e055b5500085... (/Malware/Malware /e055b550008507a6d99adc10267734bc3008237d) / Cuckoo Raporu (WINDOWS7-32)

Category	Started On	Completed On	Duration	Cuckoo Version	Machine	Options
file	2017-11-14 18:11:49	2017-11-14 18:12:16	27	1.2	Win7-32-A9O7	Internet yok:0

File Details

File name	flashplayer27pp_ka.exe
File size	1569792 bytes
File type	PE32 executable (GUI) Intel 80386, for MS Windows
CRC32	47DFFFFB
MD5	83f9b5ae553fc00f45152cefb4d9f614
SHA1	e055b550008507a6d99adc10267734bc3008237d
SHA256	8a569d74c63ff14a134b6484979be420496988e9836f71587b51c51542b2ab92
SHA512	1dc6f0b81b16ba68d55462be7c494bfc8ea66ae23862e37d623d20d4f231b20b490176e5e27c5fb06fca2dfe21855a197bc08a7b944f04fc89ec18a4a2a03920
Ssdeep	24576:MIsx2NO/kx4P7KszrdwU3z6am06LWGNLcSeIJDbxRtwgX149Hyf49+g723d:Mdkukx4TrSLWOzeMX+599r
PEiD	None matched
Yara	None matched
VirusTotal	VirusTotal lookup disabled, add your API key to the module

Signatures

The binary likely contains encrypted or compressed data.

Checks the version of Bios, possibly for anti-virtualization

Checks for the presence of known windows from debuggers and forensic tools

Tries to unhook Windows functions monitored by Cuckoo

Checks for the presence of known devices from debuggers and forensic tools

Screenshots

(/CuckooReport/Screenshot?reportId=5a0aff5017c591044899bc25&shotIndex=1)

(/CuckooReport/Screenshot?reportId=5a0aff5017c591044899bc25&shotIndex=2)

(/CuckooReport/Screenshot?reportId=5a0aff5017c591044899bc25&shotIndex=3)

(/CuckooReport/Screenshot?reportId=5a0aff5017c591044899bc25&shotIndex=4)

Static Analysis

Sections

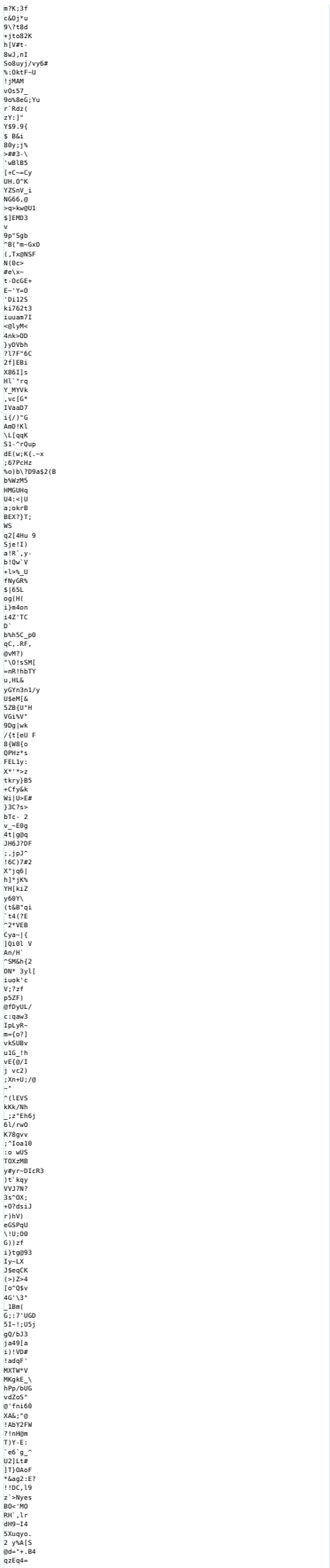
Name	Virtual Address	Virtual Size	Size of Raw Data	Entropy
\x00	0x00001000	0x0006b000	0x00032600	7.9814651472930 8
.rsrc	0x0006c000	0x000122cb	0x0000a400	7.9439021075310 5
.idata	0x0007f000	0x00001000	0x00000200	1.1451457081514 2
	0x00080000	0x001a1000	0x00000200	0.2607712760482 56
dicyzivh	0x00221000	0x0013f000	0x0013f000	7.8978248369692 9
tdhsnuds	0x00360000	0x00001000	0x00000400	6.3457098122097 4
.taggant	0x00361000	0x00003000	0x00002200	0.7777027298632 49

