Dark Comet 2: Electric Boogaloo

blog.malwarebytes.com/threat-analysis/2012/10/dark-comet-2-electric-boogaloo/

Adam Kujawa October 5, 2012

Over the past few weeks Jean-Piere Lesueur, A.K.A. DarkCoderSc, has been developing a new version of the Dark Comet Remote Administration Tool which he is calling “Dark Comet Legacy.” This newer version of the tool includes numerous features that make the tool more user-friendly and appear more legitimate. In addition, DarkCoderSc continues to include notices and required agreements that advise against using his tool for malicious purposes. He also mentions that if it IS used for evil, that he is not liable for any damages done. In this blog we will look at this new version of DC as well as look at how earlier versions used in the past, and whether you should be concerned by this new version.

Dark Comet’s Past

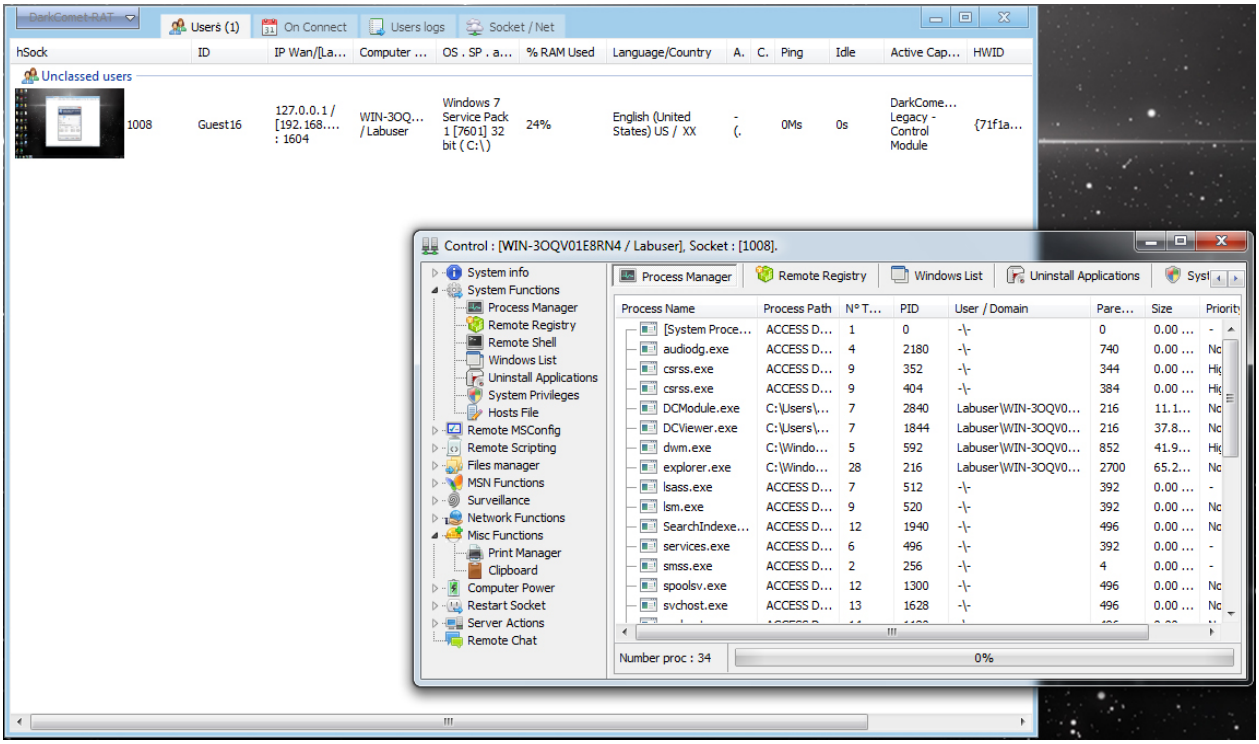
If you have kept up with my blogs, you know that I have mentioned Dark Comet numerous times. These blog posts talk about the previous version of Dark Comet that included a server binary creator that could be used to infect a system without the user ever knowing about it. Other blogs mentioned how it was used in such ways as an espionage tool in the conflicts in Syria and a mention about how DarkCoderSc announced the retirement of Dark Comet because of its use as a malicious tool.

- You Dirty RAT! Part 1 – DarkComet
- BlackShades in Syria
- BlackShades Co-Creator Arrested!

In addition to its political past, Dark Comet was most used to steal information and spy on unsuspecting users by both amateur and professional cyber criminals. Although, throughout its entire past, DarkCoderSc continued to discourage malicious use of his tool that he provided free.

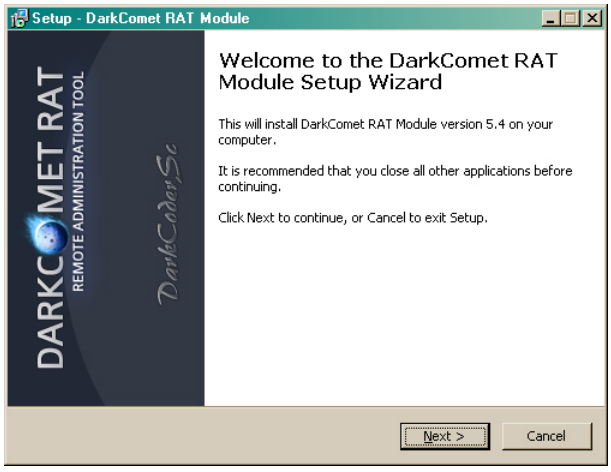
Dark Comet Legacy

As mentioned in the introduction, DarkCoderSc has released a new version of Dark Comet known as Dark Comet: Legacy. This new version is designed much more like legitimate software to be used by the average computer user.



