Taking off the Blackshades

blog.malwarebytes.com/threat-analysis/2014/05/taking-off-the-blackshades/

Adam Kujawa May 30, 2014

About two years ago, I wrote a series of blog posts that covered a particular Remote Access Trojan (RAT) known as Blackshades. The posts covered how Blackshades was used against Syrian rebels, how the co-creator was arrested and a detailed analysis of the RAT functionality.

Well if you haven't heard, they are back in the news again, this time because of a massive global effort by law enforcement to take down the RAT once and for all.

BBC

News | Sport | Weather | Capital | Future

NEWS UK

Home | US & Canada | Latin America | UK | Africa | Asia | Europe | Mid-East | Business | Health | Sci/Environment | Tech | Entertain

England | Northern Ireland | Scotland | Wales | UK Politics | Education

19 May 2014 Last updated at 16:21 ET

Share

BlackShades: Arrests in computer malware probe

Details of the operation were announced at a news conference in New York

Seventeen men have been arrested in the UK as part of a worldwide crackdown on a malicious computer program.

The FBI-co-ordinated operation targeted BlackShades software which can remotely control computers and webcams. The "malware" was said to have infected more than 500,000 computers since 2010.

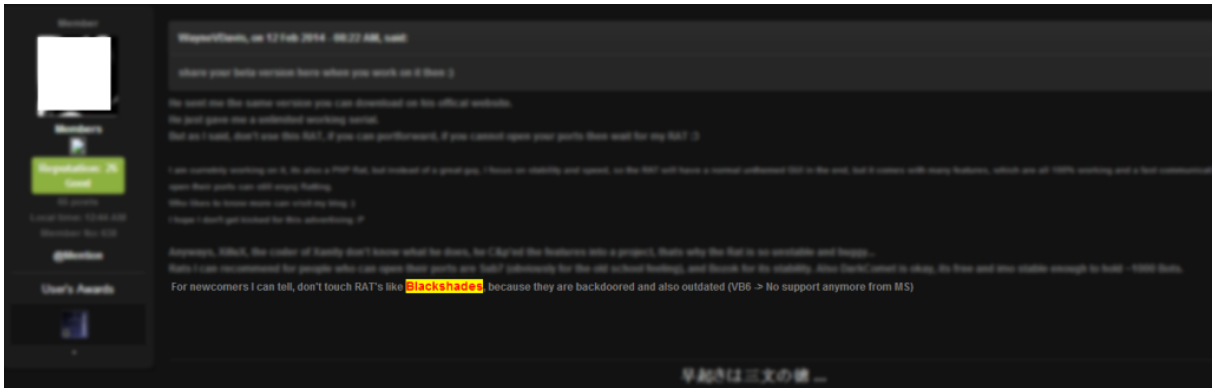
The UK's National Crime Agency said 15 arrests took place in England and two men were held in Scotland.

Last Monday, a mass arrest took place against not only the creators and distributors of Blackshades but also the customers. More than 90 people were arrested globally for being somehow involved with Blackshades in the largest offensive move against RATs ever done by global law enforcement.

Can you ever get rid of RATs?

So what does this mean for the current and potential victims of Blackshades and RAT technology?

Fortunately, the interest in Blackshades has decreased due to an array of different issues with the product. Customers are no longer trusting of the tool, not only because of the arrests but also because of bugged versions discovered that opened a backdoor onto the attackers system, essentially turning a bad guy into just another victim.



“For Newcomers I can tell, don’t touch RAT’s like Blackshades, because they are backdoored and outdated…”

Unfortunately, when one tool or bad guy gets busted in the cyber-crime community, it doesn’t stop the crime but merely modifies its execution.

