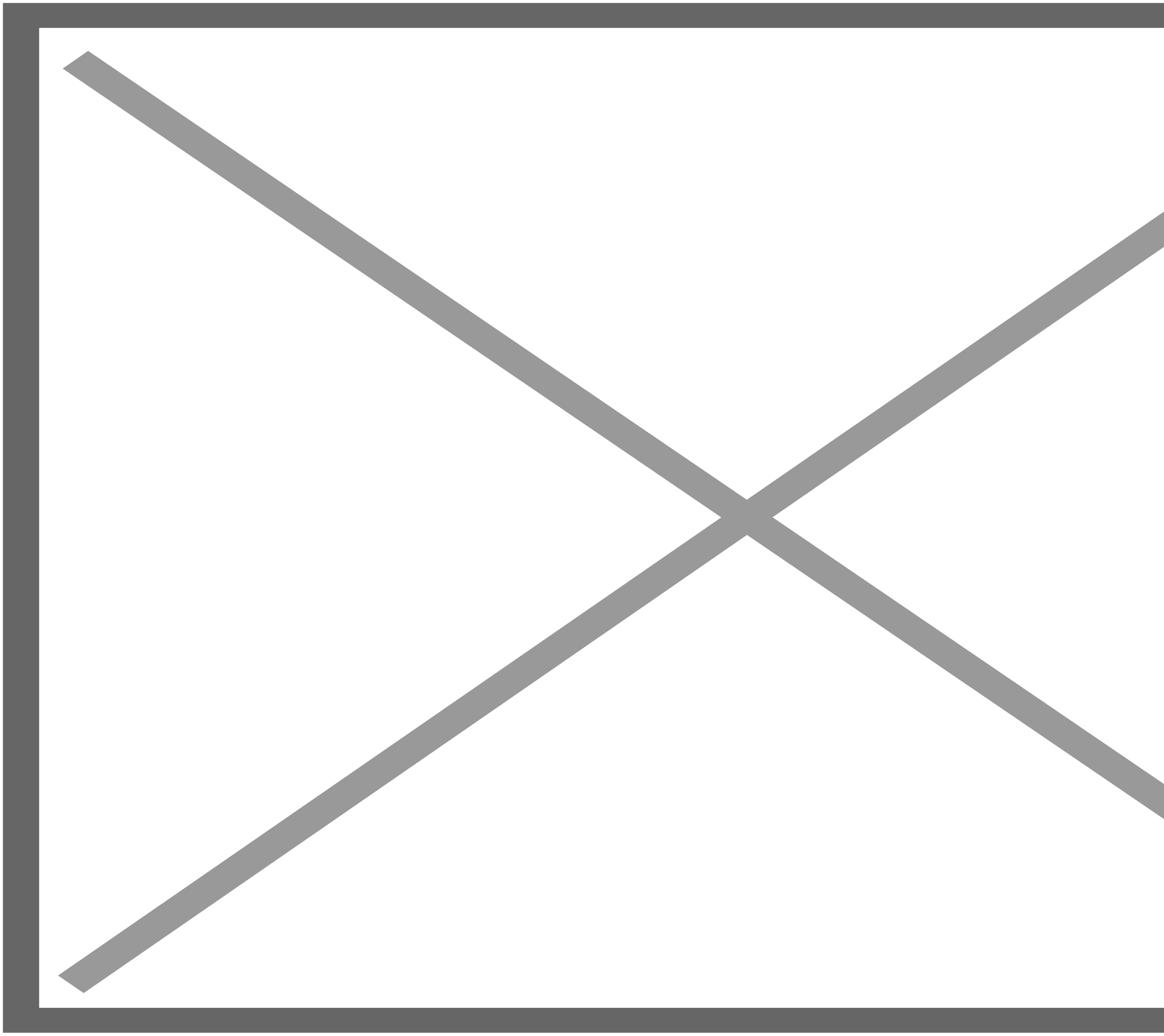
Ransomware attacks

General Features Professional standards



01 June 2017

Michael Stout provides guidance on how best to protect your company or clients from malware attacks

Key Points

What is the issue?

