MALICIOUS

Classifications: Injector

Threat Names: -

Verdict Reason: -

Sample Type	**Windows DLL (x86-64)**
File Name	**8b971c2c4c9a020eb274c36db20bc0e1b203a7909d63f48f99bef5594110929f.exe.dll**
ID	#968723
MD5	fd6992463689acf855ef55d06a01061a
SHA1	d8b3968a08b12e8ce4b1eec04eb5c86ad910145c
SHA256	8b971c2c4c9a020eb274c36db20bc0e1b203a7909d63f48f99bef5594110929f
File Size	1287.13 KB
Report Created	2021-09-28 10:38 (UTC+2)
Target Environment	win10_64_th2_en_mso2016 | exe

OVERVIEW

VMRay Threat Identifiers (9 rules, 51 matches)

Score	Category	Operation	Count	Classification
4/5	Injection	Writes into the memory of another process	1	Injector
	• (Process #2) giumlol.exe modifies memory of (process #22) svchost.exe.			
2/5	Anti Analysis	Delays execution	1	-
	• (Process #2) giumlol.exe has a thread which sleeps more than 5 minutes.			
1/5	Mutex	Creates mutex	16	-
	• (Process #2) giumlol.exe creates mutex with name "{a4f25aea-0e06-40f9-81b2-53370f3faa31}". • (Process #2) giumlol.exe creates mutex with name "{4b03c46d-9a60-4fba-bdeb-7fc0f42c98fa}". • (Process #4) giumlol.exe creates mutex with name "{a4f25aea-0e06-40f9-81b2-53370f3faa31}". • (Process #4) giumlol.exe creates mutex with name "{4b03c46d-9a60-4fba-bdeb-7fc0f42c98fa}". • (Process #5) giumlol.exe creates mutex with name "{a4f25aea-0e06-40f9-81b2-53370f3faa31}". • (Process #5) giumlol.exe creates mutex with name "{4b03c46d-9a60-4fba-bdeb-7fc0f42c98fa}". • (Process #6) giumlol.exe creates mutex with name "{a4f25aea-0e06-40f9-81b2-53370f3faa31}". • (Process #6) giumlol.exe creates mutex with name "{4b03c46d-9a60-4fba-bdeb-7fc0f42c98fa}". • (Process #7) giumlol.exe creates mutex with name "{a4f25aea-0e06-40f9-81b2-53370f3faa31}". • (Process #7) giumlol.exe creates mutex with name "{4b03c46d-9a60-4fba-bdeb-7fc0f42c98fa}". • (Process #8) giumlol.exe creates mutex with name "{a4f25aea-0e06-40f9-81b2-53370f3faa31}". • (Process #8) giumlol.exe creates mutex with name "{4b03c46d-9a60-4fba-bdeb-7fc0f42c98fa}". • (Process #9) giumlol.exe creates mutex with name "{a4f25aea-0e06-40f9-81b2-53370f3faa31}". • (Process #9) giumlol.exe creates mutex with name "{4b03c46d-9a60-4fba-bdeb-7fc0f42c98fa}". • (Process #10) giumlol.exe creates mutex with name "{a4f25aea-0e06-40f9-81b2-53370f3faa31}". • (Process #10) giumlol.exe creates mutex with name "{4b03c46d-9a60-4fba-bdeb-7fc0f42c98fa}".			
1/5	Discovery	Enumerates running processes	1	-
	• (Process #2) giumlol.exe enumerates running processes.			
1/5	Hide Tracks	Creates process with hidden window	1	-
	• (Process #2) giumlol.exe starts (process #22) svchost.exe with a hidden window.			
1/5	Obfuscation	Reads from memory of another process	1	-
	• (Process #2) giumlol.exe reads from (process #22) svchost.exe.			
1/5	Obfuscation	Creates a page with write and execute permissions	1	-
	• (Process #2) giumlol.exe allocates a page in a foreign process with "PAGE_EXECUTE_READWRITE" permissions, often used to dynamically unpack code.			
1/5	Crash	An unmonitored process crashed	1	-
	• Unmonitored process locationnotificationwindows.exe crashed.			
1/5	Obfuscation	Resolves API functions dynamically	28	-

Score	Category	Operation	Count	Classification
		• (Process #2) giumlol.exe resolves 106 API functions by name. • (Process #3) giumlol.exe resolves 48 API functions by name. • (Process #4) giumlol.exe resolves 50 API functions by name. • (Process #5) giumlol.exe resolves 51 API functions by name. • (Process #6) giumlol.exe resolves 50 API functions by name. • (Process #7) giumlol.exe resolves 51 API functions by name. • (Process #8) giumlol.exe resolves 50 API functions by name. • (Process #9) giumlol.exe resolves 51 API functions by name. • (Process #10) giumlol.exe resolves 51 API functions by name. • (Process #11) giumlol.exe resolves 48 API functions by name. • (Process #12) giumlol.exe resolves 48 API functions by name. • (Process #14) giumlol.exe resolves 48 API functions by name. • (Process #15) giumlol.exe resolves 48 API functions by name. • (Process #17) giumlol.exe resolves 48 API functions by name. • (Process #18) giumlol.exe resolves 48 API functions by name. • (Process #19) giumlol.exe resolves 46 API functions by name. • (Process #20) giumlol.exe resolves 48 API functions by name. • (Process #21) giumlol.exe resolves 48 API functions by name. • (Process #23) giumlol.exe resolves 48 API functions by name. • (Process #24) giumlol.exe resolves 48 API functions by name. • (Process #27) giumlol.exe resolves 46 API functions by name. • (Process #28) giumlol.exe resolves 46 API functions by name. • (Process #29) giumlol.exe resolves 48 API functions by name. • (Process #30) giumlol.exe resolves 46 API functions by name. • (Process #31) giumlol.exe resolves 46 API functions by name. • (Process #32) giumlol.exe resolves 46 API functions by name. • (Process #33) giumlol.exe resolves 46 API functions by name. • (Process #34) giumlol.exe resolves 42 API functions by name.		

Mitre ATT&CK Matrix

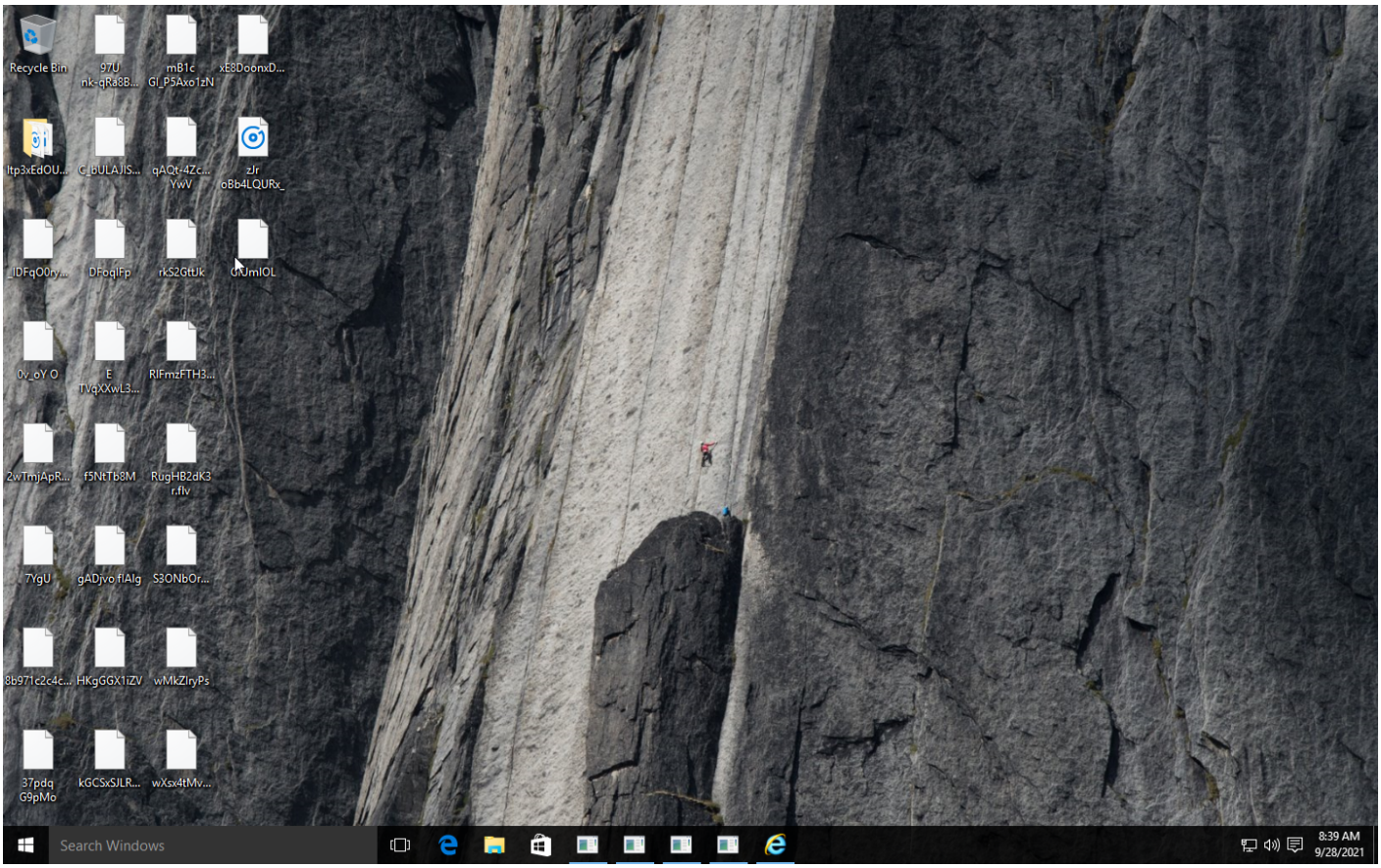
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
				#T1143 Hidden Window		#T1057 Process Discovery					
				#T1045 Software Packing							