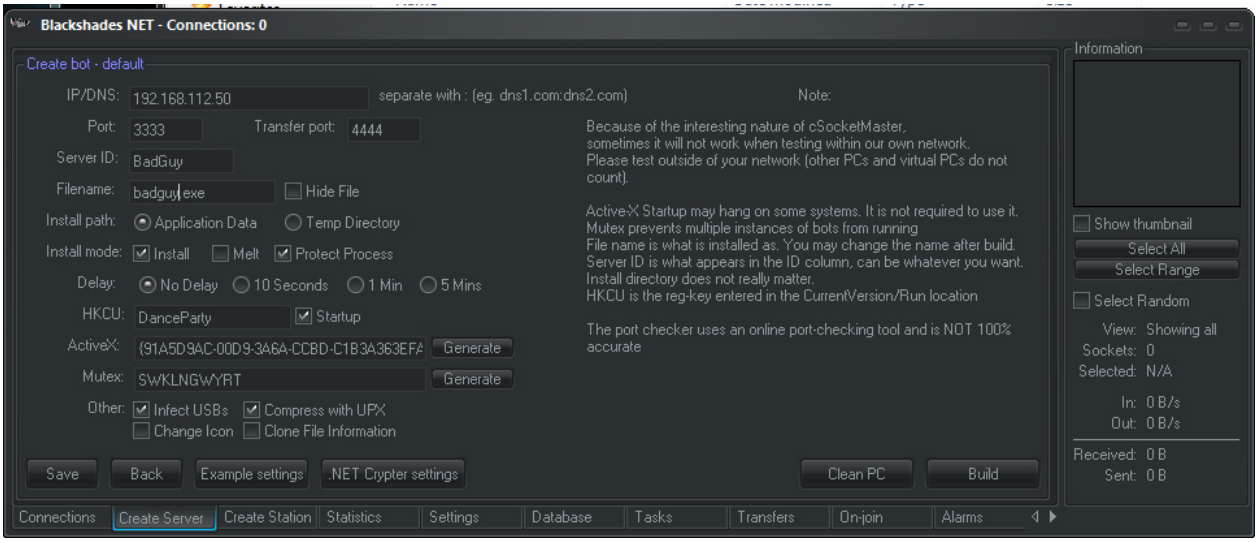
Already, criminals who were considering using Blackshades have sought out different tools that are a bit less popular in the hopes that they can still achieve their malicious goal without the greater risk of being busted by the FBI.

The appeal of Blackshades was that it was often updated and had been used so greatly that its popularity brought droves of potential customers to its door.

The Freemium Model

Blackshades was usually sold for $40 a pop, for the most updated version. This amount also came with customer support and access to new updates for the software.

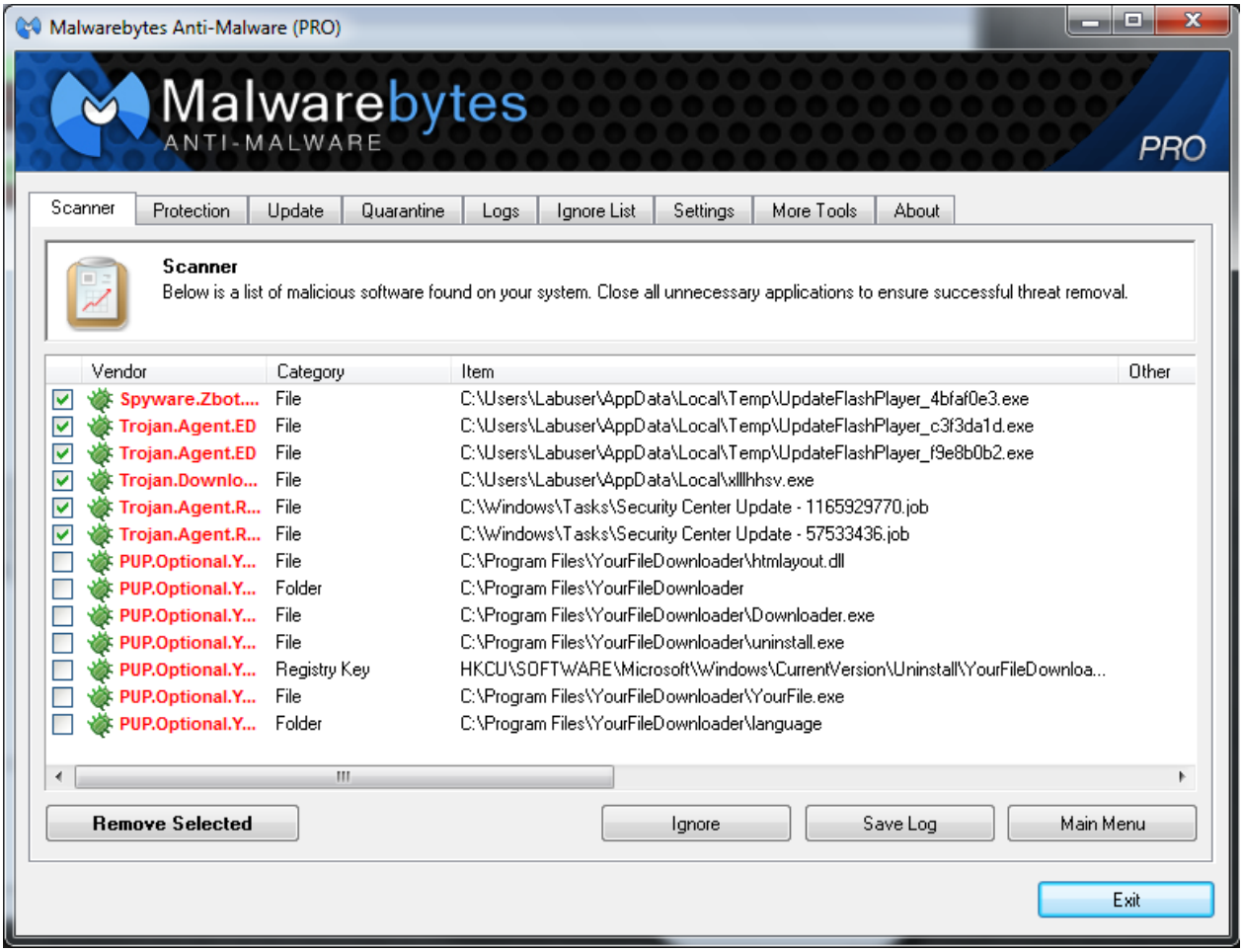
However, paying wasn’t the only option. In my previous blog posts about Blackshades, namely ‘You Dirty Rat Part 2″ I obtained a free (cracked) version of Blackshades for testing purposes.



