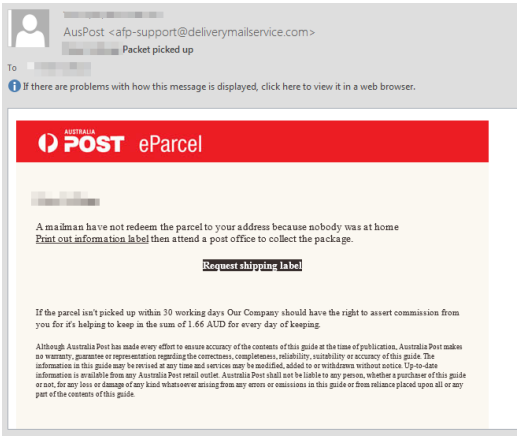
CHECK POINT
RANSOMWARE PREVENTION

CURRENT WAVE OF RANSOMWARE

Today, ransomware, like Cryptolocker, is hitting organizations around the globe. At Check Point we can help prevent these ransomware attacks via our multilayered approach to security.

The current round of ransomware is coming in via two different methods, malicious ads and via phishing links in e-mail. A common thread amongst both these methods of attack is sites protected by SSL/TLS. Most of the cyber-criminal are using HTTPS encrypted sites to infect computers with ransomware. This means that in order to protect your organization against these threats it is vital that HTTPS inspection is enabled on your gateway. Prior to enabling, you should ensure that there is sufficient capacity on your gateway to handle the additional work of enabling HTTPS inspection. This will enable Check Point's multi-layered security controls to inspect inside SSL/TLS encrypted communications and prevent ransomware.

The malicious ads technique used by these cyber criminals can in most cases be prevented by enabling and updating Check Point IPS signatures and ensuring that the CPAI-2015-0002 (Angler Landing Page) signature is set to prevent. The Angler exploit kit is a commonly used method of infecting a PC and installing all kinds of malware including ransomware. This method however is not the most common. Currently the most widely spread way of infecting PCs with Cryptolocker is via phishing e-mails.



A sample of a phishing e-mail. They are usually addressed directly to the user.

Phishing e-mails are e-mails pretending to be from a well-known and trusted source. Currently, our research team is seeing a rise in attacks targeting users in Australia. In this current round of Cryptolocker hitting Australian users, the phishing emails appear to be coming from the Australian Federal Police (AFP) and most commonly Australia Post. These particular phishing emails contain text to encourage readers to click on a link. This link takes them to a landing page which then directs them to download the malware. The malware is most commonly hosted on lesser known file sharing sites such as Cubby or Copy.com. To help stop such an attack it is recommended to use Check Point's Application Control & URL Filtering, which for better security measures, blocks access to file sharing sites except for those used by the business.

Name	Source	Destination	Applications/Sites	Action	Track	Install On	Time
Block File sharing	Any	Internet	File Storage an...	Block Blocked Message	Log	All	Any

In the case that there is a malware that is hosted on a site allowed by the business, or comes in via other means, the next layer of protection is Check Point's sandboxing solution called Threat Emulation. Threat Emulation will open the files being downloaded in a Windows virtual machine to see what it does. This allows Check Point to easily detect highly evasive pieces of malware like Cryptolocker without needing a signature. To ensure complete protection against ransomware like Cryptolocker it is important to deploy a sandboxing technology that is deployed inline, which can do HTTPS inspection and is deployed in "hold mode" so it actually stops the malware from being downloaded.

If there is an infection that comes in via the Internet, or via other means like USBs, Check Point's Anti-Bot will detect the malware communicating back to its creator and block these communications and trigger an alert. In most types of ransomware, blocking this communication will stop it from encrypting the file as their business model is based on selling you back the encryption key that is uploaded during this communication. This will also alert you to the fact that a computer on the network has been compromised and allow you to rapidly respond.

This multi-layered approach provides strong protection against Cryptolocker, other sorts of ransomware and cyber-attacks in general; however no technology is ever 100% effective. The cyber criminals will always find a new technique or way to attack. As a result it is critical that organizations plan for incidents, and have the visibility to rapidly respond to incidents via centralized management and visibility. Also ensuring your security architecture is following modern best practices is critical to limiting the damage a successful attack can do. Check Point has released a whitepaper on how to secure your business. The whitepaper, Stopping the Next Massive Cyber-attack and detailed information on Incident Response is available at the Check Point Blog. In addition Check Point's Incident Response team can assist in responding to and preparing for an incident.

SUMMARY

Using a multi-layered approach to security will allow you and your organization to significantly reduce the threat of cyber-attacks, including ransomware. The key to having multiple layers is that they provide centralized reporting and visibility and work together. Check Point's centralized security management will allow you to rapidly stop and prevent attacks via a single pane of glass. To help prevent ransomware Check Point's recommendations are:

1. Enable HTTPS inspection
2. Deploy Threat Emulation (sanboxing), and ensure support for the latest file types has been enabled
3. Stop access to non-business related file sharing sites
4. Ensure IPS is up to date
5. Deploy Anti-bot (bot-net protection) & Anti-virus and monitor the logs via SmartLog or SmartEvent (event correlation)

Check Point is the leader in protection against targeted attacks and unknown malware with the industry's fastest Threat Emulation as well as industry's best catch rate of unknown malware. This provides you with the best chance of stopping ransomware. For further questions contact your local Check Point team or contact the Check Point Incident Response team at emergency-response@checkpoint.com. For critical incidents call Check Point Incident Response customers can call +1(866) 923-0907.