VALKYRIE

CLEAN
Valkyrie Final Verdict

File Name: find.exe
File Type: PE32 executable (console) Intel 80386, for MS Windows
SHA1: 58b1a3c1637c89374706c4aee0b6532681d4c242
MD5: fcd02331fcf70114accd5bfebe7e4155
First Seen Date: 2019-03-24 09:40:11 UTC
Number of Clients Seen: 247
Last Analysis Date: 2019-03-24 15:01:52 UTC
Human Expert Analysis Date: 2019-03-24 14:28:05 UTC
Human Expert Analysis Result: Clean
Verdict Source: Valkyrie Human Expert Analysis Overall Verdict

Analysis Summary

ANALYSIS TYPE	DATE	VERDICT
Signature Based Detection	2019-03-24 15:01:52 UTC	Clean
Static Analysis Overall Verdict	2019-03-24 15:01:52 UTC	No Threat Found
Precise Detectors Overall Verdict	2019-03-24 15:01:52 UTC	No Match
Human Expert Analysis Overall Verdict	2019-03-24 14:28:05 UTC	Clean
File Certificate Validation		Not Applicable

Static Analysis

STATIC ANALYSIS OVERALL VERDICT	RESULT
No Threat Found	

DETECTOR	RESULT
Optional Header LoaderFlags field is valued illegal	Clean
Non-ascii or empty section names detected	Clean
Illegal size of optional Header	Clean
Packer detection on signature database	Unknown
Based on the sections entropy check! file is possibly packed	Clean
Timestamp value suspicious	Suspicious
Header Checksum is zero!	Clean
Enrty point is outside the 1st(.code) section! Binary is possibly packed	Clean
Optional Header NumberOfRvaAndSizes field is valued illegal	Clean
Anti-vm present	Clean
The Size Of Raw data is valued illegal! Binary might crash your disassembler/debugger	Clean
TLS callback functions array detected	Clean

Dynamic Analysis

No Dynamic Analysis Result Received

Behavioral Information is not Available

Precise Detectors Analysis Results

DETECTOR NAME	DATE	VERDICT		REASON
Static Precise PUA Detector 1	2019-03-24 09:40:08 UTC	No Match	?	NotDetected
Static Precise Trojan Detector 5	2019-03-24 09:40:08 UTC	No Match	?	NotDetected
Static Precise Trojan Detector 7	2019-03-24 09:40:08 UTC	No Match	?	NotDetected
Static Precise PUA Detector 4	2019-03-24 09:40:08 UTC	No Match	?	NotDetected
Static Precise PUA Detector 5	2019-03-24 09:40:08 UTC	No Match	?	NotDetected
Static Precise Trojan Detector 1	2019-03-24 09:40:08 UTC	No Match	?	NotDetected
Static Precise Trojan Detector 2	2019-03-24 09:40:08 UTC	No Match	?	NotDetected
Static Precise Trojan Detector 3	2019-03-24 09:40:08 UTC	No Match	?	NotDetected
Static Precise Trojan Detector 12	2019-03-24 09:40:08 UTC	No Match	?	NotDetected
Static Precise Trojan Detector 10	2019-03-24 09:40:08 UTC	No Match	?	NotDetected
Static Precise Virus Detector 1	2019-03-24 09:40:08 UTC	No Match	?	NotDetected
Static Precise Virus Detector 2	2019-03-24 09:40:08 UTC	No Match	?	NotDetected

Advance Heuristics

No Advanced Heuristic Analysis Result Received

Human Expert Analysis Results

Analysis Start Date: 2019-03-24 11:15:15 UTC
Analysis End Date: 2019-03-24 14:28:05 UTC
File Upload Date: 2019-03-24 08:37:13 UTC
Human Expert Analyst Feedback: None
Verdict: Clean

Additional File Information

Vendor Validation - Vendor Validation is not Applicable ?

Certificate Validation - Certificate Validation is not Applicable ?