Blackshades Server Binary Builder

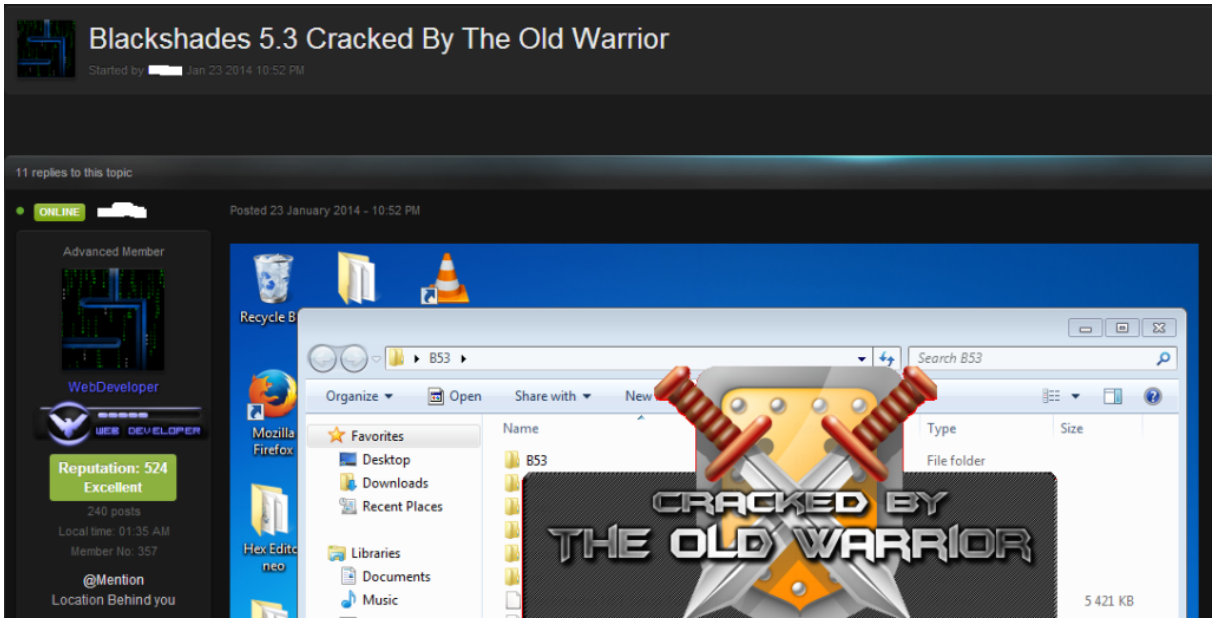
The software was an older version that was currently available so it meant that some of the more advanced features were not available.

