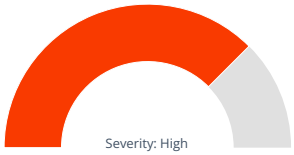
VALKYRIE COMODO

Summary

File Name: virussign.com_4942910b7370152d737ffccbe5fef1c0.vir
File Type: PE32 executable (GUI) Intel 80386 (stripped to external PDB), for MS Windows
SHA1: 2d575f552317f20c19fc5c624bd40fef2e1ea818
MD5: 4942910b7370152d737ffccbe5fef1c0

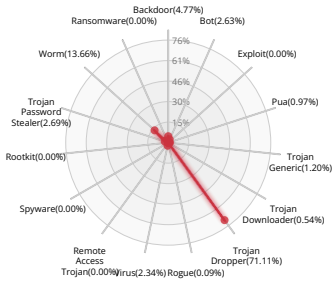
MALWARE
Valkyrie Final Verdict

DETECTION SECTION

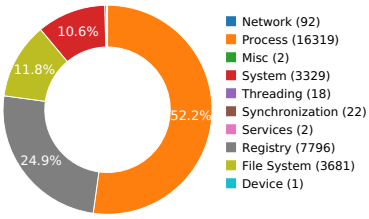


Verdict: Malware

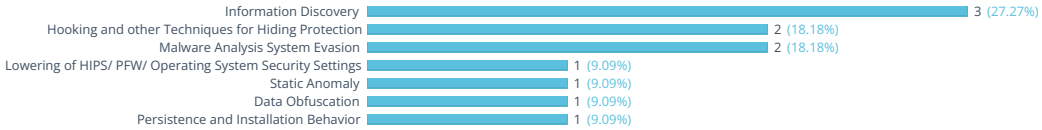
CLASSIFICATION



HIGH LEVEL BEHAVIOR DISTRIBUTION



ACTIVITY OVERVIEW



VALKYRIE COMODO

Activity Details

INFORMATION DISCOVERY

Expresses interest in specific running processes	Show sources
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

LOWERING OF HIPS/ PFW/ OPERATING SYSTEM SECURITY SETTINGS

Attempts to disable Windows Auto Updates	Show sources

STATIC ANOMALY

Anomalous binary characteristics	Show sources

HOOKING AND OTHER TECHNIQUES FOR HIDING PROTECTION

Code injection with CreateRemoteThread in a remote process	Show sources
Operates on local firewall's policies and settings	Show sources

DATA OBFUSCATION

Drops a binary and executes it	Show sources

PERSISTENCE AND INSTALLATION BEHAVIOR

Installs itself for autorun at Windows startup	Show sources

MALWARE ANALYSIS SYSTEM EVASION

Attempts to modify or disable Security Center warnings	Show sources
A process attempted to delay the analysis task by a long amount of time.	Show sources

VALKYRIE COMODO

Behavior Graph

Behavior Summary

ACCESSED FILES

C:\Users\user\AppData\Local\Temp\2d575f552317f20c19fc5c624bd40fef2e1ea818.exe
C:\Windows\SysWOW64\hgoohad.exe
C:\Windows\System32\cmd.exe
C:\Windows\System32\ouxgoasef-fom.exe
C:\Windows\System32\eatcedoon.exe
C:\Users\user\AppData\Roaming
C:\Users\user\AppData\Roaming\tmpFA7D.tmp
C:\Windows\System32\ehruteam.dll
C:\Users\user\AppData\Roaming\onhoahoos-udex.dll
\Device\KsecDD

READ REGISTRY KEYS

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\GRE_Initialize\DisableMetaFiles
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Internet Settings\Connection Policy\Extended Flags
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\Advanced\ShellRegEx
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\ShellRegEx
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Internet Settings\Connection Policy\Default Flags
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connection Policy\Default Flags
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\Advanced\g00d d0gg

MODIFIED FILES

C:\Windows\SysWOW64\hgoohad.exe
C:\Windows\System32\ouxgoasef-fom.exe
C:\Windows\System32\eatcedoon.exe
C:\Users\user\AppData\Roaming\tmpFA7D.tmp
C:\Windows\System32\ehruteam.dll
C:\Users\user\AppData\Roaming\onhoahoos-udex.dll

