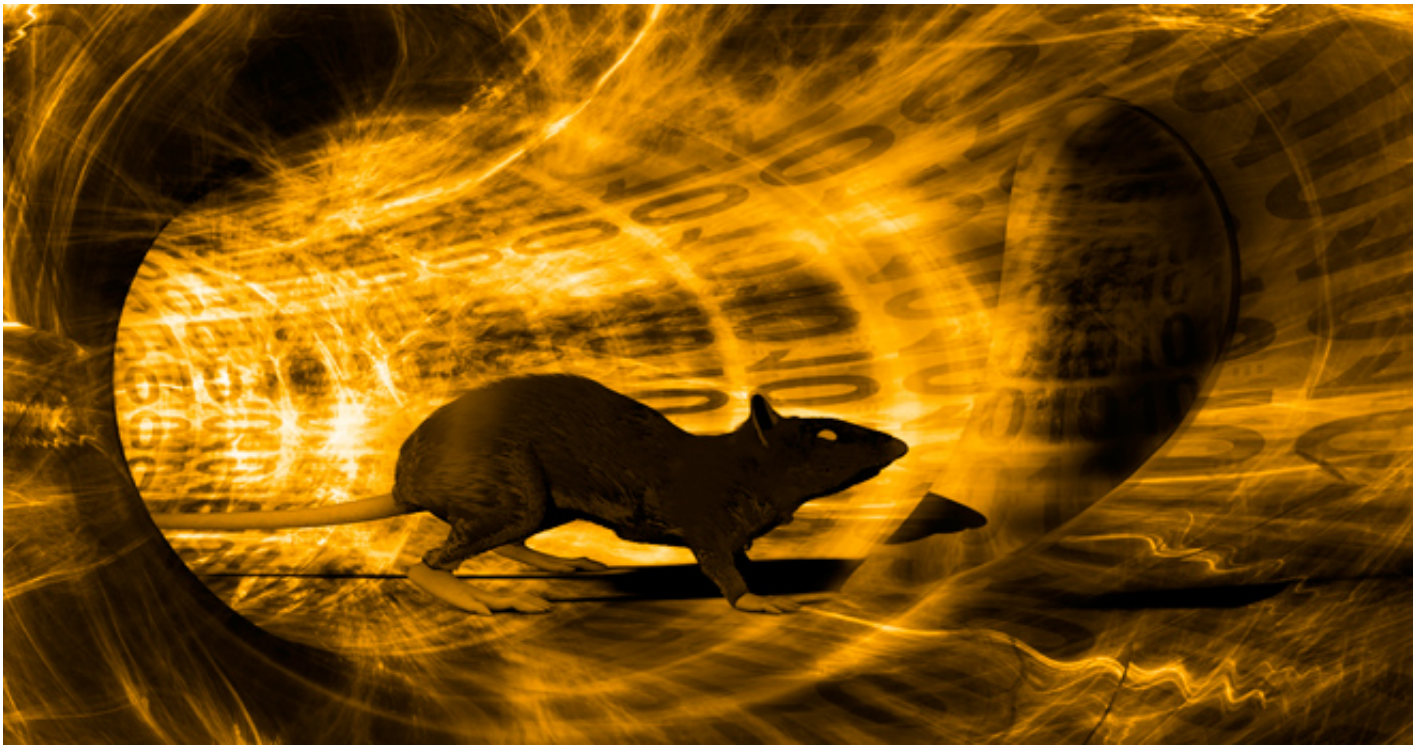
NanoCore: Another RAT tries to make it out of the gutter

The road to success is never straightforward. This is a tale of a RAT developer's persistence in the face of endless setbacks.
By: Lionel Payet
Created 23 Mar 2015

Contributor: Mark Anthony Balanza



Remote access Trojans, otherwise known as RATs, are nothing new and they frequently grab their fair share of security-related news headlines. Commonly used in both targeted and non-targeted attacks, and even on mobile devices, RATs are a popular tool among cybercriminals; whether for financial gain, espionage, or for something more creepy. Some RATs are more common than others, such as the infamous Blackshades (W32.Shadesrat), PlugX (Backdoor.Korplug), Poison Ivy (Backdoor.Darkmoon), or many others that have made a name for themselves in the cybercriminal underground. However, every once in a while a new RAT tries to emerge out of the unknown and "make it" just like its more common cousins. In this blog we'll take a look at one such up-and-coming RAT named NanoCore (Trojan.Nancrat) and see how human nature's love of cheap or, better yet, free stuff is helping this RAT in its efforts to hit the big time but potentially at a cost to the developer.

