GENERAL DYNAMICS
Fidelis Cybersecurity Solutions

www.fidelissecurity.com
www.threatgeek.com
@FidSecSys
+1800.652.4020

Fidelis Threat Advisory #1008

Darkseoul/Jokra Analysis And Recovery

March 21, 2013

Document Status: FINAL
Last Revised: 2013-03-21

A recent cyber-attack reported within the South Korean broadcasting and banking infrastructure reportedly brought down over 35,000 systems. This attack has drawn comparisons in intent and method to the recent wiping attack against Saudi Aramco by the Shamoon malware. Shamoon has been covered extensively by the community, and was covered in Fidelis Threat Advisory #1007. Naturally our curiosity was peaked and we acquired samples of the malware and started analysis.

The initial analysis has been posted on the Fidelis Threat Geek blog and will be expanded upon in this advisory. This write-up will focus on the wiper malware used and the recovery techniques that are possible.

From preliminary analysis it is known that the malware will overwrite the Master Boot Record (MBR) and Volume Boot Record (VBR). The records and files overwritten by the malware so far have been wiped with patterns of 'HASTATI' or 'PR!NCPES'.

The malware samples that have been analyzed by our team are different in code and function from the Shamoon malware. However, by using the same recovery methods found in advisory #1007 the files and data are indeed recoverable.

Wiper Malware Overview

Two malware samples obtained were used in the analysis. The malware has been named 'DarkSeoul' and 'Jokra' by the community.

Our samples have been touched on in our blog entry and other samples have been covered in blogs around the community.

239ed75323.exe:	5fcd6e1dace6b0599429d913850f0364
mb_join.exe:	0a8032cd6b4a710b1771a080fa09fb87

The malware gains disk access by opening the physical drive as a file.

```
Disk Access (Func 00401d55):
  sprintf(filename_str, "\\.\PhysicalDrive%d", 0)
  hFile = CreateFileA(filename_str, GENERIC_READ | GENERIC_WRITE,
                      FILE_SHARE_READ | FILE_SHARE_WRITE, NULL,
                      OPEN_EXISTING, NULL)
```

Example of the wiper opening the drive as a file.

The first section that the malware overwrites is located at 0x7000. This is sector 56 and is normally the VBR location of a Windows XP system. It continues the pattern of 'HASTATI' or 'PR!NCPES'' for 102,400d bytes.

```
Wiper Selection (Func 00402079):
  and [local.1], 0        ;(local.1->"PR!NCPES")
  mov esi,[arg.2]    ;arg.2 = 0x38 on first call
  eax=0
  shld eax,esi,9
  mov edi,[arg.1]
  mov [arg.2], eax
  lea eax, [arg.2]
  shl esi,9

  SetFilePointer(hFile, esi, eax, FILE_BEGIN) // on first call -- 0x009efab8:0x00007000
  WriteFile(hFile, &arg.3, 512, &local.1, NULL)
```

Example of how the wiper selected the location to overwrite on the first call.

If this is hardcoded for 0x7000 then it will not wipe the VBR of any systems after and including Vista, as those VBR locations are in different areas.

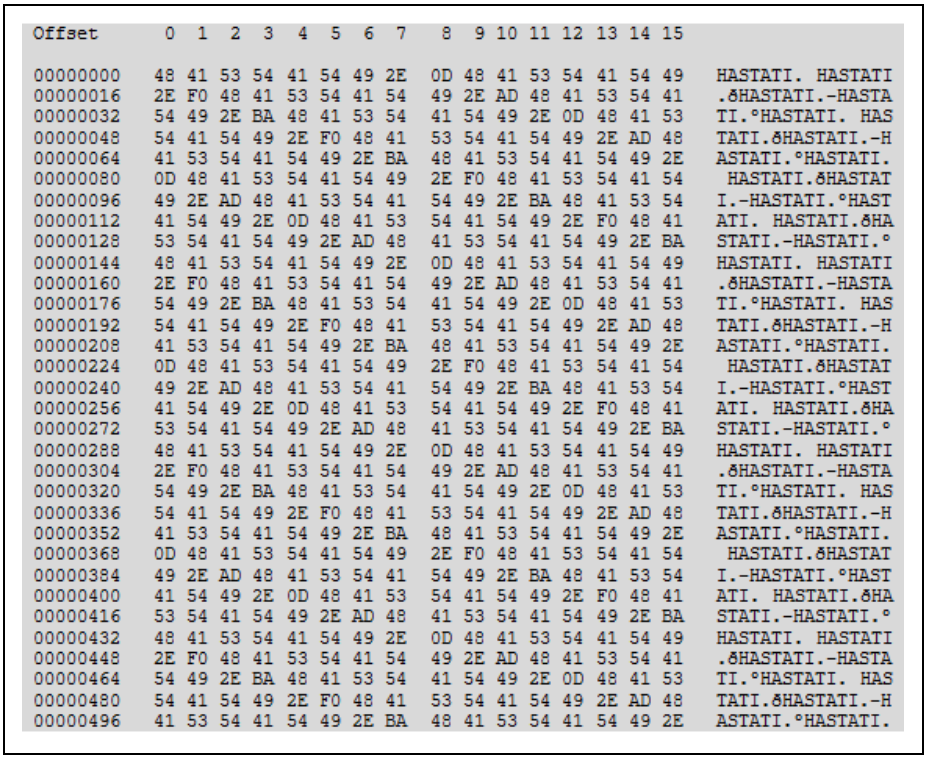
During testing both malware samples were executed in a Windows 7 VM. Neither wiped the MBR or the VBR—they only overwrote files within the file system—but the system wasn't prevented from starting up.