RESOLVED APIS

kernel32.dll.CreateRemoteThread
ntdll.dll.NtAllocateVirtualMemory
ntdll.dll.NtWriteVirtualMemory
ntdll.dll.NtShutdownSystem
ntdll.dll.RtlAdjustPrivilege
ntdll.dll.NtOpenProcessToken
ntdll.dll.NtQueryInformationToken
rasapi32.dll.RasEnumConnectionsA
iphlpapi.dll.GetIpAddrTable
wininet.dll.InternetOpenA
wininet.dll.InternetOpenUrlA
wininet.dll.InternetReadFile
wininet.dll.InternetSetOptionA
wininet.dll.InternetCloseHandle
rasapi32.dll.RasConnectionNotificationW
sechost.dll.NotifyServiceStatusChangeA
cryptbase.dll.SystemFunction036

REGISTRY KEYS

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\GRE_Initialize
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\GRE_Initialize\DisableMetaFiles
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connection Policy
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Internet Settings\Connection Policy\Extended Flags

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\explorer.exe
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\explorer.exe\Debugger
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\explorer.exe\0123456789012345
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Active Setup\Installed Components\{562D5043-562d-5043-562D-5043562D5043}
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Active Setup\Installed Components\{562D5043-562d-5043-562D-5043562D5043}\01234567890
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Active Setup\Installed Components\{562D5043-562d-5043-562D-5043562D5043}\IsInstalled
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Active Setup\Installed Components\{562D5043-562d-5043-562D-5043562D5043}\StubPath
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Advanced
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\Advanced\ShellRegEx
HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\Advanced
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced\ShellRegEx
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate\AU
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate\AU\NoAutoUpdate
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Security Center
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Security Center\AntiVirusOverride
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Security Center\AntiVirusDisableNotify
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Security Center\FirewallDisableNotify
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Security Center\UpdatesDisableNotify
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile\AuthorizedApplications\List
HKEY_LOCAL_MACHINE\sOfTwaRe\mIcRoSofT\cOdE SToRe dAtAbAsE\Distribution Units\{79AABB1D-FADB-7161-3CCB-997899295A29}
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connection Policy
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Internet Settings\Connection Policy\Default Flags
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connection Policy\Default Flags
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Notify\{BC84DF00-BC38-9902-8082-6FCBF2D87A0B}
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Winlogon\Notify\{BC84DF00-BC38-9902-8082-6FCBF2D87A0B}\01234567890
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Winlogon\Notify\{BC84DF00-BC38-9902-8082-6FCBF2D87A0B}\DLLName
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Winlogon\Notify\{BC84DF00-BC38-9902-8082-6FCBF2D87A0B}\Startup
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\Advanced\g00d d0gg

READ FILES

C:\Users\user\AppData\Local\Temp\2d575f552317f20c19fc5c624bd40fef2e1ea818.exe
C:\Windows\SysWOW64\hgoohad.exe
C:\Windows\System32\cmd.exe
C:\Windows\System32\ouxgoasef-fom.exe
C:\Windows\System32\eatcedoon.exe
C:\Users\user\AppData\Roaming\tmpFA7D.tmp
C:\Windows\System32\ehruteam.dll
C:\Users\user\AppData\Roaming\onhoahoos-udex.dll
\Device\KsecDD

MUTEXES

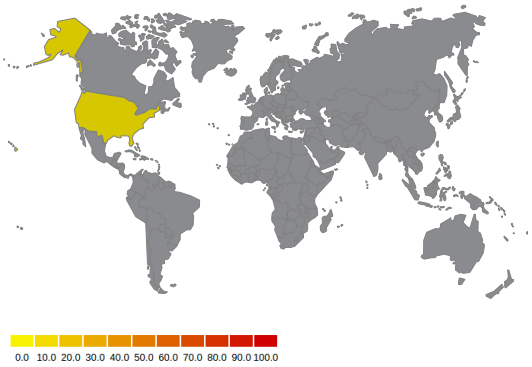
{10F5781A-0D97-0F99-EF77-BA382916E579}
qnd_b__-01
qnd_b__-02
qnd_b__-03
qnd_b__-04
qnd_b__-05
qnd_b__-06
qnd_b__-07
qnd_b__-08
qnd_b__-09

qnd_b__-0A
qnd_b__-0B
qnd_b__-0C
qnd_b__-0D
qnd_b__-0E
qnd_b__-0F
qnd_b__-10
qnd_b__-11
qnd_b__-12
qnd_b__-13
{9703941E-446E-952F-954A-3DA8A91ED84F}

