Advanced Notification of Eavesdropping Malware Discovered Gathering Audio Data in Ukraine

Security Advisory AE-Advisory 17-11

Criticality Critical

Advisory Released On 20 February 2017

Impact

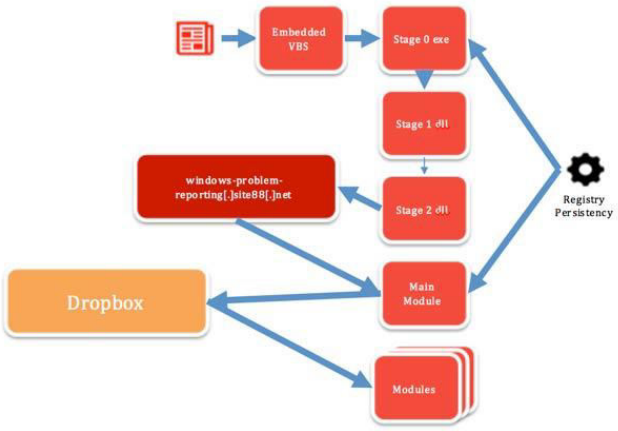
Turns onboard microphones to gather audio files which then exports it to Dropbox files and sent to a C&C server

Solution

Refer to the “Solution” section below

Summary

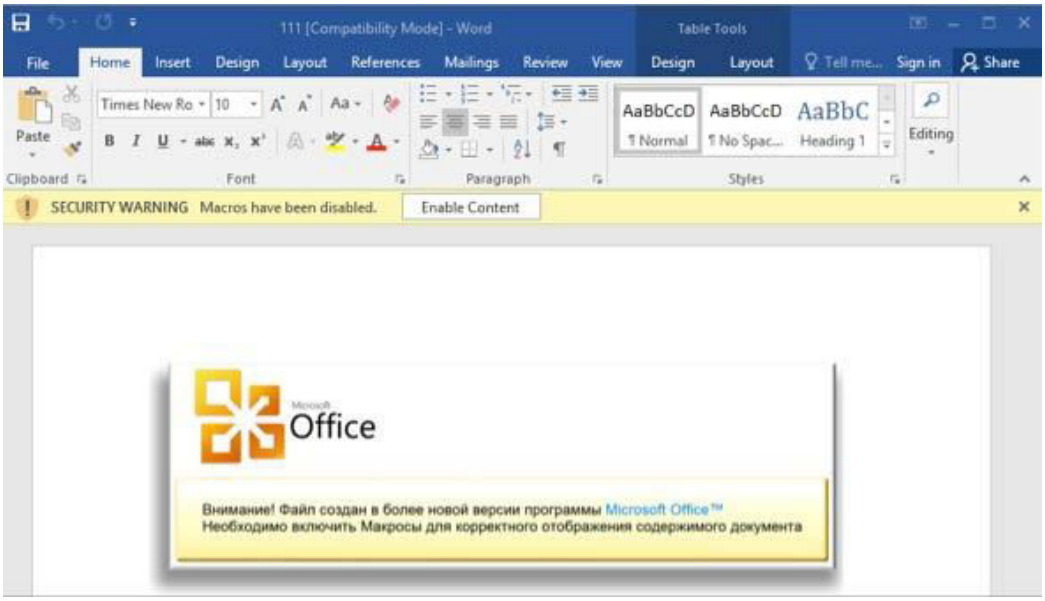
aeCERT has researched and found out about a new malware called "Operation BugDrop". This malware stealthily infects computers and turns on the onboard microphone to gather audio files, which it exports to Dropbox files for retrieval and analysis. Operation BugDrop is designed to sit quietly on computers throughout an organization and record everything heard by the microphone built into or attached to a computer. Every day the BugDrop malware sends the sound files to a Dropbox file, where it’s uploaded to the hackers for further analysis. Once the BugDrop malware infects an organization, it effectively turns every computer into a bug that in some ways is far more effective than if intelligence operatives had actually planted bugs in the same offices.



