WildFire Analysis Report

1 File Information

File Type	PE64
File Signer	
SHA-256	35d259ba0bdf7a44595f970f1779c3770a97d10afe87ba4672638736acd45396
SHA-1	53c702ba8be63a442fb13510fccb3d50de3be42e
MD5	591fb81483d9dd1c55446c960c938e02
File Size	5334455bytes
First Seen Timestamp	2018-11-12 04:07:06 UTC
Verdict	**Benign**
Antivirus Coverage	VirusTotal Information

2 Static Analysis

2.1. Suspicious File Properties

This sample was not found to contain any high-risk content during a pre-screening analysis of the sample.

Contains overlay data with high entropy

Entropy is a measurement of the randomness in data. Overlays with high entropy indicate encoded or encrypted data.

Contains overlay data

Overlay data is extra data appended to the end of a PE image. Many legitimate files, including all files that are digitally signed, contain overlay data. However, malware often uses overlays to embed encoded or encrypted data as well.

Contains sections with size discrepancies

Sections with a large discrepancy between raw and virtual sizes may indicate a packed or obfuscated PE file.

Contains non-standard section names

Standard section names are defined by the compiler. Non-standard section names may indicate a packed or obfuscated PE file.

Contains sections with zero size

Sections with zero size indicate a packed or obfuscated PE file.

3 Dynamic Analysis

3.1. VM1 (Windows 7 x64 SP1, Adobe Reader 11, Flash 11, Office 2010)

3.1.1. Behavioral Summary

This sample was found to be **benign** on this virtual machine.

Behavior	Severity
Created a file in the Windows folder The Windows folder contains the core components of the Windows operating system. Malware often modifies the contents of this folder to manipulate the system, establish persistence, and avoid detection.	
Created an executable file in a user folder User folders are storage locations for music, pictures, downloads, and other user-specific files. Legitimate applications rarely place executable content in these folders, while malware often does so to avoid detection.	
Created or modified a file Legitimate software creates or modifies files to preserve data across system restarts. Malware may create or modify files to deliver malicious payloads or maintain persistence on a system.	
Modified the Windows Registry The Windows Registry houses system configuration settings and options, including information about installed applications, services, and drivers. Malware often modifies registry data to establish persistence on the system and avoid detection.	

3.1.2. Network Activity

DNS Queries

Domain Name	Query Type	DNS Response
teredo.ipv6.microsoft.com	NXDOMAIN	

Connections

Host	Port	Protocol	Country
224.0.0.252	5355	UDP	-

3.1.3. Host Activity

Process Activity

Process Name - sample.exe

(command: C:\Users\Administrator\sample.exe)

File Activity

File	Action	Size(B)	File Type	Hash
C:\Users\ADMINI~1\AppData\Local\Temp\nsh92E9.tmp	Create	N/A	N/A	md5:N/A sha1:N/A sha256:N/A
C:\Users\ADMINI~1\AppData\Local\Temp\nsm9309.tmp	Create	N/A	N/A	md5:N/A sha1:N/A sha256:N/A
C:\Users\ADMINI~1\AppData\Local\Temp\nsc931A.tmp	Create	N/A	N/A	md5:N/A sha1:N/A sha256:N/A

C:\Users\ADMINI~1\AppData\Local\Temp\nsc931A.tmp\LangDLL.dll	Create	N/A	N/A	md5:N/A sha1:N/A sha256:N/A
C:\Program Files\Sid Meier's Alpha Centauri\fx\CPU nn already linked.wav	Create	132198	unknown	md5:5573c2fd4f67218c20dc16a8b1b8c88b sha1:36afc1f9ab41b75c57e7bba66aa52d1ea51566f4 sha256:e4c1bf6a8108afca286e794ee1996c800b074689322b976c8a132d38c5f81dce
C:\Program Files\Sid Meier's Alpha Centauri\fx\wpn missile launcher.wav	Create	77594	unknown	md5:f41931dc3cc858e55c8dfccc480110b3 sha1:3b634977b4d463328ef8892840d65484b8090084 sha256:89308ad6519d94a82b8939dbafc3ed6a24b21934465c8865993f14b5e2805891
C:\Program Files\Sid Meier's Alpha Centauri\fx\wpn singularity laser.wav	Create	260146	unknown	md5:35685e7f42fb8ce94f3d61167894502c sha1:151060296711becf17c894f8ba73ad40e529f5ea sha256:b1056a61c65abf017cf38af3de8530d650916afc227202df77010ffbb171f505
C:\Program Files\Sid Meier's Alpha Centauri\SMACX_UP_v2.00_Uninstaller.exe	Create	97442	exe64	md5:0edc78edc5ab3eca6d55cf8611e3f51b sha1:0223e07bf2fcca774e728db4daedb93ba2dd7b95 sha256:ac694b3e4eba39eae773590094125484234b4c6a8b33b2fe1435868c228de229
C:\Program Files\Sid Meier's Alpha Centauri\terran.exe	Create	3190840	exe	md5:8029b031c44484951390158e9c5e87ec sha1:cfd41b28632f78dfbb3dd0528ca9dcdb20b2d0a7 sha256:4bcb2c57b488224edec6b7aec8713b53814c6113607744713e8a72b99fa06635
C:\Program Files\Sid Meier's Alpha Centauri\logo.pcx	Create	59578	unknown	md5:c768107546f518595a8983a447d5a054 sha1:b66996347bf5c92574e23b7e91a304d6ec068ad7 sha256:0f4261ac5c97dfa0ea2261e120f447e2ddfa52798f8a76eee9475d3c6d9dea38
C:\Program Files\Sid Meier's Alpha Centauri\netcr_sm.pcx	Create	N/A	N/A	md5:N/A sha1:N/A sha256:N/A
C:\Program Files\Sid Meier's Alpha Centauri\rdminldp_sm.pcx	Create	N/A	N/A	md5:N/A sha1:N/A sha256:N/A
C:\Program Files\Sid Meier's Alpha Centauri\alpha.txt	Create	N/A	N/A	md5:N/A sha1:N/A sha256:N/A

