SEQURETEK

WastedLocker Ransomware

OVERVIEW

The Evil Corp group targets victims with WastedLocker Ransomware; uses multiple unknown distribution methods including SocGholish.

SocGholish is a fake update framework, which is delivered to the victim in a zipped file via compromised websites.

OVERVIEW

- As per NCCGroup, who first published details of the WastedLocker Ransomware operated by Evil Corp group, the ransomware first appeared in May 2020.
- The ransomware name is derived from the filename it creates which includes an abbreviation of the victim's name and the string 'wasted'.
- The distribution method uses a fake update framework called as SocGholish. Once the zipped downloaded file from fake compromised website runs on system, it sends information gathered from the infected system to the SocGholish server which, in turn, delivers a payload to the victim system.
- According to the researchers, the Evil Corp group seems to put a lot of effort into bypassing endpoint protection products; this observation is based on the fact that when a certain version of their malware is detected on victim networks the group is back with an undetected version and able to continue after just a short time.
- It appears the group regularly finds innovative but practical approaches to bypass detection in victim networks based on their practical experience gained through the years.
- In one case, they successfully compromised a target over 6 months after their initial failure to obtain privileged access. They also display attention to detail by, for example, ensuring that they obtain the passwords to disable security tools on a network prior to deploying the ransomware.
- Instead of including a list of extension targets, WastedLocker includes a list of directories and extensions to exclude from the encryption process. And it targets drive types like Removable, Fix, Shared, Remote.

TECHNICAL DETAILS

- According to the NCCGroup researchers while many things have changed in the TTPs of Evil Corp recently, one very notable element has not changed, the distribution via the SocGholish fake update framework.
- Another change is that instead of distributing Dridex loader with this framework, they are now using custom CobaltStrike loader.
- The SocGholish, is a malicious JavaScript-based framework, which contains custom CobaltStrike loader. The CobaltStrike payloads are embedded inside two types of PowerShell scripts.
- One of the more notable features of this framework is the evaluation of whether a compromised victim system is part of a larger network, as a sole end user system is of no use to the attackers.
- Before it starts to perform the encryption, it checks few other tasks to ensure the ransomware process run properly.
- In addition, the ransomware creates a log file lck.log and then sets an exception handler that creates a crash dump file in the Windows temporary folder with the filename being the ransomware's binary filename.
- If the ransomware is not executed with administrator rights or if the infected host runs Windows Vista or later, it will attempt to elevate its privileges.
- It chooses a random file (EXE/DLL) from the Windows system32 folder and copies it to the %APPDATA% location under a different hidden filename. Next, it creates an alternate data stream (ADS) into the file named bin and copies the ransomware into it. WastedLocker then copies winsat.exe and winmm.dll into a newly created folder located in the Windows temporary folder. Once loaded, the hijacked DLL (winmm.dll) is patched to execute the aforementioned ADS.

- Once a drive is found, the ransomware starts searching for and encrypting files and if a file with a size less than 10 bytes are also ignored and in case of a large file, the ransomware encrypts them in blocks of 64MB.
- For each encrypted file, the ransomware creates an additional file that includes the ransomware note. The encrypted file's extension is set according to the targeted organizations name along with the prefix wasted.

INDICATORS OF COMPROMISE

IP
185.189.151.38
185.162.235.167
185.82.127.38
195.123.227.225
38.135.104.189
88.119.175.104
91.219.237.36
91.236.116.63

C & C Domain
sodality[.]mandmsolicitors[.]com
advokat-hodonin[.]info/gate[.]php
penaz[.]info/gate[.]php
lgrarcosbann[.]club/index[.]php
cofeedback[.]com
consultane[.]com
feedbackgive[.]com
msoftwares[.]info
mwebsoft[.]com
net-giftshop[.]info
rostraffic[.]com
traffichi[.]com
typiconsult[.]com
websitesbuilder[.]info
backup[.]awarfaregaming[.]com
click[.]clickanalytics208[.]com
connect[.]clevelandskin[.]com
connect[.]clevelandskin[.]net
connect[.]clevelandskin[.]org
cushion[.]aiimss[.]com
link[.]easycounter210[.]com
rocket2[.]new10k[.]com
track[.]positiverefreshment[.]org

