CDN NETWORK DEFENDER AND RANSOMWARE

Driven largely by the advent of cryptocurrency, ransomware has quickly become the cyber criminal's preferred method to monetize an attack. Reports of high-profile ransomware episodes now litter even the popular press, and most analysts predict incidents will only increase in the coming months and years.

Given this reality, Celerium is often asked by our MSP partners if we can prevent ransomware attacks. The short answer: in many cases, no.

But, we can, often, appreciably mitigate the impact of a ransomware infection.

PROBING FOR VULNERABILITIES

Ransomware, like any malware, has to find a path onto the victim organization's network to be effective. Cyber attackers use multiple means to find ways onto a target network, including the exploitation of vulnerabilities, or unpatched software that was written and deployed with security flaws. Attackers probe networks for these vulnerabilities, then use them to gain access when they find them. The probing process includes scanning for open ports, and if those scans originate from servers known for nefarious activities, CDN Network Defender can auto-block those scans, eliminating that threat before it can even launch an attack on a vulnerable network element. If the objective of the scan was to find entry for a ransomware payload, CDN Network Defender would be effective in stopping that attack.

PHISHING

Yet, a more common technique used by bad actors to gain network access is via phishing, whereby an email designed to look like a legitimate communication is sent to as many recipients of the target organization as possible. If just one employee clicks on an attachment, or visits a website link embedded in the phishing email to provide credentials, for example, initial network penetration is successful, and the hackers can then move about the network to identify data that can be encrypted and held for ransom.

After initial network penetration via a successful phishing email, attackers must communicate with the installed malware to execute the attack. This "command and control" element of a cyber attack requires the perpetrators to communicate using a remote server/computer, and that device has to have an IP address. If the attackers are highly sophisticated nation-state actors, they may have the resources to execute and control their attack from virgin infrastructure with no reputation, but for the cyber criminal entrepreneurs that typically target the SMB community, there's a reasonable chance they're communicating from IPs that are known to be compromised. Once communication from compromised or high risk hosts begins, CDN Network Defender can block the traffic, effectively shutting down the ransomware attack in its infancy.

ALERTING

Moreover, CDN Network Defender's granular notifications capability enables MSP partners to set up alerts when an internal device is exchanging data with a high risk external device, so not only can that communication be auto-blocked, but the alert can point the MSP toward the likely compromised internal device as part of the incident response effort. Indeed, one of CDN Network Defender's current customers often deploys CDN Network Defender as one of its first tasks when launching an incident response engagement.

To learn more about how Celerium can help combat (but not necessarily prevent) ransomware, visit celerium.com to schedule a demo, trial, or request pricing.