C:\Program Files\Sid Meier's Alpha Centauri\basename.txt	Create	N/A	N/A	md5:N/A sha1:N/A sha256:N/A
C:\Program Files\Sid Meier's Alpha Centauri\believe.txt	Create	N/A	N/A	md5:N/A sha1:N/A sha256:N/A
C:\Program Files\Sid Meier's Alpha Centauri\blurbs.txt	Create	N/A	N/A	md5:N/A sha1:N/A sha256:N/A
C:\Program Files\Sid Meier's Alpha Centauri\concepts.txt	Create	N/A	N/A	md5:N/A sha1:N/A sha256:N/A
C:\Program Files\Sid Meier's Alpha Centauri\credits.txt	Create	N/A	N/A	md5:N/A sha1:N/A sha256:N/A
C:\Program Files\Sid Meier's Alpha Centauri\facedit.txt	Create	N/A	N/A	md5:N/A sha1:N/A sha256:N/A
C:\Program Files\Sid Meier's Alpha Centauri\faction.txt	Create	N/A	N/A	md5:N/A sha1:N/A sha256:N/A
C:\Program Files\Sid Meier's Alpha Centauri\flavor.txt	Create	N/A	N/A	md5:N/A sha1:N/A sha256:N/A
C:\Program Files\Sid Meier's Alpha Centauri\gaians.txt	Create	N/A	N/A	md5:N/A sha1:N/A sha256:N/A
C:\Program Files\Sid Meier's Alpha Centauri\help.txt	Create	N/A	N/A	md5:N/A sha1:N/A sha256:N/A
C:\Program Files\Sid Meier's Alpha Centauri\hive.txt	Create	N/A	N/A	md5:N/A sha1:N/A sha256:N/A
C:\Program Files\Sid Meier's Alpha Centauri\holobook.txt	Create	N/A	N/A	md5:N/A sha1:N/A sha256:N/A
C:\Program Files\Sid Meier's Alpha Centauri\interlude.txt	Create	N/A	N/A	md5:N/A sha1:N/A sha256:N/A
C:\Program Files\Sid Meier's Alpha Centauri\jackal.txt	Create	N/A	N/A	md5:N/A sha1:N/A sha256:N/A
C:\Program Files\Sid Meier's Alpha Centauri\labels.txt	Create	N/A	N/A	md5:N/A sha1:N/A sha256:N/A
C:\Program Files\Sid Meier's Alpha Centauri\menu.txt	Create	N/A	N/A	md5:N/A sha1:N/A sha256:N/A
C:\Program Files\Sid Meier's Alpha Centauri\monument.txt	Create	N/A	N/A	md5:N/A sha1:N/A sha256:N/A
C:\Program Files\Sid Meier's Alpha Centauri\morgan.txt	Create	N/A	N/A	md5:N/A sha1:N/A sha256:N/A
C:\Program Files\Sid Meier's Alpha Centauri\movlist.txt	Create	N/A	N/A	md5:N/A sha1:N/A sha256:N/A
C:\Program Files\Sid Meier's Alpha Centauri\peace.txt	Create	N/A	N/A	md5:N/A sha1:N/A sha256:N/A

C:\Program Files\Sid Meier's Alpha Centauri\scenario.txt	Create	N/A	N/A	md5:N/A sha1:N/A sha256:N/A
C:\Program Files\Sid Meier's Alpha Centauri\script.txt	Create	N/A	N/A	md5:N/A sha1:N/A sha256:N/A
C:\Program Files\Sid Meier's Alpha Centauri\spartans.txt	Create	N/A	N/A	md5:N/A sha1:N/A sha256:N/A
C:\Program Files\Sid Meier's Alpha Centauri\system.txt	Create	N/A	N/A	md5:N/A sha1:N/A sha256:N/A
C:\Program Files\Sid Meier's Alpha Centauri\techlongs.txt	Create	N/A	N/A	md5:N/A sha1:N/A sha256:N/A
C:\Program Files\Sid Meier's Alpha Centauri\techshorts.txt	Create	N/A	N/A	md5:N/A sha1:N/A sha256:N/A
C:\Program Files\Sid Meier's Alpha Centauri\tutor.txt	Create	N/A	N/A	md5:N/A sha1:N/A sha256:N/A
C:\Program Files\Sid Meier's Alpha Centauri\univ.txt	Create	N/A	N/A	md5:N/A sha1:N/A sha256:N/A
C:\Program Files\Sid Meier's Alpha Centauri\Btchi.pcx	Create	N/A	N/A	md5:N/A sha1:N/A sha256:N/A
C:\Program Files\Sid Meier's Alpha Centauri\Btisl.pcx	Create	N/A	N/A	md5:N/A sha1:N/A sha256:N/A
C:\Program Files\Sid Meier's Alpha Centauri\Btwrm.pcx	Create	N/A	N/A	md5:N/A sha1:N/A sha256:N/A
C:\Program Files\Sid Meier's Alpha Centauri\Cursor.pcx	Create	N/A	N/A	md5:N/A sha1:N/A sha256:N/A
C:\Program Files\Sid Meier's Alpha Centauri\Gaians.pcx	Create	N/A	N/A	md5:N/A sha1:N/A sha256:N/A
C:\Program Files\Sid Meier's Alpha Centauri\SMAC_XP2000_readme.txt	Create	N/A	N/A	md5:N/A sha1:N/A sha256:N/A
C:\Program Files\Sid Meier's Alpha Centauri\believe.pcx	Create	N/A	N/A	md5:N/A sha1:N/A sha256:N/A
C:\Program Files\Sid Meier's Alpha Centauri\faction.pcx	Create	N/A	N/A	md5:N/A sha1:N/A sha256:N/A
C:\Program Files\Sid Meier's Alpha Centauri\hive.pcx	Create	N/A	N/A	md5:N/A sha1:N/A sha256:N/A
C:\Program Files\Sid Meier's Alpha Centauri\interface.pcx	Create	N/A	N/A	md5:N/A sha1:N/A sha256:N/A
C:\Program Files\Sid Meier's Alpha Centauri\morgan.pcx	Create	N/A	N/A	md5:N/A sha1:N/A sha256:N/A
C:\Program Files\Sid Meier's Alpha Centauri\peace.pcx	Create	N/A	N/A	md5:N/A sha1:N/A sha256:N/A

