Advanced Notification of WannaCry Ransomware

Security Advisory AE-Advisory 17-29

Criticality Critical 

Advisory Released On 13 May 2017

CVE Reference ID

NA

Impact

Encrypt and locks all the data on a computer system which make it inaccessible user.

Summary

As the leading trusted secure cyber coordination center in the region, aeCERT has researched and found out about new variant of Ransomware known as WannaCry Ransomware. WannaCry Ransomware also known as Wanna Decryptor, WannaCry or wcry, is a specific ransomware program that locks all the data on a computer system and leaves the user with only two files: instructions on what to do next and the Wanna Decryptor program itself.

When the software is opened it tells computer users that their files have been encryted, and gives them a few days to pay up, warning that their files will otherwise be deleted. It demands payment in Bitcoin, gives instructions on how to buy it, and provides a Bitcoin address to send it to.

About Ransomware

What is Ransomware?

Malicious software that locks a device, such as a computer, tablet or smartphone and then demands a ransom to unlock it

Where did Ransomware originate?

The first documented case appeared in 2005 in the United States, but quickly spread around the world.

How does it affect a computer?

The software is normally contained within an attachment to an email that masquerades as something innocent. Once opened it encrypts the hard drive, making it impossible to access or retrieve anything stored on there – such as photographs, documents or music

How can you protect yourself ?

Anti-virus software can protect your machine, although cybercriminals are constantly working on new ways to override such protection. However the below best practices will helps in reducing the risk of being infected by the malware.

- Keep software up to date
- Installing software updates for your operating system and programs is critical. Always install the latest security updates for your devices:
- Turn on Automatic Updates for your operating system.
- Use web browsers such as Chrome or Firefox that receive frequent, automatic security updates.
- Make sure to keep browser plug-ins (Flash, Java, etc.) up to date.
- Avoid visiting untrusted or malicious site that could be infected.
- Avoid Phishing scams and don't open or click on any suspicious links or emails.

Contact Us

aeCERT
P.O. Box 116688
Dubai, United Arab Emirates

Tel (+971) 4 230 0003
Fax (+971) 4 230 0100
Email info[at]aeCERT.ae

For secure communications with aeCERT with regards to sensitive or vulnerability information please send your correspondences to aeCERT[at]aeCERT.ae