In addition, while many ‘free’ versions of Blackshades usually come bundled with a backdoor or additional malware to infect the criminals, this one was completely clean.



Just a sample of the kind of junk I got infected with looking for a legitimate version of Blackshades

I didn't get my hands on a free version by simply asking around my cyber criminal buddies, or being part of some underground forum, all I had to do was search around online a little bit until I found one. Something that even a kid could do.



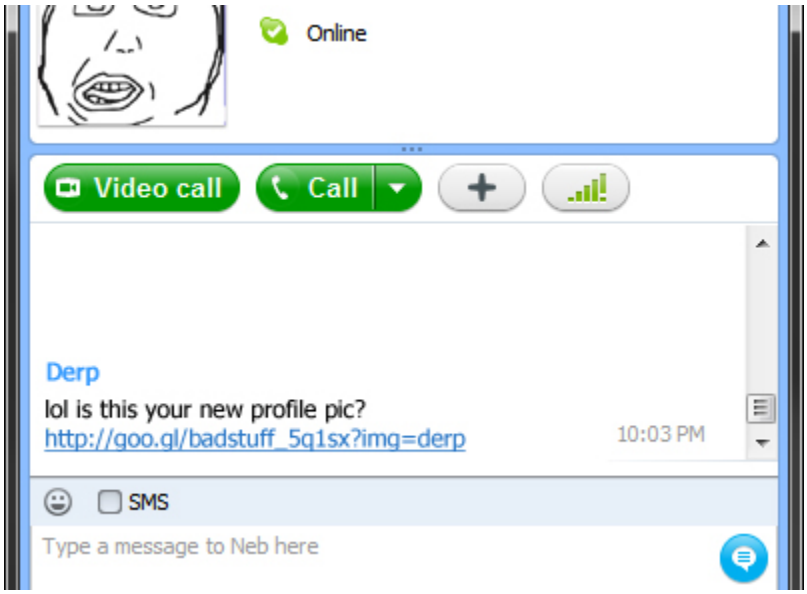
An advertisement for a cracked version of Blackshades on a overworld hacker forum

The Real Danger

So if you are wondering if an outdated version of Blackshades is even a threat, the answer is absolutely. Though its necessary to talk about the real threat associated with any malware, that is the delivery method and crypters.

So, delivery method refers to how the malware actually gets on the system. The easy methods are things like a mass phishing email that makes you download and execute some program, not many people fall for that.

Then of course there is the act of social engineering via bot or manually using things like Skype or Facebook to trick someone into trusting the criminal and then getting them to install the malware.



The third threat is drive-by exploits.

