You dirty RAT! Part 1: DarkComet

blog.malwarebytes.com/threat-analysis/2012/06/you-dirty-rat-part-1-darkcomet/

Adam Kujawa June 9, 2012

Last week, I talked a little about the Flame Trojan and how much the average user would need to worry about being infected with it, which is none. State-sponsored RAT malware, like Flame, would likely not infect average users and even in the off chance that it did, the operators behind the malware would probably remove the Trojan before being discovered. Its purpose is for very specifically targeted cyber-espionage, not stealing your Facebook password.

So are you completely safe from malware like Flame? Well not exactly. Take out the state-sponsored aspect of Flame and you've got a RAT or Remote Administration Trojan, of which there are many out there that are used every single day to spy on the average people. Before you get too freaked out, Malwarebytes Anti-Malware detects and removes these threats all the time, so don't worry too much about being a victim as long as you properly protect your system.

This blog post is one of many which I am going to use to:

- Discuss some of the RAT malware currently seen in the wild
- What they can do
- How they work
- How to protect yourself from them

This first blog is about DarkComet, a freely available Remote Administration "Tool" which was developed by DarkCoderSC, an independent programmer and computer security specialist from France. He advertises DarkComet as a tool and not a Trojan because of its many useful functions which could be used to administer a network at a very close level. However, he also mentions that his tool is often used by hackers and hence it is often detected by antivirus engines as being malicious. While the tool is free to download and use, he offers the "VIP" service, which gives the user access to direct support, updates about the product and the ability to post new ideas or software bugs, all for 20 Euros or $25.

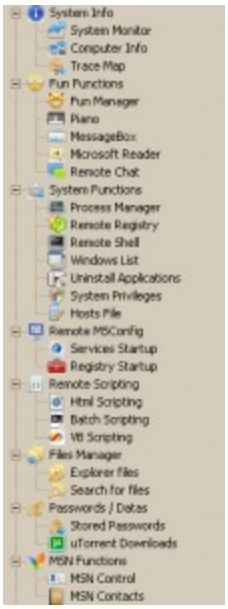
Features

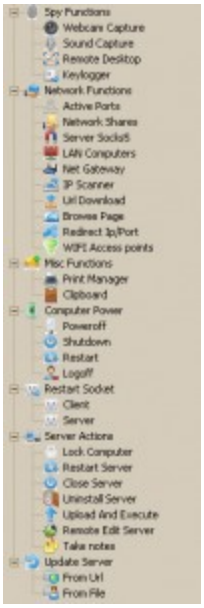
The Flame malware could do a lot of stuff, although not completely analyzed we know that it can take screenshots, modify/create/delete files and execute a keylogger. However, the capability of most RATs takes that functionality and multiplies it significantly. DarkComet is no different; it can execute over 60 different server side functions, meaning the type of things it can execute/monitor/control on the infected system.

Note: For the sake of talking about RATs, you need to turn the usual definition of “client-server” around. In this case the “server” is the RAT implant running on the infected system while the “client” is the controller application used by the attacker.

Here is a list of some of the pretty nasty things which this RAT can do:

- Find out all system information, including hardware being used and the exact version of your operating system, including security patches.
- Control all the processes currently running on your system
- View and modify your registry
- Modify your Hosts file
- Control your computer from a remote shell
- Modify your startup processes and services, including adding a few of its own
- Execute various types of scripts on your system
- Modify/View/Steal your files
- Put files of its own on your system
- Steal your stored password
- Listen to your microphone
- Log your keystrokes (duh)
- Scan your network
- View your network shares
- Mess with your MSN Messenger / Steal your contacts / Add new contacts!
- Steal from your clipboard (things you’ve copied)
- Control your printer
- Lock/Restart/Shutdown your computer
- Update the implant with a new address to beacon to or new functionality





Those are only some of what this baby can do; I left out a few of the big ones because I wanted to go into more detail about them. Also, they are my favorite!

