Detections
• Trojan.Win64.PURPLEFOX.YACAM
• Trojan.Win64.PFSHELLOADER.SM
• Possible_SMPFSHELLOADER
• Trojan.Win64.KILLAV.YCCAF

SHA-256

Shellcode Samples
• 25da2ebdbe2136f07bd414795082364cafda79d8271d099e78891b079158ed1b
• 492fdcbdf81ed196b35cdbb7fac85e3a8ee1edebe0803034df900f5e1a5049b6

Svchost.txt Samples
SHA 256 Detection
143be3d067188ae89a2c003ef2671bbdd790d6026664078098117cc7fc3373ed
Trojan.Win64.PFSHELLOADER.SM
21330417621547aa33b421a6d0834436453dd901dce75b9986ef3be743d1bdfa
Trojan.Win64.PFSHELLOADER.SM
7837ce02c57dd9fadd95882af162d46db5ae5718a59f0102478f62143a46cf71
Trojan.Win64.PFSHELLOADER.SM
88dd42dedc77e8ad117cc54d7b37083bbacaa6ecb84553bda31905b0a29e0e4d
Trojan.Win64.PFSHELLOADER.SM
1c8b01a100c0281153fe93168df3b79adc32bfb677c3a36c1d0d5d598cbe7cf3
Trojan.Win64.PFSHELLOADER.SM
0486df34e606d421e0f65aee68b5356ff1941f97c12f894f8b71318f607a54cc
Trojan.Win64.PFSHELLOADER.SM
9fb0a0dd309df7cbb7386f4de34be6ccc98ae64dde4773de99804871f49a4260
Trojan.Win64.PFSHELLOADER.SM
82490fa7297344ca9c37f901cbc5c43c5db51bba4b4a390589db0973d70475e4
Trojan.Win64.PFSHELLOADER.SM
ef979beb55c51ca22265c34a26154e916cd8f3f160d8b0ae1a2b393f13962a0c
Trojan.Win64.PFSHELLOADER.SM
ec6ea5da57991f343d28db611c076cb2bfd1100e69c6e5311d5295a05373801d
Trojan.Win64.PFSHELLOADER.SM

ojbkcg loader

SHA 256 Detection
4d0238834821461963c558e9ceb975b4e9c2a347ea447f9e044966eaf85f5281
TROJ_FRS.VSNTC922
53132712a773da3c3f15cc9879b8bc89b1a757a041fcfefbb8d75e3238d471d6
TROJ_FRS.VSNTC922
07719f8de2fe07722f1fa464fa7091830b835b58d9c5f99763b9a49ee0d0491e
TROJ_FRS.VSNTC922
8577bcbd02d38bce9601eb43511017b0bbc5176ebc3c48c08c81f755fcf216f4
TROJ_FRS.VSNTC922

360.tct DLLs
SHA 256 Detection
87d3ea42604943d2230cc0b5aea499da41fc7db46d141abf96875692040e4699
TROJ_FRS.VSNTC922
83ae0c568d6866c19960f1c2e2f2e28ee855c72d662eabc3acf50a09f1092730
TROJ_FRS.VSNTC922
799aa9612f9fffa5eab505ef3b9eabe78ac22f8f4bbe6b8f8cc2e8fca454667b
TROJ_FRS.VSNTC922

Malicious Archive Clusters
SHA 256 Detection
0926a30d0658671bf6dbb29a8cb33118930bb8211c90b170c2abfdc6a0e95b70
TROJ_GEN.R04CC0PAU22
1fd53c5ca08065fa72da9b529719166e08948204bea862681f2a04eda8c0a64b
TROJ_GEN.R04CC0PAU22
3f08a6f1998968b10bfbb19ffcb2904b96296a8c378aaa30e974cadfcd059e7f
TROJ_GEN.R04CC0PAU22
601a488c0c9804823866f1c4647fa60a90572edbb101e3247f75cfc2611999a9
TROJ_GEN.R04CC0PAU22
7bbe1fe9dc3346f40b3d6895dc9417b1c2cc5a940a41aaff39194588fc6efa20
TROJ_GEN.R04CC0PAU22
8d776597d31016863a00cee4da6a58db5c181337d7dfcacb4e239389af3cb2d8
TROJ_GEN.R04CC0PAU22
8df5b3d1e564397e838adf593714c97ade863b8caf81f666b93b4b0509062633
TROJ_GEN.R04CC0PAU22
8f7decbfc2c576c3b1401b9dd11183ea355b12a1ccfcf15d6a36d5470338bfd4
TROJ_GEN.R04CC0PAU22
937158fb5f7e2ddd0ca26e9d481be5e26efb85dee3bf77f06293ca5288973b92
TROJ_GEN.R04CC0PAU22
93d35724293f8582757fbb9f139645bb79f3ddb92c8c64c78ded31a021097ecb
TROJ_GEN.R04CC0PAU22
9a1aed2a2addafe001e8655cc869ba939f9a9b32ff55eb04282be435e12078cd

