Issued 8/17/17

Two Dangerous Ransomwares Are Back – Protect Your Computers

Ransomware has been around for a few years but has become an albatross around everyone's neck—from big businesses and financial institutions to hospitals and individuals worldwide—with cyber criminals making millions of dollars.

In just past few months, we saw a scary strain of ransomware attacks including WannaCry, Petya and LeakerLocker, which made chaos worldwide by shutting down hospitals, vehicle manufacturing, telecommunications, banks and many businesses.

Before WannaCry and Petya, the infamous Mamba full-disk-encrypting ransomware and the Locky ransomware had made chaos across the world last year, and the bad news is—they are back with their new and more damaging variants than ever before.

This time security researchers have discovered a fresh spam malware campaign distributing a new variant of Locky known as Diablo6 and targeting computers around the world, with the United States being the most targeted country, followed by Austria.

An independent security researcher using online alias Racco42 first spotted the new Locky variant that encrypts files on infected computers and appends the .diablo6 file extension.

Like usually, the ransomware variant comes in an email containing a Microsoft Word file as an attachment, which when opened, a VBS Downloader script is executed that then attempts to download the Locky Diablo6 payload from a remote file server.

The ransomware then encrypts the files using RSA-2048 key (AES CBC 256-bit encryption algorithm) on the infected computer before displaying a message that instructs victims to download and install Tor browser; and visit the attacker's site for further instructions and payments.

This Locky Diablo6 variant demands a sum of 0.49 Bitcoin (over $2,079) from victims to get their files back.

Unfortunately, at this time it is impossible to recover the files encrypted by the .Diablo6 extension, so users need to exercise caution while opening email attachments.

Although it's not clear how the ransomware initially finds its way into a corporate network, researchers believe like most ransomware variants, Mamba might be using either an exploit kit on compromised or malicious sites or malicious attachments sent via an email.

The ransom note does not immediately demand money, rather the message displayed on the infected screen only claims that the victim's hard drive has been encrypted and offers two email addresses and a unique ID number to recover the key.

Here's How to Protect Yourself From Ransomware Attacks

Ransomware has become one of the largest threats to both individuals and enterprises with the last few months happening several widespread ransomware outbreaks.

Currently, there is no decryptor available to decrypt data locked by Mamba and Locky as well, so users are strongly advised to follow prevention measures in order to protect themselves.

Beware of Phishing emails: Always be suspicious of uninvited documents sent over an email and never click on links inside those documents unless verifying the source.

Backup Regularly: To always have a tight grip on all your important files and documents, keep a good backup routine in place that makes their copies to an external storage device that is not always connected to your PC.

Keep your Antivirus software and system Up-to-date: Always keep your antivirus software and systems updated to protect against latest threats.