Advanced Notification of Cyber Threats against Weaponized Remote Desktop Viewers

aeCERT
فريق الاستجابة لطوارئ الحاسب الآلي
Computer Emergency Response Team

Security Advisory	ADV-19-15	**Criticality**	High	○○○●
Advisory Released On	7 May 2019			

Impact

A vulnerability in Remote Desktop viewers that could be exploited in aims to obtain critical and sensitive data.

Solution

Adhere the advices written under the recommendations section.

Summary

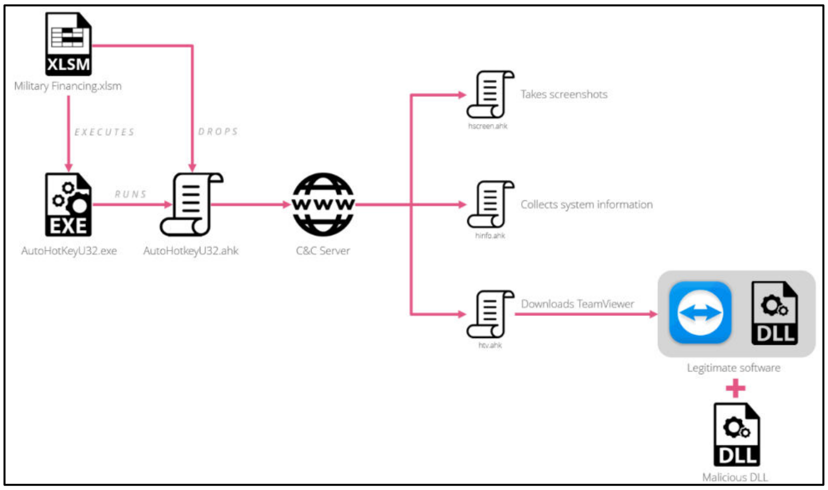
As the leading trusted secure cyber coordination center in the region, aeCERT has researched and found out about a critical vulnerability in a remote desktop viewing software. A modified version of TeamViewer side-loaded using malicious DLLs has been used to compromise government network systems, which is sent as spam email under the guise of “Military Financing Program”. Once the document in the email is opened, the macro extracts an AHK program and a script that communicates with a C&C server to download and execute the malicious scripts.

Details

TeamViewer is one of the most well-known Remote Desktop Viewing softwares – along with LogMeIn and AnyDesk. These types of softwares are in use for desktop sharing, online meetings, conferencing, and file transfer between computers. After examining the infection chain, it has been concluded that the tools used to develop the malicious script were carried out by a Russian hacker.

The first phase of the infection chain begins with a spam email sent which contains the subject “Military Financing Program”, along with a malicious XLSM document attached. The XLSM document itself has embedded macros.

The infection chain is illustrated as follows:



Once the document in the email is opened and the macro is enabled, an AHK program (AutoHotkeyU32.exe) and an AHK script (AutoHotkeyU32.ahk) are executed. The AHK script then communicates with the C&C server and downloads three additional scripts:

1. **hscreen.ahk**: takes a screenshot of the PC of the victim and uploads it to the C&C server.
2. **hinfo.ahk**: sends the login credentials and PC information to the C&C server.
3. **htv.ahk**: downloads a modified version of TeamViewer, executes it, and sends the login credentials to the C&C server.

In addition, the modified TeamViewer DLL is loaded via DLL side-loading, which adds modified functionalities such as:

1. Hiding the TeamViewer interface so that the victim would not know it is running.
2. Logging the credentials of the TeamViewer session to a text file.
3. Allowing the attacker to transfer and execute further EXE or DLL files.

The countries targeted in this attack include Nepal, Guyana, Kenya, Italy, Liberia, Bermuda, Lebanon public financial sector and government officials.

IOC

A list of the indicators of compromise are as follows:

DLLs

013e87b874477fcad54ada4fa0a274a2

799AB035023B655506C0D565996579B5

e1167cb7f3735d4edec5f7219cea64ef

6cc0218d2b93a243721b088f177d8e8f

aad0d93a570e6230f843dcdf20041e1e

1e741ebc08af09edc69f017e170b9852

c6ae889f3bee42cc19a728ba66fa3d99

1675cdec4c0ff49993a1fcbdfad85e56

72de32fa52cc2fab2b0584c26657820f

44038b936667f6ce2333af80086f877f

Documents

4acf624ad87609d476180ecc4c96c355

4dbe9dbfb53438d9ce410535355cd973

C&Cs

1c-ru[.]net/check/license

intersys32[.]com/3307/

146.0.72[.]180/3307/

146.0.72[.]180/newcpanel_gate/gate.php

185.70.186[.]145/gate.php

185.70.186[.]145/index.php

193.109.69[.]5/3307/gate.php

193.109.69[.]5/9125/gate.php

Solution

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

- Avoid opening emails with attachments from unknown sources.
- In the off-chance that the attachment is downloaded, ensure that macros embedded in XLSM documents are disabled.

References

Checkpoint

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