C:\Program Files\Sid Meier's Alpha Centauri\readme.txt	Create	N/A	N/A	md5:N/A sha1:N/A sha256:N/A
C:\Program Files\Sid Meier's Alpha Centauri\sound.dll	Create	N/A	N/A	md5:N/A sha1:N/A sha256:N/A
C:\Program Files\Sid Meier's Alpha Centauri\spartans.pcx	Create	N/A	N/A	md5:N/A sha1:N/A sha256:N/A
C:\Program Files\Sid Meier's Alpha Centauri\ter1.pcx	Create	N/A	N/A	md5:N/A sha1:N/A sha256:N/A
C:\Program Files\Sid Meier's Alpha Centauri\text.pcx	Create	N/A	N/A	md5:N/A sha1:N/A sha256:N/A
C:\Program Files\Sid Meier's Alpha Centauri\univ.pcx	Create	N/A	N/A	md5:N/A sha1:N/A sha256:N/A
C:\Program Files\Sid Meier's Alpha Centauri\arialb.ttf	Create	N/A	N/A	md5:N/A sha1:N/A sha256:N/A
C:\Program Files\Sid Meier's Alpha Centauri\ariali.ttf	Create	N/A	N/A	md5:N/A sha1:N/A sha256:N/A
C:\Program Files\Sid Meier's Alpha Centauri\arialn.ttf	Create	N/A	N/A	md5:N/A sha1:N/A sha256:N/A
C:\Program Files\Sid Meier's Alpha Centauri\arialr.ttf	Create	N/A	N/A	md5:N/A sha1:N/A sha256:N/A
C:\Windows\Fonts\ALPHC___.ttf	Create	N/A	N/A	md5:N/A sha1:N/A sha256:N/A
C:\Users\ADMINI~1\AppData\Local\Temp\nsc931A.tmp\System.dll	Create	N/A	N/A	md5:N/A sha1:N/A sha256:N/A
C:\Users\ADMINI~1\AppData\Local\Temp\nsh92E9.tmp	Delete	N/A	N/A	md5:N/A sha1:N/A sha256:N/A
C:\Users\ADMINI~1\AppData\Local\Temp\nsm9309.tmp	Delete	unknown	Sha256Empty	md5:2 sha1:Md5Empty sha256:Sha1Empty
C:\Users\ADMINI~1\AppData\Local\Temp\nsc931A.tmp	Delete	N/A	N/A	md5:N/A sha1:N/A sha256:N/A
C:\Users\ADMINI~1\AppData\Local\Temp\nsc931A.tmp\LangDLL.dll	Delete	8704	PE	md5:C9F4FDDEEAF78FC68161ED9004E1135E sha1:ae22448a795c161a649ed54e92a4f191a2064db sha256:B9A05031C6D27C067F71471AE11F636813A6D4350E64DA7ED24CFAB32FF08B91

C:\Users\ADMINI~1\AppData\Local\Temp\nsc931A.tmp\System.dll	Delete	27648	PE	md5:4E3DB9D1DF6830A091ED592DDB3DC77C sha1:4d1cfe7bd4d53c918f7b6e6c87381c367cd46a sha256:0223ABE4B01024F580EC5F662E68F7D63E13320EC0E7E6E6E99D5FBF32BFDD68

Registry Activity

Registry Key	Value	Action
HKEY_LOCAL_MACHINE\Software\Microsoft\DirectPlay\Applications\Sid Meier's Alpha Centauri		Create
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Fonts		Create
\REGISTRY\MACHINE\SOFTWARE\Microsoft\DirectPlay\Applications\Sid Meier's Alpha Centauri\UnofficialVer	2.00	Set
\REGISTRY\MACHINE\SOFTWARE\Microsoft\DirectPlay\Applications\Sid Meier's Alpha Centauri\UnofficialPath	C:\Program Files\Sid Meier's Alpha Centauri	Set
\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Fonts\Alpha Centauri (TrueType)	ALPHC___.ttf	Set

Created Mutexes

Mutex Name
<NULL>

Event Timeline

1 Created Process C:\Users\Administrator\sample.exe

2 Created file C:\Users\ADMINI~1\AppData\Local\Temp\nsh92E9.tmp

3 Deleted file C:\Users\ADMINI~1\AppData\Local\Temp\nsh92E9.tmp

4 Created file C:\Users\ADMINI~1\AppData\Local\Temp\nsm9309.tmp

5 Created file C:\Users\ADMINI~1\AppData\Local\Temp\nsm9309.tmp

6 Deleted file C:\Users\ADMINI~1\AppData\Local\Temp\nsm9309.tmp

7 Created file C:\Users\ADMINI~1\AppData\Local\Temp\nsc931A.tmp

8 Deleted file C:\Users\ADMINI~1\AppData\Local\Temp\nsc931A.tmp

9 Created file C:\Users\ADMINI~1\AppData\Local\Temp\nsc931A.tmp\LangDLL.dll

10 Created mutex

11 Set key \REGISTRY\MACHINE\SOFTWARE\Microsoft\DirectPlay\Applications\Sid Meier's Alpha Centauri\UnofficialVer to value 2.00

12 Set key \REGISTRY\MACHINE\SOFTWARE\Microsoft\DirectPlay\Applications\Sid Meier's Alpha Centauri\UnofficialPath to value C:\Program Files\Sid Meier's Alpha Centauri