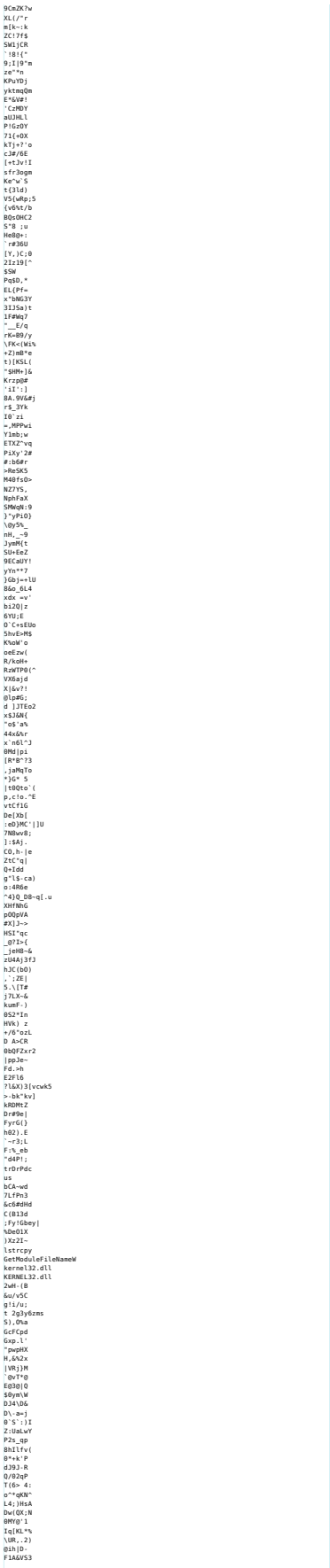
Imports

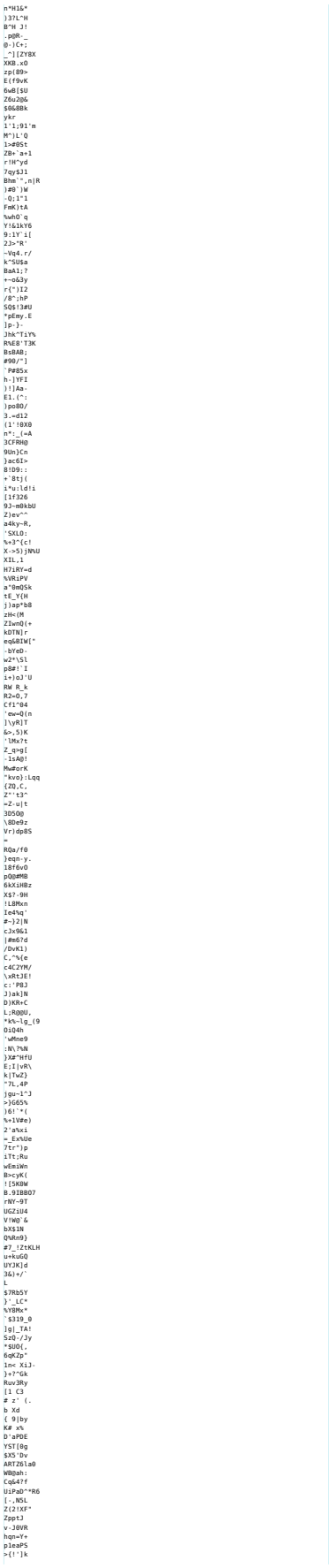
Library kernel32.dll:
- 0x47f03b - lstrcpy