File Hash (SHA 256)	Description
2f72550c99a297558235caa97d025054f70a276283998d9686c282612ebdbea0	Cobalt Strike loader
389f2000a22e839ddafb28d9cf522b0b71e303e0ae89e5fc2cd5b53ae9256848	Cobalt Strike loader
3dfb4e7ca12b7176a0cf12edce288b26a970339e6529a0b2dad7114bba0e16c3	Cobalt Strike loader
714e0ed61b0ae779af573dce32cbc4d70d23ca6cfe117b63f53ed3627d121feb	Cobalt Strike loader
810576224c148d673f47409a34bd8c7f743295d536f6d8e95f22ac278852a45f	Cobalt Strike loader
83710bbb9d8d1cf68b425f52f2fb29d5ebbbd05952b60fb3f09e609dfcf1976c	Cobalt Strike loader
91e18e5e048b39dfc8d250ae54471249d59c637e7a85981ab0c81cf5a4b8482d	Cobalt Strike loader
adabf8c1798432b766260ac42ccdd78e0a4712384618a2fc2e3695ff975b0246	Cobalt Strike loader
b0354649de6183d455a454956c008eb4dec093141af5866cc9ba7b314789844d	Cobalt Strike loader
bc1c5fecadc752001826b736810713a86cfa64979b3420ab63fe97ba7407f068	Cobalt Strike loader
c781c56d8c8daedbed9a15fb2ece165b96fdda1a85d3beeba6bb3bc23e917c90	Cobalt Strike loader