13 Created file C:\Program Files\Sid Meier's Alpha Centauri\fx\CPU nn already linked.wav

14 Created file C:\Program Files\Sid Meier's Alpha Centauri\fx\wpn missile launcher.wav

15 Created file C:\Program Files\Sid Meier's Alpha Centauri\fx\wpn singularity laser.wav

16 Created file C:\Program Files\Sid Meier's Alpha Centauri\SMACX_UP_v2.00_Uninstaller.exe

17 Created file C:\Program Files\Sid Meier's Alpha Centauri\terran.exe
18 Created file C:\Program Files\Sid Meier's Alpha Centauri\logo.pcx
19 Created file C:\Program Files\Sid Meier's Alpha Centauri\netcr_sm.pcx
20 Created file C:\Program Files\Sid Meier's Alpha Centauri\rdminldp_sm.pcx
21 Created file C:\Program Files\Sid Meier's Alpha Centauri\alpha.txt
22 Created file C:\Program Files\Sid Meier's Alpha Centauri\basename.txt
23 Created file C:\Program Files\Sid Meier's Alpha Centauri\believe.txt
24 Created file C:\Program Files\Sid Meier's Alpha Centauri\blurbs.txt
25 Created file C:\Program Files\Sid Meier's Alpha Centauri\concepts.txt
26 Created file C:\Program Files\Sid Meier's Alpha Centauri\credits.txt
27 Created file C:\Program Files\Sid Meier's Alpha Centauri\facedit.txt
28 Created file C:\Program Files\Sid Meier's Alpha Centauri\faction.txt
29 Created file C:\Program Files\Sid Meier's Alpha Centauri\flavor.txt
30 Created file C:\Program Files\Sid Meier's Alpha Centauri\gaians.txt
31 Created file C:\Program Files\Sid Meier's Alpha Centauri\help.txt
32 Created file C:\Program Files\Sid Meier's Alpha Centauri\hive.txt
33 Created file C:\Program Files\Sid Meier's Alpha Centauri\holobook.txt
34 Created file C:\Program Files\Sid Meier's Alpha Centauri\interlude.txt
35 Created file C:\Program Files\Sid Meier's Alpha Centauri\jackal.txt
36 Created file C:\Program Files\Sid Meier's Alpha Centauri\labels.txt
37 Created file C:\Program Files\Sid Meier's Alpha Centauri\menu.txt
38 Created file C:\Program Files\Sid Meier's Alpha Centauri\monument.txt
39 Created file C:\Program Files\Sid Meier's Alpha Centauri\morgan.txt
40 Created file C:\Program Files\Sid Meier's Alpha Centauri\movlist.txt
41 Created file C:\Program Files\Sid Meier's Alpha Centauri\peace.txt
42 Created file C:\Program Files\Sid Meier's Alpha Centauri\scenario.txt
43 Created file C:\Program Files\Sid Meier's Alpha Centauri\script.txt
44 Created file C:\Program Files\Sid Meier's Alpha Centauri\spartans.txt
45 Created file C:\Program Files\Sid Meier's Alpha Centauri\system.txt
46 Created file C:\Program Files\Sid Meier's Alpha Centauri\techlongs.txt
47 Created file C:\Program Files\Sid Meier's Alpha Centauri\techshorts.txt
48 Created file C:\Program Files\Sid Meier's Alpha Centauri\tutor.txt
49 Created file C:\Program Files\Sid Meier's Alpha Centauri\univ.txt
50 Created file C:\Program Files\Sid Meier's Alpha Centauri\Btchi.pcx
51 Created file C:\Program Files\Sid Meier's Alpha Centauri\Btisl.pcx
52 Created file C:\Program Files\Sid Meier's Alpha Centauri\Btwrm.pcx
53 Created file C:\Program Files\Sid Meier's Alpha Centauri\Cursor.pcx
54 Created file C:\Program Files\Sid Meier's Alpha Centauri\Gaians.pcx

55 Created file C:\Program Files\Sid Meier's Alpha Centauri\SMAC_XP2000_readme.txt

56 Created file C:\Program Files\Sid Meier's Alpha Centauri\believe.pcx

57 Created file C:\Program Files\Sid Meier's Alpha Centauri\faction.pcx

58 Created file C:\Program Files\Sid Meier's Alpha Centauri\hive.pcx

59 Created file C:\Program Files\Sid Meier's Alpha Centauri\interface.pcx

60 Created file C:\Program Files\Sid Meier's Alpha Centauri\morgan.pcx

61 Created file C:\Program Files\Sid Meier's Alpha Centauri\peace.pcx

62 Created file C:\Program Files\Sid Meier's Alpha Centauri\readme.txt

63 Created file C:\Program Files\Sid Meier's Alpha Centauri\sound.dll

64 Created file C:\Program Files\Sid Meier's Alpha Centauri\spartans.pcx

65 Created file C:\Program Files\Sid Meier's Alpha Centauri\ter1.pcx

66 Created file C:\Program Files\Sid Meier's Alpha Centauri\text.pcx

67 Created file C:\Program Files\Sid Meier's Alpha Centauri\univ.pcx

68 Created file C:\Program Files\Sid Meier's Alpha Centauri\arialb.ttf

69 Created file C:\Program Files\Sid Meier's Alpha Centauri\ariali.ttf

70 Created file C:\Program Files\Sid Meier's Alpha Centauri\arialn.ttf

71 Created file C:\Program Files\Sid Meier's Alpha Centauri\arialr.ttf

72 Created file C:\Windows\Fonts\ALPHC___.ttf

73 Created file C:\Users\ADMINI~1\AppData\Local\Temp\nsc931A.tmp\System.dll

74 Set key \REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Fonts\Alpha Centauri (TrueType) to value ALPHC___.ttf

75 Deleted file C:\Users\ADMINI~1\AppData\Local\Temp\nsc931A.tmp\LangDLL.dll

76 Deleted file C:\Users\ADMINI~1\AppData\Local\Temp\nsc931A.tmp\System.dll

3.2. VM2 (Windows 10 x64, Flash 22, Adobe Reader 11, Office 2010)

3.2.1. Behavioral Summary

This sample was found to be **benign** on this virtual machine.

Behavior	Severity
Created a file in the Windows folder The Windows folder contains the core components of the Windows operating system. Malware often modifies the contents of this folder to manipulate the system, establish persistence, and avoid detection.	
Created or modified a file in the Windows system folder The Windows system folder contains configuration files and executables that control the underlying functions of the system. Malware often modifies the contents of this folder to manipulate the system, establish persistence, and avoid detection.	
Created or modified a file Legitimate software creates or modifies files to preserve data across system restarts. Malware may create or modify files to deliver malicious payloads or maintain persistence on a system.	
Modified the Windows Registry The Windows Registry houses system configuration settings and options, including information about installed applications, services, and drivers. Malware often modifies registry data to establish persistence on the system and avoid detection.	

