IOCs for Chaes Malware Targeting Latin American E-Commerce

Cybereason Nocturnus Team has identified an active campaign targeting customers of a large e-commerce platform with newly discovered multi-stage malware that evades antivirus tools dubbed Chaes. The info-stealing malware is designed to harvest sensitive consumer information, including login credentials, credit card numbers and other financial information. **The full Chaes Malware report can be downloaded here** (ungated).

Indicators of Compromise (IOCs)

C2 Domains

awsgold[.]xyz
cnxtours.com[.]br
evolved-thief[.]online
Gilbertantonio.com[.]br
Farteresina[.]com
seriscojamais[.]live
awsvirtual[.]xyz
gbviadinho.ddns[.]net
cleanupett.ddns[.]net

IPs

45.15.27[.]216
176.123.7[.]218
176.123.7[.]135
91.208.184[.]164

Docx files SHA-1 hash:

69aff119d2504512bdc7dc9e0ed421843633bd38
7bc2950ccbfd20917071f782578673893dc5f1f5
f1f30ee4d7847a998f877ccdccfe299b6976189e
603595b5015c572067d62fced82522cd86f9b147
9d247cbb5b1fe3aea0d0a9974f7f535bec88a6fe
1440254bfa1df060600af3f00272d07be142eed0
5c9785af3c10a36183aab9d2204ed11746678f66
14e07dc3c21f4a3bd8aec01c03004d573c217b05
eade5d6b12a576d716f87ec5083d316b285161d4
4eefa2a413ccfeb66d2eec41a4f9e46e4d13b864
3fd6edcda997e45ff694f55c4f8870085b8a6350
92ccc0bc6294888ed1d044ed8d75e6b2026341d2
b574b7487b1b0aa27c9f6060601048206cb3bb13

ebefe6ba47093f6346ed1ec3eeb9fc6f7d9c6d62
b13d8214e6ce1be8292e7305c43a29404339e633
42b4525d175cad7c544fefd0ad34ab8a3e6573b7
c0323a151e8df4506df912fef078c1d7034cd51b
782b641eea77defc31c33c4180ffaf30ff622801
a9a57df17a3d27449867091b5b0d58d30d914f6f
8c915b6942d5c2db950ac20dd9a47adae25b35f5
0ab143f2857c76e6efc077b102188e54ff05db9f
aaaed8cdd6173e349b43da245ff908f516fc1a1c
fc176db11c9c2e55fb8f67e958ff73919603655d
C99bfcfa6dd1f1801b890bffd6a6eac8e3672d32

Docx files SHA-256 hash:

3292fc7a815a01bfbcd7478b0bfc28f8fda425e9a33b2848315e5ad75168bc29
0c5edb9b8b830ed35ccab57f49cab3218fcbebc5ef3127518ff2fcab64471c2d
a50e29d49df8bf6d0d6f9a8abffce8ef6158dd5a4c813bc2313344ebb468bc0b
6f4247f2b34a6e37173a5b8432f8a64e3e5b36ef3c329aa83cabe2036f97e779
dc19f7f5e7eea7cb23e30e73f55d7ec61c1b28d996085cc50a2dafdc33b3b0c7
9ddaa03d15f55099ce5d1dfc981431cd7074147c71aa094e43d4aa715b81df7b
1482f9506977e6ffc5510852d7fe02abdd394499ebbe2439475c3eb4193f5359
8a361ec47aa5f999e37ed08408c2d145d0d6e41d305f62865e6f5b40b6e0e9cb
f844708b307e0b5259714feec25c32ffe188535798e8be517e0b13f0d5ab68a4
db932b0a50c16f281a0e4f4ca1943f6867dbbf19978ef48463c3c7913acc04ec
7700f5cc5eb3149b67e8c06d893fd9a85afbe9a5c582a6db9f88a784605866cc
67ed7e369dd34ab348b2cf0fa730076a6b735aa5007acc2e5f8221b19a8799c2
e051c9a186b9f84400a01b23e5cba63ed895d8fa753390239432638a983a6268
cf1928a26bec7fa0a08ec88584d55c354e7ae0053ca618cca95608f2bc2d34b2
4b6860d1d903064750af333a69ab2aa7c118c176d3aefbcb05a074d0f3684ec3
19831b8a02d57396525fab89922e6257ebdcff44ff7866e13536be30654c998a
65ef7f5d9c66798d937fa634b534090d7863c30886c9d4a500f57471e6965e85
091e8d85423440e18883461be6a85a8ff5b7c55c4b96261b835b2a0bc8871ba5
ee6b7792b855e4df34557022fcecb5e9f9c4fd35ccdddea2007b7f7fb811252e
41a0f8cb7addac0d3d259fd8a1d72671f519afc8c47d1d80c4f495e0a2aa8c67
d353a3725adba02e2db889c86e8f53fef15b497538023689c70fd0269f269e22
cd32569498e325e8c44e15cb3317084b54e291aeff4165741ef0c3081ce4f845
0a409856f4fc32b62442163a630880a3bcb6e4169135fce194648a516e26fa6b
6c1ac7e0e87eb47c662b01ae46efe346d5c71c4ea29243b974734959222124ee

