nProtect Online Security
Setting a New Standard in Web Fraud Detection & Prevention

Malware Analysis Report

Date written: November 21, 2015

1. Overview

1.1 File information

File name	kaulj.exe
File size	96,710 bytes
Detection name	Trojan/W32.KRBanker.96710
Malicious activities	▪ Pharming attack for internet banking websites ▪ Steals a digital certificate
Features	▪ Redirect users to fake web sites after modifying hosts file to steal a digital certificate ▪ Reside in the system by automatic execution ▪ File dropper

1.2 System environments

Operating System	Windows XP SP3, 32bit
Analysis Tools	IDA, PEview, OllyDbg, ProcExp

2. Analysis Results

2.1 Paths where the file was spread

The malicious code described above has been spread out through more than 40 online shopping mall websites during October, 2015. Those websites listed below was initially redirected to www.k****.co.kr/cd1.html before downloading the malicious code except *******wire.com, and then finally it forced users to download the malicious code through the final redirection page which is 180.**.***.131/Us******sc*****x.html

www.e****.co.kr	www.h****b.co.kr
p*****.ar*****e.com	www.c***u.com
www.bo****nd****a.co.kr	www.n******en.or.kr
www.b***.co.kr	t****erc******ing.co.kr
www.s****.co.k******ain.asp	www.vi*******rl.kr
www.r****.co.kr	***.**s.or.kr
www.s****w**.biz	www.i******t.co.kr
www.t*****a**.com	www.a***d.com
www.m*******im.pe.kr	www.s****n.pe.kr
www.e***b.co.kr	www.r***a.co.kr
www.y***.com	www.a****op.co.kr
www.b*****y.com	

[Figure 1. List of websites redirected initially]

© 2015 nProtect Inc. All rights Reserved.

2.2 Sample Analysis

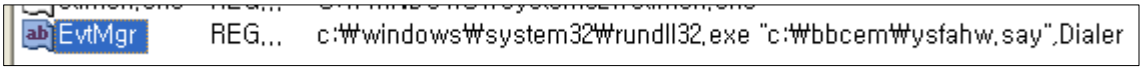
Kaulj.exe is classified with KRBanker malware, and it induces internet banking users to redirect to fake internet banking websites, called as pharming technique. In this report, the analysis was focused on the internal operation of the malicious code.

2.2.1. Deep analysis for Kaulj.exe

Malicious activities are not executed by the downloaded kaulj.exe, but executed by rundll32.exe that is dropped. At this time, the executable file(kaulj.exe) is only performed as a file dropper. Because the malicious code uses anti-debugging technique during the file dropping, the analysis and detection took a long while the longevity of malicious code was extended. As the result, the 5-digit folder name is randomly created in the D drive with a hidden attribute, and a 6-digit random dll file is dropped in the folder. If the D drive does not exist, it will be created in the C drive.

[Figure 2. A dropped file]

After executing 'rundll32.exe', it runs the Dialer which is an export function of the dll file and modifies the registry to execute this process over and over even if the system is rebooted. All of the malicious activities are designed in the Dialer function of the dropped dll file, and the executable file quits after deleting itself as soon as completing the registration for automatic execution.



[Figure 3. A registry modified for automatic execution]

2.2.2. Deep analysis for Dialer function

Dialer function checks whether wiseman.exe exists or not in the C drive, and runs if available. However, this file actually does not perform because it's neither dropped nor downloaded in terms of test environments. The wiseman.exe is a kind of infamous adware, and some KRBanker variants drop or run this file.

```
if ( j_PathFileExistsA("c:₩₩wiseman.exe") )
  j_ShellExecuteA(0, 0, "c:₩₩wiseman.exe", 0, "c:₩₩windows₩₩system32", 0);
if ( j_PathFileExistsA("c:₩₩stov.exe") )
  j_ShellExecuteA(0, 0, "c:₩₩stov.exe", 0, "c:₩₩windows₩₩system32", 0);
```

[Figure 4. Execution of wiseman.exe and stov.exe]

This malicious code also tries to connect to 174.***.65.**2 later, and writes in C:\lang.ini based on the data transmitted from this address or downloads other files. At this time, the connection to 174.***.65.**2 is not available so, we couldn't confirm the real data. The content recorded in C:\lang.ini is mostly a transfer address of

© 2015 nProtect Inc. All rights Reserved.

digital certificates. If the communication to the server is not available, it sets the transfer address with 174.***.35.**3/u.php as a default value.