All software packages have vulnerabilities. Whether it be a flaw in declaration, design, implementation, or systems integration, no programmer can account for every situation their code will encounter. Malware is software that exploits a vulnerability in a program or operating system.

What does it mean to me?

The malware the criminals create may not destroy data but compromise the victim's computer and add it to a botnet so the hacker can control it and use it to attack other victims. Protecting your company or clients from malware attacks is therefore vital.

What can I take away?

By adopting best practices, information security awareness training, and fostering a security awareness culture, businesses can make it difficult for the hackers, so they lose interest and simply move on to the less protected.

The idea of sending an email with a nefarious attachment or hyperlink to a compromised website in hopes an end-user will open or click it is nothing new. The creators of computer viruses have long depended on end-users to open or click their wares to infect computer systems and destroy valuable and or personal digital assets for decades. Sometimes, deleting data is not the objective. The malware the criminals create may not destroy data but compromise the victim's computer and add it to a botnet so the hacker can control it and use it to attack other victims.

Malware is software that exploits a vulnerability in a programme or operating system. One might think a competent software engineer would address all potential vulnerabilities before compiling their code into a program for mass distribution. I can assure you most programmers take a motherly pride in their code, but one should understand 'software engineering' is a fallacy. The writing of software programs, coding, is more an art than engineering. Certainly, there are considerations for efficiency and reusability but the end-product is more poetry than math (Alternatively, as you Brits say, 'maths')!

All software packages have vulnerabilities. Whether it be a flaw in declaration, design, implementation, or systems integration, no programmer can account for every situation their code will encounter. Vulnerabilities exist in all systems. When someone discovers a software vulnerability what he or she does with it depends on his or her motivation and ethos.

The White Hat Hacker will keep their discovery quiet and report it to the software publisher. The White Hat Hacker will only discuss it after the software publisher has issued a security patch, a small program to fix the vulnerability. The Black Hat, on the other hand, will keep it quiet, not informing the software publisher. They will shop it around criminal organisations on the dark web or approach rogue nations who will pay significant amounts of money to gain a cyber-hegemony over their rivals. When discovered by a government intelligence agency, the vulnerability remains unknown until someone else reveals it and throws it out to the public domain.

Software vulnerabilities that remain out of the public eye are known as zero-days. Zero-day vulnerabilities often result in zero-day exploits. An exploit is a defined methodology, often a software program or script, to compromise a software or system vulnerability. It may be a simple click-and-go exploit or a daisy-chained exploit requiring the sequential execution of actions. The vulnerability exploited in the widespread WannaCry ransomware attack in May 2017, was attributed to a zero-day vulnerability click-and-go exploit in the Microsoft

Windows operating system. The attack vectors used by the hackers to deliver the malware to the target systems were likely attachments or links to an infected website. Delivery using a stolen NSA exploitation tool, EternalBlue has also been cited. Regardless of how hacker presented the end-user with the dangerous payload, they clicked it.

Upon clicking the malware, the computer was compromised and started encrypting files until rendering them useless. Up until this point, ransomware attacks are pretty much the same as a virus infection. In a traditional virus attack, the user and system files are deleted and destroyed, also rendering them useless.

Perhaps, in the case of ransomware, one should be thankful. Instead of destroying valuable commercial or irreplaceable personal digital assets for the simple 'fun of it' or 'challenge', the criminals who create ransomware give the victim the opportunity to be extorted and get their digital property back. After encrypting the user and system files, the ransomware produces a screen offering instructions and demanding payment for the decryption key. Often demanding Bitcoins, the transaction is as anonymous as the hacker itself.

Creating a sense of urgency the hacker will request a payment that increases over time. For example, a victim may at first be offered the decryption key for a payment of $300 in Bitcoins if paid within 48 hours of infection. The amount increases to $600 in Bitcoins after 72 hours; possibly $900 after 96 hours; and no deal after 120 hours.

Since both computer viruses and ransomware are malware and require user interaction to deliver their damaging payloads, the same preventative measures apply. I classify risk mitigation strategies into two areas: systems administration, and end-user security awareness training.