Msi files SHA-1 hash:

b95b490ed50e9fcb32b0b3a2dc0ca0e033f518d8
b2ea8497e5416970f4e8199259b20b781b66c72b

7c2ac832e4660b12631941857601f863c94f083b
109d62e42c42d3b3b73ef6a68e2f9ae6283a985e
09baaa18942a0fd91943974edc3a25b4ac9a1f15
d0e4ecc6b3294bb929c8c3fa035e1f8841a07c5f
e2a572a4255ec196cf65bac556a1f7e006827e29
6ecc87171886fa82bb663431c5e2893c3d5c1412
5d47231f115eedc1215c1393a1623efbea6984a6
2ebf4d0d49006c798a4653556069d6d3d6b32e82
2a4116b24938c63dd408eac9dcf432ace46d8034
2523eebc2c6918269e5795a21f6750f4cc2dd693
e52d705ab996577b67d45687d66b243bb96c49c7
19cb5aff0185b704be243747e2b6facbc2b33724
5994f16422b8823d97ca488db04ae4193589608a
dfa8272ce1de6fd39d3a9a8d51c6642d0d7dc92b
abcec43c255626957f077a305b2fdcb49b00b2e7
13fbbd156f48a8d1b9adfff160e22b09a9227e95
57db475aacbfe415092e92bcded1613afe1cda65
f97515c69163e2ece45d014d0a1b9aeb3a7cde7a
ec6e47f1250425a75e7eb7f94b55612f0f6432dc
30e62596dcf0b2c4a683a3bde9f72738adb9506f

Msi files SHA-256 hash:

753f394ed529ce38411df329da1058ad4a735806e8c3deac473ca223a31795b5
f7e877d6ff7c586b71672595645d10000a438daecfa15d72cc19f65f7aff6df9
cd937db90ce7cf8e118b9ce26e26d34e022c5ae12b4e0e381f01ee72934fecae
000b76dccdfbf3fabd422ed28462dd51f3bdc63842e2067c469557632efd01ac
7ed624e5a5520bed6284e64f5d9694c9921e95f0a087c1908bfe1d2a32a42e75
0ea6a7ad2694a87775e0d4f5d97f5790859fa4d5bc10bf3d2e4bfacc8c68a6cd
ffef8252643991e1565edf6f1203b47d18b391689bb8affbd9fc3ac528cb3613
641641a5224e0bfa9c4af2eae72431bdafc2169def06059ca75f261f0168fe84
4de0654de126bed1381a09aa3685b1a3dc47ac195d9c0566e9e2bec2897f921d
9d4506549b9e4906df8de5604e9f4bfefe84fdccbe996c5cb46877b629306e02
173a01dfa5063c5ff7bac5cdb20c385a3e178c3461b9860009fbaeb0ed4dcf02
6d605664926282f5320635e4386443a849a60f97d77aac24499b2a61e2c86d1c
71624db380242302bcc8d212ccc386ee40800d20b408782a329e8ee3d52c9530
b9fdee5032c054128482d377a03f694f5aa9a9d62dabf7421a9ac9484f2d2f95
a8892cd5f77cfa720c0b242e889c406b9b873346cf6f45f6ef30f65a1f0e846a
7c1b9ba572505b7cfc0ad94c880f5662879de07cb689c990b3f98a0652631dc5
841c58cfad20e01d28f1d529560858947d929c0a47346cd13dd158571fb35bdd
8493b50dd0252b1b3f6463feeebfc652aa1899739d174bdb9906b7fadc859163
294297ad14cc26aa1a9ad159bba72bd9540493e91ff63d43870662d6e5c769d6

