Severity

High

Analysis Summary

Researchers have identified recent Mustang Panda activity that involves the use of DLL side-loading to deliver PlugX. The initial infection vector is an executable downloaded from a remote URL. The executable is responsible for installing the malware by dropping the required files (a DLL loader, a legitimate binary, and the PlugX payload) onto the system. The legitimate binary is the Adobe CEF Helper and is vulnerable to DLL side-loading. When the installer runs the legitimate binary, the dropped DLL is loaded. This DLL is the loader for the final payload. First, it reads a hardcoded .dat file that contains the XOR key for decrypting the final payload, then it performs the decryption and loads the malware into memory. Once running in memory, the PlugX payload is able to decrypt its configuration data, which includes its installation location, the XOR key for C2 communication, and any C2 addresses and ports

Impact

- Information Theft
- Exposure of Sensitive Data

Indicators of Compromise

IP

- 101[.]36[.]125[.]203
- 103[.]159[.]132[.]70
- 103[.]200[.]97[.]150
- 103[.]75[.]190[.]50
- 103[.]91[.]64[.]134
- 107[.]178[.]71[.]211
- 155[.]94[.]200[.]209
- 185[.]239[.]226[.]17
- 18[.]138[.]107[.]235
- 45[.]248[.]87[.]162
- 45[.]43[.]50[.]197
- 5[.]206[.]224[.]167
- 61[.]38[.]252[.]166
- 92[.]118[.]188[.]78
- 95[.]217[.]1[.]81

MD5

- 56f27cd9e8556e9c61fb60e6041e8c9d
- b0a7b7a1cb4bf9a1de7f4b1af46ed956
- f2ba9bdc31a95d249679f685dfd2a39f
- 84545b406b428a0028c6cb25dd85bf2d
- 7b2f41b57b9ab4151eb37ed69db9fdf8
- 25a14e50486c738bc92da69c02063e23
- 4b07e341a2bf00479dda19b18ca41362
- 69ab42012ddce428c73940dcf343910e
- ad3ddb4cbe7ece8cb723f63f3b855b85
- ae358c1915e794671a1d710d9359146d
- 6459baafa8ad9d4bd6b360d3a423f921
- a84958c32cd9884a052be62bdbe929cf

- fa063454e3bda1433bdd2725dfac4487
- 2102d225508c1f8f488a3f1574a34759
- c7c9fee23de57ff885932849a237e6d5
- 530ed2cbfc57b9e6ae6c3fb3a1ecde9e
- 8a7e2c7d4be6f17a851bc6b3d10d0d45
- 66ee022fb975899281885d0e5af55fbe
- fd7f4d575fd26bfd74c69ba1392368aa
- 50c750ddd7f79627f27e48a7dbafeec2
- 84d1d97d298fcbe237a6270b10e6984d
- 01d8305b91524d83ccf2c26c1b3b7f1f
- f31d40ea1e73c82fcbfee606fb52169e
- d404e3cd5f1c6a50f10f56f5c5b9c1e3
- 3c6173d8693510f6363b608c09feebb1
- 385a4ca1da76ca4cbbbed6e0ef659f1a
- 66ee022fb975899281885d0e5af55fbe
- 257813d292c494797a957f0992ba1405
- c5f4da8c703696e2fc034cbcc3da6336
- 706e0f37a49e013b9fc73a5c05fc861a
- c70d8dce46b4551133ecc58aed84bf0e
- c43de22826a424b2d24cf1b4b694ce07
- 43529e54971a2302ae736c40f39d65df
- e21e8f398c6d61ae8335664b1ad0444f
- 2d79767e4f6118afb9e86351be178b6d
- fc9e85df9fcbaf261117e94d0132369e
- 67e017eb7658e390534abc6f55e6af49
- 3c99e3522923b6ec94093e04b7e13fa5
- 50b3fb6a2cf209d4bcbea0546e82f58f
- 3c7469e92990c6a879fad4e1e7fde5d2
- 3b63e3ab2b668abb7eba8f84602df48a
- 6cda632104ed1cfb1d03e2bbdb3e443c
- 84aef9e9285aff8d1551b0ee6f317292
- 34161eea2f66156969291d6ec53717c8
- 27daaa3f672d6c584dab4bed2cfda8e4
- 1072897b03d0566af54edb0f3826b834
- 6be83a1652c6b3dfb8663aebec3515c7
- 41aa7cdd6c9ed2ac0932d8084c89f28f
- a5660a4a5314f45f67d36d04a37e3571
- ac1c480ca73e1122893995fad3f7f469
- e7904b4253f0b45fbe94a38b3946a621
- 81bebcb517930bef9ea182431719c132
- 6cda632104ed1cfb1d03e2bbdb3e443c
- ba9565a7faad19b2f6e80a75877fe938
- 91440c1865391355b56dd7cc3edf89e8
- 89631ca603d9943c110fcf2c7fba0f6f
- 44739c501fcd8b9c0eb5b7f74fff9a00
- 35b69a125081c5efc6960af0f9b22948
- 3f4e55daf8722d0656b3f7b9bdd4c22d
- b2a22ff19524a849dec35dc75124be91
- fec055d1adf03781e3e1427dccdb94b9
- 80f4ee699f480a6a0c47866d79ea3f4a
- 363f07437cfa756ba2bcaa59e9da9416
- bb1506cc3c26b3ee120fc7fd388a8a58
- b502b41727f1e54b8475f9947777dbe7