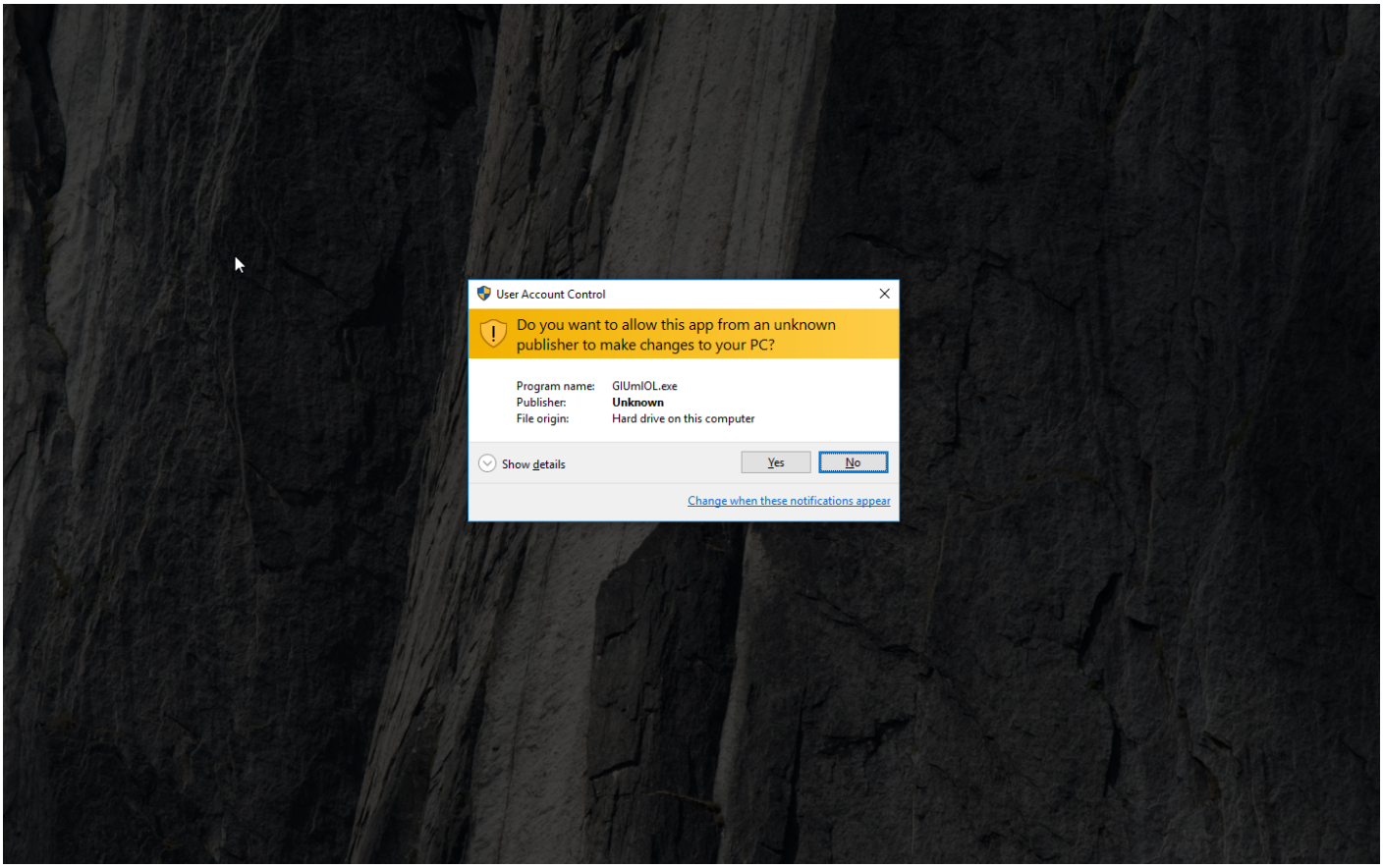
Sample Information

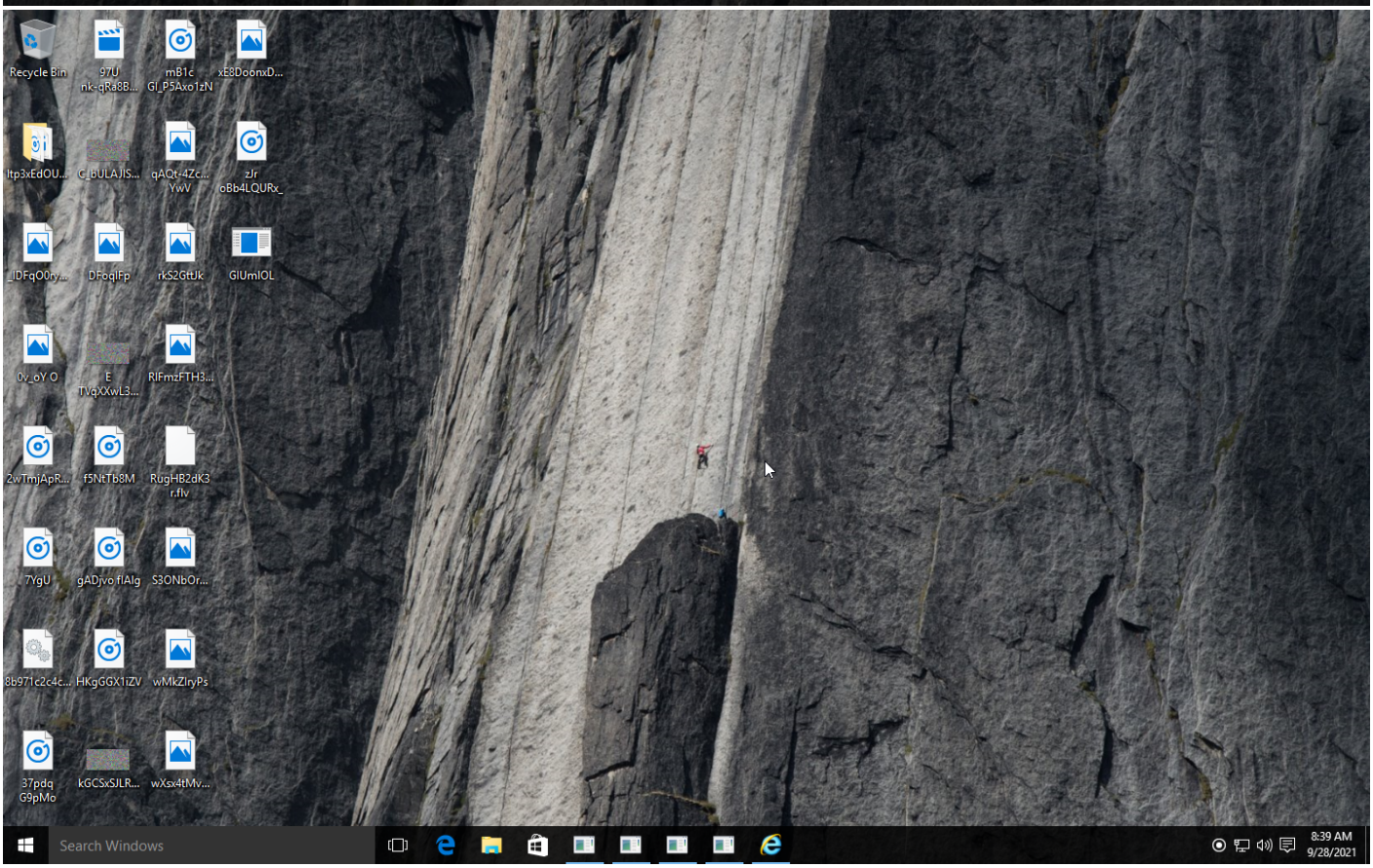
ID	#968723
MD5	fd6992463689acf855ef55d06a01061a
SHA1	d8b3968a08b12e8ce4b1eec04eb5c86ad910145c
SHA256	8b971c2c4c9a020eb274c36db20bc0e1b203a7909d63f48f99bef5594110929f
SSDeep	24576:TqSPG9Jg6TYbmGBtf9efojVpVwKYs1tRCS7SPFL3EOGTWqG5QVEzAJ24GOy2ioLi:TyWbmGBtf9efojVpVwKYs1tR/7SPFL3H
ImpHash	126feacb5b6732ad1a4ed77f47cf4f6d
File Name	8b971c2c4c9a020eb274c36db20bc0e1b203a7909d63f48f99bef5594110929f.exe.dll
File Size	1287.13 KB
Sample Type	Windows DLL (x86-64)
Has Macros	✓

Analysis Information

Creation Time	2021-09-28 10:38 (UTC+2)
Analysis Duration	00:04:00
Termination Reason	Timeout
Number of Monitored Processes	34
Execution Successful	False
Reputation Enabled	✓
WHOIS Enabled	✓
Built-in AV Enabled	✓
Built-in AV Applied On	Sample Files, PCAP File, Downloaded Files, Dropped Files, Modified Files, Memory Dumps, Embedded Files
Number of AV Matches	0
YARA Enabled	✓
YARA Applied On	Sample Files, PCAP File, Downloaded Files, Dropped Files, Modified Files, Memory Dumps, Embedded Files
Number of YARA Matches	0


Recycle Bin
Search Windows
8:39 AM
9/28/2021


User Account Control
Do you want to allow this app from an unknown publisher to make changes to your PC?
Program name: GlUmlOL.exe
Publisher: Unknown
File origin: Hard drive on this computer
Show details
Yes
No
Change when these notifications appear