3bcb2600e2a0a6f7cb3ba451a4613dc88ad3f0be7347281941ee905196508311
75a3cc5b90dfff9061baea9429cc873aa0b99cd933ea8e0edbb09ccb701a8105
05e1b536dde859f88b95123591666200af467b25803ab1ae1237d24147037c9d

Binary files SHA-1 hash:

49c0062c35a32d0aa6d9d7fa145649fc83abe0bf
53650fed814c3b9f4edabf13ea18fb783848d70c
8182e0dfe02400a2cd7c2fb2ed8af85898f9ece5
cd41756c33a86554217a619f5e8607b019fabf02
582da9931f3c858c3ffb56880594193cf2e1a379
d04e5ae914c05e993848be8970562eb227b5080a
ee657b65b8785632e14173160d7757056ce4f545

Binary files SHA-256 hash:

adc86566a64fd9f5cdaa8a220d6797b3ad171742cbf0f77e2055d396a0f1bd3b
666d82b4218e8bf0665897efa49420e4b187a1850684ff06beb5f50962636ecf
B1251a92a381ae452038244a2c8682b8a877bef8c871b8fa0f80fb8c72bedbd0
1387810eda173b0e632632ecc90666f933356be57589819d5f988a99b574d3bb
4e368a07374402bd8c6debb67b8c5a9d901e36ba2ddb20cbb206004bf4cf0bdf
Adc86566a64fd9f5cdaa8a220d6797b3ad171742cbf0f77e2055d396a0f1bd3b
dd643e7973251aefbc4555adb0c54dd4863c7cd327feb918e53a8130bad21285

Archived files SHA-1 hash:

Spm4.rar
F477a13dc8e05a507969d458095e2b75ab0248fd

Chstea01.rar
5e2ea144faf0b93c236bd872c402974bdc23a58d

Archived files SHA256 hash:

Chstea01.rar
Ee21c659ab9c4ddb0f7e2ae58df94e78c8455c4254aaebb4894c08d6705292db

Ini files SHA-1 hash:

Config.ini
bf3174b0151ff6c1b57398f37c9f381bb2b66a6c

Instructions.ini
84f38bf9df9a0153050b371033afc0d8191763bf

Ini files SHA-256 hash:

Config.ini
f09b165bae8f269e03c45827c125d361a7af9563487829a4966bc2e7fad395a4

Instructions.ini
F40766ea85bf7e0a0188c998ce2a47aef16a7b061a029862ca35f3c32df7fbaf

Scripts SHA-1 hash:

install.txt
1f4c3b1ef51a854a416adcc83e47cebd3e0f57aa

invisible.vbs
2182243567bfcefcbc88b4ebcc42ed52e1dd1e69

Index.js
D7e7ffd4f327d21b0775f08755a70afbb4aafed0

Possibly new version of Index.js
43e81fdcd00bbe9b226e4399fec5d0df0d1b23c6

Scripts SHA256 hash:

install.txt
181ef3dd877e67cf83b3712ffe6c5c2ac90abbe4f449bbee4c6080e526716fa4

invisible.vbs
51e31ef335b3fe52362a583ac02476bbec3c2a42eb0485867f978dbaaa74fd32

Index.js
4896ba0c43ffb85e7bc1656115b5c0bea9d4a135677cd256d75f7ecab1c07ac1

Possibly new version of Index.js
deb9d3b0dd46a814f71ba9fefcac4e3e689a8d2ade0a09c2bc5930fa059fc9c4

DLLs SHA-1 hash:

uninstall.dll
582da9931f3c858c3ffb56880594193cf2e1a379

ModHooksCreateWindows64.dll
0b16a5cd9a35cf4402e5a6742f4b7ccd863401d5

chaes.dll
3b18c58960f83f9072b318461d79f9528b46685d

b953bf3b49f052b296fffc4e1c7fe3aa9a85cf9b

hha.dll
Cd66494a6dbb99d2cf5ebb7dc8bf9782fb76e702

DLLs SHA256 hash:

uninstall.dll
859d46ca687205bcda73a84b9a890b853063e6be0ebc19ccd7218684f1979f2a

ModHooksCreateWindows64.dll
044c2af8e43f9a6c48207eca5ac37bd312a7ee0cff2b34d237916c151981fb9f

chaes.dll
8da49aecb2cfaacd0e7bcc593c23659b0133d781fc008d20ba15d14b878a327f
47164f7775e6e66a751e118e8e77798c40d129f1c148eb4fd70fcf1f6a5c7297

hha.dll
5b70c629563038f111c2329963cc2023a8cc6e19fb77f7fa6d857f6773c8388d