TrendLabs

The Urpage Connection to Bahamut, Confucius and Patchwork

Appendix

TrendLabs Security Intelligence Blog

Daniel Lunghi and Ecular Xu

August 2018

Android Indicators of Compromise (IoCs)

SHA256	Detection name	C&C	Encryption key
Bahamut-like Android Malware samples			
08228a76c7c443e02c03cd2c4cf79d87edaf48215fb42a5a4c110529f7cd4e06	AndroidOS_Bahamut.HRX	http://www[.]urduenglishtranslator[.]com/Adehfjl/Hudlhty/cy[.]php	7sTbYe8Qo6OqZwIQ
0aab04cbf78e9405ddf117c6461aed4debf8913b90de6e4f7b0dcd6676197630	AndroidOS_Bahamut.HRXB	http://www[.]ramadan[.]mobi/sCqOnB/AxzEqIo/CalendarData[.]php	vC54ExolPqaPpB66
0b75a8de0acd2f86806c794fd29437c6676dad026f68225f0431a4f4d8b43e43	AndroidOS_Bahamut.HRX	http://www[.]funtime[.]mobi/HuTrweOpCX/YqTrnpoUyt/porEi/funio[.]php	jsZ04Yex03jh04fX
0d349d085c81fde9febc3b67d615ff35b6823d1742f6039aff4f2b8a68f06bfb	AndroidOS_Bahamut.HRX	http://www[.]cacheremover[.]com/SshdytIjsh/Ujsgheughdy/zxt[.]php	Huisgte87Hdy4Oli
1082fab15eb90b6832851fc65a8744ac975467922cc0477a62f202992e608e28	AndroidOS_Bahamut.HRX	http://www[.]pikrpro[.]eu/ayEo/jXgh/znoor[.]php	vGHolkiuy67bujbD
17e9ba2f39b36bcc6dd0d8ee8d96c62056dd0a61ce9ba720abd386e41650e979	AndroidOS_Bahamut.HRX	http://www[.]zawajlife[.]com/UqoPyt/QazTrq/cm[.]php	0hil81ZxRo0jTfs1
19a2fe743bf4e9200438c053e31d1c014c7951979171d3b824e7c91f6e331664	AndroidOS_Bahamut.HRXB	http://www[.]gcleaner[.]com/dyUqP/sxOlA/junksSize[.]php	jsZ04Yex03jh04fX
1ae2c9c1289026495f5b61a704d643b80049ab518c35496f68a32258e14101cb	AndroidOS_Bahamut.HRX	http://www[.]scleanerup[.]com/qWeuAs/uqRzxSlQ/cacehy[.]php	1qRt34u72NMeabsa
1f108800a98ea26e548618a561552f1889eeeef2b9ed590b6c6b3a564bc9dcf7	AndroidOS_Bahamut.HRX	http://www[.]qiblacompass[.]info/QiTreaOmT/CqewPqat/QuCompasReport[.]php	7sTbYe8Qo6OqZwIQ
1f4e21ff4a494ff94ba33fc834ade01815e91d86bb6a9eeaf75fd060c2fbc295	AndroidOS_Bahamut.HRX	https://www[.]funotimz[.]com/AmOs/AnxT/mainTop[.]php	yqiYrerlI943UqCb

