https://www.trendmicro.com/content/dam/trendmicro/global/en/research/22/d/thw loaders-from-socgholish-to-blisters-lockbit-payload/iocs-thwarting-loaders-socgholish-blister.txt

LockBit ransomware
ba0cbc64186e71421df417178c9fcb28b42a652ad063abfdbb6996604d30885a

BLISTER Loader

SHA256	
27E80A2432871DB7163A59FF6ED3920318740340445C2C367F190DD1E94723DD	Trojan.Win64.BLISTERLOAD.AB
294c710f4074b37ade714c83b6b7bf722a46aef61c02ba6543de5d59edc97b60	Trojan.Win64.BLISTERLOAD.YXBL3
2aaa916d56cfe95abb65fbc222bfdfa2b16a3ffb6660c1bdc211004302a1aef3	Trojan.Win64.BLISTERLOAD.YECCI
2eab76f1d46be74c68d9562b4b32c44606fa23c0d7897f9d89a3e2534be6f2c7	Trojan.Win64.BLISTERLOAD.YECCI
3ac3fd9de619c934b0fad04b0384898d98cd69444da2d2bbf3bdd6a7e922fce2	Trojan.Win64.BLISTERLOAD.YECCI
42d737487daccf77f7c80ffd1d823ba4e51cf154e8486f420ba958e1df2a150d	Trojan.Win64.BLISTERLOAD.YECCI
49925637250438b05d3aebaac70bb180a0825ec4272fbe74c6fecb5e085bcf10	Trojan.Win64.BLISTERLOAD.YECCI
49ba10b4264a68605d0b9ea7891b7078aeef4fa0a7b7831f2df6b600aae77776	Trojan.Win64.BLISTERLOAD.SMYECCI
4faf362b3fe403975938e27195959871523689d0bf7fba757ddfa7d00d437fd4	Trojan.Win64.BLISTER.AA
4fe551bcea5e07879ec84a7f1cea1036cfd0a3b03151403542cab6bd8541f8e5	Trojan.Win64.BLISTERLOAD.YXBL3
5006ad8ba0cc6d68626fa7789a62f8256c5f28a7a86903b60ef203d16944df99	Trojan.Win64.BLISTERLOAD.YECCI
546acb39c89b8b72923aac98dd68369aa4ab8440b5ea122301626c6b082f95de	Trojan.Win64.BLISTERLOAD.YECCI
5ea74bca527f7f6ea8394d9d78e085bed065516eca0151a54474fffe91664198	Trojan.Win64.BLISTERLOAD.SMYECCI
6098371970ccf86aa5e70ebfe4f0622cdc2e2ae19fb85b17f6cb79bde981ea0b	Trojan.Win64.BLISTERLOAD.YECCI
722e75932c75a37bb9b616093c77611433da35236182615162cb4c9d6fab34f0	Trojan.Win64.BLISTERLOAD.YXCCJZ
72c410eea75347e8c5bd7e1cb6ae7d1dd0ec5c73dd7b53bc8c2155cbd3e60961	Trojan.Win64.BLISTERLOAD.YECCI
73baa040cd6879d1d83c5afab29f61c3734136bffe03c72f520e025385f4e9a2	Trojan.Win64.BLISTERLOAD.SMYECCI
7b9091c41525f1721b12dcef601117737ea990cee17a8eecf81dcfb25ccb5a8f	Trojan.Win64.BLISTERLOAD.YXBL3
812263ea9c6c44ef6b4d3950c5a316f765b62404391ddb6482bdc9a23d6cc4a6	TROJ_FRS.VSNTC822
84a67f191a93ee827c4829498d2cb1d27bdd9e47e136dc6652a5414dab440b74	Trojan.Win64.BLISTERLOAD.YXBL3
84b2d16124b690d77c5c43c3a0d4ad78aaf10d38f88d9851de45d6073d8fcb65	Trojan.Win64.BLISTERLOAD.YXCCSZ
8e6c0d338f201630b5c5ba4f1757e931bc065c49559c514658b4c2090a23e57b	Trojan.Win64.BLISTERLOAD.YXCCSZ
94646f971c52c5725a7872006c9c80b10271a838d87f20c85247c357f6ec35eb	Trojan.Win64.BLISTERLOAD.YECCI
9472d4cb393256a62a466f6601014e5cb04a71f115499c320dc615245c7594d4	Trojan.Win32.BLISTERLOAD.YXBL3
96823bb6befe5899739bd69ab00a6b4ae1256fd586159968301a4a69d675a5ec	Trojan.Win64.BLISTERLOAD.YXCCUZ
a403b82a14b392f8485a22f105c00455b82e7b8a3e7f90f460157811445a8776	TROJ_FRS.VSNTC822
a69cf4fa61217f8230e032089a8f56f7ebf31e4cd35124e6ad104db86851f17f	Trojan.Win64.BLISTERLOAD.AB
acb37a4c2552ae2f9b9bbb8ebbb9a501ad6b5787e40867270d7ff3a5369e3632	Trojan.Win64.BLISTERLOAD.YECCI
affc475c4801ef7bc467157d41e24af4d91b5234e9686bf954b13e48e473679f	Trojan.Win64.COBEACON.SVK
b062dd516cfa972993b6109e68a4a023ccc501c9613634468b2a5a508760873e	Trojan.Win64.BLISTERLOAD.YXCCUZ
b91eb833de386ea3d73d2954f0dce9fe38e4bf96594620af6c0935b9ee0d7e81	Trojan.Win64.BLISTERLOAD.YECCI
b959b003c1e558ff0ccf1d0f96509b155d6f86eb20caa97b470f3422494d8d74	Trojan.Win64.BLISTERLOAD.YECCI
c08d467966d6ca60a68ffe1715851eea366eed6b35e033a43437128c05d441dc	Trojan.Win64.BLISTERLOAD.YECCI
c0f1ebcca8a8094853aa65210ddde80f6a9ffe7b3f2d75d5652b166722b3aa4a	Trojan.Win64.BLISTERLOAD.YECCI
c3509ba690a1fcb549b95ad4625f094963effc037df37bd96f9d8ed5c7136d94	Trojan.Win64.BLISTERLOAD.YXCCUZ
c4520713189d27e21b0f9060ba95cbfe4f49cc0f348854f08d1ed3aa577e9bd0	Trojan.Win64.BLISTERLOAD.YECCI
c9cc4d95ca1197328a743a41b09c2375d54ac97fcdde5e07bda660396710eccd	Trojan.Win64.BLISTERLOAD.YECCI
cb949ebe87c55c0ba6cf0525161e2e6670c1ae186ab83ce46047446e9753a926	Trojan.Win64.BLISTERLOAD.YXBL3
cc2fe3129d312648b6be28e4d8046c36f19e0553283e64a4af7cc5efe8586c57	Trojan.Win64.BLISTERLOAD.YECCI
cc31c124fc39025f5c3a410ed4108a56bb7c6e90b5819167a06800d02ef1f028	Trojan.Win64.BLISTERLOAD.YXBL3
cccd4fb8900df5f8939e589f4e66d6819796d84620ae97e7efa2cfd7237b27cf	Trojan.Win64.BLISTERLOAD.YECCI
cfa85cc84451b870f26515da705783a3b0616b54cd2ce350281b3b0a3383a3e8	Trojan.Win64.BLISTERLOAD.YECCI
d08f9390fa610dc3976d309a859b9abc8404cee1ef8aeb886f3f9e524c1d2b9f	Trojan.Win64.BLISTERLOAD.YECCI
d3d48aa32b062b6e767966a8bab354eded60e0a11be5bc5b7ad8329aa5718c76	Trojan.Win64.BLISTERLOAD.AA