- d3ee0db7e36a88b4b446a5baae8eddf9
- a5e391d64d5771c1150bbafaa4fba173
- cc197ffd0972660b71d0f1ca86532119
- e87769ace15726fdd508c56f7cb04fcd
- 4d8dcb1f33180c55e42d0d682a6596b3
- c70d8dce46b4551133ecc58aed84bf0e
- 8568bae4c4bbd7f969ba3f1514a26c82
- e123c2f0822ec9e459f3ba16793c14a7
- 697d783f4dfb937c82250fac4efed274
- 6ca3439153577503fd71f7039a0045ab
- b8a78e4e76673b68e94f5312d7e3900d
- 37f19e06e38b2a8ad9d65a6575ad3413
- befa31048a67e9bf37afa92c97f6fbe3
- 8b941c0b80312c1c630b9c0062d86e30
- e9101cee85038bb0f306ef83bc36523c
- 4efd3d2f09f17dae19f1d5b967ec9949
- 332a4f864b1f7b1e166edb5d9b47e119
- 7f0079d2ef1fca0b4bf0789aad3d2b04
- 8b68dc5dbb99af7de3312771e828b6c8
- 37d1df5648c2e499b23b4228743f0318
- 34085fa3adebf09faac315540db16cb4
- 4a9b98832ba5c2b74f80dadd16b8a079
- be8927e1d6ce992982976cc5f3dcbb92
- 13e51c336fe50f8cbc80a7fe06a3e788
- 5959d00e2d7b57e1e5885750c0900946
- 1d281c5353d1b12afb9c4a4ae61e5675
- 377956881a132dbb70c6f0dcf07b7d47
- 866ad225f9c997a68aa916ae9c8290f3
- 1d281c5353d1b12afb9c4a4ae61e5675
- 0ed497a020ba9ca230e378f339b82f07
- 030265a85b5c84a2263e9aae8562b86a
- eeb2121925451ecb3eb5d79f18ca17cb
- e0977e26e7b850e20fd94fefc79af65f
- 10d0b2b4fd787d43ae20244788d38e8c
- d9172a525c8f4a7932559c2ea13ac002
- fcd6691fc59610a50740a170a8a5a76f
- e7d91f187ff9037d52458e2085929409
- 793d0e610ecac2da4a8b07ff2ff306ac
- 72dd4b3337e0c9a70cf772e2b21f87b9
- 6f580dc7648e7f9c025317f5ad096f3f

