TrendLabs

Autodesk's A360 Drive Abused to Deliver Adwind, Remcos, Netwire RATs

Appendix

TrendLabs Security Intelligence Blog
Jaromir Horejsi
Cyber Safety Solutions Team
September 2017

Indicators of Compromise (SHA-256):

SHA256	Trend Micro Detection
5272b050140c76dd56bed71864d653dd7cfb1e1a6ab544b5d77d7bb8c037904a	BKDR_NETWIRE.DB
0c3fa75190256a2d76a458d1469808d477c59550bcd0408bc8baba35645cf103	BKDR_NETWIRE.DB
586ecba9c1eeaefbfd78bd0e81a88dc3146087f91b20906bdd7a78e316bd01bc	BKDR_NETWIRE.DB
b7028e49f80b295f99334670b89204280c7e3c2640ed5480d6b7f01fa3f5de20	BKDR_NETWIRE.DB
b3949c120d651c9648e3d70e61b03e84732ea02d8cb2294035ebf475bcdfb7bd	BKDR_NETWIRE.DB
1cc5169e3fb6a24f412c59de648504818956642f3c5beba9034469d74af9ac15	BKDR_NETWIRE.DB
17e31a095aa51145dc13be01639aff7b0e09ae75b0eeca0de72161613d835cc1	BKDR_NETWIRE.DB
fe21970a50234b874414134280e88176a69e4df002fde1ddd13ec63380b7eaee	BKDR_RESCOMS.CG
877a31023496baf82250d78f45bd8a282359701e13df4a27d431b9614fc3781e	JAVA_ADWIND.JEJPAD
2a18683f219a292eafe673ea341d08e7e51dd83c3303e8c40fca620616b3ea0e	JAVA_ADWIND.JEJPAD
07902177ab5c3d6cf1c1cc9b2103a85b00f422107ce46964b918fc4debc604ef	JAVA_ADWIND.JEJPDR
57ff44eb698e6902cda5b9a64ae2cc2db204e6375900e0c3e3abd6e65082e5c6	JAVA_ADWIND.JEJPDY
dbb79f8e61ad7c259ca32b76c19e687890603b3efd13f5ea6e59af3c970ee452	JAVA_ADWIND.JEJPDY
c4587fbd333752b4eb9cdbc4e5732a46fcebeb47c5f96c3e2d2b6c07aba8bedb	JAVA_ADWIND.JEJPDY
2253358acc0125f3e2a9a887d19909d4eaed35ea1e2a23ef572d19897d7f5a28	JAVA_ADWIND.JEJPDY
826f96f9f7dff9f4e658c89d4cc07e62d696de3ea877702bbd6cabf41b0cd5dd	JAVA_ADWIND.JEJPDZ
c6a44928a1c6876dfd010ba3fdca206c2b96da3306b27af2cda2c467a6e1fcf2	JAVA_ADWIND.JEJPDZ
5365c0cfd50114505f3892a453c25bd34ce7aa09a0526e16213406f995e41e29	JAVA_ADWIND.JEJPDZ
91f34284f1a0054e00fe3146ea57ccd9aad324f20d6a2bf08d256148865a5ca1	JAVA_ADWIND.WIL
582ffe66a41c4259d94d94569676ac76e3dc2d772d5fe6f61736e30a163618c4	JAVA_KRYPTIK.NPP
f5399e9745467dd3d88059b825df8fdb195c9d26f5dbf1cd5764dc0ac6883c0c	JAVA_KRYPTIK.NPP
1e7b408d7e1f04400b0d389b2fcc5d1e34bc8c7ec288d4a72b39c06447ebd864	JS_DLOADR.AUC
36043cf106e1cb6b7f449d82e37dd43620ad7cbd35c0e04999ec038d7a9ea5f8	JS_DLOADR.AUC
e26bc0d515d4f70dd1f50f45e45f931b5ff541c17b9bb87a897e67feaa966b2d	TSPY_ZBOT.YUYAZW

Abused A360 URLs:

URLs/Domains
https[:]//api.autodesk[.].com/shared/9d2d013674114c6698a64af0e99d4631
https[:]//api.autodesk[.].com/shared/0315fb857d8a484cbd3c727f2dbc8a7a
https[:]//api.autodesk[.].com/shared/1752d9eaa50e442f81dcd97c63745d25
https[:]//api.autodesk[.].com/shared/1f6e5c8e311f464c80b980257b86db96
https[:]//api.autodesk[.].com/shared/1722c56e98fb4ae08464f2164b8f0e04
https[:]//api.autodesk[.].com/shared/c9c89b1b53c74407b7bc5453d62e99c4
https[:]//api.autodesk[.].com/shared/416ece8e66de4940aad6e2214a2d0023
https[:]//api.autodesk[.].com/shared/c5f4dd86a1af45d898d486cb6842a617
https[:]//api.autodesk[.].com/shared/f40ba47242d14b7cb1007c0ce739eba3
https[:]//api.autodesk[.].com/shared/05738d1934ba45eea8d57cbf11a6feb1
https[:]//api.autodesk[.].com/shared/8be0254180a84ad8915dc676be7804fa
https[:]//api.autodesk[.].com/shared/cfd3088586804168bde20c3d8a596c23
https[:]//api.autodesk[.].com/shared/456892c33afb4c728cf367943e9328c2
https[:]//api.autodesk[.]com/shared/addfc18a2c5943e880134cfcf8529488
https[:]//api.autodesk[.].com/shared/ffb94038d17c462b8e9f89881da2283c
https[:]//api.autodesk[.].com/shared/6c5758910a144940a3d595368061cd6e
https[:]//api.autodesk[.].com/shared/ab6761620fb74d4e961880be53b5cce1
https[:]//api.autodesk[.].com/shared/6e157e433c3e40c68d1b183dc9b74f6b
https[:]//api.autodesk[.].com/shared/f345f538e0324a93afd0e12e1a0fae2b
https[:]//api.autodesk[.].com/shared/0a691c5066864b1cbd3ddc5f3a6a31d5
https[:]//api.autodesk[.].com/shared/7edbabad697349c1b8246d2ee7f0d398
https[:]//api.autodesk[.].com/shared/dc8c2fc5b6ff4b5e8e90943f018a8847