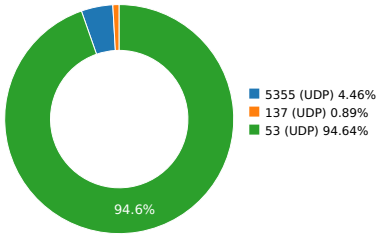
MODIFIED REGISTRY KEYS
HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connection Policy
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Internet Settings\Connection Policy\Extended Flags
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\explorer.exe
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\explorer.exe\0123456789012345678901234567890123456789012345678901234567890123456789012345678901234567890123456789012345678901234567890123456789012345678901234567890123456789012345678901234567890123456789012345
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\explorer.exe\Debugger
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Active Setup\Installed Components\{562D5043-562d-5043-562D-5043562D5043}
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Active Setup\Installed Components\{562D5043-562d-5043-562D-5043562D5043}\0123456789
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Active Setup\Installed Components\{562D5043-562d-5043-562D-5043562D5043}\IsInstalled
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Active Setup\Installed Components\{562D5043-562d-5043-562D-5043562D5043}\StubPath
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate\AU
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate\AU\NoAutoUpdate
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Security Center\AntiVirusOverride
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Security Center\AntiVirusDisableNotify
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Security Center\FirewallDisableNotify
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Security Center\UpdatesDisableNotify
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connection Policy
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Internet Settings\Connection Policy\Default Flags
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connection Policy\Default Flags
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\explorer\Advanced\ShellRegEx
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\Notify\{BC84DF00-BC38-9902-8082-6FCBF2D87A0B}
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Winlogon\Notify\{BC84DF00-BC38-9902-8082-6FCBF2D87A0B}\0123456789
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Winlogon\Notify\{BC84DF00-BC38-9902-8082-6FCBF2D87A0B}\DLLName
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows NT\CurrentVersion\Winlogon\Notify\{BC84DF00-BC38-9902-8082-6FCBF2D87A0B}\Startup

Network Behavior

CONTACTED IPS



NETWORK PORT DISTRIBUTION



Name	IP	Country	ASN	ASN Name	Trigger Process Type
	8.8.4.4		15169	Google LLC	Malware Process
	8.8.8.8	United States	15169	Google LLC	Malware Process
					Malware Process
					Malware Process
dczetim.ws	64.70.19.203	United States	3561	CenturyLink Communications, LLC	Malware Process
ofiwcxhizwj.vg	88.198.29.97	Germany	24940	Hetzner Online AG Datacenter Nuernberg	Malware Process
					Malware Process
viqsiawvtiwc.ws	64.70.19.203	United States	3561	CenturyLink Communications, LLC	Malware Process
www.aieov.com	45.33.2.79	United States	63949	Akamai Technologies, Inc.	Malware Process
					Malware Process
					Malware Process
magsuwqeiecpc.ws	64.70.19.203	United States	3561	CenturyLink Communications, LLC	Malware Process
pgqmsrwycfe.ph	45.79.222.138	United States	63949	Akamai Technologies, Inc.	Malware Process
					Malware Process
					Malware Process
					Malware Process
www.msftncsi.com	23.200.3.18	United States	20940	Akamai Technologies, Inc.	Malware Process
					Malware Process
					Malware Process

DNS QUERIES

Request	Type
wagtm.st	A
5isohu.com	A
www.msftncsi.com	A
www.aieov.com	A
muykmspei.tk	A
ofiwcxhizwj.vg	A
gynzsugwl.cm	A
viqsiawvtiwc.ws	A
tqgyu.st	A
wzsoyymkmv.tk	A
eezidfc.rw	A
uqfiwsw.rw	A
magsuwqeiecpc.ws	A
dczetim.ws	A
pgqmsrwycfe.ph	A
eqbecpkyjequrm.cm	A
xbciaeyycquhuw.rw	A

