

This is a report from a file uploaded to our Sandbox. The data from our Sandbox has recently been updated to remove benign files and data, you will not see a list of all open ports or running processes, instead we are only listing those processes and files that are directly relevant to the binary (malware) that was uploaded on our website. We hope this make our reports easier to read and more useful to you.

We welcome your comments and suggestions; please send them to the email address above.

Report Contains Output Reference to file: **sales.exe**

MD5 Hash: **093e72cbc78b46e977561c5874cfab4c**

SSDeep Hash: **12288:2Pqr7eKhHvZ3NSYqHMsd+vgp0pQe1lhJ:283vhN1qHMsd+lp8QEz**

File Description: **PE32 executable for MS Windows (GUI) Intel 80386 32-bit**

Creates Files	Sniffer Capability	Botnet Activity	Beacons Out/Download Capable	Malware Downloaded	Key Logging Capability	Opens Listening Port	Creates SMTP Traffic	Modifies MBR	SQL Attack	FTP Remote Access	Attempts lateral connection	ADS
YES	NO	NO	YES	NO	NO	NO	NO	NO	NO	NO	NO	NO

\*\*\*\* The following files are Malicious files associated with the sales.exe, Download at your own Risk \*\*\*\*

- Apache.tar
- CreatedFiles.tar
- MBR.img
- ModifiedFiles.tar
- sandnet.pcap

FTP Link: <ftp://anonymous@68.15.186.23/093e72cbc78b46e977561c5874cfab4c/>

Anti-Virus Tool	Result
McAfee+Artemis	Spam-Mailbot.h.gen.a
nProtect	Worm/W32.lksmas.454657
CAT-QuickHeal	I-Worm.lksmas.rt
McAfee	Spam-Mailbot.h.gen.a
TheHacker	W32/lksmas.rt
K7AntiVirus	Email-Worm.Win32.lksmas
VirusBuster	Trojan.Waledac.Gen!Pac.7
NOD32	Win32/Waledac.GL
F-Prot	W32/EmailWorm.OWQ
a-squared	Trojan.Win32.Waledac!IK
Norman	W32/Spambot.AEA
Avast	Win32:Nuwar-AW
Kaspersky	Email-Worm.Win32.lksmas.rt
BitDefender	Trojan.Waledac.AQ
Comodo	TrojWare.Win32.Waledac.-D
F-Secure	Packed:W32/Waledac.gen!F
DrWeb	Trojan.Spambot.4331
AntiVir	TR/Waledac.443393.A
McAfee-GW-Edition	Heuristic.BehavesLike.Win32.Obfuscated.C
Sophos	Mal/WaledPak-D
eTrust-Vet	Win32/Waledac.FK
Authentium	W32/EmailWorm.OWQ
Jiangmin	I-Worm.lksmas.dc
Antiy-AVL	Worm/Win32.lksmas.gen
Symantec	Trojan Horse
Microsoft	Trojan:Win32/Waledac.gen!A
ViRobot	I-Worm.Win32.lksmas.454657
Prevx	High Risk Worm
GData	Trojan.Waledac.AQ
AhnLab-V3	Win32/Mail.worm.454657
VBA32	Email-Worm.Win32.lksmas.rt
Sunbelt	Trojan.Win32.Generic!BT
Ikarus	Trojan.Win32.Waledac
Fortinet	PossibleThreat
AVG	Pakes.BXC
Panda	W32/Waledac.O.worm

VirusTotal link for: [093e72cbc78b46e977561c5874cfab4c](https://www.virustotal.com/093e72cbc78b46e977561c5874cfab4c)

### Files created on the File System - Count: 75

[Back To Top](#)

File Name:	~DFFE4A.tmp
File Path:	Documents and Settings/Administrator/Local Settings/Temp
MD5 Hash:	9b108e3fc0e564b67fd09b107deaabca
SSDeep Hash:	6:rI912N0xs+CFQXCB9Xh9Xh9XeIEIAj1rF5oFmi4LSahQ23PWX:rl3IKFQCb776Eipx5Om5osP2
File Name:	RestorePointSize
File Path:	System Volume Information/_restore{307E7B41-0455-430D-B7AD-0176BCF9FE0E}/RP20
MD5 Hash:	f7a5f13b324bff67ff11ee9f13a53872
SSDeep Hash:	3:9llln:Hllln
File Name:	change.log
File Path:	System Volume Information/_restore{307E7B41-0455-430D-B7AD-0176BCF9FE0E}/RP20
MD5 Hash:	0f8dfeb4a17e697400f9ecb7c2385e6c
SSDeep Hash:	24:1+xTv+3rQxnwClURXX0Xz/tweyVNNIfi2:1gv+3rQxwmVOVlfJ

**Files created on the File System - Count: 75**

[Back To Top](#)

File Name:	rp.log
File Path:	System Volume Information/_restore{307E7B41-0455-430D-B7AD-0176BCF9FE0E}/RP20
MD5 Hash:	4081cd3a0aedcd5fe594b6f9defc3f04
SSDeep Hash:	12:We1kOj9/9IH2w5EelQbldHlpAwwvRBRZBsXds:Wcxj9/Hx5EelQbLV75se
File Name:	ComDb.Dat
File Path:	System Volume Information/_restore{307E7B41-0455-430D-B7AD-0176BCF9FE0E}/RP20/snapshot
MD5 Hash:	cdc4c8ee1c6cfebe3356c61fe84b4bbe
SSDeep Hash:	384:tb6Hld+wZ2RtpL0u2ADGGsRcpbKg1/FWIDV1SKV+BdQ+lf4wTml0M0Y:56cZ2RtrKGecVfxFWIT9+BdQ+ywTml7
File Name:	\$WinMgmt.CFG
File Path:	System Volume Information/_restore{307E7B41-0455-430D-B7AD-0176BCF9FE0E}/RP20/snapshot/Repository
MD5 Hash:	b24e7591c9efe60700d6afd6b678a4c7
SSDeep Hash:	3:0IT:c
File Name:	INDEX.BTR
File Path:	System Volume Information/_restore{307E7B41-0455-430D-B7AD-0176BCF9FE0E}/RP20/snapshot/Repository/FS
MD5 Hash:	1d74131fe12c6c15f9d85ee97615251d
SSDeep Hash:	12288:C5B0OIkulb4nS8M3G7FDdVRmualQEdwjevQHeS8iV:s4Sm7baLe/
File Name:	INDEX.MAP
File Path:	System Volume Information/_restore{307E7B41-0455-430D-B7AD-0176BCF9FE0E}/RP20/snapshot/Repository/FS
MD5 Hash:	084445371268f0e2675265c54a9ac7e4
SSDeep Hash:	12:LzsHQoPaK4tAYltzGPotJgRPI9T8jU0qT9tPdt8eQal/nDR:Ps3LYzmfPPqUZVSeQa1DR
File Name:	MAPPING.VER
File Path:	System Volume Information/_restore{307E7B41-0455-430D-B7AD-0176BCF9FE0E}/RP20/snapshot/Repository/FS
MD5 Hash:	f2dd0dedb2c260419ece4a9e03b2e828
SSDeep Hash:	3:/ln:t
File Name:	MAPPING1.MAP
File Path:	System Volume Information/_restore{307E7B41-0455-430D-B7AD-0176BCF9FE0E}/RP20/snapshot/Repository/FS
MD5 Hash:	c43ddca253b2503c5b77a5df03a161fb
SSDeep Hash:	384:8iUkjrhnk0ZDRDD8NXoG4zLxpfflbOMFqnFbgL:8ivjrhnk0RDuoG4zLjg5qnS
File Name:	MAPPING2.MAP
File Path:	System Volume Information/_restore{307E7B41-0455-430D-B7AD-0176BCF9FE0E}/RP20/snapshot/Repository/FS
MD5 Hash:	c43ddca253b2503c5b77a5df03a161fb
SSDeep Hash:	384:8iUkjrhnk0ZDRDD8NXoG4zLxpfflbOMFqnFbgL:8ivjrhnk0RDuoG4zLjg5qnS
File Name:	OBJECTS.DATA
File Path:	System Volume Information/_restore{307E7B41-0455-430D-B7AD-0176BCF9FE0E}/RP20/snapshot/Repository/FS
MD5 Hash:	684b1b9396fa4f19f04ce37d7786ad1f
SSDeep Hash:	24576:k2sxq6qyCDPSG7djX+Y1GfN3yHln45X9cbuglCZZVnWq+WNr/x4ASmAT:qq6Zux5c19cbBICXVWqtbuL
File Name:	OBJECTS.MAP
File Path:	System Volume Information/_restore{307E7B41-0455-430D-B7AD-0176BCF9FE0E}/RP20/snapshot/Repository/FS
MD5 Hash:	b974d982d01f8f93596c77b548b7ddc5
SSDeep Hash:	384:8iUkjrhnk0ZDRDD8NXoG4zLxpfflbOMFqnFbw:8ivjrhnk0RDuoG4zLjg5qnK
File Name:	_REGISTRY_MACHINE_SAM
File Path:	System Volume Information/_restore{307E7B41-0455-430D-B7AD-0176BCF9FE0E}/RP20/snapshot
MD5 Hash:	6aa43c59be86f0e60b4549fbc45eadd6
SSDeep Hash:	192:luLA4jNeMMT360j3RL6+/5DbY/y8AAAAAAAYG/cTk0vliuR05Bnprn:xHYMMKchL6+/R7EWi
File Name:	_REGISTRY_MACHINE_SECURITY
File Path:	System Volume Information/_restore{307E7B41-0455-430D-B7AD-0176BCF9FE0E}/RP20/snapshot
MD5 Hash:	a97bed3cf26ba81faba870ba48526451
SSDeep Hash:	768:WBYN54Ao6KKQdaivXHYGJuwMT08Zy5z14v:WeYju/R

**Files created on the File System - Count: 75**

[Back To Top](#)

File Name:	_REGISTRY_MACHINE_SOFTWARE
File Path:	System Volume Information/_restore{307E7B41-0455-430D-B7AD-0176BCF9FE0E}/RP20/snapshot
MD5 Hash:	2abef657e28dbdbc9226a7204e53f084
SSDeep Hash:	98304:TWoutOcGYHTLH5CUKadsDBaOQOgmvr7SkyZAhpurfZFHm/sZPgbfNICTP0voGO7:6PsVmOQOgmV2ZAhcLHmk5FgbVP3o
File Name:	_REGISTRY_MACHINE_SYSTEM
File Path:	System Volume Information/_restore{307E7B41-0455-430D-B7AD-0176BCF9FE0E}/RP20/snapshot
MD5 Hash:	9cac4221b2f54f51b94f2386b6af0ab5
SSDeep Hash:	24576:iKq+Cq6QM1Sk93AuTdBuG9zCd8NGb4wy:ixHQeSk5AnnM
File Name:	_REGISTRY_USER_DEFAULT
File Path:	System Volume Information/_restore{307E7B41-0455-430D-B7AD-0176BCF9FE0E}/RP20/snapshot
MD5 Hash:	8a785abae2cfce09c6a6beb6a56b7ff2
SSDeep Hash:	6144:27uhdQrMuCSazCZOEOKBurhBEnRilbhrc:2ihHqahBJlbhrc
File Name:	_REGISTRY_USER_NTUSER_S-1-5-19
File Path:	System Volume Information/_restore{307E7B41-0455-430D-B7AD-0176BCF9FE0E}/RP20/snapshot
MD5 Hash:	abc843c4e45ef23e0e81415644f97b9c
SSDeep Hash:	6144:kk02t03OSYcmoaZ2EUOk1hVpmU01WBOET7:kb2wBVpmoBOET7
File Name:	_REGISTRY_USER_NTUSER_S-1-5-20
File Path:	System Volume Information/_restore{307E7B41-0455-430D-B7AD-0176BCF9FE0E}/RP20/snapshot
MD5 Hash:	59918940e45934e2c9b86a0974f108c5
SSDeep Hash:	6144:j0Uaqs3iSw6yg+5WEUq0QJgJWbmzL6OET7:jfaLcgJWc6OET7
File Name:	_REGISTRY_USER_NTUSER_S-1-5-21-448539723-2000478354-725345543-500
File Path:	System Volume Information/_restore{307E7B41-0455-430D-B7AD-0176BCF9FE0E}/RP20/snapshot
MD5 Hash:	40233d192f40fe558789a6aa4645841e
SSDeep Hash:	6144:IDXvPZYm2ylDFsPOETsX5rJsEkIFV0TshZSXgSK1XYUOrlirtMUZNOkRe0qUZhd7:lbvPilyPOETsX5BksTVzMUZYkRe0
File Name:	_REGISTRY_USER_USRCLASS_S-1-5-19
File Path:	System Volume Information/_restore{307E7B41-0455-430D-B7AD-0176BCF9FE0E}/RP20/snapshot
MD5 Hash:	33ae691b4ff77867613b2ef167d59c9a
SSDeep Hash:	12:limkjolfW+4z2B/fMWXh810nXOjQyd9cdS/efglXl/rFwuMxbb+9:VjolR4z2Bc2H8yOjnrkN+XORlbb6
File Name:	_REGISTRY_USER_USRCLASS_S-1-5-20
File Path:	System Volume Information/_restore{307E7B41-0455-430D-B7AD-0176BCF9FE0E}/RP20/snapshot
MD5 Hash:	c1a701d05140f7e130e729abd7ec3b7b
SSDeep Hash:	12:IYdkjolfW+4zO/yw3iMf8Q810njOjQyd9cdxcfglXgAFwuMxbb+9:WjolR4zOKw3h8yOjnrkxc+XgYlbb6
File Name:	_REGISTRY_USER_USRCLASS_S-1-5-21-448539723-2000478354-725345543-500
File Path:	System Volume Information/_restore{307E7B41-0455-430D-B7AD-0176BCF9FE0E}/RP20/snapshot
MD5 Hash:	a0e44370a2f36aa8160e385252d939c6
SSDeep Hash:	384:qey72FeFfcoK/7prAERT5dGMU8G6f+zSt6e3g+B8rkNRP9zFluiYy4LydzA/0KvL:IVeF3Kz/dGOEOD3HCHc8C/R8nR
File Name:	domain.txt
File Path:	System Volume Information/_restore{307E7B41-0455-430D-B7AD-0176BCF9FE0E}/RP20/snapshot
MD5 Hash:	4d036d8d930acea9c924c1fb04a1bc2d
SSDeep Hash:	3:qlu0olkLVqlw:euR+0+
File Name:	CollectedData_16.xml
File Path:	WINDOWS/PCHealth/HelpCtr/DataColl
MD5 Hash:	2bf822898ed3960783203dc78fd58bdb
SSDeep Hash:	384:O3KtSY86DcDKw186EUQYz86Kk8C8R8z8h6KHL+5bS86/B/10M868zEwd2:UsWsHyy5Ba
File Name:	CollectedData_17.xml
File Path:	WINDOWS/PCHealth/HelpCtr/DataColl
MD5 Hash:	6644e6a776357133fd697e6d3a4e0a68
SSDeep Hash:	384:O3qoy48Pjci/QV8PkUV458PqBcCckczcUafnOec7y8Pfbf9Us8Pcmk19d:Br25fPnZ0y

**Files created on the File System - Count: 75**

[Back To Top](#)

