Trochilus and New MoonWind RATs Used In Attack Against Thai Organizations

researchcenter.paloaltonetworks.com/2017/03/unit42-trochilus-rat-new-moonwind-rat-used-attack-thai-utility-organizations/

Jen Miller-Osborn, Josh Grunzweig March 30, 2017

By Jen Miller-Osborn and Josh Grunzweig

March 30, 2017 at 5:00 AM

Category: Unit 42

Tags: MoonWind RAT, RAT, Thailand, Trochilus RAT, Utilites

From September 2016 through late November 2016, a threat actor group used both the Trochilus RAT and a newly idenfied RAT we've named MoonWind to target organizations in Thailand, including a utility organization. We chose the name 'MoonWind' based on debugging strings we saw within the samples, as well as the compiler used to generate the samples. The attackers compromised two legitimate Thai websites to host the malware, which is a tactic this group has used in the past. Both the Trochilus and MoonWind RATs were hosted on the same compromised sites and used to target the same organization at the same time. The attackers used different command and control servers (C2s) for each malware family, a tactic we believe was meant to thwart attempts to tie the attacks together using infrastructure alone. The compromised websites are the site for a group of information technology companies in Thailand, and all the tools were stored in the same directory.

We were also able to find a post-compromise tool along with the two RATs, which afforeded us insight into one of the tools the attackers used once they gained a foothold inside an organization. In addition to Trochilus and MoonWind we found Mimikatz, a popular credential harvesting tool.

Further research led us to additional MoonWind samples using the same C2 (dns[.] webswindows [.]com) but hosted on a different compromised but legitimate website. The attacks in that case took place in late September to early October 2016 and the attackers stored the MoonWind samples as RAR files, while in the November attacks the RATs were stored as executables. We were not able to find additional tools, but the attackers again compromised a legitimate Thai website to host their malware, in this case the student portal for a Thai University.

MoonWind Analysis

The MoonWind sample used for this analysis was compiled with a Chinese compiler known as BlackMoon, the same compiler used for the BlackMoon banking Trojan. While a number of attributes match the BlackMoon banking Trojan, the malware is not the same. Both malware families were simply compiled using the same compiler, and it was the BlackMoon artifacts that resulted in the naming of the BlackMoon banking Trojan. But because this new sample is different from the BlackMoon banking Trojan, we have named it MoonWind, by combining the BlackMoon compiler artifacts with the embedded string below:

E:\StarWind\FW__Project_RTPD-PIBICs\Table.ini

When MoonWind first runs, it will copy itself to one of the following locations with a filename of ‘svcohos.exe’:

- C:\Documents and Settings\All Users\Ufyaginptxb\
- C:\Users\All Users\
- C:\PorgramData\
- C:\Program Files\Common Files\

It then executes a new instance of itself in a new process. Also, it will remove the original file via the following command that is executed in a batch script named 'date.bat’.

```
cmd /c timeout /t 6 & del "C:\ProgramData\Ufyaginptxb\svcohost.exe" & del date.bat
```

During this routine, a randomly generated victim identifier will be created and written to a file named 'micr.ini'. This file is located in the same path as the malware. The following contents represent an example of a victim ID contained in this file:

```
[mic]
Mic=2199LLLLLL
```

During the install routine, the malware will also setup a timer that will execute a file named 'sevrsvos.exe'. This sample (815df680be80b26b5dff0bcaf73f7495b9cae5e3ad3acb7348be188af3e75201) acts as a runtime persistence mechanism. It installs itself as a service with the following properties:

Service Name: Windows Ejlptxtxbfjn Rvzd
Display Name: Windows Ejlptxtxbfjn Rvzd
Description: Windows Ejlptxtxbfjn Rvzd Hlptxbfjnr
Startup Type: Automatic

This service serves the single purpose of checking every 60 seconds if the 'svcohos.exe' process is running. If not, the service will spawn a new instance of it. In doing so, this secondary malware sample acts as both a runtime persistence mechanism, as well as a persistence mechanism across reboots.

