Avecto

Defendpoint real world healthcare breach analysis

Hospitals across the globe have been thrown into a state of high alert following a series of high profile ransomware outbreaks. Unlike the human viral threats they are equipped to deal with, these outbreaks are proving far more difficult to contain and treat, putting data and patient safety at risk.

This bitesize article analyzes a recent healthcare ransomware attack and discusses how Defendpoint can proactively immunize endpoints against a broad spectrum of malware without detection.

Introduction

Hospitals across the globe have been thrown into a state of high alert following a series of high profile ransomware outbreaks. Unlike the human viral threats they are equipped to deal with, these outbreaks are proving far more difficult to contain and treat, putting data and patient safety at risk.

This bitesize article analyzes a recent healthcare ransomware attack and discusses how Defendpoint can proactively immunize endpoints against a broad spectrum of malware without detection.

Healthcare - A state of emergency

In late February 2016 the Henderson Methodist Hospital, Chino Valley Medical Centre and Desert Valley Hospital were all hit by ransomware attacks. This was only one month after a Los Angeles hospital was besieged by a ransomware attack and forced to pay $17,000 to recover data.

Henderson declared an “Internal State of Emergency” and initiated a full shut down of all desktop computers. Emergency response plans were initiated, forcing them to roll back to entirely paper-based systems.

The attacks against healthcare providers are increasing, as attackers target unpatched or unsupported systems needed to support legacy healthcare applications.

Earlier this year, the threat actors behind Qbot, who specialise in targeting unsupported systems, infected and disabled all the legacy XP systems at Melbourne Health.

When we walk through the attack chain we see a common pattern of events:

- First, a user receives a phishing email with a malicious attachment. The attachment is unique and therefore not detected by any network or endpoint detection products.
- The attachment is a Word document which appears to be an invoice. When the user opens it they are prompted to enable macros to view the invoice.
- Once the macros execute, the Locky ransomware executable payload is dropped into the user’s temporary directory and launched.
- Locky attempts to encrypt data on the local machine as well as any network drives the user can access. In the Henderson case, the ransomware succeeded in expanding its reach from the initial infection to several systems found in the network

Avecto

Locky malware analysis

Locky is the latest in an ever-increasing range of ransomware threats used by cyber criminals in an increasingly lucrative market. What makes Locky special is that it appears to have come from the same group behind several large Dridex banking trojan campaigns, showing they are possibly diversifying their range of attacks.

Avecto has observed well-orchestrated global Locky campaigns using malicious Word documents disguised as invoices to attack a wide variety of organizations.

In the Avecto Malware Labs, the majority of attacks have used fake invoices in the form of Word documents. Once the user opens the document and the macros launch, Locky attempts to do several things:

- Drop and launch the Locky payload in the user's temp directory
- Encrypt files on local and network drives
- Set the user's wallpaper to a ransom demand
- Delete local backups of the file system

Once the encryption has taken place, it is practically impossible to decrypt the files without paying the ransom. As the attackers use sites on the dark web, and Bitcoin currency, the transactions are anonymous and untraceable.

Locky has been observed to encrypt most popular file types and even specifically targets Bitcoin wallets. The file extensions targeted include:

asm, .c, .cpp, .h, .png, txt, .cs, .gif, .jpg, .rtf, .xml, .zip, .asc, .pdf, .rar, .bat, .mpeg, .qcow2, .vmdk .tar.bz2, .djvu, .jpeg, .tiff, .class, .java, .SQLITEDB, .SQLITE3, .lay6, .ms11, .sldm, .sldx, .ppsm, .ppsx, .ppam, .docb, .potx, .potm, .pptx, .pptm, .xltx, .xltm, .xlsx, .xlsm, .xlsb, .dotm, .dotx, .docm, .docx, wallet.dat

What went wrong?

Anyone running the IT operations of a healthcare provider knows there is no shortage of vendors promising to help secure networks and devices. So why in 2016, with all the technology on offer, are we still seeing breaches and infections?

The problem is that the vast majority of solutions are attempting to do the impossible and detect the unknown. This is not just limited to the well-known struggle of endpoint antivirus to keep up with constantly evolving threats, but can be witnessed in a variety of network detection products, threat intelligence feeds and exploit mitigation techniques. Whenever you try to maintain a blacklist of known threats to block malware authors can find a way around it. Even if a solution is 99% effective it only takes one threat to reach an unprotected endpoint for a breach to occur.

Best practice security

With advanced network defenses and enterprise antivirus products unable to prevent Locky and other rapidly evolving threats it is time to start thinking proactively. Let''s look at how we can mitigate risks without detection.

Screen and test

We can verify that some applications are known good, or part of the system, and we can whitelist them. Any new applications that appear can then be easily blocked until they are given the all clear.

Get the dose right

Don't prescribe the same admin rights for everyone. Make sure that users have the appropriate privileges. Giving admin rights to a user facing malware threats is like giving steroids to treat an infection... you lower the system's defenses and the infection takes over.

Defendpoint applies all these principles in a single lightweight agent that combines least privilege and application whitelisting.. This robust approach has allowed Defendpoint to prevent Locky and hundreds of other undetectable threats from ever infecting a system or accessing user data.

About Avecto

Avecto is a leader in Privilege Elevation and Delegation Management. Since 2008, the company has enabled over 8 million users to successfully work without admin rights, enabling many of the world's biggest brands to achieve the balance between overlocked and underlocked environments.

Avecto's Defendpoint software has been deployed in the most highly regulated industries, enabling organizations to achieve compliance, gain operational efficiency and stop internal and external attacks.