Army Vision: By 2028, a world-class Army that is a source of national pride.

H E A D Q U A R T E R S
P H I L I P P I N E A R M Y
OFFICE OF THE ASSISTANT CHIEF OF STAFF FOR
COMMAND AND CONTROL COMMUNICATIONS, AND CYBER SYSTEMS, G6
Fort Andres Bonifacio, Metro Manila

6/CMB 20 January 2017

CYBERSECURITY BULLETIN

Cybersecurity Bulletin: #17-04

RANSOMWARE
WHEN CYBERCRIMINALS HOLD YOUR COMPUTER HOSTAGE

Ransomware is a form of malware that will lock files on a computer using encryption. Encryption converts files into another format, like a secret code and can only be decoded by a specific decryption key.

Types of Ransomware

Ransomware can present itself in two forms.

1. **Locker ransomware** will encrypt the whole hard drive of the computer, essentially locking the user out of the entire system.

2. **Crypto ransomware** will only encrypt specific, seemingly important files on the computer, such as word documents, PDFs and image files.

Once the ransomware installs itself, it will display a warning message, usually from the FBI or other government agency, notifying the user that illegal content has been found and that the computer is now locked. The user is given a specific amount of money to pay as a "fine" and a timeframe in which to pay. The scammer then requests that the payment be made with cryptocurrencies such as Bitcoin or MoneyPak, due to the anonymity of these payment systems. If the user does not pay, the cybercriminal will destroy the decryption key and the users' data will be locked forever.

This is an extremely serious threat as there are not many ways to fix the situation once infected. There is no way to decrypt files without the original decryption key.

How is Ransomware Distributed?

Ransomware is generally delivered via phishing emails or through exploit kits. The phishing emails contain malicious attachments, which include the ransomware or will sometimes provide links directing the user to a compromised webpage hosting the malware. Exploit kits are a malicious tool that hackers use to look for security holes in software that has not been updated. Once the security vulnerability has been found, the attacker can then deliver the ransomware to the computer.

How Can I Protect Myself?

The best protection against this threat is to be proactive in your own cyber defense. Since this particular malware is so complicated in nature, it is recommended that you use multiple layers of protection against this threat.

Don't Pay The Ransom

It may seem like the easy way out, but there's no guarantee that you will actually get your files back if you pay. At the very least, you're just helping fund the criminals for their next attack.

Educate Yourself

Familiarize yourself with phishing attacks. Learn the red flags to be on the lookout for, and never, ever open attachments or click on links from unknown senders.

Update Early, Update Often

Whenever you receive a notification on your computer that there are new software updates available- do it now! These will patch any newly discovered security vulnerabilities.

Back It Up Or Lose It All

The best way to recover compromised or damaged data is by doing regular, thorough backups. Yes, it is a cumbersome task, but imagine how much worse it would be if your computer became locked up with ransomware? One important thing to note

about your backup drive- once you have completed your backup, unplug the drive from the computer. If it is not unplugged when the malware is executed, there's a good chance that the ransomware will make its way to the external drive and lock that as well.

Use Internet Security Software

Use a good Internet security solution to prevent the ransomware from being installed on the computer in the first place.

Reference:

This was cross posted from:

https://community.norton.com/en/blogs/norton-protection-blog/ransomware-when-cybercriminals-hold-your-computer-hostage

DO YOU WANT TO KNOW MORE? TALK TO US.

POC: LTC JOEY T FONTIVEROS (SC) PA – Chief, Cyberspace Management Branch, OG6, PA at Landline Telephone Nr: 02-845-9555 Local 6630 and Mobile Telephone Nr: 0917-6281057. Email: fontiverosjt@army.mil.ph.