Summary

File Name: 444.exe

File Type: PE32 executable (GUI) Intel 80386, for MS Windows

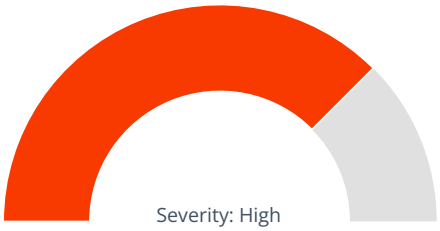
SHA1: de9b08b0b530581d0485bef9dadf032c2120f1ff

MD5: f3e6adde5e52ef7b542520c6882eb3d3

MALWARE

Valkyrie Final Verdict

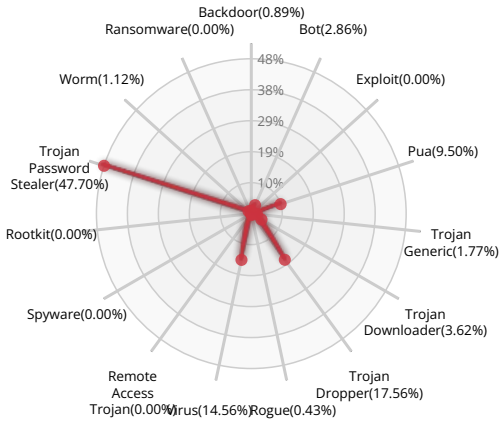
DETECTION SECTION



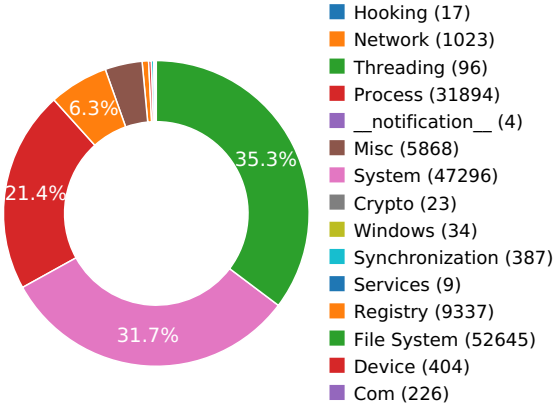
Severity: High

Verdict: Malware

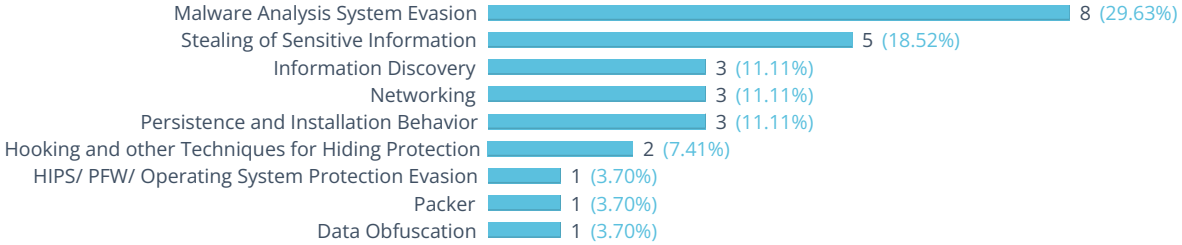
CLASSIFICATION



HIGH LEVEL BEHAVIOR DISTRIBUTION



ACTIVITY OVERVIEW



VALKYRIE COMODO

Activity Details

INFORMATION DISCOVERY

Repeatedly searches for a not-found process, may want to run with startbrowser=1 option	
Reads data out of its own binary image	Show sources
Attempts to remove evidence of file being downloaded from the Internet	Show sources

NETWORKING

Attempts to connect to a dead IP:Port (3 unique times)	Show sources
HTTP traffic contains suspicious features which may be indicative of malware related traffic	Show sources
Performs some HTTP requests	Show sources

HIPS/ PFW/ OPERATING SYSTEM PROTECTION EVASION

Detects Avast Antivirus through the presence of a library	Show sources

PACKER

The binary likely contains encrypted or compressed data.	Show sources

STEALING OF SENSITIVE INFORMATION

Steals private information from local Internet browsers	Show sources
Harvests information related to installed instant messenger clients	Show sources
Collects information about installed applications	Show sources
Harvests credentials from local FTP client softwares	Show sources
Harvests information related to installed mail clients	Show sources

HOOKING AND OTHER TECHNIQUES FOR HIDING PROTECTION

Creates RWX memory	Show sources
Likely virus infection of existing system binary	Show sources

DATA OBFUSCATION

Drops a binary and executes it	Show sources

PERSISTENCE AND INSTALLATION BEHAVIOR

Deletes its original binary from disk	Show sources
Installs itself for autorun at Windows startup	Show sources
Creates a copy of itself	Show sources

MALWARE ANALYSIS SYSTEM EVASION

Possible date expiration check, exits too soon after checking local time	Show sources
A process attempted to delay the analysis task.	Show sources
Detects Sandboxie through the presence of a library	Show sources
Checks the presence of disk drives in the registry, possibly for anti-virtualization	Show sources
Checks the CPU name from registry, possibly for anti-virtualization	Show sources
Tries to unhook or modify Windows functions monitored by Cuckoo	Show sources
Creates or sets a registry key to a long series of bytes, possibly to store a binary or malware config	Show sources
Creates a hidden or system file	Show sources

VALKYRIE COMODO

Behavior Graph

20:46:24 **20:49:11** **20:51:59**

PID 1640

20:46:24 | Create Process | The malicious file created a child process as de9b08b0b530581d0485bef9dadf032c2120f1ff.exe **(PPID 1760)**

- 20:46:24 NtAllocateVirtualMem
- 20:46:24 LdrGetDllHandle
- 20:46:24 RegQueryValueExA

PID 2092

20:46:24 | Create Process | The malicious file created a child process as explorer.exe **(PPID 1636)**

- 20:46:24 NtDelayExecution
- 20:46:25 20:46:41 Process32NextW **[147 times]**
  - 20:46:41 ConnectEx
  - 20:46:41 Process32NextW
  - 20:46:41 DeleteFileW
  - 20:46:41 Process32NextW
  - 20:46:41 DeleteFileW
  - 20:46:41 20:46:41 NtSetInformationFile **[2 times]**
  - 20:46:41 20:46:41 Process32NextW **[5 times]**
  - 20:46:41 RegSetValueExA
  - 20:46:42 20:46:47 Process32NextW **[45 times]**
    - 20:46:47 ConnectEx
    - 20:46:47 Process32NextW
    - 20:46:47 ConnectEx
    - 20:46:47 20:47:05 Process32NextW **[314 times]**
    - 20:46:48 Create Process
      - 20:47:05 ConnectEx
      - 20:47:06 20:47:06 Process32NextW **[6 times]**
      - 20:47:06 CopyFileW
      - 20:47:06 20:47:17 Process32NextW **[204 times]**
        - 20:47:17 ConnectEx
        - 20:47:17 20:47:17 Process32NextW **[4 times]**
        - 20:47:17 ConnectEx
        - 20:47:17 20:47:19 Process32NextW **[28 times]**
        - 20:47:19 NtSetInformationFile

20:47:19 20:47:30 Process32NextW [211 times]
20:47:20 Create Process
20:47:23 Create Process
20:47:27 Create Process
20:47:28 Create Process
20:47:30 Create Process

PID 2252

20:46:51 **Create Process** The malicious file created a child process as 81F2.tmp.exe **(PPID 2092)**

PID 2672

20:47:35 **Create Process** The malicious file created a child process as FDE9.tmp.exe **(PPID 2092)**

20:47:35 NtDelayExecution
20:47:37 RegQueryValueExW
20:47:37 RegSetValueExW
20:47:39 Process32NextW
20:47:44 NtReadFile
20:47:45 Create Process
20:47:57 Create Process
20:48:12 20:49:44 Process32NextW [4 times]
20:48:12 Create Process
20:48:25 Create Process
20:48:45 Create Process
20:49:00 Create Process
20:49:18 Create Process
20:49:29 Create Process
20:50:27 Create Process
20:51:53 Create Process

PID 368

20:47:47 **Create Process** The malicious file created a child process as nslookup.exe **(PPID 2672)**

20:47:58 NtTerminateProcess

PID 1840

20:48:00 **Create Process** The malicious file created a child process as nslookup.exe **(PPID 2672)**

PID 1580

20:48:14 **Create Process** The malicious file created a child process as nslookup.exe **(PPID 2672)**

PID 1148

20:48:25 **Create Process** The malicious file created a child process as nslookup.exe **(PPID 2672)**

PID 2996

20:48:38 | Create Process | The malicious file created a child process as nslookup.exe **(PPID 2672)**

PID 2652

20:48:48 | Create Process | The malicious file created a child process as nslookup.exe **(PPID 2672)**

PID 1628

20:49:03 | Create Process | The malicious file created a child process as nslookup.exe **(PPID 2672)**

PID 2440

20:49:13 | Create Process | The malicious file created a child process as nslookup.exe **(PPID 2672)**

