Advanced Notification of Cyber Threats against Abuse of .MSI Windows Installer

aeCERT Computer Emergency Response Team
فريق الاستجابة لطوارئ الحاسب الآلي

Security Advisory	ADV-19-12	**Criticality**	High	
Advisory Released On	02 May 2019			

Impact

Abuse of custom actions in Windows Installer .MSI to execute malicious JavaScript, VBScript, and PowerShell Scripts in order to bypass security.

Recommendations

Adhere the advices written under the recommendations section.

Affected Platforms

- Windows Installer .MSI

Summary

As the leading trusted secure cyber coordination center in the region, aeCERT has researched and found about a newly discovered threat targeting Windows Installer .MSI files. Threat actors are abusing .MSI files to install malicious JavaScript, VBScript, and PowerShell Scripts in Windows Installer .MSI files. Use cases of the abusage in .MSI files included shutting-down a targeted system. Some of the systems that are being targeted are financial systems that are located in various areas. The current noticed behavior to spread the .MSI files occurs through the use of spam emails and leveraging external servers to download the files, such as Amazonaws. The downloaded files in this case include a malware under the name of Jesus or dump. The attack happens after a user downloads an attachment that has been linked to a spam email.

Threat Details

Windows Installer is a software that uses MSI files in order to install and remove programs from a specific computer. A recent vulnerability has been identified whereby a hacker could bypass security measures and execute malicious scripts through the use of the custom actions that these files have. Threat actors are currently leveraging emails and external servers to distribute the attack. The exploit takes place after a .MSI file has been downloaded from spam email. An archived file would be downloaded that contains dump.msi, dump.exe, libeay32.dll, ssleay32.dll, ssleay64.dll or borlndmm.dll files, which can sometimes be encrypted. The file would then prompt the browser to open and redirects it to adobe[.]com[.]br. The malicious script also creates autorun for dump.msi and results in a complete shutdown of the computer. Evidently, the dump.msi file will execute the dump.exe file. The .MSI files that have been attached to spam emails disguise as Adobe Acrobat Reader DC and redirect users to a Portuguese website. The text file names are under desktop.txt, desktop, or desktop.ini.

The malware could come in a JavaScript code which accesses the URL https[:]//s3-eu-west-1[.]amazonaws[.]com/{random characters}/image2[.]png in order to download the malicious file. The file that has been downloaded could be stored in any of the following folders:

- %User Startup %\
- %User Profile%\Saved Games
- %User Profile%\Contacts
- %User Profile%\Links
- %User Profile%\Music

The spam emails that have a malicious file attached consist of texts that is written in Portuguese and advises the recipient to open the attachment as it claims that it is an urgent announcement. According to TrendMicro, the .zip file that is attached to the email

is under the name “Fatur432952-532-674.zip” which gets downloaded from a malicious URL.

IOC

For a full list of the IoCs, please refer to the following link:

https://fs.aecert.ae/index.php/s/NL6Z8ZC7Fb9fPBs

Solution

In order to circumvent the exploit, we highly recommend the following:

- Apply restriction to disable installing .MSI files.
- Apply restrictions so installation privilege should be permitted to specified users only.
- Avoid installation of unknown files / programs.
- Where it is not possible to apply restrictions then advise users to avoid installation of unknown files and .MSI files.
- Advise users to beware of phishing attempts, avoid clicking on unknown URLs as they may redirect to a malicious URL.
- Ensure your computer and end-point protection is always up to date with the latest security patches.

References

Trend Micro (Article, Analysis)

Contact Us

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

Tel (+971) 4 777 4003
Fax (+971) 4 777 4100
Email info[at]aeCERT.ae
Instagram @TheUAETRA
Twitter @TheUAETRA

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