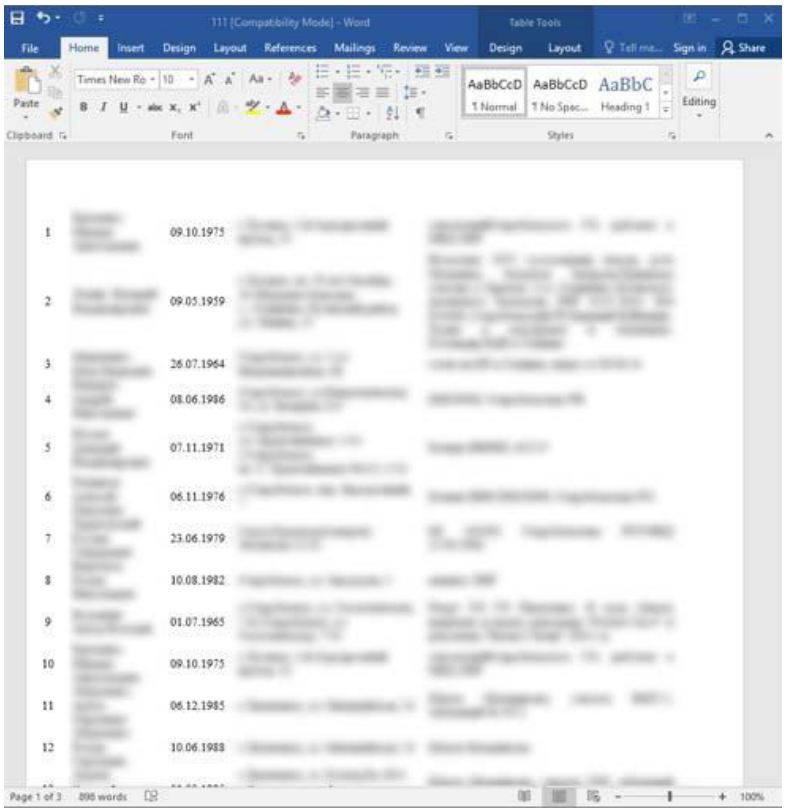
Threat Details

Infection Method

Users are targeted via specially crafted phishing emails and are prompted to open a Microsoft Word decoy document containing malicious macros. If macros are disabled, then the users are presented with a dialog box like the one in the image below prompting them to enable macros. The dialog box is designed to appear like an authentic Microsoft Office message.



The text in the image above is in Russian and translates to, "Attention! The file was created in a newer version of Microsoft Office programs. You must enable macros to correctly display the contents of a document.”. The document itself shows a list of military personnel with personal details such as birthdate and address like in the image below:



Main Downloader

Once the document has been opened, the main downloader is extracted from it via a malicious VB script that runs it from the temp folder in Microsoft Windows. At the time of this vulnerability's discovery, the downloader has low detection rates in anti-viruses.

Dropper - Stage 0

The icon for the downloader executable file was found on a Russian social media website, the icon is what is known as a "meme" in internet terms meaning a picture that is typically humorous and shared rapidly by internet users. The meme icon is a joke about Ukrainians.

The dropper has 2 DLLs stored in its resources, they are XOR'ed (XOR is an encryption algorithm) in such way that the current byte is XOR'ed with the previous byte.
This technique is much better than just plain XOR because it results in a byte distribution that doesn't look like a normal Portable Executable (PE) file loader. This is a way that hackers use to help obfuscate the file so that it will not be detected by anti-virus systems.

The DLLs are extracted into the app data folder:

- %USERPROFILE%\AppData\Roaming\Microsoft\VSA\.nlp – Stage 1
- %USERPROFILE%\AppData\Roaming\Microsoft\Protect\.nlp.hist – Stage 2

The first stage is executed and the DLL is loaded using Reflective DLL injection which is a library injection technique in which the concept of reflective programming is implemented to perform the loading of a library from memory into a host process.

Dropper - Stage 1

- Internal name: loadCryptRunner.dll
- Responsible for persistency and executing the downloader DLL, the Stage 1 Dropper registers itself in the registry under the key:
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\drvpath
- RUNDLL32 “%USERPROFILE%\AppData\Roaming\Microsoft\VSA\klnihw22.nlp”, RUNNER
- The communication DLL is also loaded using Reflective DLL Injection

Dropper - Stage 2 - Downloader for Main Module

- Internal name: esmina.dll
- The main purpose of this DLL is to download the main module
- The main module is hosted on a free web hosting site on a given URL.

- It appear as if downloading the module requires manual approval, indicating the need for a human analyst or handler in the loop.
- The main module is then downloaded and loaded into memory using Reflective DLL Injection.

Main Module

- The main module downloads the various data-stealing plugins assigned to each victim, and executes them.
- It also collects locally-stored stolen data and uploads it to Dropbox.
- The main module incorporates a number of anti-Reverse Engineering (RE) techniques:
- Checks if a debugger is present.
- Checks if process is running in a virtualized environment.
- Checks if ProcessExplorer is running. ProcessExplorer is used to identify malware hiding inside a legitimate process as a DLL, which occurs as a result of DLL injection.
- Checks to see if WireShark is running. WireShark can be used to identify malicious traffic originating on your computer.
- It registers itself in the registry under the key:
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\hlpAsist
- RUNDLL32 “%USERPROFILE%\AppData\Roaming\Microsoft\MSDN\iodonk18.dll”, IDLE

Solution

- The best way to determine whether a network has been compromised is to monitor the outgoing traffic for large amounts of data uploaded to Dropbox.
- Do not open any malicious attachments or unknown URLs.

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