SONY XCP DRM removal

By Kevin and Nancy McAleavey at nsclean.com

BEFORE you read this, it's important to note that we're EXTREMELY busy right now with far more serious issues than the media's attention to the "SONY ROOTKIT" phenomenon, and that handling panicked people over this has consumed huge amounts of our time already to the detriment of more important issues. As we near release of BOClean 4.20, all of our attention is focused on that right now. Emails regarding this issue or instant messages will have to wait until AFTER Thanksgiving. Therefore, should you respond to this offering, please don't be offended if I don't have time to respond to those at this time. I encourage further discussion and possible corrections of the advice offered below, but am not in a position to assist owing to far more pressing urgencies. I hope folks will understand the difficult situation that I'm in.

Having found some time to go back and play with the SONY rootkit has been difficult to come by, and our attorneys have been unable to obtain a definitive answer from the justice department as to our creating a specific solution to the SONY "rootkit" problem. However, I have been told that I have a right to my opinion, and as long as I express this as "my opinion" and not that of our company, (I did this on my own time) I should be free to share a chuckle with folks as to the pathetic nature of this "rootkit." And in doing so, I can explain WHY I think it's pathetic as well! So let's have at it, folks can learn from my rant to follow how to take care of this all by themselves! 

The "rootkit" indeed hides the uber-secret "sysfilesystem" folder, which is a subfolder of the WINNT (NT and 2000) or WINDOWS (XP) "SYSTEM32" folder. The rootkit sadly, is UNABLE to hide itself from being accessed directly from a COMMAND PROMPT (found in the start menu/programs/accessories list).

So for chuckles, I opened a COMMAND prompt. I then went (on an XP box, NT and Win2000 would be a WINNT rather than WINDOWS) ...

CD WINDOWS (enter)
CD SYSTEM32 (enter)
CD sysfilesystem (enter)

Low and behold, on a machine infected by this, I got a PROMPT with sysfilesystem present! (on an UNinfected machine, you'd get an error of "not found." Surprisingly, it let me HAVE it!) If this directory doesn't show, then you're NOT infected! You're finished right here. 

IF SYSFILESYSTEM exists, then the first thing we'll want to do is lose the "cloak" and that is a file called ARIES.SYS ... this command will get rid of it, you can successfully delete it while it's running. It's NOT protected! Heh. This command loses the cloak:

DEL ARIES.SYS (enter)

Once you've done this, REBOOT!

At THIS point, you have done what everyone else (including antiviruses, Microsoft and everyone else) is going to do as their FINAL solution - you have successfully "uncloaked" and prevented any further possible exploits of your system. Color it done unless you're brave enough to continue. In going further, a COMPLETE removal is necessary. Here's what I discovered ...

REMOVING THE REST OF SONY'S "TREAT"

After you've rebooted, some services (which are not really services) will run again, particularly the sysDRMServer. Trying NET STOP won't work as it's not REALLY a service. You'll get a system error. However, you can now SEE the files when you use the "My computer" file explorer and you'll be able to SEE the "sysfilesystem" folder now under the SYSTEM32 folder.

You should now be able to move to the formerly-hidden sysfilesystem folder and it should now be visible after the reboot.

BEFORE you do anything else, you now have to consider if you're brave enough to do manual registry editing, because if you remove anything else and don't clean up the registry, your CDROM and possibly your hard disk(s) *WILL* vanish if "crater.sys" and "syscor.sys" are removed. So if you're uncomfortable with registry editing, STOP NOW! You're DONE!!!

If you do the CD\WINDOWS, CD SYSTEM32, CD sysfileystem trick again, you will note that two things that weren't there before will now appear. Those are sysDRMServer and sysparking. LEAVE THEM ALONE! And there are MORE back in the SYSTEM32 folder. Leave THOSE sys*.* files alone for now ALSO!

The sysDRMServer.exe file will still be running and cannot be stopped without registry removal and another reboot. So ON to the next step(s) ...

NEXT STEP - REGISTRY CLEANING

Because the rootkit modifies registry permissions, a TEMPORARY trick needs to be applied in order to be successful.

FIRST ... run REGEDT32 (*NOT* REGEDIT) and navigate down to the HKEY_LOCAL_MACHINE key. RIGHT click it and select PERMISSIONS from the dropdown menu.

Click on "everyone" and make sure that FULL CONTROL is checked before proceeding. After you're done, be SURE to come back here and UNcheck it or your machine will be at risk. This elevated privilege is required in order to successfully edit and/or delete the remains, and it's CRUCIAL that you reset this after you're done!

