Sr 2000hd Ace Loader [VERIFIED] Download

Download

Analysis of the Google API function Analysis of the module system allows us to notice that this anti-forensic module performs three actions: downloads payload code from URLs specified in the registry, creates and overwrites the system variables, and calls the executable. The first action consists of downloading the code from several addresses – %TEMP%, %DOCUMENTS% Reload the configuration settings, and the malicious modules will be downloaded again. The new module will be saved in %APPDATA%, but this time it will not be overwritten. Let’s look at what the module does on further loading. Initiating communications with the real C&C server As soon as the bot is complete with the initial communication with the C&C and downloads the Fabric Mod Loader, the bot attempts to download some modules from the server. Fabric uses a specific batch of modules, which is loaded only once (named msg) and shared with the Botnet. It is important that the server has at least one of this batch, that's why we chose msn.com. The data structure and the address format are hidden behind the interface MODULE=8#L0#0/O/TEXTS///OCODEINJ#3#0#0#0#10038&AML=&PACKTEXTS&PACKLEN= &PACKUID=&MODALGUID= &GUIDMOD=&MUID=&BIT=&IRIGHTS=0 &MAJORVERSION= &MINORVERSION= &COMMANDCHAR= &UNLOAD_LEN= &PACKTEXTS=8#L0#0/O/TEXTS///OCODEINJ#3#0#0#0#0# As you can see, the packet has three parts: = A unique identifier of the module (in this case it is 80f9b3f5c9422d8eacfc3f3cf55a4be9) = A unique identifier of the module inside the Fabric = A unique identifier of the module's GUID The first part of the packet data is a unique identifier of the module. We can calculate it from the parameters typically used during the communication with the C&C server - the version parameter tells us that this time around, we are dealing with a 4.0 version of Fabric. For Fabric, the number of versions available are divided by 1000 for each one from 1.0 till 4.0 (i.e. 4.0 = 4000). As you know, these modules are updated multiple times per day and you can be sure that each new version keeps all the modules we are talking about in our case. The best example is -1 version (i.e. Fabric 4.0), which - as we can guess - has a different configuration for the Botnet and thus a different set of modules to load. The next part of the packet is a unique identifier of the module inside Fabric. For our case, that means GUIDMOD. The last two parts of the packet are a couple of bytes containing the size of a Text struct used as a container of the module's Text data. So the full packet will look like:

Sr 2000hd Ace Loader Download

after the original sample was downloaded, its c&c was accessed via port 27000 which is the default port of download data and logs from the c&c. these logs were found with a set of windows commands and could be used to identify the original version. the sections i will use are the earliest, latest, queued, uploading and downloaded. file names and paths in these log entries has been picked from the replicated example which was seen after the original sample was deployed. updates are another main feature of this malware. the original sample has only one file, a stage#1 file, renamed to srchd.exe. this file simply unpacks the other loader which is called stage#2. stage#1 is a exe file which gives a different payload. so, updates can be seen as a relocation of the stage#2 loader. the updates and relocations can be identified by comparing data extracted from the c&c of the original sample and the original and new sample. a final feature of these malware is the automation. the original sample was active for a long time and it was often updated. we can identify updates by comparing the differences between the default and c&c logs which were extracted from the original and updated samples. the main difference is that the updates are not isolated anymore, but are connected to the c&c. a new log file with the name of the new version is created every time the c&c is re-submitted with a new update. for example, the first update in the original sample was released on 10/13/2015 and the stage#1.exe file was renamed to srchd.exe. later, the second update was released on 10/27/2015 which changed only the stage#2.exe file to sr2000hd. we will identify each change into a separate log entry. stage#2 is a set of two files - a core and exe file. 5ec8ef588b