The malware writes a 512-byte pattern to the disk in XP and a 1023 byte pattern in Windows 7.

```
00401D43  > 57              PUSH EDI
00401D44  . 8D45 D0         LEA EAX,[LOCAL.12]
00401D47  . 50              PUSH EAX
00401D48  . FF75 08         PUSH [ARG.1]
00401D4B  . 897D D0         MOV [LOCAL.12],EDI
00401D4E  . FF75 F0         PUSH [LOCAL.4]
00401D51  . FF75 EC         PUSH [LOCAL.5]
00401D54  . FF96 74030000   CALL DWORD PTR DS:[ESI+374]   kernel32.WriteFile
00401D5A  . FF4D DC         DEC [LOCAL.9]
00401D5D  .^75 E4           JNZ SHORT 239ed753.00401D43
```

Example of the loop responsible for overwriting the disk and files.

As observed during a debugging session the following screenshot shows one of the 512-byte patterns it writes to disk:



```
Offset      0  1  2  3  4  5  6  7   8  9 10 11 12 13 14 15

00000000   48 41 53 54 41 54 49 2E  0D 48 41 53 54 41 54 49   HASTATI. HASTATI
00000016   2E F0 48 41 53 54 41 54  49 2E AD 48 41 53 54 41   .ðHASTATI.-HASTA
00000032   54 49 2E BA 48 41 53 54  41 54 49 2E 0D 48 41 53   TI.°HASTATI. HAS
00000048   54 41 54 49 2E F0 48 41  53 54 41 54 49 2E AD 48   TATI.ðHASTATI.-H
00000064   41 53 54 41 54 49 2E BA  48 41 53 54 41 54 49 2E   ASTATI.°HASTATI.
00000080   0D 48 41 53 54 41 54 49  2E F0 48 41 53 54 41 54    HASTATI.ðHASTAT
00000096   49 2E AD 48 41 53 54 41  54 49 2E BA 48 41 53 54   I.-HASTATI.°HAST
00000112   41 54 49 2E 0D 48 41 53  54 41 54 49 2E F0 48 41   ATI. HASTATI.ðHA
00000128   53 54 41 54 49 2E AD 48  41 53 54 41 54 49 2E BA   STATI.-HASTATI.°
00000144   48 41 53 54 41 54 49 2E  0D 48 41 53 54 41 54 49   HASTATI. HASTATI
00000160   2E F0 48 41 53 54 41 54  49 2E AD 48 41 53 54 41   .ðHASTATI.-HASTA
00000176   54 49 2E BA 48 41 53 54  41 54 49 2E 0D 48 41 53   TI.°HASTATI. HAS
00000192   54 41 54 49 2E F0 48 41  53 54 41 54 49 2E AD 48   TATI.ðHASTATI.-H
00000208   41 53 54 41 54 49 2E BA  48 41 53 54 41 54 49 2E   ASTATI.°HASTATI.
00000224   0D 48 41 53 54 41 54 49  2E F0 48 41 53 54 41 54    HASTATI.ðHASTAT
00000240   49 2E AD 48 41 53 54 41  54 49 2E BA 48 41 53 54   I.-HASTATI.°HAST
00000256   41 54 49 2E 0D 48 41 53  54 41 54 49 2E F0 48 41   ATI. HASTATI.ðHA
00000272   53 54 41 54 49 2E AD 48  41 53 54 41 54 49 2E BA   STATI.-HASTATI.°
00000288   48 41 53 54 41 54 49 2E  0D 48 41 53 54 41 54 49   HASTATI. HASTATI
00000304   2E F0 48 41 53 54 41 54  49 2E AD 48 41 53 54 41   .ðHASTATI.-HASTA
00000320   54 49 2E BA 48 41 53 54  41 54 49 2E 0D 48 41 53   TI.°HASTATI. HAS
00000336   54 41 54 49 2E F0 48 41  53 54 41 54 49 2E AD 48   TATI.ðHASTATI.-H
00000352   41 53 54 41 54 49 2E BA  48 41 53 54 41 54 49 2E   ASTATI.°HASTATI.
00000368   0D 48 41 53 54 41 54 49  2E F0 48 41 53 54 41 54    HASTATI.ðHASTAT
00000384   49 2E AD 48 41 53 54 41  54 49 2E BA 48 41 53 54   I.-HASTATI.°HAST
00000400   41 54 49 2E 0D 48 41 53  54 41 54 49 2E F0 48 41   ATI. HASTATI.ðHA
00000416   53 54 41 54 49 2E AD 48  41 53 54 41 54 49 2E BA   STATI.-HASTATI.°
00000432   48 41 53 54 41 54 49 2E  0D 48 41 53 54 41 54 49   HASTATI. HASTATI
00000448   2E F0 48 41 53 54 41 54  49 2E AD 48 41 53 54 41   .ðHASTATI.-HASTA
00000464   54 49 2E BA 48 41 53 54  41 54 49 2E 0D 48 41 53   TI.°HASTATI. HAS
00000480   54 41 54 49 2E F0 48 41  53 54 41 54 49 2E AD 48   TATI.ðHASTATI.-H
00000496   41 53 54 41 54 49 2E BA  48 41 53 54 41 54 49 2E   ASTATI.°HASTATI.
```

