INTEZER

Intezer File Scan Report

Malicious, Cerber, 8cc84c910910535990b7ec98b521f7bb84774a78fa488a27dacff5590a7322e3

Analysis Summary

Analysis URL	https://analyze.intezer.com/analyses/fb700d94-ac00-4e02-b8bd-3e7380cf9636
SHA256	8cc84c910910535990b7ec98b521f7bb84774a78fa488a27dacff5590a7322e3
MD5	a57745a30d63f511d28aa43e4b710e1c
SHA1	5985e7d1831784fd15de2cc62451deb16b65b046
Verdict	Malicious
Sub verdict	Malicious
Family	Cerber
Threat description	A prolific ransomware which originally added ".cerber" as a file extension to encrypted files. Has undergone multiple iterations in which the extension has changed. Uses a very readily identifiable set of of UDP activity to checkin and report infections. Primarily uses TOR for payment information.
File type	PE
Indicators	pe, i386, probably_packed
Analyzed at	Tue, 13 Dec 2022 00:33:35 UTC
Report generated at	Wed, 14 Dec 2022 23:16:26 UTC

Genetic Analysis

Genetic Summary

Original file

SHA256	Verdict	Family
8cc84c910910535990b7ec98b521f7bb84774a78fa488a27dacff5590a7322e3	Malicious	Cerber

Memory modules

SHA256	Module path	PID	PPID
968bb0f5db3410078ee54dcaa680672d2d87c66d9a0f9dc5dbd2dd2dcf4740f5	C:\Users\\AppData\Local\Temp\8cc84c910910535990b7ec98.exe	652	3052
41e9aa21f7fc7e6dab2f0185231593b6a4f051f658a00a9eddfc19950db307ca	C:\Users\\AppData\Roaming\{DF0644A9-F350-55D9-1589-647C80D44F82}\TSTheme.exe	2032	652
95977ee6e8e3cfe0f2c07cab0211d462d2cecdab168f38c320ceaada40f7fe7f	C:\Windows\explorer.exe	1464	1344
bbe73e819bd06319cd3e53755516b485f3bd059ff0e1702d01ac36d4e3b06e92	C:\Windows\sysnative\vssadmin.exe	2724	2032
ad90989f9216c86b05dc0f1560c698f52592dd095de779a3400fe251b11cfb06	C:\Windows\SysWOW64\cmd.exe	2000	652
bf801368c0ea748fb2704acd1447b450b621193cbd232586c45012d3ff1317cb	C:\Windows\SysWOW64\taskkill.exe	1528	2000
fd31bfecc6db04eabddc707c2714a3792b6cac95c0ac49f90b85f747fd2256a7	C:\Windows\SysWOW64\PING.EXE	2352	2000
e27f4b16e844551d051937dad2791b8fa07d6ed67f	C:\Windows\sysnative\svchost.exe	2136	488

3c344df92ceefeb6974c92			
a4be9d234b318b9b7f8465f3824824840ff4f4e6c1f82866f1cb16d52cf61bce	C:\Windows\sysnative\svchost.exe	600	488
56dce89bf631721244cec11d4b3550c5ffc84de4e049451498f7a137af72889a	C:\Windows\sysnative\services.exe	488	400

Dropped files

SHA256	Path
8cc84c910910535990b7ec98b521f7bb84774a78fa488a27dacff5590a7322e3	C:\Users\\AppData\Roaming\{DF0644A9-F350-55D9-1589-647C80D44F82}\TSTheme.exe

