A Bazar of Tricks: Following Team9's Development Cycles

July 13th, 2020

IOC	Type	Description
1e123a6c5d65084ca6ea78a26ec4bebcfc4800642fec480d1ceeafb1cacaaa83 56eb71f706043c7504e756379b1869adc4c07b93327c0bd4ff83d9bdca108804 a76426e269a2defabcf7aef9486ff521c6110b64952267cfe3b77039d1414a41 c55f8979995df82555d66f6b197b0fbcb8fe30b431ff9760deae6927a584b9e3 835edf1ec33ff1436d354aa52e2e180e3e8f7500e9d261d1ff26aa6daddffc55 55d95d9486d77df6ac79bb25eb8b8778940bac27021249f779198e05a2e1edae 4e4f9a467dd041e6a76e2ea5d57b28fe5a3267b251055bf2172d9ce38bea6b1f 859fa9acf0b8a989a1634a1eee309355438b9f6b6f73b69f12d53ac534618c6a 5a888d05804d06190f7fc408bede9da0423678c8f6eca37ecce83791de4df83d	Hash (sha256)	Operational Loaders

7f757770f2049c23624a483feb6e9331693ded0dafb9c636f96fe6b9307a704c b2583eb8e1d4241644ed9c366bf5ef58ab1a4fa26788358c6b14fdb48d0261b5 467c33cb979804dad154612a808f2ea234f7501f8d36bf610ed457cc48993c49 f6cddc2f46ec3e8dc95b6fe42c6f30745bf0e7d3e9788c35a96199c82fc04f66 b2478fd8e1cbaed66ad8f46e7edbc0f61b4eb94e5c10e1df23efed86a1ea4490 8a0ae971d0f4dc4c1027ff117fea0761d042baa6b8a6f6451410b580597f7021 2e99ed535a9f73bafab151ec409de04c953a0187cb8e4063317617befa09068d 911ad05e24337f4e9c648b81ff5d94d54b30cb94b69601253085a5138913adfe d04bdbff24b1bed41536664bb9696387fc6e88756efa76ecf345937e7cfa014d 04ad133967d2076e4ce4cbd04c058ba7e8e3725fb72102e2b1b5de433f44de33	Hash (sha256)	New Operational Loaders
3fe61d87c9454554b0ce9101f95e18abad8ac6c62dcc88dc651ddfb20568e060 b10dcec77e00b1f9b1f2e8e327a536987ca84bcb6b0c7327c292f87ed603837d 363b6e0bc8873a6a522fe9485c7d8b4cbcffa1da61787930341f94557487c5a8 8f552e9ca2bedd90ce9935a665758d5de2e86b6fda32d98918534a8a5881f91a a0d0cfa8bf0bc5b8f769d8b64eab22d308b108dd8a4d59872946d69c3f8c58a5 ae7daa7ce3188ccfe4069ba14c486631eea9505b7a107a17ddee29061b0ede99 f3c6d7309f00cc7009bea4be6128f0af2ea6b87ab7a687d14092f85ccd35c1f5 35b3fe2331a4a7d83d203e75ece5189b7d6d06af4abac8906348c0720b6278a4 5974d938bc3bbfc69f68c979a6dc9c412970fc527500735385c33377ab30373a c7d02d16e35449bfbd571667d2c571657aa526d58891242884e1f2b81ef932e8	Hash (sha256)	Backdoor Dev version 1

2342c736572ab7448ef8da2540cdbf0bae72625e41dab8fff58866413854ca5c 8f8673e6c6353187dbb460088adc3099c2f35ad868966b257afa1df782e48875 38c9c3800dea2761b7faec078e4bbd2794b93a251513b3f683ae166d7f186d19 f83a815ce0457b50321706957c23ce8875318cfe5a6f983a0d0c580ebe359295 079a99b696cc984375d7a3228232c44153a167c1936c604ed553ac7be91dd982 0d8aeacf4ebf227ba7412f8f057a8cddc54021846092b635c8d674b2e28052c6	Hash (sha256)	Backdoor Dev version 2
3400a7df9ec3dc8283d5ac7accb6935691e93feda066cc46c6c04d67f7f87b2b 2f0f0956628d7787c62f892e1bd9edda8b4c478cf8f1e65851052c7ad493dc28	Hash (sha256)	Backdoor Dev version 2.1
94dcaa51e792d1fa266cae508c2c62a2ca45b94e2fdfbca7ea126b6cd7bc5b21 f4a5fe23e21b6b7d63fa2d2c96a4bc4a34b40fd40a921b237a50a5976fe16001 4f258184d5462f64c3a752ec25fb5c193352c34206022c0755e48774592b7707 e90ccb9d51a930f69b78aa0d2612c4af2741311088b9eb7731857579feef89c3 6cbf7795618fb5472c5277000d1c1de92b77724d77873b88af3819e431251f00 37d713860d529cbe4eab958419ffd7ebb3dc53bb6909f8bd360adaa84700faf2 9d3a265688c1a098dd37fe77c139442a8eb02011da81972ceddc0cf4730f67cf	Hash (sha256)	Operational Backdoor
www.afboxmarket[.]com www.allacestech[.]com www.almakaan[.]com www.asg-bd[.]com www.bakedbuns[.]com www.bsrdesigns[.]com www.dubaidreamsadventure[.]com www.machunion[.]com www.petromltd[.]com www.ruths-brownies[.]com	Domain	Domains serving Bazar loader files

www.qfcallc[.]com www.thedemocraticpost[.]com www.ottenbourg[.]com www.ajeetsinghbaddan[.]com www.shawigroup[.]com		
35.208.42[.]2	IP	IPs serving Bazar loader files
bestgame[.]bazar coastdeny[.]bazar eventmoult[.]bazar forgame[.]bazar newgame[.]bazar portgame[.]bazar realfish[.]bazar tallcareful[.]bazar thegame[.]bazar workrepair[.]bazar younika-hayde[.]bazar zirabuo[.]bazar	Domain	Bazar domains
45.137.148[.]207 5.188.168[.]87 149.81.169[.]126 185.122.58[.]37 172.106.88[.]242 171.50.138[.]196 51.81.113[.]26 192.3.193[.]199 185.244.149[.]46 107.155.137[.]24 34.222.222[.]126 71.90.222[.]141 71.240.225[.]169 185.65.202[.]58 45.155.173[.]166 62.108.35[.]221 85.204.116[.]149 107.173.114[.]117 217.12.209[.]60	IP	Bazar domains' IPs