PID 1400

20:51:02 | Create Process | The malicious file created a child process as nslookup.exe **(PPID 2672)**

PID 896

20:51:59 | Create Process | The malicious file created a child process as nslookup.exe **(PPID 2672)**

PID 1888

20:47:45 | Create Process | The malicious file created a child process as 84B.tmp.exe **(PPID 2092)**

20:48:57 | LdrGetDllHandle

20:48:57
20:48:57 | __anomaly__ **[3 times]**

PID 2160

20:47:45 | Create Process | The malicious file created a child process as 1A4D.tmp.exe **(PPID 2092)**

PID 2736

20:47:45 | Create Process | The malicious file created a child process as explorer.exe **(PPID 2092)**

20:47:45
20:47:45 | RegQueryValueExA **[71 times]**

20:47:46 | FindFirstFileExW

20:47:46
20:47:46 | RegOpenKeyExA **[2 times]**

20:47:46
20:47:46 | FindFirstFileExW **[7 times]**

20:48:20
20:48:20 | CopyFileA **[2 times]**

20:48:20 | ConnectEx

PID 2060

20:47:47 | Create Process | The malicious file created a child process as explorer.exe **(PPID 2092)**

PID 872

20:46:45 | Create Process | The malicious file created a child process as svchost.exe **(PPID 460)**

PID 460

20:47:48 | Create Process | The malicious file created a child process as services.exe **(PPID 352)**

20:47:50 Create Process

PID 2140

20:47:50 **Create Process** The malicious file created a child process as lsass.exe **(PPID 460)**

VALKYRIE COMODO

Behavior Summary

ACCESSED FILES

C:\Users\user\AppData\Local\Temp\msvcr100.dll
C:\Windows\System32\msvcr100.dll
C:\Windows\system\msvcr100.dll
C:\Windows\msvcr100.dll
C:\ProgramData\Oracle\Java\javapath\msvcr100.dll
C:\Windows\System32\wbem\msvcr100.dll
C:\Windows\System32\WindowsPowerShell\v1.0\msvcr100.dll
C:\Program Files\Microsoft Network Monitor 3\msvcr100.dll
C:\Program Files (x86)\Universal Extractor\msvcr100.dll
C:\Program Files (x86)\Universal Extractor\bin\msvcr100.dll
C:\Program Files (x86)\Windows Kits\8.1\Windows Performance Toolkit\msvcr100.dll
C:\Python27\msvcr100.dll
C:\Python27\Scripts\msvcr100.dll
C:\tools\sysinternals\msvcr100.dll
C:\tools\msvcr100.dll
C:\tools\IDA_Pro_v6\python\msvcr100.dll
C:\
C:\Windows\Globalization\Sorting\sortdefault.nls
C:\Windows\winhttp.DLL
C:\Windows\sysnative\winhttp.dll
C:\Windows\webio.dll
C:\Windows\sysnative\webio.dll
C:\Users\user\AppData\Roaming\Microsoft\Windows\guujubau
C:\Users\user\AppData\Roaming\Microsoft\Windows\guujubau\cafadrev.exe
C:\Users\user\AppData\Local\Temp\de9b08b0b530581d0485bef9dadf032c2120f1ff.exe
C:\Users\user\AppData\Roaming\Microsoft\Windows\guujubau\cafadrev.exe:Zone.Identifier
C:\Windows\sysnative\advapi32.dll
C:\Windows
C:\Windows\sysnative
C:\Windows\sysnative\cmd.exe
C:\Windows\sysnative\
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\guujubau.lnk

C:\Program Files (x86)\Adobe\Reader 9.0\Reader\AcroRd32.exe
C:\Program Files (x86)\Microsoft Office\Office12\EXCEL.EXE
C:\Program Files (x86)\Microsoft Office\Office12\OUTLOOK.EXE
C:\Program Files (x86)\Microsoft Office\Office12\POWERPNT.EXE
C:\Program Files (x86)\Microsoft Office\Office12\WINWORD.EXE
C:\Program Files (x86)\Microsoft Office\Office12\MSTORE.EXE
C:\Program Files (x86)\Common Files\Microsoft Shared\OFFICE12\OFFDIAG.EXE
C:\Program Files (x86)\Microsoft Office\Office12\OIS.EXE
C:\Python27\pythonw.exe
C:\Python27\python.exe
C:\Users\user\AppData\Roaming\Microsoft\Windows\guujubau\guujubau
C:\Users\user\AppData\Local\Temp
C:\Users\user\AppData\Local\Temp\81F2.tmp
C:\Users\user\AppData\Local\Temp\81F2.tmp.exe
C:\Users\user\AppData\Roaming\Microsoft\Windows\Themes\
C:\Users\user\AppData\Roaming\Microsoft\Windows\Themes\slideshow.ini
C:\Users\user\AppData\Local\Temp\FDE9.tmp
C:\Users\user\AppData\Local\Temp\FDE9.tmp.exe
C:\Users
C:\Users\user
C:\Users\user\AppData
C:\Users\user\AppData\Local
C:\Users\user\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch\User Pinned
C:\Users\desktop.ini
C:\Users\user\AppData\Roaming
C:\Users\user\AppData\Roaming\Microsoft
C:\Users\user\AppData\Roaming\Microsoft\desktop.ini
C:\Users\user\AppData\Roaming\Microsoft\Internet Explorer
C:\Users\user\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch
C:\Users\user\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch\desktop.ini
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu
C:\Users\user\AppData\Roaming\Microsoft\Windows
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\desktop.ini
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\desktop.ini
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs

C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Accessories\Desktop.ini
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Administrative Tools\desktop.ini
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Maintenance\Desktop.ini
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\desktop.ini
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Accessories
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Accessories\Accessibility\Desktop.ini
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Accessories\System Tools\Desktop.ini
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Accessories\Accessibility
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Accessories\System Tools

READ REGISTRY KEYS

HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\Disk\Enum\0
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CustomLocale\en-US
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\ExtendedLocale\en-US
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{7007ACC7-3202-11D1-AAD2-00805FC1270E}\InProcServer32\(Default)
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{7007ACC7-3202-11D1-AAD2-00805FC1270E}\InProcServer32\LoadWithoutCOM
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{21EC2020-3AEA-1069-A2DD-08002B30309D}\SortOrderIndex
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{7007ACC7-3202-11D1-AAD2-00805FC1270E}\SortOrderIndex
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\svcVersion
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Version
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\0a-00-27-00-00-00\WpadDecision
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\0a-00-27-00-00-00\WpadDecisionTime
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\WpadExpirationDays
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Drive\shellex\FolderExtensions\{fbeb8a05-beee-4442-804e-409d6c4515e9}\DriveMask
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\StartPage\FavoritesRemovedChanges
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\StartPage2\FavoritesRemovedChanges
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\StartPage2\FavoritesChanges
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\Start_MinMFU
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Taskband\FavoritesRemovedChanges
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Taskband\FavoritesChanges
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\Start_TrackProgs
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Installer\Features\68AB67CA7DA73301B7449A0500000010\ReaderProgramFiles
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\68AB67CA7DA73301B7449A0500000010\Features\ReaderProgramFiles
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Components\721B0771CE7953B41B4784D92724CFAA\68AB67CA7DA73301B7449A0500000010

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Components\1DE7F110AFAA90C49809BCC45C22CCB7\68AB67CA7DA73301B7449A0500000010

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Components\206097A43463626498893D00E537F7D2\68AB67CA7DA73301B7449A0500000010

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Components\321519DC6CD473D47B9CB9A3D015BEA9\68AB67CA7DA73301B7449A0500000010

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Components\13A35F6AE60C2BF459F0E63FD5559FC4\68AB67CA7DA73301B7449A0500000010

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Components\AD71E371BC38E864F82DB6404D2BF408\68AB67CA7DA73301B7449A0500000010

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Components\310F03195485741439F307764C3E7D7A\68AB67CA7DA73301B7449A0500000010

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Components\81440F9466EA0E0479107C5D0A3956FC\68AB67CA7DA73301B7449A0500000010

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Components\3FA23BFB0DE8BDD4BA12A04347309859\68AB67CA7DA73301B7449A0500000010

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Components\D37F9C8794107AE4EB7242C863E97348\68AB67CA7DA73301B7449A0500000010

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Components\50998A8DA27A69B4D9116E985BAA8021\68AB67CA7DA73301B7449A0500000010

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Components\D7FF3275FE30C1F47B84DE2F326E15FB\68AB67CA7DA73301B7449A0500000010

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Components\1588992C469F2174F8431F888FBBDF73\68AB67CA7DA73301B7449A0500000010

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Components\422B819BB22CE78499BB4A3C5FC7727F\68AB67CA7DA73301B7449A0500000010

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Components\D6D5120B2BE8BE64EB95103A52283D2E\68AB67CA7DA73301B7449A0500000010

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Components\9C57278595DD8FA4A88153B1180C4A27\68AB67CA7DA73301B7449A0500000010

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Components\8E09EA1AB2886074F9576B7C0658EEF7\68AB67CA7DA73301B7449A0500000010