c7cde31daa7f5d0923f9c7591378b4992765eac12efa75c1baaaefa5f6bdb2b6	Cobalt Strike loader
f093b0006ef5ac52aa1d51fee705aa3b7b10a6af2acb4019b7bc16da4cabb5a1	Cobalt Strike loader
6088e7131b1b146a8e573c096386ff36b19bfad74c881ca68eda29bd4cea3339	.NET injector (Donut)
5cd04805f9753ca08b82e88c27bf5426d1d356bb26b28188557305104891136 7	WastedLocker
887aac61771af200f7e58bf0d02cb96d9befa11deda4e448f0a700ccb186ce9d	WastedLocker
8897db876553f942b2eb4005f8475a232bafb82a50ca7761a621842e894a3d80	WastedLocker
bcdac1a2b67e2b47f8129814dca3bcf7d55404757eb09f1c3103f57da3153ec8	WastedLocker
e3bf41de3a7edf556d43b6196652aa036e48a602bb3f7c98af9dae992222a8eb	WastedLocker
ed0632acb266a4ec3f51dd803c8025bccd654e53c64eb613e203c590897079b3	WastedLocker
aa05e7a187ddec2e11fc1c9eafe61408d085b0ab6cd12caeaf531c9dca129772	WastedLocker
817704ed2f654929623d9d3e4b71ce0082ef4eadb3fe2d80c726e874dc6952a3	WastedLocker
023f1ef0cc2c1e055b05ae1ff5bcc6bf2421003dea227aeb6d70c8a525fa3b82	Zloader
85f391ecd480711401f6da2f371156f995dd5cff7580f37791e79e62b91fd9eb	WastedLocker
d8cdf823efe1bd2ec019bd32890d40b34695cbf7ce9e0b7780e96f7d32b5b4fc	SocGholish Zip file
1b03c872c85b00b2ef2e2f9e5e3f85b703ee2190374d8aaba4da065f54efd21f	SocGholish Zip file
2334c93c4f6ae3d370a8e7ad57c72e67d950b2842360105d3074a3fdbcea6e6c	SocGholish Zip file
6ee2884c7dfcf85030e4c26e68b3d65a6a8dd3b502f895938fca86653bfa171e	SocGholish Zip file
1346085caf84eedcd8437b31b6549aa3a5f88b168efc165b67acde907d2ee691	SocGholish Zip file
00e55499c1fce017d25e27201f2919502797180264ef67a6bc8da2f0b6fe89ac	SocGholish Zip file
8f18111a4d45ecbcaa5d409afda01bff59a335f6e92895d3422f21465e6e070e	SocGholish Zip file
34c40cee6ec17b6b76249bea42dab11380310df0bb5f1fd687be5648025cf887	SocGholish Zip file
47aecefb1b8c20d1ac705581fb84331aa96bac0ba11a9dd9dcb3afe782d662d3	SocGholish Zip file
52a8a9afe1637e8faa39894d4b7ec8857aadec8c631469a982d5d0860a6f3511	SocGholish Zip file
8e8e911906e2881dab603fb446c1ca98eb989e4b1a933496b3c49e64e3d34d33	SocGholish Zip file
5d282476a27409c1eaa8d68f46bcc69f3027840a87a16159c25c0e49e87d8f9a	SocGholish Zip file
a1849335f5a9d185c514f1b963de6c9599e375046292e07feb6fec30e26a4c54	SocGholish Zip file
4df28f81d5c9e84d96137ff0a24c9902589af1f120742441ed49e68e601b9d87	SocGholish Zip file
effa6018b4d8b48e59684dc66c64a08658e118a43715f6d0902d7c83db3902c0	SocGholish Zip file
912c405cf9506288c18984f92d66f1fd263b999c2f4a346a8e133dcb846560f9	SocGholish Zip file
5eb57802b26631c22ed4ebe9f252cd22822a04a2f28a594aaf4bc4887d33caf5	SocGholish Zip file
d3705a1fd6c1736aeabcae24bc6d247e6bcbe2168523b9788a22714fb165bfec	SocGholish Zip file
d9717e971ac44f6233b3f5854f9b264040250aa39d74bfa227a4b4602b6eb832	SocGholish Zip file
1150850a7cc92b753cc9f51db547ea675f177ce290652368599a49cfa2826d34	SocGholish Zip file
cd04bf5e9383f717975e4b2e901d04782c9cab00099a5ad06a8a9429bd4cf9a5	SocGholish Zip file
a8fa11b8402bcdcf1c6cae98dba90568fdf734ba4b083d68566b5adfa66c8327	SocGholish Zip file
e38ae05677ea8137a432307214816e0c17fe22e42c2c4279e89d5019a4599acd	SocGholish Zip file
e14257ac1f2ef19a21c7ef60c29b6dce9f63d198746d59046198fa254d9d3a54	SocGholish Zip file
ec1674ec04b9b12378198526546a43a19ad3720f5a57b9b420386a17cc0f8983	SocGholish Zip file
94e17b0d20a458b997a43d6c5aaee62454e1168080574c5e472cf152046d7540	SocGholish Zip file
90221dec6d92d6f76af0240d3968a8503e821955d3cc3acf30527bc8f2a65e9c	SocGholish Zip file
36d6f04bbb409bc6e74cf4d8bbc11f250789cb2de14e243ffe891b0f75145549	SocGholish Zip file
bcddb155313a76b05e4758c6071c3ff26b3c383d705c90c0015f68e7d11f504d	SocGholish Zip file
92b79542921cab76d001d785dceb5c4f55cfa9d3a51cbc99a3e2db1cce4892e6	SocGholish Zip file
b349848b0357abd4be79b456e1019305c5105892eab768b85bc89da1932f3d22	SocGholish Zip file
289a5876bae1f28fd3817a7fc010e2dc2205372c0eeb957dcce009fa10b57bd9	SocGholish Zip file
6215316b10db41cf8ed697605074fdf59fd5967e98c62f03476d845ca46ff69e	SocGholish Zip file
631c71d88a3d0fdfbb22ed393eddc78276c0b4abc85e2d0163b4edd603306fd6	SocGholish Zip file