SHA-256

- bee9c438aced1fb1ca7402ef8665ebe42cab6f5167204933eaa07b11d44641bb
- dbdbc7ede98fa17c36ea8f0516cc50b138fbe63af659feb69990cc88bf7df0ad
- 18230e0cd6083387d74a01bfc9d17ee23c6b6ea925954b3d3c448c0abfc86bd2
- 668cc21387e01b87c438e778b3a08c964869ce2c7f22c59bcde6604112d77b2e
- 8a7fbafe9f3395272548e5aadeb1af07baeb65d7859e7a1560f580455d7b1fac
- effd63168fc7957baf609f7492cd82579459963f80fc6fc4d261fbc68877f5a1
- 6019e6ee3dee2ec798667ccb34a2ab8d70bf5960d35f55157a9cb535b00b243f
- 436d5bf9eba974a6e97f6f5159456c642e53213d7e4f8c75db5275b66fedd886
- ca622bdc2b66f0825890d36ec09e6a64e631638fd1792d792cfa02048c27c69f
- 492fd69150d0cb6765e5201c144e26783b785242f4cf807d3425f8b8df060062

- 2fc14451ef0ff0919995d46fedc7b7c7f9a9adbf9c40f6b36b480e637d581e6b
- 1aafbe976c3559b61531910c75f9bb90176641f565f9810a18dcde9564241164
- 7ded20b7d2c0428641a6ac272c15b444b37bf833bbbea09dc931d649e6dc5277
- e1dbe58393268d7ddabd4bed0cdedf0fbba85d4c3ef1300580ed4c74e147aa61
- 16dd94c228b5e2050d01edfe4849ca1388e9b3f811d39380f6ada3e75c69b353
- 6fd9d745faa77a58ac84a5a1ef360c7fc1e23b32d49ca9c3554a1edc4d761885
- 706e53480da95b17d0f9f0f5dc37a50c7abc3f954ce15b4733fd964b03910627
- 537ac2f79db06191222ba7ae7b7843f063600f87971b8dffc4a31459d6a144b1
- 3aa80dd8ffbc7b364234cdf0849b10bcead52004fc803a74afb1bd504d024305
- aa8fb15d63bd22b2ff15a9f1b4f4422b3c6af026915168c81d7bb38c9be2ab78
- 567fb0e6e6667ce1674cbdfd0ab26a8a3f68979256ef6680facf1d2d50a25dba
- 1b520e4dea36830a94a0c4ff92568ff8a9f2fbe70a7cedc79e01cea5ba0145b0
- 4c727e21312355cd9a9f0e1e0bb8fc3379f487968a832d00ffde9d5a04b8da9d
- 017ef960616182daa1ffabc5d5470340cc45bbd5ab3455d74987a3ae478fa118
- 5851043b2c040fb3dce45c23fb9f3e8aefff48e0438dec7141999062d46c592d
- e2aff9d2f5e75bdc09712722d919f2261f638b0b4da878e405b86b927dcaf1e3
- 537ac2f79db06191222ba7ae7b7843f063600f87971b8dffc4a31459d6a144b1
- ec32ff0c049bd8812a35aeaaaae1f66eaf0ce8aefce535d142862ae89435c2e2
- 930b7a798e3279b7460e30ce2f3a2deccbc252f3ca213cb022f5b7e6a25a0867
- 6a5b0cfdaf402e94f892f66a0f53e347d427be4105ab22c1a9f259238c272b60
- 0459e62c5444896d5be404c559c834ba455fa5cae1689c70fc8c61bc15468681
