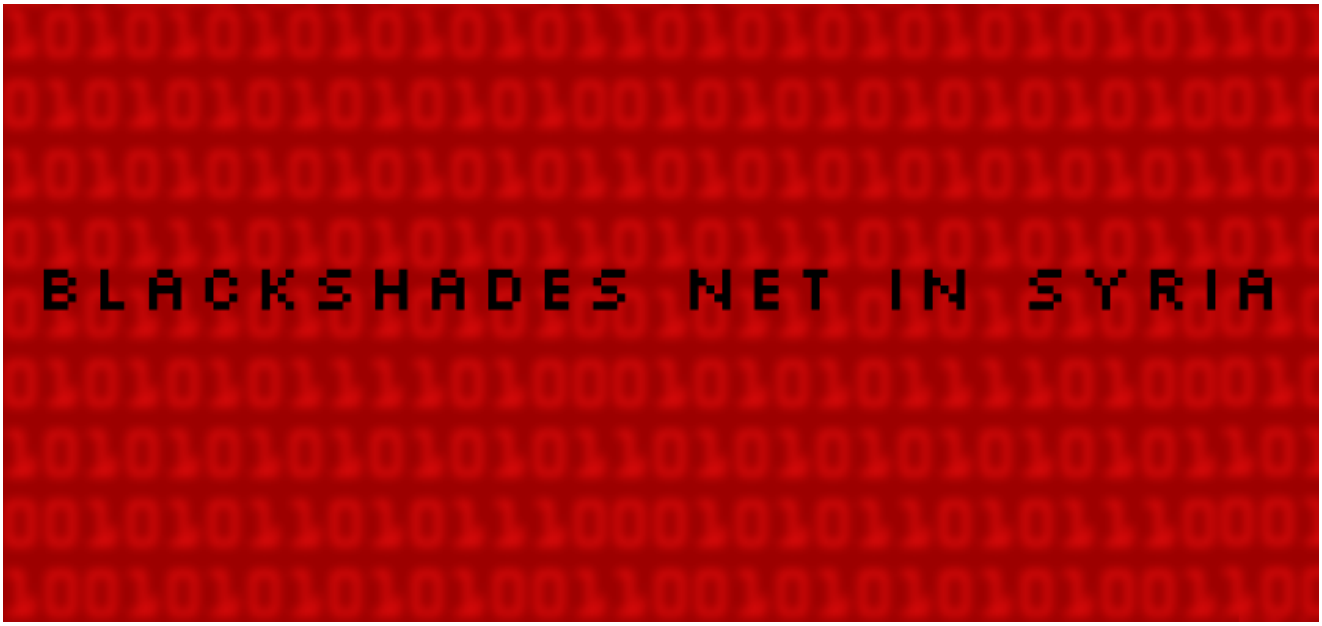
BlackShades in Syria

blog.malwarebytes.com/threat-analysis/2012/06/blackshades-in-syria/

Adam Kujawa June 21, 2012



As reported by the Electronic Frontier Foundation (EFF) earlier this week, a new Trojan is being spread to Syrian activists in an attempt to employ electronic surveillance on the group and its members. This Trojan is none other than the BlackShades RAT I blogged about last week as Part 2 of a series on different RATs found in the wild. As it turns out the first blog post on DarkComet has also been used against the activists in the past.

