BKDR_RARSTONE: New RAT to Watch Out For - TrendLabs Security Intelligence Blog

By Abraham Camba (Threat Researcher)

Published: 2013-02-27 · Archived: 2026-04-05 17:04:36 UTC

Last year, we reported about PlugX a breed of Remote Access Trojan (RAT) used in certain high-profile APT campaigns. We also noted some of its noteworthy techniques, which include its capability to hide its malicious codes by decrypting and loading a backdoor "executable file" directly into memory, without the need to drop the actual "executable file".

Recently, we uncovered a RAT using the same technique. The new sample detected by Trend Micro as BKDR_RARSTONE.A is similar (but not) PlugX, as it directly loads a backdoor "file" in memory without dropping any "file". However, as we proceeded with our analysis, we found that BKDR_RARSTONE has some tricks of its own.

We obtained the sample through a spear phishing email that contains a specially-crafted .DOC file (detected as TROJ_ARTIEF.NTZ). This Trojan drops and executes BKDR_RARSTONE.A, which in turn drops the following files:

- %System%\ymsgr_tray.exe – copy of BKDR_RARSTONE.A
- %Application Data%\profile.dat – blob file containing malware routines

BKDR_RARSTONE.A then executes the dropped copy *ymsgr_tray.exe*. This backdoor then opens a hidden *Internet Explorer* process, in which it injects the codes contained in *profile.dat*.

As with PlugX, the injected code decrypts itself in memory. Once decrypted it "downloads" a .DLL file from its C&C server and again loads it in the memory space of the hidden *Internet Explorer* process. This "downloaded" file is actually not dropped onto the system, but instead directly loaded in memory, making file-based detection ineffective.

Typical of a backdoor, BKDR_RARSTONE.A connects to specific sites and can perform several routines, which include enumerating files and directories, downloading, executing, and uploading files, and updating itself and its configuration.

Worth noting among its backdoor routine is its ability to get installer properties from Uninstall Registry Key entries. It does this to get hold of information about the installed applications in the affected system, as well as to know how to uninstall certain applications. This can be handy in silently uninstalling applications, which may interfere with the backdoor's routine, e.g. anti-malware software and the likes.

Another interesting feature of this backdoor is the communication method it uses, specifically SSL. This use of SSL has a two-fold advantage: it guarantees that communication between the C&C and infected system is encrypted, at the same time it blends in with normal traffic.

In our 2012 Security Roundup, we noted that data breaches and other targeted attacks initiated last year used several tools (including PlugX) to achieve stealth. This stealth enabled the attackers to remain hidden and continue their operations within the target network. The appearance of RATs like BKDR_RARSTONE, shows that the bad guys are continuously modifying and improving their tools.

For users and organizations to arm themselves from these attacks, they should first acknowledge that the bad guys have certain advantages. Director for Threat Research Martin Roesler believes that such acceptance enables entities to deal with the problem properly and deploy an inside-out protection.

Trend Micro users are protected by the Smart Protection Network™. In particular, file reputation service detects and deletes BKDR_RARSTONE. Web reputation and email reputation services blocks access to the said C&C and related email respectively.

Trend Micro will continue to monitor BKDR_RARSTONE's development and investigate if there are any campaigns behind it.