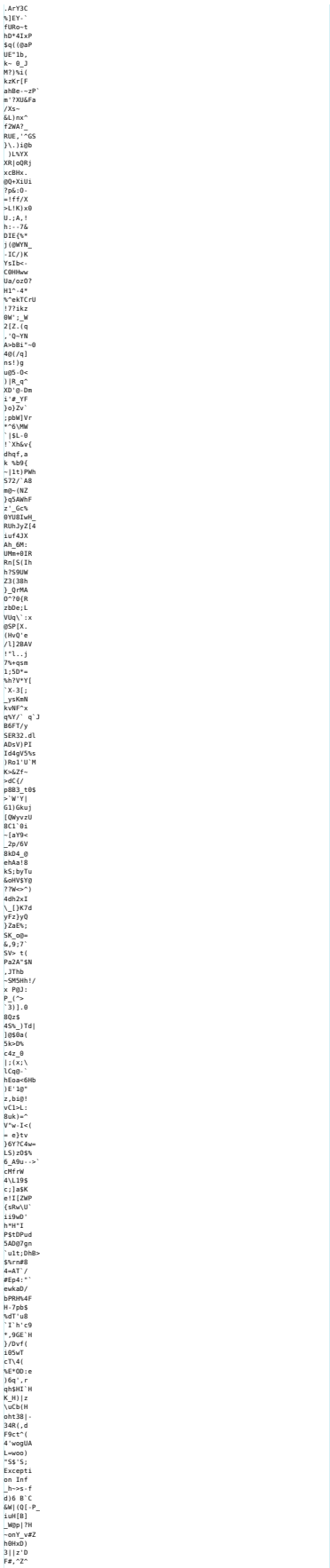
Strings

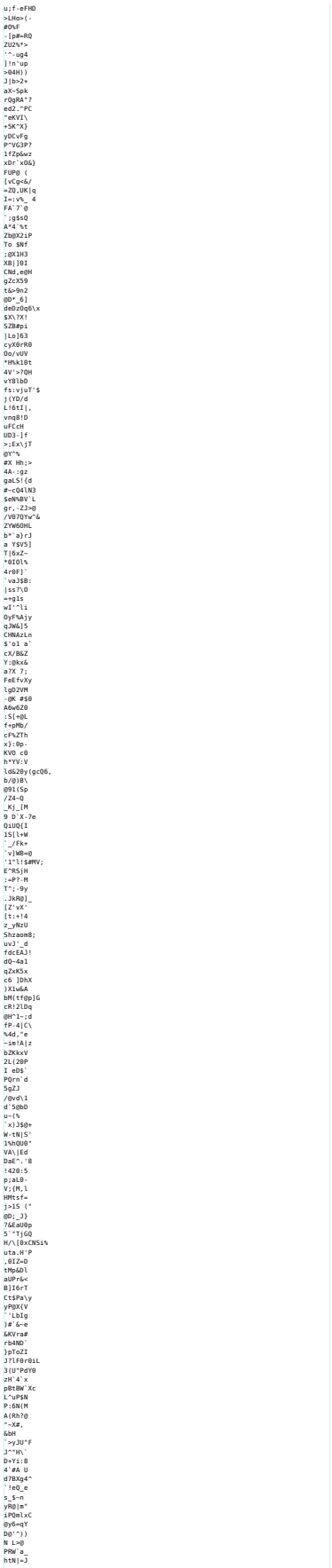
```
!This program cannot be run in DOS mode.
.idata
dicyzivh
tdhsnuds
.taggant
1P·oAP%o
i>cWL+
X}fWj
L9o".E
!VO#/fr
d9W+q_
Q2SR4[
H&Oa[nQn1
jwancX/
}PoO)9L5D
DW o]
{$\E$!
!sS,qU
V{H!c]Z
Wc?YXd
,+!)$q
Wy]`
xI/Nl=
iXt 'S
:,K!C57b
S#vbSI
fMt'ZS
]v:#+O)
%kS'Eu
~vBp6*
S~D+1=a
j1|go&A
]#'7k@Md5*
y5)f5x
$%'//t
^\nWYl
$!L_d6-
N-7`>Q.A
qM@``-
oF%KKEA
x,Hs)W2
bJV!0
6OpsQT
fo2MEl
U:0!"mw
/AcH.=I
:`WSWu
x:54)f
j'M!=
w<\WIM?
qyn|$5
bI8*9.W
5D*A%I
*GrBb,0
#!Zfi2
z{JO.[
JL0ioT
f'*qDY
2@Pep1
`u1TF+S
!YO{Iz?
x#tYz.UR%·.
D=_P2<
&\>]y[]
A%a7Y6
```