Example of overwritten disk

The malware will create new threads for each physical drive found on the affected system. It enumerates and tries to find PhysicalDrive[0-9]. The malware makes distinctions based on what type of drive is detected, such as fixed or removable devices. As long as the drive is fixed a new thread is created.

```
Thread 1 (Func 00401aa0):
    call func_00401d55
    strcpy(drive_path, "B:\")
     ...
     if (GetDriveType(drive_path) == DRIVE_FIXED)
        CreateThread(NULL, 0, 00401B7A, 0040247C, 0, &tid)
     ...
```

Example of the wiper finds fixed drives and create new thread for each drive.

The following commands have previously been reported in the community:

“taskkill /F /IM pasvc.exe”

“taskkill /F /IM Clisvc.exe”

"shutdown -r -t 0"

Example of commands run by the malware.

The first command, “taskkill /F /IM pasvc.exe”, will try to kill a process named “pasvc.exe”. This process is associated with the AhnLab Policy Agent process.

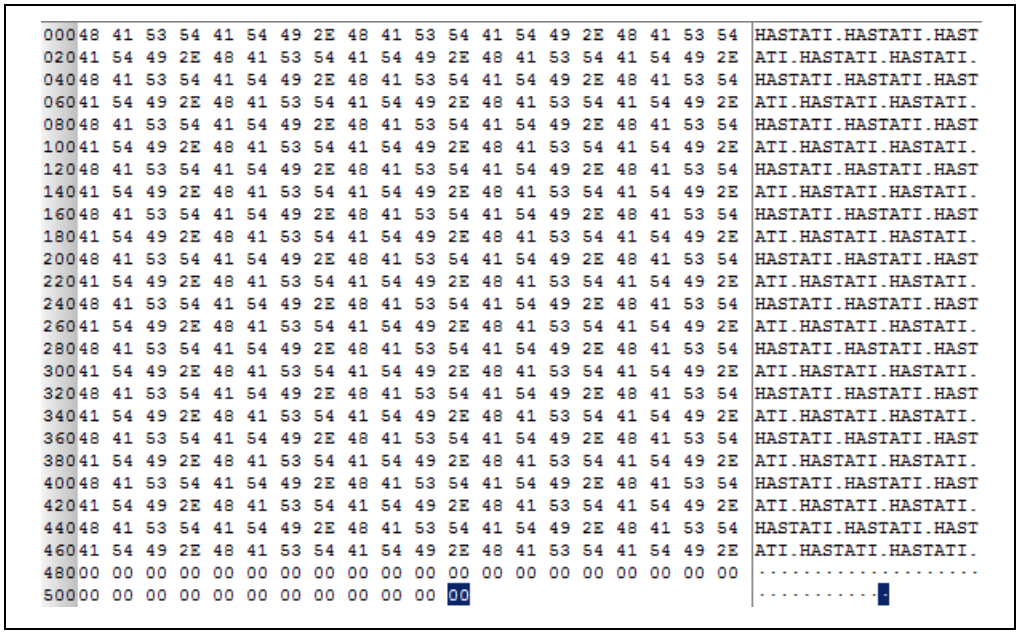
The second command, “taskkill /F /IM Clisvc.exe”, will try to kill a process named “Clisvc.exe”. This process is associated with the ViRobot ISMS security tool from HAURI Inc.
The third command, “shutdown -r -t 0”, instructs the malware to shutdown and reboot the system.