PE Headers

PROPERTY	VALUE
Compilation Time Stamp	0xD1A96334 [Thu Jun 19 06:12:04 2081 UTC] [SUSPICIOUS]
Debug Artifacts	[object Object]
Entry Point	0x402380 (.text)
Exifinfo	[object Object]
File Size	14848
File Type Enum	6
Imphash	f1ccecb8e289c2632dee607cd74a0cca
Machine Type	Intel 386 or later - 32Bit
Magic Literal Enum	1
Legal Copyright	\xa9 Microsoft Corporation. All rights reserved.
Internal Name	find
File Version	10.0.18362.1 (WinBuild.160101.0800)
Company Name	Microsoft Corporation
Product Name	Microsoft\xae Windows\xae Operating System
Product Version	10.0.18362.1
File Description	Find String (grep) Utility
Original Filename	FIND.EXE
Translation	0x0409 0x04b0
Mime Type	application/x-dosexec
Number Of Sections	5
Sha256	68ebdc30bcab4a4773100267db191454dee42773d203c3516a56f4b61d96e9bd
Ssdeep	384:6+OKTP6CRc8BRUHPDQ2m9MeIcgn6LQ00DWDIWxR:VOKj6CRc8BRUbLm9MeIcXLf0cL
Trid	64.6,Win64 Executable (generic),15.4,Win32 Dynamic Link Library (generic),10.5,Win32 Executable (generic),4.6,Generic Win/DOS Executable,4.6,DOS Executable Generic

File Paths

FILE PATH ON CLIENT	SEEN COUNT
C:\WINDOWS\SoftwareDistribution\Download\d927e2b34e6d23fbadaa49863eaaabc3\amd64_Microsoft-Windows-Client-Features-WOW64-Package~~amd64~~10.0.18362.1\wow64_microsoft-windows-m..ommandlineutilities_31bf3856ad364e35_10.0.18362.1_none_59cf07f518edc556\find.exe	80
C:\WINDOWS\SoftwareDistribution\Download\069299d7fc57c6bc3d3a71597079f528\amd64_Microsoft-Windows-Client-Features-WOW64-Package~~amd64~~10.0.18362.1\wow64_microsoft-windows-m..ommandlineutilities_31bf3856ad364e35_10.0.18362.1_none_59cf07f518edc556\find.exe	80
C:\Windows\SoftwareDistribution\Download\6dccfa5f2b6b3fcf1488f468120421a7\amd64_Microsoft-Windows-Client-Features-WOW64-Package~~amd64~~10.0.18362.1\wow64_microsoft-windows-m..ommandlineutilities_31bf3856ad364e35_10.0.18362.1_none_59cf07f518edc556\find.exe	80
C:\Windows\SoftwareDistribution\Download\12f74a66c7db08b7fadcc848508ec734\amd64_Microsoft-Windows-Client-Features-WOW64-Package~~amd64~~10.0.18362.1\wow64_microsoft-windows-m..ommandlineutilities_31bf3856ad364e35_10.0.18362.1_none_59cf07f518edc556\find.exe	80
D:\Outlook Backup\Anurag-laptop\191127-0953\C\Windows\WinSxS\wow64_microsoft-windows-m..ommandlineutilities_31bf3856ad364e35_10.0.18362.1_none_59cf07f518edc556\find.exe	80
C:\Windows\SoftwareDistribution\Download\6bc1b596af179e5b7ebcef1a64e8e4d7\amd64_Microsoft-Windows-Client-Features-WOW64-Package~~amd64~~10.0.18362.1\wow64_microsoft-windows-m..ommandlineutilities_31bf3856ad364e35_10.0.18362.1_none_59cf07f518edc556\find.exe	80
E:\Windows\WinSxS\wow64_microsoft-windows-m..ommandlineutilities_31bf3856ad364e35_10.0.18362.1_none_59cf07f518edc556\find.exe	80
C:\Windows\SoftwareDistribution\Download\36712f75e16e7c07b27be109f55b50d3\x86_Microsoft-Windows-Client-Features-Package~~x86~~10.0.18362.1\x86_microsoft-windows-m..ommandlineutilities_31bf3856ad364e35_10.0.18362.1_none_f35bc21f2c2f9225\find.exe	80
C:\Windows\Syswow64\find.exe	80
C:\Windows\SoftwareDistribution\Download\c598f05c17f6f8ae8481e549b748c1e8\amd64_Microsoft-Windows-Client-Features-WOW64-Package~~amd64~~10.0.18362.1\wow64_microsoft-windows-	80