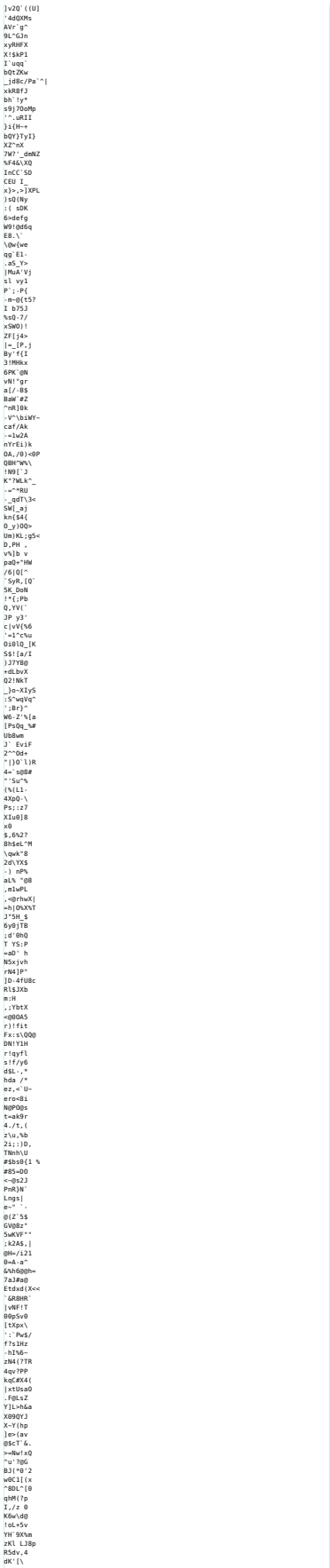


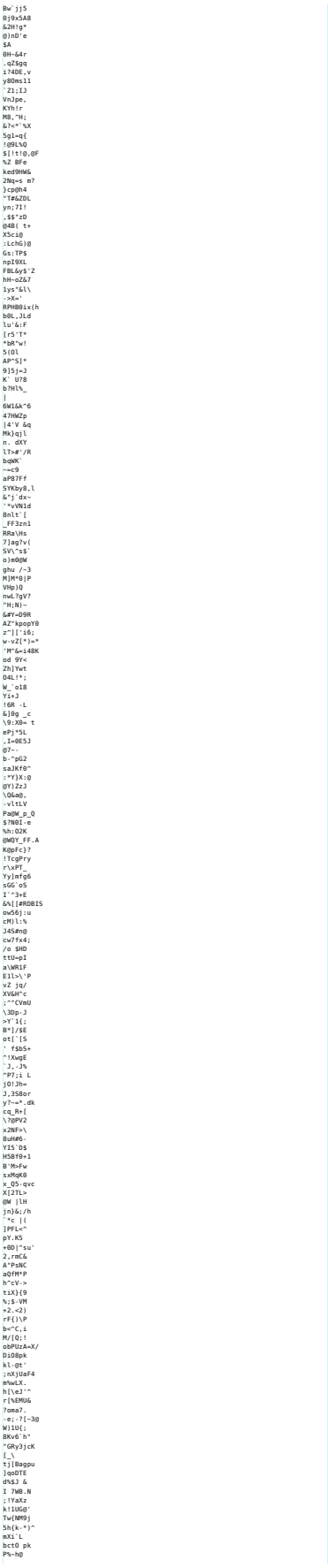


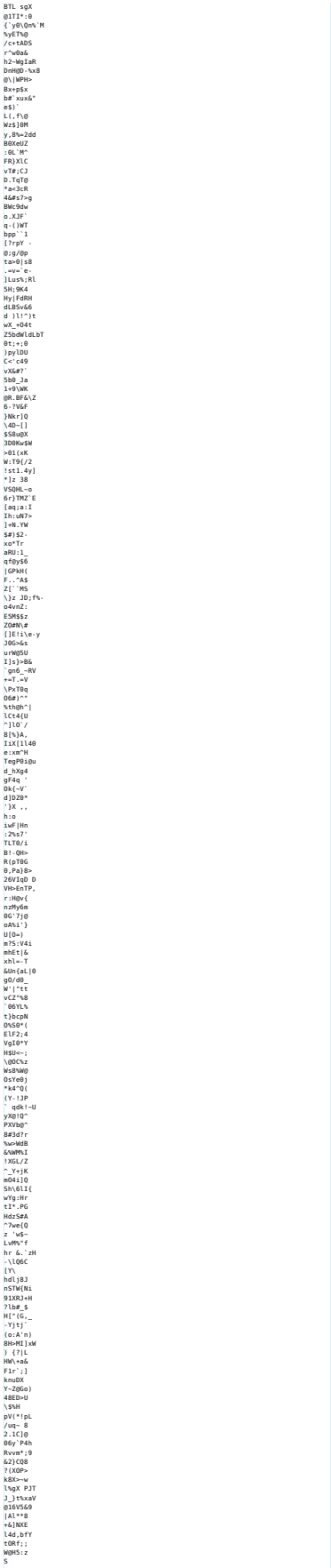


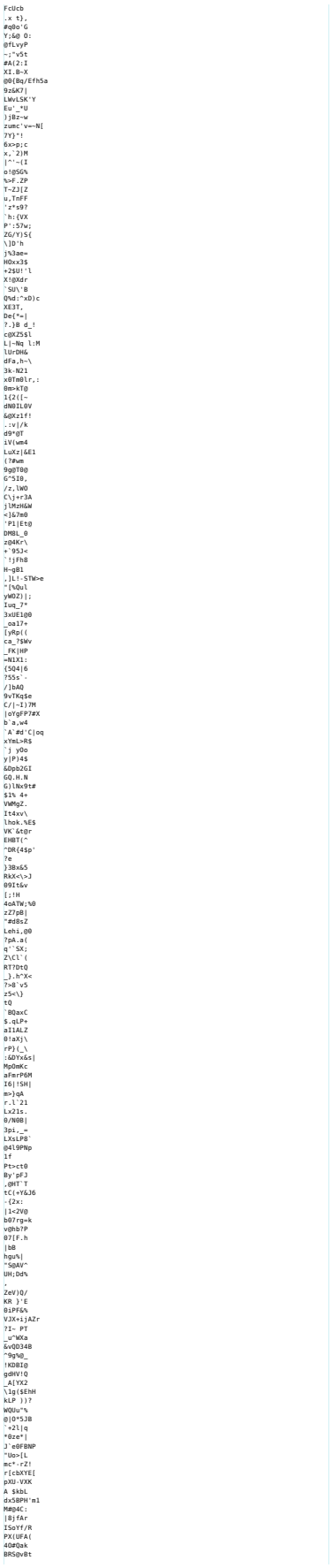


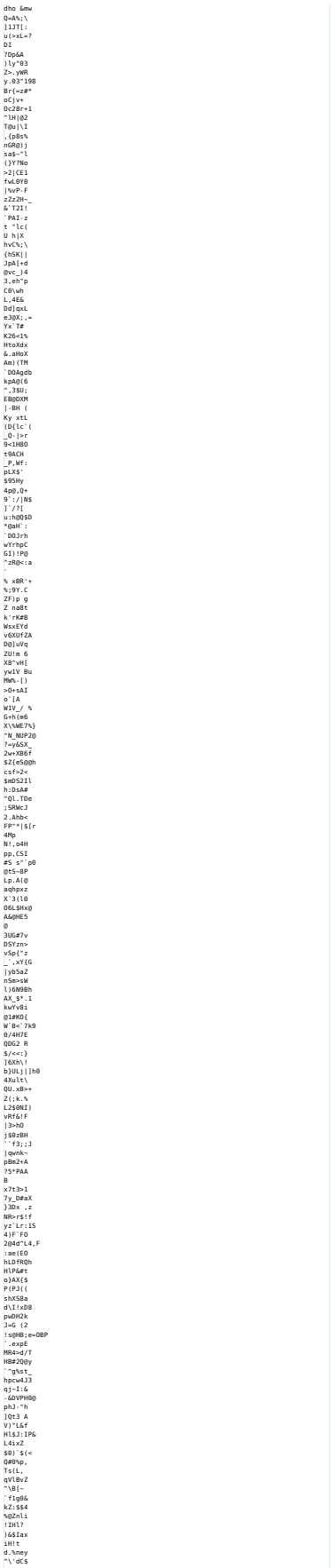


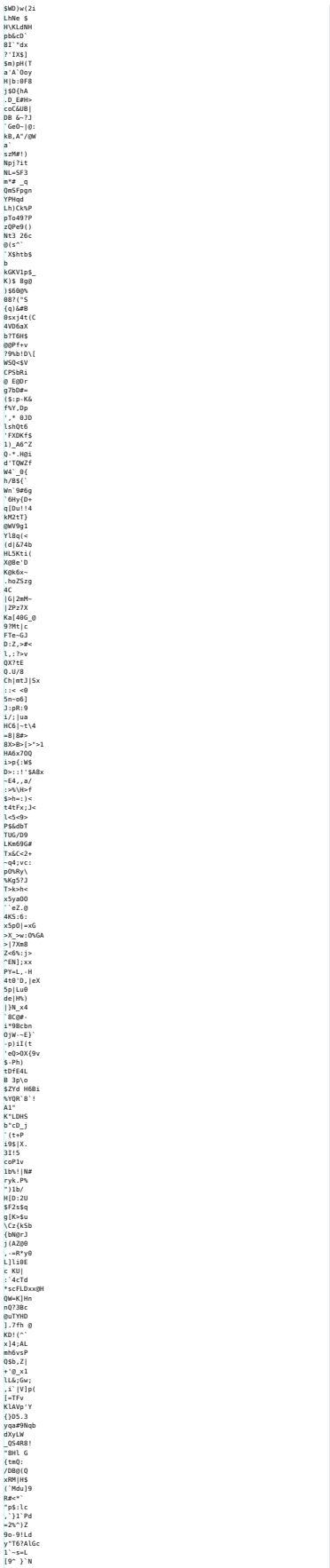


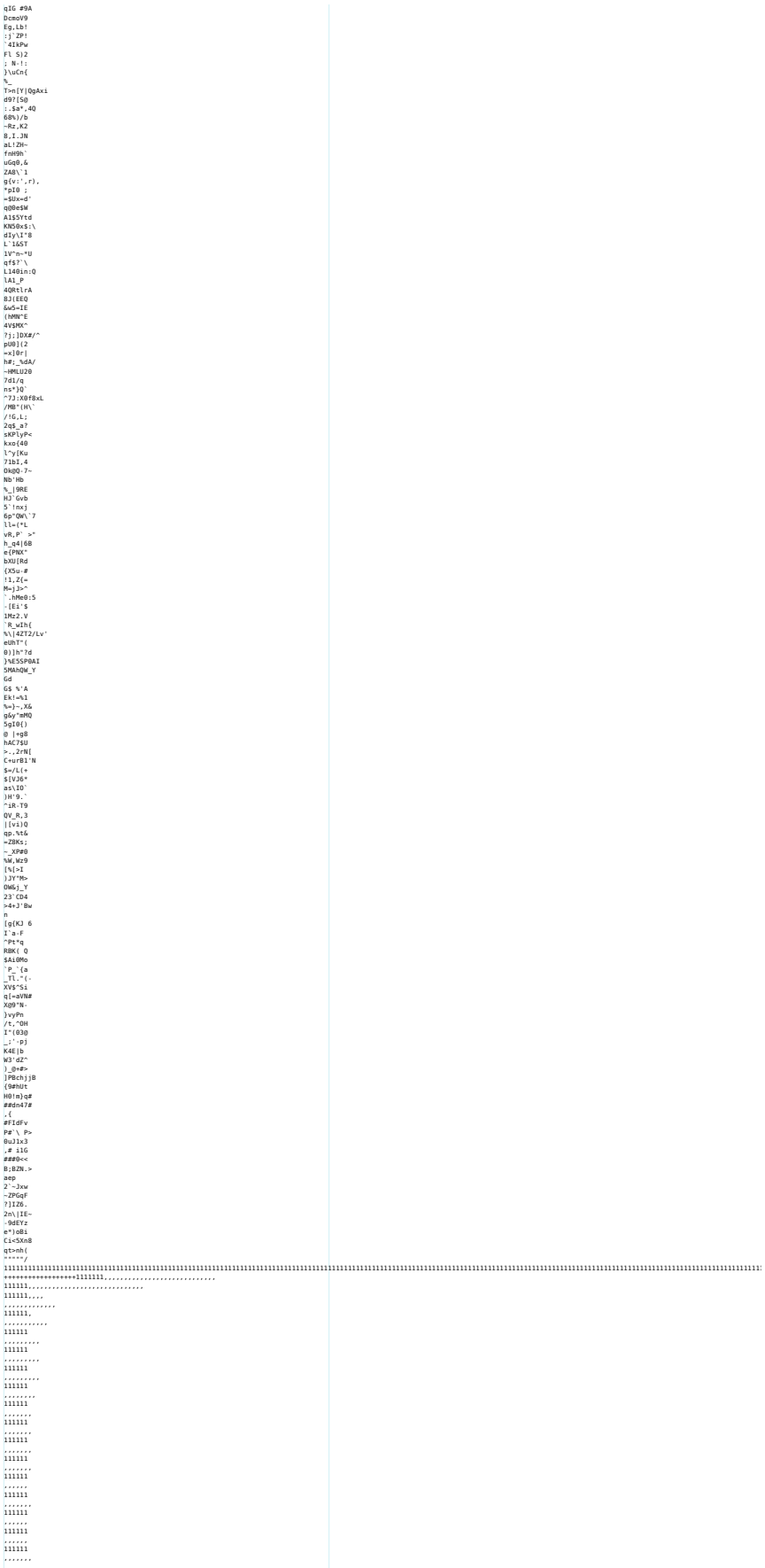












```
111111
,,,,,,
,,,,,,
,,,,,,
,,,,,,
,,,,,,
,,,,,,
,,,,,,
,,,,,,,
,,,,,,
,,,,,,
,,,,,,,
,,,,,,
,,,,,,,
1111111
,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
111111111,,,,,,
,,,,,,,11111111111
1111111111111
111111111111111
11111111111111111
1111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111111
))))))))))))))))))))))))))))))))))))))))))))))))))))))))))))))))))))))))))))))))))))))))))))))))))))
)))))))
)))))))))
)))))))))))
))))))))))))))))))))))))))))))))))))))))))))))))))))))))))))))))))))))))

*&IDATx
0X{|\Y
0RY&y
p!4h'h
E{081X
l%>xz|
HZ~Bq<
@#N{Q4fj
9@"ZaPF
^2?/^
[F5y`">
8}nn{Qs
=z6JX&
\@_Cr"
'%ES|\
'%FS|<}g
`\7?dQh
L*C~(}J
true
\2.0\de
VS_VERSION_INFO
StringFileInfo
040904b0
FileDescription
FileVersion
1.1.24.02
InternalName
LegalCopyright
OriginalFilename
ProductName
ProductVersion
1.1.24.02
VarFileInfo
Translation
```


Dropped Files

Network Analysis

Download PCAP File (/CuckooReport/PcapFile?reportId=5a0aff5017c591044899bc25)