Fun Functions:

A lot of RATs include “Fun Functions” to mess with the system (and minds) of the victim. In many cases these are built in functions to play tricks on friends or just have fun at the expense of the unfortunately infected user. DarkComet has multiple “Fun Functions” that I thought would be interesting to discuss and show you screenshots of.

Fun Manager

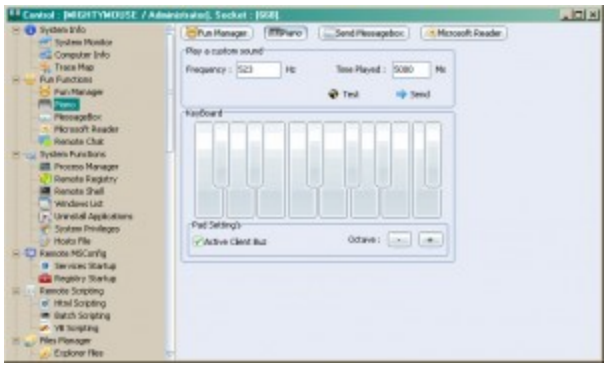
The Fun Manager is a set of different types of fun functions which an attacker can use against the user:

It includes:

- Hiding the Desktop – Hiding all the icons and making it impossible to right click on the desktop.
- Hide the Clock – Self Explanatory
- Hide Task Icons – In the little box on the right side of your start bar
- Hide Sys Tray Icons – Hide icons and open application buttons on the taskbar
- Hide Taskbar – Self Explanatory
- Hide the Start Button – Only works in Win XP
- Disable the Start Button (XP Only) – Gray out the start button, disabling it.
- Disable TaskMgr – Disables the Windows Task Manager (When you hit Ctrl+Alt+Del)
- Open/Close CD Tray – Self Explanatory

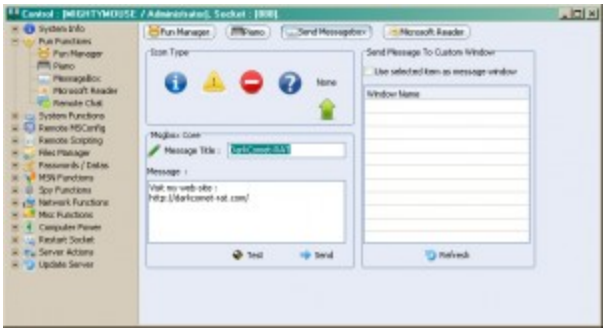
Piano

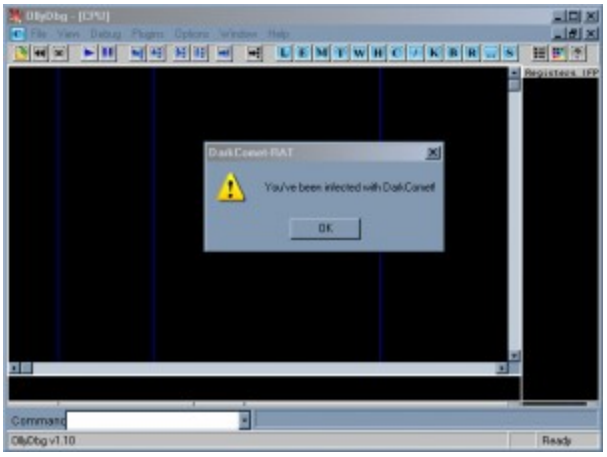
The piano function is exactly what it sounds like, the ability to play a type of piano which can be configured to play at different octaves. Another functionality of this feature is the ability to play a custom sound at a specific frequency (in Hz) and for a custom duration (Ms). The purpose of this feature (as far as I can tell) is just to annoy people.