After installation, a keylogging routine begins. The malware writes keystrokes and window information to a filename in the present working directory with the following filename:

jop[year][month][day][hour][minute][seconds].zip

Additionally, it writes a 'win.ini' file that contains this file path above.

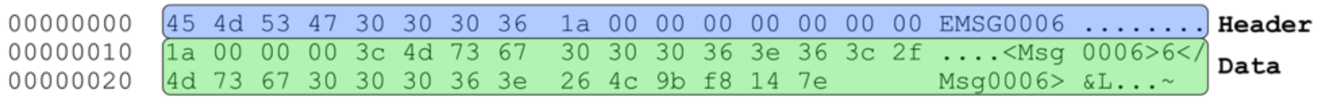
The malware proceeds to collect the following victim information:

- Hostname
- Username
- Windows version
- IP address
- Current time
- RAM amount
- Number of total drives
- Number of removable drives
- Unique victim identifier

After this information is aggregated, MoonWind enters its command and control loop, and begins reaching out to the servers and ports specified in its configuration embedded in the svcohos.exe file. The following remote hosts were specified in this particular sample:

dns.webswindows[.]com|80
dns.webswindows[.]com|443
dns.webswindows[.]com|53
dns.webswindows[.]com|8080

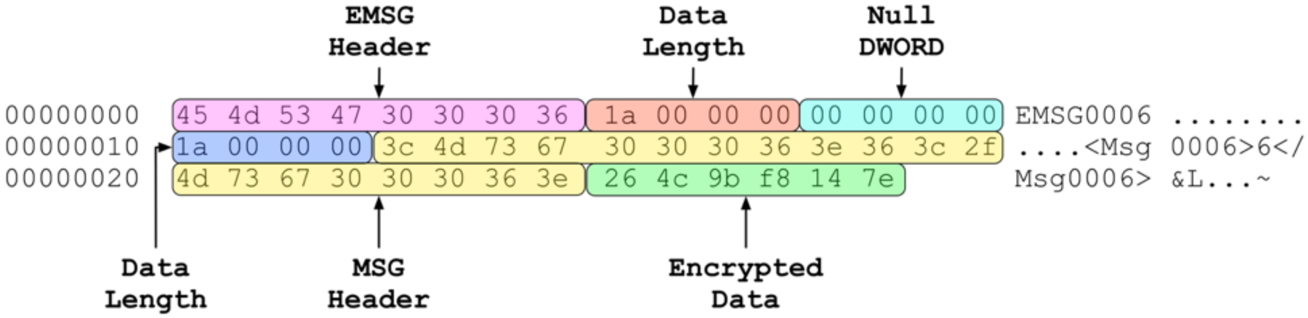
While the ports associated with this sample's configuration pertain normally to HTTP, HTTPS, or DNS, network communication takes place via raw sockets. The malware first receives data, which has the following format as shown in Figure 1:



```
00000000  45 4d 53 47 30 30 30 36  1a 00 00 00 00 00 00 00 EMSG0006 ........
00000010  1a 00 00 00 3c 4d 73 67  30 30 30 36 3e 36 3c 2f ....<Msg 0006>6</
00000020  4d 73 67 30 30 30 36 3e  26 4c 9b f8 14 7e       Msg0006> &L...~
```

Figure 1 C2 to MoonWind communication

Digging into the packet further, we can break out individual pieces, as seen in Figure 2:



```
00000000  45 4d 53 47 30 30 30 36  1a 00 00 00 00 00 00 00  EMSG0006 ........
00000010  1a 00 00 00 3c 4d 73 67  30 30 30 36 3e 36 3c 2f  ....<Msg 0006>6</
00000020  4d 73 67 30 30 30 36 3e  26 4c 9b f8 14 7e        Msg0006> &L...~
```

Figure 2 MoonWind network communication packet format

The encrypted data portion is encrypted via RC4 with the following static key:

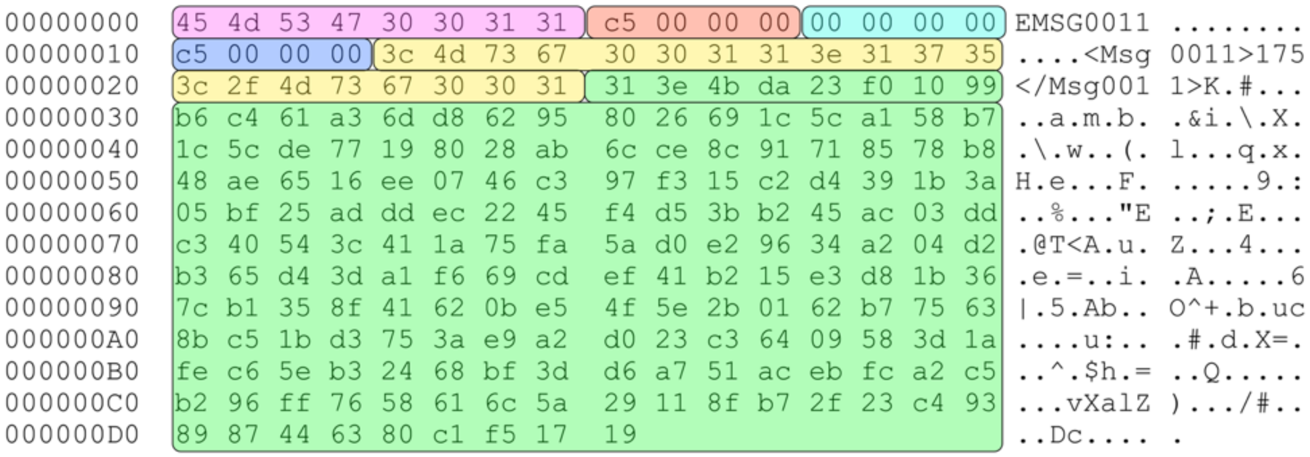
HHSADh!@#$YUAGEWYGhjfsjd5465fsaQWAFGDA/jfdafdjhhasgfh==

In the above example, the encrypted data decrypts to '\x20\x20\x20\x20\x20\x20', or six spaces. This particular command requests that the malware send the previously collected victim information.

The data returned by MoonWind has the same format, however, uses the following static key for encryption instead:

SSHqWSSAFdhjklfahj!@##4*&&!!HQ12785452!@!!$$$32#@$$11!!