Screenshots truncated

NETWORK

General

5.98 KB total sent

306.46 KB total received

2 ports 80, 443

3 contacted IP addresses

0 URLs extracted

1 files downloaded

0 malicious hosts detected

DNS

0 DNS requests for 0 domains

0 nameservers contacted

0 total requests returned errors

HTTP/S

41 URLs contacted, 36 servers

36 sessions, 5.98 KB sent, 306.46 KB received

HTTP Requests

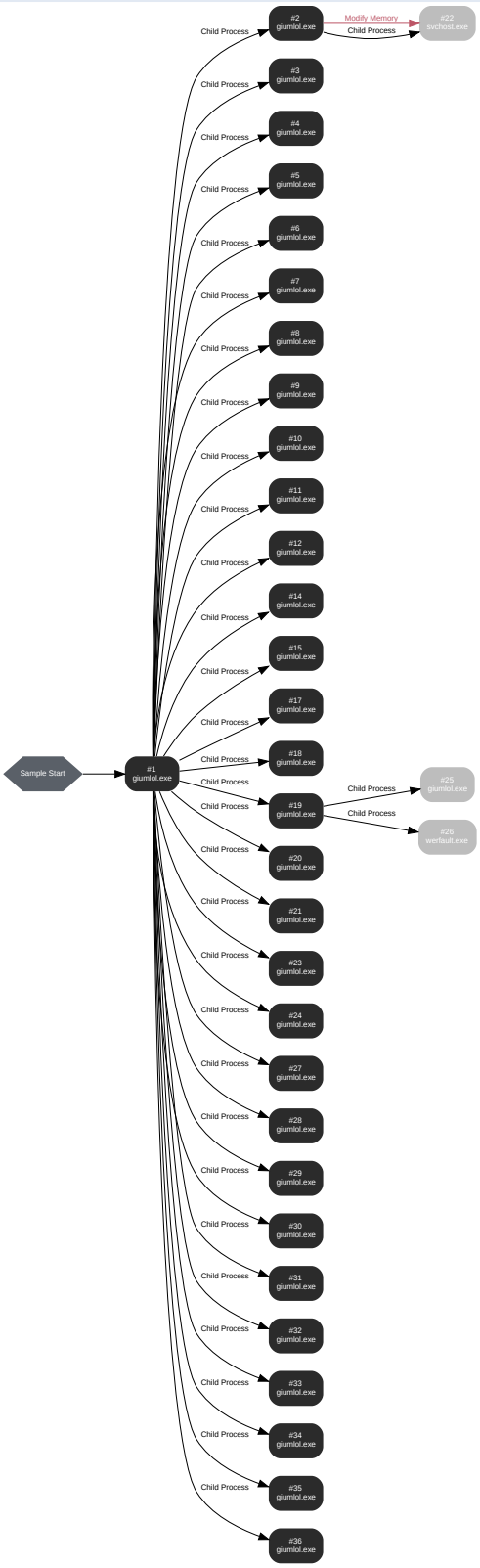
Method	URL	Dest. IP	Dest. Port	Status Code	Response Size	Verdict
GET	https://www.amazon.com/atnDhleS2dVn9jg4ai3l0npisNIdz1euwxjqd/wmiak7dezaeR8p6qawEaa35p4o91zekqTWk/s1chmv1hc1pi37bSehpmg3o4tc1ixYN8o497Cn3u3htafh2q/	-	-		0 bytes	NA
GET	https://161.35.19.83/feed/news/last	-	-		0 bytes	NA
GET	https://microsoft.com/telemetry/update.exe	-	-		0 bytes	NA
GET	https://W@çs//www.yahoo.com/et9pnv4VtdxtJocppt2nvk/74dcv6dl1zrbyvt1tCxqbqkQ9n5fduC34n/sbwau0xc4Msfuyh7Saza3Hnh9tffupmid/cttnluxpkp7q1ky6/z3g2GsyQ63lqdwra5i8GQg1t3Tz21/	-	-		0 bytes	NA
GET	https://ls8ipjtravtuc49zwr2bdf3acun9rmjgfw0icpfct6b/siw7Vl7as32rUbLjh0o2jv9e1bBSatPeffUhimSv5vg3k/jgYrf3t6Hgklfh1tsm3k8hKsi/	-	-		0 bytes	NA
GET	https://pxo/xctzqu6erqnGd7hz3ybybncibifkyxa1fE/	-	-		0 bytes	NA
GET	https://npewnu8xqxnxmz88awiq81vj/WUrqw8ynqtpjblarpucag3zfdaY3ndy5/ozep36uC1orwjn9lnAvqw0oiolI9/pfxkjetnsr83sAvYsloWgTcvzovnhtj6dz35rf/	-	-		0 bytes	NA
GET	https://ðto/qn7rToctHg6cebjiy/	-	-		0 bytes	NA
GET	https://ðßoås//www.yahoo.com/Ekl852qDv9i1hw3g10hp3ip/	-	-		0 bytes	NA
GET	https://ðxo/oe461Eo6H5fecCoxYdfbcYkhhmntHf5n15bahnkk0lnvmU/	-	-		0 bytes	NA
GET	https://¿giïs//www.yahoo.com/h1vwni8luMB2pMqkcswc39bxmoj/	-	-		0 bytes	NA
GET	https://hkwmu3f54yfwkdg2ehv/XB6gef0gXx3mgkgcdasfyviwR0yL1fi/	-	-		0 bytes	NA
GET	https://°qo/3brlOpD0oixs8lqgG17v25wrdFl82law2qwwc/	-	-		0 bytes	NA

Method	URL	Dest. IP	Dest. Port	Status Code	Response Size	Verdict
GET	https://hjxnva1u5w4syy567euoov1v68n72yrpim4tg/gHg8qblf5nvdouaA32i8lt1kr43gh1v73rbwcxiBYOc79x4/6ezrzW2hhS5oylxNGXSieXqxi10hzcb9c8x1d/aGj28dsNT4h23ebm9x8khUAwkchn51ib3g4e6aAbk8tx5va9/	-	-		0 bytes	NA
GET	https://b-ÿ³s//www.yahoo.com/v2tpk6p0lqo2umlxxgyhAsgvLwgc/bWsQjIolF9frut2po7ZOg73b01b5ypb07yn2vb86h5Mrtm/S79p4cjrh6ob26bg7z6geremdj2qnajs81W/49u4kCbl9y5pa1si/	-	-		0 bytes	NA
GET	https://ðzo/nDf6FidRrKk8MzeKsy/	-	-		0 bytes	NA
GET	https://0no/n8t8B1shgvywkanvE2ecrdCyfE6Krj8J0n/	-	-		0 bytes	NA
GET	https://ðxo/1uuy9cJlZtccvp8as2vO814x8H74fd85bjjraCyk8ko/	-	-		0 bytes	NA
GET	https://p# /vjY0hy4muwr1b4cb6Hyecjdl0d5sq4wygmqok94/inkUr2a8MUfwgtwzcD31jPlicy/99iacgPLqPgngqeYhOt3o2zs/44qcimHSv0yu0njdd7mn493xi9mXmdeR089sV8/4DmkixntB2azemrzse/	-	-		0 bytes	NA
GET	https://°nm/94qVnv5yops1culQ2ujxx0s8yfmwh5mDaos8v/ttl6sogo3pw3t43Zsq56pnvd0mnjc/wKES2qes5eqmudus1t3myshruzilivh/HtaZzlHoJkh0xjsG7Hqu0p1z1obhhed2ly9fNmt7qo/	-	-		0 bytes	NA
GET	https://°to/0oashwFumtS3cbsuf/	-	-		0 bytes	NA
GET	https://0no/k4reez13JmrVay3y3uee2879/	-	-		0 bytes	NA
GET	https://ÿ±j»s//www.yahoo.com/lwf41ov1ulo10Kahakx8kt0dhmtVplNXWg6Etefelr4v/	-	-		0 bytes	NA
GET	https://pyo/g8gxeq9drqwefzv1vT6gxU/	-	-		0 bytes	NA
GET	https://lm/9cdvoGy2zYNdvxuT06an2TlxA9/wp1locUeVeSuroipgp9vja32Hlk1rwwj1j/p7Evgdy9d2m27vyvWpmdk7apC08fbffxyT0u0/k2Vqtp9hfufqgcwmU3hvcqvdia85s35hhnKhghhtygfMx2fa/	-	-		0 bytes	NA
GET	https://ðpo/fsQmz3uwqinx0rhyofn9v5U3z2wwj3ix0d8vpwtsy2b4o99/	-	-		0 bytes	NA
GET	https://pwo/a2xmmupuc7dwyiyHx8NP7gsi4kC3fug7dfwnE5gZl/	-	-		0 bytes	NA
GET	https://oìxzs//www.yahoo.com/9l215cV14Ta719pDepto54H2Z/wb205jz69i9fenRL86w4k4k9gsi20Y1tvg4260PuzNt49tJ/ZygwcrWh91jvzOHPzN6kBgN/1ef2ygh926nxm4Qq/	-	-		0 bytes	NA
GET	https://p# /b5bgci33g1ieKv2ueoSs7f8rtotrqQuOt/6n7ezHv48Cz437kibquEA6k1f62w3/6Gg0evnAhn3vk7jype9xYxtpr1i5Ljkyelsu2zr0tWm2sz08/1vQwyJnPr0m55it32kE/p0e0fih0hlzbqCrqAn8Kip384qoolsfb9l6lh2p4ge/	-	-		0 bytes	NA
GET	https://lm/gg71fwreHoY8xrb7xuganudzVq3/abue7jomwIgp1umo12gFj09nbmc2pcbszmC/d8E997c25e8Ci0gjIYimmzs4va2epxx88ho4cok6uzsH/eZus9eeb0aem56BBV58Z1ssU3rv872xqwr4lf920h5bijt/	-	-		0 bytes	NA
GET	https://ppm/Ylc0tgt1szzpsujnwgVjrrrk3R6PH9jg8lzoKdi4/6flO4gzu0of8vowcZdbShtrcSx/v4ow3qd8nrin2dxgrkqk3s7At3opmc33ykh/ZrHpxC9rs8ihX8n4j8r2w0gok2mpji9psa4r9893s46f8qce/	-	-		0 bytes	NA
GET	https://z7¾ys//www.yahoo.com/c8qtrd464ae9yw440vtjxsvuyhrg5aKBq33luwkmWw/Pceg4es1hjg8agrvowyv9r1t4vlkdvavdmm8pqc5l4dhVt/po4bb48bitxm6xbv189oW1iox1w4yZuw7rotZzTgzq69sl/	-	-		0 bytes	NA
GET	https://¦·ees//www.yahoo.com/2fifs1Uo49H9t7jvcp3/km4bjs2wvkfXq7zecvisy2LVcql0vjvPfa/	-	-		0 bytes	NA
GET	https://0uo/p9nsfLg624gyL7bfzr3D2vdzy/	-	-		0 bytes	NA
GET	https://nemi3sj9tghpeh94z1rxo/nKSX8gThsdbev7cZz4Ac6r76rhJwIDdYqfQiSe2w4lmmu8ix/zmX32a0Sg9pn042tQ7pbi511a5qufrasyyWoc5/1gttxegZN63j56eK3ahn7rrhebq5mtvB793oleD5Jw/	-	-		0 bytes	NA