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Components\E3A377A9AA6AD014AB28757CDAD646AA\68AB67CA7DA73301B7449A0500000010

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Components\49CED8721D0CF6841B27BB5ECC02FDED\68AB67CA7DA73301B7449A0500000010

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Components\1AE339F0568D45C489F213DC56E50B66\68AB67CA7DA73301B7449A0500000010

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Components\3BAEA108B4F648940BB38C607D5B66E6\68AB67CA7DA73301B7449A0500000010

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Components\3F65A1E87DCF61D499D7190C1E8C8987\68AB67CA7DA73301B7449A0500000010

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Components\F1BC8F95270E2264A94F91ABF943EF71\68AB67CA7DA73301B7449A0500000010

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Components\4092152B411BF7B4EB862533C938D699\68AB67CA7DA73301B7449A0500000010

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Components\36AF20128E89D6F4A920F2A4636AC354\68AB67CA7DA73301B7449A0500000010

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Components\FE8D5430B37D66D4998D88A8CEC87799\68AB67CA7DA73301B7449A0500000010
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Components\8F1AE0C9111C4CA4186FF4C932C8AB0E\68AB67CA7DA73301B7449A0500000010
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Components\E3FC65AB64CE51E4A99DF582E4B1CEAB\68AB67CA7DA73301B7449A0500000010
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Components\9579C59FFA3114E44AB6BD2D1806D835\68AB67CA7DA73301B7449A0500000010
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Components\CC275594575BF0943AAEA81F6079425E\68AB67CA7DA73301B7449A0500000010
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Components\22F4DAC0B3D560C48B6ED1CFE16DED9D\68AB67CA7DA73301B7449A0500000010
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Components\438256CEC1FA32847B45768EE56D453C\68AB67CA7DA73301B7449A0500000010
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Components\F4397F6D435ECA24D81D699D63B6F39D\68AB67CA7DA73301B7449A0500000010
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Components\BFBC5C8C7FF632D43BEFE50028D06EFA\68AB67CA7DA73301B7449A0500000010
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Components\7FC201AD0BD12A34286188A3F8DA6C36\68AB67CA7DA73301B7449A0500000010
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Components\337ABE535D078D14099C57A239EF250D\68AB67CA7DA73301B7449A0500000010
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Components\B31492ABDE5EA584CA42E924A1EDC230\68AB67CA7DA73301B7449A0500000010
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Components\7A11E946102B22241B413AE2EEBAB671\68AB67CA7DA73301B7449A0500000010
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Components\101E81DEBEAC18543939D4B1989AFB7C\68AB67CA7DA73301B7449A0500000010
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Components\1963DDD4CC5F2CA4FB3CDBEEDA7D2D59\68AB67CA7DA73301B7449A0500000010
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Components\6B575167E61A6914E9C9B25DD8368F48\68AB67CA7DA73301B7449A0500000010
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Components\C3C19C1FA44616F44BB254F47F629665\68AB67CA7DA73301B7449A0500000010
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Components\47F704F177BAC3741AAF03FF2B4BA243\68AB67CA7DA73301B7449A0500000010
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Components\5B8A5F9BB528C8A41BAFB0CD822BF716\68AB67CA7DA73301B7449A0500000010
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Components\C5D9CDEE220C9F046A62F346C343C567\68AB67CA7DA73301B7449A0500000010
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Components\4F25A90420A18F145BD771D4A9C7AD52\68AB67CA7DA73301B7449A0500000010
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Components\57428418D0241C94990E116C72A6C439\68AB67CA7DA73301B7449A0500000010
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Components\378FC2EF63F82AB44BC07C8B6423ECB7\68AB67CA7DA73301B7449A0500000010
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-

18\Components\4210D39FE9C0D214DA66C66F9C686753\68AB67CA7DA73301B7449A0500000010
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Components\F5678751A1B3F6540861D057FDB0044D\68AB67CA7DA73301B7449A0500000010
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Components\4BBDDEE59EF5395479E0F98DF8FE7B4E\68AB67CA7DA73301B7449A0500000010
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Components\5D0E502A00E4341458F9CDBC6F0EE22E\68AB67CA7DA73301B7449A0500000010
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Components\CD0486F25396A2043A5E8974CB56A7BD\68AB67CA7DA73301B7449A0500000010
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Components\C1C4C10236F37B6468D9370E57370193\68AB67CA7DA73301B7449A0500000010

MODIFIED FILES

C:\Users\user\AppData\Roaming\Microsoft\Windows\guujubau\cafadrev.exe
C:\Users\user\AppData\Roaming\Microsoft\Windows\guujubau
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\guujubau.lnk
C:\Users\user\AppData\Local\Temp\81F2.tmp.exe
C:\Users\user\AppData\Roaming\Microsoft\Windows\guujubau\guujubau
C:\Users\user\AppData\Local\Temp\FDE9.tmp.exe
C:\Users\user\AppData\Local\Temp\84B.tmp.exe
C:\Users\user\AppData\Local\Temp\1A4D.tmp.exe
C:\Windows\sysnative\Tasks\Opera scheduled Autoupdate 4086469641
\??\PIPE\srvsvc
\Device\LanmanDatagramReceiver
C:\Windows\appcompat\Programs\RecentFileCache.bcf
\Device\Ndis
C:\Windows\SoftwareDistribution\DataStore\DataStore.edb
C:\Windows\SoftwareDistribution\DataStore\Logs\edb.chk
C:\Users\user\AppData\Roaming\Microsoft\cdchcp.exe
\Device\NamedPipe
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\index.dat
C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\index.dat
C:\Users\user\AppData\Local\Microsoft\Windows\History\History.IE5\index.dat
C:\Users\user\AppData\Local\Temp\A92C.tmp
C:\Users\user\AppData\Local\Temp\AA08.tmp
C:\Users\user\AppData\Local\Temp\}\x07

RESOLVED APIS

kernel32.dll.FlsAlloc

kernel32.dll.FlsGetValue
kernel32.dll.FlsSetValue
kernel32.dll.FlsFree
kernel32.dll.LoadLibraryA
kernel32.dll.VirtualAlloc
kernel32.dll.VirtualProtect
kernel32.dll.VirtualFree
kernel32.dll.GetVersionExA
kernel32.dll.TerminateProcess
kernel32.dll.SortGetHandle
kernel32.dll.SortCloseHandle
kernel32.dll.CloseHandle
user32.dll.SetPropA
ntdll.dll.RtlExitUserThread
ole32.dll.CoInitializeEx
advapi32.dll.RegDeleteTreeA
advapi32.dll.RegDeleteTreeW
ole32.dll.CoTaskMemAlloc
ole32.dll.StringFromIID
nsi.dll.NsiAllocateAndGetTable
cfgmgr32.dll.CM_Open_Class_Key_ExW
iphlpapi.dll.ConvertInterfaceGuidToLuid
iphlpapi.dll.GetIfEntry2
iphlpapi.dll.GetIpForwardTable2
iphlpapi.dll.GetIpNetEntry2
iphlpapi.dll.FreeMibTable
ole32.dll.CoTaskMemFree
nsi.dll.NsiFreeTable
ole32.dll.CoUninitialize
shlwapi.dll.StrCmpNW
ws2_32.dll.GetAddrInfoW
ws2_32.dll.WSASocketW
ws2_32.dll.#2
ws2_32.dll.#21

ws2_32.dll.#9
ws2_32.dll.WSAIoctl
ws2_32.dll.FreeAddrInfoW
ws2_32.dll.#6
ws2_32.dll.#5
ws2_32.dll.WSARecv
ws2_32.dll.WSASend
cryptsp.dll.CryptHashData
cryptsp.dll.CryptGetHashParam
cryptsp.dll.CryptDestroyHash
cryptsp.dll.CryptReleaseContext
linkinfo.dll.CreateLinkInfoW
user32.dll.IsCharAlphaW
user32.dll.CharPrevW
ntshrui.dll.GetNetResourceFromLocalPathW
shlwapi.dll.PathRemoveFileSpecW
linkinfo.dll.DestroyLinkInfo
sspicli.dll.GetUserNameExW
xmllite.dll.CreateXmlWriter
xmllite.dll.CreateXmlWriterOutputWithEncodingName
kernel32.dll.CreateThread
ntdll.dll.EtwUnregisterTraceGuids
ws2_32.dll.#22
ws2_32.dll.#3
cryptsp.dll.CryptCreateHash
oleaut32.dll.#9
mmcss.dll.ServiceMain
kernel32.dll.GetCurrentProcess
kernel32.dll.WaitForSingleObject
kernel32.dll.OpenProcess
kernel32.dll.Sleep
kernel32.dll.GetModuleFileNameW
kernel32.dll.CreateFileW
kernel32.dll.ExitThread
kernel32.dll.GetLastError

kernel32.dll.GetProcAddress
kernel32.dll.ExitProcess
kernel32.dll.GetModuleHandleA
kernel32.dll.GetCurrentProcessId
kernel32.dll.GetVersionExW
kernel32.dll.lstrlenW