Free always beats cheap
RATs sold on underground forums can vary in price, ranging anywhere from US$25 to $250. In recent years the security community has seen plenty of new RATs come and go but where things always get dirty is when a cracked version of a RAT is leaked online for free. When this happens, usage of the RAT increases; cybercriminals are (arguably) human after all and love to get things for free. The NanoCore RAT has been around for a while now and was cheap to begin with; you can get the full version for just US$25. Add to this the fact that various versions of NanoCore have been leaked in the past and you can be sure this will grab the attention of people looking to get their hands on a free remote access Trojan.

The first cracked version of NanoCore was leaked in December 2013; but this was an alpha version with

very few capabilities enabled. The second leak in mid-February 2014 was a beta version with many more capabilities enabled and it was shortly after this version was posted to underground forums that we began to see spikes in NanoCore detections. There is a relatively short period of time between the leak of the first beta version (1.0.2.0) and the first spike, possibly due to it taking time for the news to spread or the bad guys becoming familiar with the new RAT before they started using it.

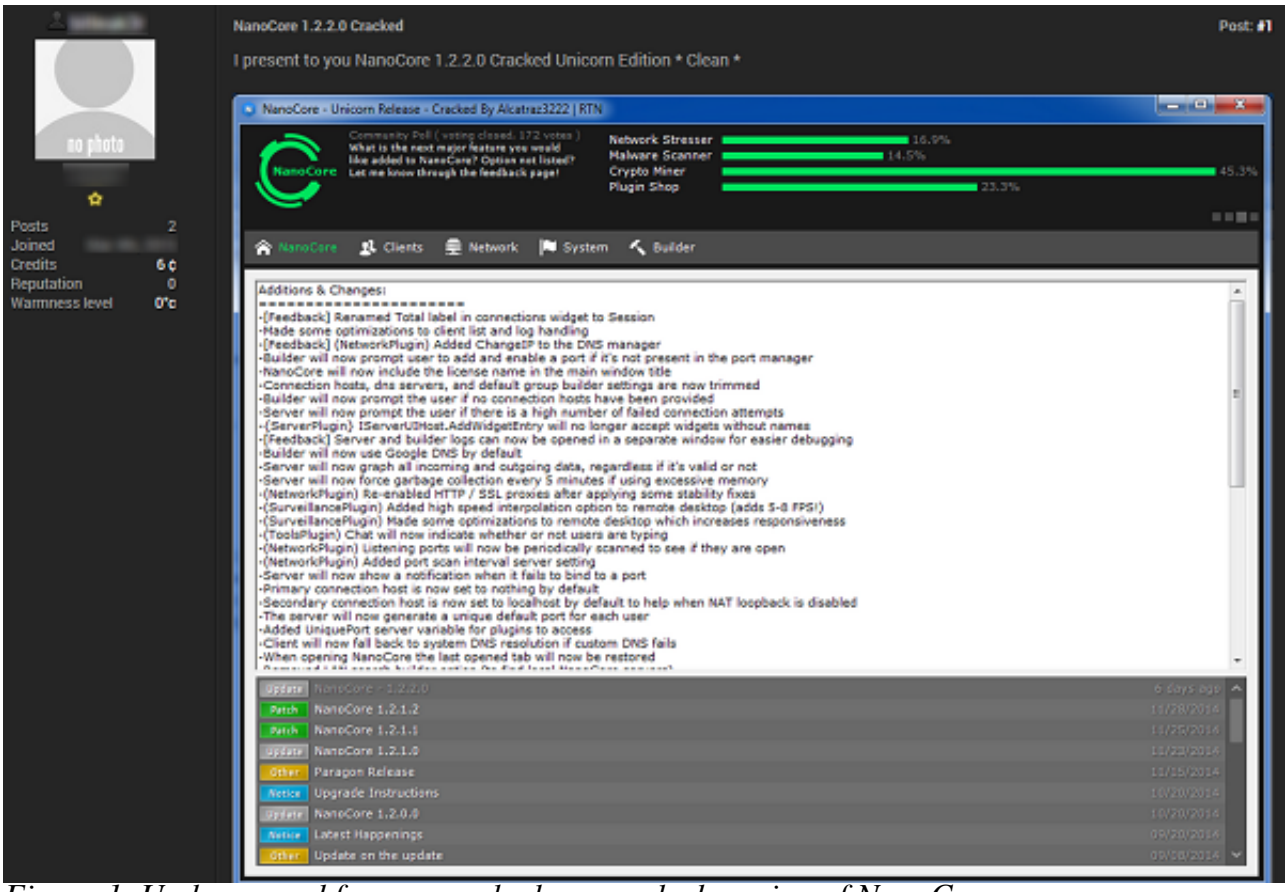


