How to “Root” a Rootkit That Supports Root Processes Using Strider GhostBuster Enterprise Scanner

Yi-Min Wang
Doug Beck

February 11, 2005

Technical Report
MSR-TR-2005-21

Microsoft Research
Microsoft Corporation
One Microsoft Way
Redmond, WA 98052

How to “Root” a Rootkit That Supports Root Processes Using Strider GhostBuster Enterprise Scanner

Yi-Min Wang & Doug Beck (February 11, 2005)

Some rootkits that hide resources through ***user-mode API interception*** support the notion of *“root processes”* [H03] (or *“privileged processes”* [N04]), which are exempt from being hooked for API interception and so can see all hidden entries. In this paper, we use Hacker Defender (1.00 and older) as an example and describe a simple technique to “root” such a rootkit (i.e., to run our program as a root process of the rootkit) using the Strider GhostBuster quick scanner to identify infected machines in the enterprise.

Step #1: Identify a Root Process

Root processes are usually hidden. So the first step is to detect hidden processes. By enumerating the processes through the regular Process32First/Process32Next APIs (or any of your favorite high-level APIs) and enumerating them again using a lower-level call described in the Appendix, and taking a diff, we can detect any user-mode hidden process ***within a fraction of a second***.

Not all hidden processes are root processes. One way to identify a root process is to inject the diff’ing code described above into every hidden process; the ones that do not report a diff are root processes. In practice, the number of hidden processes is small. So one can manually try Step #2 on every hidden process; whichever that gives us what we want is a root process.

Step #2: Launch cmd.exe as a Root Process

Suppose hxdef100.exe is the identified hidden root process. We type “copy C:\windows\system32\cmd.exe .\hxdef100.exe” and “start .\hxdef100.exe”, which will launch a command window with the process name “hxdef100.exe”. Since the support for root processes is usually based on simple filename pattern matching, this command window is now a root process of Hacker Defender; that is, we have rooted the rootkit.

Step #3: Launch Any Other Program as a Root Process

User-mode rootkits usually rely on each parent process to infect its child processes upon their creation. Since a root process is not hooked, it will not hook any of its child processes and so all its child processes are root processes as well. From the command window, we can delete hidden files; we can launch TaskMgr.exe to kill hidden processes; we can launch RegEdit to delete the hidden auto-start Registry keys under HKLM Services; we can even launch any anti-virus scanner that has signatures for Hacker Defender and let it do its job***, all while the rootkit is still running***. See Figures 1~5 at http://research.microsoft.com/rootkit.

References:

[H03] “How to become unseen on Windows NT,” May 8, 2003.
[N04] “NTIllusion -- A portable Win32 userland rootkit”, Phrack Magazine, July 13, 2004.
[NT] http://msdn.microsoft.com/library/default.asp?url=/library/en-us/sysinfo/base/ntquerysysteminformation.asp

Appendix:

Consult [NT] and do the following to retrieve the true list of processes by bypassing its rootkit-intercepted counterpart inside ntdll.dll. This can be used to detect any user-mode hiding rootkits including AFX, etc.

```
__forceinline
__declspec(naked)
NTSTATUS NTAPI NtQuerySystemInformation(
  SYSTEM_INFORMATION_CLASS SystemInformationClass, PVOID SystemInformation,
  ULONG SystemInformationLength, PULONG ReturnLength) {
    __asm {
        mov         eax, 0xAD
        mov         edx, 7FFE0300h
        call        edx   // (or call   dword ptr [edx])
        ret         10h
    }
}
```