File Name:	CollectedData_18.xml
File Path:	WINDOWS/PCHealth/HelpCtr/DataColl
MD5 Hash:	be6d1e8cb974dd8a3c8eadc119036adf
SSDeep Hash:	24:QILDsTehexw0T0weOD0+ziK0tVlShGBXlr4tK0IAalSEhkuQ0efw0e6J:yDmuagUo+Wjt3dTtKial0YI9
File Name:	CollectedData_20.xml
File Path:	WINDOWS/PCHealth/HelpCtr/DataColl
MD5 Hash:	c2270f783162cc59dc7aa965243d0b99
SSDeep Hash:	192:OH4jKx9Oq+06uvL031WP3DTwnXnL+Kkz3IZbhg5JE1:O54Yc1
File Name:	CollectedData_22.xml
File Path:	WINDOWS/PCHealth/HelpCtr/DataColl
MD5 Hash:	69eb2c3f7d7c4b12b57c122198dec2de
SSDeep Hash:	48:yDmuagUo+Wjm4caTmTelS3YgUo+Wjm4coTmT0lShYI9:OHw4nCT/Shw4BCTpST
File Name:	CollectedData_24.xml
File Path:	WINDOWS/PCHealth/HelpCtr/DataColl
MD5 Hash:	a9467d8e57fedd61e3c6e5606d50393a
SSDeep Hash:	192:OHabx9S2vgospjJ2qjEUgNPt6WKDRUBb34g6zxO/doP1HiDZl6q:Oa
File Name:	CollectedData_25.xml
File Path:	WINDOWS/PCHealth/HelpCtr/DataColl
MD5 Hash:	7c0d38a2cbd1cf7c785f315cb8471227
SSDeep Hash:	48:yDmuagUo+Wj3tFTSAIUZiYgUo+Wj3ZT/l+Z5YI9:OH3FW1GAjE8L
File Name:	CollectedData_26.xml
File Path:	WINDOWS/PCHealth/HelpCtr/DataColl
MD5 Hash:	0ee81ae91f9e89a57d980700e309bd7c
SSDeep Hash:	24:QILDsTehexw0T0weOD0+ziKOVOfG0cFXlr4VOflnXxOs6AFXj6ta8uQ0efw0e6J:yDmuagUo+WjVTFTVnnXxJ6AR6ta8YI9
File Name:	CollectedData_27.xml
File Path:	WINDOWS/PCHealth/HelpCtr/DataColl
MD5 Hash:	911a91d94b8a7099f07a341427c3a96a
SSDeep Hash:	48:yDmuagUo+WjVTFTVnnXxJ6AR6VtZnyYI9:OHjFRBgmBM
File Name:	CollectedData_28.xml
File Path:	WINDOWS/PCHealth/HelpCtr/DataColl
MD5 Hash:	bbfc1e7fbcb07172b2061a2252dc1d
SSDeep Hash:	24:QILDsTehexw0T0weOD0+ziKOVOfvYlShiwFv1ZXlr4VOFv7SMwFv1MvN/RR2uQ0G:yDmuagUo+WjV/PSTVODLvNZsYI9
File Name:	CollectedData_30.xml
File Path:	WINDOWS/PCHealth/HelpCtr/DataColl
MD5 Hash:	151bffa5ef067b9c70af8eb26e676441
SSDeep Hash:	384:OvA6il8xAzLnn1n+h6AChzhWdmhWDBA/xAt:WA3dAvPAPtBA/xAt
File Name:	CollectedData_32.xml
File Path:	WINDOWS/PCHealth/HelpCtr/DataColl
MD5 Hash:	5700d32474b264ad7242715179839d12
SSDeep Hash:	48:yDmuagUo+WjYGx470/TAqGRI8Gx47j7RoYI9:OHNYm4GrB8m4rR+
File Name:	CollectedData_34.xml
File Path:	WINDOWS/PCHealth/HelpCtr/DataColl
MD5 Hash:	2c6077e0db34c7eca5b1e8ebbad90c5f
SSDeep Hash:	384:OJuzgKNoa/urHaERXa7mMB5ET21o4FQlOdOjr2O7dQpkCPkRchCng99pJQBEg9Lx:kevH5pyUbn6ponT0qBJK4biQrN2eHc
File Name:	CollectedData_35.xml
File Path:	WINDOWS/PCHealth/HelpCtr/DataColl
MD5 Hash:	0c7ad4f9efd6a25c843793880c196a84
SSDeep Hash:	192:OHpljZdO0dJlaZR0Dplj3FdO9dJla3FR9Dplj3FdOVdJla3FRVDpljMdO0dJlaMF:OJllasbbaUbT/3Y4mWQwreB8l4VgzK

**Files created on the File System - Count: 75**

[Back To Top](#)

File Name:	CollectedData_36.xml
File Path:	WINDOWS/PCHealth/HelpCtr/DataColl
MD5 Hash:	90a7053fd903d335203c0e7a4f1e7aee
SSDeep Hash:	384:Oi6aTGk3a4Infc8dfUY4H4md04xxIkJtc5QkGliVu:JIPdeYmd04xxlko55KJ
File Name:	CollectedData_37.xml
File Path:	WINDOWS/PCHealth/HelpCtr/DataColl
MD5 Hash:	731dd274804a5c675b90c36b41b4ad46
SSDeep Hash:	192:Oht0mKbDtbTcVWUo+Gh+ZJ9ASVJYX+fHjVPi12W52W52zQLjNvUhrU5YF7sTWH:O8FUz2Y4uW5gkGlyVL
File Name:	CollectedData_38.xml
File Path:	WINDOWS/PCHealth/HelpCtr/DataColl
MD5 Hash:	9a935b6660328bbb404be505db9d3e65
SSDeep Hash:	384:OqDIjk4CUfUrE/o1axSC2pjdGnBGJEXhi/eh:Zljk4CUfUrE/o1axSC2pjdGt
File Name:	CollectedData_39.xml
File Path:	WINDOWS/PCHealth/HelpCtr/DataColl
MD5 Hash:	4e095f2508cd9210268e04e58e956c23
SSDeep Hash:	48:yDmuagUo+WjdcTqAljZCziYgUo+Wjd5TjI8ZbZiYI9:OHXcad4AX5w+I8
File Name:	CollectedData_40.xml
File Path:	WINDOWS/PCHealth/HelpCtr/DataColl
MD5 Hash:	7ed8e36586244e3a9daa7766b178792c
SSDeep Hash:	24:QILDsTehexw0T0weOD0+zCKOT0bXlr47AMf2uQ0efw0e6J:yDmuagUo+2jiT7AMf2YI9
File Name:	CollectedData_41.xml
File Path:	WINDOWS/PCHealth/HelpCtr/DataColl
MD5 Hash:	c2a9d6bc430f0081505644c3c2363f8b
SSDeep Hash:	24:QILDsTehexw0T0weOD0+zCKOT0bXlr47AMf2ZCj+uQ0efw0e6J:yDmuagUo+2jiT7AMf2Z5YI9
File Name:	CollectedData_42.xml
File Path:	WINDOWS/PCHealth/HelpCtr/DataColl
MD5 Hash:	1274da0d46ef0be06106a0563129ca26
SSDeep Hash:	768:NaJ5wDT12+GV1gTRaGRwsrGqUaQhwKbGsp:I
File Name:	CollectedData_43.xml
File Path:	WINDOWS/PCHealth/HelpCtr/DataColl
MD5 Hash:	2dd96326ffe004af67b9ba475626fef0
SSDeep Hash:	192:OHI650RezI670Lehl6t09enlfpZI768E/YlvYtlS7cloVOI2Hgl7U5lzTKlM+rlo:O4aokwC+GUT
File Name:	CollectedData_44.xml
File Path:	WINDOWS/PCHealth/HelpCtr/DataColl
MD5 Hash:	9d10506a630554bb541e37ac00b0205e
SSDeep Hash:	192:OHQL482SmYhrL44SnPtL4qShJqL4RSoylZPMU4ITuCM2nIFL4nSuywl2L4QSuPH7:O1ziktUdko
File Name:	CollectedData_45.xml
File Path:	WINDOWS/PCHealth/HelpCtr/DataColl
MD5 Hash:	1e15dfc9d14d5c2752a3f16e76d0087e
SSDeep Hash:	192:OHQL482SmYRrL44SnvtL4qShZqL4RSO6lZPMU4ITuCM2nIFL4nSuyol2L4QSuPHj:OFzqkNUdkQ
File Name:	SonndMan.exe
File Path:	WINDOWS
MD5 Hash:	d86b05df745eb9c1436eaaae01ad61a0
SSDeep Hash:	768:UsPrXQqQCNASYbpsYdURWQER41hUoqgJbLSICQiZ7usXy7zr53buZqBo:bdXQwdyPdURxu41CoqgsI1C7u7zr53b4
File Name:	Accessibility.ni.dll
File Path:	WINDOWS/assembly/NativeImages_v2.0.50727_32/Accessibility/6d85f2815aaed54fa00eba17c6f94396
MD5 Hash:	cc5c96d00414bc2e53863c671700b6df
SSDeep Hash:	384:aajuTuuJkVOMLKE8UxOVO2QnzI2QnzTNNUUKJi914WlumW:aajQuGkNuE8ZOXuUt91L

**Files created on the File System - Count: 75**

[Back To Top](#)

File Name:	AspNetMMCExt.ni.dll
File Path:	WINDOWS/assembly/NativeImages_v2.0.50727_32/AspNetMMCExt/7e52371617a33a4ba8c3a943a4c68bd9
MD5 Hash:	6e1a90353833c8f5affa3129254d13e0
SSDeep Hash:	6144:Zoda/X+I3UHQXianNMTcZDo8Joh7NW8XH+RdArl7b6oujOC7yJtj+SvENhRXG:o3MQXianGz3cmge5E
File Name:	CustomMarshalers.ni.dll
File Path:	WINDOWS/assembly/NativeImages_v2.0.50727_32/CustomMarshalers/532ed60a3d8ef742a26b0b7854f938af
MD5 Hash:	7fdd6aa3a81489617c39ef9b5c4cfcb1
SSDeep Hash:	3072:0nu1uEepZIZsYpgH04n5WP6vA92fPePqXRnz1aadJ43D8mXW:2aNepZY4nISvawPWqBnzfJ8D
File Name:	Microsoft.Build.Engine.ni.dll
File Path:	WINDOWS/assembly/NativeImages_v2.0.50727_32/Microsoft.Build.Eng#/7f820d2602777d4db7816b294199e0ee
MD5 Hash:	cca559ccc858cbae756cd25e50ddbdf9
SSDeep Hash:	24576:m8fGF2sxJEJ1EzMJEJxOJaJeJJJJJJGJJWJOQJJJd6MG16xJJrftJwyJJwXgJUO:d0Y36sj
File Name:	Microsoft.Build.Framework.ni.dll
File Path:	WINDOWS/assembly/NativeImages_v2.0.50727_32/Microsoft.Build.Fra#/25dbc9548a48c54a95dde09e6f27bd1b
MD5 Hash:	f3d32da32b911ff9422d8f19d2c37c26
SSDeep Hash:	1536:gO9A38fJ3RJJ8UHJJJJJJJJJJJJJJCBJGamOejlXIQiTm+R6a6G3TU/oYJmHtHTDG:gOC38fJ3RJJ8UHJJJJJJJJJJJJJJCBJ0
File Name:	Microsoft.Build.Tasks.ni.dll
File Path:	WINDOWS/assembly/NativeImages_v2.0.50727_32/Microsoft.Build.Tas#/3f4ede794adf0b429828db2916570433
MD5 Hash:	5724708dc01cac8878aa876f659829ca
SSDeep Hash:	24576:esaFe41ol3QTlzJJJJJJJK1Jr9bJJJJJAEG/IJJEJJJJJJJJJJJJJJyJf7SJV:evyl3UivPBj1B4pPHqHIFT
File Name:	Microsoft.Build.Utilities.ni.dll
File Path:	WINDOWS/assembly/NativeImages_v2.0.50727_32/Microsoft.Build.Uti#/202cb67c7a08a043a83c9523211d0194
MD5 Hash:	9a8a9e4e68e9e4bcebd1bf358f9d021e
SSDeep Hash:	3072:4IVNMvSVTR5js+LmuJb0JT6eeExm0xpR3eL8TJZ9Mb0pcMuHIZ0gP2OJim:fVN+StTFJJYJu1EBOIVLhp6HIZ0gpi
File Name:	Microsoft.VisualBasic.ni.dll
File Path:	WINDOWS/assembly/NativeImages_v2.0.50727_32/Microsoft.VisualBasic#/1333403cfcb40c43ad82df3ce2e8aaac
MD5 Hash:	506dfa4660c961446e1828c79dda0553
SSDeep Hash:	24576:AjUUMzNiMHF8SHJHRB5oJnJvZJFbVxvvy3fdA4fvZJBOPmIYPm63ccJP5:AjUUMBH2C3gxvvy3fSCJBmMiYPMnc
File Name:	System.Configuration.ni.dll
File Path:	WINDOWS/assembly/NativeImages_v2.0.50727_32/System.Configuration/1149a37adaa81249aed33c95fd0d8f0a
MD5 Hash:	78a7b3d4790e742a9c58fd94aaffc86c
SSDeep Hash:	24576:63J7ollak0GUYG1EAYrhMrJc5oVJMJdOJhJJJJuEJTt9JJ1JJ0JHXuuiauuJFOv:6alak0G1M06o+A
File Name:	System.Deployment.ni.dll
File Path:	WINDOWS/assembly/NativeImages_v2.0.50727_32/System.Deployment/f938c7ea3dae6c4db4875f2b849b31e1
MD5 Hash:	d1b65faf7cba52587ca599b3da2a0ed6
SSDeep Hash:	24576:HxABwPKbJJ76qDpzJJJJJJJK1JrO1C0JDJsJ9ZDJJJJbJZaxXJKsl0WJJJKJtB:2JAljefxD
File Name:	System.DirectoryServices.ni.dll
File Path:	WINDOWS/assembly/NativeImages_v2.0.50727_32/System.DirectorySer#/1776e8ea619b39458c90e80a5f72c148
MD5 Hash:	7f39b94cf5f47a5d93be75dfa309f6f6
SSDeep Hash:	24576:RPHUe37BGFwZJJmqJJwJJuJJ90uJJJKnFpke8g1nm72fCFN2nS7+kD3:RPHU2BGjm/Nl+k
File Name:	System.DirectoryServices.Protocols.ni.dll
File Path:	WINDOWS/assembly/NativeImages_v2.0.50727_32/System.DirectorySer#/cc1227708901774aad9e8ced8a909138
MD5 Hash:	37039e6f460b990ccf8e871c314a0730
SSDeep Hash:	6144:3NA+KxCcq9Um4RD3OloJJJJJkqb82PDgvsfepJlMkjEHrObI+R+49EdUPML/vjZ:3C3loJJJJk682PDgvgqMLXjmB3p0hZ
File Name:	System.EnterpriseServices.Wrapper.dll
File Path:	WINDOWS/assembly/NativeImages_v2.0.50727_32/System.EnterpriseSe#/014b742986d60a4e87bd44d24bd4ff0f
MD5 Hash:	7c1cae3ca04bd98af64e28e64c535cc5
SSDeep Hash:	6144:awJIMWwAlOitVTWbJD/+QtyRL8ffiZJzi+7X:MWROCWbJD/+QW7gYX

**Files created on the File System - Count: 75**

[Back To Top](#)

File Name:	System.EnterpriseServices.ni.dll
File Path:	WINDOWS/assembly/NativeImages_v2.0.50727_32/System.EnterpriseSe#/014b742986d60a4e87bd44d24bd4ff0f
MD5 Hash:	11ffe04d719a8eb68ce2270d993dc0c2
SSDeep Hash:	12288:xTgXcCQOJH7JJPmJvYJQJ3KJcJTGJJJJJJJJt25BQ0v0os3heKgMMTItYtW:wcCtJH7JJPmJQJQJ3KJcJTGJJJJJO
File Name:	System.Security.ni.dll
File Path:	WINDOWS/assembly/NativeImages_v2.0.50727_32/System.Security/1376a75e3b8a284a93fc613b644b0c66
MD5 Hash:	5458ff54b012f068b2128a4733d4752c
SSDeep Hash:	12288:wjUhS1OMgA7rzJJiJYJbrD4bAKp5JohJfJJJ/JJAmJJ7g6D6Uf91sd:wgmGAvzJJiJYJbrD4bAKp5JohJfJJJO
File Name:	System.Transactions.ni.dll
File Path:	WINDOWS/assembly/NativeImages_v2.0.50727_32/System.Transactions/997444903ba3344b974c58fa2e29a024
MD5 Hash:	def19953bc0e54918057d81de19dae80
SSDeep Hash:	12288:OAgfRYHEXHhouH44I7JGJALJrvQ+R4yyhrua+oiD:ORJNHR44I7JGJALJrv/R4yyhJjID
File Name:	System.Web.Mobile.ni.dll
File Path:	WINDOWS/assembly/NativeImages_v2.0.50727_32/System.Web.Mobile/8d64545543a0d545868afb5e0d72b1e8
MD5 Hash:	5e8e46584a0c7c177b873462f9d8917e
SSDeep Hash:	24576:cJhtZJIO5WM2RfxNwZLcJPKU5f+F/PEgbnv2YJiJ0JEJwJJRJJJ/CwJJJmdFu4:cJPZvqCLGEgbnJo1QbB7AenyFvXnSh
File Name:	System.Web.RegularExpressions.ni.dll
File Path:	WINDOWS/assembly/NativeImages_v2.0.50727_32/System.Web.RegularE#/1b95e2930a072845923f7ba88fd3ad
MD5 Hash:	1e65bb09bdbe75743e2a1e4f7665d454
SSDeep Hash:	6144:9OqvaAPDZRO/5QrXbZjqdar9ksZIVKkXo2vewHG+0FBhPnKeD:J5PDZRO/5QrXbZjqdar9ksZIVKkXo2vW
File Name:	System.Web.Services.ni.dll
File Path:	WINDOWS/assembly/NativeImages_v2.0.50727_32/System.Web.Services/e2c7fd564ac96a419159c5f38a7d8b68
MD5 Hash:	29279964e09637c3ae9808c71402a364
SSDeep Hash:	49152:nP0wr2999999999T9bIXAhStEBRLLwju6f7H11Njfu:Vr2999999999TabRPwH1
File Name:	System.Web.ni.dll
File Path:	WINDOWS/assembly/NativeImages_v2.0.50727_32/System.Web/674ae99f4d2a8a479445310637a932ef
MD5 Hash:	b4266649028e80ebe07f32f62e99dd19
SSDeep Hash:	98304:TGemxgMjwAM+2Fj11Cmhs6oBm/KOLaeYK3utF06b0p:TbPFj11JNK+Y+
File Name:	dfsvc.ni.exe
File Path:	WINDOWS/assembly/NativeImages_v2.0.50727_32/dfsvc/781c76f2828ea64b961936cdc191bd64
MD5 Hash:	dc1d906e2ccb2c7a9231b5f7f9e0c1c
SSDeep Hash:	192:o7eg9xNyrsasEHL2CkoxBgWfoNmX16W/:EegHNpOL2iOWf4mX16W
File Name:	index1b.dat
File Path:	WINDOWS/assembly/NativeImages_v2.0.50727_32
MD5 Hash:	d41d8cd98f00b204e9800998ecf8427e
SSDeep Hash:	3::
File Name:	index1c.dat
File Path:	WINDOWS/assembly/NativeImages_v2.0.50727_32
MD5 Hash:	d41d8cd98f00b204e9800998ecf8427e
SSDeep Hash:	3::
File Name:	inertno.exe
File Path:	WINDOWS/system32
MD5 Hash:	969272b7c38b069410fb410a2827c3fb
SSDeep Hash:	96:/lXn1tDa7FXzLIXpSeaX2UHL8dTbDSjsr04nENWg:/TfwFX45SeaXrreobDhr04nY
File Name:	ttij24.ini
File Path:	WINDOWS/system32
MD5 Hash:	10400c6faf166902b52fb97042f1e0eb
SSDeep Hash:	3:in:in

**Created Files Verified as Malicious - Count: 2**

[Back To Top](#)

This output is generated from hashes corresponding with the files created on the operating system, being submitted to the website <http://www.team-cymru.org> for analysis, as to whether they are known bad binaries.