Method	URL	Dest. IP	Dest. Port	Status Code	Response Size	Verdict
GET	https://0no/8hEm9b64xowuht8qltb3rOkedf2i6vs50itj2Liy/	-	-		0 bytes	NA
GET	https://ah6és//www.yahoo.com/4r5wxz1kqypmoo1MtBmtc/yD85X5Bux5w8PIlx5wmddjOg7oioj7r2sqnus1d7/m5eomsa9iaa5yW9lui0Zgz4r02ad0b19cEn8/	-	-		0 bytes	NA
GET	https://7x3wmysggs1wqgn5c8hj2mbldzxp8hvp2e7a4/do4huS54F9akkQpp06zsurvla8/5xkbi4id2foxbqhS/	-	-		0 bytes	NA
GET	https://°oo/qjtkuvyVqj0x3fip7r1nmei2y8vyvuFdkMFpd6o8/	-	-		0 bytes	NA
GET	https://chúùs//www.yahoo.com/vh331gkqUVbayasa4k1ueFqxvj7i07nkrha0/gscqet7rrglscBpm69R7tazkw61xd48J/	-	-		0 bytes	NA
GET	https://à_m/tcbKBlt3vh8qjg5fjIRsp/uBK3vwcbll5qvyywfrga/BhlT4nzhowUM51bj1kgz79tks/xqgny4k7bf9ajWxK5v2hxo23/	-	-		0 bytes	NA

BEHAVIOR

Process Graph



Process #1: giumlol.exe

ID	1
File Name	c:\users\rdhj0cnfevzx\desktop\giumlol.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\GIUmlOL.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8b971c2c4c9a020eb274c36db20bc0e1b203a7909d63f48f99bef5594110929f.exe.dll" /fel="C:\Users\RDHJ0C~1\AppData\Local\Temp\tmpuglwtn31" /s
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 55307, Reason: Analysis Target
Unmonitor End Time	End Time: 297460, Reason: Terminated by Timeout
Monitor duration	242.15s
Return Code	Unknown
PID	3272
Parent PID	1636
Bitness	64 Bit

Host Behavior

Type	Count
Module	14
File	6
Environment	1
Process	31

Process #2: giumlol.exe

ID	2
File Name	c:\users\rdhj0cnfevzx\desktop\giumlol.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\GIUmlOL.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8b971c2c4c9a020eb274c36db20bc0e1b203a7909d63f48f99bef5594110929f.exe.dll" /fn_id=DllRegisterServer
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 75010, Reason: Child Process
Unmonitor End Time	End Time: 297460, Reason: Terminated by Timeout
Monitor duration	222.45s
Return Code	Unknown
PID	964
Parent PID	3272
Bitness	64 Bit

Dropped Files (2)

File Name	File Size	SHA256	YARA Match
C:\Users\RDHJ0C~1\AppData\Local\Temp\5A65.tmp	0 bytes	e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855	✗
-	286.50 KB	6412223cc43f3304f9b03d12e7dddc9de3c5d0f96b148f8007dca61130e788b0	✗

Host Behavior

Type	Count
Module	27195
File	46
System	310
Environment	9
Keyboard	2
Mutex	2
COM	1
Process	374
-	134

Network Behavior

Type	Count
HTTPS	41
TCP	36

Process #3: giumlol.exe

ID	3
File Name	c:\users\rdhj0cnfevzx\desktop\giumlol.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\GIUmlOL.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8b971c2c4c9a020eb274c36db20bc0e1b203a7909d63f48f99bef5594110929f.exe.dll" /fn_id=DllUnregisterServer
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 77150, Reason: Child Process
Unmonitor End Time	End Time: 142882, Reason: Terminated
Monitor duration	65.73s
Return Code	0
PID	1156
Parent PID	3272
Bitness	64 Bit

Host Behavior

Type	Count
Module	178
File	45
Environment	2

Process #4: giumlol.exe

ID	4
File Name	c:\users\rdhj0cnfevzx\desktop\giumlol.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\GIUmlOL.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8b971c2c4c9a020eb274c36db20bc0e1b203a7909d63f48f99bef5594110929f.exe.dll" /fn_id=PauseW
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 79413, Reason: Child Process
Unmonitor End Time	End Time: 107826, Reason: Terminated
Monitor duration	28.41s
Return Code	1
PID	3900
Parent PID	3272
Bitness	64 Bit

Host Behavior

Type	Count
Module	181
File	45
Environment	2
Keyboard	2
Mutex	2

Process #5: giumlol.exe

ID	5
File Name	c:\users\rdhj0cnfevzx\desktop\giumlol.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\GIUmlOL.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8b971c2c4c9a020eb274c36db20bc0e1b203a7909d63f48f99bef5594110929f.exe.dll" /fn_id=ResumeServer
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 82356, Reason: Child Process
Unmonitor End Time	End Time: 110523, Reason: Terminated
Monitor duration	28.17s
Return Code	1
PID	5108
Parent PID	3272
Bitness	64 Bit

Host Behavior

Type	Count
Module	182
File	45
Environment	2
Keyboard	2
Mutex	2

Process #6: giumlol.exe

ID	6
File Name	c:\users\rdhj0cnfevzx\desktop\giumlol.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\GIUmlOL.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8b971c2c4c9a020eb274c36db20bc0e1b203a7909d63f48f99bef5594110929f.exe.dll" /fn_id=ResumeW
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 86104, Reason: Child Process
Unmonitor End Time	End Time: 116309, Reason: Terminated
Monitor duration	30.20s
Return Code	1
PID	4520
Parent PID	3272
Bitness	64 Bit

Host Behavior

Type	Count
Module	181
File	45
Environment	2
Keyboard	2
Mutex	2

Process #7: giumlol.exe

ID	7
File Name	c:\users\rdhj0cnfevzx\desktop\giumlol.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\GIUmlOL.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8b971c2c4c9a020eb274c36db20bc0e1b203a7909d63f48f99bef5594110929f.exe.dll" /fn_id=StartServer
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 91175, Reason: Child Process
Unmonitor End Time	End Time: 127175, Reason: Terminated
Monitor duration	36.00s
Return Code	1
PID	4712
Parent PID	3272
Bitness	64 Bit

Host Behavior

Type	Count
Module	182
File	45
Environment	2
Keyboard	2
Mutex	2

Process #8: giumlol.exe

ID	8
File Name	c:\users\rdhj0cnfevzx\desktop\giumlol.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\GIUmlOL.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8b971c2c4c9a020eb274c36db20bc0e1b203a7909d63f48f99bef5594110929f.exe.dll" /fn_id=StartW
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 95079, Reason: Child Process
Unmonitor End Time	End Time: 132839, Reason: Terminated
Monitor duration	37.76s
Return Code	1
PID	4724
Parent PID	3272
Bitness	64 Bit

Host Behavior

Type	Count
Module	181
File	45
Environment	2
Keyboard	2
Mutex	2

Process #9: giumlol.exe

ID	9
File Name	c:\users\rdhj0cnfevzx\desktop\giumlol.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\GIUmlOL.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8b971c2c4c9a020eb274c36db20bc0e1b203a7909d63f48f99bef5594110929f.exe.dll" /fn_id=StopServer
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 101263, Reason: Child Process
Unmonitor End Time	End Time: 135644, Reason: Terminated
Monitor duration	34.38s
Return Code	1
PID	4744
Parent PID	3272
Bitness	64 Bit

Host Behavior

Type	Count
Module	182
File	45
Environment	2
Keyboard	2
Mutex	2

Process #10: giumlol.exe

ID	10
File Name	c:\users\rdhj0cnfevzx\desktop\giumlol.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\GIUmlOL.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8b971c2c4c9a020eb274c36db20bc0e1b203a7909d63f48f99bef5594110929f.exe.dll" /fn_id=SuspendServer
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 105162, Reason: Child Process
Unmonitor End Time	End Time: 143386, Reason: Terminated
Monitor duration	38.22s
Return Code	1
PID	2876
Parent PID	3272
Bitness	64 Bit

Host Behavior

Type	Count
Module	182
File	45
Environment	2
Keyboard	2
Mutex	2

Process #11: giumlol.exe

ID	11
File Name	c:\users\rdhj0cnfevzx\desktop\giumlol.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\GIUmlOL.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8b971c2c4c9a020eb274c36db20bc0e1b203a7909d63f48f99bef5594110929f.exe.dll" /fn_id=opj_codec_set_threads
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 109984, Reason: Child Process
Unmonitor End Time	End Time: 174568, Reason: Terminated
Monitor duration	64.58s
Return Code	0
PID	3260
Parent PID	3272
Bitness	64 Bit

Host Behavior

Type	Count
Module	178
File	45
Environment	2

Process #12: giumlol.exe

ID	12
File Name	c:\users\rdhj0cnfevzx\desktop\giumlol.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\GIUmlOL.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8b971c2c4c9a020eb274c36db20bc0e1b203a7909d63f48f99bef5594110929f.exe.dll" /fn_id=opj_create_compress
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 116239, Reason: Child Process
Unmonitor End Time	End Time: 215032, Reason: Terminated
Monitor duration	98.79s
Return Code	0
PID	4424
Parent PID	3272
Bitness	64 Bit

