The OSI Reference Model

As many networking tutorials do, this one begins with an introduction to the Open Systems Interconnection (OSI) Reference Model (OSI Model). The OSI model is a layered, abstract description for communication and computer network protocol design, developed as part of the Open Systems Interconnection initiative. It is also called the OSI 7-layer model.

BUST 5

Purpose

The OSI model divides the functions of a protocol into a series of layers. Each layer has the property that it only uses the functions of the layer directly below, and only exports functionality to the layer directly above. A system that implements protocol behavior consisting of a series of these layers is known as a protocol stack or simply stack. Protocol stacks can be implemented either in hardware or software, or a mixture of both. Typically, only the lower layers are implemented in hardware, with the higher layers being implemented in software.

Application Layer

The application layer provides a means for the user to access information on the network through an application. This layer is the main interface for users to interact with the application and therefore the network.

Presentation Layer

The presentation layer transforms data to provide a standard interface for the application layer. Encoding, data compression, data encryption and similar manipulation of the presentation is done at this layer to present the data as a service or protocol developer sees fit.

BUST 6

Session Layer

The session layer controls the connections (sessions) between computers. It establishes, manages and terminates the connections between the local and remote application.

Transport Layer

The transport layer provides transparent transfer of data between end users, thus relieving the upper layers from transfer concerns while providing reliable data transfer. The transport layer controls the reliability of a given link through flow control, segmentation/desegmentation, and error control.

Network Layer

The network layer provides the means of transferring data sequences from a source to a destination by using one or more networks while maintaining the quality of service requested by the Transport layer. The Network layer performs network routing functions, and might also perform segmentation/de-segmentation, and report delivery errors.

Data Link Layer

The data link layer provides the means to transfer data between network entities and to detect and possibly correct errors that may occur in the Physical layer. It arranges bits from the physical layer into logical chunks of data, known as frames.

Physical Layer

The physical layer defines all the electrical and physical specifications for devices. This includes the layout of pins, voltages, and cable specifications.

Five things you need to know about CryptoLocker

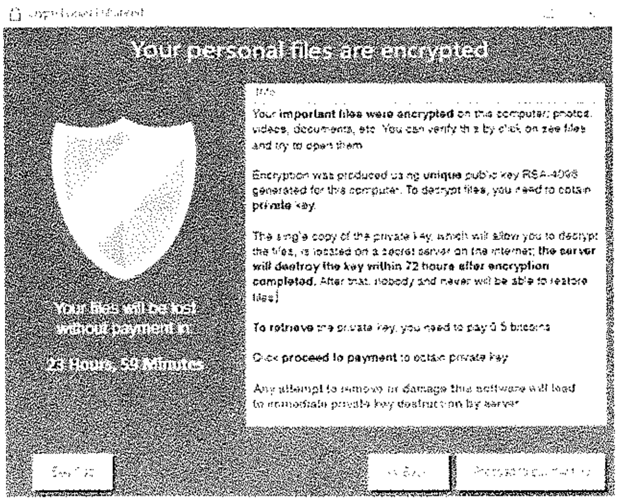
1 CRYPTOLOCKER: A BRIEF HISTORY IN CYBERCRIME

Ransomware attacks have been occurring for more than a decade, but it's been in the last few years that we've seen large-scale attacks. Computer security experts have theorized that the rise in this type of attack is due to its higher rate of success versus other cybercrimes that have become more difficult. Plus, these days, the software for ransomware is cheap and readily available—perpetrators need only malicious intent to carry out an attack. No coding required!

Once infected with ransomware, victims have two choices: either pay the ransom or permanently lose access to their files. The malware used to encrypt files can be difficult to defend against, and the encryption in most cases can't be broken.

Ransomware has become attractive to criminals, because they know that many individuals and companies have incomplete data backups—or no backup at all—and, thus, are likely to pay the ransom to recover their files. The criminals have generally kept their ransom demands low, opting for figures that were: a) likely to be paid; and b) not likely to be investigated by law enforcement.

BUSTA 1



Your personal files are encrypted

Info

Your **important files were encrypted** on this computer: photos, videos, documents, etc. You can verify this by click on see files and try to open them.

Encryption was produced using **unique** public key RSA-4096 generated for this computer. To decrypt files, you need to obtain **private** key.

The single copy of the private key, which will allow you to decrypt the files, is located on a secret server on the internet; **the server will destroy the key within 72 hours after encryption completed.** After that, nobody and never will be able to restore files!

To retrieve the private key, you need to pay 0.5 bitcoins

Click **proceed to payment** to obtain private key

Any attempt to remove or damage this software will lead to immediate private key destruction by server

Your files will be lost without payment in:

23 Hours, 59 Minutes

Once a user has opened a file infected with CryptoLocker, the ransomware encrypts files on the user's system and demands payment, within a set timeframe, in order to unlock the files.

Many have paid the ransom; even the FBI, in some instances, advised companies to "just pay the ransom." Unfortunately, paying the attackers off is a strategy that encourages the expansion of such extortion schemes. Furthermore, there's no guarantee that the files will be decrypted once the ransom has been paid.

In 2014, CryptoLocker malware was largely neutralized by Operation Tovar, an international collaboration of security companies and law enforcement, that successfully shut down the command and control centers and the GameOver Zeus botnets that drove the ransomware.

However, the scourge of ransomware is far from over. CryptoLocker, as a result of its success, spawned a slew of copycats. According to the Cyber Threat Alliance, they promise to wreak havoc in 2016.

BUSTA 2