DELETED FILES

C:\Users\user\AppData\Roaming\Microsoft\Windows\guujubau\cafadrev.exe
C:\Users\user\AppData\Local\Temp\de9b08b0b530581d0485bef9dadf032c2120f1ff.exe
C:\Users\user\AppData\Roaming\Microsoft\Windows\guujubau\cafadrev.exe:Zone.Identifier
C:\Users\user\AppData\Local\Temp\81F2.tmp
C:\Users\user\AppData\Local\Temp\81F2.tmp.exe
C:\Users\user\AppData\Roaming\Microsoft\Windows\guujubau\guujubau
C:\Users\user\AppData\Local\Temp\FDE9.tmp
C:\Users\user\AppData\Local\Temp\84B.tmp
C:\Users\user\AppData\Local\Temp\1A4D.tmp
C:\Windows\Tasks\Opera scheduled Autoupdate 4086469641.job
C:\Windows\sysnative\Tasks\Opera scheduled Autoupdate 4086469641
C:\Users\user\AppData\Local\Temp\A92C.tmp
C:\Users\user\AppData\Local\Temp\AA08.tmp

DELETED REGISTRY KEYS

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\CompatibilityAdapter\Signatures\Opera scheduled Autoupdate 4086469641.job
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\CompatibilityAdapter\Signatures\Opera scheduled Autoupdate 4086469641.job.fp

REGISTRY KEYS

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Disk\Enum
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\Disk\Enum\0
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Nls\CustomLocale
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\CustomLocale\en-US
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Nls\ExtendedLocale
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\Nls\ExtendedLocale\en-US
HKEY_CLASSES_ROOT\CLSID\{7007ACC7-3202-11D1-AAD2-00805FC1270E}\InProcServer32
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{7007ACC7-3202-11D1-AAD2-00805FC1270E}\InProcServer32\(Default)

HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{7007ACC7-3202-11D1-AAD2-00805FC1270E}\InProcServer32\LoadWithoutCOM
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\ShellCompatibility\Objects\{7007ACC7-3202-11D1-AAD2-00805FC1270E}
HKEY_CLASSES_ROOT\CLSID\{21EC2020-3AEA-1069-A2DD-08002B30309D}
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{21EC2020-3AEA-1069-A2DD-08002B30309D}\SortOrderIndex
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Explorer\Desktop\NameSpace\{21EC2020-3AEA-1069-A2DD-08002B30309D}
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Desktop\NameSpace\{21EC2020-3AEA-1069-A2DD-08002B30309D}
HKEY_CLASSES_ROOT\CLSID\{7007ACC7-3202-11D1-AAD2-00805FC1270E}
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{7007ACC7-3202-11D1-AAD2-00805FC1270E}\SortOrderIndex
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Explorer\ControlPanel\NameSpace\{7007ACC7-3202-11D1-AAD2-00805FC1270E}
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\ControlPanel\NameSpace\{7007ACC7-3202-11D1-AAD2-00805FC1270E}
HKEY_LOCAL_MACHINE\Software\Microsoft\Internet Explorer
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\svcVersion
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer\Version
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Class\{4d36e972-e325-11ce-bfc1-08002be10318}
HKEY_CURRENT_USER\Software\Microsoft\windows\CurrentVersion\Internet Settings\Wpad
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\0a-00-27-00-00-00
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\0a-00-27-00-00-00\WpadDecision
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\0a-00-27-00-00-00\WpadDecisionTime
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Wpad\WpadExpirationDays
HKEY_CLASSES_ROOT\Drive\shellex\FolderExtensions
HKEY_CLASSES_ROOT\Drive\shellex\FolderExtensions\{fbeb8a05-beee-4442-804e-409d6c4515e9}
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Drive\shellex\FolderExtensions\{fbeb8a05-beee-4442-804e-409d6c4515e9}\DriveMask
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\StartPage
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\StartPage\FavoritesRemovedChanges
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\StartPage2
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\StartPage2\FavoritesRemovedChanges
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\StartPage2\FavoritesChanges
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Advanced
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\Start_MinMFU
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Taskband
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Taskband\FavoritesRemovedChanges
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Taskband\FavoritesChanges
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\Start_TrackProgs
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\StartPage2\ProgramsCache
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\Managed\S-1-5-21-2298303332-66077612-2598613238-

1000\Installer\Features\68AB67CA7DA73301B7449A0500000010
HKEY_USERS\S-1-5-21-2298303332-66077612-2598613238-1000\Software\Microsoft\Installer\Features\68AB67CA7DA73301B7449A0500000010
HKEY_LOCAL_MACHINE\Software\Classes\Installer\Features\68AB67CA7DA73301B7449A0500000010
HKEY_LOCAL_MACHINE\SOFTWARE\Classes\Installer\Features\68AB67CA7DA73301B7449A0500000010\ReaderProgramFiles
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\68AB67CA7DA73301B7449A0500000010\Features
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\68AB67CA7DA73301B7449A0500000010\Features\ReaderProgramFiles
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Components\721B0771CE7953B41B4784D92724CFAA
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Components\721B0771CE7953B41B4784D92724CFAA\68AB67CA7DA73301B7449A0500000010
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Components\1DE7F110AFAA90C49809BCC45C22CCB7
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Components\1DE7F110AFAA90C49809BCC45C22CCB7\68AB67CA7DA73301B7449A0500000010
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Components\206097A43463626498893D00E537F7D2
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Components\206097A43463626498893D00E537F7D2\68AB67CA7DA73301B7449A0500000010
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Components\321519DC6CD473D47B9CB9A3D015BEA9
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Components\321519DC6CD473D47B9CB9A3D015BEA9\68AB67CA7DA73301B7449A0500000010
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Components\13A35F6AE60C2BF459F0E63FD5559FC4
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Components\13A35F6AE60C2BF459F0E63FD5559FC4\68AB67CA7DA73301B7449A0500000010
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Components\AD71E371BC38E864F82DB6404D2BF408
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Components\AD71E371BC38E864F82DB6404D2BF408\68AB67CA7DA73301B7449A0500000010
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Components\310F03195485741439F307764C3E7D7A
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Components\310F03195485741439F307764C3E7D7A\68AB67CA7DA73301B7449A0500000010
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Components\81440F9466EA0E0479107C5D0A3956FC
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Components\81440F9466EA0E0479107C5D0A3956FC\68AB67CA7DA73301B7449A0500000010
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Components\3FA23BFB0DE8BDD4BA12A04347309859
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Components\3FA23BFB0DE8BDD4BA12A04347309859\68AB67CA7DA73301B7449A0500000010
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Components\D37F9C8794107AE4EB7242C863E97348
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Components\D37F9C8794107AE4EB7242C863E97348\68AB67CA7DA73301B7449A0500000010
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Components\50998A8DA27A69B4D9116E985BAA8021
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Components\50998A8DA27A69B4D9116E985BAA8021\68AB67CA7DA73301B7449A0500000010
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Components\D7FF3275FE30C1F47B84DE2F326E15FB

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Components\D7FF3275FE30C1F47B84DE2F326E15FB\68AB67CA7DA73301B7449A0500000010
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Components\1588992C469F2174F8431F888FBBDF73
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Components\1588992C469F2174F8431F888FBBDF73\68AB67CA7DA73301B7449A0500000010
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Components\422B819BB22CE78499BB4A3C5FC7727F
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Components\422B819BB22CE78499BB4A3C5FC7727F\68AB67CA7DA73301B7449A0500000010

EXECUTED COMMANDS

C:\Users\user\AppData\Local\Temp\81F2.tmp.exe
C:\Users\user\AppData\Local\Temp\FDE9.tmp.exe
C:\Users\user\AppData\Local\Temp\84B.tmp.exe
C:\Users\user\AppData\Local\Temp\1A4D.tmp.exe
C:\Windows\SysWOW64\explorer.exe
nslookup carder.bit ns1.wowservers.ru
nslookup ransomware.bit ns2.wowservers.ru
C:\Windows\system32\lsass.exe

READ FILES

C:\Windows\Globalization\Sorting\sortdefault.nls
C:\Windows\sysnative\winhttp.dll
C:\Windows\sysnative\webio.dll
C:\Users\user\AppData\Local\Temp\de9b08b0b530581d0485bef9dadf032c2120f1ff.exe
C:\Users\user\AppData\Roaming\Microsoft\Windows\guujubau\cafadrev.exe
C:\Users\user\AppData\Roaming\Microsoft\Windows\guujubau
C:\
C:\Windows
C:\Windows\sysnative
C:\Windows\sysnative\cmd.exe
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\guujubau.lnk
C:\Users\user\AppData\Roaming\Microsoft\Windows\guujubau\guujubau
C:\Users\user\AppData\Local\Temp\81F2.tmp
C:\Users\user\AppData\Local\Temp\81F2.tmp.exe
C:\Users\user\AppData\Roaming\Microsoft\Windows\Themes\slideshow.ini
C:\Users\user\AppData\Local\Temp\FDE9.tmp
C:\Users\desktop.ini