- e3e3c28f7a96906e6c30f56e8e6b013e42b5113967d6fb054c32885501dfd1b7
- 235752f22f1a21e18e0833fc26e1cdb4834a56ee53ec7acb8a402129329c0cdd
- afa06df5a2c33dc0bdf80bbe09dade421b3e8b5990a56246e0d7053d5668d917
- fc8b2392b92860c7ca669d5274b65498ebd9c3992149cf6727d935c9d0fb48bb
- c73c644aa671d76918b56f2ce0124a09156a521e293091b68e2763d2ed386e8f
- 98f139983882e443116863f795c1df50dae5ceb971075914dfee264dc1502a09
- 39f9157e24fa47c400d4047c1f6d9b4dbfd067288cfe5f5c0cc2e8449548a6e8
- e4766d7e0c13f42cf1ce56efa07cee57889526f398efaae948ce487410d105f6
- cab5fa13c8239e97c15b04b27f9b70fb8b561d31935af7b0680bb80aec12c813
- aec41c4f461cd08efe1390c8de513e54f766a5903c3c1f67ac4a9c93a3213c6b
- 71d09abda31f0d7c7161cf6f371305023594bb3ef146aa9fbeab1f717885dd58
- 8a6da7e23267cadb1b8ec3996d662cbc71342f308ca6b65f545ce78612dfc9a7
- 86678ad613b4d05a8ad3013323875daa91c69b64411603187dd2bcc595d97a8e
- 033786a482641aa901a28a3e3c314dbe86723906cea15147629167d8364907f7
- 0492124645a667b1ca39002aff4b696871f12f7f21ab0a75816aaeb53ed2f78b
- ce86d647df2da33c5992c790ddc0d302b56af8a0d7b1433639c235ff03bf09ad
- cf7803d1546aab172d17345212cc4de9c2d98a9817c8f9c3770e64744e15e261
- 1d3e2eeaec0707e531593aa9aadaee0ee7757b67de43eae924fad122e86f60a0
- aa9a8f143cf61118c96a3bf226c77a05072ccbef15e990c65e0a118eccbb47e6
- 1e629fe7c8911a9adbde2e35af4f6f9e60ee538638c82edbcbd7cce5ad2ff4ab
- 36afa5b3133667f2577687b3e83d7f6c009dd65864c20a408d860b3c6678df2a
- 71d09abda31f0d7c7161cf6f371305023594bb3ef146aa9fbeab1f717885dd58
- 3407c5d054491ecf28ea10ec24e30e75915ba6fd3b2656955e94a89b67e0567e
- 67d6267e0ee81e00f97b25a892d10bd9eeb68179eb7e1b9236fcb01ec3f50beb
- e92e49b7af397f6f41a225b8778c6812f78c87f4388f527e6efda0dbe2b49251
- 2fd6e2ae0e4d78eef9d36376ac39768ec14e3bf8fe39c3ef6a347511b2cd55b1
- a1a61052eac5fbe98f28ed6b3ed38a66d333aed3f14326bcd42d0fddcc18c519
- a3e5473eb60e8dba6b97e626288b6742e141fa8a393ec7efeb7993449f84b14f
- ec60594018da8717fa6b8d93fb919f08e7a8b07401fbce1abe7982c959f78424
- b9adc1433ef7c6fee4d36f73b79744ad611d51a8e039d4c384dd453e33452d0f
- 9b7615b4c2c6ebdd283afb1dae4d951b7ef928939b98ffbe7dea49cc5c5eee02
- 951b09c559fdc1c447f3dc63870b5244c2b715d728e1318a62db64bc17dcb85d

