Question and Answer

The questions this month were wide ranging and worth considering in depth.

Preliminary

I attended a public lecture at the HP labs near Filton on Wed 24 October, given by James Lyne, the Technical Director of Sophos Ltd, on the subject of the cyber threat in the modern age. This talk was excellent, and if you get the chance to hear him in future, he is worth listening to on the subject of the state of the art in both the sophistication of the criminal fraternity in launching viruses, and in what has to be done to counter it. A few things seem worth pointing out in this forum.

The number of distinctly new viruses seen is now running about 200,000 per day, due to the ability to randomise some of the features and code that each one contains. In addition, websites are getting compromised at about the rate of one each second, due to sloppy administration. These sites should not be vulnerable in the way they are. This is important, as it is estimated that 90% of all infections come from compromised sites, and the sites are ones that you might reasonably wish to visit – they are not on the borderline of criminality or decency. If you go to these because you want genuinely to visit them for a good reason, then there is little you can do other than avoid Windows, or ensure it is locked down as securely as possible. All the malware mentioned affects only Windows.

The most alarming emerging danger is what is known as ransomware. This is a program that when triggered on a machine will find all the local data and encrypt it with a strong encryption algorithm, and then it will demand money to be paid to release the keys. Some of the criminals are honest enough to release the keys, some will string the victim along for as much as they can get, and others never answer at all. If this gets into a company's network, the damage can be enormous. A recent news report indicates some of the extent:
http://www.abc.net.au/news/2012-10-25/ransomware-targeting-aussie-businesses2c-pcs/4332526

Lyne also related how they tracked down one gang. It happened that they had not password protected their own data, and so Lyne and his team looked at all the files, and among them was a list of a few mobile phone numbers. From those numbers, he could identify any pictures taken with that phone and uploaded onto the net. (Isn't Google wonderful?) One such picture was the internals of an office, and they knew whose office now as well. But the phone had also put GPS co-ordinates into the picture, so they now had the exact address for the office. More information was gleaned by following friends on the guy's Facebook pages, including things like pictures of the Christmas office party (even criminals have office parties, it seems). He thought it appropriate that the party was in the form of a fishing trip.

The lesson here is how easy it is to track you and what you are doing, not from what you have uploaded, but from what your friends and acquaintances have done.

Finally, he demonstrated how easy it was to listen to smart phones. By using a commercially available and cheap (< $40 on eBay) wifi scanner, he listed basic information that each phone in the audience was radiating. In particular, phones with wifi enabled list the names of every wifi network to which they had at some time been attached. This is a big potential security hole if you are not aware of where the connection is being made to. And there are other dangers, too. A criminal could set up a new network close by with one of those names, and let the phone attach. The criminal can then seize the password as it is offered and so now has access to the real network, if he needs it. For

businesses, this is a serious matter. The answer is to keep wifi turned off unless in a known environment.

Q: What does 'Unknown channel 'maya-partner' mean?

This question occurred when an attempt was made to access a site that needed an updated version of the Adobe Flash plugin when using Linux Mint. The user was routed to another place wheere the latest version could be found, but the above message appeared instead of being able to install.

My suggestion here is that under Linux, it was expecting a certain repository to be available in the synaptic sources. However, that repository was missing. In the particular case, the user only accepted category one and two updates, by default; when he looked for updates to the Flash plugin, he found that there was another and that it was sufficiently up to date to get round the problem.

Q: What is gksu and where is the rubbish bin (trashcan)

Thanks to Mike Godfrey for this answer.

What Does 'gksu nautilus' Mean/Do and Where Did My Files Go?

Extracts from an email thread:

Peter Davis wrote:

“I've been trying to make some space by deleting a large program ("diogenes") which spawned a load of small files when it installed. According to a "read-me", the bulk of the stuff lies in 3 files (/usr/local/diogenes and "dio" and "diogenes" in /usr/local/bin). When I select these files, and right-click, there is no option to Send to Wastebin. So how can I get rid of them, please?”

Mike Godfrey replied:

“The GUI method is:

• Open a terminal window

• Type: `gksu nautilus`

• Enter password where requested

A file manager window will open – but with 'root' privileges. You will find that you can highlight the files you want to be rid of and delete them. BE CAREFUL as deleting the wrong file can corrupt your system.”

Peter replied:

“It worked, in that I was able very easily to find /*usr* and to right-click the offending files. They then gratifyingly disappeared when Sent to Rubbish. OTOH, they didn't show up as having arrived in my Rubbish Bin – so (asks he, suspiciously) where are they lurking?

A quick explanation

OK – actually two questions here.

1. What does `gksu nautilus` mean/do?

2. Where have my files gone?

What Does 'gksu nautilus' Mean/Do?

The *man* command is your friend – it opens the Linux built-in documentation. Open a terminal and type `man` followed by the term you want explained. So, we get from '`man gksu`':

“gksu is a frontend to su and gksudo is a front-end to sudo. Their primary purpose is to run graphical commands that need 'root' without the need to run an X terminal emulator and using su directly.”

So 'gksu' is a GUI version of 'su'. And 'man su':

“The su command is used to become another user during a login session. Invoked without a username, su defaults to becoming the superuser.”

And '`man nautilus`':

“nautilus - the GNOME File Manager ”

So: `gksu nautilus` opens the usual file manager – but with root privileges.

As an aside, opening Nautilus with root privileges was a menu option with older versions of Ubuntu, but it got dropped in 11.10 and after.

Where have my files gone?