UDP PACKETS

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
3.00699186325	Sandbox	224.0.0.252	5355
3.00951385498	Sandbox	224.0.0.252	5355
3.07862782478	Sandbox	192.168.56.255	137
4.15588593483	Sandbox	224.0.0.252	5355
5.22051382065	Sandbox	224.0.0.252	5355
5.56261086464	Sandbox	224.0.0.252	5355
5.92251777649	Sandbox	8.8.4.4	53
6.92293691635	Sandbox	8.8.8.8	53
7.0979449749	Sandbox	8.8.4.4	53
7.87537288666	Sandbox	8.8.4.4	53
8.09363079071	Sandbox	8.8.8.8	53
8.87512683868	Sandbox	8.8.8.8	53
20.6732897758	Sandbox	8.8.8.8	53
21.7506568432	Sandbox	8.8.4.4	53
21.9699649811	Sandbox	8.8.8.8	53
22.9690217972	Sandbox	8.8.4.4	53
36.688710928	Sandbox	8.8.8.8	53
37.750223875	Sandbox	8.8.4.4	53
45.2035148144	Sandbox	8.8.8.8	53
46.2339789867	Sandbox	8.8.4.4	53
52.0476808548	Sandbox	8.8.8.8	53
53.1252219677	Sandbox	8.8.4.4	53
60.0159537792	Sandbox	8.8.8.8	53
61.0157649517	Sandbox	8.8.4.4	53
66.7120018005	Sandbox	8.8.8.8	53
67.7662658691	Sandbox	8.8.4.4	53
81.7075548172	Sandbox	8.8.8.8	53
82.703291893	Sandbox	8.8.4.4	53
84.4689908028	Sandbox	8.8.8.8	53
85.5660378933	Sandbox	8.8.4.4	53
99.2349967957	Sandbox	8.8.8.8	53
100.234967947	Sandbox	8.8.4.4	53
100.344293833	Sandbox	8.8.8.8	53
101.421486855	Sandbox	8.8.4.4	53
115.094671011	Sandbox	8.8.8.8	53
116.094031811	Sandbox	8.8.4.4	53
123.875422955	Sandbox	8.8.8.8	53
124.9689188	Sandbox	8.8.4.4	53
130.015990973	Sandbox	8.8.8.8	53
131.094777822	Sandbox	8.8.4.4	53
138.594416857	Sandbox	8.8.8.8	53
139.593781948	Sandbox	8.8.4.4	53
148.953701973	Sandbox	8.8.8.8	53
149.953529835	Sandbox	8.8.4.4	53
163.187533855	Sandbox	8.8.8.8	53
163.953186989	Sandbox	8.8.8.8	53
164.281651974	Sandbox	8.8.4.4	53
164.953329802	Sandbox	8.8.4.4	53
177.907921791	Sandbox	8.8.8.8	53
178.688264847	Sandbox	8.8.8.8	53
178.906316996	Sandbox	8.8.4.4	53
179.687066793	Sandbox	8.8.4.4	53
197.468972921	Sandbox	8.8.8.8	53
198.468689919	Sandbox	8.8.4.4	53
202.298503876	Sandbox	8.8.8.8	53
203.296621799	Sandbox	8.8.4.4	53