- 4743ccff0b5dbc34027165e177143018b9ee9e3232496ca5d4fa5cd56b5646f6
- 302ae30d464d6958510dcc463e3c3d8339e38bf6ff84de6cd84866303d34c8a5
- 4d01691573542e1676fc09102ac3120d0eec37b6791f32ec103eb0d0ee2581c1
- f863dab6504fa3c4c9f7534d264d13db95ea96679689cb7e5d0460eed8f59a37
- 61a194cd413614e5ac91d648a87ff6b7e78d2130f54eff8a05c4c9608a7ac3aa
- 2bce6eb2839569ba077e24468259aa2678677275c632a0d276dcb14566cc6fcf
- 150525f4490f43877f1281aaaccc9bce78452d556326105fb77db6156095c883
- 0459e62c5444896d5be404c559c834ba455fa5cae1689c70fc8c61bc15468681
- 24437d65bee4874fba99a2d57bf050ba719a69518160cebafbd8f7441368093a
- d1f848a8477f171430b339acc4d0113660907705d85fa8ea4fbd9bf4ae20a116
- acfd58369c0a7dbc866ad4ca9cb0fe69d017587af88297f1eaf62a9a8b1b74b4
- 5928048ed1d76df1ae4f3ede0e3da0b0006734f712a78036e6f4b6a78c05f0c6
- a81719f585a9f40e4304c6ceb2292826676c2d3f7342e88b21f41139743436aa
- 02ec5c7a7ab17540164b4b499fa095e80113123b3ccba6dda59b5f7021b93e6b
- c3d113bfc14a7148419d506e9bd8d44d897f3c71f8d81a63e3b2f4d843ad1c4c
- 1d72fdb8257a6ec78367f2512ceb18be4808603209868459437769 59cb4d3dd0
- 8f07bd408838182a0328ea44156ad47dd5b6ccdcfbd53209717d555ed69adedc
- 03c5f4cd4a0889f436cd1ac2634b2c76732ce7f280e294ab3a19e8c1e957f101
- f76f1657205d7042fccfc811077bbada92c0fef735f158da35e7825da1cc6bec
- 92f1e5424d53e3f4516d4c831afe3d64e88ed265ec143fb32717f2323836d61b
- 0b949d6e2078771ed65ce1b81ae9b5619d24317846a4e67bb9494975049bf728
- 377d65bdbf2b323ef9b497b1d3e2f93521a9ce57d4f2d6c296b048ee1390173e
- 962bf22710ff07977e3ddad66117094a2cf1c0aefca3d7ed4ba947c62ee36491
- bb2990a1bbc417cfec40d5f1a6a8b22cac0ef21aed869dd8503e28573cf84401
- c26719156e644cee5e95133d31b30b80147494313e665d4243954435511f5c11
- a6057292247d928e6adcda5a48983d8702372ce195fc50ea4496f67c6ca57e26
- ce59d8cf4b6eca3420438e05b059d6f61cc484e6fb00b1b2a7033bf36446e683
- 508d6dd6c45027e3cda3d93364980f32ffc34c684a424c769954d741cf0d40d0
- e0fc2cf31a0fd7f4bfa1ba453fd8f272784330de2ecba80104455252a931789b
- 2aeef18abf22b233de5515a95cdca5aa3cbc6c21e8d2f83a68214e7272f9d947
- 508d6dd6c45027e3cda3d93364980f32ffc34c684a424c769954d741cf0d40d0
- f80d84a3f951a1b62d92a5a2799b149ed0aaca292364f101c1273f135c811565
- 887345540f1bf31c40755edcda2e3dd9fe640122fc9020f3873c895daa2378bf
- 4f29180005f3c2e776d185472227028 7111ec073ab80dfc1b4dc1bc0d9337ddf
- eef56bfc68959c6eaa66ab6abcaaf8fb54aa5b5a7da0866d97a1effeae0952b8
- a265e0db5fe311dac60171e27011087bd64b467eb442986f343fe07410e8bf46
- d7590ee95a46bc1ca7973a8f09efe23a5b00e54d6e65b95cb16acd17a0f127e8
- ef3966d15af3665ee5126df394cefdf6f78fce77db7a70d5f35c19c234715035
- ef54e266f8fc9eb97d71c76f2a53b65bef83fe5fc270fbfe83463f83678ff44c
- df84d6c284dd39c2bfed6f8eb26149a4154396c27de50595ed5d80b428930dcd
- ff1dcab09f24a4c314af3ee829f80127e5b54f5be2a13e812617f77d0deeef57
- 5009f65e7a8d84a9955d5adbdb86107b15304b1061bdaba5dd2ac2293dd8e6cb