Md5 Hash	Date Submitted to Cymru.org	Detection %(Likelihood file is malicious)
969272b7c38b069410fb410a2827c3fb	1283196850	68
d86b05df745eb9c1436eaaae01ad61a0	1265256367	62

**Files which were modified on the File System with the corresponding MD5SUM and Path - Count: 18**

File Name:	jusched.log
File Path:	Documents and Settings/Administrator/Local Settings/Temp
MD5 Hash:	ba8cf82cff154235505f3136f9ac074c
File Name:	NTUSER.DAT
File Path:	Documents and Settings/Administrator
MD5 Hash:	b617206da002d901ec4e1094168cf6b1
File Name:	NTUSER.DAT
File Path:	Documents and Settings/LocalService
MD5 Hash:	abc843c4e45ef23e0e81415644f97b9c
File Name:	NTUSER.DAT
File Path:	Documents and Settings/NetworkService
MD5 Hash:	59918940e45934e2c9b86a0974f108c5
File Name:	drivetable.txt
File Path:	System Volume Information/_restore{307E7B41-0455-430D-B7AD-0176BCF9FE0E}
MD5 Hash:	1ddd0136a679936417a33f6b451cfe2f
File Name:	fifo.log
File Path:	System Volume Information/_restore{307E7B41-0455-430D-B7AD-0176BCF9FE0E}
MD5 Hash:	494661741d8742c823350db9f1a1b2d1
File Name:	_filelst.cfg
File Path:	System Volume Information/_restore{307E7B41-0455-430D-B7AD-0176BCF9FE0E}
MD5 Hash:	00c8ff929e6599bdc293c65ffab77439
File Name:	history_db.xml
File Path:	WINDOWS/PCHealth/HelpCtr/DataColl
MD5 Hash:	1d50763d277e28c7a3f1bab5898827b7
File Name:	Layout.ini
File Path:	WINDOWS/Prefetch
MD5 Hash:	cbe9cd3bf183d230de5714ff49835e2a
File Name:	AppEvent.Evt
File Path:	WINDOWS/system32/config
MD5 Hash:	7220f1c01da1110a1b7a8990af7fd80a
File Name:	default
File Path:	WINDOWS/system32/config
MD5 Hash:	86fa90b50915351792f8d299e0066599

**Files which were modified on the File System with the corresponding MD5SUM and Path - Count: 18**

File Name:	SAM
File Path:	WINDOWS/system32/config
MD5 Hash:	12ff9cc94206392c849fb89876bc676f
File Name:	SECURITY
File Path:	WINDOWS/system32/config
MD5 Hash:	13452b668aaef5c72730c938a67df31a
File Name:	software
File Path:	WINDOWS/system32/config
MD5 Hash:	9095997fa91cec1f65a9a66e11a68a54
File Name:	SysEvent.Evt
File Path:	WINDOWS/system32/config
MD5 Hash:	0d4328c531c3ed8918b5410dde1d6b7f
File Name:	system
File Path:	WINDOWS/system32/config
MD5 Hash:	38923fa5056b21d9e48454a9dfc90bff
File Name:	Preferred
File Path:	WINDOWS/system32/Microsoft/Protect/S-1-5-18/User
MD5 Hash:	632edc87de7ab70a7c7f44d7a9830f06
File Name:	ngen_service.log
File Path:	WINDOWS/Microsoft.NET/Framework/v2.0.50727
MD5 Hash:	3af710ce9ab3e13fd4a52b568a95329b

**Malicious DNS Queries, HTTP Traffic, and GET Commands, etc. - Count: 2156**

[Back To Top](#)

**Data**

114.48.75.138114.48.75.138
114.48.75.138124.125.200.215
114.48.75.138124.173.211.167
114.48.75.138149.149.162.34
114.48.75.138193.200.95.69
114.48.75.138211.135.92.117
114.48.75.138216.63.104.50
114.48.75.13824.144.29.149
114.48.75.13824.211.77.19
114.48.75.13824.79.99.232
114.48.75.13841.249.33.213
114.48.75.13860.35.214.132
114.48.75.13861.0.133.7
114.48.75.13864.95.58.153
114.48.75.13867.188.180.68
114.48.75.13876.210.63.46
114.48.75.13881.104.221.110
114.48.75.13881.105.34.234
114.48.75.13882.237.12.170
114.48.75.13882.36.169.65
114.48.75.13884.73.28.203
114.48.75.13886.56.70.25
114.48.75.13887.9.141.78

Malicious DNS Queries, HTTP Traffic, and GET Commands, etc. - Count: 2156

[Back To Top](#)

114.48.75.13888.166.244.240  
114.48.75.13889.133.156.162  
124.125.200.215114.48.75.138  
124.125.200.215124.125.200.215  
124.125.200.215124.173.211.167  
124.125.200.215149.149.162.34  
124.125.200.215193.200.95.69  
124.125.200.215211.135.92.117  
124.125.200.215216.63.104.50  
124.125.200.21524.144.29.149  
124.125.200.21524.211.77.19  
124.125.200.21524.79.99.232  
124.125.200.21541.249.33.213  
124.125.200.21561.0.133.7  
124.125.200.21564.95.58.153  
124.125.200.21567.188.180.68  
124.125.200.21576.210.63.46  
124.125.200.21581.104.221.110  
124.125.200.21581.105.34.234  
124.125.200.21584.73.28.203  
124.125.200.21586.56.70.25  
124.125.200.21587.9.141.78  
124.173.211.167114.48.75.138  
124.173.211.167124.125.200.215  
124.173.211.167124.173.211.167  
124.173.211.167149.149.162.34  
124.173.211.167193.200.95.69  
124.173.211.167211.135.92.117  
124.173.211.167216.63.104.50  
124.173.211.16724.144.29.149  
124.173.211.16724.211.77.19  
124.173.211.16724.79.99.232  
124.173.211.16741.249.33.213  
124.173.211.16760.35.214.132  
124.173.211.16761.0.133.7  
124.173.211.16764.95.58.153  
124.173.211.16767.188.180.68  
124.173.211.16776.210.63.46  
124.173.211.16781.104.221.110  
124.173.211.16781.105.34.234  
124.173.211.16782.237.12.170  
124.173.211.16782.36.169.65  
124.173.211.16784.73.28.203  
124.173.211.16786.56.70.25  
124.173.211.16787.9.141.78  
124.173.211.16788.166.244.240  
124.173.211.16789.133.156.162  
149.149.162.34114.48.75.138  
149.149.162.34124.125.200.215  
149.149.162.34124.173.211.167  
149.149.162.34149.149.162.34  
149.149.162.34193.200.95.69  
149.149.162.34211.135.92.117  
149.149.162.34216.63.104.50  
149.149.162.3424.144.29.149  
149.149.162.3424.211.77.19  
149.149.162.3424.79.99.232

Malicious DNS Queries, HTTP Traffic, and GET Commands, etc. - Count: 2156

[Back To Top](#)

149.149.162.3441.249.33.213  
149.149.162.3460.35.214.132  
149.149.162.3461.0.133.7  
149.149.162.3464.95.58.153  
149.149.162.3467.188.180.68  
149.149.162.3476.210.63.46  
149.149.162.3481.104.221.110  
149.149.162.3481.105.34.234  
149.149.162.3482.237.12.170  
149.149.162.3482.36.169.65  
149.149.162.3484.73.28.203  
149.149.162.3486.56.70.25  
149.149.162.3487.9.141.78  
149.149.162.3488.166.244.240  
149.149.162.3489.133.156.162  
193.200.95.69114.48.75.138  
193.200.95.69124.125.200.215  
193.200.95.69124.173.211.167  
193.200.95.69149.149.162.34  
193.200.95.69193.200.95.69  
193.200.95.69211.135.92.117  
193.200.95.69216.63.104.50  
193.200.95.6924.144.29.149  
193.200.95.6924.211.77.19  
193.200.95.6924.79.99.232  
193.200.95.6941.249.33.213  
193.200.95.6960.35.214.132  
193.200.95.6961.0.133.7  
193.200.95.6964.95.58.153  
193.200.95.6967.188.180.68  
193.200.95.6976.210.63.46  
193.200.95.6981.104.221.110  
193.200.95.6981.105.34.234  
193.200.95.6982.237.12.170  
193.200.95.6982.36.169.65  
193.200.95.6984.73.28.203  
193.200.95.6986.56.70.25  
193.200.95.6987.9.141.78  
193.200.95.6988.166.244.240  
193.200.95.6989.133.156.162  
211.135.92.117114.48.75.138  
211.135.92.117124.125.200.215  
211.135.92.117124.173.211.167  
211.135.92.117149.149.162.34  
211.135.92.117193.200.95.69  
211.135.92.117211.135.92.117  
211.135.92.117216.63.104.50  
211.135.92.11724.144.29.149  
211.135.92.11724.211.77.19  
211.135.92.11724.79.99.232  
211.135.92.11741.249.33.213  
211.135.92.11760.35.214.132  
211.135.92.11761.0.133.7  
211.135.92.11764.95.58.153  
211.135.92.11767.188.180.68  
211.135.92.11776.210.63.46  
211.135.92.11781.104.221.110

Malicious DNS Queries, HTTP Traffic, and GET Commands, etc. - Count: 2156

[Back To Top](#)

211.135.92.11781.105.34.234  
211.135.92.11782.237.12.170  
211.135.92.11782.36.169.65  
211.135.92.11784.73.28.203  
211.135.92.11786.56.70.25  
211.135.92.11787.9.141.78  
211.135.92.11788.166.244.240  
211.135.92.11789.133.156.162  
216.63.104.50114.48.75.138  
216.63.104.50124.125.200.215  
216.63.104.50124.173.211.167  
216.63.104.50149.149.162.34  
216.63.104.50193.200.95.69  
216.63.104.50211.135.92.117  
216.63.104.50216.63.104.50  
216.63.104.5024.144.29.149  
216.63.104.5024.211.77.19  
216.63.104.5024.79.99.232  
216.63.104.5041.249.33.213  
216.63.104.5060.35.214.132  
216.63.104.5061.0.133.7  
216.63.104.5064.95.58.153  
216.63.104.5067.188.180.68  
216.63.104.5076.210.63.46  
216.63.104.5081.104.221.110  
216.63.104.5081.105.34.234  
216.63.104.5082.237.12.170  
216.63.104.5082.36.169.65  
216.63.104.5084.73.28.203  
216.63.104.5086.56.70.25  
216.63.104.5087.9.141.78  
216.63.104.5088.166.244.240  
216.63.104.5089.133.156.162  
24.144.28.11087.9.141.78  
24.144.29.149114.48.75.138  
24.144.29.149124.125.200.215  
24.144.29.149124.173.211.167  
24.144.29.149149.149.162.34  
24.144.29.149193.200.95.69  
24.144.29.149211.135.92.117  
24.144.29.149216.63.104.50  
24.144.29.14924.144.29.149  
24.144.29.14924.211.77.19  
24.144.29.14924.79.99.232  
24.144.29.14941.249.33.213  
24.144.29.14961.0.133.7  
24.144.29.14964.95.58.153  
24.144.29.14967.188.180.68  
24.144.29.14976.210.63.46  
24.144.29.14981.104.221.110  
24.144.29.14981.105.34.234  
24.144.29.14984.73.28.203  
24.144.29.14986.56.70.25  
24.144.29.14987.9.141.78  
24.144.29.14989.133.156.162  
24.211.77.19114.48.75.138  
24.211.77.19124.125.200.215

Malicious DNS Queries, HTTP Traffic, and GET Commands, etc. - Count: 2156

[Back To Top](#)

24.211.77.19124.173.211.167  
24.211.77.19149.149.162.34  
24.211.77.19193.200.95.69  
24.211.77.19211.135.92.117  
24.211.77.19216.63.104.50  
24.211.77.1924.144.29.149  
24.211.77.1924.211.77.19  
24.211.77.1924.79.99.232  
24.211.77.1941.249.33.213  
24.211.77.1960.35.214.132  
24.211.77.1961.0.133.7  
24.211.77.1964.95.58.153  
24.211.77.1967.188.180.68  
24.211.77.1976.210.63.46  
24.211.77.1981.104.221.110  
24.211.77.1981.105.34.234  
24.211.77.1982.237.12.170  
24.211.77.1984.73.28.203  
24.211.77.1986.56.70.25  
24.211.77.1987.9.141.78  
24.211.77.1988.166.244.240  
24.211.77.1989.133.156.162  
24.79.99.232114.48.75.138  
24.79.99.232124.125.200.215  
24.79.99.232124.173.211.167  
24.79.99.232149.149.162.34  
24.79.99.232193.200.95.69  
24.79.99.232211.135.92.117  
24.79.99.232216.63.104.50  
24.79.99.23224.144.29.149  
24.79.99.23224.211.77.19  
24.79.99.23224.79.99.232  
24.79.99.23241.249.33.213  
24.79.99.23260.35.214.132  
24.79.99.23261.0.133.7  
24.79.99.23264.95.58.153  
24.79.99.23267.188.180.68  
24.79.99.23276.210.63.46  
24.79.99.23281.104.221.110  
24.79.99.23281.105.34.234  
24.79.99.23282.237.12.170  
24.79.99.23282.36.169.65  
24.79.99.23284.73.28.203  
24.79.99.23286.56.70.25  
24.79.99.23287.9.141.78  
24.79.99.23288.166.244.240  
24.79.99.23289.133.156.162  
41.249.33.213114.48.75.138  
41.249.33.213124.125.200.215  
41.249.33.213124.173.211.167  
41.249.33.213149.149.162.34  
41.249.33.213193.200.95.69  
41.249.33.213211.135.92.117  
41.249.33.213216.63.104.50  
41.249.33.21324.144.29.149  
41.249.33.21324.211.77.19  
41.249.33.21324.79.99.232

Malicious DNS Queries, HTTP Traffic, and GET Commands, etc. - Count: 2156

[Back To Top](#)