Host Behavior

Type	Count
Module	178
File	45
Environment	2

Process #14: giumlol.exe

ID	14
File Name	c:\users\rdhj0cnfevzx\desktop\giumlol.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\GIUmlOL.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8b971c2c4c9a020eb274c36db20bc0e1b203a7909d63f48f99bef5594110929f.exe.dll" /fn_id=opj_create_decompress
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 124841, Reason: Child Process
Unmonitor End Time	End Time: 190181, Reason: Terminated
Monitor duration	65.34s
Return Code	0
PID	4516
Parent PID	3272
Bitness	64 Bit

Host Behavior

Type	Count
Module	178
File	45
Environment	2

Process #15: giumlol.exe

ID	15
File Name	c:\users\rdhj0cnfevzx\desktop\giumlol.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\GIUmlOL.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8b971c2c4c9a020eb274c36db20bc0e1b203a7909d63f48f99bef5594110929f.exe.dll" /fn_id=opj_decode
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 136675, Reason: Child Process
Unmonitor End Time	End Time: 205978, Reason: Terminated
Monitor duration	69.30s
Return Code	0
PID	3400
Parent PID	3272
Bitness	64 Bit

Host Behavior

Type	Count
Module	178
File	45
Environment	2

Process #17: giumlol.exe

ID	17
File Name	c:\users\rdhj0cnfevzx\desktop\giumlol.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\GIUmlOL.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8b971c2c4c9a020eb274c36db20bc0e1b203a7909d63f48f99bef5594110929f.exe.dll" /fn_id=opj_decode_tile_data
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 147993, Reason: Child Process
Unmonitor End Time	End Time: 217034, Reason: Terminated
Monitor duration	69.04s
Return Code	0
PID	4692
Parent PID	3272
Bitness	64 Bit

Host Behavior

Type	Count
Module	178
File	45
Environment	2

Process #18: giumlol.exe

ID	18
File Name	c:\users\rdhj0cnfevzx\desktop\giumlol.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\GIUmlOL.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8b971c2c4c9a020eb274c36db20bc0e1b203a7909d63f48f99bef5594110929f.exe.dll" /fn_id=opj_destroy_codec
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 155171, Reason: Child Process
Unmonitor End Time	End Time: 228466, Reason: Terminated
Monitor duration	73.30s
Return Code	0
PID	4736
Parent PID	3272
Bitness	64 Bit

Host Behavior

Type	Count
Module	178
File	45
Environment	2

Process #19: giumlol.exe

ID	19
File Name	c:\users\rdhj0cnfevzx\desktop\giumlol.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\GIUmlOL.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8b971c2c4c9a020eb274c36db20bc0e1b203a7909d63f48f99bef5594110929f.exe.dll" /fn_id=opj_destroy_cstr_index
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 165292, Reason: Child Process
Unmonitor End Time	End Time: 297460, Reason: Terminated by Timeout
Monitor duration	132.17s
Return Code	Unknown
PID	3228
Parent PID	3272
Bitness	64 Bit

Host Behavior

Type	Count
Module	165
File	45
Environment	2

Process #20: giumlol.exe

ID	20
File Name	c:\users\rdhj0cnfevzx\desktop\giumlol.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\GIUmlOL.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8b971c2c4c9a020eb274c36db20bc0e1b203a7909d63f48f99bef5594110929f.exe.dll" /fn_id=opj_destroy_cstr_info
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 174528, Reason: Child Process
Unmonitor End Time	End Time: 271162, Reason: Terminated
Monitor duration	96.63s
Return Code	0
PID	2488
Parent PID	3272
Bitness	64 Bit

Host Behavior

Type	Count
Module	178
File	45
Environment	2

Process #21: giumlol.exe

ID	21
File Name	c:\users\rdhj0cnfevzx\desktop\giumlol.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\GIUmlOL.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8b971c2c4c9a020eb274c36db20bc0e1b203a7909d63f48f99bef5594110929f.exe.dll" /fn_id=opj_dump_codec
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 181433, Reason: Child Process
Unmonitor End Time	End Time: 276041, Reason: Terminated
Monitor duration	94.61s
Return Code	0
PID	3920
Parent PID	3272
Bitness	64 Bit

Host Behavior

Type	Count
Module	178
File	45
Environment	2

Process #22: svchost.exe

ID	22
File Name	c:\windows\system32\svchost.exe
Command Line	C:\Windows\system32\svchost.exe -k UnistackSvcGroup
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 186384, Reason: Child Process
Unmonitor End Time	End Time: 297460, Reason: Terminated by Timeout
Monitor duration	111.08s
Return Code	Unknown
PID	452
Parent PID	964
Bitness	64 Bit

Injection Information (1)

Injection Type	Source Process	Source / Target TID	Address / Name	Size	Success	Count
Modify Memory	#2: c:\users\rdhj0cnfevzx\desktop\giumlol.exe	0x69c	0x7ff60e670000(140694780313600)	0x400	✓	1

Process #23: giumlol.exe

ID	23
File Name	c:\users\rdhj0cnfevzx\desktop\giumlol.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\GIUmlOL.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8b971c2c4c9a020eb274c36db20bc0e1b203a7909d63f48f99bef5594110929f.exe.dll" /fn_id=opj_encode
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 186684, Reason: Child Process
Unmonitor End Time	End Time: 283186, Reason: Terminated
Monitor duration	96.50s
Return Code	0
PID	3524
Parent PID	3272
Bitness	64 Bit

Host Behavior

Type	Count
Module	178
File	45
Environment	2

Process #24: giumlol.exe

ID	24
File Name	c:\users\rdhj0cnfevzx\desktop\giumlol.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\GIUmlOL.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8b971c2c4c9a020eb274c36db20bc0e1b203a7909d63f48f99bef5594110929f.exe.dll" /fn_id=opj_encoder_set_extra_options
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 191239, Reason: Child Process
Unmonitor End Time	End Time: 287801, Reason: Terminated
Monitor duration	96.56s
Return Code	0
PID	4112
Parent PID	3272
Bitness	64 Bit

Host Behavior

Type	Count
Module	178
File	45
Environment	2

Process #25: giumlol.exe

ID	25
File Name	c:\users\rdhj0cnfevzx\desktop\giumlol.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\GIUmlOL.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8b971c2c4c9a020eb274c36db20bc0e1b203a7909d63f48f99bef5594110929f.exe.dll" /fn_id=opj_destroy_cstr_index
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 193300, Reason: Child Process
Unmonitor End Time	End Time: 297460, Reason: Terminated by Timeout
Monitor duration	104.16s
Return Code	Unknown
PID	4160
Parent PID	3228
Bitness	64 Bit

Process #26: werfault.exe

ID	26
File Name	c:\windows\system32\werfault.exe
Command Line	C:\Windows\system32\WerFault.exe -u -p 3228 -s 408
Initial Working Directory	C:\Windows\system32\
Monitor Start Time	Start Time: 194938, Reason: Child Process
Unmonitor End Time	End Time: 297460, Reason: Terminated by Timeout
Monitor duration	102.52s
Return Code	Unknown
PID	4272
Parent PID	3228
Bitness	64 Bit

Process #27: giumlol.exe

ID	27
File Name	c:\users\rdhj0cnfevzx\desktop\giumlol.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\GIUmlOL.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8b971c2c4c9a020eb274c36db20bc0e1b203a7909d63f48f99bef5594110929f.exe.dll" /fn_id=opj_end_compress
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 200056, Reason: Child Process
Unmonitor End Time	End Time: 297460, Reason: Terminated by Timeout
Monitor duration	97.40s
Return Code	Unknown
PID	4328
Parent PID	3272
Bitness	64 Bit

Host Behavior

Type	Count
Module	165
File	45
Environment	2

Process #28: giumlol.exe

ID	28
File Name	c:\users\rdhj0cnfevzx\desktop\giumlol.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\GIUmlOL.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8b971c2c4c9a020eb274c36db20bc0e1b203a7909d63f48f99bef5594110929f.exe.dll" /fn_id=opj_end_decompress
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 213157, Reason: Child Process
Unmonitor End Time	End Time: 297460, Reason: Terminated by Timeout
Monitor duration	84.30s
Return Code	Unknown
PID	4772
Parent PID	3272
Bitness	64 Bit

Host Behavior

Type	Count
Module	165
File	45
Environment	2

Process #29: giumlol.exe

ID	29
File Name	c:\users\rdhj0cnfevzx\desktop\giumlol.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\GIUmlOL.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8b971c2c4c9a020eb274c36db20bc0e1b203a7909d63f48f99bef5594110929f.exe.dll" /fn_id=opj_get_cstr_index
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 226575, Reason: Child Process
Unmonitor End Time	End Time: 290432, Reason: Terminated
Monitor duration	63.86s
Return Code	0
PID	96
Parent PID	3272
Bitness	64 Bit

Host Behavior

Type	Count
Module	178
File	45
Environment	2

Process #30: giumlol.exe

ID	30
File Name	c:\users\rdhj0cnfevzx\desktop\giumlol.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\GIUmlOL.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8b971c2c4c9a020eb274c36db20bc0e1b203a7909d63f48f99bef5594110929f.exe.dll" /fn_id=opj_get_cstr_info
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 238215, Reason: Child Process
Unmonitor End Time	End Time: 297460, Reason: Terminated by Timeout
Monitor duration	59.24s
Return Code	Unknown
PID	4716
Parent PID	3272
Bitness	64 Bit

Host Behavior

Type	Count
Module	165
File	45
Environment	2

Process #31: giumlol.exe

ID	31
File Name	c:\users\rdhj0cnfevzx\desktop\giumlol.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\GIUmlOL.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8b971c2c4c9a020eb274c36db20bc0e1b203a7909d63f48f99bef5594110929f.exe.dll" /fn_id=opj_get_decoded_tile
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 248046, Reason: Child Process
Unmonitor End Time	End Time: 297460, Reason: Terminated by Timeout
Monitor duration	49.41s
Return Code	Unknown
PID	4568
Parent PID	3272
Bitness	64 Bit