Call Time During Execution(sec)	Source IP	Dest IP	Dest Port
212.203337908	Sandbox	8.8.8.8	53
213.202890873	Sandbox	8.8.4.4	53
216.922681808	Sandbox	8.8.8.8	53
217.937838793	Sandbox	8.8.4.4	53
227.017928839	Sandbox	8.8.8.8	53
228.110668898	Sandbox	8.8.4.4	53
241.484764814	Sandbox	8.8.8.8	53
242.484369993	Sandbox	8.8.4.4	53
245.703574896	Sandbox	8.8.8.8	53
246.781176805	Sandbox	8.8.4.4	53
256.016837835	Sandbox	8.8.8.8	53
257.109447956	Sandbox	8.8.4.4	53
260.703701973	Sandbox	8.8.8.8	53
261.703662872	Sandbox	8.8.4.4	53
275.859390974	Sandbox	8.8.8.8	53
276.93718791	Sandbox	8.8.4.4	53
280.719164848	Sandbox	8.8.8.8	53
281.812557936	Sandbox	8.8.4.4	53
294.484852791	Sandbox	8.8.8.8	53
295.469326973	Sandbox	8.8.8.8	53
295.578063965	Sandbox	8.8.4.4	53
296.531239986	Sandbox	8.8.4.4	53
309.172066927	Sandbox	8.8.8.8	53
310.171950817	Sandbox	8.8.4.4	53
320.141625881	Sandbox	8.8.8.8	53
321.234542847	Sandbox	8.8.4.4	53
323.939062834	Sandbox	8.8.8.8	53
324.937414885	Sandbox	8.8.4.4	53
334.812872887	Sandbox	8.8.8.8	53
335.812812805	Sandbox	8.8.4.4	53
338.581286907	Sandbox	8.8.8.8	53
339.625432968	Sandbox	8.8.4.4	53
353.297565937	Sandbox	8.8.8.8	53
354.296992779	Sandbox	8.8.4.4	53
359.297273874	Sandbox	8.8.8.8	53
360.296507835	Sandbox	8.8.4.4	53
368.082011938	Sandbox	8.8.8.8	53
369.077914953	Sandbox	8.8.4.4	53
371.675336838	Sandbox	8.8.8.8	53
372.765769005	Sandbox	8.8.4.4	53
394.125389814	Sandbox	8.8.8.8	53
395.218583822	Sandbox	8.8.4.4	53
409.016671896	Sandbox	8.8.8.8	53
410.109778881	Sandbox	8.8.4.4	53
433.687469006	Sandbox	8.8.8.8	53
434.781039953	Sandbox	8.8.4.4	53
448.56277585	Sandbox	8.8.8.8	53
449.562306881	Sandbox	8.8.4.4	53
473.327963829	Sandbox	8.8.8.8	53
474.327736855	Sandbox	8.8.4.4	53
485.376015902	Sandbox	8.8.8.8	53
486.469329834	Sandbox	8.8.4.4	53
503.276812792	Sandbox	8.8.8.8	53
504.354899883	Sandbox	8.8.4.4	53
507.91473484	Sandbox	8.8.8.8	53
508.986886978	Sandbox	8.8.4.4	53