Use the FIND item to locate anything that matches "sys" ... there's going to be a PILE of them all over the place, and failure to carry out this portion of it will cause drives to no longer work!

Using FIND, have it search for sys ... certain registry entries can simply be

deleted, certain ones must be EDITED, and here's where it gets tricky ...

First things you'll encounter are under the HKEY_LOCAL_MACHINE files, under the SOFTWARE key ... you'll want to delete outright these three:

sysreference (right click, DELETE!)
ECDDiskProducers (byebye)
SONYBMG (hasta la vista!)

Then, as you continue to FIND more sys items, BE CAREFUL! Some can be deleted, SOME HAVE TO BE EDITED!!! To find the next, simply hit the F3 key!

In "WBEM\WDM" you'll spot some UUID's and there will be crater.sys. Any such references that DON'T have IMAPI are safe to just delete. This will be the first one you encounter after the above. DELETE. Same for the one in WBEM\WDM\DREDGE ... DELETE!

This qwap also copies itself all over the "CurrentControlSet" keys, and does up ALL of them. 

So next stop will be under various "ControlSet00x" keys. You'll stop at the "CoDeviceInstallers" ... for each "syscaj.dll" you encounter. On OUR lab rats, it was the first UUID entry and the last. Look for the syscaj.dll entry and remove ONLY that particular value for a UUID where it appears and do NOT touch anything else in there!

NEXT STOP IS THE TRICKY!

Next stop is the "Enum" area - IDE or SCSI depending on what you have. HERE, we need to EDIT rather than DELETE! Look for an entry on the right side that says "LowerFilters" ... DO NOT DELETE!!!!! You need to double-click on the "LowerFilters" name. That will bring up an EDIT screen.

In this EDIT screen, what you need to do is move the cursor up where it says "syscrater" and CAREFULLY remove that, and pull any lines below it up. NORMALLY the line below will be IMAPI.SYS but could be something else, and more following. The OBJECTIVE is to remove the syscrater ONLY and then pull the line below it up to where the crater.sys WAS. Objective is to leave everything ELSE intact and JUST lose syscrater!

Should you encounter a "LowerFilters" that *ONLY* contains "syscrater," then you can DELETE it, but usually the "LowerFilters" has another item. Make certain that the top item isn't blank!

Next stop in your search will result in "UpperFilters" and here, what you want to remove is "syscor." If "syscor is the ONLY entry, then you can delete that item. If there is anything ELSE in there, then you must edit OUT the "syscor" as was done with "syscrater." Each system is different and thus the uncertainty here. You ONLY want to get rid of "syscrater" and "syscor" and LEAVE EVERYTHING ELSE INTACT or your drives will vanish.

syscor will show up in other places, under the name "ActiveChannel." You can DELETE that whole value too. ANY place where only syscor or syscrater shows up as a value can be DELETED as LONG AS there are no other "dependencies" listed. If there are other items, you MUST edit OUT the syswhatever and LEAVE THE OTHERS INTACT by removing the entire line which contains either syscrater or syscor ...

NEXT STOP, "ROOT" entries! You'll see the following KEYS which need to be deleted:

LEGACY_SYSARIES
LEGACY_SYSDRMSERVER
LEGACY_SYSLIM
LEGACY_SYSOCT

Just delete the entire KEYS themselves, so the above are GONE.

NEXT STOP, "SERVICES" entries! You'll see the following keys next:

sysaries
syscor
syscrater
sysDRMServer

Same deal as above ...

That completes the "CurrentControlSet" ... expect to go through a repeat of the above for EACH user's individual "ControlSet" until you've done them all. How many depends on how many "users" on the machine. 

Once done, BE SURE TO GO BACK and CORRECT the security change to the registry that was necessary to do this - REMOVE the checkbox for "everybody" that granted "everyone" "FULL CONTROL." You DON'T want to leave that permission granted!

And finally, REBOOT!

When the system comes back up, GO to that sysfilesystem folder and delete the remainder - you'll now have permissions to do so. And finally, wipe THESE files from your SYSTEM32 folder:

SYSCAJ.DLL
SYSUPGTOOL.EXE

You're done!

PREVENTING REINFECTION

1. Disable "autostart" (google for how)
2. Install BOClean (sorry, I *work* for a living and if I didn't, I wouldn't have KNOWN this answer.)

Permission granted to redistribute and expand upon, please include the original

source though - Kevin McAleavey at nsclean.com, makers of BOClean. If I'm going to be sued for this, the least I've earned is credit for the answer.