TTPs

MITRE ATT&CK	Technique	Severity	Details
-	Attempts to delete or modify volume shadow copies	High	-
-	Deletes its original binary from disk	High	-
-	Modifies boot configuration settings	High	disables_system_recovery: Modifies the boot configuration to disable startup recovery, ignorefailures: Modifies the boot configuration to disable Windows error recovery
-	Exhibits behavior characteristic of Cerber ransomware	High	-
Defense Evasion::Modify Registry [T1112]	Creates or sets a registry key to a long series of bytes, possibly to store a binary or malware config	High	regkeyval: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\StartPage2\ProgramsCache
Execution::Native API [T1106]	Created a process from a suspicious location	High	File executed: C:\Users\mike\AppData\Roaming\{DF0644A9-F350-55D9-1589-647C80D44F82}\TSTheme.exe, Commandline executed:
Persistence::Boot or Logon Autostart Execution::Registry Run Keys / Startup Folder [T1547.001]	Installs itself for autorun at Windows startup	High	key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run\TSTheme, data: "C:\Users\mike\AppData\Roaming\{DF0644A9-F350-55D9-1589-647C80D44F82}\TSTheme.exe", key: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce\TSTheme, data: "C:\Users\mike\AppData\Roaming\{DF0644A9-F350-55D9-1589-647C80D44F82}\TSTheme.exe", key: HKEY_CURRENT_USER\Software\Microsoft\Command Processor\AutoRun, data: "C:\Users\mike\AppData\Roaming\{DF0644A9-F350-55D9-1589-647C80D44F82}\TSTheme.exe", file: C:\Users\mike\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\TSTheme.lnk, file: C:\Users\mike\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\TSTheme.lnk
Discovery::Software Discovery::Security Software Discovery [T1518.001]	Attempts to identify installed AV products by installation directory	High	file: C:\Program Files (x86)\avast software, file: C:\Program Files\avast software, file: C:\Program Files (x86)\kaspersky lab, file: C:\Program Files\kaspersky lab, file: C:\Program Files\eset, file: C:\Program Files (x86)\eset, file: C:\Program Files (x86)\bitdefender agent, file: C:\Program Files (x86)\bitdefender, file: C:\Program Files\bitdefender, file: C:\Program Files\bitdefender agent, file: C:\Program Files\arcabit, file: C:\Program Files (x86)\arcabit, file: C:\Program Files (x86)\f-secure, file: C:\Program Files\f-secure, file: C:\Program Files\g data, file: C:\Program Files (x86)\g data, file: C:\Program Files\lavasoft, file: C:\Program

			Files (x86)\lavasoft
-	Creates a copy of itself	High	copy: C:\Users\mike\AppData\Roaming\{DF0644A9-F350-55D9-1589-647C80D44F82}\TSTheme.exe
-	Attempts to modify Explorer settings to prevent hidden files from being displayed	High	-
-	Uses suspicious command line tools or Windows utilities	High	command: /d /c taskkill /f /im "8cc84c910910535990b7ec98.exe" > NUL & ping -n 1 127.0.0.1 > NUL & del "C:\Users\mike\AppData\Local\Temp\8cc84c910910535990b7ec98.exe" > NUL, command: /d /c taskkill /f /im "8cc84c910910535990b7ec98.exe" > NUL & ping -n 1 127.0.0.1 > NUL & del "C:\Users\mike\AppData\Local\Temp\8cc84c910910535990b7ec98.exe" > NUL, command: C:\Windows\system32\cmd.exe /d /c taskkill /f /im "8cc84c910910535990b7ec98.exe" > NUL & ping -n 1 127.0.0.1 > NUL & del "C:\Users\mike\AppData\Local\Temp\8cc84c910910535990b7ec98.exe" > NUL, command: C:\Windows\system32\cmd.exe /d /c taskkill /f /im "8cc84c910910535990b7ec98.exe" > NUL & ping -n 1 127.0.0.1 > NUL & del "C:\Users\mike\AppData\Local\Temp\8cc84c910910535990b7ec98.exe" > NUL, command: "C:\Windows\system32\vssadmin.exe" delete shadows /all /quiet, command: C:\Windows\sysnative\vssadmin.exe delete shadows /all /quiet, command: "C:\Windows\System32\bcdedit.exe" /set {default} recoveryenabled no, command: bcdedit.exe /set {default} recoveryenabled no, command: "C:\Windows\System32\bcdedit.exe" /set {default} bootstatuspolicy ignoreallfailures, command: bcdedit.exe /set {default} bootstatuspolicy ignoreallfailures, command: taskkill /f /im "8cc84c910910535990b7ec98.exe"
-	Guard pages use detected - possible anti-debugging.	Medium	-
-	Reads data out of its own binary image	Medium	self_read: process: 8cc84c910910535990b7ec98.exe, pid: 652, offset: 0x30785c3d6266785c, length: 0x00000005, self_read: process: TSTheme.exe, pid: 2032, offset: 0x30785c3d6266785c, length: 0x00000005
-	A process created a hidden window	Medium	Process: TSTheme.exe -> C:\Windows\sysnative\vssadmin.exe, Process: TSTheme.exe -> C:\Windows\sysnative\wbem\WMIC.exe, Process: TSTheme.exe -> bcdedit.exe, Process: TSTheme.exe -> bcdedit.exe
Execution::Shared Modules [T1129]	Drops a binary and executes it	Medium	binary: C:\Users\mike\AppData\Roaming\{DF0644A9-F350-55D9-1589-647C80D44F82}\TSTheme.exe
-	Bad response status for URL	Medium	-
-	Multiple direct IP connections	Medium	direct_ip_connections: Made direct connections to 513 unique IP addresses
-	HTTP traffic contains suspicious features which may be indicative of malware related traffic	Medium	get_no_useragent: HTTP traffic contains a GET request with no user-agent header, suspicious_request: http://ip-api.com/json
-	Creates an excessive number of UDP connection attempts to external IP addresses	Medium	-
-	Performs some HTTP requests	Medium	url: http://ip-api.com/json

