Containment is the New Prevention

Ransomware Can’t Cause Damage if it Can’t “Phone Home”

We’re often asked, “How do you stop this latest malware threat?” While preventing infections is the ideal answer, no vendor can achieve 100% prevention. The delivery (e.g. email) and infection (e.g. executable) are just the first few steps of CryptoLocker’s multi-stage cyber-attack. Our answer is to block Ransomware’s ability to phone home to botnets.

The Achilles Heel: CryptoLocker’s DGA-Based Botnet

Infected systems must rendezvous with their botnet controller via one of many domain names generated every day. But if none of the domains can be resolved to the controller’s IP address, then CryptoLocker stays dormant.

Big Data Delivers Protection Before Malware Analysis

Antivirus and other security vendors’ time-intensive approach must collect and then analyze the binary code of every CryptoLocker variant. In the meantime, customers become victims as the polymorphic malware evades signature-based detection. OpenDNS uses a predictive, network-level approach, which discovers and blocks unknown domains that co-occur before or after CryptoLocker’s known domains via the 50+ billion DNS requests resolved daily by OpenDNS. As domain co-occurrences are validated by algorithmic classifications, they are quickly added as new known CryptoLocker domains, and then used in the next iteration.

As a result, OpenDNS blocks our customers’ infected systems attempts to phone home; containing the ensuing damage well before antivirus solutions.

First, Predict the Unknown...Then, Block the Known

Researchers have reverse engineered the DGA. OpenDNS contributes to, and participates in, leading security research communities. As a result, we obtained the algorithm and have blacklisted every CryptoLocker domain name candidate through 2014 to proactively protect our customers.