

# You Dirty RAT! Part 2 – BlackShades NET

[blog.malwarebytes.com/threat-analysis/2012/06/you-dirty-rat-part-2-blackshades-net/](http://blog.malwarebytes.com/threat-analysis/2012/06/you-dirty-rat-part-2-blackshades-net/)

Adam Kujawa

June 15, 2012



Last week we talked about the Remote Administration Trojan DarkComet and all the wonderful and scary things it can do. In response to the twitter post announcing the blog, the author of DarkComet tweeted an answer to my big bold question:

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

His answer was that he typically uses it for “Performing tests on his personal network to make sure it can protect against those kinds of attacks.” To simplify the answer, it’s like he built a bomb in order to see if his house was explosion-proof. He isn’t lying, it is possible to test your own defenses with such a weapon. I will leave it up to you, the reader, to decide whether or not that is a good enough reason to include the capability to perform Distributed Denial of Service attacks in his software.

Moving on, I know that I talked about how dangerous DarkComet was and that while there were a lot of illegitimate uses for it, it was mostly designed as a network administration tool and therefore, could be used for legitimate purposes. This week I am going to tell you about the opposite of DarkComet, a very powerful and very dangerous RAT Trojan known as BlackShades NET.

## Introduction:

---

There are quite a few different types of RAT malware floating around in the wild right now that are used by people ranging from amateur hackers all the way up to cyber-crime organizations. DarkComet is one of them and BlackShades NET is another, more dangerous one.

BlackShades is a very powerful RAT which sports all the functionality of DarkComet and then some. The methods in which it infects its victims spread over a large band of different methods, to name a few:

- Fake torrent downloads on Person to Person (P2P) sites
- Malicious links spread in chat rooms
- Drive-by attacks
- Java exploits
- Spreading via hacked social media/chat accounts
- Phishing e-mails

This list applies to most methods of spreading RATs and malware in general.

---

## Background:

---

BlackShades NET is developed (I say IS because new versions are always coming out) by BlackShades the company, their official "About Us" is:

*"BlackShades is mainly an IT surveillance and security-based company, directed at making your PC experiences easier. Our main goal is to offer affordable software solutions comparable to bigger names out there."*

They also mention the reasons people should buy and use their products including:

- Spying on spouses or children
- Being suspicious about possibly cheating partners
- Being paranoid about people using your PC in unwanted ways

Finally, to ease the tension about whether or not their software is legal, for the paranoid delusional with a conscience, they include a legal notice about an Act passed in 2004 allowing people to spy on their own systems:

*"... according to the Spy Act passed in October 5th 2004 by US houses, installation of advertising or data gathering spyware without authorization or the computer owner's consent is prohibited, but it is still legal to install any program you want to your own computer. Main*

*part of the Spy Act is about adware and spyware related software and website which use to gather user information for advertisement. It's 100% legal for you to install spy software on your own computer."*

The BlackShades website offers a variety of products which can help to accomplish the goals listed above; however the only one we are interested in is the BlackShades Remote Controller or BlackShades NET. While there are multiple methods available to obtain free or cracked versions of the RAT, the BlackShades website includes a method to buy the up-to-date software from them for only \$40!

## Terms of Use

---



In order to keep their product legal and keep themselves out of any sort of trouble or blame for the actions of the users of the product, BlackShades includes a Terms of Use, basically requiring the user to agree to not stealing their software and not using it in the wrong way, for example:

***“INTENTIONALLY SPREADING APPLICATIONS FOR MALICIOUS OR DAMAGING PURPOSES IS A CRIME PUNISHABLE BY FINE OR IMPRISONMENT. BY USING BlackShades NET PRODUCTS FOR MALICIOUS PURPOSES YOU ARE BREAKING THE TERMS AND CONDITIONS SET IN THIS AGREEMENT AND THEREFORE ACCEPT FULL RESPONSIBILITY FOR ANY CONSEQUENCES WHICH MAY RESULT FROM YOUR ACTIONS.”***

This is just one piece of a very long use agreement; it even makes the user wait a few seconds before they can click the “I Agree” button, I suppose to make them read at least some of it.

## What does it do?

---

Last week I listed a lot of different kinds of functionality used by DarkComet including spying on the webcam, uninstalling programs, fun functions, etc. Well BlackShades can do nearly all of these things so I am not going to repeat any previously mentioned functionality in any detail. Instead, I will discuss a few interesting things that BlackShades can do that DarkComet cannot...also, when I say interesting I mean frightening.