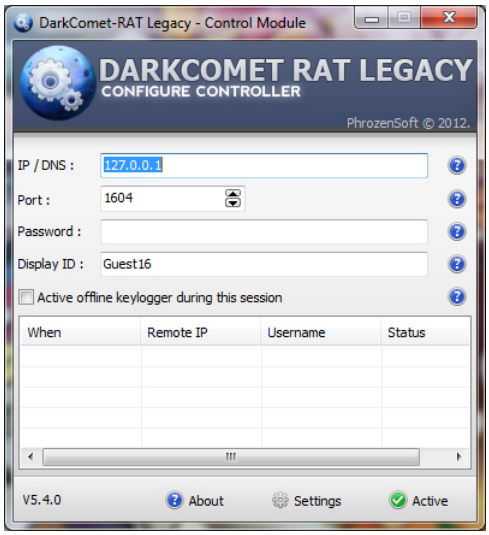
The Dark Comet Legacy Viewer Interface

One of the more user-friendly features is the brand new installers included with both the RAT controller/client and the server module. This makes it more user-friendly because the average user can just double click the installers, install the software and even be able to find the controller application in the Start Menu. As far as the module goes, using the traditional approach by using an installer application makes it difficult for the novice attacker to try to hide the installation of the application as with the previous version of Dark Comet that could be installed by only executing the binary.



Dark Comet Legacy Module Installer Screen

In addition, the server module includes a GUI that makes it easy for the user to configure a callback address on the fly rather than needing to recreate another binary with new instructions. The use of the GUI also makes it more difficult to hide the use of the server module from an unsuspecting user who might have had their system compromised via physical means or otherwise.



Dark Comet Legacy Server Module GUI

Dark Comet Legacy includes all the same functionality of the original Dark Comet, with the exception of the “Fun Functions” making it less of a tool to pull pranks on people with and more a legitimate system-monitoring tool. You could compare Dark Comet Legacy to some of the other legitimate system monitoring tools like TeamViewer; in addition, it has numerous purposes to keep your information and your family safe.

It might be used to:

- Keep an eye on your kids
- Access your system remotely in case of being locked out
- Remotely control systems on a private network
- Have access to key-logging and webcam monitoring to know who might be using your system if it is stolen.

Is it still a threat?

While there are numerous purposes for Dark Comet Legacy to be used as a legitimate system-monitoring tool, it is in no way considered “Not a threat.” In fact, if you were to find the server module running on your system, you should consider yourself compromised. Numerous Anti-Malware and antivirus products will agree that Dark Comet Legacy can still be used for malicious purposes, if not for its functionality than for the ability to undermine DarkCoderSc’s good intentions. I will go over a few of ways in which DC Legacy can be used in the same fashion as the original DC a little later and prove why it is necessary (at least for

now) to detect this tool as malware. DarkCoderSC and his company Phrozensoft acknowledge this fact and advise disabling Anti-Malware/antivirus applications when using DC Legacy.

Possible Infection Scenarios

Now that we have described what Dark Comet Legacy is capable of and how it can be used legitimately as well as the reasons why it would be difficult for amateur cyber criminals to use it to steal personal information or more, we will look into how this tool can be used maliciously just as the original Dark Comet was.

Masked as a legitimate application

This method is commonly associated with Rogue AV products that claim to detect malicious software on an otherwise clean system and when installed, infects the system with subsequent malware. An attacker might target novice computer users, informing them that DC Legacy is actually a tool that can help the user to remove malware or make their systems run faster. This method requires a high amount of social engineering to accomplish and being able to convince a novice to install malware themselves.

Installed along with other software

This method is often found within download site installers that are included along with legitimate software from shady websites. Usually, these installers will add toolbars or spyware to the system executing it. In this case, it could easily begin the installation process for DC Legacy by explaining it as a necessary tool to make the intended application work correctly.

Could be manually installed by other malware

The installation of malware by other malware is not a new thing, however it is possible for one malware to manually install DC Legacy by modifying the registry settings, saving the files and doing everything else the installer does for the user, automatically using the malware. I can personally see this method as being used frequently by cyber-criminals attempting to spread malware.

Conclusion

DarkCoderSc created the original Dark Comet with good intentions although it was abused by cyber-criminals in order to steal personal information, spy on unsuspecting users and use it for their own nefarious purposes without the user ever knowing. Dark Comet Legacy may follow the same path as its predecessor, created with even more of a legitimate purpose in mind however easily modified and molded to be used for malicious purposes. Check out the reasons behind the re-birth of Dark Comet on the Phrozensoft blog:

DarkComet RAT Legacy

The DC family is not the only set of tools created for legitimate purposes then abused by cyber criminals; tools like Netcat, NetBus and even a tool like a telnet terminal can be used for malicious purposes easily and therefore are often grouped into the malware or hacker tool category. The tool itself, outside of full-blown malware, is often developed to make things easier or give the user more power and control than they had before, some are created for educational purposes and some are created for administration. However, at the end of the day, it is in the intention of the tools user that determines whether it is used for evil and if the possibility exists that a tool might be abused to cause harm to other users, companies like Malwarebytes and others have no choice other than to protect their customers from harm.