An analysis of Regin's Hopscotch and Legspin

With high profile threats like Regin, mistakes are incredibly rare. However, when it comes to humans writing code, some mistakes are inevitable. Among the most interesting things we observed in the Regin malware operation were the forgotten codenames for some of its modules.

These are:

- Hopscotch
- Legspin
- Willischeck
- U_STARBUCKS

We decided to analyze two of these modules in more detail - **Hopscotch** and **Legspin**.

Despite the overall sophistication (and sometimes even over-engineering) of the Regin platform, these tools are simple, straightforward and provide interactive console interfaces for Regin operators. What makes them interesting is the fact they were developed many years ago and could even have been created before the Regin platform itself.

The Hopscotch module

MD5	6c34031d7a5fc2b091b623981a8ae61c
Size	36864 bytes
Type	Win32 EXE
Compiled	2006.03.22 19:09:29 (GMT)

This module has another binary inside, stored as resource 103:

MD5	42eaf2ab25c9ead201f25ecbdc96fb60
Size	18432 bytes
Type	Win32 EXE
Compiled	2006.03.22 19:09:29 (GMT)

This executable module was designed as a standalone interactive tool for **lateral movement**. It does not contain any exploits but instead relies on previously acquired credentials to authenticate itself at the remote machine using standard APIs.

The module receives the name of the target machine and an optional remote file name from the standard input (operator). The attackers can choose from several options at the time of execution and the tool provides human-readable responses and suggestions for possible input.

Here's an example of "Hopscotch" running inside a virtual machine:

Authentication Mechanism (SU or NETUSE) [S]/N:
Continue? [n]:
A File of the same name was already present on Remote Machine - Not deleting...

The module can use two routines to authenticate itself at the target machine: either connecting to the standard share named "IPC$" (method called "NET USE") or logging on as a local user ("SU", or "switch user") who has enough rights to proceed with further actions.

It then extracts a payload executable from its resources and writes it to a location on the target machine. The default location for the payload is: ***%target%*\ADMIN$\SYSTEM32\SVCSTAT.EXE**. Once successful, it connects to the remote machine's service manager and creates a new service called "Service Control Manager" to launch the payload. The service is immediately started and then stopped and deleted after one second of execution.

The module establishes a two-way encrypted communication channel with the remote payload **SVCSTAT.EXE** using two named pipes. One pipe is used to forward input from the operator to the payload and the other writes data from the payload to the standard output. Data is encrypted using the RC4 algorithm and the initial key exchange is protected using asymmetric encryption.

\\%target%\pipe\{66fbe87a-4372-1f51-101d-1aaf0043127a}
\\%target%\pipe\{44fdg23a-1522-6f9e-d05d-1aaf0176138a}

Once completed, the tool deletes the remote file and closes the authenticated sessions, effectively removing all the traces of the operation.

The SVCSTAT.EXE payload module launches its copy in the process dllhost.exe and then prepares the corresponding named pipes on the target machine and waits for incoming data. Once the original module connects to the pipe, it sets up the encryption of the pipe communication and waits for the incoming shellcode.

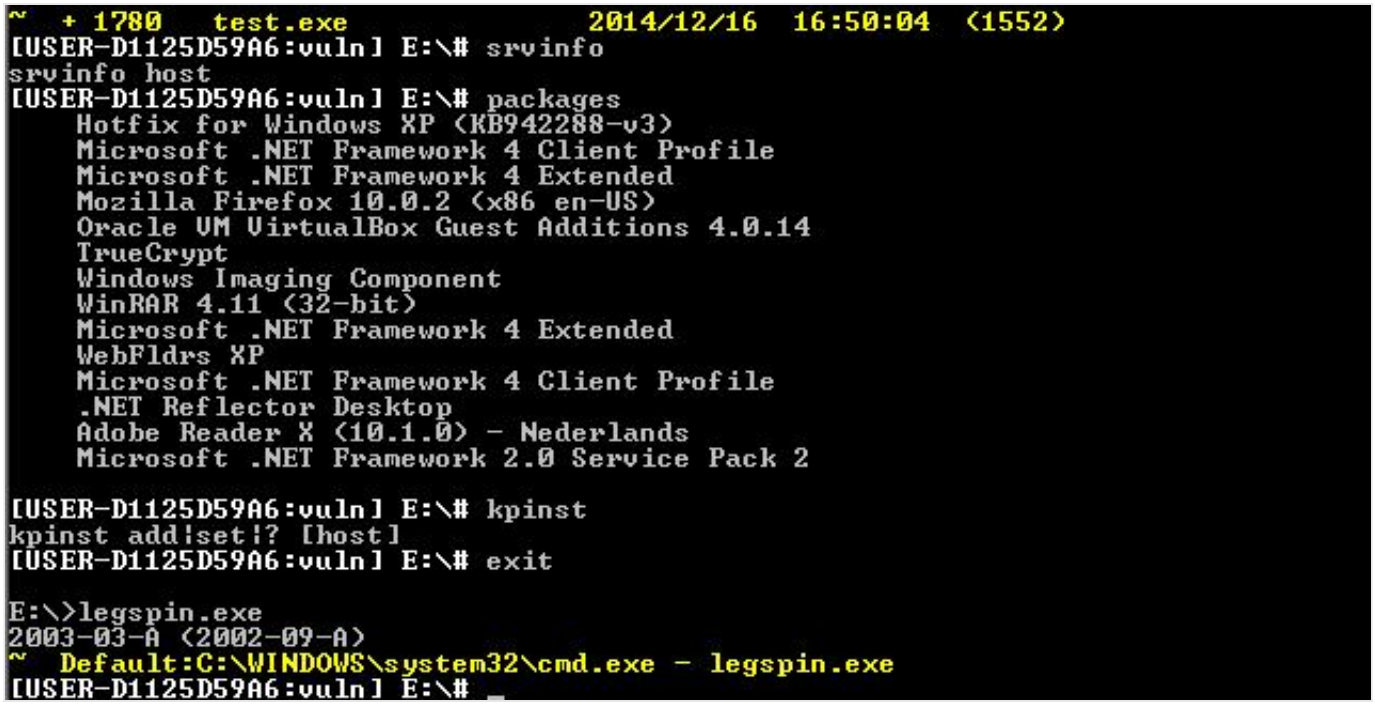
The executable is injected in a new process of dllhost.exe or svchost.exe and executed, with its input and output handles redirected to the remote plugin that initiated the attack. This allows the operator to control the injected module and interact with it.