Crashed when loaded Compatibility issues and missing resources might cause legitimate applications to crash. However, malware also often crashes applications as a side-effect of attempting to exploit them, and may still be successful in spite of the crash.	
Created an executable file in a user folder User folders are storage locations for music, pictures, downloads, and other user-specific files. Legitimate applications rarely place executable content in these folders, while malware often does so to avoid detection.	

3.2.2. Network Activity

DNS Queries

Domain Name	Query Type	DNS Response
dscg.akamaiedge.net	NS	n6dscg.akamaiedge.net
phicdn.net	NS	ns4.phicdn.net
phicdn.net	NS	ns3.phicdn.net
akadns6.net	NS	a6-130.akadns.org
dspg.akamaiedge.net	NS	n4dspg.akamaiedge.net
dspg.akamaiedge.net	NS	n1dspg.akamaiedge.net
dscg.akamaiedge.net	NS	n0dscg.akamaiedge.net
dscg.akamaiedge.net	NS	n1dscg.akamaiedge.net
c-msedge.net	NS	ns2.c-msedge.net
phicdn.net	NS	ns1.phicdn.net
dspg.akamaiedge.net	NS	n2dspg.akamaiedge.net
akadns6.net	NS	a18-131.akadns.org
phicdn.net	NS	ns2.phicdn.net
dscg.akamaiedge.net	NS	n3dscg.akamaiedge.net
akadns6.net	NS	a12-130.akadns.org
akadns6.net	NS	a11-128.akadns6.net
trafficmanager.net	NS	tm1.edgedns-tm.info
dspg.akamaiedge.net	NS	n5dspg.akamaiedge.net
dscg.akamaiedge.net	NS	n4dscg.akamaiedge.net
akadns6.net	NS	a1-131.akadns6.net
c-msedge.net	NS	ns1.c-msedge.net
akadns6.net	NS	a7-130.akadns6.net
akadns6.net	NS	a3-128.akadns6.net
dscg.akamaiedge.net	NS	n2dscg.akamaiedge.net
dspg.akamaiedge.net	NS	n6dspg.akamaiedge.net
trafficmanager.net	NS	tm2.msft.net
akadns6.net	NS	a9-131.akadns6.net
dspg.akamaiedge.net	NS	n0dspg.akamaiedge.net
dscg.akamaiedge.net	NS	n5dscg.akamaiedge.net
trafficmanager.net	NS	tm1.msft.net
dspg.akamaiedge.net	NS	n3dspg.akamaiedge.net

dscg.akamaiedge.net	NS	n7dscg.akamaiedge.net
dspg.akamaiedge.net	NS	n7dspg.akamaiedge.net
akadns6.net	NS	a13-129.akadns.org
win10.ipv6.microsoft.com	A	157.56.144.215
akadns6.net	NS	a5-129.akadns.org

Connections

Host	Port	Protocol	Country
224.0.0.252	5355	UDP	-

3.2.3. Host Activity

Process Activity

Process Name - sample.exe

(command: C:\Users\Administrator\sample.exe)

File Activity

File	Action	Size(B)	File Type	Hash
C:\Users\ADMINI~1\AppData\Local\Temp\nswF618.tmp	Create	N/A	N/A	md5:N/A sha1:N/A sha256:N/A
C:\Users\ADMINI~1\AppData\Local\Temp\nsbF638.tmp	Create	N/A	N/A	md5:N/A sha1:N/A sha256:N/A
C:\Users\ADMINI~1\AppData\Local\Temp\nsbF639.tmp	Create	N/A	N/A	md5:N/A sha1:N/A sha256:N/A
C:\Users\ADMINI~1\AppData\Local\Temp\nsbF639.tmp\LangDLL.dll	Create	N/A	N/A	md5:N/A sha1:N/A sha256:N/A
C:\Program Files\Sid Meier's Alpha Centauri\fx\CPU nn already linked.wav	Create	132198	unknown	md5:5573c2fd4f67218c20dc16a8b1b8c88b sha1:36afc1f9ab41b75c57e7bba66aa52d1ea51566f4 sha256:e4c1bf6a8108afca286e794ee1996c800b074689322b976c8a132d38c5f81dce
C:\Program Files\Sid Meier's Alpha Centauri\fx\wpn missile launcher.wav	Create	77594	unknown	md5:f41931dc3cc858e55c8dfccc480110b3 sha1:3b634977b4d463328ef8892840d65484b8090084 sha256:89308ad6519d94a82b8939dbafc3ed6a24b21934465c8865993f14b5e2805891
C:\Program Files\Sid Meier's Alpha Centauri\fx\wpn singularity laser.wav	Create	260146	unknown	md5:35685e7f42fb8ce94f3d61167894502c sha1:151060296711becf17c894f8ba73ad40e529f5ea sha256:b1056a61c65abf017cf38af3de8530d650916afc227202df77010ffbb171f505