SHA-1

- 04356f101a5f53f0eff7b1a6b24d1463074f142a
- 937975e3ea50c15476aef050295f4031f5fda2a4
- c71300967110b899eabf81fe96bf5fd927a10564
- 4dcb1eb86caaf9fe5bbd8f729679435f1f14adc6
- 2f46a7ed5d7a303c0f25d5e4a18bcbf01ce9af26
- 22d80be7d7916763648a98a0afdb7c0c7e42b3d9
- 70f066c77a080d0003fb3047a9e3731828d3b164
- 698d1ade6defa07fb4e4c12a19ca309957fb9c40

- 6856bb506a0858cc5597666d966b5b7499e38542
- cacc3eb2f415852f57579a69662744f75438e891
- db999a5ecf4e1c87fae10983f6d23b26069cbba1
- 7b90dcdf6ea88b1efa1cee36a0b1ab71e34c8d1d
- e4805324ebfb97f3004847de306bf4fd567ed2a3
- 68af654d9c6bf1d671531d81f0f78a6a75960040
- c0bf51550f050e099328b3e228adf16483e30e53
- 6f20d6d12e793d69126359352ce34c09d4692f85
- 7fb634831f57c518707b697720f759ce9ae5c7a3
- 54fc5d132a50dc86fda117fee90b088c6dd9d361
- acfd2f5c8efea720cbc40c9da215a733f777037f
- 52ddd7483eeb8b096457178a7f9f2136af33e604
- f586995978e3250d9fa7fd05c89732bfde1a383f
- c13d0d669365dfaff9c472e615a611e058ebf596
- 630a2cd81e605cf418811a8fe12c4bc9ce377656
- 62bc9524f2c773c0dd486f48f584b309e04f16e0
- 477a1ce31353e8c26a8f4e02c1d378295b302c9e
- f37c1a1d11fd5a90dc3a30edd752eb67f9917f01
- 54fc5d132a50dc86fda117fee90b088c6dd9d361
- eb376b77cb6e2a6d89e3cc7368867c12bcc3317a
- 13ea93c06e3cb65ab7c5603de713d862a4956404
- 74d918acc5838177614cf63f2e327bd2d8fa0cc5
- 00626346632fdfb2a1d5831793e92a3601ec4d9f
- 6d8e50c567f80372a6f82f1ae2fc2c1177c56d45
- b8c40fcec38711a1c0cd663b87c175f7509201ff
- 94988d605982dc2f10e422505eed6e38fb7093f4
- 74b269cdf488b09d06ac6b6e8c9c8e75254d642e
- 35092d156e12d4c500ee999d913c1380a41b3908
- 92b74d3eeffaad370c9c6f36501fb6cd140c3b12
- 2cf4bafe062d38faf4772a7d1067b80339c2ce82
- 50e141b03bcd5b1f6d5d1d3956c42e188782c8dc
- 9d2dc6be9d580f4acb61d3d28239b601ca332a89
- 39f65f635a8572e8a4061a5df72c5425da517dfd
- c046fba176f44d91c43a920ed35ac96470ecb67d
- e23284f42db9d6e4cc259b359612b22e8e3cad87
- 7276989a740ea1d82bb94fb6d4d3ed921fa1177a
- f757e49d4126098b554af41630cf8932b57ecd1b
- 04063c50d1400f2bd62833d33c3f567c3b796660
- b72bedc3183fcb8dcdbfceb93065e253e5921a63
- b66f0f8f41722945814fae50ca17a7a19e227626
- f66dbfdb6d38a819443bb924a793544698fd8b03
- c63b333fa20eedce6d5757d58f54ff1ca1cc80d9
- d27f2f75d222c6a85c8a88d76bd9a25aea076b82
- d484b8311307a75eaf413e9b3911b0aacef6d27c
- c046fba176f44d91c43a920ed35ac96470ecb67d
- caf631b79f2078f73ee494adecf33d0df7ba9dad
- 94f3cfffb2697397b9032f449a8db61747083d11
- c413fb3d6d69a5f4405c8c97e1af1955716e9623
- 21fdb5107d0a38bd4cb8fb7714a2cad913bac7e1
- 56e43c278aa0398e8933a91f41849fbf97453e5b
- caff9e675dbf337badfdbd543d97c68cbf959610
- b7f53ea5784e1e699d22b353d5ebb72c5f757e17
- 077ed17c4757d08db2921b9ba030d2636ca5f130