The BlackShades web site mentions a lot of the functionality the RAT is capable of, from various system administration functions to surveillance functions and computer security. It doesn't actually mention ALL of its functionality, as we will discuss, and I think that they might have a hard time explaining on their website the purpose of some of the following functions.

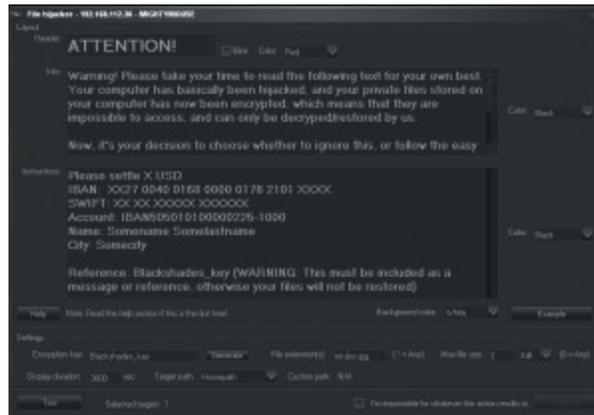
## Ransomware

---

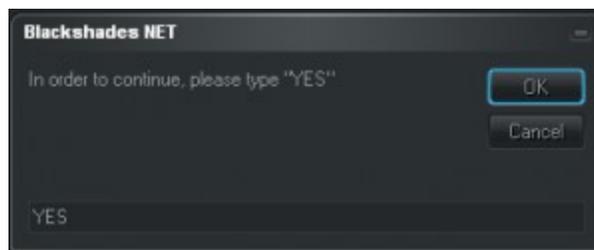


You might be aware of all the attention Ransom Malware, or Ransomware, has been getting lately. To refresh anyone's memory, Ransomware is used to hijack a system, sometimes by locking the user out entirely, sometimes by encrypting all the files with a unique key. A notice like the one above will show up and the user has the choice to either pay a Ransom fee or lose access to their files and/or system. Named the 'File Hijacker', BlackShades has the ability to use its server implant to create a Ransomware situation.

The configuration interface includes customization of the ransom message, screen colors, timer, encryption key and the target path of the files to be encrypted as well as which file extensions to encrypt. Depending on how many files the 'Hijacker' has to encrypt determines how long it will take for the ransom functionality to encrypt all requested files and show the ransom information screen (above) to the user. If, for example, the attacker decides to encrypt all .EXE files in the root C:\ partition and all the folders included in that partition, then it might take a while. In that time the user might experience some system lag and an inability to access certain files or applications. Once the demands of the attacker are met, they repeat the exact same encryption process and it fixes everything; which makes me believe that the encryption process is probably nothing more than a simple encryption algorithm (XOR, Bit Shifting, etc).



To add to how much BlackShades wants the attacker to really think about how severe a ransom attack is, he/she must click the “I’m responsible for whatever this action results in” button and type ‘YES” into a confirmation popup.



If the attacker clicks the “Help” button in the configuration window, it will give an explanation of what the attack does, how to fix it and a little notice at the end stating:

**WARNING!**  
*You should be extremely careful when dealing with this feature.  
Use this feature at your own risk.  
However, one thing to put in mind:  
This feature was made for educational purposes only.*

This is another example of BlackShades removing all liability of anything done with this tool from themselves and putting it on the user. Pretty slick if you ask me.

## Facebook Controller

Have you ever wondered how hackers are able to control the Facebook posts of victim users? Well there are a lot of ways to do that, including stealing saved credentials, keylogging, etc. BlackShades has its own method, where it allows the attacker to post text on the wall of the victim. The functionality is called ‘Facebook Controller’ and can be used as long as the victim user is logged into Facebook.

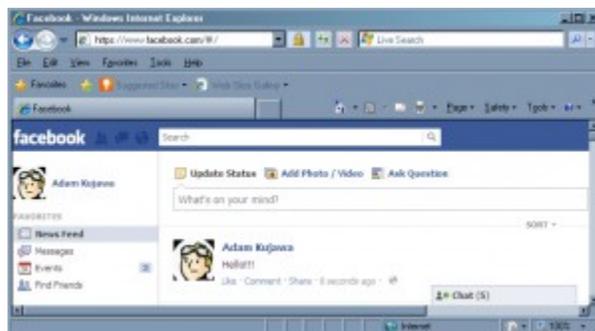
When I say logged in, I of course mean having Facebook up in a window, etc. I also mean that if you don’t properly log-out of Facebook, you just close your browser, your Facebook credentials are still valid and you are still logged in. The RAT will secretly post whatever text

it wants to your Facebook wall. This can be something as simple as “Hello!” or it could be a URL or link to a malicious website or executable which could spread the malware to your friends and family.