41.249.33.21341.249.33.213  
41.249.33.21360.35.214.132  
41.249.33.21361.0.133.7  
41.249.33.21364.95.58.153  
41.249.33.21367.188.180.68  
41.249.33.21376.210.63.46  
41.249.33.21381.104.221.110  
41.249.33.21381.105.34.234  
41.249.33.21382.237.12.170  
41.249.33.21382.36.169.65  
41.249.33.21384.73.28.203  
41.249.33.21386.56.70.25  
41.249.33.21387.9.141.78  
41.249.33.21388.166.244.240  
41.249.33.21389.133.156.162  
60.35.214.132114.48.75.138  
60.35.214.132124.173.211.167  
60.35.214.132149.149.162.34  
60.35.214.132193.200.95.69  
60.35.214.132211.135.92.117  
60.35.214.132216.63.104.50  
60.35.214.13224.211.77.19  
60.35.214.13224.79.99.232  
60.35.214.13241.249.33.213  
60.35.214.13260.35.214.132  
60.35.214.13261.0.133.7  
60.35.214.13264.95.58.153  
60.35.214.13267.188.180.68  
60.35.214.13276.210.63.46  
60.35.214.13281.104.221.110  
60.35.214.13281.105.34.234  
60.35.214.13282.237.12.170  
60.35.214.13282.36.169.65  
60.35.214.13284.73.28.203  
60.35.214.13286.56.70.25  
60.35.214.13287.9.141.78  
60.35.214.13288.166.244.240  
60.35.214.13289.133.156.162  
61.0.133.7114.48.75.138  
61.0.133.7124.125.200.215  
61.0.133.7124.173.211.167  
61.0.133.7149.149.162.34  
61.0.133.7193.200.95.69  
61.0.133.7211.135.92.117  
61.0.133.7216.63.104.50  
61.0.133.724.144.29.149  
61.0.133.724.211.77.19  
61.0.133.724.79.99.232  
61.0.133.741.249.33.213  
61.0.133.760.35.214.132  
61.0.133.761.0.133.7  
61.0.133.764.95.58.153  
61.0.133.767.188.180.68  
61.0.133.776.210.63.46  
61.0.133.781.104.221.110  
61.0.133.781.105.34.234  
61.0.133.782.237.12.170

Malicious DNS Queries, HTTP Traffic, and GET Commands, etc. - Count: 2156

[Back To Top](#)

61.0.133.782.36.169.65  
61.0.133.784.73.28.203  
61.0.133.786.56.70.25  
61.0.133.787.9.141.78  
61.0.133.788.166.244.240  
61.0.133.789.133.156.162  
64.95.58.153114.48.75.138  
64.95.58.153124.125.200.215  
64.95.58.153124.173.211.167  
64.95.58.153149.149.162.34  
64.95.58.153193.200.95.69  
64.95.58.153211.135.92.117  
64.95.58.153216.63.104.50  
64.95.58.15324.144.29.149  
64.95.58.15324.211.77.19  
64.95.58.15324.79.99.232  
64.95.58.15341.249.33.213  
64.95.58.15360.35.214.132  
64.95.58.15361.0.133.7  
64.95.58.15364.95.58.153  
64.95.58.15367.188.180.68  
64.95.58.15376.210.63.46  
64.95.58.15381.104.221.110  
64.95.58.15381.105.34.234  
64.95.58.15384.73.28.203  
64.95.58.15386.56.70.25  
64.95.58.15387.9.141.78  
64.95.58.15388.166.244.240  
64.95.58.15389.133.156.162  
67.188.180.68114.48.75.138  
67.188.180.68124.125.200.215  
67.188.180.68124.173.211.167  
67.188.180.68149.149.162.34  
67.188.180.68193.200.95.69  
67.188.180.68211.135.92.117  
67.188.180.68216.63.104.50  
67.188.180.6824.144.29.149  
67.188.180.6824.211.77.19  
67.188.180.6824.79.99.232  
67.188.180.6841.249.33.213  
67.188.180.6860.35.214.132  
67.188.180.6861.0.133.7  
67.188.180.6864.95.58.153  
67.188.180.6867.188.180.68  
67.188.180.6876.210.63.46  
67.188.180.6881.104.221.110  
67.188.180.6881.105.34.234  
67.188.180.6882.237.12.170  
67.188.180.6882.36.169.65  
67.188.180.6884.73.28.203  
67.188.180.6886.56.70.25  
67.188.180.6887.9.141.78  
67.188.180.6888.166.244.240  
67.188.180.6889.133.156.162  
76.210.63.46114.48.75.138  
76.210.63.46124.125.200.215  
76.210.63.46124.173.211.167

Malicious DNS Queries, HTTP Traffic, and GET Commands, etc. - Count: 2156

[Back To Top](#)

76.210.63.46149.149.162.34  
76.210.63.46193.200.95.69  
76.210.63.46211.135.92.117  
76.210.63.46216.63.104.50  
76.210.63.4624.144.29.149  
76.210.63.4624.211.77.19  
76.210.63.4624.79.99.232  
76.210.63.4641.249.33.213  
76.210.63.4660.35.214.132  
76.210.63.4661.0.133.7  
76.210.63.4664.95.58.153  
76.210.63.4667.188.180.68  
76.210.63.4676.210.63.46  
76.210.63.4681.104.221.110  
76.210.63.4681.105.34.234  
76.210.63.4682.237.12.170  
76.210.63.4682.36.169.65  
76.210.63.4684.73.28.203  
76.210.63.4686.56.70.25  
76.210.63.4687.9.141.78  
76.210.63.4688.166.244.240  
76.210.63.4689.133.156.162  
81.104.221.110114.48.75.138  
81.104.221.110124.125.200.215  
81.104.221.110124.173.211.167  
81.104.221.110149.149.162.34  
81.104.221.110193.200.95.69  
81.104.221.110211.135.92.117  
81.104.221.110216.63.104.50  
81.104.221.11024.144.29.149  
81.104.221.11024.211.77.19  
81.104.221.11024.79.99.232  
81.104.221.11041.249.33.213  
81.104.221.11060.35.214.132  
81.104.221.11061.0.133.7  
81.104.221.11064.95.58.153  
81.104.221.11067.188.180.68  
81.104.221.11076.210.63.46  
81.104.221.11081.104.221.110  
81.104.221.11081.105.34.234  
81.104.221.11082.237.12.170  
81.104.221.11082.36.169.65  
81.104.221.11084.73.28.203  
81.104.221.11086.56.70.25  
81.104.221.11087.9.141.78  
81.104.221.11088.166.244.240  
81.104.221.11089.133.156.162  
81.105.34.234114.48.75.138  
81.105.34.234124.125.200.215  
81.105.34.234124.173.211.167  
81.105.34.234149.149.162.34  
81.105.34.234193.200.95.69  
81.105.34.234211.135.92.117  
81.105.34.234216.63.104.50  
81.105.34.23424.144.29.149  
81.105.34.23424.211.77.19  
81.105.34.23424.79.99.232

Malicious DNS Queries, HTTP Traffic, and GET Commands, etc. - Count: 2156

[Back To Top](#)

81.105.34.23441.249.33.213  
81.105.34.23460.35.214.132  
81.105.34.23461.0.133.7  
81.105.34.23464.95.58.153  
81.105.34.23467.188.180.68  
81.105.34.23476.210.63.46  
81.105.34.23481.104.221.110  
81.105.34.23481.105.34.234  
81.105.34.23482.237.12.170  
81.105.34.23482.36.169.65  
81.105.34.23484.73.28.203  
81.105.34.23486.56.70.25  
81.105.34.23487.9.141.78  
81.105.34.23488.166.244.240  
81.105.34.23489.133.156.162  
82.237.12.170114.48.75.138  
82.237.12.170124.173.211.167  
82.237.12.170149.149.162.34  
82.237.12.170193.200.95.69  
82.237.12.170211.135.92.117  
82.237.12.170216.63.104.50  
82.237.12.17024.211.77.19  
82.237.12.17024.79.99.232  
82.237.12.17041.249.33.213  
82.237.12.17060.35.214.132  
82.237.12.17061.0.133.7  
82.237.12.17067.188.180.68  
82.237.12.17076.210.63.46  
82.237.12.17081.104.221.110  
82.237.12.17081.105.34.234  
82.237.12.17082.237.12.170  
82.237.12.17082.36.169.65  
82.237.12.17086.56.70.25  
82.237.12.17087.9.141.78  
82.237.12.17088.166.244.240  
82.237.12.17089.133.156.162  
82.36.169.65114.48.75.138  
82.36.169.65124.173.211.167  
82.36.169.65149.149.162.34  
82.36.169.65193.200.95.69  
82.36.169.65211.135.92.117  
82.36.169.65216.63.104.50  
82.36.169.6524.79.99.232  
82.36.169.6541.249.33.213  
82.36.169.6560.35.214.132  
82.36.169.6561.0.133.7  
82.36.169.6567.188.180.68  
82.36.169.6576.210.63.46  
82.36.169.6581.104.221.110  
82.36.169.6581.105.34.234  
82.36.169.6582.237.12.170  
82.36.169.6582.36.169.65  
82.36.169.6586.56.70.25  
82.36.169.6587.9.141.78  
82.36.169.6588.166.244.240  
82.36.169.6589.133.156.162  
84.73.28.203114.48.75.138

Malicious DNS Queries, HTTP Traffic, and GET Commands, etc. - Count: 2156

[Back To Top](#)

84.73.28.203124.125.200.215  
84.73.28.203124.173.211.167  
84.73.28.203149.149.162.34  
84.73.28.203193.200.95.69  
84.73.28.203211.135.92.117  
84.73.28.203216.63.104.50  
84.73.28.20324.144.29.149  
84.73.28.20324.211.77.19  
84.73.28.20324.79.99.232  
84.73.28.20341.249.33.213  
84.73.28.20360.35.214.132  
84.73.28.20361.0.133.7  
84.73.28.20364.95.58.153  
84.73.28.20367.188.180.68  
84.73.28.20376.210.63.46  
84.73.28.20381.104.221.110  
84.73.28.20381.105.34.234  
84.73.28.20384.73.28.203  
84.73.28.20386.56.70.25  
84.73.28.20387.9.141.78  
84.73.28.20389.133.156.162  
86.56.70.25114.48.75.138  
86.56.70.25124.125.200.215  
86.56.70.25124.173.211.167  
86.56.70.25149.149.162.34  
86.56.70.25193.200.95.69  
86.56.70.25211.135.92.117  
86.56.70.25216.63.104.50  
86.56.70.2524.144.29.149  
86.56.70.2524.211.77.19  
86.56.70.2524.79.99.232  
86.56.70.2541.249.33.213  
86.56.70.2560.35.214.132  
86.56.70.2561.0.133.7  
86.56.70.2564.95.58.153  
86.56.70.2567.188.180.68  
86.56.70.2576.210.63.46  
86.56.70.2581.104.221.110  
86.56.70.2581.105.34.234  
86.56.70.2582.237.12.170  
86.56.70.2582.36.169.65  
86.56.70.2584.73.28.203  
86.56.70.2586.56.70.25  
86.56.70.2587.9.141.78  
86.56.70.2588.166.244.240  
86.56.70.2589.133.156.162  
87.9.141.78114.48.75.138  
87.9.141.78124.125.200.215  
87.9.141.78124.173.211.167  
87.9.141.78149.149.162.34  
87.9.141.78193.200.95.69  
87.9.141.78211.135.92.117  
87.9.141.78216.63.104.50  
87.9.141.7824.144.29.149  
87.9.141.7824.211.77.19  
87.9.141.7824.79.99.232  
87.9.141.7841.249.33.213

Malicious DNS Queries, HTTP Traffic, and GET Commands, etc. - Count: 2156

[Back To Top](#)

87.9.141.7860.35.214.132  
87.9.141.7861.0.133.7  
87.9.141.7864.95.58.153  
87.9.141.7867.188.180.68  
87.9.141.7876.210.63.46  
87.9.141.7881.104.221.110  
87.9.141.7881.105.34.234  
87.9.141.7882.237.12.170  
87.9.141.7882.36.169.65  
87.9.141.7884.73.28.203  
87.9.141.7886.56.70.25  
87.9.141.7887.9.141.78  
87.9.141.7888.166.244.240  
87.9.141.7889.133.156.162  
88.166.244.240114.48.75.138  
88.166.244.240124.173.211.167  
88.166.244.240149.149.162.34  
88.166.244.240193.200.95.69  
88.166.244.240211.135.92.117  
88.166.244.240216.63.104.50  
88.166.244.24024.211.77.19  
88.166.244.24024.79.99.232  
88.166.244.24041.249.33.213  
88.166.244.24060.35.214.132  
88.166.244.24061.0.133.7  
88.166.244.24064.95.58.153  
88.166.244.24067.188.180.68  
88.166.244.24076.210.63.46  
88.166.244.24081.104.221.110  
88.166.244.24081.105.34.234  
88.166.244.24082.237.12.170  
88.166.244.24082.36.169.65  
88.166.244.24086.56.70.25  
88.166.244.24087.9.141.78  
88.166.244.24088.166.244.240  
88.166.244.24089.133.156.162  
89.133.156.162114.48.75.138  
89.133.156.162124.173.211.167  
89.133.156.162149.149.162.34  
89.133.156.162193.200.95.69  
89.133.156.162211.135.92.117  
89.133.156.162216.63.104.50  
89.133.156.16224.144.29.149  
89.133.156.16224.211.77.19  
89.133.156.16224.79.99.232  
89.133.156.16241.249.33.213  
89.133.156.16260.35.214.132  
89.133.156.16261.0.133.7  
89.133.156.16264.95.58.153  
89.133.156.16267.188.180.68  
89.133.156.16276.210.63.46  
89.133.156.16281.104.221.110  
89.133.156.16281.105.34.234  
89.133.156.16282.237.12.170  
89.133.156.16282.36.169.65  
89.133.156.16284.73.28.203  
89.133.156.16286.56.70.25

Malicious DNS Queries, HTTP Traffic, and GET Commands, etc. - Count: 2156

[Back To Top](#)

89.133.156.16287.9.141.78  
89.133.156.16288.166.244.240  
89.133.156.16289.133.156.162  
114.48.75.138  
124.125.200.215  
124.173.211.167  
149.149.162.34  
193.200.95.69  
211.135.92.117  
216.63.104.50  
24.144.28.110  
24.144.29.149  
24.211.77.19  
24.79.99.232  
41.249.33.213  
61.0.133.7  
64.95.58.153  
67.188.180.68  
76.210.63.46  
81.104.221.110  
81.105.34.234  
84.73.28.203  
86.56.70.25  
87.9.141.78  
/aabszcj.htm  
/aabyavjgt.png  
/aakc.png  
/aaqmpaji.htm  
/abjbdgbzwbp.png  
/acszrgwhrys.png  
/acvpfymtjd.htm  
/adb.htm  
/adrwhvxlqu.png  
/adsqmakthfhp.htm  
/ady.htm  
/aefumubmbqj.htm  
/aelnqa.htm  
/aewb.htm  
/afbwjmd.htm  
/afhqgawijt.htm  
/afpertfodjf.png  
/afzzyy.png  
/agvwhull.png  
/ahd.png  
/aihorpablbn.htm  
/aijbxxyifygb.htm  
/aiybtwsgqmhw.htm  
/ajiblbn.png  
/ajwlcugeic.htm  
/akvbupzavrly.htm  
/anjkaadamy.png  
/aocfikhs.png  
/aoojwem.png  
/aopbgqej.png  
/aoxbjbxdt.htm  
/apeunjvbm.htm  
/asirc.htm

Malicious DNS Queries, HTTP Traffic, and GET Commands, etc. - Count: 2156

[Back To Top](#)

/ask.png  
/asspecsyrb.png  
/atcxleqkl.htm  
/atobw.png  
/atsnukgtcsx.png  
/auiweptb.png  
/aujilsesce.png  
/aulrepxosgwj.htm  
/auoxkwc.png  
/auxdipbrktd.htm  
/avlox.htm  
/awc.png  
/awknvuqwnw.png  
/axcpnd.htm  
/axjkkk.htm  
/ayajanz.png  
/aymncgdjfwq.png  
/ayzlqbxjhr.png  
/azdhydvw.htm  
/bbaezxc.png  
/bbgrdkbw.png  
/bbnvu.htm  
/bboafwajp.htm  
/bbpgozvfeiqd.png  
/bbtxvlk.png  
/bbyb.png  
/bbyvkuofrz.htm  
/bcgfbpwqc.htm  
/bcnada.png  
/bcpugr.png  
/bdnlc.png  
/beumql.png  
/bffe.htm  
/bfflbs.htm  
/bgajce.htm  
/bgbpyc.png  
/bglzcgpiubhr.htm  
/bgvcjeqg.htm  
/bhykd.png  
/biayxuf.png  
/biugqpo.png  
/bjjg.png  
/bjsv.htm  
/blhwfsci.png  
/blmmwnim.png  
/bmbfcbnd.htm  
/bmn.png  
/bmsm.htm  
/bnsvwb.htm  
/bnvxfomzaje.htm  
/bnxuvy.png  
/bohz.htm  
/bokdnpv.htm  
/boktjghf.htm  
/boatuy.png  
/bouzlewp.htm  
/bowdwkuhvpt.htm

