CAPABILITIES

Understand what ransomware attackers are doing inside a network and what they might still be capable of doing. Lock it down!

03 LEARN FROM OTHERS' MISTAKES

The failure to detect attackers inside your network and give them the boot can have serious implications. Don't assume that because your ransomware attack is resolved, that the attackers aren't still somewhere within your network.

05 MOVE QUICKLY

Identify unusual traffic within the network first and thwart any attacks to soften the impact. Don't just watch for malware, be proactive and find traces of compromised assets at an early stage.



06 MONITOR FOR ODD EVENTS

Monitor “odd events” like binaries (aka LOLBins) with malware detection tools, web scanning tools and next generation firewalls, to quickly block known attacks as well as block users from connecting to known bad IP addresses.

07 PREPARE A SECURE COMMUNICATIONS CHANNEL

Always have a separate, secure communications channel as well as a walled-off storage channel to keep your data for any digital forensic investigations.

08 DON'T RESTORE, REBUILD

Think about how you rebuild your network and infrastructure rather than decrypting your current data and restoring it to eliminate the threat of another attack.