Background

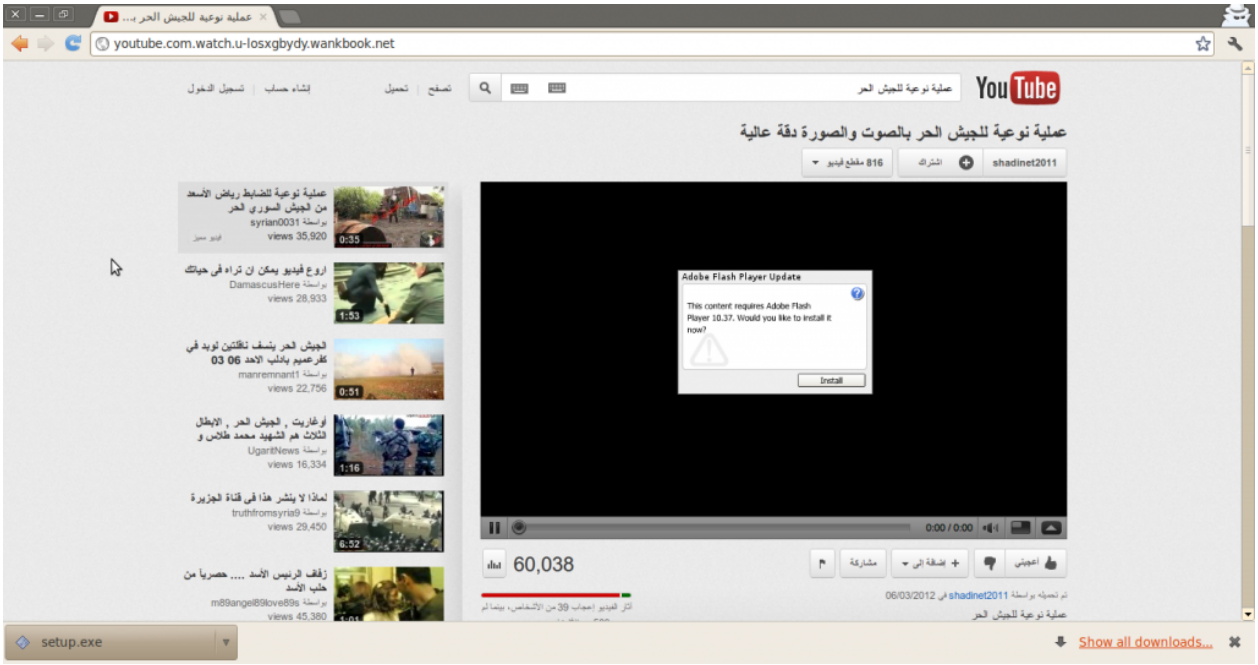
Syria is currently undergoing a very serious and bloody internal war between the government and the opposition forces or activists who want to see the tyranny and injustice shown by the country's top leaders come to an end. I cannot speak about it in detail but can only refer you to this video by CNN which explains everything very well up to now:

Syria: How a year of horror unfolded (CNN)

Beyond attempting to squash opposition on the ground with the use of tanks and guns, attempts have been made to do the same thing in the cyber arena, by pitting people against each other and destroying communication, at the same time collecting vital information on the communications of the activists. In order to accomplish this, three types of Remote Access Trojans/Tools have been used against the activists with various methods of infection.

Infection

According to the EFF, the hackers who have been infecting the systems of the Syrian activists are the same ones who had previously been infecting them with DarkComet. They had accomplished this by leading the victims to a fake YouTube video page which had anti-government opposition themes, upon accessing these pages, the download and installation of an Adobe Flash Update would be required, however the updater executable was actually a DarkComet implant in disguise. It also allowed for the victims to log-in with their real YouTube credentials to leave comments, at which point the credentials would be stolen and used against the activists, possibly to spread the fake YouTube video to any contacts.



This image is from the EFF report on Fake Youtube Pages used to infect Syrian Activists: https://www.eff.org/deeplinks/2012/03/fake-youtube-site-targets-syrian-activists-malware

The new infection method used with BlackShades includes distributing the implants through Skype as a “.pif” file. The EFF was able to document this based on the sample they obtained of the malware, which was obtained by an officer of the Free Syrian Army through his Skype account. After downloading and executing the file, it automatically infected his system and sent out the same link to the file as he received, which described the download as an “Important Video”, to all of his contacts.

Evading Detection

As I mentioned in the blog post, BlackShades NET has the ability to create implant binaries which employ custom obfuscation algorithms or Crypters, which can be bought through the Bot/Crypter marketplace embedded in the BlackShades controller. The implant sample collected from infected systems of the Syrian activists uses one of these custom Crypters in order to hide the implant binary from detection.

According to Citizen Lab, a laboratory at the University of Toronto whom conducted an in-depth analysis of the collected implant sample, at the time they released their results online, the malware variant was undetected by any of the antivirus engines used by VirusTotal. However, thanks to the diligence and observations of the Researchers at Malwarebytes, the samples noted as 'Undetected' by Citizen Lab were being detected by Malwarebytes Anti-Malware definitions 9 days before the release of the Citizen Lab report on June 7th.