A new module downloaded is saved with "5-digit random strings.mp3", and being used to create a service or process. When it is particularly used to create a service, it modifies the Dllpath value of the registry, which is \CurrentControlSet\Services\RemoteAccess\RouterManagers\IP. The normal Dllpath value is "%WIDDIR%\system32\iprtrmgr.dll". This registry specifies necessary dll for "Routing and Remote Access" service, and the normal dll exports necessary functions so that a PC works as a router. After modifying the registry, it still has a routine that creates a service with 31-digit random strings.

```
if ( strstr(&Parameter, "zip") )
  CreateThread(0, 0, (LPTHREAD_START_ROUTINE)Thread_Download_Service, &Parameter, 0, 0);
else
  Download_Process(&Parameter);
```

[Figure 5. Download and Service/Process creation]

```
wsprintfA(&v87, "%c%c%c%c%c.mp3", v82[v16], v15, v14, v13, v12);
wsprintfA(&PathName, "%s₩₩%s", &PathName, &v87);
Substitute_RRAS_dll_andRunSvc((int)&PathName, &PathName);
WriteFile_Wrap(&PathName, v2, nNumberOfBytesToWrite);
WinExec("cmd.exe /c net start RemoteACCESS", 0);
```

[Figure 6. Service creation]

```
StartupInfo.lpDesktop = "WinSta0₩₩Default";
StartupInfo.wShowWindow = 5;
j_CreateProcessA(0, &CommandLine, 0, 0, 0, 0x20u, 0, 0, &StartupInfo, &ProcessInformation);
```

[Figure 7. Process creation]

After the downloader and stealing certificates are done, it attempts to modify the hosts file. It has an interesting routine that enables to check the virtual environments. The malicious code checks the below registry, and identify whether it's virtual environments or not with the existence of VMwareHostOpen.exe.

Under HKCR\Applications\, various executable file names and its options are specified depends on each system. Therefore, if VMwareHostOpen.exe exists in this registry, we can identify whether it's virtual machine or not.

```
[HKCR₩Applications₩cmd.exe]
[HKCR₩Applications₩access.exe]
...
[HKCR₩Applications₩VMwareHostOpen.exe]
```

[Figure 8. Examples of registry]

If a virtual machine is identified, the malicious code attempts to connect to another malicious web site, which is http://b***.s***.com.**/u/5*****98**, and executes service or process after downloading a file.

© 2015 nProtect Inc. All rights Reserved.

```
LOBYTE(v8) = RegOpenKeyEx_VMwareHostOpen_exe(pHKey_Result);
if ( !v8 )                                      // VMwareHostOpen.exe
{
  Sleep(600000u);
  CreateThread(0, 0, (LPTHREAD_START_ROUTINE)CreateThread_Wrap_ConnMalServer, 0, 0, 0);
}
```

[Figure 9. Malicious activities in virtual machine]

3. Conclusion

kaulj.exe is not much different from other KRBanker malware as it also performs a pharming attack for internet banking users, however, several unique malicious routines were existed internally even though it does not work according to the deep analysis. The analysis result implies that those malicious codes are continuously updated and developed as well as adding more malicious features. Furthermore, we can see plainly that hackers are more aggressive to distribute malicious codes through the initial transfer websites. Currently, nProtect security solutions detect both the dropper kaulj.exe and the dropped dll files.

For more specific information, please contact us using the details below:

nProtect, Inc.
3003 N. First Street #301
San Jose, CA 95134
Tel: 408.477.1742
Email: support@nProtect.com
www.nProtect.com

© 2015 nProtect Inc. All rights Reserved.