Send Message Box

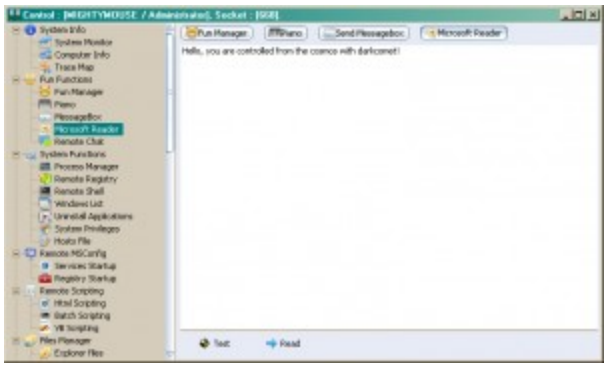
This is a pretty simple function which can mess with the user on a LOT of levels; it basically allows the attacker (or Administrator) to create a custom message box to the user, like an error or informative notice that one would normally see. The interesting thing about this feature is that not only are you able to create a message box belonging to the system but also to any active Windows on the system, for example notepad or Windows Media Player. The messages then appear to be coming from the application and that might make the user believe the application is malicious rather than the actual malware running behind the scenes.





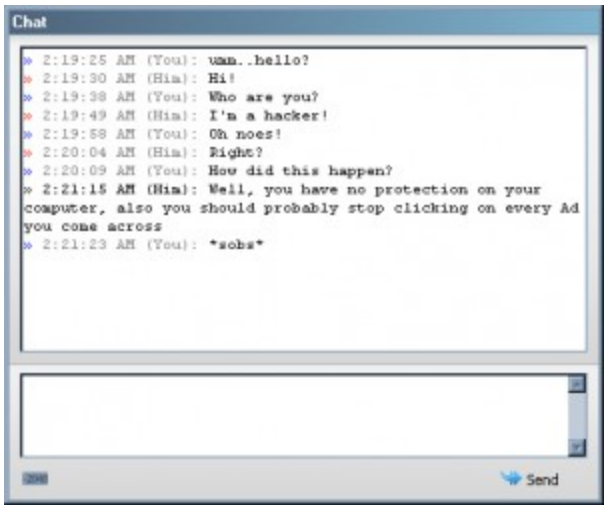
Microsoft Reader

This feature isn't anything new and is more fun than anything. If you've ever used a Mac, you know that one of the features of the text editor is to read the text you wrote out loud. The Microsoft Reader function is no different and will read whatever the attacker types, to the unsuspecting user. I could only imagine the kind of shock and panic that the user would experience upon hearing the electronic voice of evil saying to them "I OWN YOU" through the speakers.



Remote Chat

I think this feature is really fun, it gives the operator the ability to create a chat window on both ends (server and client) in order to have a conversation with the infected user. This has a lot of legitimate network administration purposes but none the less, it can really confuse a victim.



So that sums up all of the Fun Features, I thought it would be a good idea to discuss them because quite frankly, RATs are the only malware I have found that have a sense of humor and it's good to point out that not all malware is used to steal information or crash systems, some of it still likes to just mess with people, the same way hackers of yesterday did it for fun.

Uninstall Applications:

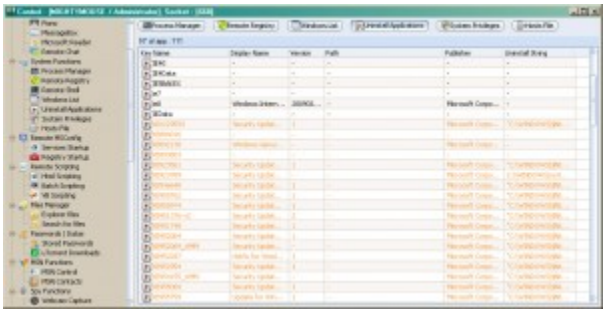
Unfortunately, we need to stray from the lighthearted side of this blog post and talk about some of the more scary functionality that DarkComet has. A very powerful and dangerous function of this RAT is the ability to uninstall applications at a whim. The attacker will receive a listing of all installed applications and be given the option to uninstall them. This could be used for multiple reasons; however one of the big ones is to disable security products. Here is an example of the worst possible situation:

You have an antivirus engine running on your system; you paid a lot for it so you feel secure. It came with an e-mail scanner so you don't mind opening on any e-mails or links you don't trust.