FILE PATH ON CLIENT	SEEN COUNT
m..ommandlineutilities_31bf3856ad364e35_10.0.18362.1_none_59cf07f518edc556\find.exe	80
C:\Windows\15060\Download\98d94a3f68353dc47fbe50bbf63f378b\x86_Microsoft-Windows-Client-Features-Package~~x86~~10.0.18362.1\x86_microsoft-windows-m..ommandlineutilities_31bf3856ad364e35_10.0.18362.1_none_f35bc21f2c2f9225\find.exe	
C:\Windows\SoftwareDistribution\Download\0048a33a3d14e4ace5cc61cd15b92b75\amd64_Microsoft-Windows-Client-Features-WOW64-Package~~amd64~~10.0.18362.1\wow64_microsoft-windows-m..ommandlineutilities_31bf3856ad364e35_10.0.18362.1_none_59cf07f518edc556\find.exe	80
C:\Windows\SoftwareDistribution\Download\88842eeefa0649d9128cf563b74a16ab\amd64_Microsoft-Windows-Client-Features-WOW64-Package~~amd64~~10.0.18362.1\wow64_microsoft-windows-m..ommandlineutilities_31bf3856ad364e35_10.0.18362.1_none_59cf07f518edc556\find.exe	80
C:\WINDOWS\Syswow64\find.exe	80
F:\Windows\WinSxS\wow64_microsoft-windows-m..ommandlineutilities_31bf3856ad364e35_10.0.18362.1_none_59cf07f518edc556\find.exe	80
C:\Windows\SoftwareDistribution\Download\61953c8d6002f25ea642328c2e3c68fe\x86_Microsoft-Windows-Client-Features-Package~~x86~~10.0.18362.1\x86_microsoft-windows-m..ommandlineutilities_31bf3856ad364e35_10.0.18362.1_none_f35bc21f2c2f9225\find.exe	80
C:\Windows\SoftwareDistribution\Download\191a51b0e62f456d6ffdc606d0a91795\amd64_Microsoft-Windows-Client-Features-WOW64-Package~~amd64~~10.0.18362.1\wow64_microsoft-windows-m..ommandlineutilities_31bf3856ad364e35_10.0.18362.1_none_59cf07f518edc556\find.exe	80
C:\Windows\SoftwareDistribution\Download\560ea0c6d0e62d56096dd444db6c56be\amd64_Microsoft-Windows-Client-Features-WOW64-Package~~amd64~~10.0.18362.1\wow64_microsoft-windows-m..ommandlineutilities_31bf3856ad364e35_10.0.18362.1_none_59cf07f518edc556\find.exe	80
D:\Windows\SysWOW64\find.exe	80
C:\Windows\SoftwareDistribution\Download\5f2e5dbeb88ba33ccbe17fd997c0c82d\amd64_Microsoft-Windows-Client-Features-WOW64-Package~~amd64~~10.0.18362.1\wow64_microsoft-windows-m..ommandlineutilities_31bf3856ad364e35_10.0.18362.1_none_59cf07f518edc556\find.exe	80
C:\$WINDOWS.~BT\NewOS\Windows\WinSxS\wow64_microsoft-windows-m..ommandlineutilities_31bf3856ad364e35_10.0.18362.1_none_59cf07f518edc556\find.exe	80
D:\Outlook Backup\Anurag-laptop\200304-1448\C\Windows\SysWOW64\find.exe	80
C:\WINDOWS\SoftwareDistribution\Download\7ef4b4d561ab3b9ca4a8c14cd55d1367\amd64_Microsoft-Windows-Client-Features-WOW64-Package~~amd64~~10.0.18362.1\wow64_microsoft-windows-m..ommandlineutilities_31bf3856ad364e35_10.0.18362.1_none_59cf07f518edc556\find.exe	80