20d9fada15d3340d06f90286ed627bb79c89e077c331c9e3c01074b4e4208401	AndroidOS_Bahamut.HRX	http://www[.]funtime[.]mobi/HuTrweOpCX/YqTrnpoUyt/porEi/funio[.]php	jsZ04Yex03jh04fX
23164f64a3330316bbe2b14f01bc0de368f86716e4d367bef79cdecb7fc28e2f	AndroidOS_Bahamut.HRX	http://www[.]zawajlife[.]com/UqoPyt/QazTrq/cm[.]php	0hil81ZxRo0jTfs1
297cb76d16a1d875240e7495841ff61ee104b6b8c75e3b2db27e8eadae3c73bf	AndroidOS_Bahamut.HRX	http://www[.]funtime[.]mobi/HuTrweOpCX/YqTrnpoUyt/porEi/funio[.]php	jsZ04Yex03jh04fX
2dd6b448359a9073055f71311caa69960ca2250cc64e7faf40ba32fe6b74526f	AndroidOS_Bahamut.HRX	http://www[.]cacheremover[.]com/SshdytIjsh/Ujsgheughdy/hgtu[.]php	Huisgte87Hdy4Oli
2e9f458a0c63283e7fe79bd8514a8945010265d041a565723884b26a20905a9d	AndroidOS_BahmutSpy.HRXA	https://www[.]notekeeper[.]co/note/notlog/gnoteapi[.]php	Iosty896Hsgteyio
31631e36f26826b32196b0263f3aabb2eb14fcfb12c8c73ee0b40c8e9c0b8a27	AndroidOS_Bahamut.HRX	http://www[.]funtime[.]mobi/HuTrweOpCX/YqTrnpoUyt/porEi/funio[.]php	jsZ04Yex03jh04fX
39005b9c310f448b3201e09b7bc2db5d18c1f3eb31540fb615336e3b09bf9e8e	AndroidOS_Bahamut.HRX	http://www[.]funtime[.]mobi/HuTrweOpCX/YqTrnpoUyt/porEi/funio[.]php	jsZ04Yex03jh04fX
3b12ee9df0191ab320f4d792e8be9e208dd39c4a3906db6fcc674fd8699c71a8	AndroidOS_Bahamut.HRX	http://www[.]qiblacompass[.]info/omBi/pUyt/colmix[.]php	7sTbYe8Qo6OqZwIQ
44c19662a1270ab0f338b5110d8e647a206a47bdede18350de9eae55aa6fbadc	AndroidOS_Bahamut.HRXB	http://www[.]gcleaner[.]com/dyUqP/sxOlA/gsecureSecurity[.]php	jsZ04Yex03jh04fX
45a353090b3e3607460a29914ce1d418be91f3aecc8140ac969c91141b9f642a	AndroidOS_BahmutSpy.HRXA	https://www[.]perfectcamerapro[.]com/camXt/ZaoPp/camfresh[.]php	IPo9087gtfglioOd
472b35357dab8d277c711d34537217a2ba48625af004ec52734492ad86655873	AndroidOS_BahmutSpy.HRXA	https://www[.]devout-muslim[.]com/ramadan/zomp/praysize[.]php	90IijdhyghVgd786
49aaed9dec956d345610cc724c0d1fae52ca319b8635f96bfc49ae0421ccfbaa	AndroidOS_BahmutSpy.HRXA	https://www[.]autorecorder[.]co/ApPt/lOptR/fSuper[.]php	yqiYrerlI943UqCb

4c7f04d8f6463411126dd597489e776b3b3427d03b68a459ab4746008afa724f	AndroidOS_Bahamut.A	http://www[.]notekeeper[.]co/xdTqioP/pPwsDqlV/CheckSync[.]php	ZbvRtjGqaOqmPrIt
55dc64e648f3b282a7073d9c775f737b24bd9fd1ab5495cd191e9c1bdcb3f538	AndroidOS_BahmutSpy.HRXA	https://www[.]smsbarrier[.]com/style/sms/smso[.]php	iuytfvdg654fdrty
64c6d6d26d6e3b7f919f1b03607b847278162225e93951de17a2bf517f0321b5	AndroidOS_Bahamut.HRX	http://www[.]riquitz[.]com/JoUc/NcVr/suPer[.]php	vGHolkiuy67bujbD
8af837d3f54ce0f1cd4deacf235f6bd8f4e89872a34bdf427c13172343cece98	AndroidOS_Bahamut.HRX	http://www[.]arjewelmart[.]com/hGdY/mOxUt/final[.]php	vGHolkiuy67bujbD
900ce88a3a4e0f897aae175aabb10a59ed31eccb92c2c353b514e6c136e401a5	AndroidOS_Bahamut.HRX	https://www[.]infowiper[.]com/jc1/jc2/jc3/control[.]php	jruTesdgt6784SfX (unused)
974c182fb9872a4d108109ef84d86333fabe585b604217a72fcd7c84cd4b95a4	AndroidOS_Bahamut.HRX	http://electrobric[.]com/autoc/cam/EveryKin[.]php	yqiYrerlI943UqCb
a05a04a4d552dacd9db6bdb57b52e720d5851db1ab74c0e954f15433c5838367	AndroidOS_BahmutSpy.HRXA	https://www[.]notekeeper[.]co/note/notlog/gnoteapi[.]php	Iosty896Hsgteyio
a5a818af5c88e3a87da7632c8faee1aa52685bd4a306ebdaa4e59a71f2dca80d	AndroidOS_BahmutSpy.HRXA	https://www[.]autorecorder[.]co/ApPt/lOptR/fSuper[.]php	yqiYrerlI943UqCb
a5b2d73f904072d4da642105fb2092e12ca115d0f7deeff3dc24dd3c7b9b216c	AndroidOS_BahmutSpy.HRXA	https://www[.]allgameson[.]com/news/zone/zonenews[.]php	OooOxX0IO0iIrtet
a5ba85f082785c4368ac9d16663636d297ebc6eefacb5ab6303abac765de1b4c	AndroidOS_Bahamut.HRX	http://www[.]kashmir-weather-info[.]com/WqAeX/ZluEqW/cot[.]php	7sTbYe8Qo6OqZwIQ
aafb5c720bfb3f610f1844f49228c7d4289777016fb33eb91f287ce7868e8171	AndroidOS_Bahamut.HRXB	http://www[.]ramadan[.]mobi/sCqOnB/AxzEqIo/CalendarData[.]php	vC54ExolPqaPpB66