You get an e-mail from an unfamiliar source, telling you to click on a link to see a funny video of a LoLCat. You do so and are directed to a fake YouTube page; you shrug it off as nothing and go on your business.

Unbeknownst to you, the fake page exploited a zero-day browser exploit and infected your system with a DarkComet implant, this is a new variant of the malware and therefore, your AV has yet to write signatures to detect it. The first thing the controller of the RAT does is uninstall your antivirus engine, allowing it to do whatever it wants without being detected.

Another aspect of the Uninstall functionality is to remove security patches put into place to secure security holes in the operating system. This could lead to the DarkComet removing security measures put in place and being able to exploit older vulnerabilities in your operating system, allowing for even more malware to be downloaded to your system and executed. Now you are completely infected and your options are limited.



Remote Desktop:

This is a pretty neat functionality that you don't often see used by other RATs. It allows the attacker to not only see the active screen of the infected user but also be able to take control of the mouse and keyboard, using it as though they were sitting in front of the system itself.

This functionality is probably the most dangerous to the infected user because it can go beyond what the Uninstall function can do and instead of just uninstalling an AV engine, it can set the DarkComet executable to "Allowed". This means that even though the users

system is completely infected with DarkComet, the AV engine will not bother to try and stop it. This is something that many users might never know is even happening.

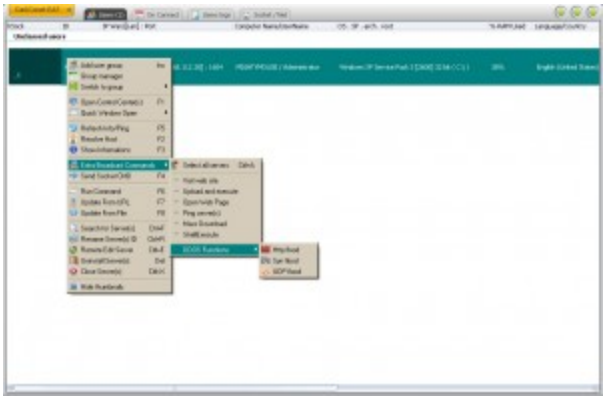
The drawbacks to this functionality is how loud it is, imagine playing an online game, you will receive data from the remote server in order to see what is going on in the game and the actions of other players, however you will also be sending a large amount of data as you interact with the game itself. This is along the same lines as if the remote desktop was being run, in which case it is possible to experience some serious network lag and for experienced computer users who might be running network monitoring software, a suspicious clue to something being very wrong.

DDOS

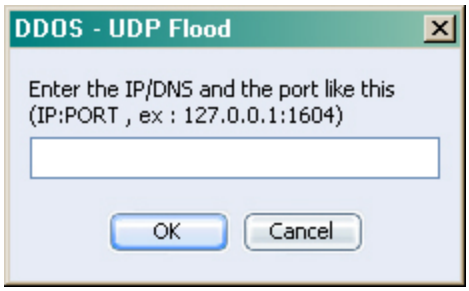
As I mentioned earlier, DarkComet is advertised as a network administration tool that helps to control systems in a network. Most of the functionality we have seen here so far (except for the Fun Functions) can be used to that end and you couldn't really dispute the use and purpose of the RAT. However, there is one question I have:

Considering that this is a Remote Administration Tool, to be used for good and what not….**WHY DOES IT HAVE DDOS FUNCTIONALITY!?**

As you probably know, DDOS means Distributed Denial of Service and is an attack where multiple systems, usually infected with botnet malware, will send multiple packets of network data to one location in an attempt to overload the receiving web server and disable its ability to respond to legitimate requests. This is a very well-known and used hacker attack, and yet, it's one of the miscellaneous functions that DarkComet comes with.