Host Behavior

Type	Count
Module	165
File	45
Environment	2

Process #32: giumlol.exe

ID	32
File Name	c:\users\rdhj0cnfevzx\desktop\giumlol.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\GIUmlOL.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8b971c2c4c9a020eb274c36db20bc0e1b203a7909d63f48f99bef5594110929f.exe.dll" /fn_id=opj_get_num_cpus
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 257917, Reason: Child Process
Unmonitor End Time	End Time: 297460, Reason: Terminated by Timeout
Monitor duration	39.54s
Return Code	Unknown
PID	3256
Parent PID	3272
Bitness	64 Bit

Host Behavior

Type	Count
Module	165
File	45
Environment	2

Process #33: giumlol.exe

ID	33
File Name	c:\users\rdhj0cnfevzx\desktop\giumlol.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\GIUmlOL.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8b971c2c4c9a020eb274c36db20bc0e1b203a7909d63f48f99bef5594110929f.exe.dll" /fn_id=opj_has_thread_support
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 266713, Reason: Child Process
Unmonitor End Time	End Time: 297460, Reason: Terminated by Timeout
Monitor duration	30.75s
Return Code	Unknown
PID	5060
Parent PID	3272
Bitness	64 Bit

Host Behavior

Type	Count
Module	165
File	45
Environment	2

Process #34: giumlol.exe

ID	34
File Name	c:\users\rdhj0cnfevzx\desktop\giumlol.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\GIUmlOL.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8b971c2c4c9a020eb274c36db20bc0e1b203a7909d63f48f99bef5594110929f.exe.dll" /fn_id=opj_image_create
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 275852, Reason: Child Process
Unmonitor End Time	End Time: 297460, Reason: Terminated by Timeout
Monitor duration	21.61s
Return Code	Unknown
PID	5072
Parent PID	3272
Bitness	64 Bit

Host Behavior

Type	Count
Module	111
File	24
Environment	2

Process #35: giumlol.exe

ID	35
File Name	c:\users\rdhj0cnfevzx\desktop\giumlol.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\GIUmlOL.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8b971c2c4c9a020eb274c36db20bc0e1b203a7909d63f48f99bef5594110929f.exe.dll" /fn_id=opj_image_data_alloc
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 287429, Reason: Child Process
Unmonitor End Time	End Time: 297460, Reason: Terminated by Timeout
Monitor duration	10.03s
Return Code	Unknown
PID	4752
Parent PID	3272
Bitness	64 Bit

Host Behavior

Type	Count
Module	31
File	6
Environment	2

Process #36: giumlol.exe

ID	36
File Name	c:\users\rdhj0cnfevzx\desktop\giumlol.exe
Command Line	"C:\Users\RDhJ0CNFevzX\Desktop\GIUmlOL.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8b971c2c4c9a020eb274c36db20bc0e1b203a7909d63f48f99bef5594110929f.exe.dll" /fn_id=opj_image_data_free
Initial Working Directory	C:\Users\RDhJ0CNFevzX\Desktop\
Monitor Start Time	Start Time: 293464, Reason: Child Process
Unmonitor End Time	End Time: 297460, Reason: Terminated by Timeout
Monitor duration	4.00s
Return Code	Unknown
PID	1080
Parent PID	3272
Bitness	64 Bit

Host Behavior

Type	Count
Module	31
File	6
Environment	2

ARTIFACTS

File

SHA256	File Names	Category	File Size	MIME Type	Operations	Verdict
8b971c2c4c9a020eb274c36db20bc0e1b203a7909d63f48f99bef5594110929f	C:\Users\RDhJ0CNFevzX\Desktop\8b971c2c4c9a020eb274c36db20bc0e1b203a7909d63f48f99bef5594110929f.exe.dll	Sample File	1287.13 KB	application/vnd.microsoft.portable-executable	Access	MALICIOUS
c2d814a34b184b7cdf10e4e7a4311ff15db99326d6dd8d328b53bf9e19ccf858	c:\users\rdhj0cnfevzx\appdata\local\microsoft\windows\inetcache\counters.dat	Modified File	128 bytes	application/octet-stream	-	CLEAN
6412223cc43f3304f9b03d12e7dddc9de3c5d0f96b148f8007dca61130e788b0	c:\users\rdhj0cnfevzx\appdata\local\microsoft\windows\inetcache\ie\ma0k5hvd\0otu73hxkl[1]	Downloaded File	286.50 KB	application/octet-stream	-	CLEAN

Filename

File Name	Category	Operations	Verdict
C:\Users\RDhJ0CNFevzX\Desktop\GIUmlOL.exe	Accessed File	Access	CLEAN
C:\Users\RDHJ0C~1\AppData\Local\Temp\tmpuglwtn31	Accessed File	Read, Access	CLEAN
C:\Windows\system32\KERNEL32.DLL	Accessed File	Read, Access	CLEAN
C:\Windows\SYSTEM32\Wininet.dll	Accessed File	Read, Access	CLEAN
C:\Windows\system32\advapi32.dll	Accessed File	Read, Access	CLEAN
C:\Windows\system32\ole32.dll	Accessed File	Read, Access	CLEAN
C:\Windows\SYSTEM32\ntdll.dll	Accessed File	Read, Access	CLEAN
C:\Windows\system32\SHELL32.dll	Accessed File	Read, Access	CLEAN
C:\Windows\SYSTEM32\Bcrypt.dll	Accessed File	Read, Access	CLEAN
C:\Windows\system32\Crypt32.dll	Accessed File	Read, Access	CLEAN
C:\Windows\SYSTEM32\Dnsapi.dll	Accessed File	Read, Access	CLEAN
C:\Windows\system32\Netapi32.dll	Accessed File	Read, Access	CLEAN
C:\Windows\system32\shlwapi.dll	Accessed File	Read, Access	CLEAN
C:\Windows\system32\USER32.dll	Accessed File	Read, Access	CLEAN
C:\Windows\SYSTEM32\KtmW32.dll	Accessed File	Read, Access	CLEAN
C:\Users\RDHJ0C~1\Desktop\8b971c2c4c9a020eb274c36db20bc0e1b203a7909d63f48f99bef5594110929f.exe.dll	Sample File	Access	CLEAN
C:\Users\RDHJ0C~1\AppData\Local\Temp\5A65.tmp	Accessed File	Create, Access	CLEAN

URL

URL	Category	IP Address	Country	HTTP Methods	Verdict
https://www.amazon.com/atnDhleS2dVn9jg4ai3l0npisNldz1euwxjqd/wmiak7dezaeR8p6qawEaa35p4o91zekqTWk/s1chmv1hc1pi37bSehpmg3o4tc1ixYN8o497Cn3u3htafh2q/	-	162.219.225.118	-	GET	CLEAN
https://161.35.19.83/feed/news/last	-	161.35.19.83	-	GET	CLEAN
https://microsoft.com/telemetry/update.exe	-	-	-	GET	CLEAN

URL	Category	IP Address	Country	HTTP Methods	Verdict
https://W@xn--s-5fa//www.yahoo.com/et9pnv4VtdxtJocppt2nvk/74dcv6dl1zrbyvt1tCxqbqkQ9n5fduC34n/sbwau0xc4Msfuyh7Saza3Hnh9tffupmid/cttnluxpkp7q1ky6/z3g2GsyQ63lqdwra5i8GQg1t3Tz21/	-	-	-	GET	CLEAN
https://ls8ipjtravtuc49zwr2bdf3acun9rmjgfw0icpfct6b/siw7Vl7as32rUbLjh0o2jv9e1bBSatPeffUhimSv5vg3k/jgYrf3t6HgklfIh1tsm3k8hKsi/	-	-	-	GET	CLEAN
https://pxo/xctzqu6erqnGd7hz3ybybncibifkyxa1fE/	-	-	-	GET	CLEAN
https://npewnu8xqxnxmz88awiq81vj/WUrqw8ynqtpjblarpucag3zfdaY3ndy5/ozep36uC1orwjn9lnAvqw0oiolI9/pfxkjetnsr83sAvYsloWgTcvzovnhtj6dz35rf/	-	-	-	GET	CLEAN
https://xn--to-vja/qn7rToctHg6cebjiy/	-	-	-	GET	CLEAN
https://xn--os-fiaz6c//www.yahoo.com/Ekl852qDv9i1hw3g10hp3ip/	-	-	-	GET	CLEAN
https://xn--xo-vja/oe461Eo6H5fecCoxYdfbcYkhhmntHf5n15bahnkk0lnvmU/	-	-	-	GET	CLEAN
https://xn--gis-hha6v//www.yahoo.com/h1vwni8luMB2pMqkcswc39bxmoj/	-	-	-	GET	CLEAN
https://hkwmu3f54yfwkdg2ehv/XB6gef0gXx3mgkgcdasfyviwR0yL1fi/	-	-	-	GET	CLEAN
https://xn--qo-eea/3brlOpD0oixs8lqgG17v25wrdFl82law2qwwc/	-	-	-	GET	CLEAN
https://hjxnva1u5w4syy567euoov1v68n72yrpim4tg/gHg8qblf5nvdouaA32i8lt1kr43gh1v73rbwcxiBYOc79x4/6ezrzW2hhS5oylxNGXSieXqxi10hzcb9c8x1d/aGj28dsNT4h23ebm9x8khUAwkchn51ib3g4e6aAbk8tx5va9/	-	-	-	GET	CLEAN
https://xn--b-3s-hsa//www.yahoo.com/v2tpk6p0lqo2umlxxgyhAsgvLwgc/bWsQjIolF9frut2po7ZOg73b01b5ypb07yn2vb86h5Mrtm/S79p4cjrh6ob26bg7z6geremdj2qnajs81W/49u4kCbl9y5pa1si/	-	-	-	GET	CLEAN
https://xn--zo-vja/nDf6FidRrKk8MzeKsy/	-	-	-	GET	CLEAN
https://0no/n8t8B1shgvywkanvE2ecrdCyfE6Krj8J0n/	-	-	-	GET	CLEAN
https://xn--xo-vja/1uuy9cJlZtccvp8as2vO814x8H74fd85bjjraCyk8ko/	-	-	-	GET	CLEAN
https://p#/vjY0hy4muwr1b4cb6Hyecjdl0d5sq4wygmqok94/inkUr2a8MUfwgtwzcD31jPlicy/99iacgPLqPgnggqeYhOt3o2zs/44qcimHSv0yu0njdd7mn493xi9mXmdeR089sV8/4DmkixntB2azemrzse/	-	-	-	GET	CLEAN
https://xn--nm-eea/94qVnv5yops1culQ2ujxx0s8yfmwh5mDaos8v/ttl6sogo3pw3t43Zsq56pnvd0mnjc/wKES2qes5eqmudus1t3myshruzilivh/HtaZzlHoJkh0xjsG7Hqu0p1z1obhhed2ly9fNmt7qo/	-	-	-	GET	CLEAN
https://xn--to-eea/0oashwFumtS3cbsuf/	-	-	-	GET	CLEAN
https://0no/k4reez13JmrVay3y3uee2879/	-	-	-	GET	CLEAN
https://xn--js-hea5b3w//www.yahoo.com/lwf41ov1ulo10Kahakx8kt0dhmtVplNXWg6Etefelr4v/	-	-	-	GET	CLEAN
https://pyo/g8gxeq9drqwefzv1vT6gxU/	-	-	-	GET	CLEAN