Linux is a kindly operating system and tries to protect its users from their errors. So, when a user attempts to delete a file the default behaviour is to 'move' it to the Rubbish Bin, from whence it can be restored if the user changes her/his mind. Actually, the file is 'tagged' but not physically moved – and the space it occupies is not released!

In order to delete a file, one needs to specify 'Delete' in the right-click menu or click the Delete key. You will be asked to confirm. There is a key combination with 'Delete' which removes the need to confirm but, for obvious reasons, its use is not recommended!

As Peter used 'Move to Rubbish Bin', his files were not physically deleted. So where did they go?

'Rubbish Bin' is a British English term – the name down at the working level is 'Trash'. This page: http://www.ehow.co.uk/how_8219428_empty-trash-can-through-terminal.html explains where the Trash Can is and how to empty it. It states:

“The Trash directory is usually found at "*/home/user/.Trash*" or

"*/home/user/.local/share/Trash*", depending on the distribution and desktop environment you are using. Replace "user" with your user name.”

Note that because some of the directory names start with '.' they will only be visible in the file manager if the 'View > Show Hidden Files' option is selected (or Ctrl+H pressed).

Note also that if you are using an external storage device (camera, USB stick, hard drive ...) and you 'delete' a file the system will create a .Trash directory on the external device.

If in any doubt, you can find the Trash directories using the search capability in the file manager or by typing:

```
find . -name "*Trash"
```

in a terminal window.

To empty Trash using the file manager, use:

```
gksu nautilus
```

navigate to the Trash directory, select its contents and press 'Delete'. Confirm when asked. The directories and the files they contain should be gone for good and their space freed up for re-use. Note that you can delete the directories within the Trash directory, or even the Trash directory itself without harming the system. It will automatically re-create the deleted directories the next time anything is 'Moved to Trash'.

Q: How much memory am I using?

This question arose from wondering whether a machine was running slowly because it had too little memory. So how can you find out what the situation is when in use.

The principle command to get some level of detail is the 'top' command, run in a terminal. Just open a terminal window and type `top` at the prompt. It will list at the top of the screen various information about the use of the cpu, processes, and memory. Then below, a list of processes will appear showing what is chewing up the processing power and/or memory, together with other information. It will also indicate how much of the swap area is in use. When a machine slows down it may indicate that it is swapping processes in and out of memory, so a large amount of swap area in use a warning that RAM is insufficient. The immediate answer is to close down some applications to give the ones you do use more space.

The display will update at regular and frequent intervals. To stop the listing, just type the letter 'q'.

However, this is often overkill and Ubuntu (and other Linux distros) come with two convenient graphical displays, both of which can be found in . One is a small graphical display that can be parked in the system panel. For Ubuntu-like systems, it is called 'system load indicator' and can be found in the Ubuntu Software Centre (or through synaptic) by searching for 'system' and scanning down the list for the full name. When this is started (from System Tools menu, or via the Dash [top left logo] and type system and pick it out from the list) it will put a small display showing the cpu usage. A right click on this display and go to Preferences will open a window where you can adjust the size of display, and what you wish to display, among other things. I usually have cpu, memory, network and maybe disk displays open depending on the system.

The other one is known as 'system monitor', also available in the standard software sources. This is started in the usual way and gives a larger graph, more easily readable, then the tiny indicator displays. However it does occupy a lot of desktop space when running, and on a small machine may get in the way too much.

Q: How do I get a command line to type in these commands?

Linux is a Unix-style system. This means it is based on a system that was invented before graphical interfaces were even thought of, and so the heart of all the work is through a simple command line. Often the graphical manner of effecting jobs is just a front-end to a command run in the background when the dialog is complete. Sometimes the command line is the only way to do something.

To start a terminal in a window, look for the application called 'Terminal' or 'Terminal emulator' or 'XTerm' or some such name. It may be under Accessories, or System submenu, or elsewhere depending on the distribution. The terminal emulators are often easier to look at than XTerm windows, but your distro may differ.

The window will then display a flashing cursor, with some text to its left. The text is known as the '*prompt*' and typically contains things like the user name, the machine name, and the current directory in which you are working.

To type a command, just type and edit with the arrow, backspace and delete keys if necessary. When the Enter key is hit, the command will be executed and when finished, the prompt will re-appear ready for the next command.

Q: How do I set up a wireless connection?

This question referred to an Acer Aspire One netbook running Peppermint (a Linux variant) for which the user had been unable to connect to his home router. The following instructions should work with most common distros.

Assuming that any hardware switches for your PC have been enabled for wifi, then doing a RIGHT click on the network icon in the system tray should show you an option to Enable Wireless – make sure that this is ticked.

Then do a LEFT click on the icon to list the wireless access points that are visible to the machine at that time. If one of these is the network you are looking for, then just select that and supply a password if it asks for one. After a short wait, you should be connected.

If the network does not advertise itself, then you will have to set it up manually:

1. RIGHT click on the icon and select Edit Connections
2. Open the Wireless tab
3. Hit the +Add button
4. Put in the name of your network (SSID)
5. Set Mode to Infrastructure (you should not have an Ad Hoc network for this connection)
6. Open the Wireless Security tab
7. Select the type for your network (mine is WPA2 Personal)
8. Open the IPv4 tab
9. Set Method to Automatic (DHCP)
10. Close the dialog and after a short time, it should connect.

If your distro uses a different wireless manager, some of the detail of the dialog will differ, but the information to be supplied should be the same.