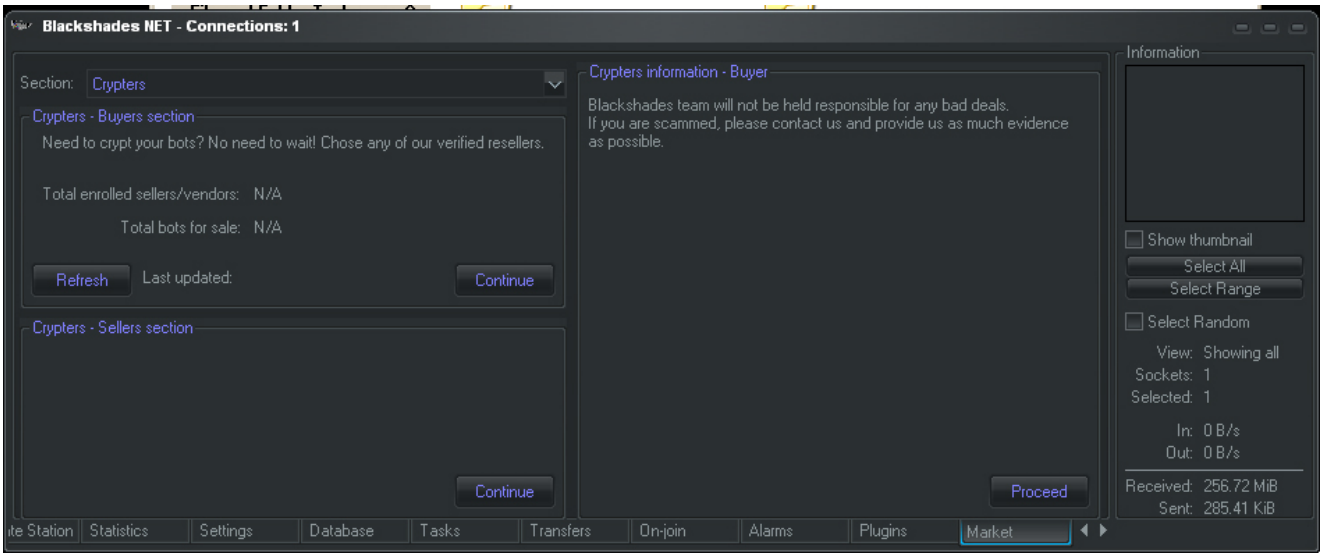
We have seen many types of malware distributed by drive-by exploits, all this attack requires is that a victim visit a certain website that exploits an application through the browser, something like Java or Flash. Usually this is a huge concern if the victim has failed to update those applications with security patches.

Next up are crypters, which are basically just applications that apply a custom algorithm to the malware binary, mixing up the code and making it difficult to detect using traditional passive scan methods.

This means that if an old version of Blackshades was encrypted with a modern crypter tool, it could potentially bypass an antivirus scan and even email filters that check for malware (Thanks Gmail!)

Crypters are the real underground market commodity and since they are usually created by individuals and maybe even small teams then sold to bot herders.

It is unlikely that we will see a mass arrest toward the entire crypter industry. They are also usually sold for far more than the malware itself, in fact Blackshades had a built-in crypter marketplace that it included in it's control panel, to make it easy for the bad guys to find a crypter and apply it to their malware.



Crypter marketplace — built into Blackshades interface

Lucky for us, most antivirus and anti-malware software includes active protection will detect the operations of the malware after it has "decrypted" itself, which all malware must do before it can actually run on the system.

In addition, a scan with a security product AFTER the malware has been installed will most likely remove it from your system, no problem.

Proactive Protection

So what can you do to protect yourself from RATs? Well common security practices are always recommended, but specifically with this type of threat:

