Dr.WEB®
Anti-virus

Win32.Ntldrbot (aka Rustock.C) no longer a myth, no longer a threat

Rootkit is a program (or combination of several programs) designed to take fundamental control (in Unix terms «root» access, in Windows terms «Administrator» access) of a computer system, without authorization by the system's owners and legitimate managers and obscure their presence on the system through subversion or evasion of standard operating system security mechanisms.

After Wikipedia

Preface

Various anti-virus evasion techniques have become a predominant trend of the malware development. Rootkits are getting more and more complex; their number grows month after month. Most of them are dull coded implementations of someone else's ideas. However, very interesting pieces of malware emerge every now and then. One of such phantom rootkits that has been moving around undetected is described in this article.

Botnets

In order to understand the material provided in the article you need to become familiar with several malware-related terms. One of them is a botnet. Again according to Wikipedia, a botnet is a term for a set of software robots, or bots, which run autonomously and automatically. They run on groups of zombie computers controlled remotely. Typically a bot included in a botnet is covertly installed on a target machine so an intruder can perform certain actions exploiting software and hardware of an infected computer. As a rule botnets are applied for illegal activities – spamming, brute force hack attacks of a remote host, DDoS attacks, etc.

According to Secure Works, the botnet built by Rustock is the third largest and distributes around 30 billion spam messages daily, most of them are about securities and medicines. The Rustock botnet summary:

- an estimated number of infected machines – about 150, 000;
- the botnet spamming capability: about 30 billion messages a day;
- rootkit component: yes.

Now you can see what we are dealing with and what impact of such networks can be.

Rustock growing up

The name Rustock was given to the malware by Symantec anti-virus experts. The author of the rookit liked it so much that he came to use it from then on. In early version of the rootkit one could come across with the following string: "Z:\NewProjects\spambot\last\driver\objfre\i386\driver.pdb". In subsequent versions a string containing «spambot» was supplemented by a string «Rustock rootkit v 1.2".

Three «age-groups» are distinguished among rootkits of this class: A, B and C. It is not quite accurate, as the author often modified the rootkit code, changed the functions` interception methods and improved the program's stability. However, one version didn't undergo too many modifications. In fact switching from one version to another can be followed pretty easily.

At the end of 2005 or early in 2006 the first beta-versions of Rustock.A cane into being and were used to test new technologies. The most obvious difference between them was the driver names: i386.sys, sysbus32. The rootkit intercepted the system calls table (SSDT) and IRP-packets for hiding.

The betas were followed by a completed Rustock.A – pe386.sys (version 1.0), that used more sophisticated stealth techniques. First of all the author abandoned the SSDT interception and resorted to intercepting the 0x2E interrupt (Windows 2000) and MSR_SYSENTER(Windows XP+). ADS (Alternate Data Stream) were used to hide a malware file on an NTFS disk. The body of the rootkit was placed at %SystemRoot%\system32:[a string of random digits].

Still in 2006 a Rustock.B beta (huy32.sys) appeared, a completed Rustock.B - lzx32.sys (version 1.2) came shortly after it. The new version intercepted INT2E/MSR_SYSENTER, ADS (%Windir%\System32:lzx32.sys). Moreover, the author enhanced the rootkit with interception of network drivers: tcpip.sys, wanarp.sys and ndis.sys, so it could bypass firewalls and hide spam traffic.

Variations of the malicious programs with limited functionality were also released to restore interceptions in case they were detected and blocked by anti-rootkit or anti-virus software. Variations with random driver name were used as well.

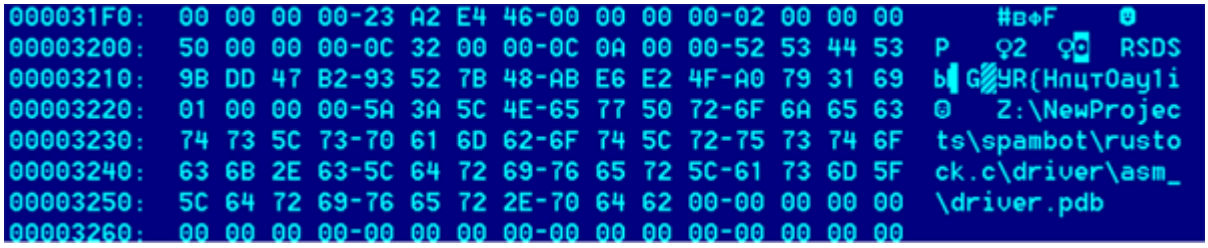
Some anti-virus vendors, TrendMicro for example, provided a description of Rustock.C in their virus encyclopedia, however, the subject piece of the malicious code turned out to be another experimental variation of Rustock.B.

Rustock.C

Rumours on Rustock.C started in summer 2006. Anti-virus labs and virus makers began their search. The first wanted to analyze it and improve their rootkit detection methods, the latter – to steal and then to use more efficient stealth and self-protection techniques.

