blackcon / **Exploit raonk.svc (LPE)**

Last active 2 years ago

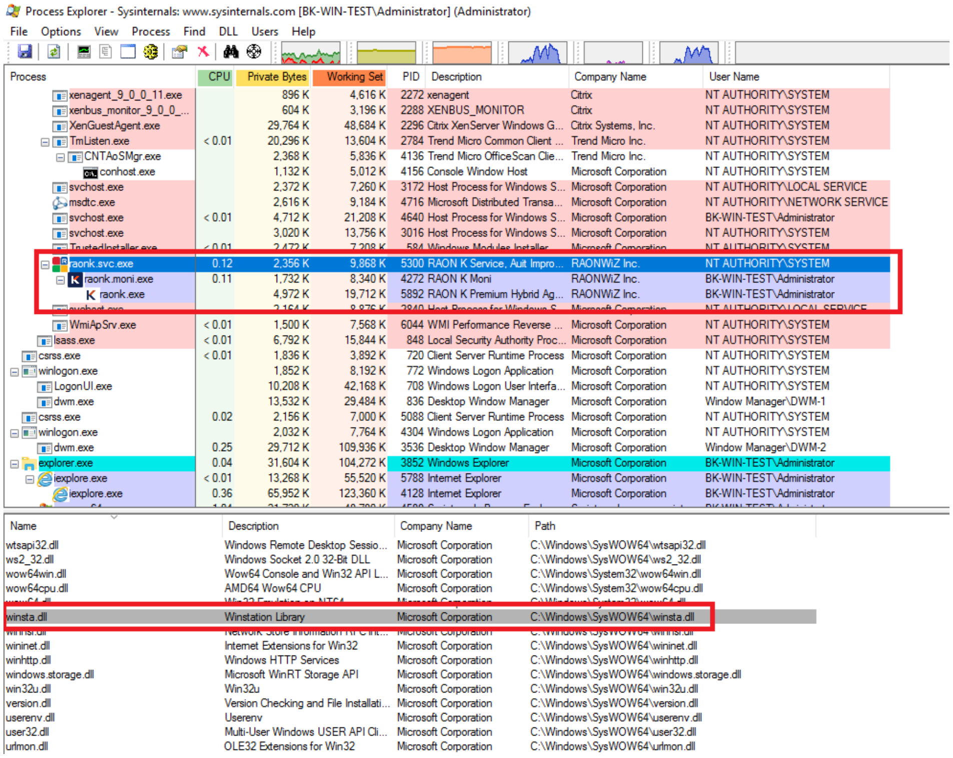
Exploit raonk.svc (LPE)

```
1. Vulnerability
   - DLL Search Order Hijacking Vulnerability (LPE)

2. Product
   - product: raonk.svc.exe (version: 2018.0.0.10)
   - company: RAONWIZ Inc

3. Vulnerebility Version
   - before 2018.0.0.10

4. Update Version
   - Not yet

5. Describe vulnerability
  - read this apply
    https://gist.github.com/blackcon/ae155656d21a2228aa25fdcb79c85159#gistcomment-3445913

6. Reference URL
   - http://www.raonk.com/page/intro/solution_intro.aspx
   - https://resources.infosecinstitute.com/dll-hijacking-attacks-revisited/#gref

7. Discoverer
  - Jihwan Yoon in NBP(NAVER BUSINESS PLATFORM)
  - Security Engineer
  - Service : https://www.ncloud.com, https://www.naver.com
```

blackcon commented on Sep 8, 2020 • edited ▾ Author

5. Proof

1) Load DLL List

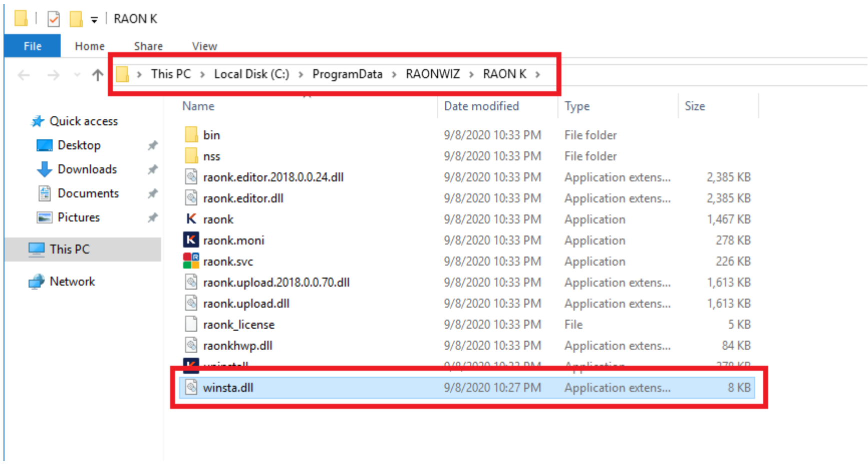


Process Explorer - Sysinternals: www.sysinternals.com [BK-WIN-TEST\Administrator] (Administrator)
File Options View Process Find DLL Users Help