C:\Program Files\Sid Meier's Alpha Centauri\SMACX_UP_v2.00_Uninstaller.exe	Create	97442	exe64	md5:0edc78edc5ab3eca6d55cf8611e3f51b sha1:0223e07bf2fcca774e728db4daedb93ba2dd7b95 sha256:ac694b3e4eba39eae773590094125484234b4c6a8b33b2fe1435868c228de229
C:\Program Files\Sid Meier's Alpha Centauri\terran.exe	Create	3190840	exe	md5:8029b031c44484951390158e9c5e87ec sha1:cfd41b28632f78dfbb3dd0528ca9dcdb20b2d0a7 sha256:4bcb2c57b488224edec6b7aec8713b53814c6113607744713e8a72b99fa06635
C:\Program Files\Sid Meier's Alpha Centauri\logo.pcx	Create	59578	unknown	md5:c768107546f518595a8983a447d5a054 sha1:b66996347bf5c92574e23b7e91a304d6ec068ad7 sha256:0f4261ac5c97dfa0ea2261e120f447e2ddfa52798f8a76eee9475d3c6d9dea38
C:\Program Files\Sid Meier's Alpha Centauri\netcr_sm.pcx	Create	N/A	N/A	md5:N/A sha1:N/A sha256:N/A
C:\Program Files\Sid Meier's Alpha Centauri\rdminldp_sm.pcx	Create	N/A	N/A	md5:N/A sha1:N/A sha256:N/A
C:\Program Files\Sid Meier's Alpha Centauri\alpha.txt	Create	N/A	N/A	md5:N/A sha1:N/A sha256:N/A
C:\Program Files\Sid Meier's Alpha Centauri\basename.txt	Create	N/A	N/A	md5:N/A sha1:N/A sha256:N/A
C:\Program Files\Sid Meier's Alpha Centauri\believe.txt	Create	N/A	N/A	md5:N/A sha1:N/A sha256:N/A
C:\Program Files\Sid Meier's Alpha Centauri\blurbs.txt	Create	N/A	N/A	md5:N/A sha1:N/A sha256:N/A
C:\Program Files\Sid Meier's Alpha Centauri\concepts.txt	Create	N/A	N/A	md5:N/A sha1:N/A sha256:N/A
C:\Program Files\Sid Meier's Alpha Centauri\credits.txt	Create	N/A	N/A	md5:N/A sha1:N/A sha256:N/A
C:\Program Files\Sid Meier's Alpha Centauri\facedit.txt	Create	N/A	N/A	md5:N/A sha1:N/A sha256:N/A
C:\Program Files\Sid Meier's Alpha Centauri\faction.txt	Create	N/A	N/A	md5:N/A sha1:N/A sha256:N/A
C:\Program Files\Sid Meier's Alpha Centauri\flavor.txt	Create	N/A	N/A	md5:N/A sha1:N/A sha256:N/A
C:\Program Files\Sid Meier's Alpha Centauri\gaians.txt	Create	N/A	N/A	md5:N/A sha1:N/A sha256:N/A

C:\Program Files\Sid Meier's Alpha Centauri\help.txt	Create	N/A	N/A	md5:N/A sha1:N/A sha256:N/A
C:\Program Files\Sid Meier's Alpha Centauri\hive.txt	Create	N/A	N/A	md5:N/A sha1:N/A sha256:N/A
C:\Program Files\Sid Meier's Alpha Centauri\holobook.txt	Create	N/A	N/A	md5:N/A sha1:N/A sha256:N/A
C:\Program Files\Sid Meier's Alpha Centauri\interlude.txt	Create	N/A	N/A	md5:N/A sha1:N/A sha256:N/A
C:\Program Files\Sid Meier's Alpha Centauri\jackal.txt	Create	N/A	N/A	md5:N/A sha1:N/A sha256:N/A
C:\Program Files\Sid Meier's Alpha Centauri\labels.txt	Create	N/A	N/A	md5:N/A sha1:N/A sha256:N/A
C:\Program Files\Sid Meier's Alpha Centauri\menu.txt	Create	N/A	N/A	md5:N/A sha1:N/A sha256:N/A
C:\Program Files\Sid Meier's Alpha Centauri\monument.txt	Create	N/A	N/A	md5:N/A sha1:N/A sha256:N/A
C:\Program Files\Sid Meier's Alpha Centauri\morgan.txt	Create	N/A	N/A	md5:N/A sha1:N/A sha256:N/A
C:\Program Files\Sid Meier's Alpha Centauri\movlist.txt	Create	N/A	N/A	md5:N/A sha1:N/A sha256:N/A
C:\Program Files\Sid Meier's Alpha Centauri\peace.txt	Create	N/A	N/A	md5:N/A sha1:N/A sha256:N/A
C:\Program Files\Sid Meier's Alpha Centauri\scenario.txt	Create	N/A	N/A	md5:N/A sha1:N/A sha256:N/A
C:\Program Files\Sid Meier's Alpha Centauri\script.txt	Create	N/A	N/A	md5:N/A sha1:N/A sha256:N/A
C:\Program Files\Sid Meier's Alpha Centauri\spartans.txt	Create	N/A	N/A	md5:N/A sha1:N/A sha256:N/A
C:\Program Files\Sid Meier's Alpha Centauri\system.txt	Create	N/A	N/A	md5:N/A sha1:N/A sha256:N/A
C:\Program Files\Sid Meier's Alpha Centauri\techlongs.txt	Create	N/A	N/A	md5:N/A sha1:N/A sha256:N/A
C:\Program Files\Sid Meier's Alpha Centauri\techshorts.txt	Create	N/A	N/A	md5:N/A sha1:N/A sha256:N/A
C:\Program Files\Sid Meier's Alpha Centauri\tutor.txt	Create	N/A	N/A	md5:N/A sha1:N/A sha256:N/A
C:\Program Files\Sid Meier's Alpha Centauri\univ.txt	Create	N/A	N/A	md5:N/A sha1:N/A sha256:N/A
C:\Program Files\Sid Meier's Alpha Centauri\Btchi.pcx	Create	N/A	N/A	md5:N/A sha1:N/A sha256:N/A

