Network Box USA

Ransomware: How We Protect You

Ransomware spreads via links inside emails. The email makes it through the filters, the user clicks, the malware is downloaded.

Our protection begins with over 2,000,000 AV signatures against ransomware, plus a number of policy engines that scan for active content inside emails. We also partner with over 150 threat intelligence companies to get real time information on things like web links or IP addresses that need to be blocked.

Most of the blocking is done in the email scanning, which you are doing with us. Tools to block threats include not just AV scanning, but anti-spam signatures, anti-phishing, anti-spoofing, DMARC/DKIM/SPF analysis, reputation and blacklist systems to block mass emails as spam, URL scanning to block links to known ransomware campaigns, and much more.

Should an email make it through, and should the user click on a dangerous link, the web filtering function kicks in. In your case, we have HTTPS decoding turned on. Therefore, that link would be scanned for malware by the same AV and policy engines that scanned the email. The URL scanning also deals with redirects and scripting.

We also have a 2 layer IPS (layer 3 and layer 7) that scans outbound traffic for infections. This Infected LAN IPS not only monitors single TCP packets headers for traffic destined for known bad IP addresses, it also monitors the packet content for URLs that are known to be bad. In this instance, the proxy blocks them.

While there is never a 100% guarantee of success in these things, this layered approach has allowed us to have a very high track record of success against ransomware over the years. Layered approach, scanning every aspect of anything that could cause ransomware to be downloaded, is the only viable approach to securing against this threat.