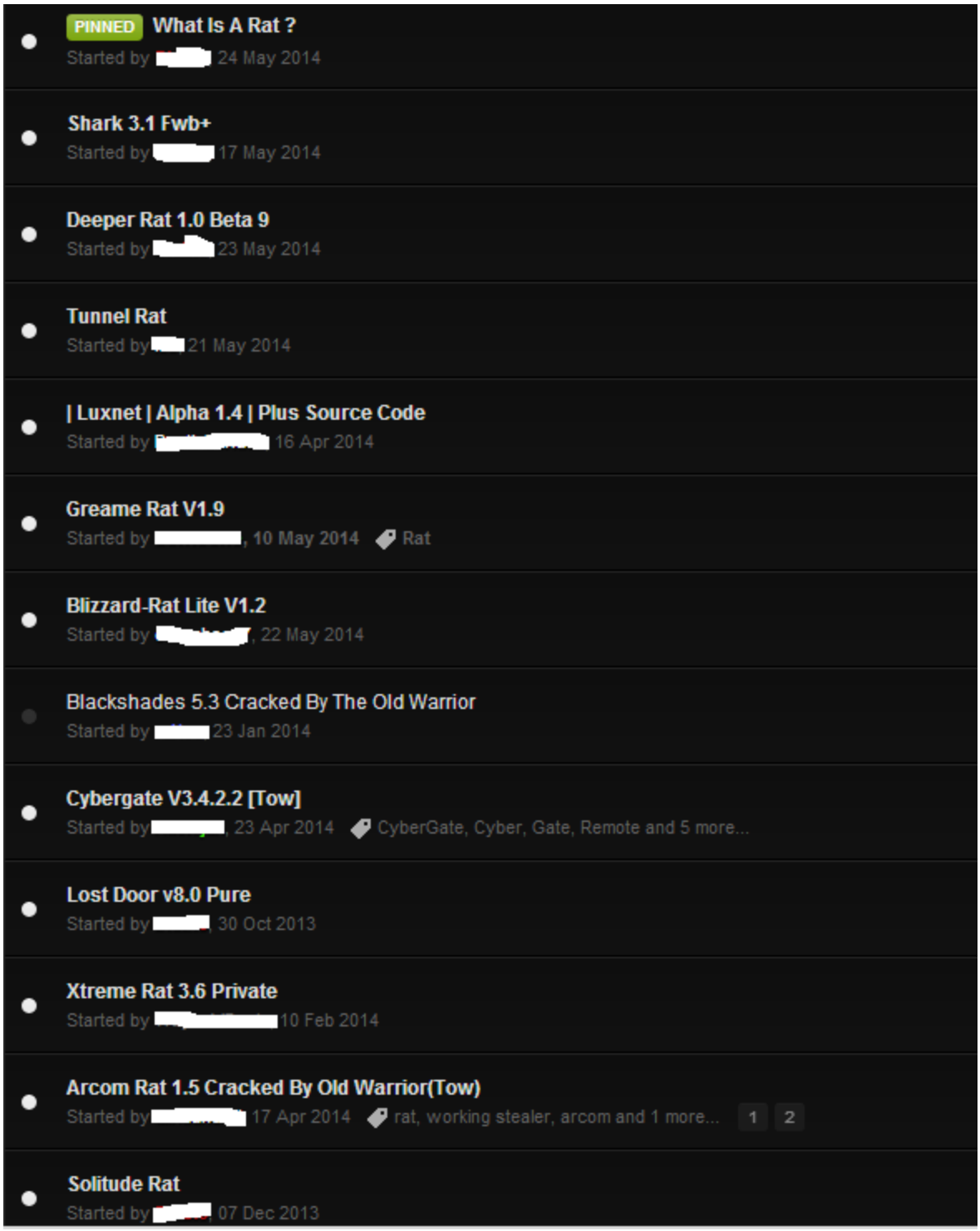
- Install security software, be it a free or paid version of something like Malwarebytes Anti-Malware, Kaspersky AV or whatever you want, as long as it stays updated and can detect the most common RATs.
- Put a piece of opaque tape over your webcam OR unplug your webcam (if possible)
- Keep your microphone muted when not using it. You can do this through the operating system in many cases.
- A common trick used by bad guys controlling a RAT is to paste the contents of whatever is currently loaded in the systems copy cache. It's important that whenever you copy something sensitive, like a password, you copy something less important when you are done.
- Log off of social media when you are done using it, a RAT can take control of your browser that includes a valid and open instance of a social media site, allowing them to post on your behalf.
- Be suspicious of everything, if your mouse moves on it's own or if your cursor suddenly types something that you don't remember typing or if a window closes or opens on it's own, maybe it's a good time to run a deep scan.

Is It Over?

Like I mentioned before, the threats that RATs pose will never be over, at least not for a while. We will see an evolution of their ability based on the market needs and the capabilities of hardware and software, you can expect that much of a change.

As far as Blackshades being done with, it's possible that a lack of interest due to the high profile of this malware might drive away a large portion of the market, in which case Blackshades won't be updated and it's functionality will become obsolete.

It will only be a matter of time though until we see the next big RAT malware making its way from underground forums to user systems, we certainly know there are plenty of them that can take the throne.



A listing of different RATs being advertised on hacker forums

The Bright Side

While RATs are incredibly dangerous, the bright side is that they are very inefficient.

The largest customer group for Remote Access Trojans are individuals or small groups who just want to use it to mess with people or steal valuable and sensitive information (images included). Even still, the time and effort it takes to launch an attack using a RAT and

obtaining anything juicy against a stranger is usually greater than most cyber criminals have the patience for.

The bottom line is that while RATs are a danger and you should keep an eye out for the possibility of one running on your system, we can all be even more afraid of things like Ransomware and Banker Trojans that have been skillfully created for the purpose of efficient user destruction.

Thanks for reading and safe surfing! @kujman5000