d83a6cddf932d129f49b871d8a42f8b1a885cbdc8ae3f44b215d409d8f7eaf05	SocGholish Zip file
54c8ff32e714a1160235683a26bbf9cbaa267a45e20fa34544e9b9b3b2753cfc	SocGholish Zip file
a5d3b330150b5de4e2d484fefe7cbbcf0273aa5f043c3d54c83437785e6af1d5	SocGholish Zip file
61099171f2bce433e2a8cdb1d24811cc2f6c01b8d9f08f66f5023c97306aa9ca	SocGholish Zip file
73a3d35902745b2b3e46efa884f711f6aa490a7961105ed1d735ac0878fe8b26	SocGholish Zip file
05a9ee3b90da5fcc6c4bb888125d00f36a150eb271f956793ef1d74cf57d1493	SocGholish JS file
45d611f352993041e3da849597e9411f2d6682a65d6f324a474d4ad2b409cb3f	SocGholish JS file
288ffd4ceba91bcc4a95036014f7a7615911b12f88f03db8d70c47bf3db8f0d4	SocGholish JS file
90d8e358f27ff85b40b5cee46d636d5390b868ffc05d068a36b29f2dce6c62f6	SocGholish JS file
fb576ea0d43d21a3899535ef2fe7c03c477259a899a90b4a266af0a391273a0e	SocGholish JS file
7861cf7ec016aeda6db3472bf572d50c377400c2c59ba0b37705569c95510f09	SocGholish JS file
b4df0635436d46418aa93aa72244ab8090463611132d7804decfbc2fa1eff047	SocGholish JS file
034ec5eb976e5243aa7df416b3657a0f84cf28dfdfa896ac9f627631d64171d7	SocGholish JS file
14c46c371127b3025ab7ee242f5f0b4e9397a39471004657f247722e3b9d9951	SocGholish JS file
1b1b50285f7653c3e8e2190db2c3801ecaf1a1168f30fc38665f2715397c809b	SocGholish JS file
6515a4b8f5447a644dd7c741ab062ac59b1b34bd1064435e0f43d282bd70e4d4	SocGholish JS file
b70df428c04e69f3ac3aab97c93ca327eeff91005fc9a6b4a824caaae2df5f88	SocGholish JS file
d0679c245e7fdc321f10aed472d7dd41cc13cbad9adbcceab1e378f61b02612d	SocGholish JS file
736657779bfe8a99b9f75e8aabb3d517427cf9f2ae18d5f0461fe0d3fbf50145	SocGholish JS file
82f3d67830c3680b71059c04002f6a0ae0f20e82dd99bf877f37e753f1756eab	SocGholish JS file
d6020b5e4a6dc0df5f6b1b38b5912ac5a623224cd1c64a934c678e1a88fc8c38	SocGholish JS file
49fec94faae5ec209c8ab143088d8a2bc5359e71d14806ac035071c90c120d05	SocGholish JS file
e492d2f1c8d718a8ac06f15f3e21e1434d0ee1889c0b4023901bf5cc680668e8	SocGholish JS file
5f30f3669e954b028b8aaabd84449bf1ddec5ca25b9ca6308fc6b68dc131fe57	SocGholish JS file
8279ff428765065945ffcc854c7b89f1449bcab42a7f41c9a8db98fb23104981	SocGholish JS file
abf625d0b4fc46a57d102a460d08f948203abb18bd8fc6b349f724825deafb32	SocGholish JS file
7b6c382fd85e740ac83d88804b713bec5cccf42cb5ac55bc909d85d02a078921	SocGholish JS file
c9ad39666e0325af0db6ad5ceba49426989f1b79a1c7e948fd721041ea403b8b	SocGholish JS file
ef4a97b17c24569454cd9d28a37fb7acdf947e6067052da6ec3ae40d8ce48a01	SocGholish JS file
e69c70c23563cfc4eb975611bac2514e7210dacd24fa07236856261d797ba05c	SocGholish JS file
ffab63f7037817aa5f7f627c3b31b8ba8e9ded16e0c07044d477110978dab519	SocGholish JS file
1ae6f7888789d427431fd69bd79a0059a6d1faee77a271c0678f31b417a4dc87	SocGholish JS file
061bdbf149adb99d3187ca21b6516ec0144711142bb7b97ee663261d9efe7560	SocGholish JS file
89355cdc3fd592b2630764290edb340ba0c24b69d82231b4c444f098080b53f7	SocGholish JS file
b0fd99793eb891f89de6b4757d10c8c58d3ee6e8139e2b594ac9f1116868f8ed	SocGholish JS file
be7acff64e95605852c4a9a7be7d013e37d3975f59b2bad1381e1ef0f2fd0693	SocGholish JS file
c1e90b1028c33a8296090bb4b280167b2af2bbe13a6505f0efa72fbaf47d6610	SocGholish JS file
740e254bf1030441581a1a90b84a34f770dc5ddacfc26f2bdcc21d1e1adf4117	SocGholish JS file
17652ca0a0674f3d33aadc5fc8aa83281a4c504a63b5a2b45a7ff06bf8db776a	SocGholish JS file
f9ea04b6d8254480741f4dffcd5c71361446c3151a88af728c8f02ded1662ebf	SocGholish JS file
3c6ddfec710fdc626eaedf335ef0d5e062b58bf2018c07cc4f86957dce84b15b	SocGholish JS file
08c2a598370400b6ae2e821bca121ef1ae2109c63ea547f972c0ccc281bf958e	SocGholish JS file
9551700ba4099618b7d89e375f508ce1dcf8c9838318017ddbe081c0cf0b4693	SocGholish JS file
1858d80f6fdfc6ff796357d49d7c453a7cf17583dcc8d2d0c5be8a1695ad20f5	SocGholish JS file
39ea5c8bdf1f5c3345de71b78e9894081559c5b90720542b3ef3afe8432b1a4f	SocGholish JS file
81cb83ad3095554ea36932e5c8ae2b96d013a19dadeb56e9f11ecba8eb804591	SocGholish JS file
ce2b122a1204a1ab7effb52e7008661951bf192a1f184fe549a8bc09ee0df76e	SocGholish JS file