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name	User Name
xenagent_9_0_0_11.exe		896 K	4,616 K	2272	xenagent	Citrix	NT AUTHORITY\SYSTEM
xenbus_monitor_9_0_0_...		604 K	3,196 K	2288	XENBUS_MONITOR	Citrix	NT AUTHORITY\SYSTEM
XenGuestAgent.exe		29,764 K	48,684 K	2296	Citrix XenServer Windows G...	Citrix Systems, Inc.	NT AUTHORITY\SYSTEM
TmListen.exe	< 0.01	20,296 K	13,604 K	2784	Trend Micro Common Client ...	Trend Micro Inc.	NT AUTHORITY\SYSTEM
CNTAoSMgr.exe		2,368 K	5,836 K	4136	Trend Micro OfficeScan Clie...	Trend Micro Inc.	NT AUTHORITY\SYSTEM
conhost.exe		1,132 K	5,012 K	4156	Console Window Host	Microsoft Corporation	NT AUTHORITY\SYSTEM
svchost.exe		2,372 K	7,260 K	3172	Host Process for Windows S...	Microsoft Corporation	NT AUTHORITY\LOCAL SERVICE
msdtc.exe		2,616 K	9,184 K	4716	Microsoft Distributed Transa...	Microsoft Corporation	NT AUTHORITY\NETWORK SERVICE
svchost.exe	< 0.01	4,712 K	21,208 K	4640	Host Process for Windows S...	Microsoft Corporation	BK-WIN-TEST\Administrator
svchost.exe		3,020 K	13,756 K	3016	Host Process for Windows S...	Microsoft Corporation	NT AUTHORITY\SYSTEM
TrustedInstaller.exe	< 0.01	2,472 K	7,208 K	584	Windows Modules Installer	Microsoft Corporation	NT AUTHORITY\SYSTEM
raonk.svc.exe	0.12	2,356 K	9,868 K	5300	RAON K Service, Auit Impro...	RAONWiZ Inc.	NT AUTHORITY\SYSTEM
raonk.moni.exe	0.11	1,732 K	8,340 K	4272	RAON K Moni	RAONWiZ Inc.	BK-WIN-TEST\Administrator
raonk.exe		4,972 K	19,712 K	5892	RAON K Premium Hybrid Ag...	RAONWiZ Inc.	BK-WIN-TEST\Administrator
svchost.exe		2,164 K	8,876 K	2840	Host Process for Windows S...	Microsoft Corporation	NT AUTHORITY\LOCAL SERVICE
WmiApSrv.exe	< 0.01	1,500 K	7,568 K	6044	WMI Performance Reverse ...	Microsoft Corporation	NT AUTHORITY\SYSTEM
lsass.exe	< 0.01	6,792 K	15,844 K	848	Local Security Authority Proc...	Microsoft Corporation	NT AUTHORITY\SYSTEM
csrss.exe	< 0.01	1,836 K	3,892 K	720	Client Server Runtime Process	Microsoft Corporation	NT AUTHORITY\SYSTEM
winlogon.exe		1,852 K	8,192 K	772	Windows Logon Application	Microsoft Corporation	NT AUTHORITY\SYSTEM
LogonUI.exe		10,208 K	42,168 K	708	Windows Logon User Interfa...	Microsoft Corporation	NT AUTHORITY\SYSTEM
dwm.exe		13,532 K	29,484 K	836	Desktop Window Manager	Microsoft Corporation	Window Manager\DWM-1
csrss.exe	0.02	2,156 K	7,000 K	5088	Client Server Runtime Process	Microsoft Corporation	NT AUTHORITY\SYSTEM
winlogon.exe		2,032 K	7,764 K	4304	Windows Logon Application	Microsoft Corporation	NT AUTHORITY\SYSTEM
dwm.exe	0.25	29,712 K	109,936 K	3536	Desktop Window Manager	Microsoft Corporation	Window Manager\DWM-2
explorer.exe	0.04	31,604 K	104,272 K	3852	Windows Explorer	Microsoft Corporation	BK-WIN-TEST\Administrator
iexplore.exe	< 0.01	13,268 K	55,520 K	5788	Internet Explorer	Microsoft Corporation	BK-WIN-TEST\Administrator
iexplore.exe	0.36	65,952 K	123,360 K	4128	Internet Explorer	Microsoft Corporation	BK-WIN-TEST\Administrator