Anomalies

- **unhook LdrLoadDll** Function hook was modified! (pid=2484, process=flashplayer27pp_ka.exe)
- **unhook NtCreateUserProcess** Function hook was modified! (pid=2484, process=flashplayer27pp_ka.exe)
- **unhook ExitProcess** Function hook was modified! (pid=2484, process=flashplayer27pp_ka.exe)
- **unhook GetCursorPos** Function hook was modified! (pid=2484, process=flashplayer27pp_ka.exe)
- **unhook getaddrinfo** Function hook was modified! (pid=2484, process=flashplayer27pp_ka.exe)
- **unhook gethostbyname** Function hook was modified! (pid=2484, process=flashplayer27pp_ka.exe)
- **unhook send** Function hook was modified! (pid=2484, process=flashplayer27pp_ka.exe)
- **unhook closesocket** Function hook was modified! (pid=2484, process=flashplayer27pp_ka.exe)
- **unhook WSASend** Function hook was modified! (pid=2484, process=flashplayer27pp_ka.exe)

Behavior Summary

Files

Read
- C:\Users\W\xc8\xb1n7-32-A9O7\AppData\Roaming\Xywexa\veaf.feh
- C:\Windows\system32\ntdll.dll
- C:\Windows\Fonts\staticcache.dat
- C:\Windows\system32\rsaenh.dll
- C:\Device\KsecDD
- C:\Windows\system32\en-US\MSCTF.dll.mui

Mutexes
- Global\{597DE0D3-1A0D-477B-F787-939FB57D1573}
- Local\{231CC6A1-3C7F-3D1A-F787-939FB57D1573}
- DBWinMutex
- Local\MSCTF.Asm.MutexDefault1
- Local\{0E877469-8EB7-1081-F787-939FB57D1573}

Registry Keys

Read
- HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\ComputerName\ActiveComputerName
- HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Privacy
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\0
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\1
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\2
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\3
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\4
- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\Windows Error Reporting\WMR
- HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Nls\Locale
- HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Nls\Language Groups
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\DataStore_V1.0
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\LanguagePack\SurrogateFallback
- Software\Microsoft\Rpc
- Software\Policies\Microsoft\Windows NT\Rpc
- Software\Microsoft\Windows\CurrentVersion\Explorer\FolderDescriptions
- {1AC14E77-02E7-4E5D-B744-2EB1AE5198B7}
- Software\Microsoft\Windows\CurrentVersion\Explorer\KnownFolderSettings
- {F38BF404-1D43-42F2-9305-67DE0B28FC23}
- SOFTWARE\Microsoft\Cryptography\Defaults\Provider Types\Type 001
- Software\Policies\Microsoft\Cryptography
- Software\Microsoft\Cryptography\Offload
- PropertyBag
- KnownFolders
- Software\Microsoft\Windows\CurrentVersion\Explorer\User Shell Folders
- Software\Wine
- SYSTEM\ControlSet001\Control\Class\{4D36E968-E325-11CE-BFC1-08002BE10318}\0000
- Hardware\description\System
- SOFTWARE\Microsoft\CTF\Compatibility\flashplayer27pp_ka.exe
- Software\Microsoft\CTF\TIP\{0000897b-83df-4b96-be07-0fb58b01c4a4}\LanguageProfile\0x00000000\{0001bea3-ed56-483d-a2e2-aeae25577436}
- SOFTWARE\Microsoft\CTF\TIP\
- {0000897b-83df-4b96-be07-0fb58b01c4a4}\Category\Category\{534C48C1-0607-4098-A521-4FC899C73E90}
- {03B5835F-F03C-411B-9CE2-AA23E1171E36}\Category\Category\{534C48C1-0607-4098-A521-4FC899C73E90}
- {07EB03D6-B001-41DF-9192-BF9B841EE71F}\Category\Category\{534C48C1-0607-4098-A521-4FC899C73E90}
- {3697C5FA-60DD-4B56-92D4-74A569205C16}\Category\Category\{534C48C1-0607-4098-A521-4FC899C73E90}
- {531FDEBF-9B4C-4A43-A2AA-960E8FCDC732}\Category\Category\{534C48C1-0607-4098-A521-4FC899C73E90}
- {70FAF614-E0B1-11D3-8F5C-00C04F9CF4AC}\Category\Category\{534C48C1-0607-4098-A521-4FC899C73E90}
- {81D4E9C9-1D3B-41BC-9E6C-4B40BF79E35E}\Category\Category\{534C48C1-0607-4098-A521-4FC899C73E90}
- {8613E14C-D0C0-4161-AC0F-1DD2563286BC}\Category\Category\{534C48C1-0607-4098-A521-4FC899C73E90}
- {A028AE76-01B1-46C2-99C4-ACD9858AE02F}\Category\Category\{534C48C1-0607-4098-A521-4FC899C73E90}

