COMSEC Consulting UK
Information Security

News Brief: Flame Worm

Background

On Monday, 28.5.12 a new worm, known as Flame and Skywiper, was discovered as being prominent in the Middle East. This is the first document by **Comsec Consulting** which describes the abilities of the newly-discovered worm, as well as ways to check if the worm has infected your environment.

Initial Findings

The worm **gathers data** from the computer using different methods:

a. Key Logging – saving the key strokes.
b. Taking screenshots.
c. Activating the microphone and setting to record.
d. Gathering information from documents and images on the computer.

The worm **spreads** itself via several infection vectors:

a. Using existing exploits (MS10-061 and MS-10-041).
b. Using user credentials to attack other computers.
c. Spreading through removable media devices (such as USB).
d. There is also an unverified assumption that the worm uses 0-day exploits.

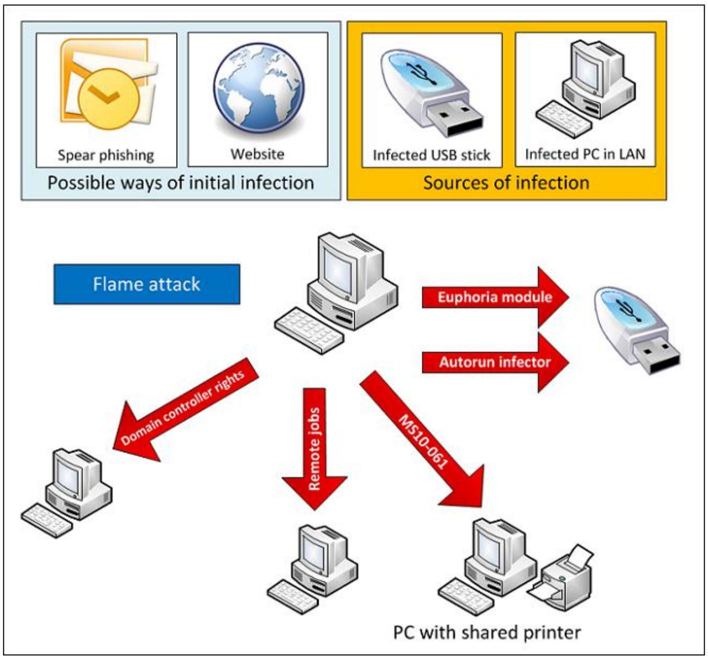


Figure 1: The method used by the Flame Worm to spread.

