blog.sonicwall.com /en-us/2024/01/blackwood-apt-group-has-a-new-dll-loader/

Blackwood APT Group Has a New DLL Loader

Security News ⋮⋮ 1/29/2024

Overview

This week, the SonicWall Capture Labs threat research team analyzed a sample tied to the Blackwood APT group. This is a DLL that, when loaded onto a victim's computer, will escalate privileges and attempt to install a backdoor for communications monitoring and diversion. It has evasive capabilities and, as of this writing, is targeting companies and individuals in Japan and China.

Technical Overview

The sample is detected as a 32-bit DLL (Figure 1) with no packer or protector. It has minimal strings and no obvious obfuscation or encryption.

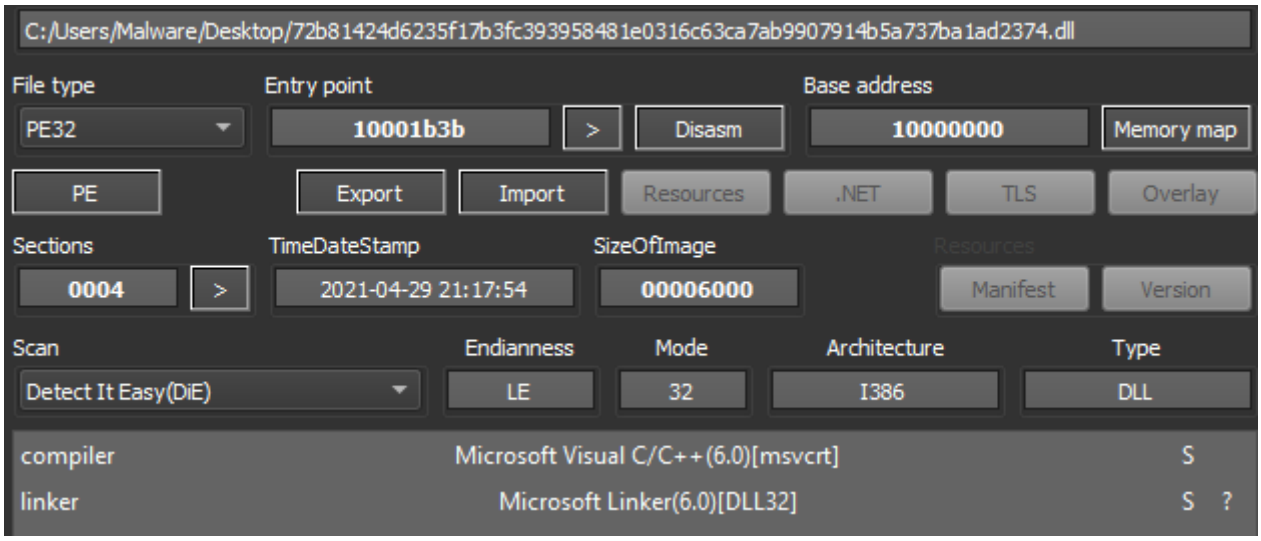


Figure 1: Sample detection

Strings show several API calls of concern, including GetCurrentProcessID, OpenProcess and VirtualAlloc – all of which are used to load malicious DLLs into memory. There are also two files listed: '333333333333333.txt' and 'Update.ini', as shown in Figure 2.

blacklist (3)	hint (20)	value (164)
-	utility	SET
-	utility	Update
-	function	VirtualAllocEx
x	function	OpenProcess
x	function	GetCurrentProcessId
-	function	CoUninitialize
-	function	CoGetObject
-	function	CoInitialize
-	function	IIDFromString
-	function	_initterm
-	function	_adjust_fdiv
-	function	_stricmp
-	format-string	D$%s
-	file	KERNEL32.dll
-	file	ole32.dll
-	file	MSVCRT.dll
-	file	agent.dll
-	file	333333333333333.txt
-	file	Update.ini

Figure 2: Static string detection

The name of the file is shown as 'agent.dll' (Figure 3) and there is one anonymous export that is only shown as an ordinal value when looking at the file with multiple tools.

indicator (31)	detail
strings > blacklist	count: 3
functions > blacklist	count: 3
checksum > invalid	expected: 0x0000D5B5
file > name > original	name: agent.dll
file > signature	name: Microsoft Visual C++ 6.0 DLL (Debug)
exports > functions	type: anonymous, count: 1

Figure 3: Original name and anonymous export

When dynamically analyzing the sample, it has multiple anti-analysis capabilities that prevent most of its function from being observed. It will look for debuggers, processor features and security settings in the registry (Figure 3). There are also locale checks that, when failed, will kill the process.