- {AE6BE008-07FB-400D-8BEB-337A64F7051F}\Category\Category\{534C48C1-0607-4098-A521-4FC899C73E90}
- {C1EED1F2-B3B6-4A6A-9DDD-E988C088EC82}\Category\Category\{534C48C1-0607-4098-A521-4FC899C73E90}
- {DCBD6FA8-032F-11D3-B5B1-00C04FC324A1}\Category\Category\{534C48C1-0607-4098-A521-4FC899C73E90}
- {E429B25A-E5D3-4D1F-9BE3-0C608477E3A1}\Category\Category\{534C48C1-0607-4098-A521-4FC899C73E90}
- {F25E9F57-2FC8-4EB3-A41A-CCE5F08541E6}\Category\Category\{534C48C1-0607-4098-A521-4FC899C73E90}
- {F9E0E5B-8D2F-4D08-9AC2-0F816C09F4EE}\Category\Category\{534C48C1-0607-4098-A521-4FC899C73E90}
- Software\Microsoft\CTF\DirectSwitchHotkeys
- {F1B32785-6FBA-4FCF-9D55-7B8E7F157091}
- SOFTWARE\Microsoft\CTF\KnownClasses

Modify
- HKEY_CURRENT_USER\SOFTWARE\Microsoft\Qyysa

Processes

registry filesystem process services network synchronization

flashplayer27pp_ka.exe PID: 2484, Parent PID: 540

Show 10 entries Search:

Timestamp	Thread	Function	Arguments	Status	Return	Repeated
2015-04-22 20:11:54,137	804	NtOpenDirectoryObject	DirectoryHandle ⇒ 0x0000007c DesiredAccess ⇒ 15 ObjectAttributes ⇒ C:\Sessions\1\BaseNamedObjects	SUCCESS	0x00000000	0
2015-04-22 20:11:54,137	804	LdrLoadDll	Flags ⇒ 7268764 BaseAddress ⇒ 0x76ad0000 FileName ⇒ KERNEL32.dll	SUCCESS	0x00000000	0
2015-04-22 20:11:54,137	804	LdrGetProcedureAddress	Ordinal ⇒ 0 FunctionName ⇒ LoadLibraryA FunctionAddress ⇒ 0x76b22864 ModuleHandle ⇒ 0x76ad0000	SUCCESS	0x00000000	0
2015-04-22 20:11:54,137	804	LdrGetProcedureAddress	Ordinal ⇒ 0 FunctionName ⇒ Process32FirstW FunctionAddress ⇒ 0x76b13097 ModuleHandle ⇒ 0x76ad0000	SUCCESS	0x00000000	0
2015-04-22 20:11:54,137	804	LdrGetProcedureAddress	Ordinal ⇒ 0 FunctionName ⇒ RemoveDirectoryW FunctionAddress ⇒ 0x76b077d7 ModuleHandle ⇒ 0x76ad0000	SUCCESS	0x00000000	0
2015-04-22 20:11:54,137	804	LdrGetProcedureAddress	Ordinal ⇒ 0 FunctionName ⇒ QueryDosDeviceW FunctionAddress ⇒ 0x76b07e6b ModuleHandle ⇒ 0x76ad0000	SUCCESS	0x00000000	0
2015-04-22 20:11:54,137	804	LdrGetProcedureAddress	Ordinal ⇒ 0 FunctionName ⇒ Process32NextW FunctionAddress ⇒ 0x76b13155 ModuleHandle ⇒ 0x76ad0000	SUCCESS	0x00000000	0
2015-04-22 20:11:54,137	804	LdrGetProcedureAddress	Ordinal ⇒ 0 FunctionName ⇒ FindNextFileW FunctionAddress ⇒ 0x76b1cb2d ModuleHandle ⇒ 0x76ad0000	SUCCESS	0x00000000	0
2015-04-22 20:11:54,147	804	LdrGetProcedureAddress	Ordinal ⇒ 0 FunctionName ⇒ VirtualProtect FunctionAddress ⇒ 0x76b150ab ModuleHandle ⇒ 0x76ad0000	SUCCESS	0x00000000	0
2015-04-22 20:11:54,147	804	LdrGetProcedureAddress	Ordinal ⇒ 0 FunctionName ⇒ CreateToolhelp32Snapshot FunctionAddress ⇒ 0x76b12bb1 ModuleHandle ⇒ 0x76ad0000	SUCCESS	0x00000000	0

Previous 1 2 3 4 5 … 207 Next

Volatility