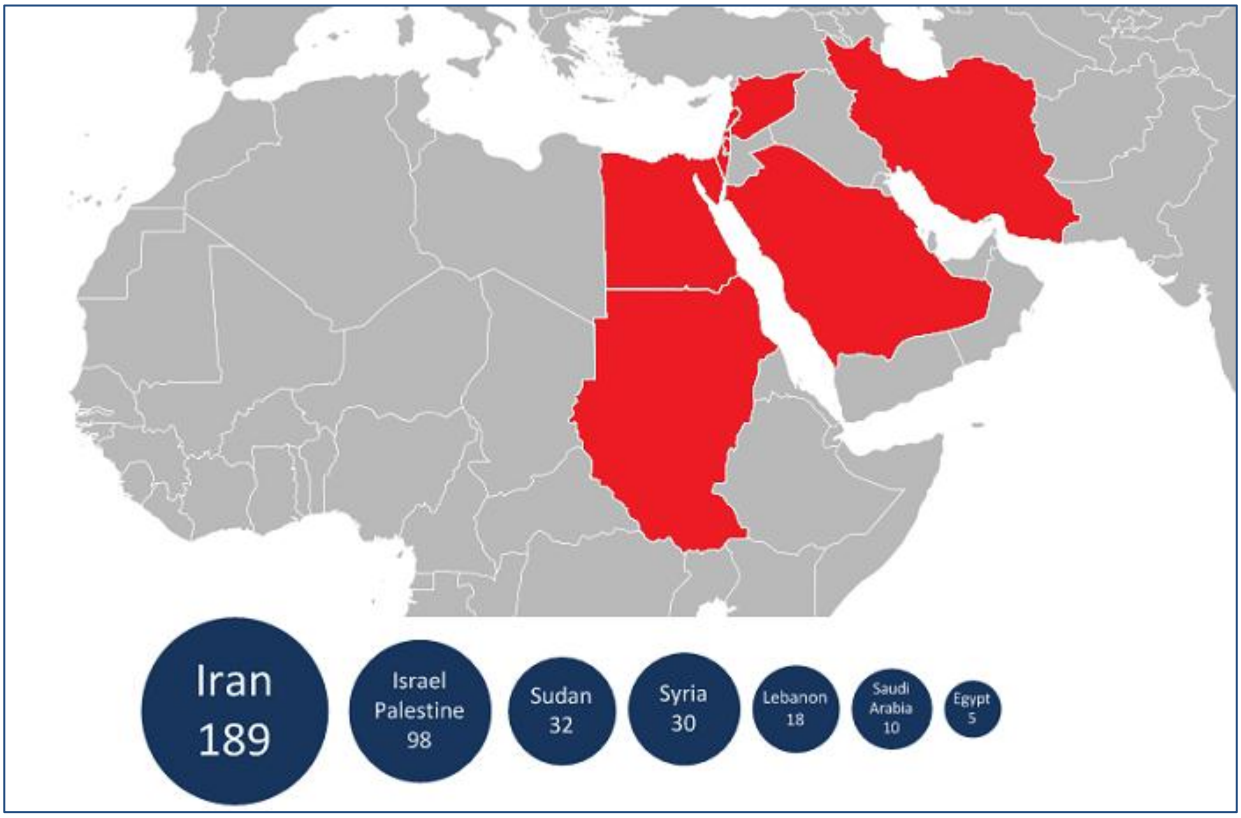


Figure 2: The current dispersion of the worm (data from Kaspersky)

Identifying the Worm

1. **Registry** – The worm uses the LSA Authentication Packages method for start-up. As a result, the data **mssecmgr** is added to the following registry key:

   HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\Authenticatio Packages.

2. **Files** – The worm uses several files. The existence of each might indicate the presence of the worm. The file extension could be either ocx or sys:

   - %windir%\system32\mssecmgr.ocx
   - %windir%\system32\advnetcfg.ocx
   - %windir%\system32\ccalc32.sys
   - %windir%\system32\msglu32.ocx
   - %windir%\system32\nteps32.ocx
   - %windir%\system32\boot32drv.sys
   - %windir%\system32\soapr32.ocx

3. **Network** - The worm communicates by browsing to Command and Control servers that are on the web. At this time there is no published address or domain list. However, if there has been a request to one of the following URLs: wp-content/rss.php or cgi-big/counter.cgi, one can conclude that an infection is present. Please note that the absence of this pattern is not evidence that the worm does not exist on your network.

Recommendations

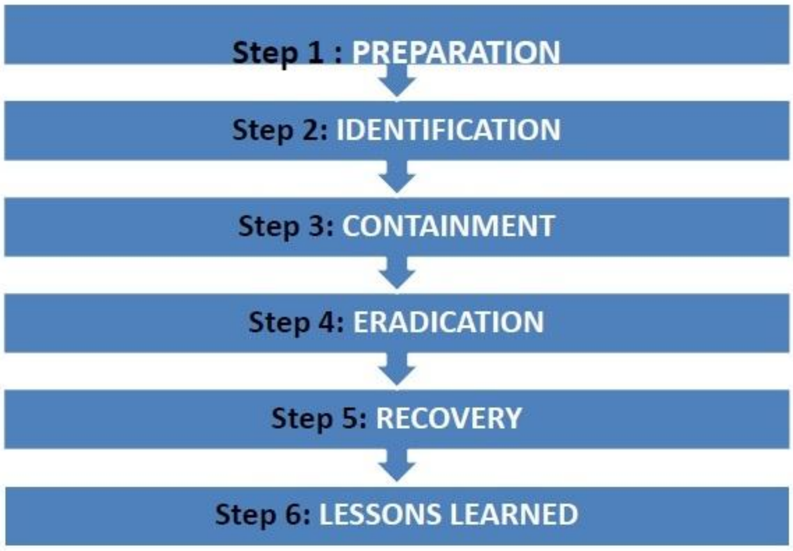
1. Use the HOST signature as described above in order to allocate the existence of the worm in the network.

2. Update all computers in the network with Microsoft patches, in Particular MS10-061 and MS10-046 which are known ways for the worm to spread itself.

3. Should you identify the worm on your network, it is recommended to initiate your organisation's internal procedure to identify, isolate and mitigate against the threat, and to make an assessment of the potential damage.

4. **Comsec will be happy to assist with any question you may have:** Comsec Consulting UK - 0207 268 3050.

The flow chart below describes the Incident Response actions we recommend following:



References

Symantec:	http://www.symantec.com/connect/blogs/flamer-highly-sophisticated-and-discreet-threat-targets-middle-east
Kaspersky:	http://www.securelist.com/en/blog?weblogid=208193522
CrySys Lab:	http://www.crysys.hu/skywiper/skywiper.pdf