aec070198839e3531f9311061135fd65304d91c90b1eac017f685307c7c6b648	AndroidOS_Bahamut.HRXB	http://www[.]gcleaner[.]com/dyUqP/sxOlA/gsecureSecurity[.]php	jsZ04Yex03jh04fX
bf2968b7a3ba3687dee6122de538d3d59e062553e77a80d29817f2ff4137f4ea	AndroidOS_BahmutSpy.HRXA	https://www[.]jukemusicmania[.]com/musoc/drama/msplash[.]php	uytrefdgc765Xxxx
c402706f4277d3d8a4d7e677165f892c7c1a42c5794cf368bc86e50a4416280d	AndroidOS_Bahamut.A	http://www[.]notekeeper[.]co/xdTqioP/pPwsDqlV/CheckNote[.]php	ZbvRtjGqaOqmPrIt
c840552ec1a1fb7e9c3f31777ff88cbb36a0ef337c72e2e736a5432c8e8903bd	AndroidOS_Bahamut.HRX	http://www[.]androiddatingnetwork[.]com/hSzx63YsK/St930XzFe4/conn[.]php	vGHolkiuy67bujbD
c91158e43093f6bc53c55e73acbc2227de59b571d3e1126ed4460f2b31c508e9	AndroidOS_Bahamut.HRX	http://electrobric[.]com/mobile/dial/MainDialer[.]php	yqiYrerlI943UqCb
c9934f106caf503bc552aa364b0ad1c6632c3a947c737cbb4442ae67d4116a43	AndroidOS_BahmutSpy.HRXA	https://www[.]notekeeper[.]co/note/notlog/gnoteconf[.]php	Iosty896Hsgteyio
d7fb80c71fc6d50ce44036a3116c3ae7e1b5800fca45f2876854ed7f5220d45c	AndroidOS_Bahamut.HRX	http://www[.]khuaitranslator[.]com/TQaxcTr/spPlVl/WordCorrection[.]php	Huisgte87Hdy4Oli
e24f888bd85a108abf7e2c003fb115a5bb6197cb55fb6d1dba2d878f846110f1	AndroidOS_Bahamut.HRX	http://www[.]flplayer[.]com/fl/playfl/pnk[.]php	JrKtUt675GtsIIiO
eb9c8df2fa47a81c89fc55bed1e204be3b6fc2983d9d9725797eb0697d60073d	AndroidOS_BahmutSpy.HRXA	https://www[.]notekeeper[.]co/note/notlog/gnoteapi[.]php	Iosty896Hsgteyio
f25965abef6abbdd9b7c8477f66d599dac346658fff67a728df66efcc74757e9	AndroidOS_Bahamut.HRX	http://www[.]cacheremover[.]com/SshdytIjsh/Ujsgheughdy/zxt[.]php	Huisgte87Hdy4Oli
f36dd30c3cb5b0aef28d35079e9392ee8ce3a8964b8b41f67e73ca83a4a89a1e	AndroidOS_Bahamut.HRXB	http://www[.]vlpplayer[.]co/VcKip/FqAwPp/opo[.]php	IOdghtyu46758IOI
fdc6d21986046e90482650e28544d26ce77126adb6e3ea72262ad52ef282a729	AndroidOS_BahmutSpy.HRXA	http://www[.]gtrimmer[.]com/sguri/seqY/cpull[.]php	qwertyuiopasdfgc