Implant Infection Breakdown:

The exact technical details about the infection can be found on the report from the EFF and Citizen Lab:

To summarize a very interesting and technical explanation:

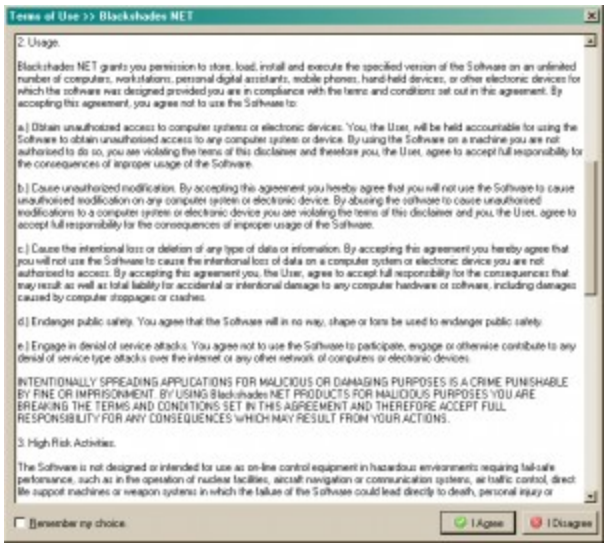
> Once downloaded and executed, the ".pif" file drops multiple files into:
>
> - The User "Templates" directory
> - The User "Temp" directory

- The malware then creates multiple registry entries which serve the purpose of allowing the dropped files access to the internet without being stopped by the local Windows firewall
- The malware establishes persistence (so it will start again if the system is rebooted) by creating an "AutoRun" registry key for one particular dropped file named "VSCover.exe"
- "VSCover.exe" runs an internal decryption algorithm which reveals the hidden BlackShades implant executable
- Initially the implant beacons to TCP port 4444 to the website alosh55.myftp.org

> It is important to note that alosh55 is of a similar naming convention of the beacon address for the previously used DarkComet RAT which, according to Citizen Lab, was alosh66. This connection, in addition to their finding of both the alosh55 and alosh66 pointing to the same IP address for consecutive days, allowed for the conclusion that both the attacks used with the DarkComet RAT and the new ones with the BlackShades RAT are being performed by the same actor.

Personal Observations

To start off with, obviously the hackers using BlackShades NET for their nefarious espionage purposes have violated the terms of use agreement:



They may have voided their warranty.

EFF mentioned that one of the capabilities of BlackShades is installing a keylogger and a screenshot grabber; we know that these are only the minor capabilities of BlackShades. However taking that into consideration, what can happen if the information obtained from using these types of functionality were put in the wrong hands? I created a list of what that info is and what it can be used for in the hands of state-sponsored hackers:

Keylogging:

Keylogging is one of the simple features available to BlackShades users, however unlike most keyloggers, the BlackShades interface allows for a very understandable feed of key presses by the infected user. Using this functionality, hackers can obtain:

- Login credentials for chat clients, forums, social networking accounts, bank information, etc.

  The hacker or group of hackers behind the attacks can pose as the activists, as they have in the past, to do more than just spread more malware but also to inject doubt or worry into the group, defeating morale or ending discussions on particular plans of action.
- The text of emails being sent between activists and the text of the chat sessions between them
  - This information can be used to obtain plans for activist rallies and any anti-government actions taken by the Free Syrian Army, essentially being able to predict when and how they will happen and come up with a plan to stop them before they even start.
  - This information can also be used to blackmail activists into giving up information on other activists or their activities. It can also be used to paint a negative picture of the activists to the public by taking their words or plans out of context. Already the President of Syria refers to the opposition forces as “Criminal Terrorists”, revealing text or actions from the opposition in the wrong light might just back up that claim to the non-combatant public.

Remote Controlling:

We know that BlackShades has the capability to remotely control a system by taking over the input of the user, combined with other features of BlackShades, the hacker has the ability to:

- Disable any sort of antivirus protection against further malware
- Steal files and documents from the victims system
- Reroute network traffic
- Monitor the activities of the victim while using the system

Webcam Viewing:

While the use of being able to remotely activate and monitor the webcam attached to a computer allows a hacker to invade user privacy on many levels, I can think of only a few uses to government sponsored hackers:

- Obtaining a visual identification of any persons using the system flagged as being used by activists
- Obtaining intelligence on the kinds of resources which might be discussed or revealed in front of a webcam.
- Determining possible location of the system
    Certain features available to the BlackShades RAT allow it to pinpoint to a certain level the location of the infected system based upon the IP address being used, however if one was able to determine a near location of the system, then narrow it down based upon visual cues, for example if the victim was on a laptop outside, then the probability of finding the exact location would increase drastically