C:\Users
C:\Users\user
C:\Users\user\AppData
C:\Users\user\AppData\Roaming
C:\Users\user\AppData\Roaming\Microsoft\desktop.ini
C:\Users\user\AppData\Roaming\Microsoft
C:\Users\user\AppData\Roaming\Microsoft\Internet Explorer
C:\Users\user\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch\desktop.ini
C:\Users\user\AppData\Roaming\Microsoft\Internet Explorer\Quick Launch
C:\Users\user\AppData\Roaming\Microsoft\Windows
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\desktop.ini
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\desktop.ini
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Accessories\Desktop.ini
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Administrative Tools\desktop.ini
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Maintenance\Desktop.ini
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\desktop.ini
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Accessories
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Accessories\Accessibility\Desktop.ini
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Accessories\System Tools\Desktop.ini
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Accessories\Accessibility
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Accessories\System Tools
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Administrative Tools
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\JetBrains
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Maintenance
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Oracle VM VirtualBox Guest Additions
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Total Commander
C:\ProgramData
C:\ProgramData\Microsoft\desktop.ini
C:\ProgramData\Microsoft
C:\ProgramData\Microsoft\Windows
C:\ProgramData\Microsoft\Windows\Start Menu\desktop.ini
C:\Users\user\Desktop\desktop.ini

C:\Users\Public\desktop.ini
C:\Users\Public
C:\Users\Public\Desktop\desktop.ini
C:\Users\user\AppData\Local\Temp\fde9.tmp.exe
C:\Users\user\AppData\Local\Temp\84B.tmp
C:\Users\user\AppData\Local\Temp\1A4D.tmp
C:\Windows\sysnative\Tasks\Opera scheduled Autoupdate 4086469641
\??\PIPE\srvsvc
\Device\LanmanDatagramReceiver
C:\Windows\SysWOW64\nslookup.exe
C:\Windows\appcompat\Programs\RecentFileCache.bcf
C:\Windows\AppPatch\sysmain.sdb
C:\Windows\SysWOW64\
C:\Windows\SysWOW64\en-US\nslookup.exe.mui
C:\Windows\SysWOW64\sc.exe
C:\Windows\SysWOW64\en-US\sc.exe.mui
\Device\Ndis
C:\Windows\SoftwareDistribution\DataStore\DataStore.edb
C:\Windows\SoftwareDistribution\DataStore\Logs\edb.chk
\Device\KsecDD
C:\Users\user\AppData\Local\Temp\FDE9.tmp.exe
\Device\NamedPipe\
C:\Users\user\AppData\Local\Temp\1A4D.tmp.exe.2.Manifest
C:\Users\user\AppData\Local\Temp\1A4D.tmp.exe.3.Manifest

MUTEXES

6DD9D10DB17609386646BC0690600DBA20503A4E
CicLoadWinStaWinSta0
Local\MSCTF.CtfMonitorInstMutexDefault1
Global\pc_group=WORKGROUP&ransom_id=e9d7e6f420503a4e
IESQMMUTEX_0_208
Local_!MSFTHISTORY!_
Local\c:!users!user!appdata!local!microsoft!windows!temporary internet files!content.ie5!
Local\c:!users!user!appdata!roaming!microsoft!windows!cookies!
Local\c:!users!user!appdata!local!microsoft!windows!history!history.ie5!

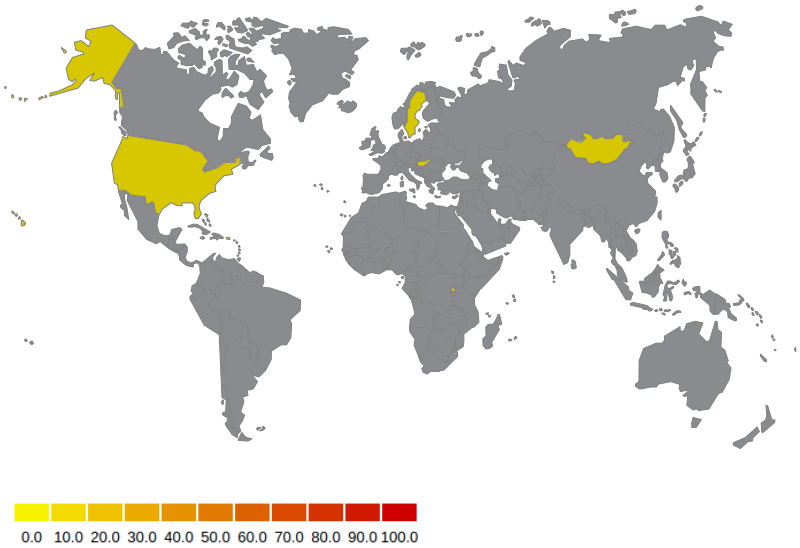
ServiceEntryPointThread
DBWinMutex

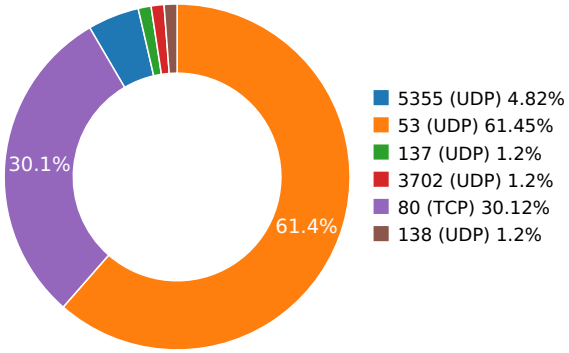
MODIFIED REGISTRY KEYS

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\StartPage2\ProgramsCache
HKEY_CURRENT_USER\Software\Classes\Local Settings\MuiCache\6D\52C64B7E\LanguageList
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks\{C29841B8-99E9-42EF-8583-2DEE3FC71B70}\Path
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks\{C29841B8-99E9-42EF-8583-2DEE3FC71B70}\Hash
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tree\Opera scheduled Autoupdate 4086469641\Id
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tree\Opera scheduled Autoupdate 4086469641\Index
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks\{C29841B8-99E9-42EF-8583-2DEE3FC71B70}\Triggers
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks\{C29841B8-99E9-42EF-8583-2DEE3FC71B70}\DynamicInfo
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks\{7040EF52-A762-44C3-AFAF-F4E795AF4494}\Path
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks\{7040EF52-A762-44C3-AFAF-F4E795AF4494}\Hash
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks\{7040EF52-A762-44C3-AFAF-F4E795AF4494}\Triggers
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache\Tasks\{7040EF52-A762-44C3-AFAF-F4E795AF4494}\DynamicInfo
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\RunOnce\jdlcverlkps
HKEY_USERS\.DEFAULT\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\Connections\DefaultConnectionSettings
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\services\MMCSS\Type

Network Behavior

CONTACTED IPS	NETWORK PORT DISTRIBUTION





Name	IP	Country	ASN	ASN Name	Trigger Process Type
	8.8.4.4	United States	15169	Level 3 Parent, LLC	Malware Process
	202.21.117.236	Mongolia	9484	MobiNet-Customer-134	Malware Process
ipv4bot.whatismyipaddress.com	66.171.248.178	United States	7296	CGP HOLDINGS, INC.	Malware Process
ns1.wowservers.ru	94.249.60.127	Jordan	8376		Malware Process
www.msftncsi.com	23.215.130.146	United States	20940	Akamai Technologies, Inc.	Malware Process
ns2.wowservers.ru	89.203.10.56	Kuwait	21050		Malware Process
dafuritynuu.top	199.127.99.213	United States	54444	Avesta Networks LLC	Malware Process
tgrftrinituy.top	207.250.29.221	United States	3549	tw telecom holdings, inc.	Malware Process

HTTP PACKETS

Host	Port	Method	Version	User Agent	Count	Call Time During Execution(Sec)
www.msftncsi.com	80	GET	1.1	Mozilla/4.0 (compatible; MSIE...	2	22.6502759457
Path: /ncsi.txt **URI:** http://www.msftncsi.com/ncsi.txt						
tgrftrinituy.top	80	POST	1.1	Mozilla/4.0 (compatible; MSIE...	2	28.6531329155
Path: / **URI:** http://tgrftrinituy.top/						
dafuritynuu.top	80	POST	1.1	Mozilla/4.0 (compatible; MSIE...	11	28.8629360199
Path: / **URI:** http://dafuritynuu.top/						
carder.bit	80	GET	1.1	Mozilla/5.0 (Windows NT 6.1;...	5	71.2943029404
Path: / **URI:** http://carder.bit/						
carder.bit	80	POST	1.1	Mozilla/5.0 (Windows NT 6.1;...	1	88.6294920444
Path: /deea?ui=uiloere **URI:** http://carder.bit/deea?ui=uiloere						
dafuritynuu.top	80	POST	1.1	Mozilla/4.0 (compatible; MSIE...	1	106.453999043
Path: / **URI:** http://dafuritynuu.top/						
carder.bit	80	POST	1.1	Mozilla/5.0 (Windows NT 6.1;...	1	119.747119904
Path: /owseess?geuipl=ageow&deerss=gh **URI:** http://carder.bit/owseess?geuipl=ageow&deerss=gh						
carder.bit	80	POST	1.1	Mozilla/5.0 (Windows NT 6.1;...	1	150.867041111
Path: /eyssay?eefay=aupler&ore=za **URI:** http://carder.bit/eyssay?eefay=aupler&ore=za						
carder.bit	80	POST	1.1	Mozilla/5.0 (Windows NT 6.1;...	1	180.373132944
Path: /eeza **URI:** http://carder.bit/eeza						