-	Looks up the external IP address	Medium	domain: ip-api.com
-	A ping command was executed with the -n argument possibly to delay analysis	Medium	command: /d /c taskkill /f /im "8cc84c910910535990b7ec98.exe" > NUL & ping -n 1 127.0.0.1 > NUL & del "C:\Users\mike\AppData\Local\Temp\8cc84c910910535990b7ec98.exe" > NUL, command: C:\Windows\system32\cmd.exe /d /c taskkill /f /im "8cc84c910910535990b7ec98.exe" > NUL & ping -n 1 127.0.0.1 > NUL & del "C:\Users\mike\AppData\Local\Temp\8cc84c910910535990b7ec98.exe" > NUL, command: ping -n 1 127.0.0.1, command: C:\Windows\system32\PING.EXE ping -n 1 127.0.0.1
-	Uses Windows utilities for basic functionality	Medium	command: /d /c taskkill /f /im "8cc84c910910535990b7ec98.exe" > NUL & ping -n 1 127.0.0.1 > NUL & del "C:\Users\mike\AppData\Local\Temp\8cc84c910910535990b7ec98.exe" > NUL, command: C:\Windows\system32\cmd.exe /d /c taskkill /f /im "8cc84c910910535990b7ec98.exe" > NUL & ping -n 1 127.0.0.1 > NUL & del "C:\Users\mike\AppData\Local\Temp\8cc84c910910535990b7ec98.exe" > NUL, command: C:\Windows\system32\cmd.exe /d /c taskkill /f /im "8cc84c910910535990b7ec98.exe" > NUL & ping -n 1 127.0.0.1 > NUL & del "C:\Users\mike\AppData\Local\Temp\8cc84c910910535990b7ec98.exe" > NUL, command: "C:\Windows\system32\wbem\wmic.exe" shadowcopy delete, command: "C:\Windows\system32\wbem\wmic.exe" shadowcopy delete, command: C:\Windows\sysnative\wbem\WMIC.exe shadowcopy delete, command: C:\Windows\sysnative\wbem\WMIC.exe shadowcopy delete, command: "C:\Windows\System32\bcdedit.exe" /set {default} recoveryenabled no, command: bcdedit.exe /set {default} recoveryenabled no, command: "C:\Windows\System32\bcdedit.exe" /set {default} bootstatuspolicy ignoreallfailures, command: bcdedit.exe /set {default} bootstatuspolicy ignoreallfailures, command: ping -n 1 127.0.0.1, command: C:\Windows\system32\PING.EXE ping -n 1 127.0.0.1
-	Enumerates user accounts on the system	Low	Process: 8cc84c910910535990b7ec98.exe (652)

