Shadow Force Uses DLL Hijacking, Targets South Korean Company

- Posted on:September 9, 2015 at 1:00 am
- Posted in:Malware, Targeted Attacks

- Author:
  Dove Chiu (Threat Researcher)

0

What sort of interest would a businessman have in a news agency?

That was the question that arose from our recent investigation on an attack that appears to target a media agency in South Korea. Shadow Force is a new backdoor that replaces a DLL called by a particular Windows service. Once that backdoor is open, the attacker can use one or more tools to open up further holes or cause damage. This type of backdoor attack has been previously documented by Trend Micro in a blog post in May.

Beginnings of an attack

The attack begins when the Windows OS starts the Microsoft Distributed Transaction Coordinator (MSDTC) service, which coordinates transactions that span multiple resource managers, such as databases, message queues, and file systems. When the target computer joins a domain, once the MSDTC service starts, it will search the registry.

Figure 1. MSDTC service DLL plugins

Specifically, the MTxOCI component in MSDTC service searches for three DLLs: *oci.dll*, *SQLLib80.dll*, and *xa80.dll*. *oci.dll* isn't normally found on the computer, but in this case, the hacker has created a backdoor component , renamed it to *oci.dll*, and placed it in *%SystemRoot%\system32*. Once the *oci.dll* is in place, the hacker uses a remote job command to kill the MSDTC service (*taskkill /im msdtc.exe /f*), causing MSDTC to reload itself. This time, however, it looks for and finds the *oci.dll*. Calling this DLL opens up Shadow Force.

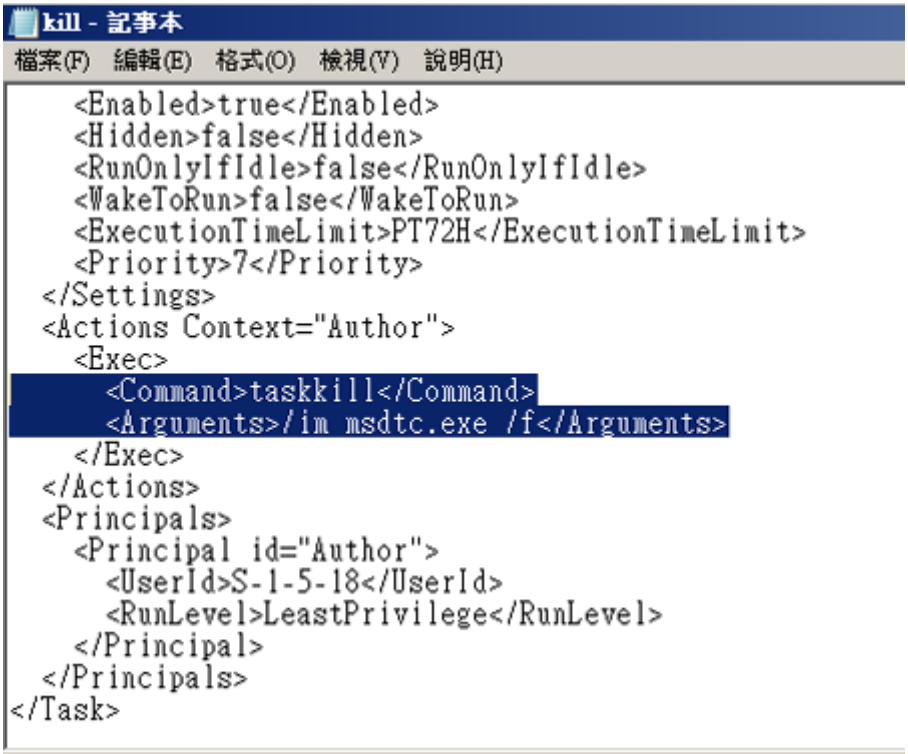

Figure 2. The kill command kills the MSDTC service, causing it to restart

This simple technique bypasses forensics tools such as *autorun.exe*, and makes live detection and remediation more difficult.

Analysis of Shadow Force

Shadow Force has several different variations, both in DLL and EXE formats and in a 32-bit or 64-bit implementations. The type of variation will rely on *installe.exe*, the file that downloads and installs Shadow Force on the computer. If *install.exe* runs in 32-bit mode, it will download *SuperBot.exe*. If it runs in 64-bit mode, it will download *SuperBotx64.exe*.

Address	Length	Type	String
.rdata:0040…	0000000D	C	KERNEL32.dll
.rdata:0040…	0000000B	C	USER32.dll
.rdata:0040…	0000000A	C	GDI32.dll
.rdata:0040…	0000000B	C	MSVCRT.dll
.data:0040…	00000021	C	AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
.data:0040…	00000025	C	http://61.137.223.48:81/SuperBot.exe
.data:0040…	00000028	C	http://61.137.223.48:81/SuperBotx64.exe
.data:0040…	00000008	C	Traffic
.data:0040…	00000014	C	InternetCloseHandle
.data:0040…	00000011	C	InternetReadFile
.data:0040…	00000012	C	InternetCrackUrlA
.data:0040…	0000000F	C	HttpQueryInfoA
.data:0040…	00000011	C	HttpSendRequestA
.data:0040…	00000011	C	InternetConnectA
.data:0040…	0000000E	C	InternetOpenA
.data:0040…	00000011	C	HttpOpenRequestA
.data:0040…	0000000C	C	WININET.DLL
.data:0040…	0000000A	C	text/html
.data:0040…	00000009	C	HTTP/1.1
.data:0040…	00000010	C	Range:bytes=%s-
.data:0040…	00000010	C	Range:bytes=%u-
.data:0040…	0000000D	C	KERNEL32.DLL
.data:0040…	00000014	C	GetNativeSystemInfo
.data:0040…	00000019	C	Mozilla/4.0 (compatible)

Figure 3. Strings in the Shadow Force install.exe downloader

Take SuperBot.exe as an example. It is a Shadow Force .exe version, and it will connect to a C&C server (*irc[.]itembuy[.]org*) like a normal IRC bot.