Figure 1. Underground forum user leaks a cracked version of NanoCore

A history of leaks

- Alpha version leaked in December 2013
- Beta version 1.0.2.0 leaked in February 2014
- Beta version 1.0.3.0 leaked by multiple sources in March and April 2014
- Beta version 1.1.0.7 leaked by multiple sources in July and August 2014
- Beta version 1.1.0.10 leaked in October 2014
- Full version 1.2.2.0 (premium plugins) leaked in March 2015

It seems that every time the author tries to develop and improve NanoCore, one of the customers invariably ends up leaking a copy of it for free. This surely has to be a major disincentive for the original developer but they seem to possess endless optimism and persist to create new versions with enhanced capabilities, maybe in the hope that eventually enough customers will pay.

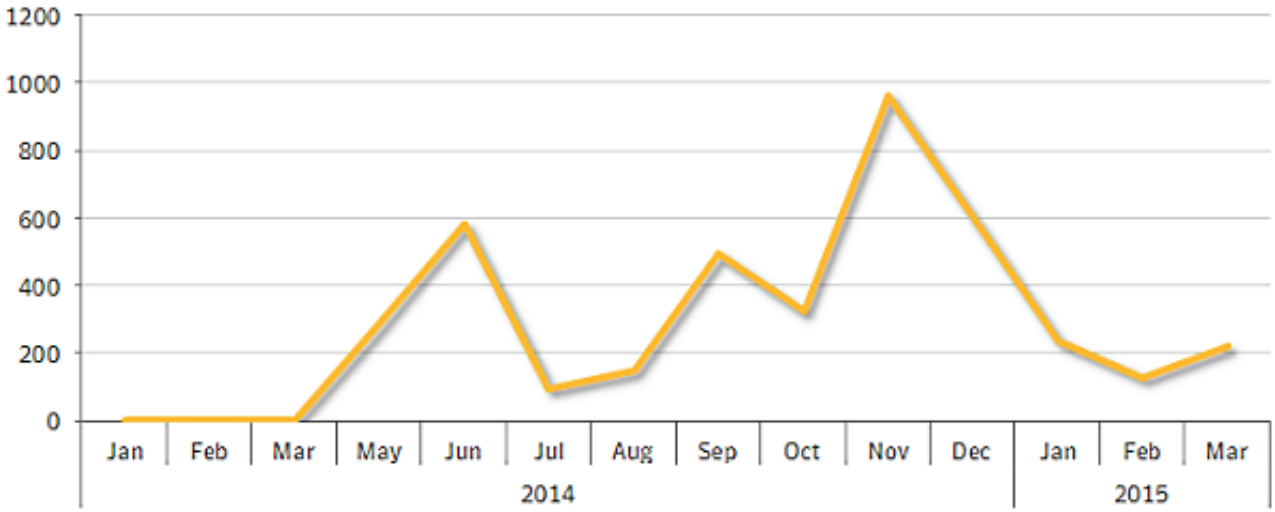


Figure 2. Detection overtime for Trojan.Nancrat

We can see from the graph shown in Figure 2 that following the leak of a version of NanoCore there is an obvious increase in our detections of the RAT. This can be seen following the multiple leaks of version 1.0.3.0 in March and April, version 1.1.0.7 in July and August, version 1.1.0.10 in October, and finally the most recent leak of version 1.2.2.0 in March.

NanoCore detections are not confined to specific geographical regions but cover countries right across the globe, as can be seen in Figure 3.