IOCs

Network IOCs

Type	IOC	Source type
ip	31.184.235.255	Network communication
ip	31.184.235.254	Network communication
ip	31.184.235.253	Network communication
ip	31.184.235.252	Network communication
ip	31.184.235.251	Network communication
ip	31.184.235.250	Network communication
ip	31.184.235.249	Network communication
ip	31.184.235.248	Network communication
ip	31.184.235.247	Network communication

ip	31.184.235.246	Network communication
ip	31.184.235.245	Network communication
ip	31.184.235.244	Network communication
ip	31.184.235.243	Network communication
ip	31.184.235.242	Network communication
ip	31.184.235.241	Network communication
ip	31.184.235.240	Network communication
ip	31.184.235.239	Network communication
ip	31.184.235.238	Network communication
ip	31.184.235.237	Network communication
ip	31.184.235.236	Network communication
ip	31.184.235.235	Network communication
ip	31.184.235.234	Network communication
ip	31.184.235.233	Network communication
ip	31.184.235.232	Network communication
ip	31.184.235.231	Network communication
ip	31.184.235.230	Network communication
ip	31.184.235.229	Network communication
ip	31.184.235.228	Network communication
ip	31.184.235.227	Network communication
ip	31.184.235.226	Network communication
ip	31.184.235.225	Network communication
ip	31.184.235.224	Network communication
ip	31.184.235.223	Network communication
ip	31.184.235.222	Network communication
ip	31.184.235.221	Network communication
ip	31.184.235.220	Network communication
ip	31.184.235.219	Network communication
ip	31.184.235.218	Network communication
ip	31.184.235.217	Network communication
ip	31.184.235.216	Network communication
ip	31.184.235.215	Network communication
ip	31.184.235.214	Network communication
ip	31.184.235.213	Network communication
ip	31.184.235.212	Network communication
ip	31.184.235.211	Network communication
ip	31.184.235.210	Network communication
ip	31.184.235.209	Network communication
ip	31.184.235.208	Network communication
ip	31.184.235.207	Network communication
ip	31.184.235.206	Network communication
ip	31.184.235.205	Network communication
ip	31.184.235.204	Network communication
ip	31.184.235.203	Network communication
ip	31.184.235.202	Network communication
ip	31.184.235.201	Network communication
ip	31.184.235.200	Network communication

ip	31.184.235.199	Network communication
ip	31.184.235.198	Network communication
ip	31.184.235.197	Network communication
ip	31.184.235.196	Network communication
ip	31.184.235.195	Network communication
ip	31.184.235.194	Network communication
ip	31.184.235.193	Network communication
ip	31.184.235.192	Network communication
ip	31.184.235.191	Network communication
ip	31.184.235.190	Network communication
ip	31.184.235.189	Network communication
ip	31.184.235.188	Network communication
ip	31.184.235.187	Network communication
ip	31.184.235.186	Network communication
ip	31.184.235.185	Network communication
ip	31.184.235.184	Network communication
ip	31.184.235.183	Network communication
ip	31.184.235.182	Network communication
ip	31.184.235.181	Network communication
ip	31.184.235.180	Network communication
ip	31.184.235.179	Network communication
ip	31.184.235.178	Network communication
ip	31.184.235.177	Network communication
ip	31.184.235.176	Network communication
ip	31.184.235.175	Network communication
ip	31.184.235.174	Network communication
ip	31.184.235.173	Network communication
ip	31.184.235.172	Network communication
ip	31.184.235.171	Network communication
ip	31.184.235.170	Network communication
ip	31.184.235.169	Network communication
ip	31.184.235.168	Network communication
ip	31.184.235.167	Network communication
ip	31.184.235.166	Network communication
ip	31.184.235.165	Network communication
ip	31.184.235.164	Network communication
ip	31.184.235.163	Network communication
ip	31.184.235.162	Network communication
ip	31.184.235.161	Network communication
ip	31.184.235.160	Network communication
ip	31.184.235.159	Network communication
ip	31.184.235.158	Network communication
ip	31.184.235.157	Network communication
ip	31.184.235.156	Network communication
ip	31.184.235.155	Network communication
ip	31.184.235.154	Network communication