BlackShades includes many more features which would be useful to government sponsored hackers, including:

- Activating a Ransomware functionality which would encrypt all the files on the system
- Using the infected system as a proxy for all traffic, this could be used to frame a user by forcing them to visit websites or perform cyber-attacks against their will.
- Host torrent files; imagine if the next variation of the espionage malware was downloaded from one of the victim systems belonging to the enemy
- Listen in to any conversations or sounds around the area of the infected systems microphone
- And many more…

If you are curious about any further functionality of BlackShades, please check out my blog post from last week: **You Dirty RAT Part 2: BlackShades NET**

Protecting Yourself

Unlike Flame, which had little likelihood of reaching the general public and being a threat to the normal person, BlackShades is a very real threat to the average user. It is because it isn't only used in political or international conflicts, it is used on the everyday person to steal information, spy and exploit people every day. My BlackShades blog post goes into some detail about how to most effectively protect your system from being compromised by a BlackShades implant. In addition, the EFF included a portion of their report on how to protect yourself from this threat and I encourage you to check it out.

As stated previously, Malwarebytes Anti-Malware was able to detect the obfuscated BlackShades implants 9 days before the release of the Citizen Lab report. In saying that, Malwarebytes Anti-Malware works in conjunction with pre-existing antivirus software to add a second layer of protection against new and upcoming threats. If you are concerned with the possibility of being infected by this or a similar type of malware, please download and install, at the very least, the free version of Malwarebytes Anti-Malware to protect your information.

How bad are these guys?

While writing this I couldn't help but consider a few things that threw up some flags for me and I thought would be interesting to share. Namely it was about the choices made by the hackers in their design and execution of their attacks compared to the espionage efforts of other, more developed countries.

Port 4444

While we didn't go into it very deep in my BlackShades blog post, port 4444 is set as the default transfer port, and according to Citizen Lab, it was the port they saw being used by BlackShades to connect to its C2C. This means that regardless of all the obfuscation used by the hackers to hide the implant binary, they are still using the at least some of the default settings for the implants themselves. This is usually a sign of a lack of experience using this kind of tool or a lack of concern for using the tool correctly.

DarkComet / BlackShades NET

Despite BlackShades being a pretty mean piece of software, you still have to wonder about the fact that a state-sponsored hacker or hacker group is using freely available malware that is more often seen in the hands of Script Kiddies and organized cyber-crime organizations. There is a small price ($40) for BlackShades and of course however much they paid for the Crypters, but DarkComet is completely free! Over the past few weeks, we have seen the most intricate piece of spy malware ever developed (Flame) and being used for cyber espionage purposes against the infrastructure of developed countries, and then we look at the poverty stricken government of Syria and see over-the-counter RATs being used. It is clear that even in cyber war, the more developed countries have better weapons while the poorer countries use whatever they can get their hands on.

Conclusion

The hackers behind the attacks and infection of Syrian activists are not employing sophisticated methods of espionage and infection but only the same tactics as the average cybercriminal. The fact that default settings and publicly used RATs are being used means that the hackers are not especially skilled in cyber espionage and are just using what they can in order to get the most results.

In addition, this is just one case of publicly available malware being used beyond the means it was ever intended. A while ago, when speaking about Flame, I asked the question “How much super malware could really be out there?” In this instance, I ask: ‘How much publicly available and widely used malware is being used every day for purposes of great importance, such as war or cyber-espionage on a corporate or international level?’ Lucky for us there is only so many ways to mask a variant of the same malware, as long as we know about it, we can fight it.

References:

1. http://blog.malwarebytes.org/intelligence/2012/06/you-dirty-rat-part-2-blackshades-net/
2. https://www.eff.org/deeplinks/2012/06/darkshades-rat-and-syrian-malware
3. https://www.eff.org/deeplinks/2012/03/fake-youtube-site-targets-syrian-activists-malware
4. https://citizenlab.org/2012/06/syrian-activists-targeted-with-blackshades-spy-software/
5. http://edition.cnn.com/2012/02/17/tech/web/computer-virus-syria/index.html
6. http://blog.trendmicro.com/fake-skype-encryption-software-cloaks-darkcomet-trojan/
7. https://threatpost.com/en_us/blogs/syrian-dissidents-hit-another-wave-targeted-attacks-062012