Malicious DNS Queries, HTTP Traffic, and GET Commands, etc. - Count: 2156

[Back To Top](#)

/bpubqdiw.png  
/bqqx.htm  
/bqzbehpl.png  
/brcurnks.png  
/breqlwua.htm  
/brmfduqtnq.htm  
/bsczadjtq.htm  
/bsqjhjil.htm  
/btditsmxeqwc.htm  
/btdqxmng.htm  
/btqjaeob.png  
/btrgstyojeyr.png  
/bttnaqyavwwc.htm  
/btwzpvfegxed.png  
/btyib.png  
/bupcjsbo.htm  
/bvcgqv.png  
/bvhpq.png  
/bvioaqleysz.htm  
/bvn.png  
/bwhk.png  
/bwibfdaxujx.htm  
/bwoyuf.htm  
/bwudsnaosl.htm  
/bwwq.htm  
/bxhuodpbvmb1.png  
/bxoggraddm.png  
/byneuctvh.htm  
/bztlj.htm  
/caclzs.htm  
/caiaibdwdjlz.htm  
/caouac.htm  
/cbc.htm  
/cbcde.png  
/cbipbr.png  
/cbytl.htm  
/ccypmhtl.png  
/cdnlefatisaq.png  
/cduemhypp.png  
/cfbuvfwwig.png  
/cfggtdyep.png  
/cfkvuqo.png  
/cgixmwnxsq.htm  
/cgjgyysqdij.htm  
/cguisjgf.htm  
/chmsbzlmfg.htm  
/chviwoijo.png  
/cigvpbke.htm  
/ciwbjhnq.htm  
/cjnsognjl.png  
/cjwzdqps.htm  
/ckidkp.png  
/clbqeybj.htm  
/clki.htm  
/cmbotgiwifxv.png  
/cmkfsnja.png  
/cmnsl.png

Malicious DNS Queries, HTTP Traffic, and GET Commands, etc. - Count: 2156

[Back To Top](#)

/cmscnjzswtl.png  
/cnbigpx.png  
/cnknmyygs.htm  
/coimhyg.htm  
/coldngn.png  
/coqdrp.png  
/coqktoouxw.png  
/corqypr.png  
/coufhoktxu.png  
/cozeghkxj.png  
/cpd.png  
/cpzzvnks.htm  
/cqmihmmnqs.png  
/cqvxajwyfcs.htm  
/cqwwqwjaj.png  
/crbyyrcoq.png  
/crcnollo.htm  
/crmvsqxt.htm  
/csusd.png  
/ctcb.png  
/ctdot.png  
/ctnhq.htm  
/cunprpdlxpx.png  
/cvabgpqnk.png  
/cvdwamhx.htm  
/cvlee.htm  
/cwcldehklqnx.htm  
/cwwj.png  
/cwygr.htm  
/cxhlnfoakgh.png  
/cxrr.png  
/cyd.htm  
/cygyx.png  
/cyuvexuhrn.png  
/czltfeuichoq.png  
/czsbfaes.htm  
/czu.png  
/davpoomxkcg.htm  
/dazxn.png  
/dbfyrmsvmb.png  
/dbiwtacevqo.htm  
/dbziliuj.htm  
/deuwoxakctd.png  
/dezjtsygvri.htm  
/dfroyoijamw.png  
/dgiplwcryhq.htm  
/dgpwii.png  
/dgqdatd.png  
/dgvsgddiqzk.htm  
/dgyoiqkja.png  
/dgzr.htm  
/dhmd.htm  
/dhmurn.png  
/dizeibpyiajb.htm  
/dja.png  
/dkbqo.png  
/dlqryodlybh.htm

Malicious DNS Queries, HTTP Traffic, and GET Commands, etc. - Count: 2156

[Back To Top](#)

/dltgeiz.htm  
/dmrbt.png  
/dnhpqrvtm.htm  
/dnigrdes.png  
/dnlmu.htm  
/dnmhue.png  
/dnmidlmzgwk.htm  
/dnth.png  
/dnxfnmigxpr.png  
/doky.png  
/dowdt.png  
/dpjlc.htm  
/dpn.png  
/dprfyhrsfu.htm  
/drf.htm  
/drfsmulpwfq.png  
/drnwjxkwchh.htm  
/drxhthg.png  
/dshvedigroc.png  
/dskhgjvzve.htm  
/dso.png  
/dsxhqnn.png  
/dtpvxylibfn.htm  
/duhenmc.png  
/dvbmwccggyk.htm  
/dvhejks.png  
/dwpkw.htm  
/dwqevmy.png  
/dwzofilqre.png  
/dwzsilcdx.png  
/dxkegdayq.htm  
/dydb.png  
/dyov.htm  
/dzmfw.png  
/dznbv.png  
/dzpktgoqb.htm  
/eaosbjsc.htm  
/eaz.htm  
/eckiiab.htm  
/ecszlajb.png  
/ecv.htm  
/ecxktwowrfe.png  
/edcrjflnai.htm  
/edgfzvjvf.png  
/edogzaeq.png  
/edpxwvsscbnc.htm  
/eejlpqhcwrpl.png  
/efywmiuowm.htm  
/egn.htm  
/eiaytmappi.png  
/eiearxikywd.htm  
/ekbba.htm  
/ekg.htm  
/ekqvfpmavlz.png  
/ekwhwn.png  
/ekxsxqtdeu.png  
/embuwugdvn.png

Malicious DNS Queries, HTTP Traffic, and GET Commands, etc. - Count: 2156

[Back To Top](#)

/emqydd.png  
/emuyxsn.htm  
/emvylktdsmfx.png  
/enb.png  
/eoeav.htm  
/eogs.png  
/eohjchd.png  
/eotwzp.htm  
/epharxyeft.png  
/epilwcfuxwx.htm  
/eponin.png  
/epxkdrdenip.htm  
/eqhpahhf.png  
/eqxli.htm  
/erpxuwnwzr.png  
/erxbylfrmzy.png  
/esyg.png  
/etft.htm  
/etzg.htm  
/eumpoaz.png  
/evlhp.htm  
/evscxtempu.png  
/ewcyons.png  
/ewlrltbrtelr.png  
/ewxylnje.htm  
/exeyftpmgk.htm  
/eyesiq.htm  
/eymnotqj.png  
/eyqgfaio.png  
/eznihfnvf.htm  
/eztusrwhq.htm  
/fano.png  
/fbiph.htm  
/fbszhlylsnn.htm  
/fcogmkjqkqjm.png  
/fdnhvjvlpzi.png  
/fdssjxrly.htm  
/felxkna.htm  
/fexeov.png  
/fflbcfbth.png  
/ffvcml.png  
/ffzowowljpm.png  
/fhghyjl.png  
/fhhhag.htm  
/fin.png  
/fjckegyph.htm  
/fjiga.png  
/fjjzqtfd.htm  
/fjzgbwjaeo.png  
/fkt.png  
/flrlgljke.png  
/flrqca.png  
/fluwthbkpdp.htm  
/fmgqyz.htm  
/fmpzhfp.png  
/fmdtpebt.htm  
/fmw.htm

Malicious DNS Queries, HTTP Traffic, and GET Commands, etc. - Count: 2156

[Back To Top](#)

/fnaojnio.png  
/fonsjgqde.png  
/foro.htm  
/fptawitqfb.htm  
/fpzddhexgpd.png  
/fqcyatenmgl.htm  
/fqtn.htm  
/fqzvcdbxqq.png  
/frvn.htm  
/ftsnxehfym.png  
/fut.htm  
/fvomcxfg.htm  
/fwiekufa.htm  
/fwjsgjx.htm  
/fxg.htm  
/fxrrawwuqc.png  
/fxvitnhu.htm  
/fxwhwqsk.png  
/fyb.htm  
/fyjfinkwuhu.htm  
/fykshlfl.png  
/fyucwrz.png  
/fyywxykdrq.htm  
/gaba.htm  
/gaopangcm.png  
/gbdzlltylztc.htm  
/gbhxxdmrpr.htm  
/gbneywnl.png  
/gbqyk.htm  
/gcivrltvojq.png  
/gcopgksvlty.htm  
/gcslf.htm  
/gcswdastxvr.htm  
/gdqk.png  
/gdupa.png  
/gdvgdnajdb.htm  
/gdvwdirl.htm  
/geckw.htm  
/gfgsxlxo.png  
/gfpwtjzfbmkx.png  
/ggbznuv.htm  
/ggvp.png  
/ghaivsr.png  
/ghru.htm  
/ghwmmatbitm.png  
/gibtvyugqgh.htm  
/gibwuawtdzsg.htm  
/giighhkichoy.htm  
/jgmdylcqli.png  
/gjl.png  
/jimwoye.htm  
/jiw.htm  
/gkdmvsxsbbx.png  
/gkpywtjfk.png  
/gllglppysam.htm  
/gndynzk.htm  
/gpervralqyei.htm

Malicious DNS Queries, HTTP Traffic, and GET Commands, etc. - Count: 2156

[Back To Top](#)

/gpghkpr.htm  
/gpsdcbjtopu.htm  
/gqdrfkrmmjo.htm  
/grbynax.png  
/grgvze.htm  
/grqpwavqoefk.htm  
/gsbngahwfm.png  
/gslhcxun.png  
/gtdwri.png  
/gtvfmawiu.png  
/gukqxuai.htm  
/guldlqci.png  
/gutaenudvs.png  
/gvd.png  
/gvfanqvtdmv.png  
/gvgyfix.png  
/gwlrtaqtgiy.png  
/gwnngmrcija.png  
/gwzxambb.png  
/gxzhjfcckin.htm  
/gywoj.htm  
/gzop.png  
/hba.png  
/hbjohhcojv.png  
/hcgmmrnfchn.png  
/hdvyic.htm  
/hdwos.png  
/hedczbbun.png  
/heqlscxn.png  
/heviwpyleqdo.png  
/heyrdcce.png  
/hfkeivc.htm  
/hgkgewnzkjeu.png  
/hgsftu.png  
/hifft.htm  
/higkkwk.png  
/hik.htm  
/hincebjh.htm  
/hipgmxfbyr.htm  
/hismcswyzzym.htm  
/hixexhxishaj.png  
/hjsvufyzn.htm  
/hkb.htm  
/hkokzxew.htm  
/hkp.png  
/hkwf.htm  
/hlpamci.htm  
/hmkwhb.png  
/hmtw.png  
/hmylrjd.htm  
/hntn.htm  
/hokdorchs.png  
/hoobqlmie.htm  
/hoofdvpq.png  
/houawiyazroa.htm  
/hovbopwgy.png  
/hoysddnrx.htm

Malicious DNS Queries, HTTP Traffic, and GET Commands, etc. - Count: 2156

[Back To Top](#)

/hpdhs.png  
/hphxokkzlkz.htm  
/hpq.png  
/hptzzjnsjkw.png  
/hqengm.png  
/hqjtbctotrfc.png  
/hqztuusdsx.png  
/hrfflrfoeoz.htm  
/hrllh.png  
/hrr.png  
/hscndth.png  
/hsuyo.png  
/htndbmf.png  
/hts.htm  
/hufojprjsk.htm  
/huhojkzzus.png  
/huhyqm.png  
/hui.png  
/hunmmpx.htm  
/huwfu.htm  
/hvneapkehgsj.htm  
/hvyurkukn.htm  
/hweswvut.htm  
/hwic.htm  
/hwikzc.htm  
/hwpplmryfip.htm  
/hxane.htm  
/hxm.png  
/hxnbiuax.htm  
/hxsgf.htm  
/hxtgdgynupd.htm  
/hxvt.png  
/hyd.htm  
/hzcvgwgm.htm  
/hze.png  
/ialypa.png  
/ibzb.png  
/icshxsx.htm  
/idvjgd.htm  
/iedrl.htm  
/iegqcze.htm  
/iepthgdcitqh.png  
/iexgqur.png  
/iffy.png  
/ifoemamf.png  
/ifueocb.htm  
/igcdhr.png  
/iggc.htm  
/igp.htm  
/ihthbnojprc.png  
/ibatp.png  
/iikpvs.htm  
/ijfejnbnm.htm  
/ijg.png  
/ijzmni.htm  
/ikbd.htm  
/ikmopdtlovji.png

Malicious DNS Queries, HTTP Traffic, and GET Commands, etc. - Count: 2156

[Back To Top](#)

/iksappvue.htm  
/ilgg.htm  
/ilpy.png  
/imjdgz.htm  
/imnhzrxsjmf.png  
/imoldp.htm  
/impghw.png  
/inb.png  
/inborgy.htm  
/inlxmz.png  
/invcp.png  
/inxnetq.png  
/iokubxjkt.htm  
/ipjnjatu.png  
/ipsbbavtsj.htm  
/ipvj.htm  
/iqj.htm  
/iqjwoe.htm  
/iqmjo.png  
/iqtgzhxbxi.htm  
/irkq.png  
/isqzwukqjo.htm  
/itlmny.png  
/itoyi.htm  
/iueh.png  
/iufbadwstntd.htm  
/iuoqjtckhxag.png  
/iupdygdoss.png  
/iuqwhu.htm  
/iutbue.png  
/iuxq.htm  
/ivmlx.png  
/iwm.png  
/iwrqdpvrvi.htm  
/ixfa.png  
/ixmhhqocuzf.htm  
/ixwkbevrzqug.png  
/iyef.htm  
/iykobat.htm  
/iyytog.htm  
/izeyov.png  
/jayocs.png  
/jaz.png  
/jbfpguope.htm  
/jbsimcccgpj.png  
/jdbzvqqnjx.png  
/jekdrrslogqy.png  
/jevwdzlvspk.png  
/jfmaccxj.htm  
/jfmliildtyp.png  
/jzfyyaon.htm  
/jgkio.htm  
/jglrujzjdwdw.htm  
/jgul.png  
/jhalhdherhi.png  
/jhcpsvxq.png  
/jhjsqe.htm

Malicious DNS Queries, HTTP Traffic, and GET Commands, etc. - Count: 2156

[Back To Top](#)

/jhno.htm  
/jigqc.png  
/jimsryj.png  
/jrxhhsdrq.htm  
/jknonygci.htm  
/jkworrucbpd.png  
/jkxby.png  
/jkyqblfc.htm  
/jlicvsx.png  
/jmb.png  
/jmcr.htm  
/jmepwtz.png  
/jmrilsvmrc.png  
/jmw.png  
/jmxzbt.htm  
/jnbwa.png  
/jnkafj.htm  
/jnnkliyjia.png  
/jooc.htm  
/joxqczyd.htm  
/joxwshjdfed.png  
/jpgid.png  
/jpizcagkk.htm  
/jpm.htm  
/jpoooyndee.htm  
/jpxgvr.htm  
/jpzickjly.htm  
/jqnayszuo.png  
/jqqtkcwbq.png  
/jqzqg.htm  
/jqwfsyqke.png  
/jrafktqqstb.htm  
/jrgzkynm.png  
/jryvgfhzk.png  
/jtf.png  
/jthadpgkku.png  
/jtiowugo.htm  
/jtpbwb.htm  
/jtxuitdu.htm  
/jubovzosnkx.htm  
/jujryquosuu.png  
/jurojqa.png  
/jutranvoraty.png  
/jvc.png  
/jvg.png  
/jvsbsbvc.png  
/jwbbpxgpgyxy.htm  
/jwbdnds.png  
/jwg.htm  
/jwurcpuytnbw.htm  
/jycmrnhowu.png  
/jyrivh.htm  
/kaegtulua.htm  
/kagehvmsxlnp.htm  
/kaqfjqwcm.htm  
/kavlu.htm  
/kbjibbm.htm

Malicious DNS Queries, HTTP Traffic, and GET Commands, etc. - Count: 2156

[Back To Top](#)

/kbmmnfefv.htm  
/kbz.png  
/kcwm.htm  
/kdzsswupuz.htm  
/kebyfbze.htm  
/kehharjak.png  
/keloa.png  
/kenojqnm.png  
/kexvhngzu.htm  
/kezn.png  
/khhkdc.png  
/kiaiukprmue.htm  
/kin.png  
/kiocbrbj.htm  
/kjbkbwogwh.png  
/kkhbqmw.htm  
/kkmoynbpzjqx.png  
/kknpdacpte.png  
/kkrprfvkttep.png  
/kkzf.png  
/klqcdboyg.htm  
/klqxmpnz.png  
/klylsff.png  
/klzwnwhuxj.png  
/kmxdol.htm  
/knnxjeig.htm  
/kob.htm  
/korontljgr.png  
/kqdut.htm  
/kqdyiuvr.htm  
/kqwd.htm  
/kqx.htm  
/krdw.png  
/kltl.png  
/kttewpxadwcs.png  
/kujxvlzy.htm  
/kupuuvbwfktf.png  
/kuxia.htm  
/kvhgsaqbqgz.htm  
/kvkgeapad.png  
/kvpilnoavi.htm  
/kvtmhztakpl.png  
/kwggcozi.htm  
/kwtoxb.png  
/kxobz.png  
/kxue.htm  
/kyklc.htm  
/kyniol.htm  
/kypocihzhaoia.htm  
/kzhktrrtu.htm  
/lbnekb.png  
/lbpxebi.htm  
/lbu.png  
/ldasjp.htm  
/leabwaj.htm  
/lekk.htm  
/lepj.htm