H:\found.000\dir0000.chk\SysWOW64\find.exe	80
C:\Windows\SoftwareDistribution\Download\39c262fb09b1cd2815e775a73d1ba991\x86_Microsoft-Windows-Client-Features-Package~~x86~~10.0.18362.1\x86_microsoft-windows-m..ommandlineutilities_31bf3856ad364e35_10.0.18362.1_none_f35bc21f2c2f9225\find.exe	80
C:\WINDOWS\SoftwareDistribution\Download\8f01dee45798261d6d33db90a3da815c\amd64_Microsoft-Windows-Client-Features-WOW64-Package~~amd64~~10.0.18362.1\wow64_microsoft-windows-m..ommandlineutilities_31bf3856ad364e35_10.0.18362.1_none_59cf07f518edc556\find.exe	80
E:\$WINDOWS.~BT\NewOS\Windows\SysWOW64\find.exe	80
G:\found.000\dir0000.chk\SysWOW64\find.exe	80
E:\Windows\SysWOW64\find.exe	80
C:\Windows\SoftwareDistribution\Download\2b9c48c3beadba0b56efa3009204ac3b\amd64_Microsoft-Windows-Client-Features-WOW64-Package~~amd64~~10.0.18362.1\wow64_microsoft-windows-m..ommandlineutilities_31bf3856ad364e35_10.0.18362.1_none_59cf07f518edc556\find.exe	80
E:\Windows.old\WINDOWS\WinSxS\wow64_microsoft-windows-m..ommandlineutilities_31bf3856ad364e35_10.0.18362.1_none_59cf07f518edc556\find.exe	80
C:\Windows\SoftwareDistribution\Download\cf3078108719eacb588665ee796a0ac2\amd64_Microsoft-Windows-Client-Features-WOW64-Package~~amd64~~10.0.18362.1\wow64_microsoft-windows-m..ommandlineutilities_31bf3856ad364e35_10.0.18362.1_none_59cf07f518edc556\find.exe	80
C:\\Windows\SysWOW64\find.exe	80
C:\Windows\SoftwareDistribution\Download\5c4111ccd51bf1e7ad0437abae668689\amd64_Microsoft-Windows-Client-Features-WOW64-Package~~amd64~~10.0.18362.1\wow64_microsoft-windows-m..ommandlineutilities_31bf3856ad364e35_10.0.18362.1_none_59cf07f518edc556\find.exe	80
G:\Windows\SysWOW64\find.exe	80
J:\Windows\SysWOW64\find.exe	80
/System/Volumes/Data/Volumes/BOOTCAMP/Windows/SysWOW64/find.exe	80
C:\Windows\SoftwareDistribution\Download\8527c98e5dc6a451b25429615b5ef868\amd64_Microsoft-Windows-Client-Features-WOW64-Package~~amd64~~10.0.18362.1\wow64_microsoft-windows-m..ommandlineutilities_31bf3856ad364e35_10.0.18362.1_none_59cf07f518edc556\find.exe	80
D:\Outlook Backup\Anurag-laptop\201106-1214\C\Windows\SysWOW64\find.exe	80
C:\Windows\SoftwareDistribution\Download\d927e2b34e6d23fbadaa49863eaaabc3\amd64_Microsoft-Windows-Client-Features-WOW64-Package~~amd64~~10.0.18362.1\wow64_microsoft-windows-m..ommandlineutilities_31bf3856ad364e35_10.0.18362.1_none_59cf07f518edc556\find.exe	80