URL	Category	IP Address	Country	HTTP Methods	Verdict
https://lm/9cdvoGy2zYNdvxuT06an2TlxA9/wp1IocUeVeSuroipgp9vja32Hlk1rwwj1j/p7Evgdy9d2m27vyvWpmdk7apC08fbffxyT0u0/k2Vqtp9hfufqgcwmU3hvcqvdia85s35hhnKhghhtygfMx2fa/	-	-	-	GET	CLEAN
https://xn--po-vja/fsQmz3uwqinx0rhyofn9v5U3z2wwj3ix0d8vpwtsy2b4o99/	-	-	-	GET	CLEAN
https://pwo/a2xmmupuc7dwyiyHx8NP7gsi4kC3fug7dfwnE5gZl/	-	-	-	GET	CLEAN
https://xn--oxzs-qpa//www.yahoo.com/9l215cV14Ta719pDepto54H2Z/wb205jz69i9fenRL86w4k4k9gsi20Y1tvg4260PuzNt49tJ/ZygwcrWh91jvzOHPzN6kBgN/1ef2ygh926nxm4Qq/	-	-	-	GET	CLEAN
https://p# /b5bgci33g1ieKv2ueoSs7f8rtotrqQuOt/6n7ezHv48Cz437kibquEA6k1f62w3/6Gg0evnAhn3vk7jype9xYxtpr1i5LjkyeIsu2zr0tWm2sz08/1vQwyJnPr0m55it32kE/p0e0fih0hlzbqCrqAn8Kip384qoolsfb9l6lh2p4ge/	-	-	-	GET	CLEAN
https://lm/gg71fwreHoY8xrb7xuganudzVq3/abue7jomwIgp1umo12gFj09nbmc2pcbszmC/d8E997c25e8Ci0gjIYimmzs4va2epxx88ho4cok6uzsH/eZus9eeb0aem56BBV58Z1ssU3rv872xqwr4lf920h5bijt/	-	-	-	GET	CLEAN
https://ppm/Ylc0tgt1szzpsujnwgVjrrrk3R6PH9jg8lzoKdi4/6flO4gzu0of8vowcZdbShtrcSx/v4ow3qd8nrin2dxgrkqk3s7At3opmc33ykh/ZrHpxC9rs8ihX8n4j8r2w0gok2mpji9psa4r9893s46f8qce/	-	-	-	GET	CLEAN
https://xn--z734ys-rq0c//www.yahoo.com/c8qtrd464ae9yw440vtjxsvuyhrg5aKBq33luwkmWw/Pceg4es1hjg8agrvowyv9r1t4vlkdvavdmm8pqc5l4dhVt/po4bb48bitxm6xbv189oW1iox1w4yZuw7rotZzTgzq69sl/	-	-	-	GET	CLEAN
https://xn--ees-mea9f//www.yahoo.com/2fifs1Uo49H9t7jvcp3/km4bjs2wvkfXq7zecvisy2LVcql0vjvPfa/	-	-	-	GET	CLEAN
https://0uo/p9nsfLg624gyL7bfzr3D2vdzy/	-	-	-	GET	CLEAN
https://nemi3sj9tghpeh94z1rxo/nKSX8gThsdbev7cZz4Ac6r76rhJwlDdYqfQiSe2w4lmmu8ix/zmX32a0Sg9pn042tQ7pbi511a5qufrasyyWoc5/1gttxegZN63j56eK3ahn7rrhebq5mtvB793oleD5Jw/	-	-	-	GET	CLEAN
https://0no/8hEm9b64xowuht8qltb3rOkedf2i6vs50itj2Liy/	-	-	-	GET	CLEAN
https://xn--ah6s-dpa//www.yahoo.com/4r5wxz1kqypmoo1MtBmtc/yD85X5Bux5w8PIlx5wmddjOg7oioj7r2sqnus1d7/m5eomsa9iaa5yW9lui0Zgz4r02ad0b19cEn8/	-	-	-	GET	CLEAN
https://7x3wmysggs1wqgn5c8hj2mbldzxp8hvp2e7a4/do4huS54F9akkQpp06zsurvla8/5xkbi4id2foxbqhS/	-	-	-	GET	CLEAN
https://xn--oo-eea/qjtkuvyVqj0x3fip7r1nmei2y8vyvuFdkMFpd6o8/	-	-	-	GET	CLEAN
https://xn--chs-5nae//www.yahoo.com/vh331gkqUVbayasa4k1ueFqxvj7i07nkrha0/gscqet7rrglscBpm69R7tazkw61xd48J/	-	-	-	GET	CLEAN
https://xn--_m-iia/tcbKBlt3vh8qjg5fjlRsp/uBK3vwcbll5qvyywfrga/BhlT4nzhowUM51bj1kgz79tks/xqgny4k7bf9ajWxK5v2hxo23/	-	-	-	GET	CLEAN

Domain

Domain	IP Address	Country	Protocols	Verdict
www.amazon.com	162.219.225.118	-	HTTPS	CLEAN
microsoft.com	-	-	HTTPS	CLEAN
xn--s-5fa	-	-	HTTPS	CLEAN
ls8ipjtravtuc49zwr2bdf3acun9rmjgfw0icpfct6b	-	-	HTTPS	CLEAN
pxo	-	-	HTTPS	CLEAN
npewnu8xqxnxmz88awiq81vj	-	-	HTTPS	CLEAN
xn--to-vja	-	-	HTTPS	CLEAN
xn--os-fiaz6c	-	-	HTTPS	CLEAN
xn--xo-vja	-	-	HTTPS	CLEAN
xn--gis-hha6v	-	-	HTTPS	CLEAN
hkwmu3f54yfwkdg2ehv	-	-	HTTPS	CLEAN
xn--qo-eea	-	-	HTTPS	CLEAN
hjxnva1u5w4syy567euoov1v68n72yrpim4tg	-	-	HTTPS	CLEAN
xn--b-3s-hsa	-	-	HTTPS	CLEAN
xn--zo-vja	-	-	HTTPS	CLEAN
0no	-	-	HTTPS	CLEAN
p	, 162.219.225.118	-	HTTPS	CLEAN
xn--nm-eea	-	-	HTTPS	CLEAN
xn--to-eea	-	-	HTTPS	CLEAN
xn--js-hea5b3w	-	-	HTTPS	CLEAN
pyo	-	-	HTTPS	CLEAN
lm	-	-	HTTPS	CLEAN
xn--po-vja	-	-	HTTPS	CLEAN
pwo	-	-	HTTPS	CLEAN
xn--oxzs-qpa	-	-	HTTPS	CLEAN
ppm	-	-	HTTPS	CLEAN
xn--z734ys-rq0c	-	-	HTTPS	CLEAN
xn--ees-mea9f	-	-	HTTPS	CLEAN
0uo	-	-	HTTPS	CLEAN
nemi3sj9tghpeh94z1rxo	-	-	HTTPS	CLEAN
xn--ah6s-dpa	-	-	HTTPS	CLEAN
7x3wmysggs1wqgn5c8hj2mbldzxp8hvp2e7a4	-	-	HTTPS	CLEAN
xn--oo-eea	-	-	HTTPS	CLEAN
xn--chs-5nae	-	-	HTTPS	CLEAN
xn--_m-iia	-	-	HTTPS	CLEAN

IP

IP Address	Domains	Country	Protocols	Verdict
162.219.225.118	www.amazon.com, www-amazon-com.customer.fastly.net, tp.47cf2c8c9-frontier.amazon.com	United States	DNS, HTTPS, TCP	CLEAN
161.35.19.83	-	Germany	HTTPS, TCP	CLEAN

Mutex

Name	Operations	Parent Process Name	Verdict
{a4f25aea-0e06-40f9-81b2-53370f3faa31}	access	giumlol.exe	CLEAN
{4b03c46d-9a60-4fba-bdeb-7fc0f42c98fa}	access	giumlol.exe	CLEAN