DNS QUERIES

Request	Type
www.msftncsi.com	A
Answers - a1961.g2.akamai.net (CNAME) - 23.215.130.146 (A) - www.msftncsi.com.edgesuite.net (CNAME) - 23.215.130.179 (A)	
tgrftrinituy.top	A
Answers - 207.250.29.221 (A)	
dafuritynuu.top	A
Answers - 199.127.99.213 (A)	
ipv4bot.whatismyipaddress.com	A
Answers - 66.171.248.178 (A)	
ns1.wowservers.ru	A
Answers - 89.203.10.56 (A) - 94.249.60.127 (A)	
56.10.203.89.in-addr.arpa	PTR
carder.bit	A
carder.bit	AAAA
ns2.wowservers.ru	A
127.60.249.94.in-addr.arpa	PTR
ransomware.bit	A
Answers - 86.126.136.160 (A) - 178.169.217.56 (A) - 84.54.187.24 (A) - 84.217.4.106 (A) - 41.74.170.134 (A) - 202.21.117.236 (A) - 86.127.155.117 (A) - 91.104.123.141 (A) - 109.199.157.158 (A) - 91.83.171.131 (A)	
ransomware.bit	AAAA

TCP PACKETS

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
22.6502759457	Sandbox	23.215.130.146	80
28.6531329155	Sandbox	207.250.29.221	80
28.8629360199	Sandbox	199.127.99.213	80
47.0616619587	Sandbox	23.215.130.146	80
59.1111319065	Sandbox	207.250.29.221	80
59.3431239128	Sandbox	199.127.99.213	80
71.2943029404	Sandbox	66.171.248.178	80
88.6294920444	Sandbox	84.217.4.106	80
99.5697569847	Sandbox	66.171.248.178	80
106.453999043	Sandbox	199.127.99.213	80
119.747119904	Sandbox	41.74.170.134	80
131.142800093	Sandbox	66.171.248.178	80
150.867041111	Sandbox	91.104.123.141	80
161.940732002	Sandbox	66.171.248.178	80
180.373132944	Sandbox	202.21.117.236	80
201.881576061	Sandbox	66.171.248.178	80

UDP PACKETS

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
3.15768098831	Sandbox	192.168.56.255	137
3.20107102394	Sandbox	224.0.0.252	5355
3.24829411507	Sandbox	224.0.0.252	5355
3.28258395195	Sandbox	239.255.255.250	3702
5.81251001358	Sandbox	224.0.0.252	5355
9.20103192329	Sandbox	192.168.56.255	138
22.4820969105	Sandbox	8.8.4.4	53
28.5940580368	Sandbox	8.8.4.4	53
28.748267889	Sandbox	8.8.4.4	53
47.0128691196	Sandbox	8.8.4.4	53
68.1532850266	Sandbox	224.0.0.252	5355
71.1554470062	Sandbox	8.8.4.4	53
73.4675679207	Sandbox	8.8.4.4	53
73.7795739174	Sandbox	89.203.10.56	53
75.8031439781	Sandbox	89.203.10.56	53
77.7948961258	Sandbox	89.203.10.56	53

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
79.7943499088	Sandbox	89.203.10.56	53
81.7942650318	Sandbox	89.203.10.56	53
85.5727550983	Sandbox	8.8.4.4	53
85.8329179287	Sandbox	94.249.60.127	53
87.825783968	Sandbox	94.249.60.127	53
88.0136220455	Sandbox	94.249.60.127	53
100.663007975	Sandbox	89.203.10.56	53
102.653908968	Sandbox	89.203.10.56	53
104.653584003	Sandbox	89.203.10.56	53
106.653544903	Sandbox	89.203.10.56	53
108.656548977	Sandbox	89.203.10.56	53
116.700544119	Sandbox	94.249.60.127	53
118.701219082	Sandbox	94.249.60.127	53
118.909586906	Sandbox	94.249.60.127	53
136.141300917	Sandbox	89.203.10.56	53
138.141210079	Sandbox	89.203.10.56	53
140.140806913	Sandbox	89.203.10.56	53
142.141365051	Sandbox	89.203.10.56	53
144.14172101	Sandbox	89.203.10.56	53
148.118082047	Sandbox	94.249.60.127	53
150.118509054	Sandbox	94.249.60.127	53
150.295638084	Sandbox	94.249.60.127	53
166.67694211	Sandbox	89.203.10.56	53
168.676667929	Sandbox	89.203.10.56	53
170.6770401	Sandbox	89.203.10.56	53
172.677504063	Sandbox	89.203.10.56	53
174.677371025	Sandbox	89.203.10.56	53
177.643224001	Sandbox	94.249.60.127	53
179.643357992	Sandbox	94.249.60.127	53
179.855637074	Sandbox	94.249.60.127	53
287.809175968	Sandbox	8.8.4.4	53
288.011166096	Sandbox	89.203.10.56	53
290.011585951	Sandbox	89.203.10.56	53
292.011326075	Sandbox	89.203.10.56	53
294.011606932	Sandbox	89.203.10.56	53
296.011842966	Sandbox	89.203.10.56	53
365.821842909	Sandbox	8.8.4.4	53

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
366.010500908	Sandbox	89.203.10.56	53
368.011029959	Sandbox	89.203.10.56	53
370.011018038	Sandbox	89.203.10.56	53
372.010710001	Sandbox	89.203.10.56	53
374.010948896	Sandbox	89.203.10.56	53

VALKYRIE COMODO

DETAILED FILE INFO

CREATED / DROPPED FILES

FILE PATH	TYPE AND HASHES
C:\Users\User\AppData\Local\Temp\81F2.Tmp.Exe	**Type :** PE32 executable (GUI) Intel 80386, for MS Windows **MD5 :** fbb3b6da55833f4d15d902790d577588 **SHA-1 :** ecbd04a5b9c7b22f8c713c9867debaf1fb4fae65 **SHA-256 :** e83cfb3bdbf988eae33471f48ab3d2e9e84cf6b1c **SHA-512 :** 4677c093ad71d2d0623669994f8425fa12d7960b **Size :** 253.952 Kilobytes.
C:\Users\User\AppData\Local\Temp\A92C.Tmp	**Type :** SQLite 3.x database **MD5 :** 4093d416041f86e413a3a16db0174cc5 **SHA-1 :** 458ff8d14cc96744b536ab855880f47ac836d11d **SHA-256 :** 4202ae01b7badc53a5fee5ee0cdb8c33b283b41c **SHA-512 :** 34df446f6474d32b958cef422c5e86ff8dd2df6a0(**Size :** 63.488 Kilobytes.
C:\Users\User\AppData\Local\Temp\AA08.Tmp	**Type :** SQLite 3.x database **MD5 :** adf1452686215b01ffe6ea5c47a924d8 **SHA-1 :** 855a0209604cebc85ef0226bd4836fee0f96bf1e **SHA-256 :** 3a444b4258c8493e6e9bb4f17bfd17c8caad48a4 **SHA-512 :** 82fb2b61e64553c58ad608c596e13b7f5c4b3da1 **Size :** 18.432 Kilobytes.
C:\Windows\Sysnative\Tasks\Opera Scheduled Autoupdate 4086469641	**Type :** XML 1.0 document, Little-endian UTF-16 Unicode text, with CRLF line terminators **MD5 :** c0999b077daa1732c051bb3e92bf1498 **SHA-1 :** 7d2d55dba2bd2811a3950290d6b7967cb7b75081 **SHA-256 :** c69a2508b96cfb4becaee5372ad9288b4a88c810 **SHA-512 :** 087ed7e39e8c22e0b0e610f01c358ecdf351210d **Size :** 3.578 Kilobytes.
C:\Users\User\AppData\Roaming\Microsoft\Windows\Guujubau\Cafadrev.Exe	**Type :** PE32 executable (GUI) Intel 80386, for MS Windows **MD5 :** f3e6adde5e52ef7b542520c6882eb3d3 **SHA-1 :** de9b08b0b530581d0485bef9dadf032c2120f1ff **SHA-256 :** 2acd5a3773d876f1af651f4f39538e7c3fa0899bff **SHA-512 :** 04a15142072a26477792a55368ef90536bc866cf **Size :** 243.2 Kilobytes.

