PREVENTING RANSOMWARE – THINKING BEYOND THE ENDPOINT AND INTO THE NETWORK

Security teams work diligently to ensure that their organizations don't fall victim to ransomware, whether as part of a wave of attacks or a highly targeted attack. It's common knowledge that the endpoint is the optimal place to prevent against ransomware, but it's not the only place prevention can, and should, occur.

The endpoint is the most vulnerable vector to ransomware. As such, endpoint security managers are focused on ensuring their protections can prevent against the latest ransomware. Security operations managers comb through data searching for indicators of a successful ransomware attack to remediate and minimize the spread of the attack. But how does ransomware impact the day-to-day duties of the network administrators when their priority is to ensure the network is operating as optimally as possible? What follows are the four reasons why network administrators must care about preventing ransomware.

1. Lack of Visibility

Malicious files are commonly hidden within encrypted traffic in order to evade detection by network security controls. When traffic is encrypted, security policies are difficult to enforce as there is little visibility and control of the data. This allows malicious traffic to traverse the network, ultimately putting organizations at risk of falling victim to ransomware attacks.

When enabled and configured appropriately, SSL decryption can decrypt, inspect and enforce security policy on encrypted traffic. However, if that feature is not configured appropriately, malware can bypass detection and expose the network to ransomware.

To avoid this risk, outside of ensuring SSL decryption is configured appropriately, network teams need to coordinate with security teams to maintain awareness of any changes to the security policy made based on observed malicious activity. This will reduce any impact to the network when new changes are deployed. Endpoint teams must also ensure that their endpoint security products can identify malicious files, tag them and distribute that information throughout the security infrastructure, including to the network. This allows for a standardized, risk-based approach that delivers consistent visibility, control and policy.

2. Lateral Movement

Ransomware attacks will encrypt a device and prevent a user from accessing their data. However, locking a user out of a device is not always the primary motivation, and the ultimate payout might not always be the ransom. Ransomware can contain a worming component and use the initial compromised endpoint as the starting point of a much larger attack. Attackers will penetrate the network from an unprotected vector and then move laterally within the organization – either to spread ransomware throughout the network and increase payout or to gain access to more valuable targets, like data and applications. In this case, the network becomes a vehicle for the attack to spread and increase damage.

Network teams need to work closely with security teams and become involved in the forensic mapping of ransomware attacks. Identifying how an attack moved from point to point and where it succeeded allows network teams to identify where appropriate network segmentation should be applied. Additionally, endpoint teams must deploy protections that can adequately prevent endpoints from getting infected outside the network and then bringing the infection inside.

3. Roaming Users

With workforces becoming increasingly mobile, the number of endpoints vulnerable to threats and ransomware attacks has also increased. Roaming users may not benefit from the same protections they would have received from within the network perimeter. Traditionally, secure tunneling via a VPN has been used to extend network protections to remote users. However, these protections may not always be enabled, or as comprehensive, depending on the settings, user preferences and capabilities of the technology.

Network teams should work to ensure their network protections extend to their VPN tools consistently and efficiently. This involves security awareness training to ensure users enable the feature, or don't disable the feature, when outside the network perimeter. In concert with VPN tools, endpoint protection must be capable of identifying and preventing ransomware encryption methods.

4. Bandwidth Impact

Many organizations have begun to move away from backhauling to minimize bandwidth issues. This transition has moved protections farther away from the network perimeter and left organizations reliant on the protections offered by endpoint security products and VPNs. This shift has been driven by organizations' concerns about bandwidth issues and costs.

Network productivity is also a concern for attackers, as ransomware is designed to consume minimal amounts of bandwidth. Ransomware relies on the network to download malware, phone home and move laterally; and organizations would face substantial downtime and productivity losses. The last thing attackers deploying ransomware – or the organizations themselves, for that matter – want is for the network to slow down or, even worse, shut down entirely.

Infected machines' and ransomware's connections to command-and-control servers consume additional bandwidth, adding to avoidable, albeit minimal, unnecessary budget spend. As bandwidth is an ongoing concern, network teams should work with endpoint teams to ensure the endpoint protections cause minimal impact to bandwidth when pushing out signature files.

Palo Alto Networks® Next-Generation Security Platform natively integrates the efforts of the various components of the security organization into one platform that enables a consistent security posture across the endpoint, on the network and in the cloud; all while supporting open communication, orchestration and visibility of users and data. An integral part of the Next-Generation Security Platform is Traps™ advanced endpoint protection. Traps employs a multi-method approach to malware and exploit prevention to protect against known and unknown threats, like ransomware. Included in Traps multi-method prevention is behavior-based ransomware protection, in which Traps analyzes the endpoint for ransomware-type behavior. Upon detecting the initial encryption activity, Traps blocks the attack and prevents the encryption of additional files.

Click here to learn more about Traps.