d439f941b293e3ded35bf52fac7f20f6a2b7f2e4b189ad2ac7f50b8358110491	TROJ_FRS.VSNTC822
d625d21f6ac0677ce386e09ca1d78eefd3f223991642cabc72c756da5ec048dc	Trojan.Win64.BLISTERLOAD.YECCI
e0888b80220f200e522e42ec2f15629caa5a11111b8d1babff509d0da2b948f4	Trojan.Win64.BLISTERLOAD.SMYECCI
e30503082d3257737bba788396d7798e27977edf68b9dba7712a605577649ffb	Trojan.Win64.BLISTERLOAD.AA
e5ebb489a8ac483ad3daf258f6ff74ae7bec6b67b0deb9a571f8ce90c82d7380	Trojan.Win64.BLISTERLOAD.YECCI
e7a070adb5d238ccd7daa249f26516e2bdbf72e1e866d54189e96272117720c0	Trojan.Win64.BLISTERLOAD.YECCI
eba37e8cea693569462061fbc0a82c609e4e855c827a6228babcdf798c3c9885	Trojan.Win64.BLISTERLOAD.YECCI
ebf40e12590fcc955b4df4ec3129cd379a6834013dae9bb18e0ec6f23f935bba	Backdoor.Win64.COBEACON.OSLJBJ
ed6910fd51d6373065a2f1d3580ad645f443bf0badc398aa77185324b0284db8	Trojan.Win64.BLISTERLOAD.YXBL3
efbffc6d81425ffb0d81e6771215c0a0e77d55d7f271ec685b38a1de7cc606a8	Trojan.Win64.BLISTERLOAD.YXCCSZ
f6f116e43261ad432b5c5edd44faa01641621e9c728902053f235877ff22431d	Trojan.Win64.BLISTERLOAD.YECCI
f74a32a67a94fd711da78af2f8f4bdb83fe7deaa049ad11f2f980bb6e3c037a7	Trojan.Win64.BLISTERLOAD.YECCI

Java Script C&C
host.integrativehealthpartners.com
Apps.weightlossihp.com
Xen.hill-family.us
Platform.windsorbongvape.ca

URLs
<8-Characters>. Host.integrativehealthpartners.com
<8-Characters>. Apps.weightlossihp.com
<8-Characters>. Xen.hill-family.us
<8-Characters>. Platform.windsorbongvape.ca

Java script C&C
87.249.50.201
91.219.236.192
91.219.236.202
15.197.142.173
184.168.131.241
184.168.221.18
198.71.233.254
208.109.181.175
3.33.152.147
50.63.202.55
72.167.106.35
50.62.160.77
50.63.197.201
50.63.202.33
72.167.191.69
23.227.38.32
52.60.114.31
198.71.232.3

Cobalt Strike C&C
Sikescomposites.com
Bootsinthebigcity.com
Couponbrothers.com
Discountshadesdirect.com
Bimelectrical.com
Setechnowork.com
Braprest.com
Pastor.com
Hardwarebajaar.com
Wasfatsahla.com
Technicollit.com
Clippershipintl.com
Ksplsoft.com

```
Geotypico.com
bookmark-tag.com
altreeservicellc.com
imsensors.com
propertyexpoandshowcase.com
```