Malicious DNS Queries, HTTP Traffic, and GET Commands, etc. - Count: 2156

[Back To Top](#)

/levwcmiwnbw.png  
/lfcatlrvtj.htm  
/lfrspfjric.png  
/lgcyrxefch.htm  
/lgdjodsdayqq.png  
/lgptc.png  
/lhreot.htm  
/ligzluxqamot.htm  
/liigltx.htm  
/linzlbkqy.png  
/liuueyxfmf.htm  
/ljxznatx.htm  
/ljtzt.htm  
/lkhz.htm  
/lkibyuvpf.htm  
/lkj.png  
/lkyliqnhe.png  
/lxcszbrqi.htm  
/llhwycautt.htm  
/lsezgvozmqn.htm  
/llyll.htm  
/lmgjyh.png  
/lmuhpbsts.htm  
/lnwcr.htm  
/loeynzxxlx.htm  
/loglocpmluj.htm  
/lotgkerjjkg.png  
/loy.png  
/lozlcqswigeq.htm  
/lpbleze.png  
/lqarwjtguljm.png  
/lqco.png  
/lqofmig.htm  
/lqkjpokpfu.png  
/qlitowr.png  
/lrfese.png  
/lrtzffdzsele.png  
/lsfxidgzk.png  
/lsjxtehixe.png  
/ltmm.png  
/ltsh.png  
/lui.png  
/luiqyg.png  
/luk.htm  
/lunivhwqy.htm  
/luwqetxxh.htm  
/lvohnrfa.htm  
/lvwjsafspz.png  
/lvxjgsicvc.png  
/lweo.htm  
/lwzumteflah.png  
/lwpqd.htm  
/lwrmddwkr.htm  
/lwulsjuak.htm  
/lxarrqnc.png  
/lxbhggaq.htm  
/lxlmorqhigv.png

Malicious DNS Queries, HTTP Traffic, and GET Commands, etc. - Count: 2156

[Back To Top](#)

/xltkzlx.png  
/xunt.png  
/yduxft.png  
/lyf.htm  
/lyyiwprdvkn.htm  
/zgjkl.png  
/lzmi.htm  
/lzqmy.htm  
/mamcrxg.png  
/mamypm.htm  
/manoqn.htm  
/mar.htm  
/mbf.htm  
/mbjac.htm  
/mbwwstf.htm  
/mcbiwljyrog.png  
/mcd.htm  
/mcidqfampux.png  
/mcynquojn.png  
/mdr.htm  
/mec.htm  
/mfflfoola.png  
/mfl.png  
/mfmppscolz.png  
/mgibjioiph.htm  
/mibohmfrwggd.htm  
/miomwi.png  
/mipy.htm  
/misnya.htm  
/mixelf.png  
/mjojnnpuf.htm  
/mkbwvweukcq.htm  
/mkcfhsivkiia.png  
/mkxgt.htm  
/mlretjfsv.png  
/mltpbxjkhjy.htm  
/mmacqgbe.htm  
/mmhykrnvqxs.htm  
/mmsl.png  
/mmyakvngdoz.png  
/mnv.png  
/mobiyhms.htm  
/mpeqthchhuh.htm  
/mprue.htm  
/mqnsm.png  
/mqwz.htm  
/mqyyr.png  
/mrcbksgje.htm  
/mrfl.htm  
/mrlljbjwra.htm  
/msogodull.png  
/mtfioxqjg.png  
/mttyqrn.htm  
/mupavwwk.htm  
/mvmmnqaukb.png  
/mwjbfktpfvb.png  
/mwmt.htm

Malicious DNS Queries, HTTP Traffic, and GET Commands, etc. - Count: 2156

[Back To Top](#)

/mwpoq.png  
/mwqkveyl.png  
/mwsuqh.htm  
/mxjfvmykeitq.htm  
/mxlwqonhjyi.htm  
/mxmgnheygik.png  
/myha.png  
/myrt.htm  
/myszwppr.htm  
/myxtacfcwi.png  
/myzuwzvi.htm  
/mzs.htm  
/navunxy.png  
/naw.png  
/nbeayxo.png  
/nbysaoux.png  
/ncpznurpevl.htm  
/ndisfr.png  
/neaapibitxi.png  
/neaswfuon.png  
/necuwd.htm  
/neqp.htm  
/neug.htm  
/newsavdlqsor.png  
/nfmirgctlvpk.png  
/nfouftzfqz.htm  
/nfsnxpj.htm  
/ngjix.htm  
/ngubieo.png  
/nhddcv.htm  
/nhgrfhduir.htm  
/nhtmeiptl.htm  
/nihmaufsovtk.htm  
/nij.png  
/niuxvnraafec.htm  
/njaoxqhoimll.png  
/nkcongltjdr.htm  
/nkxxdowtck.htm  
/nmbldzkzzif.htm  
/nmggnl.htm  
/nmlzss.png  
/nmmdl.htm  
/nmqrzji.htm  
/nmxiapqdykk.htm  
/nmyhxtnbqz.png  
/nnxwuwqauhq.png  
/nnyk.htm  
/nnylpwkfj.htm  
/noniabqh.png  
/noprxxlvz.png  
/nowug.htm  
/nozrcnv.png  
/nqfxd.htm  
/nqjlcxhtpiw.png  
/nrgbwsvprvu.png  
/nrjcw.htm  
/nrr.png

Malicious DNS Queries, HTTP Traffic, and GET Commands, etc. - Count: 2156

[Back To Top](#)

/nryhkrzvo.png  
/nsjhe.htm  
/ntrt.htm  
/nttmyu.htm  
/nwdgqu.png  
/nxcimtchqa.htm  
/nxdmf.png  
/nxmikapbmt.png  
/nysmi.png  
/nzhzwsskpf.htm  
/nzibjl.htm  
/oacdmsz.png  
/oadfek.png  
/obaxfepjgcy.png  
/obb.htm  
/obgaykr.png  
/obkfhbwvpc.htm  
/obq.png  
/obtypbwivw.png  
/oceiadfn.png  
/ocloitvqgejq.png  
/ocwzasqd.htm  
/oczx.htm  
/oddisx.png  
/odhq.htm  
/oduunzweub.htm  
/odz.htm  
/oelxeqc.htm  
/ofbtvv.png  
/ofertmeuzqo.png  
/ogppfxwws.htm  
/ogzrzrgksx.png  
/oheoq.png  
/oipdnbgdwj.htm  
/ojbyoxqukxu.png  
/ojji.htm  
/ojqdwwebo.htm  
/ojwgkhissh.png  
/ojwnv.htm  
/okhujnrtfss.htm  
/okr.png  
/okssddvihnqb.htm  
/oktgt.htm  
/okxvao.png  
/olfagdd.htm  
/olg.png  
/omuax.png  
/oni.png  
/onjlpfmpmhbb.htm  
/ons.png  
/oofds.png  
/oostvgrev.png  
/oozsq.png  
/oposfc.png  
/orfawlgujz.png  
/orjyrg.png  
/osifcjfvawu.png

Malicious DNS Queries, HTTP Traffic, and GET Commands, etc. - Count: 2156

[Back To Top](#)

/osjqu.png  
/otlvq.htm  
/otqrv.png  
/otwvkdndo.htm  
/oudsrnyxv.png  
/ouqh.png  
/ovgj.htm  
/ovjc.htm  
/owio.htm  
/owu.png  
/owwiyxhm.htm  
/oxsatufwv.htm  
/oyg.png  
/pabq.htm  
/paefzwz.htm  
/pagmlfk.png  
/pawwrvryftg.htm  
/pbafk.png  
/pbmebdql.png  
/pbyemgmwuii.htm  
/pccgaezyfy.htm  
/pdkrpkq.htm  
/pdzvlhwu.png  
/pejihnoxz.htm  
/petktojfl.htm  
/pfjzm.png  
/pfpzy.htm  
/pfzdsmkznc.htm  
/pgegwgpfxx.htm  
/pgilljz.htm  
/pgisytj.png  
/pjcqwqbsi.htm  
/pji.htm  
/pkoatxviwk.png  
/pkuxhrq.htm  
/plakwhgcct.png  
/plixki.htm  
/plpvcond.png  
/plpzmotufp.htm  
/pnuycenf.htm  
/poqimgxf.htm  
/poteniuchftz.htm  
/powmbj.png  
/ppeytz.htm  
/ppghgphwtz.png  
/pphctwikryq.htm  
/pplf.htm  
/ppx.htm  
/ppyclx.htm  
/pqhxxvtwe.png  
/preospn.png  
/prtiwwablyia.png  
/psaqdvjuxvfs.png  
/psfy.htm  
/psssrwlrwf.png  
/pstjrv.htm  
/ptnkcma.htm

Malicious DNS Queries, HTTP Traffic, and GET Commands, etc. - Count: 2156

[Back To Top](#)

/puhmknbnfn.htm  
/puiwk.htm  
/pulvfgm.png  
/pung.htm  
/pvelvdhbimc.htm  
/pvpeiinux.htm  
/pwefta.png  
/pwqhvsctyzu.png  
/pxhdwldtxqh.htm  
/pxmdwn.png  
/pxwylez.htm  
/pysf.htm  
/pzmbeim.png  
/pzrk.htm  
/pztbnbuie.htm  
/qachpivzpt.png  
/qacy.htm  
/qawzzlig.png  
/qbd.htm  
/qbivjdrlos.png  
/qcdtvgipzrbo.htm  
/qcg.htm  
/qcgjaymaxn.png  
/qcnujwvj.htm  
/qcnweri.htm  
/qct.png  
/qdhfw.htm  
/qdwwcv.png  
/qegf.htm  
/qepanbldltj.png  
/qfchnvdkldt.htm  
/qfmxdhtzqs.htm  
/qfp.png  
/qfwrn.png  
/qgklhumy.htm  
/qhbqk.htm  
/qhchrdm.png  
/qhsvidjmcvhs.htm  
/qicvtbwd.png  
/qijf.png  
/qjdnmprqu.htm  
/qjjauj.htm  
/qkjfq.htm  
/qkl.png  
/qklmmrjle.png  
/qkuygisyttiy.png  
/qlftwsaw.htm  
/qlizvyw.htm  
/qltkzojqzn.png  
/qmfua.png  
/qmh.htm  
/qmmv.htm  
/qnmgtqh.png  
/qnzjmcvdh.htm  
/qocsg.png  
/qogbaf.png  
/qosoejoixqr.png

Malicious DNS Queries, HTTP Traffic, and GET Commands, etc. - Count: 2156

[Back To Top](#)

/qpdly.htm  
/qphiyesufb.htm  
/qpinvczuujrk.png  
/qpx.png  
/qqfcr.png  
/qqpkauuyqv.png  
/qqwvkvmgd.png  
/qrilm.png  
/qrplf.png  
/qrsjoyzgeyd.htm  
/qrxmdpohj.htm  
/qsa.htm  
/qsvikcij.htm  
/qswjihzlrwgf.htm  
/qtaapdwkum.htm  
/qtcbuyjvr.htm  
/qtjuyzumygl.png  
/qttvazhswkb.htm  
/qubhaoqcnf.png  
/quk.htm  
/quophlqerlr.htm  
/quwwjcxao.htm  
/qvdc.htm  
/qwsvb.png  
/qxxgugadzppd.htm  
/qxthhvio.htm  
/qyjoovyq.htm  
/qymgt.htm  
/qyryqahz.png  
/qzfbuzlqfbdy.png  
/qzg.htm  
/qzkmygvstyob.htm  
/rac.htm  
/rau.png  
/raxnnrdhnqit.htm  
/rbbyljeig.png  
/rbvduipv.htm  
/rbx.htm  
/rbyeh.png  
/rfrovgqveqba.png  
/rhl.png  
/rhpcd.png  
/rhvw.htm  
/rim.htm  
/riqubi.htm  
/rjpwwklav.htm  
/rktsvvugk.htm  
/rkuoxlv.htm  
/rlhthk.png  
/rlynrpbtqvp.png  
/rngyyxc.htm  
/mzkajk.png  
/robjamz.png  
/rocf.png  
/rogtjdjyjt.png  
/rotldjydd.png  
/rpgdutnkxh.png

Malicious DNS Queries, HTTP Traffic, and GET Commands, etc. - Count: 2156

[Back To Top](#)

/rpmhch.htm  
/rpntuudfiy.htm  
/rpzgm.htm  
/rpzrqctj.htm  
/rqhrg.htm  
/rqq.htm  
/rsbdgbzuu.png  
/rshsvxspg.png  
/rsxirkfhr.png  
/rsy.htm  
/ruasaqurvt.png  
/rulxbex.htm  
/ruveuzpaaqfr.png  
/rwfs.htm  
/rwilhsdau.htm  
/rwobllav.htm  
/ryby.htm  
/ryflmetiu.htm  
/ryha.png  
/rzlpoxfwr.htm  
/rzojndzw.htm  
/rzoofissg.htm  
/sakpwamawaz.htm  
/sanhzpcoo.png  
/satiuqpsqux.htm  
/sazsmisjw.htm  
/sbhselm.htm  
/scebxazu.htm  
/sdyczj.png  
/sevzzuttlw.png  
/sglv.png  
/shksltqu.png  
/shlhyr.htm  
/shonpktwjixh.htm  
/shqbwypoj.png  
/shsixrj.png  
/shszy.htm  
/shuxuazvohbe.htm  
/shycn.htm  
/sit.png  
/sjhdwrmpg.png  
/sjk.png  
/skxxln.htm  
/skzpzsqwr.htm  
/slffw.htm  
/slgwjbkc.htm  
/smcizywxh.htm  
/smgemfxj.htm  
/smlic.htm  
/smuohsngile.htm  
/snpgxlvitrcq.htm  
/snswjb.png  
/sokirxmxagi.htm  
/sppiv.png  
/spvhva.htm  
/spzdopxn.htm  
/sqbvxbvvhb.png

Malicious DNS Queries, HTTP Traffic, and GET Commands, etc. - Count: 2156

[Back To Top](#)

/sqwscxdtpo.png  
/srfvczrrsx.png  
/srmxideimbyc.png  
/stum.png  
/suic.htm  
/svexwewqg.png  
/svhb.png  
/sviuawonf.htm  
/swjtlmaq.htm  
/swrptxv.htm  
/swyxruss.png  
/sxgexivabqwq.png  
/sxgnd.htm  
/sxmleuxkao.png  
/sxtdtveks.png  
/sxxj.png  
/syjpedmbm.png  
/syvmxsawo.png  
/taab.png  
/taqblz.png  
/tarn.htm  
/taxdeae.htm  
/tbl.png  
/tbohxmfox.htm  
/tcagli.png  
/tcjwwpuu.htm  
/tclycpn.png  
/tdbwkzkoyes.png  
/tduachlh.png  
/tebiga.htm  
/tequkyxtaf.png  
/terwjpjv.png  
/tevgbqrkb.htm  
/tfjokqstc.htm  
/tfkaaxg.png  
/tfkf.htm  
/tfn.htm  
/tfp.png  
/tfvmwhcavodt.htm  
/tfvwt.png  
/tfxppnk.htm  
/tgqntsaonngj.png  
/tgt.png  
/thkcxywqt.png  
/thmtplvwxmst.htm  
/tht.png  
/tiukprs.htm  
/tjijjys.png  
/tjonmqyfoakn.htm  
/tjxdiwnh.png  
/tjzhrehqtml.png  
/tkhsv.htm  
/tnc.htm  
/tnqzdx.htm  
/tphsnoo.htm  
/tqmxkgrqr.png  
/tqvanovzg.htm

Malicious DNS Queries, HTTP Traffic, and GET Commands, etc. - Count: 2156

[Back To Top](#)