TROJ_GEN.R04CC0PAU22
9d8f53dcf25223d42c818e9f644b332064e43b9e3a26cfbdbc73b68af5580dd3
TROJ_GEN.R04CC0PAU22
9e20db31a624b1a255b2f7650efd9a1f20d6b077bc41edcfae88410198978941
TROJ_GEN.R04CC0PAU22
a24469103e727ece260bee7623387a2b339df206779bfb364388712606a1904d
TROJ_GEN.R04CC0PAU22
b061de89d542cd0a10558f6006e9a808ba32ac4d7ea54d2ba40f531d46919548
TROJ_GEN.R04CC0PAU22
b07b090547cb65dffb865dc9ef258a5e67e88555e798e6aaf3d0834bf2c742e3
TROJ_GEN.R04CC0PAU22
b2e0bd930dae20b4516b35d169b0583592050058d31ae84bcecefd2c15f13ddc
TROJ_GEN.R04CC0PAU22
c5245249c4f3d8851f6ce58d31b8406059e2a8530cfdbd4335f73110a1040f3e
TROJ_GEN.R04CC0PAU22
d152a38aa36cbdf9d384092fe81e3ddc93798999eb769e0e78bbcba4065f6b8c
TROJ_GEN.R04CC0PAU22
d239365a5e07cea9f7e56b9e1063f1fccfa883f654c68dc5f609d10a612262c8
TROJ_GEN.R04CC0PAU22
e9f7db12761d414a58aa2f4d1bda32698979e4e08bf42d03ae5fb1ebf11abb77
TROJ_GEN.R04CC0PAU22

Malicious Kernel Drivers
SHA 256 Detection
638fa26aea7fe6ebefe398818b09277d01c4521a966ff39b77035b04c058df60 (x64 Driver) Trojan.Win64.PURPLEFOX.YACAM
0ed3bb6be804402d10ee575d466cfaad59a0be42230a3aa47cf1e952f64970e8 (x86 Driver) Trojan.Win64.PURPLEFOX.YACAM
8cb47e54d1514bc4e6b4577d2a57117f1fbf9d89ecc6622c7a2515097b2e9b17 (x64 user-mode client) Trojan.Win64.PURPLEFOX.YACAM
e2c463ac2d147e52b5a53c9c4dea35060783c85260eaac98d0aaeed2d5f5c838 (x86 user-mode client) Trojan.Win64.PURPLEFOX.YACAM

Weaponized Execution Parents
SHA 256
• bae1270981c0a2d595677a7a1fefe8087b07ffea061571d97b5cd4c0e3edb6e0
• d25542837c28619603fce465a6876b2984a3c191a908fa57ca7f5b8f8d803180
• 4c2ce3ed2ad22a531500046c0a9d790979b7885682aec6160a73ad259eb08cbe
• 5f4d31e77dd5b36943212dd55a0747923a69ca1e0f5efea607fc063d86b35995
• 111760bb8191b37f89e27f474d29faf77b0db1ae4758d6d08a152e36a9167cae
• 71ea052cf6919ed6da26e5fc27df0236bbc0cd36509852c74144b0ba76ee1264
• 2d288f2cd6752a01360f2669959e2c61f676f8156d5cc40d4b415245ae04cf6d

• cd38695e4760df90b049f3faa19a826814b60632f74402cd0feddc93d116848e
• a5d478171338ab83634f39d6663ba8db328b24ddffe32dbbddb0da8784ef644b
• 608b3486309d15bed054e22e20d87c44e43a6cde3dad6942ef592c9d3c4f3cff
• 8ade56bd356d12804d384ca24fe876346498a25870f6caf08e16d0c73e5abe59
• b8950b21a65f9699f0965dda2d61d61ceb1ac8b888b84adde8040b3cf25d09c4

URLs Distributing Malicious Installers

• hxxp://58585[.]xyz/tsetup20473[.]exe
• hxxp://xiaotaiyang[.]xyz/tsetup20473[.]exe
• hxxp://1077cp111[.]com/x[.]exe
• hxxp://whats[.]jsnsgjy[.]cn/whatsappsetupr.exe
• hxxp://kkiiz[.]com/safety3[.]exe
• hxxp://zhiyingzhifu8[.]com/flashc[.]exe
• hxxp://whats[.]hswlkjh[.]cn/whatsappsetupr[.]exe

First Stage C&C

IP Port
194.146.84.244 4397
194.146.84.243 4397
194.146.84.245 4397
194.146.84.242 4397
194.146.84.246 4397
107.151.64.102 4397/7788
107.151.64.101 4397
107.151.94.68 4397
107.151.94.69 4397
107.151.94.70 4397
107.151.94.66 4397
107.151.94.67 4397
107.151.64.100 4397
107.151.64.99 4398
107.151.64.98 4398
23.225.132.246 4398
23.225.132.245 4398
23.225.132.243 7456

23.225.132.242 7456
193.164.223.77 7456
107.151.113.219 7456
107.151.113.222 7456
107.151.113.221 7456
193.164.223.78 7456
107.151.113.220 7456
107.151.113.218 7456
193.164.223.76 7456
193.164.223.75 7456
193.164.223.74 7456
193.36.112.189 7456
193.36.112.190 7456
193.36.112.188 7456
193.164.222.130 7456
193.36.112.187 7456
193.164.222.132 4567
156.234.65.84 4567
193.164.222.131 4567
156.234.65.86 4567
156.234.65.83 4567
156.234.65.82 6688
156.234.65.83 6688
43.240.238.252 6688
43.240.238.254 6688
43.240.238.253 6688
154.39.248.37 6688
202.8.123.68 6547
43.240.238.251 6688
160.202.170.62 6688
202.8.123.124 6547
202.8.123.122 6547
202.8.123.117 6547
202.8.123.99 6547
202.8.123.232 6547
202.8.123.81 6547
202.8.123.233 6547
202.8.123.36 6547
202.8.123.35 6547
202.8.123.190 6547
202.8.123.153 6547
202.8.123.160 6547

202.8.123.159 6547
202.8.123.98 6547
202.8.123.97 6547
202.8.123.97 6547
144.48.222.252 6547
144.48.222.220 7777

Second Stage C&C

216.83.35.130:10022
43.129.210.43:10022
103.145.86.160:10022
156.226.173.202
144.48.243.79