Related malicious files found on VirusTotal from June to August, 2017:

First Submission	SHA256	Trend Micro Detection
8/23/2017 14:57	3a6f4fad8e2c10311ce2727681b75b0b485a14ca2618f15e8992f9bba333c98e	ZIP, one file: TSPY_ZBOT.YUYAZW
8/24/2017 12:38	2cf1b50faed6c18c22c8b9d5be31cff1d854a099181410ebe74e7ac6874cffb3	JAR, one file: JAVA_ADWIND.AUJC
8/24/2017 12:28	b488954087b192705b842a3461bde62e6a253cc5c21e3b17e527cd1788fcf9ce	TROJ_INJECT.AUSPQY
8/24/2017 11:30	78436b50bcc47e38bf3c45de3e4aab266eac1427c6c9fce3db452953c56a92a9	JAR, one file: JAVA_ADWIND.JEJPDY
8/16/2017 14:31	aab7ccad549e1c79390624e1c1363fcd2ff3e34fbc448a783ae87dc04692496a	JAR, one file: JAVA_ADWIND.JEJPDY
8/18/2017 9:49	626af18a1ef6654cde49727eea4f69c503bc1af0bb620165051da8e0469e1813	JAR, one file: JAVA_ADWIND.JEJPDY
8/22/2017 19:38	39b85041122c4d9687dcb467a566d81e0cd0758eb73d24b9b7cb7ceef9f09f9b	ZIP, two files: BKDR_NETWIRE.DB, JAVA_ADWIND.JEJPDY
8/23/2017 12:56	0898cc0ada40eff1d9d8e4e6d1e3a750edbd3e3c478a1ad72307ee6017998cfe	ZIP, one file: BKDR_NETWIRE.DB
8/18/2017 7:32	b3ab615fc7ef0ae60757e8834aef64123c971904a9174b401795349eb047b165	JAR, one file: JAVA_ADWIND.JEJPDR
8/23/2017 4:42	e3f94eb7a4808d435fd43a70a3bb363cf21465c45e9a746b4ce158d14f6a95c4	ZIP, one file: BKDR_NETWIRE.DB
8/18/2017 11:01	d833a4070e609cb188be0ba4baf9708e90b188394c076ae895af0df7c57813d0	ZIP, one file: BKDR_NETWIRE.DB
8/18/2017 1:16	46d7223e9c9f561f5a4e614f7883235ffc211d42d1ffad5248d79aa5e5ca961d	ZIP, two files: BKDR_NETWIRE.DB, VAN_WORM.UMXX
8/16/2017 21:08	efebb78f2fdd649d94aa036c8ef98fc58fe1fa26a48f0338e0b1a845cdcf4d62	ZIP, two files: BKDR_NETWIRE.DB, VAN_WORM.UMXX
8/18/2017 9:23	13ad23dc65a7148d2fd3470f3aedfa05e1aba3444d5fc493146a138883170e4b	ZIP, two files: BKDR_RESCOMS.CG, JAVA_KRYPTIK.NPP
8/16/2017 4:40	a4ec05304a5d4ac4c2623e3ddaaee0a41a7a534e346d5be45eb56d0ff161c506	JAR, one file: JAVA_KRYPTIK.NPP
8/17/2017 11:39	f39504e844e06cb51654322cf36c6ff36aa423464512922bcbf183051d713e58	JAR, one file: JAVA_ADWIND.JEJPDZ
8/15/2017 11:11	dd4a74079d945cfc917c6a2a16da25cbe7c0fce8b562ff6072a9c7721c41cd51	JAR, one file: JAVA_KRYPTIK.NPP
8/16/2017 23:22	60abad4e727fd7614ebb6b120e822b6c30b1255086fef59fbbde73c802e05cc2	ZIP, two files: BKDR_NETWIRE.DB, VAN_WORM.UMXX
7/4/2017 18:10	e986a7f64ab32a43883f20f69a87811a7b230178776c1a45164a65b19c85d2f2	ZIP, one file: JS_DLOADR.AUC / HEUR_JS.O.ELBP
6/22/2017 13:43	1e7b408d7e1f04400b0d389b2fcc5d1e34bc8c7ec288d4a72b39c06447ebd864	ZIP, one file: JS_DLOADR.AUC / HEUR_JSRANSOM.O6
6/30/2017 9:21	f26b8d36c5ee66ae2667898c4b3ce2ac6761d028707d895701aa2daeb0c25f2d	ZIP, one file: JS_DLOADR.AUC / HEUR_JSRANSOM.O6

Securing Your Journey to the Cloud

Trend Micro Incorporated, a global leader in security software, strives to make the world safe for exchanging digital information. Our innovative solutions for consumers, businesses and governments provide layered content security to protect information on mobile devices, endpoints, gateways, servers and the cloud. All of our solutions are powered by cloud-based global threat intelligence, the Trend Micro™ Smart Protection Network™, and are supported by over 1,200 threat experts around the globe. For more information, visit www.trendmicro.com.

Created by:

TrendLabs

Global Technical Support & R&D Center of TREND MICRO