MATCH YARA RULES

MATCH RULES

STATIC FILE INFO

File Name:	444.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
SHA1:	de9b08b0b530581d0485bef9dadf032c2120f1ff
MD5:	f3e6adde5e52ef7b542520c6882eb3d3
First Seen Date:	2018-05-24 09:02:22.528957 (4 years ago)
Number Of Clients Seen:	6
Last Analysis Date:	2018-05-24 09:02:22.528957 (4 years ago)
Human Expert Analysis Date:	2019-01-20 14:25:27.859729 (4 years ago)
Human Expert Analysis Result:	Malware

DETAILED FILE INFO

ADDITIONAL FILE INFORMATION

PE Headers

PROPERTY	VALUE
Magic Literal Enum	3
File Type Enum	6
Debug Artifacts	[]
Number Of Sections	5
Trid	[]
Compilation Time Stamp	0x5B066A31 [Thu May 24 07:30:57 2018 UTC]
Entry Point	0x405fdc (.text)
Machine Type	Intel 386 or later - 32Bit
File Size	243200
Ssdeep	
Sha256	2acd5a3773d876f1af651f4f39538e7c3fa0899bffe464050c47e10eedef5ca0
Exifinfo	[]
Mime Type	application/x-dosexec
Imphash	

PE Sections

NAME	VIRTUAL ADDRESS	VIRTUAL SIZE	RAW SIZE	ENTROPY	MD5
.text	0x1000	0x15cd5	0x15e00	6.68848768528	ead1df20e9d41a9070dfa7040e5d0f21
.rdata	0x17000	0x6648	0x6800	5.81058113983	f442f03dec2c035c98a5406c0af54c9f
.data	0x1e000	0x374fee4	0x2000	3.41762454054	498e5943a6f5361812d2a12059229f00
.rsrc	0x376e000	0x12054	0x12200	7.40578175938	2f9c233bc6f6655ae5799e759a38d57a
.reloc	0x3781000	0xa92c	0xaa00	1.217633304	c3fed903293b620c5db9e54b1912820b

PE Resources

{u'lang': u'LANG_NEUTRAL', u'name': u'LAMOTWBDTC', u'offset': 58124560, u'sha256': u'4d5cf4c9693697bd09ffc1928ad43b91d4c0355642eb116366dd5a4bebef9788', u'type': u'data', u'size': 34996}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_BITMAP', u'offset': 58159556, u'sha256': u'f77bd4581d37d310f9739d56451f163a26ca7b81639f59e2eb20d9aa1fa2da9c', u'type': u'data', u'size': 19240}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_ICON', u'offset': 58178796, u'sha256': u'2f16108625d788e051d556cdf624c77d21d752709afe7b7139e6519ec363fd52', u'type': u'data', u'size': 3752}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_ICON', u'offset': 58182548, u'sha256': u'6b37f9b25588e1ec2cee71b1b9ae648ad64a21770c49aa495c906581e40b4b7c', u'type': u'data', u'size': 4264}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_ICON', u'offset': 58186812, u'sha256': u'871407cdb2255554e25285a73ed8a466aae82b996f0ea6573fcc6af169de4850', u'type': u'GLS_BINARY_LSB_FIRST', u'size': 1128}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_STRING', u'offset': 58187940, u'sha256': u'a52e6d429f86a05cc0c3918eb062b1d67d7bc4d926b648a180eecf0bb15dae9d', u'type': u'data', u'size': 246}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_STRING', u'offset': 58188188, u'sha256': u'7ed824fe16954260f13b2e6a28bf074e92a58f2de6e668653211b73b28215364', u'type': u'data', u'size': 192}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_STRING', u'offset': 58188380, u'sha256': u'69ce808b7a3c5c0991d3a44c93b8a4b0eedf4e1807e91e6b1331717026e95d38', u'type': u'data', u'size': 154}
{u'lang': u'LANG_NEUTRAL', u'name': u'RT_STRING', u'offset': 58188536, u'sha256': u'872c888902aba37abcc14809750170d183018ae09b49821a0b9e631583d85d45', u'type': u'data', u'size': 298}
{u'lang': u'LANG_NEUTRAL', u'name': u'RT_STRING', u'offset': 58188836, u'sha256': u'3220237583c0b3524a03ff6d99a4c98ab6ed68180920c416cf73e116aef48fff', u'type': u'data', u'size': 298}
{u'lang': u'LANG_NEUTRAL', u'name': u'RT_STRING', u'offset': 58189136, u'sha256': u'886859492714093b4aa91e57d62a5eaa4519e00d44fd0b86b7dd44a77aaa68ad', u'type': u'data', u'size': 132}
{u'lang': u'LANG_NEUTRAL', u'name': u'RT_STRING', u'offset': 58189268, u'sha256': u'2a5016f3d73f7864ac2e3bce5e036b2cdeb2c139b51aefb68ff3f76bf7691077', u'type': u'data', u'size': 288}
{u'lang': u'LANG_NEUTRAL', u'name': u'RT_STRING', u'offset': 58189556, u'sha256': u'9be1e56de5ae1ac5a2ba1e38e47ba5f3fba479b01226f137724a15fc5bd9b5da', u'type': u'data', u'size': 132}
{u'lang': u'LANG_NEUTRAL', u'name': u'RT_STRING', u'offset': 58189688, u'sha256': u'e584df8e3907e60da6afd20e6471eea9dc73aea35c63bb493bf62cc320fea30d', u'type': u'data', u'size': 168}
{u'lang': u'LANG_NEUTRAL', u'name': u'RT_STRING', u'offset': 58189856, u'sha256': u'bb13a850c37fde8d8282ee64290f0a4c6eb8a86bacd5edc6bfe1e34bdd6a430c', u'type': u'data', u'size': 114}
{u'lang': u'LANG_NEUTRAL', u'name': u'RT_STRING', u'offset': 58189972, u'sha256': u'922a60789571700b8d5e8743176f32fe3c4379122a659df12319749315e18ec5', u'type': u'data', u'size': 102}
{u'lang': u'LANG_NEUTRAL', u'name': u'RT_STRING', u'offset': 58190076, u'sha256': u'fa20ff40a4043a2db32968ab6b44a4ff2f86d4ee491a8a7151772b2fb4adb16e', u'type': u'data', u'size': 82}
{u'lang': u'LANG_NEUTRAL', u'name': u'RT_STRING', u'offset': 58190160, u'sha256': u'a5b53707a2478a35668ff6b5eaa9caffa12c3dcba1b5f44c387ab9afe422bb33', u'type': u'data', u'size': 152}
{u'lang': u'LANG_NEUTRAL', u'name': u'RT_STRING', u'offset': 58190312, u'sha256': u'bb967e0fe59628ba020d3443861a92d2bfd86efa9a7f6fa4575296635d9ee066', u'type': u'data', u'size': 234}
{u'lang': u'LANG_NEUTRAL', u'name': u'RT_STRING', u'offset': 58190548, u'sha256': u'7ad2ac2cbf1de96d32a5adc1c4541239d500929db0d83ffb3b9810e583e624b3', u'type': u'data', u'size': 276}
{u'lang': u'LANG_NEUTRAL', u'name': u'RT_STRING', u'offset': 58190824, u'sha256': u'10911606e0b416983d39036a4ddc0794d3ea6dedf62a60790f30f6c79910fbe2', u'type': u'data', u'size': 202}
{u'lang': u'LANG_NEUTRAL', u'name': u'RT_STRING', u'offset': 58191028, u'sha256': u'46380b2fd547417cb7daa862fb50dd63b242c0ab3afbecc3cd6d8cb17a15c148', u'type': u'data', u'size': 110}
{u'lang': u'LANG_NEUTRAL', u'name': u'RT_STRING', u'offset': 58191140, u'sha256': u'cf2040c00091dc9e4643ac5f63a691292cdaf66f9be1ad68feb41913746e53b6', u'type': u'data', u'size': 358}
{u'lang': u'LANG_NEUTRAL', u'name': u'RT_STRING', u'offset': 58191500, u'sha256': u'827431e4b867abb426f2958c135f5175317b78d793eb929c60751c66629ef6a2', u'type': u'data', u'size': 144}
{u'lang': u'LANG_NEUTRAL', u'name': u'RT_STRING', u'offset': 58191644, u'sha256': u'8b1fe31c26d18604f390ba061118d5ba99dd062af0dc04b0b28cd8ce5e5d3321', u'type': u'data', u'size': 138}
{u'lang': u'LANG_NEUTRAL', u'name': u'RT_STRING', u'offset': 58191784, u'sha256': u'2adc523e96b74f2e4f515f28c93fcbcdf5129e49dfc30500c24394c24b3f4c8a', u'type': u'data', u'size': 318}
{u'lang': u'LANG_NEUTRAL', u'name': u'RT_STRING', u'offset': 58192104, u'sha256': u'885568c29af7e5430be5cdfd37a6a9ee03867066b7ca6d08d082d2cb280e48c1', u'type': u'data', u'size': 594}
{u'lang': u'LANG_NEUTRAL', u'name': u'RT_STRING', u'offset': 58192700, u'sha256': u'956aacd5b39fc7cba4e0463548d288be52974291d83bdbc3e032dbec586b14c6', u'type': u'data', u'size': 88}
{u'lang': u'LANG_NEUTRAL', u'name': u'RT_STRING', u'offset': 58192788, u'sha256': u'65a6c2c79758098e681f183937c4fb015120104159e72d422c3338d79b8568ad', u'type': u'data', u'size': 244}
{u'lang': u'LANG_NEUTRAL', u'name': u'RT_STRING', u'offset': 58193032, u'sha256': u'0e1c2517374b73fb964ecd7bfd0e59e3b827a263d357429251ebb1b5a53c2b9c', u'type': u'data', u'size': 140}
{u'lang': u'LANG_NEUTRAL', u'name': u'RT_STRING', u'offset': 58193172, u'sha256': u'30f98c710509912079bff1cf2beaa738ab08ff4f6866e6eaa0ce4edb164a637b', u'type': u'data', u'size': 262}
{u'lang': u'LANG_NEUTRAL', u'name': u'RT_STRING', u'offset': 58193436, u'sha256': u'8073541a1f4c141206deb9e4a147a2e55cc0452844d1b8cd10f8899119b98f73', u'type': u'data', u'size': 62}
{u'lang': u'LANG_NEUTRAL', u'name': u'RT_STRING', u'offset': 58193500, u'sha256': u'5be3819b1b0c30d74721a9a4bdb700d33ac9c9c1c470b26cea55d1b6bbd63b65', u'type': u'data', u'size': 70}
{u'lang': u'LANG_NEUTRAL', u'name': u'RT_STRING', u'offset': 58193572, u'sha256': u'013f2d1bb6fe2ae9bc8843e747699f171af391f9c7075507d18610bfae570abe', u'type': u'data', u'size': 202}
{u'lang': u'LANG_NEUTRAL', u'name': u'RT_STRING', u'offset': 58193776, u'sha256': u'c3c1cf5ebec14229444e38eb90a326756ad1c311f250b537037cee3dee65d571', u'type': u'data', u'size': 48}
{u'lang': u'LANG_NEUTRAL', u'name': u'RT_STRING', u'offset': 58193824, u'sha256': u'29ca8e0a007d644bfb502db803d3870f3b1bf7d6ecd2241f37fc301ed8b67a2f', u'type': u'data', u'size': 236}
{u'lang': u'LANG_NEUTRAL', u'name': u'RT_STRING', u'offset': 58194060, u'sha256': u'98b6cff0c295b2af1a1693d2012a8665160a8b1f486dda4b7406e71111cb71b7', u'type': u'data', u'size': 270}
{u'lang': u'LANG_NEUTRAL', u'name': u'RT_STRING', u'offset': 58194332, u'sha256': u'ace64a14ef95d7da4fcf138adabaafa5057784b7c4bbba222a8335a8e47b80af', u'type': u'data', u'size': 74}
{u'lang': u'LANG_NEUTRAL', u'name': u'RT_STRING', u'offset': 58194408, u'sha256': u'c2482967bc5bc0557973562d67f9c450b35d5abcb87d2047ead81d009bdb51bd', u'type': u'data', u'size': 242}
{u'lang': u'LANG_NEUTRAL', u'name': u'RT_STRING', u'offset': 58194652, u'sha256': u'3a98667798be8f67a1e2495a0103863f6a3b40ca15d5e3e8c70c3c47c88adcde', u'type': u'data', u'size': 318}
{u'lang': u'LANG_NEUTRAL', u'name': u'RT_STRING', u'offset': 58194972, u'sha256': u'2a46aee850d68409bf43bbe424553cb14c44b76939f7c0cafb7f0edad65022bb', u'type': u'data', u'size': 266}
{u'lang': u'LANG_NEUTRAL', u'name': u'RT_STRING', u'offset': 58195240, u'sha256':