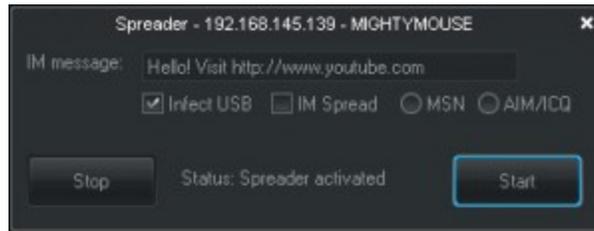
The above screenshot is a view of the Facebook Controller configuration window. It allows the attacker to customize what text to use for the wall post, it also gives the status of whether the attack succeeded or not.

I wanted to do some more testing and see if the Facebook Controller actually worked. I wouldn't recommend doing this at home since I knew that I had full control of the RAT and you might not be able to obtain that same confidence. I decided to log into my own Facebook and try this out, notice the text at the bottom of the Facebook Controller configuration window (above) and the new status update I apparently posted (below):

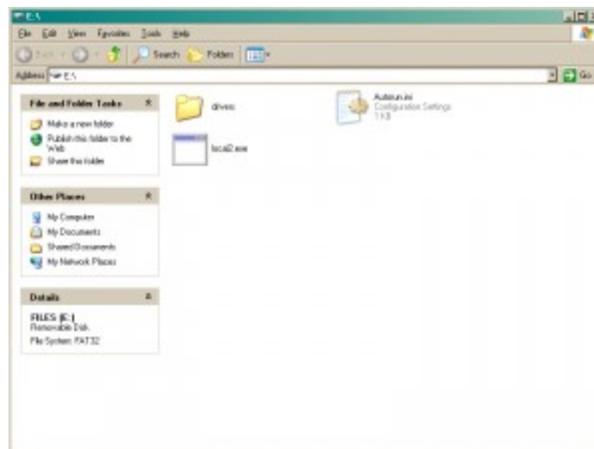


## USB Infector / IM Spreader

You've probably heard in the news lately about USBs being infected to spread malware to any systems they are plugged into, etc. etc. Well this particular type of attack has been happening for at least 5 years now, with different methods being used to accomplish it. Lucky for us, BlackShades uses an older method of USB infection that is easy to get around by just disabling any auto-run feature in your version of Windows.



The above screenshot shows the configuration window for the USB infection/IM sending function known as 'Spreader'. The USB infector simply puts a copy of the originating infections binary or 'server' onto any USB drive currently connected to the victim, it then creates an 'Autorun.inf' script which is used to execute the file once run, both files are hidden. If this USB driver were to be plugged into another system, one which did not disable the auto-run feature, the auto-run file would run and execute the malware, the result being that the attacker has another system to play with:



The other functionality of the 'spreader' is to send an IM to everyone on the contact list of the victim using MSN or AIM/ICQ. This message is customizable and could include a link to a malicious site or a download for the RAT infection binary.

## Torrent Seeder

---



Torrents are most commonly referenced when talking about pirating software or movies and music and as mentioned before, using P2P torrent sites, spreading malware! This functionality allows the attacker to download a torrent file from somewhere on the web and host it on the victims system or 'seed' it; allowing other people to download it directly from the user. This could result in the malware, which is used to trick someone else into installing a Blackshades implant binary, being downloaded from an already infected victim system. There would be no trace of the identity of the hacker spreading the malware.

There are a few requirements for this functionality to work, first of all the victim must have some kind of P2P file transfer software installed. If the victim does not have any installed, the attacker could go through the effort of downloading and installing it for them by using the download and execute functionality, as well as the remote desktop. There are also only a certain group of P2P clients which can be used:

- uTorrent
- BitTorrent
- Azerus/Vuze
- LimeWire

There are multiple uses for this type of functionality; including being able to spread even more malware with fake torrent descriptions. Using the user to host and spread pirated movies and software, etc. If tracked down by a law enforcement agency, they would only find the torrent file being seeded by the victim user and not be able to trace it back to the attacker, unless of course the attacker was still running the BlackShades implant on the victim system and beaconing back at regular intervals.