The Legspin module

MD5	29105f46e4d33f66fee346cfd099d1cc
Size	67584 bytes
Type	Win32 EXE

Compiled	2003.03.17 08:33:50 (GMT)

This module was also developed as a standalone command line utility for computer administration. When run remotely it becomes a powerful backdoor. It is worth noting that the program has full console support and features colored output when run locally. It can even distinguish between consoles that support Windows Console API and TTY-compatible terminals that accept escape codes for coloring.



"Legspin" output in a standard console window with color highlighting

In addition to the compilation timestamp found in the PE headers, there are two references that point to 2003 as its true year of compilation. The program prints out two version labels:

- 2002-09-A, referenced as "lib version"
- 2003-03-A

In addition the program uses legacy API functions, like "NetBIOS" that was introduced in Windows 2000 and deprecated in Windows Vista.

Once started and initialized, it provides the operator with an interactive command prompt, waiting for incoming commands. The list of available commands is pretty large and allows the operators to perform many administrative actions. Some of the commands require additional information that is requested from the operator, and the commands provide a text description of the available parameters. The program is actually an administrative shell that is intended to be operated manually by the attacker/user.

Command	**Description**
cd	Change current working directory

dir ls dirl dirs	List files and directories
tar	Find files matching a given mask and time range, and write their contents to a XOR-encrypted archive
tree	Print out a directory tree using pseudographics 
trash	Read and print out the contents of the Windows "Recycle Bin" directory
get	Retrieve an arbitrary file from the target machine, LZO compressed
put	Upload an arbitrary file to the target machine, LZO compressed
del	Delete a file
ren mv copy cp	Copy or move a file to a new location
gtm	Get file creation, access, write timestamps and remember the values
stm	Set file creation, access, write timestamps to the previously retrieved values
mtm	Modify the previously retrieved file timestamps
scan strings	Find and print out all readable strings from a given file
more	Print out the contents of an arbitrary file
access	Retrieve and print out DACL entries of files or directories
audit	Retrieve and print out SACL entries of files or directories
finfo	Retrieve and print out version information from a given file
cs	Dump the first 10,000 bytes from an arbitrary file or from several system files: advapi32.dll

	kernel32.dll msvcrt.dll ntdll.dll ntoskrnl.exe win32k.sys cmd.exe ping.exe ipconfig.exe tracert.exe netstat.exe net.exe user32.dll gdi32.dll shell32.dll
lnk	Search for LNK files, parse and print their contents
info	Print out general system information: • CPU type • memory status • computer name • Windows and Internet Explorer version numbers • Windows installation path • Codepage
dl	Print information about the disks: • Type • Free/used space • List of partitions, their filesystem types
ps	List all running processes
logdump	Unfinished, only displays the parameter description
reglist	Dump registry information for a local or remote hive
windows	Enumerate all available desktops and all open windows
view	List all visible servers in a domain
domains	List the domain controllers in the network
shares	List all visible network shares
regs	Print additional system information from the registry: • IE version • Outlook Express version • Logon default user name • System installation date • BIOS date • CPU frequency • System root directory
ips	List network adapter information: • DHCP/static IP address • Default gateway's address

times	Obtain the current time from a local or remote machine
who	List the names of current users and the domains accessed by the machine
net nbtstat tracert ipconfig netstat ping	Run the corresponding system utility and print the results
tel	Connect to a given TCP port of a host, send a string provided by the operator, print out the response
dns arps	Resolve a host using DNS or ARP requests
users	List information about all user accounts
admins	List information about user accounts with administrative privileges
groups	List information about user groups
trusts	List information about interdomain trust user accounts
packages	Print the names of installed software packages
sharepw	Run a brute-force login attack trying to obtain the password of a remote share
sharelist	Connect to a remote share
srvinfo	Retrieve current configuration information for the specified server
netuse	Connect, disconnect or list network shares
netshare	Create or remove network shares on the current machine
nbstat	List NetBIOS LAN adapter information
run	Create a process and redirect its output to the operator
system	Run an arbitrary command using WinExec API
exit	Exit the program
set	Set various internal variables used in other shell commands
su	Log on as a different user
kill	Terminate a process by its PID
kpinst	Modify the registry value: [HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon] System This value should normally point to "lsass.exe".
svc drv	Create, modify or remove a system service
help ?	Print the list of supported commands

The Legspin module we recovered doesn't have a built-in C&C mechanism. Instead, it relies on the Regin platform to redirect the console input/output to/from the operators.

Conclusions

Unlike most other Regin modules, Legspin and Hopscotch appear to be stand-alone tools developed much

earlier. The Legspin backdoor in particular dates back to 2003 and perhaps even 2002. It's worth pointing that not all Regin deployments contain the Legspin module; in most cases, the attackers manage their victims through other Regin platform functions.

This means that Legspin could have been used independently from the Regin platform, as a simple backdoor together with an input/output wrapper.

Although more details about Regin are becoming available, there is still a lot that remains unknown. One thing is already clear – what we know about Regin is probably already retired information that has been replaced by new modules and techniques as time passes.