u'6d136402ad12d808633b79cd3c902f571772ed4ba2c4468925a1b5de958e93a4', u'type': u'data', u'size': 336}

{u'lang': u'LANG_NEUTRAL', u'name': u'RT_STRING', u'offset': 58195576, u'sha256': u'7f814de4ad8b4d0b5ac973fecb806bc5a7fad1e04c0bf0b33cf64a454beb61a1', u'type': u'data', u'size': 246}

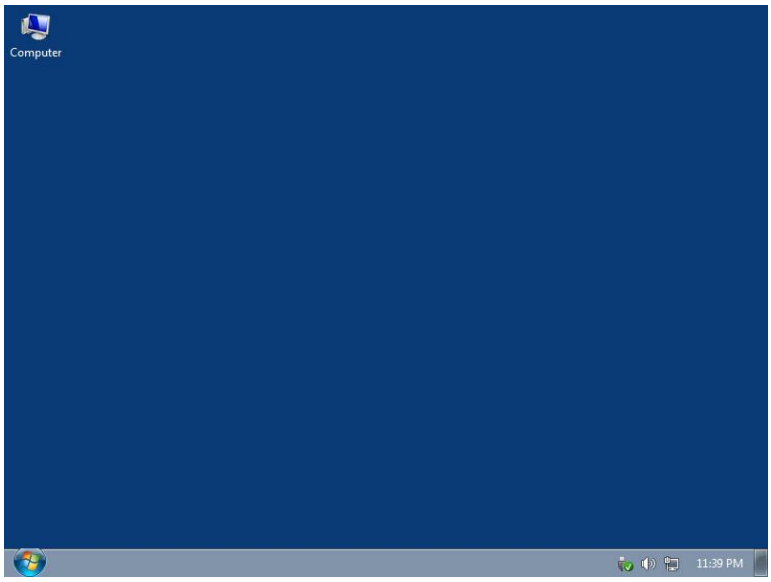
{u'lang': u'LANG_NEUTRAL', u'name': u'RT_STRING', u'offset': 58195824, u'sha256': u'b333ab1da4b17deea8b4b57e44e08ea23ef4bfea7613e30a8f335f4173fa9690', u'type': u'data', u'size': 180}

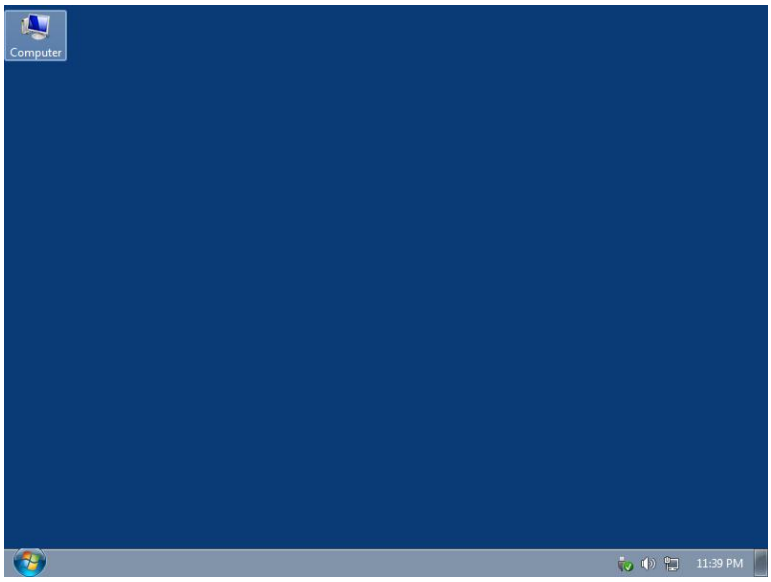
{u'lang': u'LANG_NEUTRAL', u'name': u'RT_GROUP_ICON', u'offset': 58196004, u'sha256': u'd427e9f4ab2f44d675eb3a0afbff2676dabccdf012dca7a3ff6a519f31897d80', u'type': u'MS Windows icon resource - 3 icons, 48x48', u'size': 48}

CERTIFICATE VALIDATION

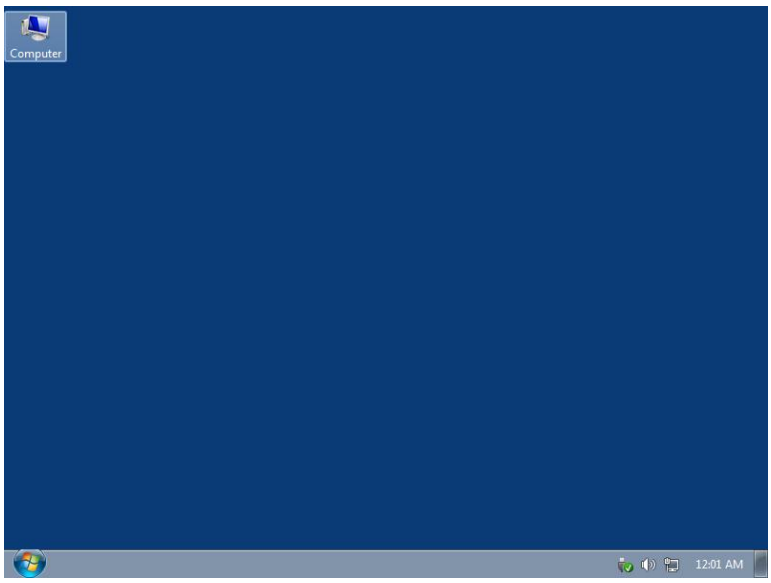
- Certificate Validation is not Applicable ?

SCREENSHOTS




Computer
11:39 PM


Computer
8:46 PM


Computer
12:01 AM