IoC from Operation Dragon Castling

github.com/avast/ioc/tree/master/OperationDragonCastling

avast

Malware analysis and more technical information at https://decoded.avast.io/luigicamastra/operation-dragon-castling-apt-group-targeting-betting-companies/

Table of Contents

Samples (SHA-256)

setup_CN_2052_11.1.0.8830_PersonalDownload_Triale.exe
b9bea7d1822d9996e0f04cb5bf5103c48828c5121b82e3eb9860e7c4577e2954

QMSpeedupRocketTrayInjectHelper64.exe
a3f3bc958107258b3aa6e9e959377dfa607534cc6a426ee8ae193b463483c341

QMSpeedupRocketTrayStub64.dll
76adf4fd93b70c4dece4b536b4fae76793d9aa7d8d6ee1750c1ad1f0ffa75491

IcbcLog
FFylbet0825.exe, icbc_logtmp.exe
A428351DCB235B16DC5190C108E6734B09C3B7BE93C0EF3D838CF91641B328B3
F95441B1CD6399887E99DBE6AA0CEB0CA907E8175192E71F8F1A4CCA49E8FC82
A428351DCB235B16DC5190C108E6734B09C3B7BE93C0EF3D838CF91641B328B3
21EC1DD34D4B7E13A474A1F31373AD041486111EB490527B6533AE2F5A38B73C
1099523C5509DB1C60C9C5D57AA625636CFD820DB4AC60E08E881C256D20EB72
E97C242C5A520F3C34E844032D9545E4B492D45643ED16F4E4884382769C75F2
21F20033AD20070BCCDB4502A50844172EBB0707B8A2F17F573417C861CDDE33
07E9A7732890CF06E479FEE41218EEFE404EFF1BB29F888D9384752EC8D51E6C

log.dll,logexts.dll, xps1.dll, kwsui64.dll, MainLdr.dll
97c392ca71d11de76b69d8bf6caf06fa3802d0157257764a0e3d6f0159436c42
e5adbe232c40ebc8fb01eb255e53780f8d2802917dac3bff46c891532766c43f
cad70ba1f6d84f24c9fdfdedde4b7ba30eafb1df0fd44d31f5c7fe79c3101d5c
97c392ca71d11de76b69d8bf6caf06fa3802d0157257764a0e3d6f0159436c42
8597851af00c45643b32385f087d4f738b646db99b7d7b1c1de347441513be13
50a02323e184ce986338c32f22017045432179be5ae23f3154ac214b7966a7fe
0de5029181ae2a9e20bf63afb27bbf0ba4c4b99ed042780af0dfd3c568f3c8aa

Proto8RAT
725E252B9A759587BFFE569832C002108B57127DBDC4ED7BDDFEC04C6A2E1D41
FC79292D018D012A862DF3410843D46C0ED98C7BD31D6D14A6FE37E31F029854
2DCA8979132502986F63AC9EA31BC97B94F057767445AC13F4E973C8D6C41DC9
24CB273098E09256BCD512DAA980C1260533EA7133EBF1D8F2169C059431F2FB
598CB15CD9238505F52254E4FB21820EA7778C370D2BE7E3B855B2D89B2E07BD
EE0F0728298D82D776D8AEA6ACB74B05B0FC0662B547B2808A21B96102D491F4
2039388615E2E23B1AD18BAB3325610B1EFA384CD9BBB35046B18FB6C8C9434F
98CDAB8E5B0ED2F36F02B3B4B8DCB7C87A64E6295166F9B55324463CB327A454
48F11027EF15D68C3E6D943F21B948D346EF16BEC3E0F3E0E658929C96505275
63ACBCA38798B7C22BCE921625AA6698BFC831AC78B62D4E17A9C56E224D1A46
0A7B22D9736964187FFE62B90E94024EC877351089AB08DE21E617DC1B412087
6D0C6985409FA2BE2A22E187877C8318914A53DBDB760561E1D8162DB7E29371
C7F5D2E0C9E70B850EC49E817A5018DAD6676C77D50DCE3B1B4292156486C57F
3361E03AD94152F1B7823F8256F4DCB857A43BB84DCBB44E6E84A5338D5029D1
93318870A3F07E37DA24D779599EA49D678599A9BB853DFFC9A5680320886F04
EA5FD29FD8BDE88061F96F009FA7C2F34B128D9B4713779B2F8D2BB33B42FDB7
9F1CFC0C76527627E05ED9A4517861173309D30B624BAA4DB0E2D105C3C47960
0FC8216BE472B8CA45AAAC5AC0BC50DDB9655B5FD8CBFE743482F4C9CBA27DE9
88A55AEB2A66E71ED20C5E852C7AF04686C1D9A1C36769F5094FB68D2047F8EA
E1C6A75BCB10F2F058F8896FB30FA3087F3F39E1B26CA1567A8092165DBCE6FC
F3ED09EE3FE869E76F34EEE1EF974D1B24297A13A58EBFF20EA4541B9A2D86C7