ip	31.184.235.153	Network communication
ip	31.184.235.152	Network communication
ip	31.184.235.151	Network communication
ip	31.184.235.150	Network communication
ip	31.184.235.149	Network communication
ip	31.184.235.148	Network communication
ip	31.184.235.147	Network communication
ip	31.184.235.146	Network communication
ip	31.184.235.145	Network communication
ip	31.184.235.144	Network communication
ip	31.184.235.143	Network communication
ip	31.184.235.142	Network communication
ip	31.184.235.141	Network communication
ip	31.184.235.140	Network communication
ip	31.184.235.139	Network communication
ip	31.184.235.138	Network communication
ip	31.184.235.137	Network communication
ip	31.184.235.136	Network communication
ip	31.184.235.135	Network communication
ip	31.184.235.134	Network communication
ip	31.184.235.133	Network communication
ip	31.184.235.132	Network communication
ip	31.184.235.131	Network communication
ip	31.184.235.130	Network communication
ip	31.184.235.129	Network communication
ip	31.184.235.128	Network communication
ip	31.184.235.127	Network communication
ip	31.184.235.126	Network communication
ip	31.184.235.125	Network communication
ip	31.184.235.124	Network communication
ip	31.184.235.123	Network communication
ip	31.184.235.122	Network communication
ip	31.184.235.121	Network communication
ip	31.184.235.120	Network communication
ip	31.184.235.119	Network communication
ip	31.184.235.118	Network communication
ip	31.184.235.117	Network communication
ip	31.184.235.116	Network communication
ip	31.184.235.115	Network communication
ip	31.184.235.114	Network communication
ip	31.184.235.113	Network communication
ip	31.184.235.112	Network communication
ip	31.184.235.111	Network communication
ip	31.184.235.110	Network communication
ip	31.184.235.109	Network communication
ip	31.184.235.108	Network communication
ip	31.184.235.107	Network communication

ip	31.184.235.106	Network communication
ip	31.184.235.105	Network communication
ip	31.184.235.104	Network communication
ip	31.184.235.103	Network communication
ip	31.184.235.102	Network communication
ip	31.184.235.101	Network communication
ip	31.184.235.100	Network communication
ip	31.184.235.99	Network communication
ip	31.184.235.98	Network communication
ip	31.184.235.97	Network communication
ip	31.184.235.96	Network communication
ip	31.184.235.95	Network communication
ip	31.184.235.94	Network communication
ip	31.184.235.93	Network communication
ip	31.184.235.92	Network communication
ip	31.184.235.91	Network communication
ip	31.184.235.90	Network communication
ip	31.184.235.89	Network communication
ip	31.184.235.88	Network communication
ip	31.184.235.87	Network communication
ip	31.184.235.86	Network communication
ip	31.184.235.85	Network communication
ip	31.184.235.84	Network communication
ip	31.184.235.83	Network communication
ip	31.184.235.82	Network communication
ip	31.184.235.81	Network communication
ip	31.184.235.80	Network communication
ip	31.184.235.79	Network communication
ip	31.184.235.78	Network communication
ip	31.184.235.77	Network communication
ip	31.184.235.76	Network communication
ip	31.184.235.75	Network communication
ip	31.184.235.74	Network communication
ip	31.184.235.73	Network communication
ip	31.184.235.72	Network communication
ip	31.184.235.71	Network communication
ip	31.184.235.70	Network communication
ip	31.184.235.69	Network communication
ip	31.184.235.68	Network communication
ip	31.184.235.67	Network communication
ip	31.184.235.66	Network communication
ip	31.184.235.65	Network communication
ip	31.184.235.64	Network communication
ip	31.184.235.63	Network communication
ip	31.184.235.62	Network communication
ip	31.184.235.61	Network communication