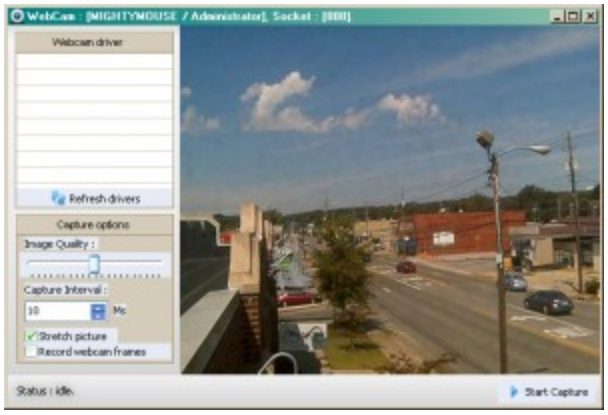
The above screen shows the "Users" tab, which lists all of the currently controlled systems, if you right click on one of these User entries and scroll down to the "Extra Broadcast Commands" you will see a menu for DDOS Functions. It includes an HTTP, Syn and UDP attack. When clicked it will request the kind of data to be sent and/or the IP/URL and port of the target:



I can't think of an occasion where a network admin would need to try and bring down a web server using the network he/she is controlling as a weapon but I don't work Network Administration, so what do I know?

Webcam Control

While it isn't a new or unique functionality, webcam control is still a very dangerous and effective way to spy on people.



The possible use of these webcam videos/images, which can be obtained from the webcam control function, range from cyber espionage, victim blackmailing, the normal perversion of spying on people while they don't know it and the worst one of all child pornography. Although not the intention of every attacker using this tool, it can be used to spread or sell child pornography and therefore make this function, in my opinion, the worst one out of the bunch.

How does DarkComet Work?

Good question! Most RATs usually have very intricate programming included in the implant themselves, including a large network of command checking algorithms which take the input from the controller and executes specific functionality based upon that input. The functionality is usually condensed as much as possible to make the implant binary smaller, however they are still usually larger than other types of malware which have less functionality. For example, a general range of size for normal malware is between 5KB and

15KB with the occasional outlier to 20KB. The sample implant binary I created for DarkComet, even after being packed, is 352KB. If you recall, the Flame RAT was 20MB; so in comparison, DarkComet is tiny.

Here is a breakdown of what happens with DarkComet when taking commands from the C2 or controller:

- Implant beacons every 20 seconds back to the C2 to check in and wait for any more commands
- When desired by the operator, the C2 will send back a command using some custom traffic encryption scheme.
- The command is taken in by the implant, decrypted and then analyzed for:

> - Authenticity – Meaning an ID or some other value which confirms that the implant is receiving a command from the correct source
> - Command – The exact function requested, I.E. List Active Processes or Disable Task Bar, etc.
> - Parameters – What extra options should the implant take into consideration when executing the requested functionality

- The implant will take this parsed information and execute the functionality
- The output from execution of the functionality will be sent back to the C2 in the same encrypted form
- The C2 will decrypt the data and present it to the operator

One of the key elements in network detection is the Beacon or the Beacon Response. Since DarkComet it is a repetitive string and the encryption only distorts the values in a set way (such as an XOR), the exact data sent to the C2 or back from the C2 will remain constant while the implant is inactive. These values can be used to develop network detection signatures which would flag a possible infection. The next step from a network security standpoint would be to track down the exact system which is infected by the malware and clean it accordingly. Although this kind of detection is usually only done on the networks of large organizations or governments, not really single users.

You might be thinking at this point: “Well hey, if that network detection stuff works well, why was it not used for Flame?”

Answer: I assume that after the detection of the infection (that rhymes) and a preliminary analysis of the Flame malware, it was put into place to keep track of which systems were infected and what kind of data was being sent. However, before the detection of Flame, the malware would of most likely kept its beacons as far apart as possible and maybe even send the data through a series of other infected systems before it went out to its C2. This would keep the traffic down and not throw any suspicious flags.