VALKYRIE COMODO

DETAILED FILE INFO

CREATED / DROPPED FILES

FILE PATH	TYPE AND HASHES
C:\Users\User\AppData\Roaming\Onhoahoos-Udex.Dll	**Type :** PE32 executable (DLL) (GUI) Intel 80386 (stripped to external PDB), for MS Windows **MD5 :** eb9474598b42c55cc62d098b8c5d8b7e **SHA-1 :** 1d73f3da3c1ba4dea3ee051e41cf8b991685b8ef **SHA-256 :** 7cd473a4b131e8beb8f9baae5876d47a74d7dfe0ad76b5f189dde8fbe0285e91 **SHA-512 :** e6d84dc5c513aa41ed053ba2bc113346d7caec5d782871a5d72803c64b3d54b93236 **Size :** 25.6 Kilobytes.
C:\Windows\System32\Ehruteam.Dll	**Type :** PE32 executable (DLL) (GUI) Intel 80386 (stripped to external PDB), for MS Windows **MD5 :** f37b21c00fd81bd93c89ce741a88f183 **SHA-1 :** b2796500597c68e2f5638e1101b46eaf32676c1c **SHA-256 :** 76cf016fd77cb5a06c6ed4674ddc2345e8390c010cf344491a6e742baf2c0fb0 **SHA-512 :** 252fe66dea9a4b9aebc5fd2f24434719cb25159ba51549d9de407f44b6a2f7bce6e071 **Size :** 5.12 Kilobytes.
C:\Windows\System32\Eatcedoon.Exe	**Type :** PE32 executable (GUI) Intel 80386 (stripped to external PDB), for MS Windows **MD5 :** 1832abe69b66f80851f90c1441650700 **SHA-1 :** 07f660477da1d351be11e5153570e5634e4be969 **SHA-256 :** b8e993de067fa6174c4c6a40234c929c5bb3bafe3d2762abb865aa8422df3e78 **SHA-512 :** 37d7aebc7cd89741f4ad13fe8714797d884e206fa844734fe14a68ad9a121693fdcd97 **Size :** 73.888 Kilobytes.
C:\Users\User\AppData\Roaming\TmpFA7D.Tmp	**Type :** data **MD5 :** 89136458baaf23035e18937dd35fa48c **SHA-1 :** 26f29107cb3178c623c5b8c9ed192a5e69801d8f **SHA-256 :** 2bccc5522298d5fa52a36f86468bd10662dd0a1c9ca25489f9d2f77704aec81e **SHA-512 :** 5c28e7e196ecc9b963984fa3c4a991d3c5916af08d05bdf16502155c48892e079d4ca5 **Size :** 71.717 Kilobytes.
C:\Windows\SysWOW64\Hgoohad.Exe	**Type :** PE32 executable (GUI) Intel 80386 (stripped to external PDB), for MS Windows **MD5 :** d2f5fca791eecd3a242b04fe76ecb03f **SHA-1 :** d08595714fbce076f09221a11de5b35ccfab97e0 **SHA-256 :** 770bed237b2078fe328a711c112a82f73770f148781b5f79492a7c07a4327b13 **SHA-512 :** 67c7630b9a5b7d91d60068ad34d3bcd22d08f7b9f8a8b1954677cea27abb93ec0b82c **Size :** 71.717 Kilobytes.
C:\Windows\System32\Ouxgoasef-Fom.Exe	**Type :** PE32 executable (GUI) Intel 80386 (stripped to external PDB), for MS Windows **MD5 :** 8c3c10efbd700d9670479864cca2f554 **SHA-1 :** 93230e977d601f06c071daf9897a2e6c590bec82 **SHA-256 :** 364a798fba759d168f7d2387bcf0a61e3b9a302eb752eef1eea7eef3db874a59 **SHA-512 :** 6291b9b3570bb736d80376a14729ced8d2937fcf7a93370ce2fd6672367abca737659 **Size :** 74.944 Kilobytes.

MATCH YARA RULES

MATCH RULES

STATIC FILE INFO

File Name:	virussign.com_4942910b7370152d737ffccbe5fef1c0.vir
File Type:	PE32 executable (GUI) Intel 80386 (stripped to external PDB), for MS Windows
SHA1:	2d575f552317f20c19fc5c624bd40fef2e1ea818
MD5:	4942910b7370152d737ffccbe5fef1c0
First Seen Date:	2024-12-01 20:15:11.284995 (6 months ago)
Number Of Clients Seen:	2
Last Analysis Date:	2024-12-01 20:16:43.998512 (6 months ago)
Human Expert Analysis Date:	2024-12-02 17:40:07.175205 (6 months ago)
Human Expert Analysis Result:	Malware

VALKYRIE COMODO

DETAILED FILE INFO

ADDITIONAL FILE INFORMATION

PE Headers

PROPERTY	VALUE
Magic Literal Enum	3
File Type Enum	6
Debug Artifacts	[]
Number Of Sections	2
Trid	[]
Compilation Time Stamp	0x48976F60 [Mon Aug 4 21:06:40 2008 UTC]
Entry Point	0x401000 (.text)
Machine Type	Intel 386 or later - 32Bit
File Size	73888
Ssdeep	
Sha256	f0588c32dad82c2a19f423cb12c44e4ef37c7a8fe04dbbaad4769dfbc798149c
Exifinfo	[]
Mime Type	application/x-dosexec
Imphash	

PE Sections

NAME	VIRTUAL ADDRESS	VIRTUAL SIZE	RAW SIZE	ENTROPY	MD5
.text	0x1000	0x318	0x400	4.50058643334	fe131c915a72dbc34dafc57c03eeca31
.idata	0x2000	0x1b4	0x200	3.60472977541	83a7f0520ee48f434e49900d752f8da3

CERTIFICATE VALIDATION

- Certificate Validation is not Applicable ?

SCREENSHOTS