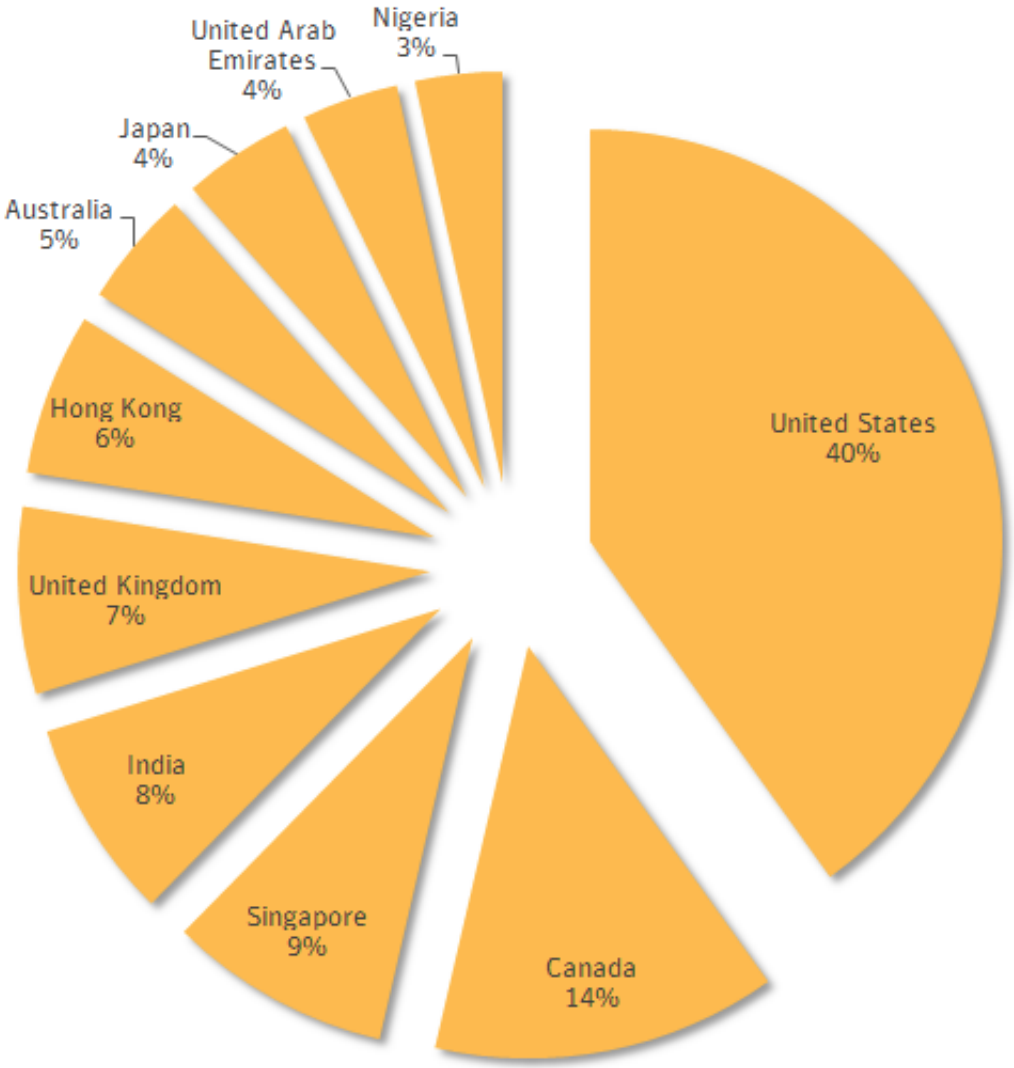


Figure 3. Top ten countries affected by Trojan.Nancrat (Jan 2014 to March 2015)

NanoCore targets the energy sector

Earlier this month, the full version of NanoCore (1.2.2.0) was leaked, which again resulted in an increase of its usage in both targeted and non-targeted attacks. The RAT is being distributed through malicious emails in most instances. One example we came across of NanoCore being used in a targeted attack involved a spam run that started on March 6. The targeted emails are being sent to energy companies in Asia and the Middle East and the cybercriminals behind the attack are spoofing the email address of a legitimate oil company in South Korea. Attached to the email is a malicious RTF file that exploits the Microsoft Windows Common Controls ActiveX Control Remote Code Execution Vulnerability (CVE-2012-0158) and drops Trojan.Nancrat.