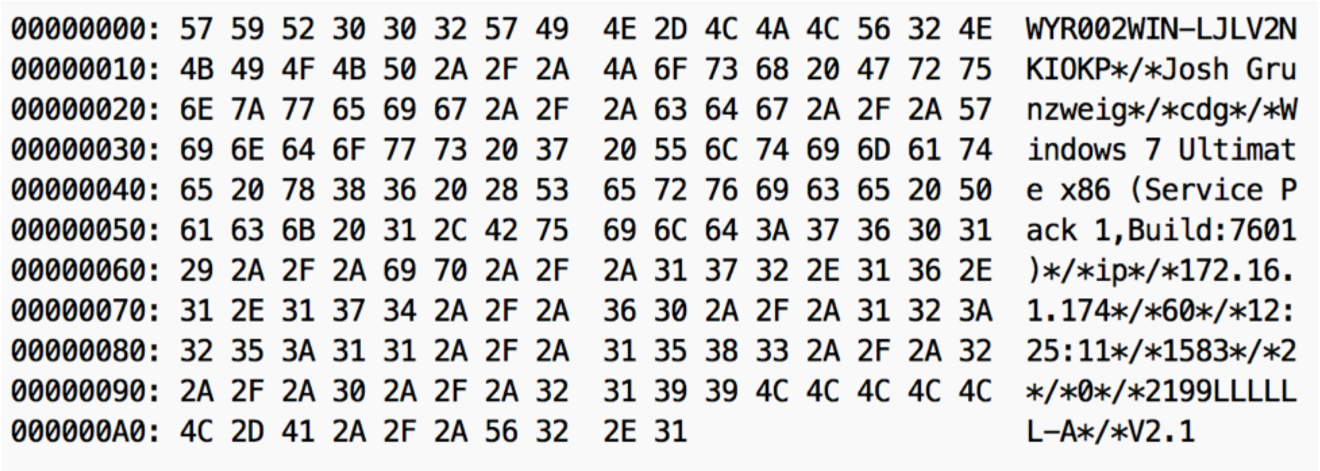
An example of such data returned by the malware can be seen below in figure 3.



```
00000000  45 4d 53 47 30 30 31 31  c5 00 00 00 00 00 00 00  EMSG0011 ........
00000010  c5 00 00 00 3c 4d 73 67  30 30 31 31 3e 31 37 35  ....<Msg 0011>175
00000020  3c 2f 4d 73 67 30 30 31  31 3e 4b da 23 f0 10 99  </Msg001 1>K.#...
00000030  b6 c4 61 a3 6d d8 62 95  80 26 69 1c 5c a1 58 b7  ..a.m.b. .&i.\.X.
00000040  1c 5c de 77 19 80 28 ab  6c ce 8c 91 71 85 78 b8  .\.w..(. l...q.x.
00000050  48 ae 65 16 ee 07 46 c3  97 f3 15 c2 d4 39 1b 3a  H.e...F. .....9.:
00000060  05 bf 25 ad dd ec 22 45  f4 d5 3b b2 45 ac 03 dd  ..%..."E ..;.E...
00000070  c3 40 54 3c 41 1a 75 fa  5a d0 e2 96 34 a2 04 d2  .@T<A.u. Z...4...
00000080  b3 65 d4 3d a1 f6 69 cd  ef 41 b2 15 e3 d8 1b 36  .e.=..i. .A.....6
00000090  7c b1 35 8f 41 62 0b e5  4f 5e 2b 01 62 b7 75 63  |.5.Ab.. O^+.b.uc
000000A0  8b c5 1b d3 75 3a e9 a2  d0 23 c3 64 09 58 3d 1a  ....u:.. .#.d.X=.
000000B0  fe c6 5e b3 24 68 bf 3d  d6 a7 51 ac eb fc a2 c5  ..^.$h.= ..Q.....
000000C0  b2 96 ff 76 58 61 6c 5a  29 11 8f b7 2f 23 c4 93  ...vXalZ )..../#..
000000D0  89 87 44 63 80 c1 f5 17  19                       ..Dc.... .
```

Figure 3 MoonWind to C2 communication

When decrypted, we see the data shown in Figure 4. Note that the first six bytes contains the return command ('WYR002'), followed by the payload. The payload contains information previously discussed, delimited by '*/*'. Certain variables, such as 'cdg' and 'ip' are hardcoded. We also see what is most likely a malware versioning string at the end (V2.1). This string is also hardcoded to the sample.



```
00000000: 57 59 52 30 30 32 57 49  4E 2D 4C 4A 4C 56 32 4E  WYR002WIN-LJLV2N
00000010: 4B 49 4F 4B 50 2A 2F 2A  4A 6F 73 68 20 47 72 75  KIOKP*/*Josh Gru
00000020: 6E 7A 77 65 69 67 2A 2F  2A 63 64 67 2A 2F 2A 57  nzweig*/*cdg*/*W
00000030: 69 6E 64 6F 77 73 20 37  20 55 6C 74 69 6D 61 74  indows 7 Ultimat
00000040: 65 20 78 38 36 20 28 53  65 72 76 69 63 65 20 50  e x86 (Service P
00000050: 61 63 6B 20 31 2C 42 75  69 6C 64 3A 37 36 30 31  ack 1,Build:7601
00000060: 29 2A 2F 2A 69 70 2A 2F  2A 31 37 32 2E 31 36 2E  )*/*ip*/*172.16.
00000070: 31 2E 31 37 34 2A 2F 2A  36 30 2A 2F 2A 31 32 3A  1.174*/*60*/*12:
00000080: 32 35 3A 31 31 2A 2F 2A  31 35 38 33 2A 2F 2A 32  25:11*/*1583*/*2
00000090: 2A 2F 2A 30 2A 2F 2A 32  31 39 39 4C 4C 4C 4C 4C  */*0*/*2199LLLLL
000000A0: 4C 2D 41 2A 2F 2A 56 32  2E 31                    L-A*/*V2.1
```