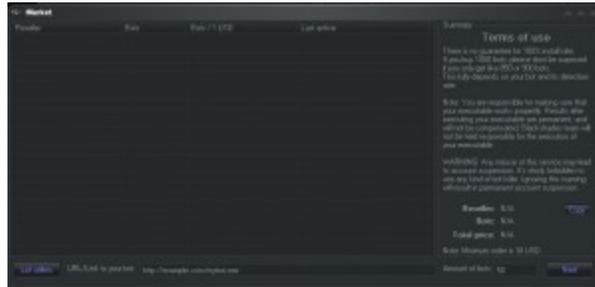
## Bot Marketplace

---

As we know, the world of botnets and espionage is also very marketable. That's why BlackShades included a marketplace interface into their RAT controller:



Here the attacker can buy and/or sell bots to other BlackShades users to make their network larger, the interface includes information on how to buy and sell and a listing of all current buyers or sellers currently in the network:



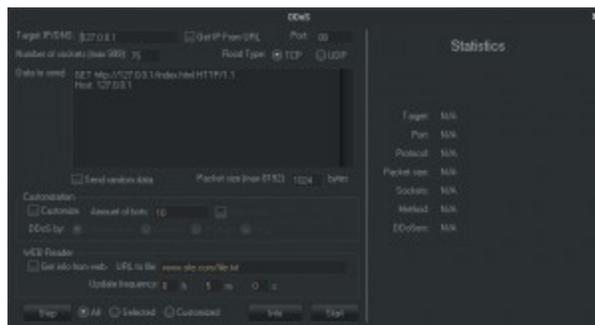
You can also buy Crypters using this interface, which are essentially packers and obfuscation tools to make it more difficult for antivirus engines to detect the implant binary:



This functionality, as well as some others mentioned, takes BlackShades out of the realm of the personal use system administration tool. It elevates it to the same level as cybercrime organizations.

## DDOS

I said earlier that I wasn't going to go into any detail about repeated functionality from DarkComet to BlackShades, however I wanted to show you the configuration interface for BlackShades RAT. It is very clean and streamlined and makes it very easy to send multiple types of DDOS attacks:



## Other Functions

I didn't mention every function of BlackShades, just the ones I thought were the most important to mention, I wanted to give a short list of the ones I left out and there might even be some duplicates from DarkComet in there too:

- Webcam Control

- Screenshot/Remote Desktop Control
- Keylogger (streamlined and much cleaner than DarkComet)
- Proxy manager
- Download and Execute Files (or more malware)
- Visit a website numerous times
- Redirect or Block URLs
- Use victim as a reverse relay, meaning that the attacker can set their browser to connect to the internet through the victim system.
- Control MSN messenger, including add/remove/msg contacts.
- Set an alarm for when a certain window title or keyword is present on the victim system
- Ability to setup a web interface for remote use!
- And much more!

## How does it do it?

---

It does it in the same way that DarkComet did it, an encrypted stream of data going between the client and the server, often with constant beaoning. Safe to say, RATs are not quiet when it comes to network traffic, but when your targets are pirated movie downloaders or click-happy social networking users, traffic detection is not really a huge concern.

## Server Creation

---



The server creator for BlackShades comes with fewer options than the server creator for DarkComet did:

- Beacon IP/Hostname
  - Port / Transfer Port
  - Server ID
  - Filename
  - Install path – where the server will be stored upon installation
- Application Data
  - Temp Directory

Install Mode

- Install – copy the file to the designated directory (%AppData%, %Temp%)
- Melt – Delete the file after it's run
- Protect Process – Do not allow the process to be killed

Delay – How long after execution to wait before installation

- No Delay
- 10 Seconds
- 1 Min
- 5 Mins

- HKCU – What Registry entry to use for installation.
- ActiveX Key – Generate a unique value for the binary to use during operations and installation
- Mutex – Generate a unique value for the binary to use during operations and installation, also keeps from multiple instances of the same server running at the same time.
- And the ability to:
  - Infect USBs
  - Compress the binary with the UPX packer
  - Change the Icon
  - Clone file information – For example the installed binary will match the same properties of a legitimate file. The file to clone is chosen by the attacker.

Basically, DarkComet was able to configure various types of “Upon installation” actions as well as the ability to make each server binary slightly different from the previous one. Blackshades will produce nearly the same binary every time, as long as the default configurations available with the server builder are used. This means that if the attacker decides to purchase a new and undetected crypter, they could potentially avoid antivirus detection and still obtain the same results of DarkComet.

## How do you protect yourself?

---

If you have Malwarebytes Anti-Malware Pro installed, one of three 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.

On top of that, RAT infection is usually the product of targeted attacks, though not always the case. They do make a lot of noise and more often than not antivirus/Anti-Malware software will detect and remove any infection. 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 Anti-Virus/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.)

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