First thing I did when I ran the VM was look through the root C: file system, and registry. At that point we stumbled upon something called vanquish. Vanquish readme noted how to remove Vanquish ran on the VM was GMER

what was maliciously changed on the system:

- System service installed called vanquish
- Hides files/folders with string vanquish
- Hides registry with string vanquish
- Hides services called vanquish
- Intercepts LogonUserW calls and dumps user/pass to log @ c:\vanquish.log

what files are responsible for the changes:

- within the vanquish-0.2.1\bin, there is a vanquish.exe autoloader binary, and dll

how to remove the changes:

- removal flag within rootkit installer/setup

what tools and techniques you tried:

- removal through setup.cmd –remove flag.

In the registry, there are a few interesting startups:

- FAT Filesystem initialization - wscript "C:\windows\fat.vbs" "c:\windows\fat.bat"
- ISW - checkpoint\ZAForceField\ForceField.exe /icon="hidden
- ZoneAlarm Client – Zone Labs\ZoneAlarm\zlclient.exe

The latter two were only suspicious because I had not seen forcefield before, and was not familiar with the latest zonealarm so the extra paranoid part of me thought "maybe xeno hooked/changed these programs somehow". My thinking there would be to potentially do an md5 checksum to see if it matched what it was supposed to:

how to remove the changes:

- removal registry keys from registry

what tools and techniques you tried:

- regedit, md5 checker

The “FAT Filesystem initialization” turned us to fat.bat and fat.vbs in system. There we noticed that the FU rootkit was installed. Also GMER reported that fu.exe was installed.

what was maliciously changed on the system:

- phd command hides drivers. Hidden drivers include:
  - msdirectx.sys
  - mmpc.sys
- ph command hides pid 4. pid4 is SYSTEM. At that point we tried to pull down all processes run by SYSTEM.
- Fu rootkit can set the AUTH_ID to system on processes.

what files are responsible for the changes:

- c:\windows\system32\drivers\fu.exe
- c:\windows\system32\drivers \msdirectx.sys

how to remove the changes:

- fu.exe is hidden, so there must be some way to un-hide it, so that you can run it. Alternatively it seems like you can use whatever methods to load msdirectx.sys and issue the remove command for fu.exe through msdirectx.sys?

what tools and techniques you tried:

GMER

I already had a suspicion that hackerdefender was installed because it’s a fairly popular rootkit. Using GMER unveiled hacker defender:

what was maliciously changed on the system:

- Hides table entries named hxdef* and rcmd.exe
- Hides processes named hxdef* and rcmd.exe
- Hides services named HackerDefender*
- Hides regkeys HackerDefender100, Legacy_HackerDefender100, HackerDefenderDrv100, and Legacy_HackerDefenderDrv100
- Runs [blob]taskmgr.exe on startup
- Hides UDP port 4500
- Establishes a backdoor shell that binds to any TCP process?

what files are responsible for the changes:

- hxdef100

how to remove the changes:

- HackerDefender can uninstall with “net stop HackerDefender100”

what tools and techniques you tried:

GMER

Misc:

Saw a folder in GMER: c:\windows\system32\drivers\cool_beans, but didn’t know what it was used for.

Saw a bunch of suspicious Drivers entries in Autoruns.exe:

- C:\Windows\system32\Drivers\azdow88m.sys
- C:\Windows\system32\Drivers\basic.sys
- C:\Windows\system32\Drivers\breakonthrutotheotherside.sys
- C:\Windows\system32\Drivers\Changer.sys
- C:\Windows\system32\Drivers\ctr12cap.sys
- C:\Windows\system32\Drivers\i2omgmt.sys
- C:\Windows\system32\Drivers\lbrtfdc.sys
- system32\Drivers\npf.sys
- system32\Drivers\passthru.sys
- system32\Drivers\PCIDump.sys
- C:\Windows\system32\Drivers\PDCOMP.sys
- C:\Windows\system32\Drivers\PDFRAME.sys
- C:\Windows\system32\Drivers\PDRELI.sys
- C:\Windows\system32\Drivers\PDRFRAME.sys
- SelfCheck - C:\mordor\branches\POCAP\i386\stop
- WDICA - C:\Windows\system32\Drivers\WDICA.sys

Some are obviously more suspicious than others, like mordor which was hidden. breakonthrutotheotherside I think is from one of the x86 classes. The other sys files I wasn’t really sure about so the only thing I can really think of is to run them through virus total or some md5 checksum online tool which I haven’t discovered yet.

We ran strings on mmpc and that found:

C:\shadowwalker_corey\BIN\i386\mmpc.pdb, so I assume this is some variant of the shadowwalker rootkit. I read things that said this hooks IDT stuff, and something with the page fault handler and the way virtual memory works.

Autoruns picked up ctl.exe

Strings on ctl.exe unveiled that it is actually He4HookControl

what was maliciously changed on the system:

- Looks like He4hook installs drivers, adds proc/users to some sort of list, maybe changes RWDV privileges, hooks file systems, and does something with heaps…but I wasn't able to find what/where it is called.

what files are responsible for the changes:

how to remove the changes:

what tools and techniques you tried:

- Autoruns, wordpad