2:00:0...	DLLLoader32_...	6740	RegQueryValue	HKLM\System\CurrentControlSet\Control\WMI\Security\1aff6089-e863-4d36-bdfd-3581f07440be
2:00:0...	DLLLoader32_...	6740	RegQueryValue	HKLM\System\CurrentControlSet\Control\WMI\Security\f0558438-f56a-5987-47da-040ca75aef05
2:00:0...	DLLLoader32_...	6740	RegQueryValue	HKLM\System\CurrentControlSet\Control\WMI\Security\c7e09e2a-c663-5399-af79-2fccd321d19a
2:00:0...	DLLLoader32_...	6740	RegQueryValue	HKLM\System\CurrentControlSet\Control\WMI\Security\703fcc13-b66f-5868-ddd9-e2db7f381ffb
2:00:0...	DLLLoader32_...	6740	RegQueryKey	HKLM
2:00:0...	DLLLoader32_...	6740	RegQueryKey	HKLM
2:00:0...	DLLLoader32_...	6740	RegOpenKey	HKLM\Software\WOW6432Node\Microsoft\OLE\Tracing
2:00:0...	DLLLoader32_...	6740	RegOpenKey	HKLM\SOFTWARE\Microsoft\Ole\Tracing
2:00:0...	DLLLoader32_...	6740	RegQueryValue	HKLM\System\CurrentControlSet\Control\WMI\Security\1aff6089-e863-4d36-bdfd-3581f07440be
2:00:0...	DLLLoader32_...	6740	RegQueryValue	HKLM\System\CurrentControlSet\Control\WMI\Security\f0558438-f56a-5987-47da-040ca75aef05

Figure 4: WMI registry keys being queried for security checks

The anonymous export at address 0x10001A70 is the file calling ‘Rundll32.exe’ for process injection, as shown in Figure 5.

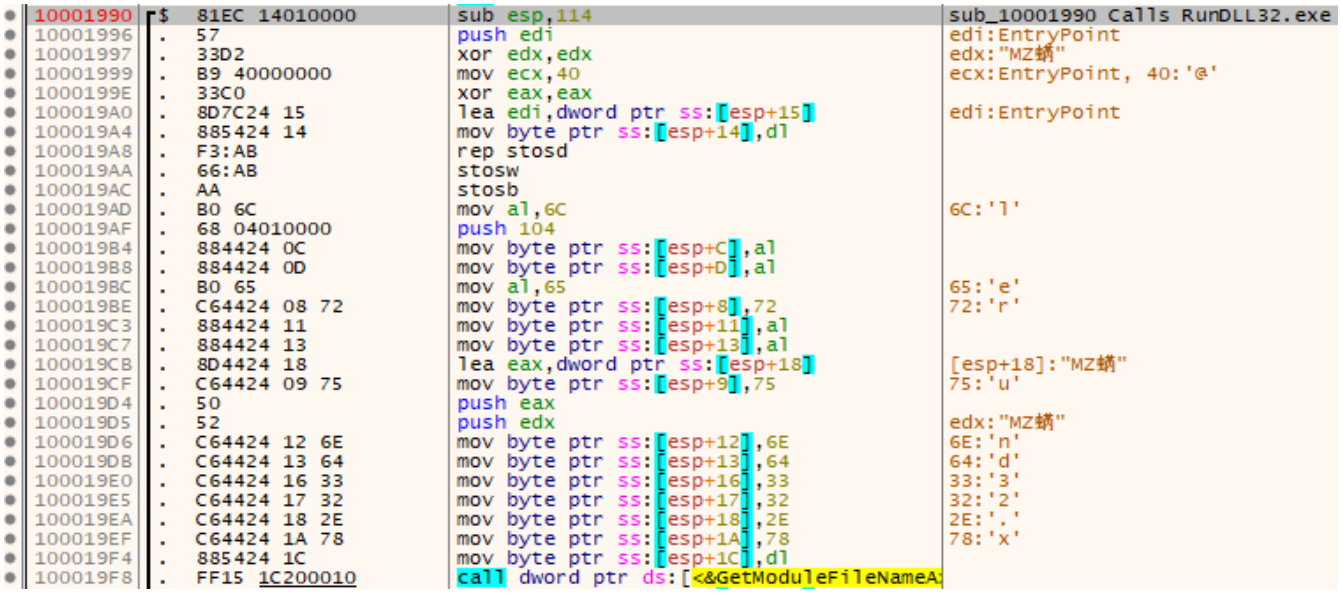
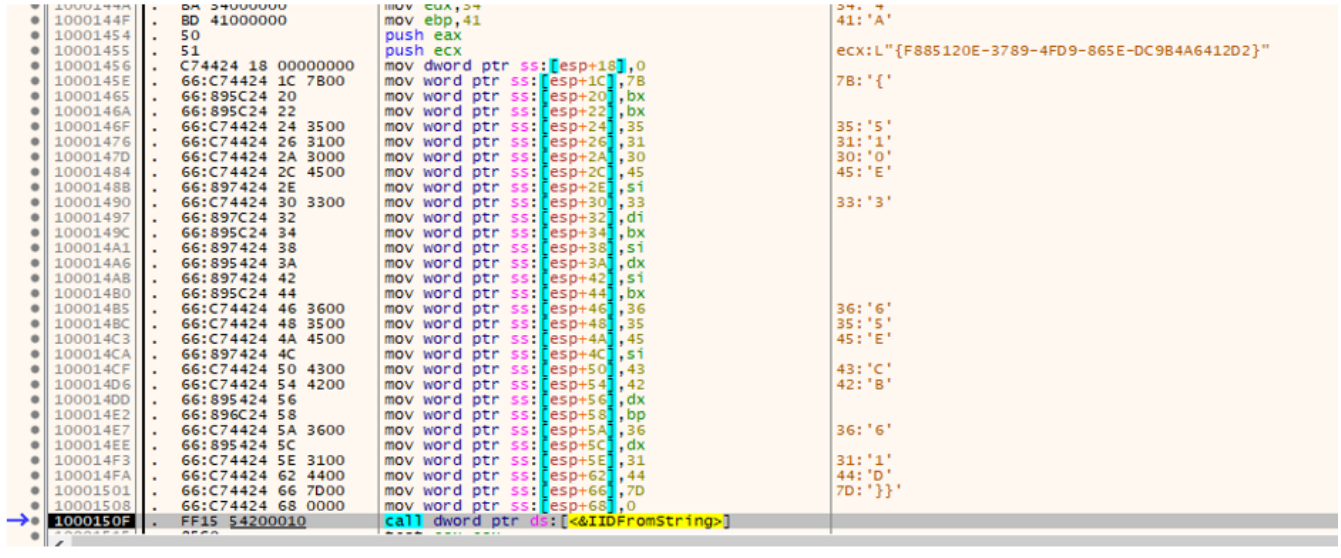