C:\Program Files\Sid Meier's Alpha Centauri\Btisl.pcx	Create	N/A	N/A	md5:N/A sha1:N/A sha256:N/A
C:\Program Files\Sid Meier's Alpha Centauri\Btwrm.pcx	Create	N/A	N/A	md5:N/A sha1:N/A sha256:N/A
C:\Program Files\Sid Meier's Alpha Centauri\Cursor.pcx	Create	N/A	N/A	md5:N/A sha1:N/A sha256:N/A
C:\Program Files\Sid Meier's Alpha Centauri\Gaians.pcx	Create	N/A	N/A	md5:N/A sha1:N/A sha256:N/A
C:\Program Files\Sid Meier's Alpha Centauri\SMAC_XP2000_readme.txt	Create	N/A	N/A	md5:N/A sha1:N/A sha256:N/A
C:\Program Files\Sid Meier's Alpha Centauri\believe.pcx	Create	N/A	N/A	md5:N/A sha1:N/A sha256:N/A
C:\Program Files\Sid Meier's Alpha Centauri\faction.pcx	Create	N/A	N/A	md5:N/A sha1:N/A sha256:N/A
C:\Program Files\Sid Meier's Alpha Centauri\hive.pcx	Create	N/A	N/A	md5:N/A sha1:N/A sha256:N/A
C:\Program Files\Sid Meier's Alpha Centauri\interface.pcx	Create	N/A	N/A	md5:N/A sha1:N/A sha256:N/A
C:\Program Files\Sid Meier's Alpha Centauri\morgan.pcx	Create	N/A	N/A	md5:N/A sha1:N/A sha256:N/A
C:\Program Files\Sid Meier's Alpha Centauri\peace.pcx	Create	N/A	N/A	md5:N/A sha1:N/A sha256:N/A
C:\Program Files\Sid Meier's Alpha Centauri\readme.txt	Create	N/A	N/A	md5:N/A sha1:N/A sha256:N/A
C:\Program Files\Sid Meier's Alpha Centauri\sound.dll	Create	N/A	N/A	md5:N/A sha1:N/A sha256:N/A
C:\Program Files\Sid Meier's Alpha Centauri\spartans.pcx	Create	N/A	N/A	md5:N/A sha1:N/A sha256:N/A
C:\Program Files\Sid Meier's Alpha Centauri\ter1.pcx	Create	N/A	N/A	md5:N/A sha1:N/A sha256:N/A
C:\Program Files\Sid Meier's Alpha Centauri\text.pcx	Create	N/A	N/A	md5:N/A sha1:N/A sha256:N/A
C:\Program Files\Sid Meier's Alpha Centauri\univ.pcx	Create	N/A	N/A	md5:N/A sha1:N/A sha256:N/A
C:\Program Files\Sid Meier's Alpha Centauri\arialb.ttf	Create	N/A	N/A	md5:N/A sha1:N/A sha256:N/A
C:\Program Files\Sid Meier's Alpha Centauri\ariali.ttf	Create	N/A	N/A	md5:N/A sha1:N/A sha256:N/A
C:\Program Files\Sid Meier's Alpha Centauri\arialn.ttf	Create	N/A	N/A	md5:N/A sha1:N/A sha256:N/A

C:\Program Files\Sid Meier's Alpha Centauri\arialr.ttf	Create	N/A	N/A	md5:N/A sha1:N/A sha256:N/A
C:\Windows\Fonts\ALPHC___.ttf	Create	N/A	N/A	md5:N/A sha1:N/A sha256:N/A
C:\Users\ADMINI~1\AppData\Local\Temp\nsbF639.tmp\System.dll	Create	N/A	N/A	md5:N/A sha1:N/A sha256:N/A
C:\Users\ADMINI~1\AppData\Local\Temp\nswF618.tmp	Delete	N/A	N/A	md5:N/A sha1:N/A sha256:N/A
C:\Users\ADMINI~1\AppData\Local\Temp\nsbF638.tmp	Delete	unknown	Sha256Empty	md5:2 sha1:Md5Empty sha256:Sha1Empty
C:\Users\ADMINI~1\AppData\Local\Temp\nsbF639.tmp	Delete	N/A	N/A	md5:N/A sha1:N/A sha256:N/A
C:\Users\ADMINI~1\AppData\Local\Temp\nsbF639.tmp\LangDLL.dll	Delete	8704	PE	md5:C9F4FDDEEAF78FC68161ED9004E1135E sha1:ae22448a795c161a649ed54e92a4f191a2064db sha256:B9A05031C6D27C067F71471AE11F636813A6D4350E64DA7ED24CFAB32FF08B91
C:\Users\ADMINI~1\AppData\Local\Temp\nsbF639.tmp\System.dll	Delete	27648	PE	md5:4E3DB9D1DF6830A091ED592DDB3DC77C sha1:4d1cfe7bd4d53c918f7b6e6c87381c367cd46a sha256:0223ABE4B01024F580EC5F662E68F7D63E13320EC0E7E6E6E99D5FBF32BFDD68

Registry Activity

Registry Key	Value	Action
HKEY_LOCAL_MACHINE\Software\Microsoft\DirectPlay\Applications\Sid Meier's Alpha Centauri		Create
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Fonts		Create
\REGISTRY\MACHINE\SOFTWARE\Microsoft\DirectPlay\Applications\Sid Meier's Alpha Centauri\UnofficialVer	2.00	Set
\REGISTRY\MACHINE\SOFTWARE\Microsoft\DirectPlay\Applications\Sid Meier's Alpha Centauri\UnofficialPath	C:\Program Files\Sid Meier's Alpha Centauri	Set
\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Fonts\Alpha Centauri (TrueType)	ALPHC___.ttf	Set