Name	Description	Company Name	Path
wtsapi32.dll	Windows Remote Desktop Sessio...	Microsoft Corporation	C:\Windows\SysWOW64\wtsapi32.dll
ws2_32.dll	Windows Socket 2.0 32-Bit DLL	Microsoft Corporation	C:\Windows\SysWOW64\ws2_32.dll
wow64win.dll	Wow64 Console and Win32 API L...	Microsoft Corporation	C:\Windows\System32\wow64win.dll
wow64cpu.dll	AMD64 Wow64 CPU	Microsoft Corporation	C:\Windows\System32\wow64cpu.dll
wow64.dll	Win32 Emulation on NT64	Microsoft Corporation	C:\Windows\System32\wow64.dll
winsta.dll	Winstation Library	Microsoft Corporation	C:\Windows\SysWOW64\winsta.dll
winnsi.dll	Network Store Information RPC int...	Microsoft Corporation	C:\Windows\SysWOW64\winnsi.dll
wininet.dll	Internet Extensions for Win32	Microsoft Corporation	C:\Windows\SysWOW64\wininet.dll
winhttp.dll	Windows HTTP Services	Microsoft Corporation	C:\Windows\SysWOW64\winhttp.dll
windows.storage.dll	Microsoft WinRT Storage API	Microsoft Corporation	C:\Windows\SysWOW64\windows.storage.dll
win32u.dll	Win32u	Microsoft Corporation	C:\Windows\SysWOW64\win32u.dll
version.dll	Version Checking and File Installati...	Microsoft Corporation	C:\Windows\SysWOW64\version.dll
userenv.dll	Userenv	Microsoft Corporation	C:\Windows\SysWOW64\userenv.dll
user32.dll	Multi-User Windows USER API Cli...	Microsoft Corporation	C:\Windows\SysWOW64\user32.dll
urlmon.dll	OLE32 Extensions for Win32	Microsoft Corporation	C:\Windows\SysWOW64\urlmon.dll

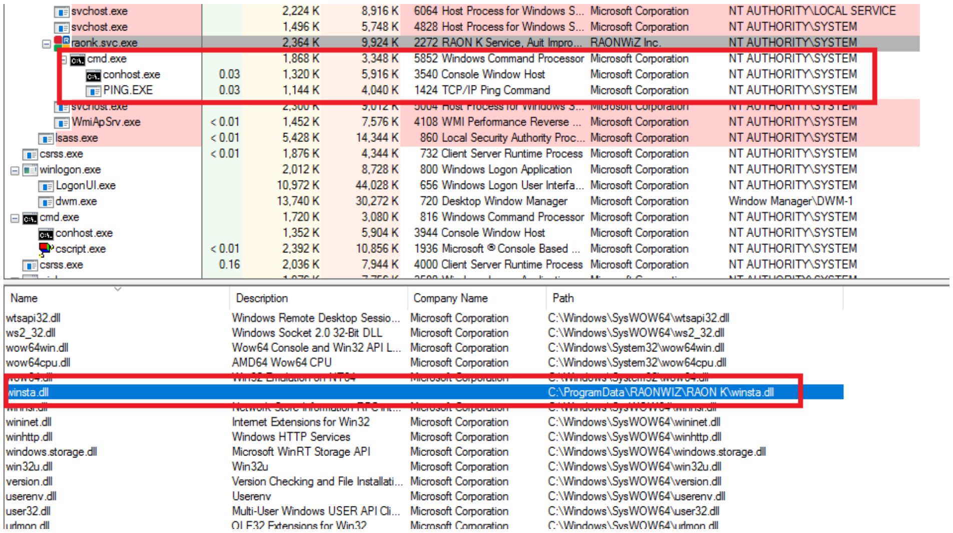
2) move the new DLL for hijacking and restart the service(raonk.svc)



This PC › Local Disk (C:) › ProgramData › RAONWIZ › RAON K ›

Name	Date modified	Type	Size
bin	9/8/2020 10:33 PM	File folder	
nss	9/8/2020 10:33 PM	File folder	
raonk.editor.2018.0.0.24.dll	9/8/2020 10:33 PM	Application extens...	2,385 KB
raonk.editor.dll	9/8/2020 10:33 PM	Application extens...	2,385 KB
raonk	9/8/2020 10:33 PM	Application	1,467 KB
raonk.moni	9/8/2020 10:33 PM	Application	278 KB
raonk.svc	9/8/2020 10:33 PM	Application	226 KB
raonk.upload.2018.0.0.70.dll	9/8/2020 10:33 PM	Application extens...	1,613 KB
raonk.upload.dll	9/8/2020 10:33 PM	Application extens...	1,613 KB
raonk_license	9/8/2020 10:33 PM	File	5 KB
raonkhwp.dll	9/8/2020 10:33 PM	Application extens...	84 KB
uninstall	9/8/2020 10:33 PM	Application	278 KB
winsta.dll	9/8/2020 10:27 PM	Application extens...	8 KB