The malware shuts the system down quickly after initial execution, it was found to finish wiping in ten to fifteen minutes in our tests. Due to the speed of the wiping it was very easy to find that the malware did not actually wipe all the data on the computer. It wiped just enough to make the machine unusable after the operation was complete. This is notable and can be seen in the operation of the malware as it makes sure to overwrite the VBR first then continue overwriting the MBR and other files.

Note: *The sample Fidelis Security Systems researchers had available looked very similar to that detailed in community write-ups. However, as of the date of this post, researchers were still analyzing the available sample. Therefore, differences between the available sample and others available to the community may become apparent in the future.*

File System Recovery

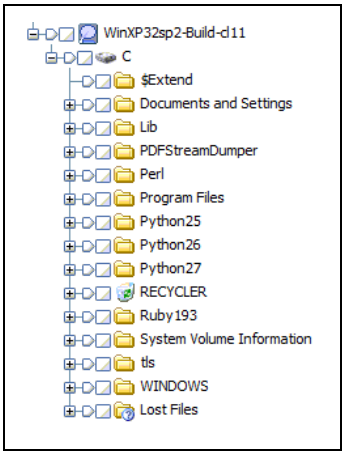
The following is the view of the wiped disk for each of the operating systems that we tested:



Example of wiped MBR by the Malware.

The malware never actually overwrote the backup VBR. It was found that the same techniques utilized to recover data from Shamoon could be applied here. The recovery methods were covered in depth in Fidelis Threat Advisory #1007 so we will not show them here. What will be shown are the results of the recovery.

When the backup VBR is found within EnCase (v6.19.6) it was possible to add a manual NTFS partition into the system to recover the file system and data within.



Example of a file system recovered

Once the logical file system is recovered relevant forensic artifacts can be located. It will be important to note that a lot of files will be recoverable and a lot of system files are left untouched. The wiper corrupts file systems very quickly, but the expense of this is leaving more files untouched and recoverable.

Note: *When multiple partitions are suspected then it will be likely the recovery will need to be done manually with a hex editor. The method for this was also covered in advisory #1007.*

Using a hex editor it is possible to repair an image with the backup VBR and build a new MBR to boot the affected computer. This comes with a warning, just being able to boot the machine and accessing the data within doesn't mean that system will operate properly. The system still has files that were corrupted by the malware, and some of those files will affect the user experience. However, in our testing we were able to rebuild the MBR and recover the VBR to boot the affected system.

Our repaired system was missing the start button and a few of the shortcuts to executables on the desktop were no longer functioning. The XP system when repaired always asked to complete a chkdisk cycle, and on the whole didn't operate normally. The Windows 7 systems that were affected by the two malware samples did not experience these issues, and appeared to operate normally. Attempts to repair the XP system with the windows recovery CD always ended in a bluescreen error before the operation finished any repairing.

The Fidelis Take

Fidelis XPS sensors detect the DarkSeoul/Jokra malware as it enters the network as "Trojan.Win32.EraseMBR.b". Fidelis XPS is capable of detecting this threat regardless of delivery method employed by the Threat Actors responsible. Fidelis XPS can detect and alert on executables such as the DarkSeoul malware multiple layers deep inside of zip files, or even XOR'ed inside of a weaponized MS Office document or Adobe PDF File. The Fidelis Threat Research and Network Forensics and Incident Response teams will continue to actively monitor the ever-evolving threat landscape for the latest threats to our customers network security.