Process

Process Name	Commandline	Verdict
giumlol.exe	"C:\Users\RDhJ0CNFevzX\Desktop\GIUmlOL.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8b971c2c4c9a020eb274c36db20bc0e1b203a7909d63f48f99bef5594110929f.exe.dll" /fel="C:\Users\RDHJ0C~1\AppData\Local\Temp\tmpuglwtn31" /s	CLEAN
giumlol.exe	"C:\Users\RDhJ0CNFevzX\Desktop\GIUmlOL.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8b971c2c4c9a020eb274c36db20bc0e1b203a7909d63f48f99bef5594110929f.exe.dll" /fn_id=DllRegisterServer	CLEAN
giumlol.exe	"C:\Users\RDhJ0CNFevzX\Desktop\GIUmlOL.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8b971c2c4c9a020eb274c36db20bc0e1b203a7909d63f48f99bef5594110929f.exe.dll" /fn_id=DllUnregisterServer	CLEAN
giumlol.exe	"C:\Users\RDhJ0CNFevzX\Desktop\GIUmlOL.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8b971c2c4c9a020eb274c36db20bc0e1b203a7909d63f48f99bef5594110929f.exe.dll" /fn_id=PauseW	CLEAN
giumlol.exe	"C:\Users\RDhJ0CNFevzX\Desktop\GIUmlOL.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8b971c2c4c9a020eb274c36db20bc0e1b203a7909d63f48f99bef5594110929f.exe.dll" /fn_id=ResumeServer	CLEAN
giumlol.exe	"C:\Users\RDhJ0CNFevzX\Desktop\GIUmlOL.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8b971c2c4c9a020eb274c36db20bc0e1b203a7909d63f48f99bef5594110929f.exe.dll" /fn_id=ResumeW	CLEAN
giumlol.exe	"C:\Users\RDhJ0CNFevzX\Desktop\GIUmlOL.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8b971c2c4c9a020eb274c36db20bc0e1b203a7909d63f48f99bef5594110929f.exe.dll" /fn_id=StartServer	CLEAN
giumlol.exe	"C:\Users\RDhJ0CNFevzX\Desktop\GIUmlOL.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8b971c2c4c9a020eb274c36db20bc0e1b203a7909d63f48f99bef5594110929f.exe.dll" /fn_id=StartW	CLEAN
giumlol.exe	"C:\Users\RDhJ0CNFevzX\Desktop\GIUmlOL.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8b971c2c4c9a020eb274c36db20bc0e1b203a7909d63f48f99bef5594110929f.exe.dll" /fn_id=StopServer	CLEAN
giumlol.exe	"C:\Users\RDhJ0CNFevzX\Desktop\GIUmlOL.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8b971c2c4c9a020eb274c36db20bc0e1b203a7909d63f48f99bef5594110929f.exe.dll" /fn_id=SuspendServer	CLEAN
giumlol.exe	"C:\Users\RDhJ0CNFevzX\Desktop\GIUmlOL.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8b971c2c4c9a020eb274c36db20bc0e1b203a7909d63f48f99bef5594110929f.exe.dll" /fn_id=opj_codec_set_threads	CLEAN
giumlol.exe	"C:\Users\RDhJ0CNFevzX\Desktop\GIUmlOL.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8b971c2c4c9a020eb274c36db20bc0e1b203a7909d63f48f99bef5594110929f.exe.dll" /fn_id=opj_create_compress	CLEAN
giumlol.exe	"C:\Users\RDhJ0CNFevzX\Desktop\GIUmlOL.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8b971c2c4c9a020eb274c36db20bc0e1b203a7909d63f48f99bef5594110929f.exe.dll" /fn_id=opj_create_decompress	CLEAN
giumlol.exe	"C:\Users\RDhJ0CNFevzX\Desktop\GIUmlOL.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8b971c2c4c9a020eb274c36db20bc0e1b203a7909d63f48f99bef5594110929f.exe.dll" /fn_id=opj_decode	CLEAN
giumlol.exe	"C:\Users\RDhJ0CNFevzX\Desktop\GIUmlOL.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8b971c2c4c9a020eb274c36db20bc0e1b203a7909d63f48f99bef5594110929f.exe.dll" /fn_id=opj_decode_tile_data	CLEAN
giumlol.exe	"C:\Users\RDhJ0CNFevzX\Desktop\GIUmlOL.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8b971c2c4c9a020eb274c36db20bc0e1b203a7909d63f48f99bef5594110929f.exe.dll" /fn_id=opj_destroy_codec	CLEAN

Process Name	Commandline	Verdict
giumlol.exe	"C:\Users\RDhJ0CNFevzX\Desktop\GIUmlOL.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8b971c2c4c9a020eb274c36db20bc0e1b203a7909d63f48f99bef5594110929f.exe.dll" /fn_id=opj_destroy_cstr_index	CLEAN
giumlol.exe	"C:\Users\RDhJ0CNFevzX\Desktop\GIUmlOL.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8b971c2c4c9a020eb274c36db20bc0e1b203a7909d63f48f99bef5594110929f.exe.dll" /fn_id=opj_destroy_cstr_info	CLEAN
giumlol.exe	"C:\Users\RDhJ0CNFevzX\Desktop\GIUmlOL.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8b971c2c4c9a020eb274c36db20bc0e1b203a7909d63f48f99bef5594110929f.exe.dll" /fn_id=opj_dump_codec	CLEAN
svchost.exe	C:\Windows\system32\svchost.exe -k UnistackSvcGroup	CLEAN
giumlol.exe	"C:\Users\RDhJ0CNFevzX\Desktop\GIUmlOL.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8b971c2c4c9a020eb274c36db20bc0e1b203a7909d63f48f99bef5594110929f.exe.dll" /fn_id=opj_encode	CLEAN
giumlol.exe	"C:\Users\RDhJ0CNFevzX\Desktop\GIUmlOL.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8b971c2c4c9a020eb274c36db20bc0e1b203a7909d63f48f99bef5594110929f.exe.dll" /fn_id=opj_encoder_set_extra_options	CLEAN
werfault.exe	C:\Windows\system32\WerFault.exe -u -p 3228 -s 408	CLEAN
giumlol.exe	"C:\Users\RDhJ0CNFevzX\Desktop\GIUmlOL.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8b971c2c4c9a020eb274c36db20bc0e1b203a7909d63f48f99bef5594110929f.exe.dll" /fn_id=opj_end_compress	CLEAN
giumlol.exe	"C:\Users\RDhJ0CNFevzX\Desktop\GIUmlOL.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8b971c2c4c9a020eb274c36db20bc0e1b203a7909d63f48f99bef5594110929f.exe.dll" /fn_id=opj_end_decompress	CLEAN
giumlol.exe	"C:\Users\RDhJ0CNFevzX\Desktop\GIUmlOL.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8b971c2c4c9a020eb274c36db20bc0e1b203a7909d63f48f99bef5594110929f.exe.dll" /fn_id=opj_get_cstr_index	CLEAN
giumlol.exe	"C:\Users\RDhJ0CNFevzX\Desktop\GIUmlOL.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8b971c2c4c9a020eb274c36db20bc0e1b203a7909d63f48f99bef5594110929f.exe.dll" /fn_id=opj_get_cstr_info	CLEAN
giumlol.exe	"C:\Users\RDhJ0CNFevzX\Desktop\GIUmlOL.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8b971c2c4c9a020eb274c36db20bc0e1b203a7909d63f48f99bef5594110929f.exe.dll" /fn_id=opj_get_decoded_tile	CLEAN
giumlol.exe	"C:\Users\RDhJ0CNFevzX\Desktop\GIUmlOL.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8b971c2c4c9a020eb274c36db20bc0e1b203a7909d63f48f99bef5594110929f.exe.dll" /fn_id=opj_get_num_cpus	CLEAN
giumlol.exe	"C:\Users\RDhJ0CNFevzX\Desktop\GIUmlOL.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8b971c2c4c9a020eb274c36db20bc0e1b203a7909d63f48f99bef5594110929f.exe.dll" /fn_id=opj_has_thread_support	CLEAN
giumlol.exe	"C:\Users\RDhJ0CNFevzX\Desktop\GIUmlOL.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8b971c2c4c9a020eb274c36db20bc0e1b203a7909d63f48f99bef5594110929f.exe.dll" /fn_id=opj_image_create	CLEAN
giumlol.exe	"C:\Users\RDhJ0CNFevzX\Desktop\GIUmlOL.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8b971c2c4c9a020eb274c36db20bc0e1b203a7909d63f48f99bef5594110929f.exe.dll" /fn_id=opj_image_data_alloc	CLEAN
giumlol.exe	"C:\Users\RDhJ0CNFevzX\Desktop\GIUmlOL.exe" /dll="C:\Users\RDHJ0C~1\Desktop\8b971c2c4c9a020eb274c36db20bc0e1b203a7909d63f48f99bef5594110929f.exe.dll" /fn_id=opj_image_data_free	CLEAN

YARA / AV

No YARA or AV matches available.

ENVIRONMENT

Virtual Machine Information

Name	win10_64_th2_en_mso2016
Description	win10_64_th2_en_mso2016
Architecture	x86 64-bit
Operating System	Windows 10 Threshold 2
Kernel Version	10.0.10586.0 (0de6dc23-8e19-4bb7-8608-d54b1e6fa379)
Network Scheme Name	Local Gateway
Network Config Name	Local Gateway

Platform Information

Platform Version	4.3.0
Dynamic Engine Version	4.3.0 / 09/20/2021 03:59
Static Engine Version	4.3.0.0 / 2021-09-20 03:00:12
AV Exceptions Version	4.3.0.0 / 2021-09-20 03:00:12
Link Detonation Heuristics Version	4.3.0.4 / 2021-09-16 11:30:34
Signature Trust Store Version	4.3.0.0 / 2021-09-20 03:00:12
VMRay Threat Identifiers Version	4.3.1.7 / 2021-09-22 10:00:51
YARA Built-in Ruleset Version	4.3.0.5

Anti Virus Information

Built-in AV Version	AVCORE v2.2 Linux/x86_64 11.0.1.19 (March 15, 2021)
Built-in AV Database Update Release Date	2021-09-28 01:56:46+00:00
Built-in AV Database Records	10476967

Software Information

Adobe Acrobat Reader Version	Not installed
Microsoft Office	2016
Microsoft Office Version	16.0.4266.1003
Hangul Office	Not installed
Hangul Office Version	Not installed
Internet Explorer Version	11.0.10586.0
Chrome Version	Not installed
Firefox Version	Not installed
Flash Version	Not installed
Java Version	Not installed

System Information

Sample Directory	C:\Users\RDhJ0CNFevzX\Desktop
Computer Name	XC64ZB
User Domain	XC64ZB

User Name	RDhJ0CNFevzX
User Profile	C:\Users\RDhJ0CNFevzX
Temp Directory	C:\Users\RDHJ0C~1\AppData\Local\Temp
System Root	C:\Windows