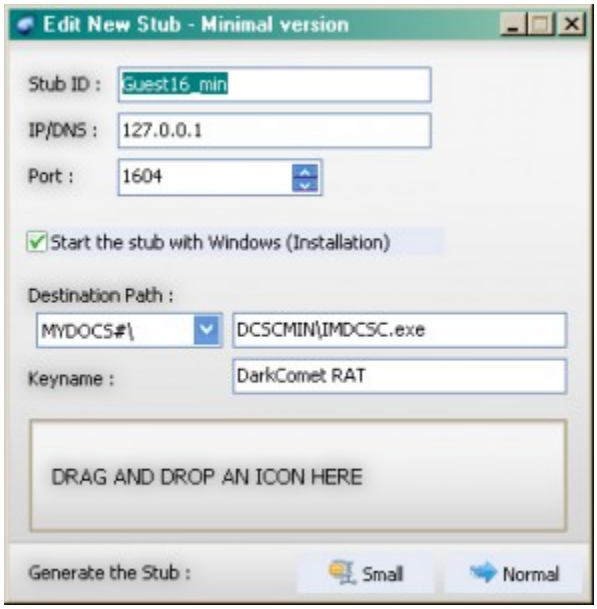
Moving on, we know how DarkComet talks to its C2 and how it processes the data and executes its functionality, that's great and all but does DarkComet use the same implant for every controller that is downloaded? The answer is no and that answer fits for most RATs. See certain things need to be configured in an implant, for example the beacon address, target specifications and the level of infection required. DarkComet is no different and comes with its own implant building tools.

There are two types of implant creation (or as it calls them, server module) tools, a Minimalistic one which is quick to develop or a Full Editor which requires expert knowledge of the RAT.

Minimalist:

The minimalist version of the implant creator includes configuration for:

- The Implant ID
- The beacon back address
- The port to use – The default is 1604, it was used in the past for Citrix related operations, it was probably chosen because of the high amount of traffic it used to receive.
- The installation destination path and "KeyName"
- An area to Drag-And-Drop an Icon to be used.



It is useful for on-the-fly creation of an implant but I think most users will probably use the Full Editor instead.

Full Editor:

The Full editor gives the user a lot more options when creating the implant, here is a list of those options:

- A security Password to further authenticate the implant to the controller
- The Process Mutex to use
- The Server ID
- A profile name to save the settings as
- The ability to hijack processes to get around Firewall restrictions
- The Address/Port to beacon to
- Installation location and filename
- Keyname
- Options to:

> - Destroy the installation binary after first execution
> - Change the file creation date
> - Create persistence on the system
> - Dropped File and Folder attributes (Hidden/System)

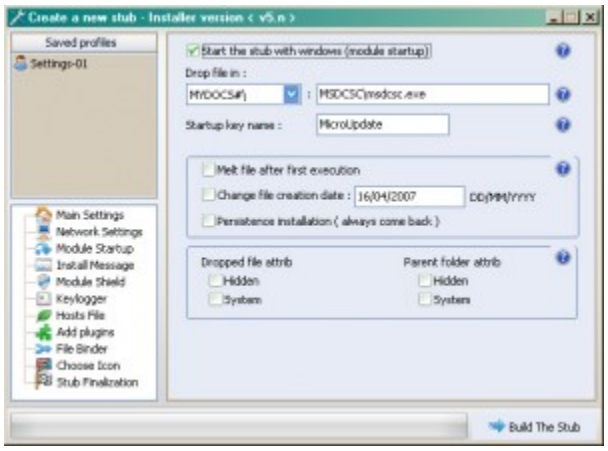
- Ability to display a message box with text upon installation
- Various stealth and persistence functions or Rootkit functions
- Ability to disable various system functions upon installation
- Options to use an offline keylogger or send keylogger data to a remote FTP server (with FTP configuration options)
- Installation modifications to the Hosts File – to redirect traffic
- Ability to load “Plug-ins”
- Addition files to drop and execute upon installation (Piggybacking)
- Which Icon to use for the Binary
- Compression or Packer to use:

> - UPX
> - MPRESS

The file extension to use:

> - .exe
> - .com
> - .bat
> - .pif
> - .scr

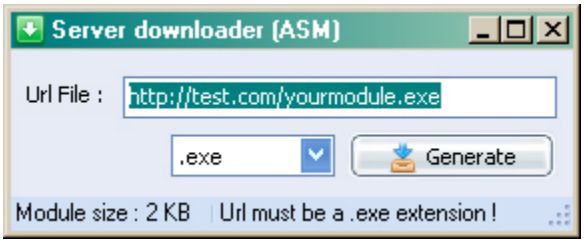
That is a lot of options! It is clearly the best method of creating the implant binary. The scary part about the functionality of the implant installation binary is that even without being blocked to its C2, this one file can execute enough functionality to completely infect your system.