Time passed, but the hard-sought sample didn't turn up or anti-virus labs failed to find time for proper analysis. Indeed, they have thousands of files to work on every day. Apart from forum discussions no one provided clear evidence if Rustock.C actually existed or the opposite. Many vendors found it more convenient to avoid the subject of the C-version saying, "Since we haven't found it, it doesn't exist. It's just a myth" or: "Speak of a nonsense, you might as well bring up Rustock.C here, the rumour has it being in the wild but no one actually has seen it".

But it turned out that Rustock.C is not a myth. Some anti-virus labs didn't give up searching and succeeded.



As the snapshot above shows, its author accepted the suggested name of Rustock. 18 months passed and Rustock.C was discovered at the beginning of 2008. All this time the rootkit was in the wild compromising PCs and turning them into bots.

Virus Monitoring Service of Doctor Web, Ltd. collected about 600 samples of this version of the rootkit but nobody knows how many of them exist in the wild. Most of them are built in September – October, 2007. Dr.Web virus analysts spent several weeks on its unpacking, thorough examination and perfection of the detection and curing techniques.

Assuming that the malware has been running free and completely invisible since October 2007, one could asses the resulting amount of infected traffic. Unsolicited mail has become a worldwide issue. Many of us notice our traffic increase for no apparent reason and experts assess up to 90 per cent of our e-mail correspondence to be completely irrelevant and irritating. Win32.Ntldrbot is one of the reasons behind the booming activity of spammers. Win32.Ntldrbot has been able to hide from anti-viruses for quite a while. It means that no one can guarantee that your machine is not infected. Probably it has become a bot and is sending out spam right now.

Key features of the rootkit

- Sophisticated polymorphic self-protection of the rootkit makes its extraction and analysis extremely difficult.
- Implemented as a driver, it runs on the lowest kernel level.
- Has a self-protect function, prevents runtime changes.
- Uses active anti-debugging techniques: monitors setting hardware breakpoints (DR-registers), disrupts operation of the kernel-level debuggers (e.g. Syser, SoftIce). WinDbg debugger won't work, if the rootkit is running.
- Intercepts the following system functions using non-standard method:
  - NtCreateThread
  - NtDelayExecution
  - NtDuplicateObject
  - NtOpenThread
  - NtProtectVirtualMemory
  - NtQuerySystemInformation
  - NtReadVirtualMemory
  - NtResumeThread
  - NtTerminateProcess

  - NtTerminateThread
  - NtWriteVirtualMemory
- Functions as a file-virus and infects system drivers.
- A particular sample of the rootkit becomes adjusted to the hardware of an infected machine and most likely won't run on another computer.
- Utilizes time-triggered re-infection feature. An old infected file is cured. So the rootkit «wonders» through system drivers infecting only one at a time.
- Filters calls to an infected file, intercepts FSD-procedures of a file system driver and redirects a call to the original file instead of the infected one.
- Features anti-rootkit protection.
- Links its library to one of the Windows system processes, so the library starts spamming. A driver is connected to the DLL using a special command transfer mechanism.

Conclusions

Once virus writers manage to obtain a sample of the rootkit, the flourishing of similar technologies and their implantation into viral programs will become a matter of time.

At present, no other anti-virus program, except for Dr.Web anti-virus can detect Rustock.C. None anti-virus, except for Dr.Web anti-virus, can cure system files infected by it. Those who are not Dr.Web customers can download free Dr.Web CureIt! utility and scan the computer, to be on the safe side.

In 90s there was a saying popular among IT-guys. Today I devote it to the Rustock author: *"Everything which can be run, can be cracked"*.

Virus analysts

Vyacheslav Rusakoff

Doctor Web, Ltd.

Dr.WEB®
Anti-virus

About Doctor Web, Ltd.

Doctor Web, Ltd. is a Russian company developing and distributing Dr.Web IT-security solutions.

Dr.Web anti-virus has been developed since 1992; it has always shown perfect results of malicious programmes` detection and complies with international security standards.

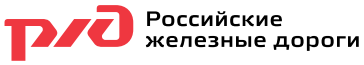
Doctor Web, Ltd. is one of a few anti-virus vendors in the world that owns its technologies for detecting and curing malware, has its own virus monitoring service and analytical laboratory. This provides a rapid response to latest threats and allows to solve any problems of customers in a few hours.

State certificates and awards received by the Dr.Web Anti-virus, as well as the geography of our users are the best evidence of exceptional trust to the products created by the talented Russian programmers.

Large enterprise-network experience

Customers of Doctor Web, Ltd include large and well-known companies: Russian and, international banks, state and educational institutions, research departments with dozens of thousands computers in their networks. Highest government institutions and oil and gas companies of Russia entrust their information security to Doctor Web, Ltd.





125124, Russia, Moscow, 3-ja ulitsa Yamskogo polya 2-12A
Tel: +7 (495) 789-45-87
Fax: +7 (495) 789-45-97
http://www.drweb.com
http://www.freedrweb.com
http://www.av-desk.com

Technical support service:
http://support.drweb.com/new/

Demo-versions:
http://buy.drweb.com/demo