Figure 4 Decrypted data sent by MoonWind

In total, MoonWind has 73 possibly commands that it can accept. We have not yet fully researched all of the commands, but the majority of them have been identified, as we can see in the Appendix.

Conclusion

Trochilus was first reported by Arbor Networks in their Seven Pointed Dagger report tying its use to other targeted Southeast Asia activity. The activity dates to at least 2013 and has ties to multiple reports by other researchers. It is highly likely MoonWind is yet another new tool being used by the group or groups responsible for that activity, indicating they are not only still active but continuing to evolve their playbook.

Palo Alto Networks customers are protected from this threat in the following ways:

- The malware discussed in this report is blocked by WildFire and Traps
- The domain names included in this report are blocked by Threat Prevention

AutoFocus subscribers can investigate the activities further with the following tags:

- Trochilus
- MoonWind

Appendix

MoonWind Commands

Command	Description	Response Command	Notes
\x20\x20\x20\x20\x20\x20	Returns collected victim information.	WYR002	
WYR002	Null command.	None	
WYR003	Spawns message box that allows victim to send a message.	WYR003	
WYR005	Modifies services.	WYR005	Subcommands of either 'fuwu' (create service), 'exit' (stop service), 'stop' (pause service), 'reun' (continue service), or 'yrun' (start service)
WYR006	Returns a list of running processes.	WYR006	
WYR007	Kills specified process.	None	
qdcmdl	Spawns an interactive shell.	cmdok1	

WYR009	Send command to interactive shell and receive results.	WYRCCC	
WYR010	Terminates interactive shell.	None	
WYR011	Get size of disks.	WYR011	
WYR012	Returns space of given directory.	WYR012	
WYR013	Return a directory listing of specified directory (C:\ default).	WYR013	
WYR014	Execute specified command.	None	
WYR015	Open specified command with ShellExecuteA.	None	
WYR016	Open specified command with ShellExecuteA (Hidden).	None	
WYR018	Perform directory listing with file attributes.	WYR018	
xiazai	Read contents of file specified.	wrdown	
cxqdcx	Restart MoonWind.	None	Uses %TEMP%/restart.bat to perform restart.
pingmu	Return screen resolution.	pmgksj	
qdkzpm	Unknown.		

jixujj	Unknown.		
sbkzxx	Performs various mouse actions.	None	Subcommands of either 'sj' (double left-click), 'yk' (move to position and right-up), 'zk' (move to position and right-down), 'zx' (move to position and left-up), or 'yd' (move to position and left-down)
xhpmkz	Unknown.		
axjpsj	Submits keyboard inputs.	None	
ksjljp	Starts keylogging functionality.	None	
tzjljp	Stops keylogging functionality.	None	
hqjljp	Return keylogging data.	jpjlhq	
scjpjl	Deletes the keylogging file.	None	
xzcxzs	Uninstalls malware.	None	Uses ‘x.bat’ to accomplish uninstall. Written to present working directory (PWD) of malware.
httpxx	Unknown.		
zaicif	Unknown.		
xiaokl	Unknown.		
juxuxi	Null command.	None	
shangc	Unknown.		
ecscwj	Unknown.		
scwjwb	Unknown.		