/tropmxlg.png  
/trscvcsbqhg.htm  
/ttdpayofw.htm  
/ttrvcqcfurp.htm  
/ttrvymubpaez.png  
/tudkehbfyoy.png  
/tuialp.htm  
/txmm.png  
/tygipytov.htm  
/tylgvdyldwa.htm  
/tzjappatrkw.png  
/uaftrngeio.htm  
/uairbqqgw.png  
/uasxiwnftn.htm  
/ubspoebhogom.png  
/ubt.png  
/ucessxm.png  
/udgluhaknxi.htm  
/udlueew.htm  
/ufbah.png  
/ufepwdqw.htm  
/ugnfxmeh.png  
/uhepqt.png  
/uhffw.png  
/uhgye.htm  
/uigegou.htm  
/uiws.htm  
/ujbbrcinruv.htm  
/ujhqeewwzya.htm  
/ujkxmpdoo.htm  
/ukzabcl.png  
/ulmkilelnm.htm  
/umfg.png  
/uneq.png  
/unwnn.htm  
/unxztmy.htm  
/uoablj.png  
/uobimpyovaew.htm  
/uolsg.png  
/uoreurcewzj.htm  
/uowwfsgg.png  
/upl.htm  
/uppwcpig.htm  
/uqawqir.png  
/uqrkltnc.htm  
/uqrxoapkc.png  
/uqwkdzmgui.png  
/urcgkjkg.png  
/ushoz.htm  
/uslzwwfwae.htm  
/usnyl.htm  
/utfepi.htm  
/uptyvlgjgy.htm  
/uuyepzvammln.png  
/uva.htm  
/uvjbcwbpvn.htm  
/uweemm.png

Malicious DNS Queries, HTTP Traffic, and GET Commands, etc. - Count: 2156

[Back To Top](#)

/uwlle.htm  
/uxstryitokc.png  
/uxtkzpxxv.htm  
/uzyyogup.htm  
/uzy.png  
/vbbvstihubo.png  
/vbous.htm  
/vbseo.png  
/vbzyoqmpwv.htm  
/vcgctncgxp.htm  
/vdbv.png  
/vdlb.png  
/vdogmxmxi.png  
/vdvrlqlhrr.htm  
/vec.htm  
/veom.png  
/veullzla.htm  
/vfwysexfqh.png  
/vgemqi.png  
/vgyyy.htm  
/vhxazhtezc.htm  
/vhspqdrzx.png  
/viaffyxy.png  
/vijvynktgy.htm  
/vim.png  
/visgquov.png  
/ldhmzul.htm  
/vmfvvtgjfqqx.htm  
/vnfm.png  
/vpnn.htm  
/vpq.png  
/vqbfioad.png  
/vqkauplqub.png  
/vranuo.htm  
/vdrizyzn.htm  
/vsdvmsjppne.png  
/vsk.png  
/vsrbckdvutbm.htm  
/vsxmcjfxto.png  
/vtlyvwb.png  
/ungqotdza.png  
/vwdtlyfin.png  
/vxh.png  
/vxuzjoj.htm  
/vzhatyc.png  
/vzmkv.htm  
/vzq.htm  
/vzuscro.png  
/vzuvsckbtswn.png  
/vzx.htm  
/vzzwtc.png  
/wars.htm  
/wbkd.htm  
/wbnasbgsidi.htm  
/wcq.htm  
/wctmpja.png  
/wcz.htm

Malicious DNS Queries, HTTP Traffic, and GET Commands, etc. - Count: 2156

[Back To Top](#)

/wdrtngb.png  
/wdtrhedii.htm  
/wduumxcp.png  
/wenjkt.png  
/wetr1bp.htm  
/wfki.htm  
/wgiqrdriqx.png  
/wgk.png  
/wg1ck.htm  
/wgmot.png  
/wgqwasal.png  
/wgx.htm  
/wha.htm  
/whb.htm  
/whk.png  
/whnmvdibdeex.png  
/whtmwseqemly.htm  
/wiudm.png  
/wjcjpaie.htm  
/wjnhjbaqhrk.png  
/wkjllaic.png  
/wlcpgdgk.png  
/wlijwqmt.htm  
/wltr.png  
/wmdfcacbnuieg.png  
/wnup.htm  
/wose.png  
/wpbjty.png  
/wphm.htm  
/wpjbrvkedye.png  
/wple.htm  
/wpzaz.png  
/wqhnpzvj.htm  
/wqwe.htm  
/wqzhwmlhweqh.png  
/wqzobpk.png  
/wrh.htm  
/wrhvbpuzejp.htm  
/wrjlyun.htm  
/wsdi.htm  
/wsnjactevtlo.htm  
/wtazblxk.png  
/wtodugqvqk.htm  
/wtpcylrwed.png  
/wtqpbxscsku.htm  
/wtwwffunen.png  
/wtvhvl.png  
/wursvcxvismb.png  
/wvehmpddjpk.htm  
/wvsjnzyiwya.htm  
/wwlgfrggtkty.png  
/wwouexxo.htm  
/wwpdchf.png  
/wwqeyailho.htm  
/wwrtitfuv.htm  
/wwskofz.htm  
/wwwv.png

Malicious DNS Queries, HTTP Traffic, and GET Commands, etc. - Count: 2156

[Back To Top](#)

/wxkif.htm  
/wxiixpgz.htm  
/wxxfwdk.png  
/wywgro.png  
/wzyoufssv.htm  
/xatpnirwmnb.png  
/xavz.png  
/xayxbpga.png  
/xbjisenfozfq.png  
/xbmeokfigtj.htm  
/xbpb.png  
/xbppxeum.png  
/xbur.png  
/xbwxqzshsty.png  
/xcasqxg.htm  
/xcpsynyoj.htm  
/xcpusgnhc.png  
/xdabwjtq.htm  
/xdsuz.htm  
/xdzu.htm  
/xeiskhyaa.htm  
/xeljpzwvyw.htm  
/xenqril.png  
/xepdhorf.htm  
/xer.htm  
/xfkvkj.png  
/xflo.htm  
/xgwtbykrfvse.htm  
/xhcckhodx.htm  
/xhffmbdosz.htm  
/xiogybulxvi.png  
/xizdadtq.png  
/xizmxvgsyzfv.htm  
/xja.htm  
/xjf.png  
/xjj.png  
/xjlelclpjc.htm  
/xjnyhintyab.htm  
/xjsmybped.htm  
/xjsxp.png  
/xjykmzmt.png  
/xkfocgvkezuj.htm  
/xln.png  
/xma.png  
/xmdfetnyky.htm  
/xndxqabq.png  
/xnjjgnw.htm  
/xojqemquhnd.png  
/xotbjild.htm  
/xoz.htm  
/xrjhlxgbu.png  
/xrrjngzqtq.png  
/xrvlgbmujv.png  
/xsf.png  
/xtfjpgqab.htm  
/xtq.png  
/xugeu.png

Malicious DNS Queries, HTTP Traffic, and GET Commands, etc. - Count: 2156

[Back To Top](#)

/xuknlwmb1.png  
/xunhcmi.png  
/xvcovqafaih.htm  
/xvrvsyrzl.htm  
/xvs.htm  
/xvstxpminogb.png  
/xwzfexbypc.png  
/xxcnaxauri.htm  
/xxdmloo.png  
/xxhmfbspck.png  
/xxikjtuc.htm  
/xxk.htm  
/xxwoe.png  
/xyuldo.png  
/xyveesjuikm.png  
/xyybwqxwym.png  
/xzqwfkvu.png  
/yafioen.png  
/yassygw.htm  
/yavwo.htm  
/ybo.png  
/yckaalvrsu.htm  
/ycmwpn.htm  
/ycnwwu.htm  
/ydbpoa.htm  
/ydkcphx.png  
/yee.htm  
/yeku.png  
/yfjh.htm  
/yfnh.png  
/ygjrop.htm  
/yglsspm.png  
/ygzf.png  
/yhbmrk.png  
/yhmablfixae.png  
/yiv.htm  
/yixlfe.htm  
/yiyftzzf.htm  
/yjc.htm  
/yjil.png  
/yjqdylhd.htm  
/yjwqrtnowam.png  
/ykrvtzy.png  
/ykt.png  
/ylefdmntszy.png  
/ylid.htm  
/ylzeqvplrj.png  
/ymbztupyor.htm  
/ynchfvhwz.htm  
/ynjecup.htm  
/ynmwwr.png  
/yog.png  
/ypbs.png  
/ypgdwpkd.png  
/ypqdf.htm  
/yptywuchvd.htm  
/ypxmcglgwz.htm

Malicious DNS Queries, HTTP Traffic, and GET Commands, etc. - Count: 2156

[Back To Top](#)

/ypzvtuibv.htm  
/yqcimee.png  
/yqijcor.png  
/yqwu.png  
/yqyi.htm  
/yrafmyjxee.png  
/yrljxxzy.htm  
/yructa.htm  
/ysfcnkbzz.htm  
/ysjktz.png  
/ysr.htm  
/ysrtpbc.htm  
/ytgzzwlyfit.png  
/ytt.png  
/yupbcgw.png  
/yuvheqk.png  
/yve.htm  
/ywbuuabry.png  
/ywstcvnqhf.htm  
/yxbt.htm  
/yycrs.png  
/yyhjqdn.htm  
/yyj.htm  
/yyulkllmr.htm  
/zabnuv.htm  
/zcaci.htm  
/zccqxrscfmjj.png  
/zcpwe.png  
/zdbn.htm  
/zdjvpkfisu.htm  
/zdyhoq.png  
/zerri.htm  
/zfayvikif.png  
/zfp.htm  
/zfpbezd.htm  
/zfwfmrcebryy.htm  
/zgg.png  
/zgr.htm  
/zidj.png  
/ziyuffgop.htm  
/zjuwaica.png  
/zki.png  
/zlbe.htm  
/zmkgevpkvp.png  
/znjwalhvd.png  
/znksqsgsyjrb.png  
/zod.htm  
/zoemnp.png  
/zor.htm  
/zot.png  
/zoxpeftaka.png  
/zpdcrsagslfh.htm  
/zqdz.png  
/zqlhwhfjmr.htm  
/zqrlga.png  
/zquaptp.htm  
/zqzynu.htm

### Malicious DNS Queries, HTTP Traffic, and GET Commands, etc. - Count: 2156

[Back To Top](#)

/zrccwabqz.htm  
/zrjruo.png  
/zscnlbi.png  
/zslxktmf.htm  
/zta.htm  
/ztorc.png  
/ztr.htm  
/ztx.htm  
/zuhwnhlgzr.htm  
/zukq.png  
/zuvujtaxr.png  
/zvemgv.png  
/zwipvzcbrrz.png  
/zxakok.htm  
/zxgfbuqxwktw.htm  
/zxqnkuzj.htm  
/zxlsle.htm  
/zyag.htm  
/zyain.png  
/zylwsfm.htm  
/zytkwzt.htm  
/zyzgr.htm  
/zzbm.htm  
/zzwobpnpkt.htm

### Potentially Malicious Changes in System Registry File - Count: 3

[Back To Top](#)

#### Data

[system\ControlSet001\Enum\Root\LEGACY\_RDPWD\0000\LogConf]  
[system\ControlSet001\Enum\Root\LEGACY\_TDTCPP\0000\LogConf]  
"ImagePath"="C:\WINDOWS\system32\inertno.exe"

### Potentially Malicious Changes in Software Registry File - Count: 281

[Back To Top](#)

#### Data

"ScheduleId"="S-1-5-21-448539723-2000478354-725345543"  
00  
"LcnStartLocation"="1540223"  
"LcnEndLocation"="1742346"  
[software\Microsoft\Fusion\NativeImagesIndex\v2.0.50727\_32\IL\19693f50]  
[software\Microsoft\Fusion\NativeImagesIndex\v2.0.50727\_32\IL\19693f50\cc73547]  
[software\Microsoft\Fusion\NativeImagesIndex\v2.0.50727\_32\IL\19693f50\cc73547\20]  
[software\Microsoft\Fusion\NativeImagesIndex\v2.0.50727\_32\IL\19693f50\cc73547\20\InvertDependencies]  
"58052d2f\26f5efb3\b"=""  
"476b8f1d\6afda123\10"=""  
"4d8855e2\598d9267\d"=""  
"58052d2f\26f5efb3\b"=""  
"159a66b8\b1a55bd\18"=""  
"64be1fa4\40088d2a\17"=""  
"340dcf4c\2e2a50d1\16"=""  
"f3eb9d9\6a9f89de\15"=""

Potentially Malicious Changes in Software Registry File - Count: 281

[Back To Top](#)

"57d4b1bf\268e3c43\14"=""  
"6f06001f\c92e325\13"=""  
"6eae2d34\36586d98\12"=""  
"7fe99dd6\5c27cbda\19"=""  
"7367db5c\522fbc61\20"=""  
"72522657\14c2e55d\1e"=""  
"476b8f1d\6afda123\10"=""  
"1c22df2f\52628d2e\11"=""  
"7fe99dd6\5c27cbda\19"=""  
"7367db5c\522fbc61\20"=""  
"72522657\14c2e55d\1e"=""  
[software\Microsoft\Fusion\NativeImagesIndex\v2.0.50727\_32\IL\27d9a480]  
[software\Microsoft\Fusion\NativeImagesIndex\v2.0.50727\_32\IL\27d9a480\69e57438]  
[software\Microsoft\Fusion\NativeImagesIndex\v2.0.50727\_32\IL\27d9a480\69e57438\19]  
[software\Microsoft\Fusion\NativeImagesIndex\v2.0.50727\_32\IL\27d9a480\69e57438\19\InvertDependencies]  
"4d885e2\598d9267\d"=""  
"7b22525f\19e52ce4\c"=""  
"58052d2f\26f5efb3\b"=""  
"3c0e944b\83b44cf\1a"=""  
[software\Microsoft\Fusion\NativeImagesIndex\v2.0.50727\_32\IL\2b1a4e4]  
[software\Microsoft\Fusion\NativeImagesIndex\v2.0.50727\_32\IL\2b1a4e4\1d99584f]  
[software\Microsoft\Fusion\NativeImagesIndex\v2.0.50727\_32\IL\2b1a4e4\1d99584f\1d]  
[software\Microsoft\Fusion\NativeImagesIndex\v2.0.50727\_32\IL\2b1a4e4\1d99584f\1d\InvertDependencies]  
"1c22df2f\52628d2e\11"=""  
[software\Microsoft\Fusion\NativeImagesIndex\v2.0.50727\_32\IL\2b351479]  
[software\Microsoft\Fusion\NativeImagesIndex\v2.0.50727\_32\IL\2b351479\69f02adf]  
[software\Microsoft\Fusion\NativeImagesIndex\v2.0.50727\_32\IL\2b351479\69f02adf\28]  
[software\Microsoft\Fusion\NativeImagesIndex\v2.0.50727\_32\IL\2b351479\69f02adf\28\InvertDependencies]  
"7fe99dd6\5c27cbda\19"=""  
"72522657\14c2e55d\1e"=""  
"50a69a2e\3255dcb4\9"=""  
[software\Microsoft\Fusion\NativeImagesIndex\v2.0.50727\_32\IL\2e829ffb]  
[software\Microsoft\Fusion\NativeImagesIndex\v2.0.50727\_32\IL\2e829ffb\32742fa4]  
[software\Microsoft\Fusion\NativeImagesIndex\v2.0.50727\_32\IL\2e829ffb\32742fa4\1a]  
[software\Microsoft\Fusion\NativeImagesIndex\v2.0.50727\_32\IL\2e829ffb\32742fa4\1a\InvertDependencies]  
"f3eb9d9\6a9f89de\15"=""  
"7fe99dd6\5c27cbda\19"=""  
"58052d2f\26f5efb3\b"=""  
"7fe99dd6\5c27cbda\19"=""  
"7367db5c\522fbc61\20"=""  
"72522657\14c2e55d\1e"=""  
[software\Microsoft\Fusion\NativeImagesIndex\v2.0.50727\_32\IL\357ee49a]  
[software\Microsoft\Fusion\NativeImagesIndex\v2.0.50727\_32\IL\357ee49a\14ae5dfb]  
[software\Microsoft\Fusion\NativeImagesIndex\v2.0.50727\_32\IL\357ee49a\14ae5dfb\13]  
[software\Microsoft\Fusion\NativeImagesIndex\v2.0.50727\_32\IL\357ee49a\14ae5dfb\13\InvertDependencies]  
"109d7e79\46399e7e\1e"=""  
[software\Microsoft\Fusion\NativeImagesIndex\v2.0.50727\_32\IL\3a6a696d]  
[software\Microsoft\Fusion\NativeImagesIndex\v2.0.50727\_32\IL\3a6a696d\3469b773]  
[software\Microsoft\Fusion\NativeImagesIndex\v2.0.50727\_32\IL\3a6a696d\3469b773\1b]  
[software\Microsoft\Fusion\NativeImagesIndex\v2.0.50727\_32\IL\3a6a696d\3469b773\1b\InvertDependencies]  
"340dcf4c\2e2a50d1\16"=""  
"f3eb9d9\6a9f89de\15"=""  
"57d4b1bf\268e3c43\14"=""  
"7fe99dd6\5c27cbda\19"=""  
"72522657\14c2e55d\1e"=""  
[software\Microsoft\Fusion\NativeImagesIndex\v2.0.50727\_32\IL\3a70aef]  
[software\Microsoft\Fusion\NativeImagesIndex\v2.0.50727\_32\IL\3a70aef\4f62dc72]