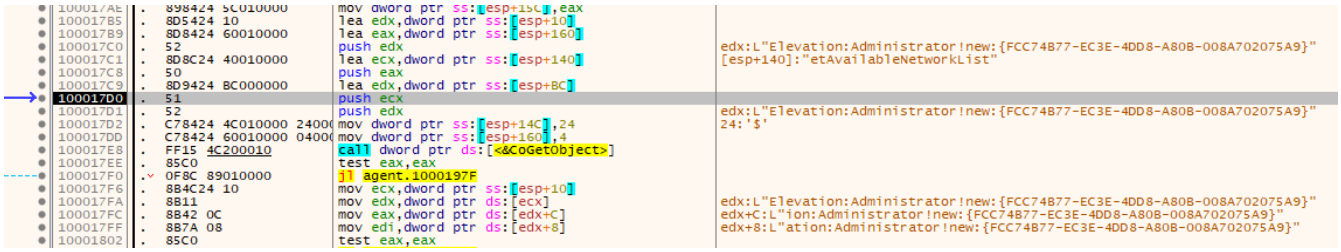
Figure 5: Export address calls sub_10001990, which creates ‘rundll32.exe’

Controlling the program’s execution allows the check for a UAC bypass to be generated. The DLL will attempt to escalate privileges via CMSTPLUA interface[1]. The following strings are created, as shown in Figures 5 and 6:

- Elevation:Administrator!new:{FCC74B77-EC3E-4DD8-A80B-008A702075A9}
- Elevation:Administrator!new:{F885120E-3789-4FD9-865E-DC9B4A6412D2}



[1] https://gist.github.com/hfiref0x/196af729106b780db1c73428b5a5d68d



Figures 6 (top) and 7 (bottom): A function creates GUIDs for privilege escalation

The two files that are listed within the strings are also referenced during runtime (Figure 7), but despite multiple attempts at controlling execution, the files were not observed on test systems.

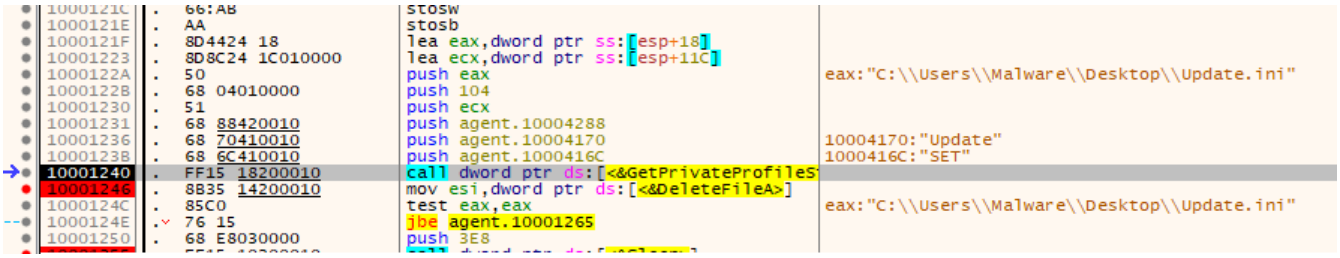


Figure 8: Update.ini is referenced but never created

Protection

To ensure SonicWall customers are prepared for any exposure that may occur due to this malware, the following signatures have been released:

- MalAgent.Blackwood

IOCs

- 72B81424D6235F17B3FC393958481E0316C63CA7AB9907914B5A737BA1AD2374