3) Success dll hijacking and execute commnad as SYSTEM auth.



svchost.exe		2,224 K	8,916 K	6064	Host Process for Windows S...	Microsoft Corporation	NT AUTHORITY\LOCAL SERVICE
svchost.exe		1,496 K	5,748 K	4828	Host Process for Windows S...	Microsoft Corporation	NT AUTHORITY\SYSTEM
raonk.svc.exe		2,364 K	9,924 K	2272	RAON K Service, Auit Impro...	RAONWiZ Inc.	NT AUTHORITY\SYSTEM
cmd.exe		1,868 K	3,348 K	5852	Windows Command Processor	Microsoft Corporation	NT AUTHORITY\SYSTEM
conhost.exe	0.03	1,320 K	5,916 K	3540	Console Window Host	Microsoft Corporation	NT AUTHORITY\SYSTEM
PING.EXE	0.03	1,144 K	4,040 K	1424	TCP/IP Ping Command	Microsoft Corporation	NT AUTHORITY\SYSTEM
svchost.exe		2,300 K	9,012 K	5004	Host Process for Windows S...	Microsoft Corporation	NT AUTHORITY\SYSTEM
WmiApSrv.exe	< 0.01	1,452 K	7,576 K	4108	WMI Performance Reverse ...	Microsoft Corporation	NT AUTHORITY\SYSTEM
lsass.exe	< 0.01	5,428 K	14,344 K	860	Local Security Authority Proc...	Microsoft Corporation	NT AUTHORITY\SYSTEM
csrss.exe	< 0.01	1,876 K	4,344 K	732	Client Server Runtime Process	Microsoft Corporation	NT AUTHORITY\SYSTEM
winlogon.exe		2,012 K	8,728 K	800	Windows Logon Application	Microsoft Corporation	NT AUTHORITY\SYSTEM
LogonUI.exe		10,972 K	44,028 K	656	Windows Logon User Interfa...	Microsoft Corporation	NT AUTHORITY\SYSTEM
dwm.exe		13,740 K	30,272 K	720	Desktop Window Manager	Microsoft Corporation	Window Manager\DWM-1
cmd.exe		1,720 K	3,080 K	816	Windows Command Processor	Microsoft Corporation	NT AUTHORITY\SYSTEM
conhost.exe		1,352 K	5,904 K	3944	Console Window Host	Microsoft Corporation	NT AUTHORITY\SYSTEM
cscript.exe	< 0.01	2,392 K	10,856 K	1936	Microsoft ® Console Based ...	Microsoft Corporation	NT AUTHORITY\SYSTEM
csrss.exe	0.16	2,036 K	7,944 K	4000	Client Server Runtime Process	Microsoft Corporation	NT AUTHORITY\SYSTEM

Name	Description	Company Name	Path
wtsapi32.dll	Windows Remote Desktop Sessio...	Microsoft Corporation	C:\Windows\SysWOW64\wtsapi32.dll
ws2_32.dll	Windows Socket 2.0 32-Bit DLL	Microsoft Corporation	C:\Windows\SysWOW64\ws2_32.dll
wow64win.dll	Wow64 Console and Win32 API L...	Microsoft Corporation	C:\Windows\System32\wow64win.dll
wow64cpu.dll	AMD64 Wow64 CPU	Microsoft Corporation	C:\Windows\System32\wow64cpu.dll
wow64.dll	Win32 Emulation on NT64	Microsoft Corporation	C:\Windows\System32\wow64.dll
winsta.dll			C:\ProgramData\RAONWIZ\RAON K\winsta.dll
winnsi.dll	Network Store Information RPC int...	Microsoft Corporation	C:\Windows\SysWOW64\winnsi.dll
wininet.dll	Internet Extensions for Win32	Microsoft Corporation	C:\Windows\SysWOW64\wininet.dll
winhttp.dll	Windows HTTP Services	Microsoft Corporation	C:\Windows\SysWOW64\winhttp.dll
windows.storage.dll	Microsoft WinRT Storage API	Microsoft Corporation	C:\Windows\SysWOW64\windows.storage.dll
win32u.dll	Win32u	Microsoft Corporation	C:\Windows\SysWOW64\win32u.dll
version.dll	Version Checking and File Installati...	Microsoft Corporation	C:\Windows\SysWOW64\version.dll
userenv.dll	Userenv	Microsoft Corporation	C:\Windows\SysWOW64\userenv.dll
user32.dll	Multi-User Windows USER API Cli...	Microsoft Corporation	C:\Windows\SysWOW64\user32.dll
urlmon.dll	OLE32 Extensions for Win32	Microsoft Corporation	C:\Windows\SysWOW64\urlmon.dll