FILE PATH ON CLIENT	SEEN COUNT
C:\Windows\SoftwareDistribution\Download\069299d7fc57c6bc3d3a71597079f528\amd64_Microsoft-Windows-Client-Features-WOW64-Package~~amd64~~10.0.18362.1\wow64_microsoft-windows-m..ommandlineutilities_31bf3856ad364e35_10.0.18362.1_none_59cf07f518edc556\find.exe	80
C:\Windows\SoftwareDistribution\Download\14bedb279a21ede251d44f486e7c5a22\amd64_Microsoft-Windows-Client-Features-WOW64-Package~~amd64~~10.0.18362.1\wow64_microsoft-windows-m..ommandlineutilities_31bf3856ad364e35_10.0.18362.1_none_59cf07f518edc556\find.exe	80
C:\WINDOWS\SoftwareDistribution\Download\0bf71525fbe13b2c2688dbb6b7e6e18e\x86_Microsoft-Windows-Client-Features-Package~~x86~~10.0.18362.1\x86_microsoft-windows-m..ommandlineutilities_31bf3856ad364e35_10.0.18362.1_none_f35bc21f2c2f9225\find.exe	80
C:\Windows\SoftwareDistribution\Download\144e49a30267cd2d4f5eaf86258f6a6e\amd64_Microsoft-Windows-Client-Features-WOW64-Package~~amd64~~10.0.18362.1\wow64_microsoft-windows-m..ommandlineutilities_31bf3856ad364e35_10.0.18362.1_none_59cf07f518edc556\find.exe	80
C:\Windows\SoftwareDistribution\Download\5c43a650bfbb86bf765cb7ee806c3474\amd64_Microsoft-Windows-Client-Features-WOW64-Package~~amd64~~10.0.18362.1\wow64_microsoft-windows-m..ommandlineutilities_31bf3856ad364e35_10.0.18362.1_none_59cf07f518edc556\find.exe	80
C:\Windows.old\WINDOWS\SysWOW64\find.exe	80
C:\Windows\SysWOW64\find.exe	80
F:\Windows\SysWOW64\find.exe	80
C:\Windows.old\Windows\SysWOW64\find.exe	80
C:\Windows\SoftwareDistribution\Download\6dd98858494166e8abc9dea0950ee6ab\x86_Microsoft-Windows-Client-Features-Package~~x86~~10.0.18362.1\x86_microsoft-windows-m..ommandlineutilities_31bf3856ad364e35_10.0.18362.1_none_f35bc21f2c2f9225\find.exe	80
C:\OldSYS\Windows\SysWOW64\find.exe	80
D:\Outlook Backup\Anurag-laptop\201106-1214\C\Windows\WinSxS\wow64_microsoft-windows-m..ommandlineutilities_31bf3856ad364e35_10.0.18362.1_none_59cf07f518edc556\find.exe	80
C:\$WINDOWS.~BT\NewOS\Windows\SysWOW64\find.exe	80
C:\Windows.old\windows\SysWOW64\find.exe	80
c:\\Windows.old\WINDOWS\SysWOW64\find.exe	80
C:\Windows\System32\find.exe	80
C:\Windows.old\windows\WinSxS\wow64_microsoft-windows-m..ommandlineutilities_31bf3856ad364e35_10.0.18362.1_none_59cf07f518edc556\find.exe	80
C:\Windows\SoftwareDistribution\Download\5e395d9a036affb784df4e570ab387c0\amd64_Microsoft-Windows-Client-Features-WOW64-Package~~amd64~~10.0.18362.1\wow64_microsoft-windows-m..ommandlineutilities_31bf3856ad364e35_10.0.18362.1_none_59cf07f518edc556\find.exe	80
C:\$WINDOWS.~BT\NewOS\Windows\System32\find.exe	80
C:\Windows\SoftwareDistribution\Download\8a838d8bc7e8e79b32656f62384585e3\amd64_Microsoft-Windows-Client-Features-WOW64-Package~~amd64~~10.0.18362.1\wow64_microsoft-windows-m..ommandlineutilities_31bf3856ad364e35_10.0.18362.1_none_59cf07f518edc556\find.exe	80
D:\C-Drive\Windows\WinSxS\wow64_microsoft-windows-m..ommandlineutilities_31bf3856ad364e35_10.0.18362.1_none_59cf07f518edc556\find.exe	80
D:\Outlook Backup\Anurag-laptop\200130-1711\C\Windows\SysWOW64\find.exe	80
C:\Windows\SoftwareDistribution\Download\59fa0a63d2a81818593b7af827ec0a69\amd64_Microsoft-Windows-Client-Features-WOW64-Package~~amd64~~10.0.18362.1\wow64_microsoft-windows-m..ommandlineutilities_31bf3856ad364e35_10.0.18362.1_none_59cf07f518edc556\find.exe	80
C:\Windows\SoftwareDistribution\Download\7b5698dcd4df803ca9a6079bb2f19b98\amd64_Microsoft-Windows-Client-Features-WOW64-Package~~amd64~~10.0.18362.1\wow64_microsoft-windows-m..ommandlineutilities_31bf3856ad364e35_10.0.18362.1_none_59cf07f518edc556\find.exe	80
C:\Windows\SoftwareDistribution\Download\7ef4b4d561ab3b9ca4a8c14cd55d1367\amd64_Microsoft-Windows-Client-Features-WOW64-Package~~amd64~~10.0.18362.1\wow64_microsoft-windows-m..ommandlineutilities_31bf3856ad364e35_10.0.18362.1_none_59cf07f518edc556\find.exe	80
c:\$WINDOWS.~BT\NewOS\Windows\SysWOW64\find.exe	80
C:\Windows\WinSxS\wow64_microsoft-windows-m..ommandlineutilities_31bf3856ad364e35_10.0.18362.1_none_59cf07f518edc556\find.exe	80
C:\Windows\SoftwareDistribution\Download\f4bed0705d0f5a2a0b0be800e23fad3f\amd64_Microsoft-Windows-Client-Features-WOW64-Package~~amd64~~10.0.18362.1\wow64_microsoft-windows-m..ommandlineutilities_31bf3856ad364e35_10.0.18362.1_none_59cf07f518edc556\find.exe	80
c:\Windows\SysWOW64\find.exe	80
D:\Windows.old\WINDOWS\SysWOW64\find.exe	80
C:\Windows.old\Windows\WinSxS\wow64_microsoft-windows-m..ommandlineutilities_31bf3856ad364e35_10.0.18362.1_none_59cf07f518edc556\find.exe	80
D:\C-Drive\Windows\SysWOW64\find.exe	80