5b1a2c9072623434e5fa9147359ce67ea0ffd1f16ebcefc56670485f76084390	SocGholish JS file
bcd670fa6c4c943b3b4375d833adf8e0cc909ca98fb0c93414288e27dd80c2fa	SocGholish JS file
2bfdac333098b55eb4c9b65f2a6da758c2990338c39f1a4ba552ea4b34a9b742	SocGholish JS file
ed1dcf691183d593451e02d1e1b5ee8f1315b472efb9955f0a0158134dec29f4	SocGholish JS file
30a6e295d616c9c7a638530f4fcc4fc82c5496c8f69811eaf0df42904c2fd3b9	SocGholish JS file
96c6e2936ffc2797d86feaa19c912898e77dcb392df9808ed4a135f6cee99664	SocGholish JS file
dab5af9b9a633ac329e40522341579a3ad6511ef293c1b6ce0274883af9fb9c9	SocGholish JS file
733e4c6232b380c449dc906b60f5f15d29c9d49c3912a173eff15cfb6232b383	SocGholish JS file
afa42b2f92b076e1dae6257e27bd6cfeb2102fbe3da569f233bd6b85c0f88b8d	SocGholish JS file
2c8de9f78d25ec81d0408dea82a5e449f68c9cc9ffc8cca68efbbbddb9b7edda	SocGholish JS file
4a1457a6589c201dd79c49e0a0d19b3b742c7ec9eb8703ee998fcfcbed118f10	SocGholish JS file
e96c47a7540c87778af38934d6c0a35a68d83fb1da80b9499480b7a8ffbdf5ed	SocGholish JS file
df068eb71951ff0950fbbc0595540818dd63d490e8f8ede46185ee75f20b0a72	SocGholish JS file
b3955a0deb80e5bc5baed0002d7e2761e1b0d5165f02134ad7ee1151f91424bd	SocGholish JS file
6e44875045594d2f22da11544c49336f6a242a1ad3e8eaeaf025cd61fb9e168a	SocGholish JS file
038563215659a42d6d5b1009756716d969105e1f85155d9d1a6ff4c4d691fb3b	SocGholish JS file
b935a4e4b589adb6cfffd67ae9400caef9f8e087a5943a5feaec21361693c606	SocGholish JS file
fe09d6a7df1e5817d0f9c732c0a17bdf4d51f1967c7ec1b2871051af7fdad78a	SocGholish JS file
36cdac5b539227bc6dc88842bbe351478662ef6118b9145dec62aabd2c47c9c8	SocGholish JS file
cf7734c8606a472aa2dbd38a74a60dff4e8a5d00b05eb850de535a7019cc9904	SocGholish JS file
5a4a7e37686388fe6f887021e16ee2226a27263c329f98d1501426a8d7152630	SocGholish JS file
55cbedf65b3c49c4fd456beb9ba25b9e770d93a51fd303f15727b35d33b1cb9e	SocGholish JS file
f6b546179d2b499e552e03001c2aa7c994f4c5e568113601dbab2dd7bbfb9429	SocGholish JS file
9d5416ae461d9c4bef4e674aee34bee263261e734d22c8c0053d37d5b3aba56c	SocGholish JS file
5d6920e744d44a0ed95b0e6dfb6daf1953a2b3ac288c9821d77455584229338f	SocGholish JS file
e2431e102d6ac41f91216e4a8b2bd93a126cd6988254406fcdd95340e3a0a219	SocGholish JS file
2cd386577165e39c36f5274488f6796b0e0634c33d42a9bbb432f58dc1096d60	SocGholish JS file
95658de9198378e20deb453fc888083864ea189ccd87653a14e2c39c524e3d84	SocGholish JS file
3e3b419541631e4f0d123993a1df52d49f3d2b9a484af44f5e302b3b4a58cc10	SocGholish JS file
faba871c8af45b94a300400999aa3a26d8bc57f16095c5485d45c9a4bdd7e1db	SocGholish JS file
13f0cf420ca489ddf33ee7551251c27e0b80aeabb77c082d164ceb3620ea89c7	SocGholish JS file
b26917a47ce0c19deae73f23bd8f26f6ee8ea0c307590e9d2b7a42aa9ddee297	SocGholish JS file
cbbc0a5e557785549766d538fe3bc1625b91b40fa74b910a7e654abc7d0ed7cf	SocGholish JS file
7c55d7753e22562c77d1d20e48293a233d9fbf84a654a0236f3edb3491809219	SocGholish JS file
40876cec2391304003e3792afd49b8c41981da0d8629b3edb7b7dd42dbf16e45	SocGholish JS file
73afcfba2476ad0de83a180a50e169878c070f8ee17c72d0c8360706dcd32cd4	SocGholish JS file
cfe3628d6bd279b2d43dcf8e7d3898893ea24fd2bf757fc51b764c0393b45976	SocGholish JS file
0cbc11499a01fc3e712f30f5ce0ffa88d23f490846c1a4ce0e7f5812af12edcc	SocGholish JS file
42807830ede9edc495c8632210c8d7516c2b5f0e0d766e0a150f73dad9287e0c	SocGholish JS file
0e0832d0970cc95d1ce326a8d59068cf5757b6720ef2f89411eafcb077117b32	SocGholish JS file
284c097b60e2e3cc65ae4047df57be15c0c9ee87e554c841b63e26bc7b0febbf	SocGholish JS file
8b04f39738a58cb4a46a13b50dcead651e1cc1a0e23caf8adf00bc6d3e6ba684	SocGholish JS file
9b06c7ce8c21e3439650d0d6478f7ba35a63a61efe97496c8258963fb88181a2	SocGholish JS file
189341461b49056358fe3b5d20558dc132d83fca43560ac96dccce5994fdd0c6	SocGholish JS file