From a systems management perspective, the updating of the operating system software is essential. In the case of the WannaCry attack, Microsoft issued a patch in March (MS17-010). Had the patch been applied, it would have removed the vulnerability, and the exploit would not have worked. Those whose systems were infected have learned a valuable lesson to keep their system software, in fact, all software, current.

Malware protection is also vital to any cyber defence strategy. Do you want to rely on the free software and hope it is updated, or do you want to sleep better knowing a company’s business model is dependent on the accountability of their product? The choice is yours but as my grandfather used to say, 'There ain’t no free lunch'. The investment will pay for itself in the long run as long as the software is kept up-to-date and monitored.

An often neglected systems administration mitigation strategy is limiting administrative rights. In other words, end-users should not have rights allowing them to install software on their computers. When malware hits a system, it will inherit the rights of the end-user affected. In other words, if you have administrative rights and get an infection, then your malware will also have administrative rights.

Although limiting end-user rights does not appear to have been necessary for the WannaCry attack, it is a best practice. Users should only have the rights and access to their computers they need to fulfill their duties.

Of equal importance are the availability of data backups. Backups should be off-line and off-site to avoid infection and physical risks. Restoring yesterday’s backup may only start the cycle over again as the infection may have taken place weeks ago. A hybrid strategy of regular daily, weekly, monthly, quarterly and annual backups with separate critical data backups focusing on the enterprise’s core digital assets could come in handy if a quick recovery is necessary. Considering the relatively cheap cost of storage, especially cloud storage, versus the potential loss of date, extra storage is cheap by comparison.

When it comes to the end-users, let’s be frank: there is no patch for human gullibility. Security awareness training for all employees, contractors, and temps is a must. Everyone needs to understand their part in the information security strategy. An ongoing security awareness program should also be initiated to reiterate the enterprise’s commitment to information security and reminding users of their individual responsibilities. Every end-user should have end-user training so they can identify phishing emails and potential malware attacks such as the WannaCry virus. The training should reiterate a culture where an abundance of caution is the norm.

When an email arrives, the end users should instinctively question:

- Does the end-user know the sender? Is it a trusted source? Has the end-user checked the actual email address? It is unlikely for you to receive official email through a Gmail or Yahoo account and these are often used by hackers to deliver their wares.
- Is the email related to the end user’s responsibilities? It is often acceptable office culture to send links to funny videos or jokes. Best to save these for smartphones and sending by way of SMS.
- Does the subject of the email look legitimate? Hackers might add the target’s email address or company in the subject to fake authenticity. They might also spoof from a senior manager demanding immediate action to entice the end-user to react and click.
- Does the email suggest or request action be taken? Any email with little content and a link asking the user to click should immediately be suspicious.
- Does the email contain attachments? Why would anyone send a .exe, .vbs, or .com file? If the email contains unknown attachments, chances are the malware is in the attachment or link. It is never wrong to question and call the sender to verify their email.
- Finally, how are the spelling and grammar? Does it dip below ‘normal’ spelling and grammatical errors? If the spelling errors are above average, chances are this, not a valid email.

The battle against malware, ransomware, and hackers require vigilance. Best practices in systems administration, the development of emergency response procedures, and practice of disaster recovery procedures are vital but secondary to end-user security awareness training. Prevention is better than the cure, and the promotion of an information security-aware culture in your organisation is the first step in winning this battle.

If you find yourself the victim of ransomware, the question to pay or not to pay is a risky one. In some cases, you will, and the hacker will send you the decryption key. In others, you will not receive anything. There is a trend encouraging victims not to pay. The fact is, you are dealing with a criminal and why should you trust them?

Should you choose not to pay, I advise making an image of your encrypted drive and storing it. One day, someone could post at decryption key or software crack to break the ransomware.

The Dutch police have done just that. Partnering with Europol and others, they have created a website to help victims of ransomware, No More Ransom, and have already published decryption solutions for past ransomware attacks.

The challenge against hackers is ongoing. It is the nature of hacking to be one step ahead of information security professionals. By adopting best practices, information security awareness training, and fostering a security awareness cultures, businesses can make it difficult for the hackers, so they lose interest and move on to the less protected.

Image

Image