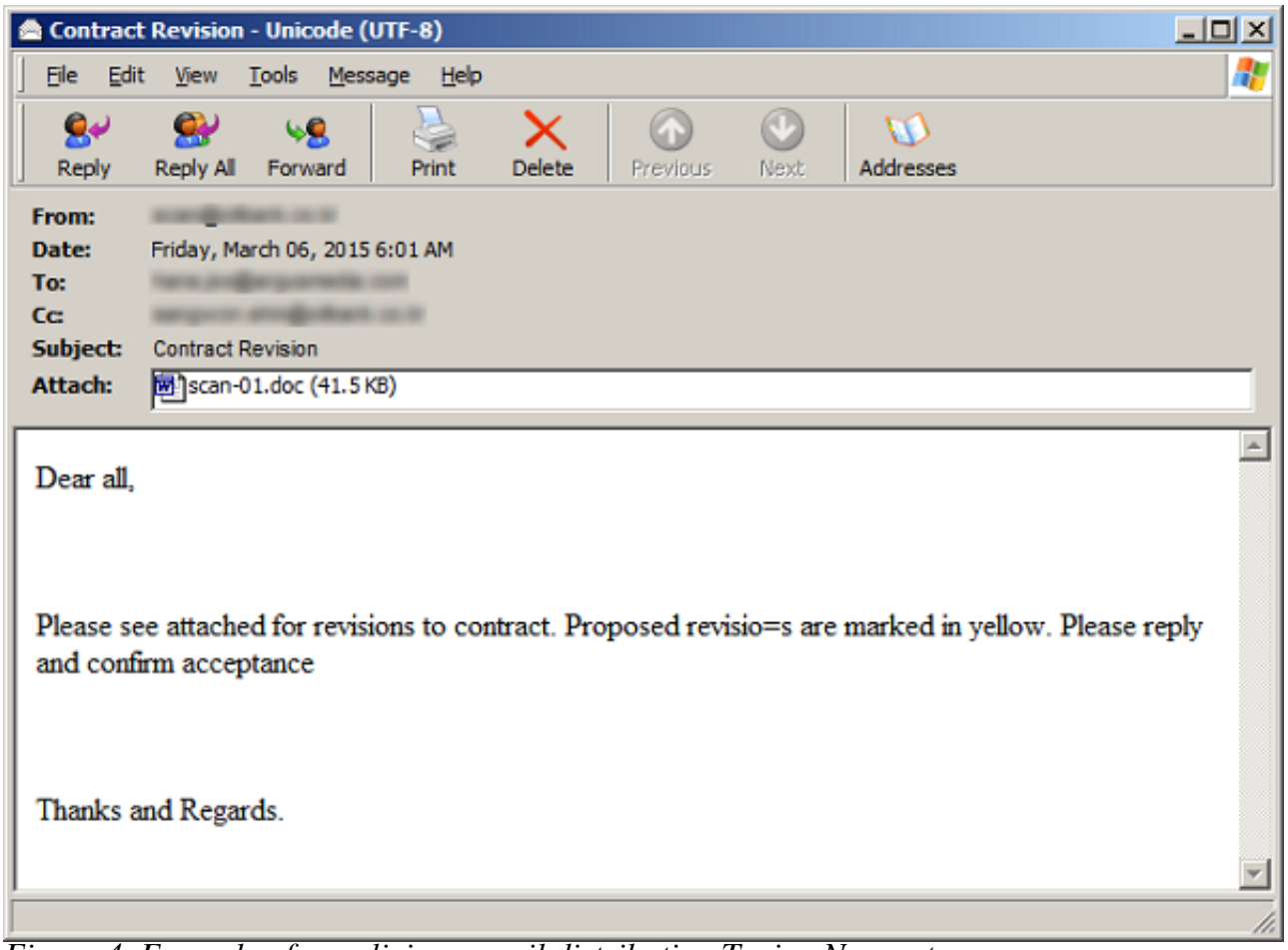


Figure 4. Example of a malicious email distributing Trojan.Nancrat

What does the future hold?
If the past is a guide to the future, considering the latest leak of this RAT we can expect to see more Trojan.Nancrat detections in the coming weeks.

The cracked versions of NanoCore are now not only available on the dark web but also on the visible web. That means it's not just the more experienced cybercriminals who can easily access this malware for free, but also script kiddies eager to start their cybercriminal careers. The more the NanoCore malware is used and is visible on the underground, the higher the chances that one day it may end up just as well-known as some of the notorious RATs that have come before it. The question is, will the developer make the money that they intended to in developing NanoCore or does success only comes at the expense of lost revenue due to piracy?