PREVENTIVE AND CORRECTIVE ACTIONS

- **For Organizations**

  - **Preventive Actions**
    - Block the IoCs at gateway and endpoint security.
    - All these IoCs are combined in our Threat Intelligence Feeds that is integrated with our SOC to provide proactive threat protection to our clients.
    - Employ content scanning and filtering on the organization mail servers. Inbound e-mails should be scanned for known threats and should block any attachment types that could pose a threat.
    - Use strong passwords and multi-factor authentication on Remote Desktop connection especially on administrator accounts.
    - Limit the number of third-party vendors and employees that have access to RDP connections, create a user group that will be allowed remote access.
    - Backup your data regularly and Keep it away from network connection.
    - Make sure that all systems and software are up-to-date with relevant security patches.
    - Do not pay the ransom. It only encourages and funds these attackers. Even if the ransom is paid, there is no guarantee that one will be able to regain access to his/her files.

  - **Corrective Actions**
    - If infected, disconnect the system from the Network.
    - Inform the Information Security Team.

- **For Individuals**

  - **Preventive Actions**
    - Do not download or use software cracks and illegal software.
    - Be careful of the external devices you connect to your computer.
    - Use up-to-date antivirus solution.
    - Take regular backups of your data.
    - Do not open attachments in emails from unknown sources or click on any links.

  - **Corrective Actions**
    - If infected, disconnect your system from the Network.
    - Scan the computer using legitimate anti-malware or antivirus software.