<table>
<tr><td></td><td></td><td></td><td></td></tr>
<tr><td>scmlcj</td><td>Creates specified directory.</td><td>mlwzcj</td><td></td></tr>
<tr><td>ycxiaz</td><td>Unknown.</td><td></td><td></td></tr>
<tr><td>zcycxz</td><td>Unknown.</td><td></td><td></td></tr>
<tr><td>ycxjml</td><td>Creates specified directory.</td><td>None</td><td></td></tr>
<tr><td>xjwjcj</td><td>Writes specified file with provided contents.</td><td>None</td><td>Command format is ‘[filename]|[data]’.</td></tr>
<tr><td>shanwj</td><td>Deletes specified file.</td><td>None</td><td></td></tr>
<tr><td>shanml</td><td>Removes specified directory.</td><td>None</td><td></td></tr>
<tr><td>gengmj</td><td>Moves specified file.</td><td>None</td><td>Command format is ‘[src]|^|[dst]’.</td></tr>
<tr><td>ycgwjj</td><td>Sets hidden attribute on specified file.</td><td>None</td><td></td></tr>
<tr><td>copywj</td><td>Copies specified file.</td><td>copyok</td><td>Command format is ‘[src]^|^[dst]’.</td></tr>
<tr><td>fzmlwj</td><td>Copies specified directory.</td><td>copyok</td><td>Command format is ‘[src]^|^[dst]’.</td></tr>
<tr><td>sdxtcs</td><td>Unknown.</td><td></td><td></td></tr>
<tr><td>qypxxl</td><td>Get disk space of specified drive.</td><td>qdypxx</td><td></td></tr>
<tr><td>scdqwj</td><td>Unknown.</td><td></td><td></td></tr>
<tr><td>wyycwj</td><td>Unknown.</td><td></td><td></td></tr>
<tr><td>xzwcsc</td><td>Unknown.</td><td></td><td></td></tr>
</table>

xzwcyx	Executes specified command within batch script.	None	Uses ‘boot.bat’ to accomplish uninstall. Written to PWD of malware.
dwjjxc	Unknown.		
dwjcwj	Unknown.		
dqscds	Returns filesize of specified file.	qcwjcd	
sjkqzd	Unknown.		
sswjsj	Finds specified file and returns results including attributes.	wjsswb	
dwjsjx	Unknown.		
xzbwza	Unknown.		
hqurl1	Returns C2 configuration of MoonWind.	qcsxdz	
ghsxip	Writes data to win.dll and loads it.	sdczip	
khljcg	Unknown.		
dqyxml	Unknown.		
gxycwj	Unknown.		
gxwjbc	Unknown.		
gxwjok	Unknown.		
fxgxcs	Unknown.		
gxwjsy	Open specified command with ShellExecuteA.	None	
gxyxcx	Unknown.		

bddkzf	Unknown.
scwjdx	Unknown.
xzwjdx	

Indicators of Compromise

MoonWind

fd4856f2ec676f273ff71e1b0a1729cf6251c82780fc9e7d628deca690b02928
ce3da112e68e00621920911b1f9c72d7175894901173e703a44ac3700e4d427c
e31679b82be58ace96b1d9fdfc2b62b6e91d371ed93957e0764cd7c464b04b9d
f2589745671949422b19beec0856ca8b9608c02d5df4402f92c0dcc9d403010b

MoonWind Persistence Mechanism

815df680be80b26b5dff0bcaf73f7495b9cae5e3ad3acb7348be188af3e75201

Trochilus

59f8a31d66f053f1efcc8d7c7ebb209a8c12233423cc2dc3673373dde9b3a149

webswindows[.]com
192.225.226[.]195

ignite 17
Security Conference
JUNE 12-15, 2017 | VANCOUVER, CANADA
Join 4000+ security professionals
Register now >
paloalto NETWORKS

security industry. Visit the Ignite website for more information on tracks, workshops and marquee sessions.