- d22427829001ad66105a3fda8f97cb200f169896
- d4ec2dd90e1f2415f3dfe62d0a6627602c6ffee8
- 74e6171938b75dfd268e2c25ab51850d7d34f7b0
- 73d730a37699fac734e7a6da508283212ec10016
- 8c0addc6b1761586b4d8830beb550c7aeb5e186b
- 62063e502a6a96994e46408bb6a04e5b86c18055
- 412411c2ab000f61dfcbdc2cf8d2a00c0e631c0c
- 7e1fc00aece9b3d3df4fd44a6fec5fb77058abed
- 6af2ade9c744b4689e411536df07040f7f2722ba
- 00626346632fdfb2a1d5831793e92a3601ec4d9f
- c53aa6676f2a4e4f0c372b902dad5aa27c4ef859
- ee57cab4bc7065dc8257be0f28c6ed465d5ce3b6
- 3c78af6efbe0f15b4ff55077152ba5e3675a4ff0
- 55e57c6bc9f9db1556b6527f60d86edb603c2325
- c2533664ffcd4e25ed68a303fcaa3f25b39be848
- f4e1de4575a687932029ee4875b59a8a83385a27
- 8bc1aeda5d3d3b8e88920fee1f99360da1df038d
- bcc654fecbb77f643c3616b679075c08bbc6f780
- 4a6edb973747bce4512f635a076cb47b1b934a83
- b8cd43f605eab84838ed36943752c4ffc167f647
- fa9ede75fc19abe4b4fc46d37e234926af8744b6
- 78bb2c6b9a2ca3d79bfd4f313759385705b00922
- cf452a470bf3b6654d46e098d13538fe3c547224
- 3526c49ca637ca2130699590e7bfd22b98c08673
- d10f139d4a0e4591968bd8518dd152debaf15638
- 610f6ca6aa436fd0329d22a639ee2b4ad4ebe484
- 8a680e220a007d875e82a25c6aead202935415de
- 5e294219b54bec8933c1d765ed5884b7b174ca35
- 3f69df382de737a7dee988f98ea35d0b44dc48eb
- cd7f8684f6bfabbf733b724e00f5c8782613663c
- 0b83391363bc2c6fb261781423a9a611a5af0764
- 95c32bf141584db152fb7fc178a0877f70a838a6
- cd7f8684f6bfabbf733b724e00f5c8782613663c
- b91ae855e9db2b1129eb3a0380fe86a49e04320c
- 41a28ee8546ffbe33f92b9589c05d09da10318b5
- 682488c3fad02a93c2d0614f2b33eebe34c632b4
- 4a3749c33d235715a84ec4964e1d69d758645a82
- e92b86b55fbb1e3533e640c6dfa958603c68d14d
- c9f926a2eb5a0ba36d82556ccf820b6838b3108c
- 396c9bf470fed61ed771561346b60678a6958fce
- 6020bde7924e6e7933b2b4fc573e6e8f529ebc55
- dc479c9002ba733165171f2179d7beadbc64b305
- 13dd0945827cb1f5f8b929633f911eaa563577d3
- a81f8f77d9a2681f1ad2290eb9ae85dd971af0be

URL

- http[:]//103[.]107[.]104[.]19/2022/eu[.]docx
- http[:]//103[.]107[.]104[.]19/DocConvDll[.]dll
- http[:]//103[.]107[.]104[.]19/FontEDL[.]exe
- http[:]//103[.]107[.]104[.]19/FontLog[.]dat
- http[:]//103[.]85[.]24[.]158/eeas[.]dat
- http[:]//107[.]178[.]71[.]211/eu/DocConvDll[.]dll