Server Downloader:

The final option that an operator has in creating an infection binary would be the Server Downloader. I think this is a neat little tool that automatically creates a lightweight (2KB) application that automatically downloads and executes the real implant installation binary from a given remote URL. It makes it easy to hide it as being non-malicious when going through the motions of tricking a user into downloading and executing it. The options given to the operator are:

- The URL of the file to download
- The extension to use (The same as the Full Editor)



How to protect yourself:

There are multiple methods used in the spread of RATs, as for DarkComet, some of the biggest methods are:

- Drive-By Attacks
- Warez Downloads
- Social Networking Sites

Drive-By attacks mean that when visiting a web page, a malicious script embedded in the page will execute and usually exploit some kind of vulnerability on your system, dropping malware and executing it without you ever knowing. Drive-by attacks are usually used by cyber-criminals for the purpose of spreading malware. The use of drive-by attacks to spread

DarkComet doesn't seem to make a lot of sense since it is easily detected and removed. However, as noted on the DarkCoderSC web site for DarkComet, purchasing a VIP account will provide the attacker with version updates of DarkComet before it is released to the public. Therefore the new version or variant hasn't been seen and has a greater chance of getting past AV scanners, so it makes sense to try and infect as many systems as possible with it before it's too late.

Warez Downloads, or the downloading of illegal/cracked software can sometimes lead to downloading something you wish you hadn't, like DarkComet malware. Often used as a method by the less experienced hackers or "script-kiddies", advertising a cracked piece of software and actually providing malware is common practice and since DarkComet is so easy to obtain, set up and run, it's no wonder why it's being spread this way. I can imagine that a majority of people who participate in such actives (I don't judge) do not employ the use of AV scanners for numerous reasons (paranoia?) and therefore are great targets for not only DarkComet but any malware!

Social networking sites are a great way to spread malware, send a link out to a group of people all at once and hope some of them click it. Maybe hack someones account and post the link, disguised as another user. Either way, it's a great way to spread malware and RAT malware especially.

Luckily, not all is lost. If you have Malwarebytes Anti-Malware Pro installed, a few things can happen to protect you.

- The web site you were sent to with the exploit would have never loaded thanks to Malwarebytes Web Protection Module
- Malwarebytes Anti-Malware definitions scan for unique features at a deeper level than other AV vendors and are more likely to detect new variants of the same malware.
- Malwarebytes Anti-Malwares Active Protection module would have detected the malware being executed on your system and prevented it from going any further based upon its functionality.
- You can download Malwarebytes Anti-Malware and install it, even after being infected to detect and remove the threat.

On top of that, RAT infections can be the product of targeted attacks, though not always the case as mentioned above. They do make a lot of noise and more often than not antivirus/Anti-Malware software will detect and remove any infection. However, this is just one of many other types of RATs that are out there and while this one has the capability to do malicious things, it is a really good option for network administration.

Some of the other RATs we will discuss in this series are not so friendly, they are developed for the sole purpose of espionage and that is apparent in the infection methods used. As a general precaution, here is a list of standard security practices you can do to keep yourself safe:

- Always keep up to date definitions of your antivirus/Anti-Malware software
- Always update your operating system
- Never click on links in e-mails from people you do not know or trust
- Always keep the most up to date security patches for your browser and extension applications (Adobe products, Java, etc.)
- If possible, completely disable the Java functionality in your browser, this makes it impossible to be exploited through Java.

While these measures seem simple enough, they are the best protection for your system while not draining your ability to perform standard tasks or your wallet.