## Tools used

The following table outlines the tools used.

|  |  |  |  |
| --- | --- | --- | --- |
| Tool Name | Usage | Static/Dynamic | URL |
| Flare VM | VM script used to download and install all tools on a Windows VM | Static | <https://www.fireeye.com/services/freeware/flare-vm.html> |
| Trid (Tridnet) | Identify information on executable | Static | <https://mark0.net/soft-trid-e.html> |
| CFF Explorer | Portable Executable (PE) information and debuggers | Static | <https://ntcore.com/?page_id=388> |
| ExePEInfo | Used to see if executable is compressed | Static | <http://www.exeinfo.byethost18.com/?i=1> |
| Bintext | Exports all strings found in a file | Static | <https://www.aldeid.com/wiki/BinText> |
| Xorsearch | Used to search for encrypted text in the file | Static | <https://blog.didierstevens.com/programs/xorsearch/> |
| PE Studio | Portable Executable (PE) information and debuggers | Static | <https://www.winitor.com/> |
| HashCalc | Use to calculate different HASHs | Static | <https://www.slavasoft.com/hashcalc/> |
| Regshot | Used to create a snapshot of the VM | Dynamic | <https://github.com/Seabreg/Regshot> |
| Fakenet | Used to create a fake network to trap the malware calls | Dynamic | <https://github.com/mandiant/flare-fakenet-ng> |
| Wireshark | Used to review network captures | Dynamic | <https://www.wireshark.org/> |
| Procmon | Used to capture running process calls on the VM while Malware was running | Dynamic | <https://docs.microsoft.com/en-us/sysinternals/downloads/procmon> |
| Procdot | Review and document process captures | Dynamic | <https://www.procdot.com/> |

Table 1 Tools Used