Created Mutexes

Mutex Name
Local\SessionImmersiveColorMutex
<NULL>

Event Timeline

1	Created Process C:\Users\Administrator\sample.exe
2	Created file C:\Users\ADMINI~1\AppData\Local\Temp\nswF618.tmp
3	Deleted file C:\Users\ADMINI~1\AppData\Local\Temp\nswF618.tmp
4	Created file C:\Users\ADMINI~1\AppData\Local\Temp\nsbF638.tmp
5	Created file C:\Users\ADMINI~1\AppData\Local\Temp\nsbF638.tmp
6	Deleted file C:\Users\ADMINI~1\AppData\Local\Temp\nsbF638.tmp
7	Created file C:\Users\ADMINI~1\AppData\Local\Temp\nsbF639.tmp
8	Deleted file C:\Users\ADMINI~1\AppData\Local\Temp\nsbF639.tmp
9	Created file C:\Users\ADMINI~1\AppData\Local\Temp\nsbF639.tmp\LangDLL.dll
10	Created mutex Local\SessionImmersiveColorMutex
11	Created mutex
12	Set key \REGISTRY\MACHINE\SOFTWARE\Microsoft\DirectPlay\Applications\Sid Meier's Alpha Centauri\UnofficialVer to value 2.00
13	Set key \REGISTRY\MACHINE\SOFTWARE\Microsoft\DirectPlay\Applications\Sid Meier's Alpha Centauri\UnofficialPath to value C:\Program Files\Sid Meier's Alpha Centauri
14	Created file C:\Program Files\Sid Meier's Alpha Centauri\fx\CPU nn already linked.wav
15	Created file C:\Program Files\Sid Meier's Alpha Centauri\fx\wpn missile launcher.wav
16	Created file C:\Program Files\Sid Meier's Alpha Centauri\fx\wpn singularity laser.wav
17	Created file C:\Program Files\Sid Meier's Alpha Centauri\SMACX_UP_v2.00_Uninstaller.exe
18	Created file C:\Program Files\Sid Meier's Alpha Centauri\terran.exe
19	Created file C:\Program Files\Sid Meier's Alpha Centauri\logo.pcx
20	Created file C:\Program Files\Sid Meier's Alpha Centauri\netcr_sm.pcx
21	Created file C:\Program Files\Sid Meier's Alpha Centauri\rdminldp_sm.pcx
22	Created file C:\Program Files\Sid Meier's Alpha Centauri\alpha.txt
23	Created file C:\Program Files\Sid Meier's Alpha Centauri\basename.txt
24	Created file C:\Program Files\Sid Meier's Alpha Centauri\believe.txt
25	Created file C:\Program Files\Sid Meier's Alpha Centauri\blurbs.txt
26	Created file C:\Program Files\Sid Meier's Alpha Centauri\concepts.txt
27	Created file C:\Program Files\Sid Meier's Alpha Centauri\credits.txt
28	Created file C:\Program Files\Sid Meier's Alpha Centauri\facedit.txt
29	Created file C:\Program Files\Sid Meier's Alpha Centauri\faction.txt
30	Created file C:\Program Files\Sid Meier's Alpha Centauri\flavor.txt
31	Created file C:\Program Files\Sid Meier's Alpha Centauri\gaians.txt
32	Created file C:\Program Files\Sid Meier's Alpha Centauri\help.txt
33	Created file C:\Program Files\Sid Meier's Alpha Centauri\hive.txt
34	Created file C:\Program Files\Sid Meier's Alpha Centauri\holobook.txt
35	Created file C:\Program Files\Sid Meier's Alpha Centauri\interlude.txt
36	Created file C:\Program Files\Sid Meier's Alpha Centauri\jackal.txt
37	Created file C:\Program Files\Sid Meier's Alpha Centauri\labels.txt

38 Created file C:\Program Files\Sid Meier's Alpha Centauri\menu.txt
39 Created file C:\Program Files\Sid Meier's Alpha Centauri\monument.txt
40 Created file C:\Program Files\Sid Meier's Alpha Centauri\morgan.txt
41 Created file C:\Program Files\Sid Meier's Alpha Centauri\movlist.txt
42 Created file C:\Program Files\Sid Meier's Alpha Centauri\peace.txt
43 Created file C:\Program Files\Sid Meier's Alpha Centauri\scenario.txt
44 Created file C:\Program Files\Sid Meier's Alpha Centauri\script.txt
45 Created file C:\Program Files\Sid Meier's Alpha Centauri\spartans.txt
46 Created file C:\Program Files\Sid Meier's Alpha Centauri\system.txt
47 Created file C:\Program Files\Sid Meier's Alpha Centauri\techlongs.txt
48 Created file C:\Program Files\Sid Meier's Alpha Centauri\techshorts.txt
49 Created file C:\Program Files\Sid Meier's Alpha Centauri\tutor.txt
50 Created file C:\Program Files\Sid Meier's Alpha Centauri\univ.txt
51 Created file C:\Program Files\Sid Meier's Alpha Centauri\Btchi.pcx
52 Created file C:\Program Files\Sid Meier's Alpha Centauri\Btisl.pcx
53 Created file C:\Program Files\Sid Meier's Alpha Centauri\Btwrm.pcx
54 Created file C:\Program Files\Sid Meier's Alpha Centauri\Cursor.pcx
55 Created file C:\Program Files\Sid Meier's Alpha Centauri\Gaians.pcx
56 Created file C:\Program Files\Sid Meier's Alpha Centauri\SMAC_XP2000_readme.txt
57 Created file C:\Program Files\Sid Meier's Alpha Centauri\believe.pcx
58 Created file C:\Program Files\Sid Meier's Alpha Centauri\faction.pcx
59 Created file C:\Program Files\Sid Meier's Alpha Centauri\hive.pcx
60 Created file C:\Program Files\Sid Meier's Alpha Centauri\interface.pcx
61 Created file C:\Program Files\Sid Meier's Alpha Centauri\morgan.pcx
62 Created file C:\Program Files\Sid Meier's Alpha Centauri\peace.pcx
63 Created file C:\Program Files\Sid Meier's Alpha Centauri\readme.txt
64 Created file C:\Program Files\Sid Meier's Alpha Centauri\sound.dll
65 Created file C:\Program Files\Sid Meier's Alpha Centauri\spartans.pcx
66 Created file C:\Program Files\Sid Meier's Alpha Centauri\ter1.pcx
67 Created file C:\Program Files\Sid Meier's Alpha Centauri\text.pcx
68 Created file C:\Program Files\Sid Meier's Alpha Centauri\univ.pcx
69 Created file C:\Program Files\Sid Meier's Alpha Centauri\arialb.ttf
70 Created file C:\Program Files\Sid Meier's Alpha Centauri\ariali.ttf
71 Created file C:\Program Files\Sid Meier's Alpha Centauri\arialn.ttf
72 Created file C:\Program Files\Sid Meier's Alpha Centauri\arialr.ttf
73 Created file C:\Windows\Fonts\ALPHC___.ttf
74 Created file C:\Users\ADMINI~1\AppData\Local\Temp\nsbF639.tmp\System.dll

75 Set key \REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Fonts\Alpha Centauri (TrueType) to value ALPHC___.ttf

76 Deleted file C:\Users\ADMINI~1\AppData\Local\Temp\nsbF639.tmp\LangDLL.dll

77 Deleted file C:\Users\ADMINI~1\AppData\Local\Temp\nsbF639.tmp\System.dll