ip	31.184.235.60	Network communication
ip	31.184.235.59	Network communication
ip	31.184.235.58	Network communication
ip	31.184.235.57	Network communication
ip	31.184.235.56	Network communication
ip	31.184.235.55	Network communication
ip	31.184.235.54	Network communication
ip	31.184.235.53	Network communication
ip	31.184.235.52	Network communication
ip	31.184.235.51	Network communication
ip	31.184.235.50	Network communication
ip	31.184.235.49	Network communication
ip	31.184.235.48	Network communication
ip	31.184.235.47	Network communication
ip	31.184.235.46	Network communication
ip	31.184.235.45	Network communication
ip	31.184.235.44	Network communication
ip	31.184.235.43	Network communication
ip	31.184.235.42	Network communication
ip	31.184.235.41	Network communication
ip	31.184.235.40	Network communication
ip	31.184.235.39	Network communication
ip	31.184.235.38	Network communication
ip	31.184.235.37	Network communication
ip	31.184.235.36	Network communication
ip	31.184.235.35	Network communication
ip	31.184.235.34	Network communication
ip	31.184.235.33	Network communication
ip	31.184.235.32	Network communication
ip	31.184.235.31	Network communication
ip	31.184.235.30	Network communication
ip	31.184.235.29	Network communication
ip	31.184.235.28	Network communication
ip	31.184.235.27	Network communication
ip	31.184.235.26	Network communication
ip	31.184.235.25	Network communication
ip	31.184.235.24	Network communication
ip	31.184.235.23	Network communication
ip	31.184.235.22	Network communication
ip	31.184.235.21	Network communication
ip	31.184.235.20	Network communication
ip	31.184.235.19	Network communication
ip	31.184.235.18	Network communication
ip	31.184.235.17	Network communication
ip	31.184.235.16	Network communication
ip	31.184.235.15	Network communication
ip	31.184.235.14	Network communication

ip	31.184.235.13	Network communication
ip	31.184.235.12	Network communication
ip	31.184.235.11	Network communication
ip	31.184.235.10	Network communication
ip	31.184.235.9	Network communication
ip	31.184.235.8	Network communication
ip	31.184.235.7	Network communication
ip	31.184.235.6	Network communication
ip	31.184.235.5	Network communication
ip	31.184.235.4	Network communication
ip	31.184.235.3	Network communication
ip	31.184.235.2	Network communication
ip	31.184.235.1	Network communication
ip	31.184.235.0	Network communication
ip	31.184.234.255	Network communication
ip	31.184.234.254	Network communication
ip	31.184.234.253	Network communication
ip	31.184.234.252	Network communication
ip	31.184.234.251	Network communication
ip	31.184.234.250	Network communication
ip	31.184.234.249	Network communication
ip	31.184.234.248	Network communication
ip	31.184.234.247	Network communication
ip	31.184.234.246	Network communication
ip	31.184.234.245	Network communication
ip	31.184.234.244	Network communication
ip	31.184.234.243	Network communication
ip	31.184.234.242	Network communication
ip	31.184.234.241	Network communication
ip	31.184.234.240	Network communication
ip	31.184.234.239	Network communication
ip	31.184.234.238	Network communication
ip	31.184.234.237	Network communication
ip	31.184.234.236	Network communication
ip	31.184.234.235	Network communication
ip	31.184.234.234	Network communication
ip	31.184.234.233	Network communication
ip	31.184.234.232	Network communication
ip	31.184.234.231	Network communication
ip	31.184.234.230	Network communication
ip	31.184.234.229	Network communication
ip	31.184.234.228	Network communication
ip	31.184.234.227	Network communication
ip	31.184.234.226	Network communication
ip	31.184.234.225	Network communication
ip	31.184.234.224	Network communication

ip	31.184.234.223	Network communication
ip	31.184.234.222	Network communication
ip	31.184.234.221	Network communication
ip	31.184.234.220	Network communication
ip	31.184.234.219	Network communication
ip	31.184.234.218	Network communication
ip	31.184.234.217	Network communication
ip	31.184.234.216	Network communication
ip	31.184.234.215	Network communication
ip	31.184.234.214	Network communication
ip	31.184.234.213	Network communication
ip	31.184.234.212	Network communication
ip	31.184.234.211	Network communication
ip	31.184.234.210	Network communication
ip	31.184.234.209	Network communication
ip	31.184.234.208	Network communication
ip	31.184.234.207	Network communication
ip	31.184.234.206	Network communication
ip	31.184.234.205	Network communication
ip	31.184.234.204	Network communication
ip	31.184.234.203	Network communication
ip	31.184.234.202	Network communication
ip	31.184.234.201	Network communication
ip	31.184.234.200	Network communication
ip	31.184.234.199	Network communication
ip	31.184.234.198	Network communication
ip	31.184.234.197	Network communication
ip	31.184.234.196	Network communication
ip	31.184.234.195	Network communication
ip	31.184.234.194	Network communication
ip	31.184.234.193	Network communication
ip	31.184.234.192	Network communication
ip	31.184.234.191	Network communication
ip	31.184.234.190	Network communication
ip	31.184.234.189	Network communication
ip	31.184.234.188	Network communication
ip	31.184.234.187	Network communication
ip	31.184.234.186	Network communication
ip	31.184.234.185	Network communication
ip	31.184.234.184	Network communication
ip	31.184.234.183	Network communication
ip	31.184.234.182	Network communication
ip	31.184.234.181	Network communication
ip	31.184.234.180	Network communication
ip	31.184.234.179	Network communication
ip	31.184.234.178	Network communication