573423DA0EFA9B5E46948C75D1BB9552E2723BA4FA075E65BF0CD4B1FE91441C
FF556C45BB1734BC2F29D7465291A3A4C209EF4DEB91AEBFF81634934466C00D
8C6762907239CC90BF35B7B37708D98D25B374A3BBA8E6DA45CAA12785050224
DDB2EDB9096674A916C0CD88C81BE333DEFC7D01D0C36848E57246DEBCCC6DD2
EDC0E6B563A0FF923399FA001797D634DBDDBA83E6B724B190EF6D07943BCE87
C834C78F38E6BE48AF2D28777D9D2ABEC06B665307DA78C31F652EDA19A52FFE
2DFDE7FA4F4D5E0DFAC3E62A18CFF7A8EB148DCC114DC9A641B7CBD7715ED252
6101F635240EE5805C29EC2CB3A9AC0D34F7F7E05D021FBC55EEA3E0B8D4D55F
E074DA895E4C030D047C7785D3DC95B9256EE40A1BDF16D58E569BE421901E0D
1C8F486475A433B908599E4A38DED1293A492421E9C476F62C0D499066B76904

MulCom
ABA89668C6E9681671A95B3D7A08AAE2A067DEED2D835BA6F6FD18556C88A5F2
F1B96BD59CDF8F180DDDB7F374777A1A9C34FAA6FC14AA3F1EEB5A185702F888

Atomx.dll,xps1.dll
2abc43865e49f8835844d30372697fda55992e5a6a13808cfeed1c37ba8f7876
3988d3fc02f3139d16536e5e7b34fd0fbe8cd19102a2c8ed56c2d77d105b3119
ea1bd2a9a76ce691f729f3a1b71e35abe68e2150f72538fa31ef9d5183e8a16d

kb%num%.dll
4C73A62A9F19EEBB4FEFF4FDB88E4682EF852E37FFF957C9E1CFF27C5E5D47AD
2152cfc0ba9efeb10ef4b1578bf75c507503e7c8fa1c4dd7d21080ef6327c69f
ae357f0965758777950f8554c69f836eba20be0568eea98cd714f6d16411277f
b1d0ec3a0779132afe3b4f9ca8b84c59ebf036a40e64d85deec2b21ca0344a85
c5e53e3d485fdda982cd5949ea125482256bfd76d4e725a874ddbe89dd06e9d0
2d80b1562cc68d68ff1ebf9b46d901ad5db12464bb4c8533432d30aba608b896
fc4c4d523708432defdf7f68d3c13efbac06d57173feb45bbbd76442ba37cdaa
652f4ac2143ffd69366caf53c26bdf5a5197f0145d86cb8cb7fbfc97b7fac1e9
ee21e0964bf4609a5fcfab0b207e550f14e434567352e81f1abd08ee794eada0
7dfab9618fdc46fcf9c072a2bb93be8360c90a67b5e21da0359b636387955d82
8cdfb7c4bf1102bd7cbc5806bddc983b8ba6a2158d2efd31d76eb1b4ebe08fdc
99553649c24af7d5e72c26ea50302fb165fc2407985a536284a52670eb02b625
0adc108340ec513f0f73991ff1f60952be7f9b8a8448f4663b711b1c9c8acb73
3d29a00fe8c3b79efbb745216971286b331e5791959eff92a6a2064506e2fdc2
e9990aa62a587ddd5b33fb1f251d3c4a8de3a0cd5d5e99a326dd70ce2245f9fe
176b5808fb0e8de31912121aec8802898ca648149ec5de1830c64c283bebecd0
2b946ceed774dd9961e8cf60f633144fca5c558d4b4922102daa3b3cade2db6b
547c6a00c623fa4d88bac6be46ffff076d6e35dc20f9ab91327a6bc5f5de4f9e
66e7f55a02a53ce43272ae3fabbbd47191d02292d8b4ffd2aa5f590ed6f2245e
a2ce1f19522ce3a88b4c90b8db5fd688e18366ad3a7d1831141b449c1e854305
5676f1a9de017dafff2dab09a8ff269945d900bea6d2ce7d53fdb7d4d7e5311a
f94ec386ced1cd5e480b4a483a5c55586d157be69808f83afa50c75150c5da0d
88658a1d5e6758c098ac7e5ab7284ff53e172aaadf4a6a4bf8b0f0e7fefff14a
77890e3c6f1228408abda3722e69a0c43c4517bf060734850878af144724fa1a
263e7da3d34b1753b75f3423a52790e8f666fe5c9f9c8cb6accdec186d50d24c
796accd99b52b646cc6622792d7fa08baf53c741ac5fe88fb1f9b51de7b5de51
5a42d03593d17f6440be019b55e54b11fbcff74aa02b9399eb23fafd6f2d7310
7acc7c25cfede4c7a30185d61853b887f799773e5d6ad4251260871bbc68131f
4c73a62a9f19eebb4feff4fdb88e4682ef852e37fff957c9e1cff27c5e5d47ad

Network indicators

C&C servers

```
103.140.187[.]16 - DNS resolution on
htxp://update.wps[.]cn/newupdate11111111111111111111/2052/bigpatch/setup_CN_2052_11.1

23.106.123[.]196
207.148.125[.]97 - in smcache.dat

server.avastbusines[.]com
api.gpk-demo[.]com
api.geming8888[.]com
cdn2.twmicrosoft[.]com
http://www.ffyl-bet[.]com/
help.tiger266[.]com
www.animal777[.]com
mirrors.centos.8788912[.]com
themerecord.com
yd.full-subscription[.]com
zk.full-subscription[.]com
cdn.1685810[.]com
static.1685810[.]com
login.good-enough-8fe4[.]com
http://23.106.124[.]136:7865

time.daytimegamers[.]com
static.daytodayup[.]com
http://cache.download.banner.dragonfish88[.]com
cachedownload.goldenrose88[.]com
```