- http[:]//107[.]178[.]71[.]211/eu/FontEDL[.]exe
- http[:]//107[.]178[.]71[.]211/eu/FontLog[.]dat
- http[:]//107[.]178[.]71[.]211/eu/Report[.]pdf
- http[:]//155[.]94[.]200[.]206/images/branding/newtap[.]css
- http[:]//155[.]94[.]200[.]206/resources/Invitation[.]jpg
- http[:]//155[.]94[.]200[.]209/assets/mail/fonts/v1/fonts/last[.]jpg
- http[:]//155[.]94[.]200[.]211/en-US/docs/Web/JavaScript/Reference/Global_Objects/Object/server[.]gif
- http[:]//155[.]94[.]200[.]211/news/live/world-europe-60830013
- http[:]//45[.]154[.]14[.]235/2022/COVID-19%20travel%20restrictions%20EU%20reviews%20list%20of%20third%20coun
- tries[.]doc
- http[:]//45[.]154[.]14[.]235/2022/PotPlayer[.]dll
- http[:]//45[.]154[.]14[.]235/2022/PotPlayer[.]exe
- http[:]//45[.]154[.]14[.]235/2022/PotPlayerDB[.]dat
- http[:]//45[.]154[.]14[.]235/2023/PotPlayer[.]dll
- http[:]//45[.]154[.]14[.]235/2023/PotPlayer[.]dll
- http[:]//45[.]154[.]14[.]235/2023/PotPlayer[.]exe
- http[:]//45[.]154[.]14[.]235/2023/PotPlayerDB[.]dat
- http[:]//45[.]154[.]14[.]235/mfa/Council%20conclusions%20on%20the%20European%20security%20situation[.]pdf
- http[:]//45[.]154[.]14[.]235/PotPlayer[.]dll
- http[:]//45[.]154[.]14[.]235/PotPlayer[.]exe
- http[:]//45[.]154[.]14[.]235/PotPlayerDB[.]dat
- http[:]//45[.]154[.]14[.]235/State_aid__Commission_approves_2022-2027_regional_aid_map_for_Greece[.]pdf
- http[:]//95[.]217[.]1[.]81/maps/overlayBFPR
- http[:]//95[.]217[.]1[.]81/maps/overlaybfpr?q=san%20diego%20ca%20zoo
- http[:]//upespr[.]com/PotPlayer[.]exe
- http[:]//upespr[.]com/PotPlayerDB[.]dat
- http[:]//upespr[.]com/State_aid__Commission_approves_2022-2027_regional_aid_map_for_Greece[.]pdf
- http[:]//www[.]zyber-i[.]com/europa/2022[.]zip
- https[:]//45[.]154[.]14[.]235/2023/EU
- https[:]//45[.]154[.]14[.]235/2023/PotPlayer[.]dll
- https[:]//45[.]154[.]14[.]235/2023/PotPlayer[.]exe
- https[:]//45[.]154[.]14[.]235/2023/PotPlayerDB[.]dat
- https[:]//drive[.]google[.]com/uc?id=1BG0F1NdkPZOY6w2Y0YEs6nMGYLvSJiQo&export=download
- https[:]//drive[.]google[.]com/uc?id=1ITPqIFuWOQZ08RmMUDMmzWpg69_EbLTO
- https[:]//president-office[.]gov[.]mm/sites/default/files/font/All-in-One_Pyidaungsu_Font[.]zip
- https[:]//www[.]president-office[.]gov[.]mm/sites/default/files/font/All-in-One_Pyidaungsu_Font[.]zip

Remediation

- Always be suspicious about emails sent by unknown senders.
- Never click on links/attachments sent by unknown senders.
- Block all threat indicators at your respective controls.
- Search for IOCs in your environment.