Potentially Malicious Changes in Software Registry File - Count: 281

[Back To Top](#)

[software\Microsoft\Fusion\NativeImagesIndex\v2.0.50727\_32\IL\3a70aef4f62dc72\14]  
[software\Microsoft\Fusion\NativeImagesIndex\v2.0.50727\_32\IL\3a70aef4f62dc72\14\InvertDependencies]  
"4b235cde\1c8f7763\1f"=""  
"57d4b1bf\268e3c43\14"=""  
"6eae2d34\36586d98\12"=""  
[software\Microsoft\Fusion\NativeImagesIndex\v2.0.50727\_32\IL\3c9c8d7b]  
[software\Microsoft\Fusion\NativeImagesIndex\v2.0.50727\_32\IL\3c9c8d7b\253a4b19]  
[software\Microsoft\Fusion\NativeImagesIndex\v2.0.50727\_32\IL\3c9c8d7b\253a4b19\21]  
[software\Microsoft\Fusion\NativeImagesIndex\v2.0.50727\_32\IL\3c9c8d7b\253a4b19\21\InvertDependencies]  
"7fe99dd6\5c27cbda\19"=""  
"4b235cde\1c8f7763\1f"=""  
"1c22df2f\52628d2e\11"=""  
"64be1fa4\40088d2a\17"=""  
"109d7e79\46399e7e\1e"=""  
"57d4b1bf\268e3c43\14"=""  
"476b8f1d\6afda123\10"=""  
"159a66b8\b1a55bd\18"=""  
"340dcf4c\2e2a50d1\16"=""  
"6eae2d34\36586d98\12"=""  
"7fe99dd6\5c27cbda\19"=""  
"7367db5c\522fbc61\20"=""  
"72522657\14c2e55d\1e"=""  
"58052d2f\26f5efb3\1b"=""  
"159a66b8\b1a55bd\18"=""  
"64be1fa4\40088d2a\17"=""  
"6f06001f\c92e325\13"=""  
[software\Microsoft\Fusion\NativeImagesIndex\v2.0.50727\_32\IL\4f99a7c9]  
[software\Microsoft\Fusion\NativeImagesIndex\v2.0.50727\_32\IL\4f99a7c9\14e3164a]  
[software\Microsoft\Fusion\NativeImagesIndex\v2.0.50727\_32\IL\4f99a7c9\14e3164a\1e]  
[software\Microsoft\Fusion\NativeImagesIndex\v2.0.50727\_32\IL\4f99a7c9\14e3164a\1e\InvertDependencies]  
"1c22df2f\52628d2e\11"=""  
[software\Microsoft\Fusion\NativeImagesIndex\v2.0.50727\_32\IL\4fd4b97d]  
[software\Microsoft\Fusion\NativeImagesIndex\v2.0.50727\_32\IL\4fd4b97d\37876d53]  
[software\Microsoft\Fusion\NativeImagesIndex\v2.0.50727\_32\IL\4fd4b97d\37876d53\27]  
[software\Microsoft\Fusion\NativeImagesIndex\v2.0.50727\_32\IL\4fd4b97d\37876d53\27\InvertDependencies]  
"7367db5c\522fbc61\20"=""  
[software\Microsoft\Fusion\NativeImagesIndex\v2.0.50727\_32\IL\5668366c]  
[software\Microsoft\Fusion\NativeImagesIndex\v2.0.50727\_32\IL\5668366c\1b9ff661]  
[software\Microsoft\Fusion\NativeImagesIndex\v2.0.50727\_32\IL\5668366c\1b9ff661\1f]  
[software\Microsoft\Fusion\NativeImagesIndex\v2.0.50727\_32\IL\5668366c\1b9ff661\1f\InvertDependencies]  
"58052d2f\26f5efb3\1b"=""  
"3c0e944b\83b44cf\1a"=""  
"7fe99dd6\5c27cbda\19"=""  
"7367db5c\522fbc61\20"=""  
"72522657\14c2e55d\1e"=""  
[software\Microsoft\Fusion\NativeImagesIndex\v2.0.50727\_32\IL\614f9804]  
[software\Microsoft\Fusion\NativeImagesIndex\v2.0.50727\_32\IL\614f9804\223e4f74]  
[software\Microsoft\Fusion\NativeImagesIndex\v2.0.50727\_32\IL\614f9804\223e4f74\12]  
[software\Microsoft\Fusion\NativeImagesIndex\v2.0.50727\_32\IL\614f9804\223e4f74\12\InvertDependencies]  
"4d8855e2\598d9267\1d"=""  
[software\Microsoft\Fusion\NativeImagesIndex\v2.0.50727\_32\IL\6b98653e]  
[software\Microsoft\Fusion\NativeImagesIndex\v2.0.50727\_32\IL\6b98653e\14c85e3e]  
[software\Microsoft\Fusion\NativeImagesIndex\v2.0.50727\_32\IL\6b98653e\14c85e3e\15]  
[software\Microsoft\Fusion\NativeImagesIndex\v2.0.50727\_32\IL\6b98653e\14c85e3e\15\InvertDependencies]  
"476b8f1d\6afda123\10"=""  
"476b8f1d\6afda123\10"=""  
"58052d2f\26f5efb3\1b"=""

Potentially Malicious Changes in Software Registry File - Count: 281

[Back To Top](#)

"1c22df2f\52628d2e\11"=""  
"64be1fa4\40088d2a\17"=""  
"7fe99dd6\5c27cbda\19"=""  
"7367db5c\522fbc61\20"=""  
"6f06001f\c92e325\13"=""  
"57d4b1bf\268e3c43\14"=""  
"6ae2d34\36586d98\12"=""  
"7fe99dd6\5c27cbda\19"=""  
"72522657\14c2e55d\1e"=""  
"7fe99dd6\5c27cbda\19"=""  
"7367db5c\522fbc61\20"=""  
"1afb76b9\22908e3d\1f"=""  
"476b8f1d\6afda123\10"=""  
"58052d2f\26f5efb3\b"=""  
"1c22df2f\52628d2e\11"=""  
"64be1fa4\40088d2a\17"=""  
"7fe99dd6\5c27cbda\19"=""  
"7367db5c\522fbc61\20"=""  
[software\Microsoft\Fusion\NativeImagesIndex\v2.0.50727\_32\IL\6e8397]  
[software\Microsoft\Fusion\NativeImagesIndex\v2.0.50727\_32\IL\6e8397\746fdbb8]  
[software\Microsoft\Fusion\NativeImagesIndex\v2.0.50727\_32\IL\6e8397\746fdbb8\1c]  
[software\Microsoft\Fusion\NativeImagesIndex\v2.0.50727\_32\IL\6e8397\746fdbb8\1c\InvertDependencies]  
"1c22df2f\52628d2e\11"=""  
"57d4b1bf\268e3c43\14"=""  
[software\Microsoft\Fusion\NativeImagesIndex\v2.0.50727\_32\index1b]  
[software\Microsoft\Fusion\NativeImagesIndex\v2.0.50727\_32\index1c]  
[software\Microsoft\Fusion\NativeImagesIndex\v2.0.50727\_32\NI\109d7e79]  
[software\Microsoft\Fusion\NativeImagesIndex\v2.0.50727\_32\NI\109d7e79\46399e7e]  
[software\Microsoft\Fusion\NativeImagesIndex\v2.0.50727\_32\NI\109d7e79\46399e7e\e]  
"ConfigString"="ZAP--0000-0000"  
00  
[software\Microsoft\Fusion\NativeImagesIndex\v2.0.50727\_32\NI\159a66b8]  
[software\Microsoft\Fusion\NativeImagesIndex\v2.0.50727\_32\NI\159a66b8\b1a55bd]  
[software\Microsoft\Fusion\NativeImagesIndex\v2.0.50727\_32\NI\159a66b8\b1a55bd\18]  
"ConfigString"="ZAP--0000-0000"  
"50a69a2e\3255dcb4\9"=""  
"476b8f1d\6afda123\10"=""  
"4b235cde\1c8f7763\1f"=""  
"109d7e79\46399e7e\le"=""  
"4d8855e2\598d9267\d"=""  
"7b22525f\19e52ce4\c"=""  
"58052d2f\26f5efb3\b"=""  
"3c0e944b\83b44cf\1a"=""  
"1c22df2f\52628d2e\11"=""  
"159a66b8\b1a55bd\18"=""  
"64be1fa4\40088d2a\17"=""  
"340dcf4c\2e2a50d\116"=""  
"f3eb9d9\6a9f89de\15"=""  
"57d4b1bf\268e3c43\14"=""  
"6f06001f\c92e325\13"=""  
"6ae2d34\36586d98\12"=""  
"7fe99dd6\5c27cbda\19"=""  
"7367db5c\522fbc61\20"=""  
"1afb76b9\22908e3d\1f"=""  
"72522657\14c2e55d\1e"=""  
[software\Microsoft\Fusion\NativeImagesIndex\v2.0.50727\_32\NI\1afb76b9]  
[software\Microsoft\Fusion\NativeImagesIndex\v2.0.50727\_32\NI\1afb76b9\22908e3d]

Potentially Malicious Changes in Software Registry File - Count: 281

[Back To Top](#)

```
[software\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\NI\1afb76b9\22908e3d\1f]
"ConfigString"="ZAP--0000-0000"
00
[software\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\NI\1c22df2f]
[software\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\NI\1c22df2f\52628d2e]
[software\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\NI\1c22df2f\52628d2e\11]
"ConfigString"="ZAP--0000-0000"
"476b8f1d\6afda123\10"=""
"4d8855e2\598d9267\d"=""
"58052d2f\26f5efb3\b"=""
"3c0e944b\83b44cf\1a"=""
"1c22df2f\52628d2e\11"=""
"159a66b8\b1a55bd\18"=""
"64be1fa4\40088d2a\17"=""
"340dcf4c\2e2a50d1\16"=""
"f3eb9d9\6a9f89de\15"=""
"57d4b1bf\268e3c43\14"=""
"6f06001f\c92e325\13"=""
"6eae2d34\36586d98\12"=""
"7fe99dd6\5c27cbda\19"=""
"7367db5c\522fbc61\20"=""
"1afb76b9\22908e3d\1f"=""
"72522657\14c2e55d\1e"=""
[software\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\NI\340dcf4c]
[software\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\NI\340dcf4c\2e2a50d1]
[software\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\NI\340dcf4c\2e2a50d1\16]
"ConfigString"="ZAP--0000-0000"
[software\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\NI\3c0e944b]
[software\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\NI\3c0e944b\83b44cf]
[software\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\NI\3c0e944b\83b44cf\1a]
"ConfigString"="ZAP--0000-0000"
[software\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\NI\476b8f1d]
[software\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\NI\476b8f1d\6afda123]
[software\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\NI\476b8f1d\6afda123\10]
"ConfigString"="ZAP--0000-0000"
00
[software\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\NI\4b235cde]
[software\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\NI\4b235cde\1c8f7763]
[software\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\NI\4b235cde\1c8f7763\1f]
"ConfigString"="ZAP--0000-0000"
00
[software\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\NI\4d8855e2]
[software\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\NI\4d8855e2\598d9267]
[software\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\NI\4d8855e2\598d9267\d]
"ConfigString"="ZAP--0000-0000"
[software\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\NI\50a69a2e]
[software\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\NI\50a69a2e\3255dcb4]
[software\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\NI\50a69a2e\3255dcb4\9]
"ConfigString"="ZAP--0000-0000"
00
00
[software\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\NI\57d4b1bf]
[software\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\NI\57d4b1bf\268e3c43]
[software\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\NI\57d4b1bf\268e3c43\14]
"ConfigString"="ZAP--0000-0000"
00
[software\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\NI\58052d2f]
```

### Potentially Malicious Changes in Software Registry File - Count: 281

[Back To Top](#)

```
[software\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\NI\58052d2f26f5efb3]
[software\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\NI\58052d2f26f5efb3\b]
"ConfigString"="ZAP--0000-0000"
[software\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\NI\64be1fa4]
[software\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\NI\64be1fa4\40088d2a]
[software\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\NI\64be1fa4\40088d2a\17]
"ConfigString"="ZAP--0000-0000"
[software\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\NI\6eae2d34]
[software\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\NI\6eae2d34\36586d98]
[software\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\NI\6eae2d34\36586d98\12]
"ConfigString"="ZAP--0000-0000"
[software\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\NI\6f06001f]
[software\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\NI\6f06001fc92e325]
[software\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\NI\6f06001fc92e325\13]
"ConfigString"="ZAP--0000-0000"
[software\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\NI\72522657]
[software\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\NI\72522657\14c2e55d]
[software\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\NI\72522657\14c2e55d\1e]
"ConfigString"="ZAP--0000-0000"
[software\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\NI\7367db5c]
[software\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\NI\7367db5c\522fbc61]
[software\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\NI\7367db5c\522fbc61\20]
"ConfigString"="ZAP--0000-0000"
[software\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\NI\7b22525f]
[software\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\NI\7b22525f\19e52ce4]
[software\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\NI\7b22525f\19e52ce4\c]
"ConfigString"="ZAP--0000-0000"
00
00
[software\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\NI\7fe99dd6]
[software\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\NI\7fe99dd6\5c27cbda]
[software\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\NI\7fe99dd6\5c27cbda\19]
"ConfigString"="ZAP--0000-0000"
[software\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\NI\f3eb9d9]
[software\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\NI\f3eb9d9\6a9f89de]
[software\Microsoft\Fusion\NativeImagesIndex\v2.0.50727_32\NI\f3eb9d9\6a9f89de\15]
"ConfigString"="ZAP--0000-0000"
```

### Potentially Malicious Changes in SAM Registry File - Count: 4

[Back To Top](#)

#### Data

```
[SAM\SAM\Domains\Account\Users\000003F0]
[SAM\SAM\Domains\Account\Users\Names\new1]
@="?"
[SAM\SAM\Domains\BuiltIn\Aliases\Members\S-1-5-21-448539723-2000478354-725345543\000003F0]
```

#### Potentially Malicious Changes in Default Registry File - Count: 5

[Back To Top](#)

**Data**  
"AppData"="C:\\Documents and Settings\\NetworkService\\Application Data"  
"Favorites"=""  
"NetHood"=""  
"Start Menu"=""  
"Templates"=""

#### Potentially Malicious Changes in NTUSER.DAT File - Count: 4

[Back To Top](#)

**Data**  
[NTUSER\\Software\\JavaSoft\\Java Update\\Policy\\JavaFX]  
[NTUSER\\Software\\Microsoft\\Windows\\CurrentVersion\\Explorer\\FileExts\\.pl]  
[NTUSER\\Software\\Microsoft\\Windows\\CurrentVersion\\Explorer\\FileExts\\.pl\\OpenWithProgids]  
"Perl"=hex(0):

If you are interested in your own Sandbox, contact our sales staff @ 1-(888) 256-7425 | Email: sales@netscty.com

This is an automated report provided free of charge, it was generated in part by a custom script and utilizes the following tools:

- The Reusable Malware Analysis Net (Truman\*) server
- Norton Anti-Virus
- Malwarebytes Anti-malware\*
- Sysinternals Tools
- Ngrep
- Tcpdump
- Sed Editor
- Awk
- Volatile Systems Volatility Framework
- SSdeep
- MD5sum
- MS Office
- Adobe Acrobat

If you would like a full forensic examination that would tell you more about how the malware was placed on the system and if additional malicious applications are still there please contact us. In some cases we can determine if data was exfiltrated, but data from your other network devices is sometimes necessary. (example: firewalls and IDS)

Credits:

- TRUMAN: Authored by Mr. Joe Stewart under the General Public License.
- VirusTotal is a service developed by Hispasec Sistemas that analyzes suspicious files and URLs enabling the identification of viruses, worms, trojans and other kinds of malicious content detected by antivirus engines and web analysis toolbars.
- Ngrep: Authored by Jordan Ritter Norton Anti Virus: Product of Symantec Corp.
- Malwarebytes Anti-Malware, Product of Malwarebytes Corporation Windows Sysinternals Tools, Sysinternals was created in 1996 by Mark Russinovich and Bryce Cogswell to host their advanced system utilities and technical information. Microsoft acquired Sysinternals in July, 2006
- Virus Total checks multiple AV products, here is a list of all the AV applications and versions they are currently using. If our report does not show an AV application above, it did not hit on the binary submitted.