ip	31.184.234.177	Network communication
ip	31.184.234.176	Network communication
ip	31.184.234.175	Network communication
ip	31.184.234.174	Network communication
ip	31.184.234.173	Network communication
ip	31.184.234.172	Network communication
ip	31.184.234.171	Network communication
ip	31.184.234.170	Network communication
ip	31.184.234.169	Network communication
ip	31.184.234.168	Network communication
ip	31.184.234.167	Network communication
ip	31.184.234.166	Network communication
ip	31.184.234.165	Network communication
ip	31.184.234.164	Network communication
ip	31.184.234.163	Network communication
ip	31.184.234.162	Network communication
ip	31.184.234.161	Network communication
ip	31.184.234.160	Network communication
ip	31.184.234.159	Network communication
ip	31.184.234.158	Network communication
ip	31.184.234.157	Network communication
ip	31.184.234.156	Network communication
ip	31.184.234.155	Network communication
ip	31.184.234.154	Network communication
ip	31.184.234.153	Network communication
ip	31.184.234.152	Network communication
ip	31.184.234.151	Network communication
ip	31.184.234.150	Network communication
ip	31.184.234.149	Network communication
ip	31.184.234.148	Network communication
ip	31.184.234.147	Network communication
ip	31.184.234.146	Network communication
ip	31.184.234.145	Network communication
ip	31.184.234.144	Network communication
ip	31.184.234.143	Network communication
ip	31.184.234.142	Network communication
ip	31.184.234.141	Network communication
ip	31.184.234.140	Network communication
ip	31.184.234.139	Network communication
ip	31.184.234.138	Network communication
ip	31.184.234.137	Network communication
ip	31.184.234.136	Network communication
ip	31.184.234.135	Network communication
ip	31.184.234.134	Network communication
ip	31.184.234.133	Network communication
ip	31.184.234.132	Network communication
ip	31.184.234.131	Network communication

ip	31.184.234.130	Network communication
ip	31.184.234.129	Network communication
ip	31.184.234.128	Network communication
ip	31.184.234.127	Network communication
ip	31.184.234.126	Network communication
ip	31.184.234.125	Network communication
ip	31.184.234.124	Network communication
ip	31.184.234.123	Network communication
ip	31.184.234.122	Network communication
ip	31.184.234.121	Network communication
ip	31.184.234.120	Network communication
ip	31.184.234.119	Network communication
ip	31.184.234.118	Network communication
ip	31.184.234.117	Network communication
ip	31.184.234.116	Network communication
ip	31.184.234.115	Network communication
ip	31.184.234.114	Network communication
ip	31.184.234.113	Network communication
ip	31.184.234.112	Network communication
ip	31.184.234.111	Network communication
ip	31.184.234.110	Network communication
ip	31.184.234.109	Network communication
ip	31.184.234.108	Network communication
ip	31.184.234.107	Network communication
ip	31.184.234.106	Network communication
ip	31.184.234.105	Network communication
ip	31.184.234.104	Network communication
ip	31.184.234.103	Network communication
ip	31.184.234.102	Network communication
ip	31.184.234.101	Network communication
ip	31.184.234.100	Network communication
ip	31.184.234.99	Network communication
ip	31.184.234.98	Network communication
ip	31.184.234.97	Network communication
ip	31.184.234.96	Network communication
ip	31.184.234.95	Network communication
ip	31.184.234.94	Network communication
ip	31.184.234.93	Network communication
ip	31.184.234.92	Network communication
ip	31.184.234.91	Network communication
ip	31.184.234.90	Network communication
ip	31.184.234.89	Network communication
ip	31.184.234.88	Network communication
ip	31.184.234.87	Network communication
ip	31.184.234.86	Network communication
ip	31.184.234.85	Network communication
ip	31.184.234.84	Network communication