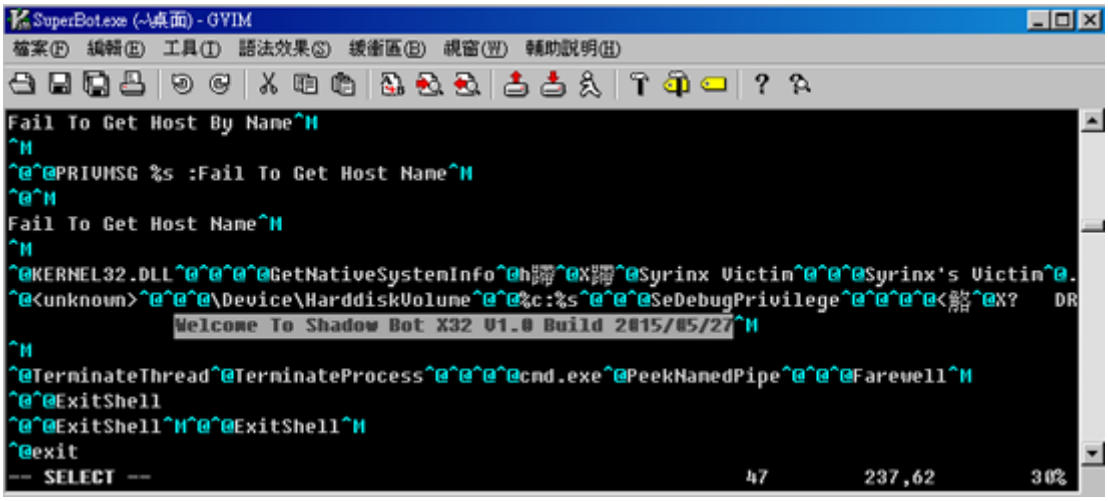

Figure 4. The version string inside the Shadow Force 32-bit EXE version

The DLL version of Shadow Force uses another type of attack. Rather than connect to a C&C server, it uses a port-reuse technique by downloading and installing the file *npf.sys*. The *npf.sys file* (downloaded by Shadow Force as a part of its function) comes from famous open source project Wireshark, a well-known network protocol analyzer. Therefore, the *npf.sys* has a valid signature and can be loaded in Windows, to be used in capturing network packets. Connecting to Shadow Force requires a specific password in the correct format.

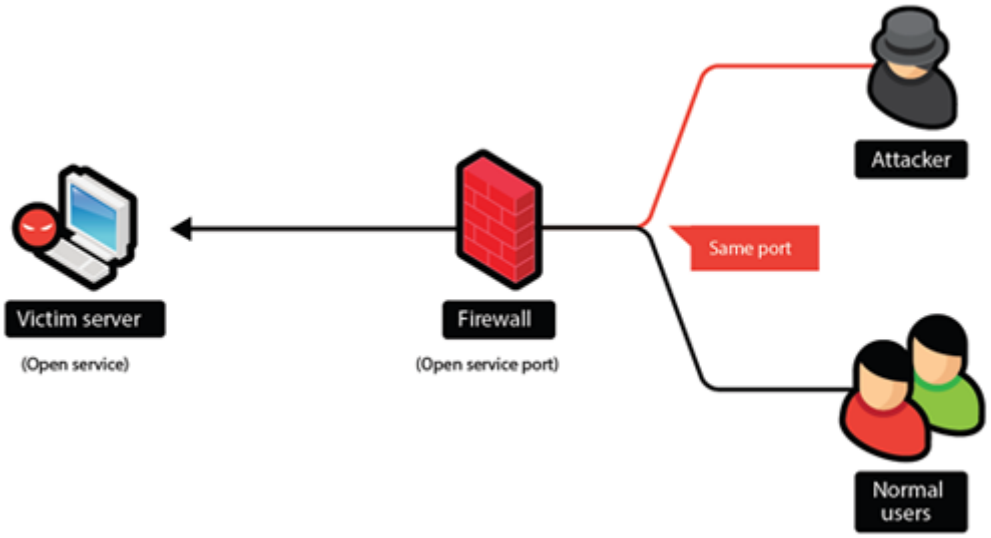

Figure 5. With port-reuse, the attacker is able to get in through an open port in the firewall and the client, just as legitimate users would

Once an attacker has gained access to a client system on an otherwise protected network, there are a number of tools that are available to exploit systems, networks, and beyond. These include *fileh.exe*, *latinfect.exe*, and *aio.exe*. More information about these tools, along with information about the presumed attacker can be found in the technical brief.

Trend Micro Custom Defense solutions can protect organizations from this type of backdoor attack. These solutions provide in-depth contextual analysis and insight that help IT administrators properly identify suspicious behavior on individual computers and on the network, such as the access to computers and servers.

Tags: APTbackdoorshadow forceSouth Korea