FILE PATH ON CLIENT	SEEN COUNT
C:\Windows\SoftwareDistribution\Download\8f01dee45798261d6d33db90a3da815c\amd64_Microsoft-Windows-Client-Features-WOW64-Package~~amd64~~10.0.18362.1\wow64_microsoft-windows-m..ommandlineutilities_31bf3856ad364e35_10.0.18362.1_none_59cf07f518edc556\find.exe	80
E:\Windows.old\WINDOWS\SysWOW64\find.exe	80
C:\Windows\SoftwareDistribution\Download\d31cf38f633ff5218018d81b8d54a591\amd64_Microsoft-Windows-Client-Features-WOW64-Package~~amd64~~10.0.18362.1\wow64_microsoft-windows-m..ommandlineutilities_31bf3856ad364e35_10.0.18362.1_none_59cf07f518edc556\find.exe	80
C:\Windows\SoftwareDistribution\Download\e5ee8087f8752925c676b1d4b3aac1c8\amd64_Microsoft-Windows-Client-Features-WOW64-Package~~amd64~~10.0.18362.1\wow64_microsoft-windows-m..ommandlineutilities_31bf3856ad364e35_10.0.18362.1_none_59cf07f518edc556\find.exe	80
C:\Windows\SoftwareDistribution\Download\e31335173c3ebdda4a770d01aefe6f5d\amd64_Microsoft-Windows-Client-Features-WOW64-Package~~amd64~~10.0.18362.1\wow64_microsoft-windows-m..ommandlineutilities_31bf3856ad364e35_10.0.18362.1_none_59cf07f518edc556\find.exe	80
C:\Windows\SoftwareDistribution\Download\5a0d764ececef0c950f0fa8b4c0fc5d2\amd64_Microsoft-Windows-Client-Features-WOW64-Package~~amd64~~10.0.18362.1\wow64_microsoft-windows-m..ommandlineutilities_31bf3856ad364e35_10.0.18362.1_none_59cf07f518edc556\find.exe	80
C:\Windows.old\WINDOWS\WinSxS\wow64_microsoft-windows-m..ommandlineutilities_31bf3856ad364e35_10.0.18362.1_none_59cf07f518edc556\find.exe	80
D:\\Windows\SysWOW64\find.exe	80

PE Sections

NAME	VIRTUAL ADDRESS	VIRTUAL SIZE	RAW SIZE	ENTROPY	MD5
.text	0x1000	0x19b4	0x1a00	5.76485738262	04f95784bd02f7f9df75370f6fe4d6b8
.data	0x3000	0x374	0x200	0.183338791656	bcb053506e7c83e9b9455a0b5f85fd94
.idata	0x4000	0xd08	0xe00	5.19047738931	704d9d9d52c57b3826a8d825108394a7
.rsrc	0x5000	0x7f8	0x800	4.3381832069	8c58292c53952a08c567a796e38a3b69
.reloc	0x6000	0x2b4	0x400	5.13704444817	65d412d6da26df296cce894148aac677