ip	31.184.234.83	Network communication
ip	31.184.234.82	Network communication
ip	31.184.234.81	Network communication
ip	31.184.234.80	Network communication
ip	31.184.234.79	Network communication
ip	31.184.234.78	Network communication
ip	31.184.234.77	Network communication
ip	31.184.234.76	Network communication
ip	31.184.234.75	Network communication
ip	31.184.234.74	Network communication
ip	31.184.234.73	Network communication
ip	31.184.234.72	Network communication
ip	31.184.234.71	Network communication
ip	31.184.234.70	Network communication
ip	31.184.234.69	Network communication
ip	31.184.234.68	Network communication
ip	31.184.234.67	Network communication
ip	31.184.234.66	Network communication
ip	31.184.234.65	Network communication
ip	31.184.234.64	Network communication
ip	31.184.234.63	Network communication
ip	31.184.234.62	Network communication
ip	31.184.234.61	Network communication
ip	31.184.234.60	Network communication
ip	31.184.234.59	Network communication
ip	31.184.234.58	Network communication
ip	31.184.234.57	Network communication
ip	31.184.234.56	Network communication
ip	31.184.234.55	Network communication
ip	31.184.234.54	Network communication
ip	31.184.234.53	Network communication
ip	31.184.234.52	Network communication
ip	31.184.234.51	Network communication
ip	31.184.234.50	Network communication
ip	31.184.234.49	Network communication
ip	31.184.234.48	Network communication
ip	31.184.234.47	Network communication
ip	31.184.234.46	Network communication
ip	31.184.234.45	Network communication
ip	31.184.234.44	Network communication
ip	31.184.234.43	Network communication
ip	31.184.234.42	Network communication
ip	31.184.234.41	Network communication
ip	31.184.234.40	Network communication
ip	31.184.234.39	Network communication
ip	31.184.234.38	Network communication
ip	31.184.234.37	Network communication

ip	31.184.234.36	Network communication
ip	31.184.234.35	Network communication
ip	31.184.234.34	Network communication
ip	31.184.234.33	Network communication
ip	31.184.234.32	Network communication
ip	31.184.234.31	Network communication
ip	31.184.234.30	Network communication
ip	31.184.234.29	Network communication
ip	31.184.234.28	Network communication
ip	31.184.234.27	Network communication
ip	31.184.234.26	Network communication
ip	31.184.234.25	Network communication
ip	31.184.234.24	Network communication
ip	31.184.234.23	Network communication
ip	31.184.234.22	Network communication
ip	31.184.234.21	Network communication
ip	31.184.234.20	Network communication
ip	31.184.234.19	Network communication
ip	31.184.234.18	Network communication
ip	31.184.234.17	Network communication
ip	31.184.234.16	Network communication
ip	31.184.234.15	Network communication
ip	31.184.234.14	Network communication
ip	31.184.234.13	Network communication
ip	31.184.234.12	Network communication
ip	31.184.234.11	Network communication
ip	31.184.234.10	Network communication
ip	31.184.234.9	Network communication
ip	31.184.234.8	Network communication
ip	31.184.234.7	Network communication
ip	31.184.234.6	Network communication
ip	31.184.234.5	Network communication
ip	31.184.234.4	Network communication
ip	31.184.234.3	Network communication
ip	31.184.234.2	Network communication
ip	31.184.234.1	Network communication
ip	31.184.234.0	Network communication
ip	208.95.112.1	Network communication
domain	ip-api.com	Network communication
url	hxxp://ip-api.com/json	Network communication

File IOCs

SHA256	Path	Type	Classification
8cc84c910910535990b7ec98b521f7bb84774a78fa488a27dacff5590a7322e3	8cc84c910910535990b7ec98b521f7bb84774a78fa488a27dacff5590a7322e3	Main file	Malicious , Cerber
8cc84c910910535990b7ec98b	C:\Users\\AppData\Roaming\		

521f7bb84774a78fa488a27dacff5590a7322e3	{DF0644A9-F350-55D9-1589-647C80D44F82}\TSTheme.exe	Dropped file	Malicious , Cerber