OpenDNS

OpenDNS is now part of Cisco.

LOOKINGPOINT

Ransomware

WHAT IS RANSOMWARE

Ransomware is a malicious software designed to hold a user's files (such as healthcare records, financial contracts, manufacturing blueprints, software code, and other documents) for ransom by encrypting them and demanding the user pay a fee (often in Bitcoin) to decrypt them.

HOW RANSOMWARE WORKS

Attackers initiate attacks using an array of tactics. Ransomware infections often first begin with an exploit kit — which are software kits designed to identify software vulnerabilities on endpoints and then upload and execute malicious code on the endpoint. This can happen when users click on links in phishing emails or if malicious ads or compromised sites redirect users to domains hosting exploit kits like 'Angler'. Exploit kits can also be delivered via email attachments or infected thumbdrives, but interestingly, this initial payload is not the ransomware.

If the initial payload successfully exploits a system, it analyzes its environment (for example, looks at the operating system, and unpatched applications) to drop an effective ransomware variant. A callback is then made to the ransomware infrastructure to retrieve the private keys needed to encrypt the endpoint. Most popular exploit kits and ransomware variants have to resolve a domain name to an IP address to initiate the callback.

Infected users have two options: pay the ransom or potentially reimage the endpoint and reinstall a recent backup and hope the ransomware won't spread to other systems on their network.

Although variants of ransomware behave differently — there are many ways that OpenDNS and Cisco can help. OpenDNS learns from Internet activity patterns from 80+ billion daily DNS requests to identify attacker infrastructure being staged for the next threat. Using statistical models developed by the OpenDNS Security Labs team, we're able to automatically discover, classify, and even predict the callback destinations used by exploit kits, phishing campaigns, and many ransomware variants.

WASTE LESS TIME FIGHTING RANSOMWARE ATTACKS

Cisco Security Solutions provide an extraordinary breadth of coverage against ransomware attacks:

OpenDNS Umbrella protects devices on and off the corporate network. In the case of the initial infiltration, OpenDNS Umbrella flags the exploit or phishing domain as malicious and blocks the DNS request before the browser connects to the malicious site. Umbrella stops C2 callbacks — over any port or protocol — which can stop the ransomware drop or the C2 callback for the encryption key.

Cisco Advanced Malware Protection (AMP) for Endpoints provides point-in-time protection to detect malware that evades initial inspection. Using a combination of file signatures, file reputation, behavioral indicators, and sandboxing, AMP can stop the initial exploit kit from executing on the endpoint and can also stop the execution of the ransomware file and remove it.

Cisco Email Security gateways employ Advanced Malware Protection (AMP) technology to detect ransomware that arrives by email in attachments and URLs. The technology is the same as that applied in the endpoint, but it's deployed at the email gateway. For email attachments, AMP uses file reputation and file sandboxing to identify and block suspicious files where no known signature exists. Catching ransomware at the email gateway is preferred to detecting it downstream because a Cisco Email Security gateway can drop one email carrying ransomware to many recipients. AMP in email security provides a defense-in-depth approach to remediating ransomware attacks.

Some things to consider:

- How many ransomware infections do you see monthly?
- How much time does your security team spend remediating ransomware infections?
- What security solutions do you use today to try to stop ransomware?
- How do you research and proactively hunt for information about ransomware threats? (i.e. information about files, exploit kits, domains, etc. associated with ransomware)