ff1d07e0839887123cd6690079425d47781e1392f778363340055d54ee36fe31	AndroidOS_BahmutSpy.HRXA	https://www[.]jukemusicmania[.]com/musoc/drama/msplash[.]php	uytrefdgc765Xxxx
Possible Patchwork samples			
c0de04050bdf26e8bdb8559db396cd959f1770f299a7090491289f0792339623	AndroidOS_Bahamut.HRX	https://www[.]qianglongmil[.]com/jc1/jc2/jc3/control[.]php	jruTesdgt6784SfX (unused)
819e940b9f6c109cbd50d53a9a601bd2e6f15c79a644a674908625280429dd40	AndroidOS_Bahamut.HRX	https://qianglongmil[.]com/vr1/vr2/vr3/control[.]php	jruTesdgt6784SfX (unused)

Windows Indicators of Compromise (IoCs)

SHA256	Detection name
Delphi Filestealers	
16099bfe11029702fb1fafb9eca00865244e035a18250c4f3284799f334aa8ad	TSPY_DELF.BFJ
1f0dabd61947b6df8a392b77a0eae33777be3caad13698aecc223b54ab4b859a	TSPY_DELF.BFJ
26b77bd33ace3d2ae5a56dcd463a57b78fef09fcbcf4e838687a1145af97d9f5	TSPY_DELF.BFJ
815466ec21c59f7704f094a0e4cfc4f817c8b98231d10fe01919b6bd60eca64e	TSPY_DELF.BFJ
917dae26c88baecb8b17d4161be6e635cfc0e7572815870848c874e07786a1e9	TSPY_DELF.BFJ
9f204d2e9c66842812ad42907334498b1dda11ce4bce937e72de9fa768b7a217	TSPY_DELF.BFJ
be76f24280919f1cb952c9996bc927e6e485123839ba84bbadc8fb9eb885c354	TSPY_DELF.BFJ
f558351453096e02e5fbeddc10f59f6f8e5311cefa626aa78f06ef8474997df5	TSPY_DELF.BFJ
Delphi Backdoors	
b4a6b39d5c7339fbb22c5113090e2d87486052bf45c0599f96959817c8a3aafb	BKDR_DELF.XXVR
184446bcb17021c39128369e9fe3d06cd0dde430c7f2e90c945c5a3299ef7b52	BKDR_DELF.XXVR
1a510082dbcd23a86569c713a848100a1ea018a6f35f8fecf9bbe6a86f555ad9	BKDR_DELF.XXVR
1be9579507a8b20110b740c65f1b65d920c455ab1c026cadb1a250a267c206be	BKDR_DELF.XXVR
229805c8c6b2c54f7e34e23dba61268a1ef89b04f9052efec292366aa86c224a	BKDR_DELF.XXVR
2af07c7cee0743b9ab84eb5947d0334cb0b1dc874fa562920aafbc4ad95b12fc	BKDR_DELF.XXVR
33c5867b3375ef7e879caf614e79455df26adafdbb6aad11bde23edf695b5d85	BKDR_DELF.XXVR
34c420caf4d86e8cf73acb558556fc687983d10d512c772f0f0c31e2aa04a959	BKDR_DELF.XXVR

3bf87393abc6344a3e0dc751c81cced760b886e2f97b319c1443636b9957f2b9	BKDR_DELF.XXVR
408e7360b5f382d1fe90719dcbd1343c22a48bd17017ac47374e15c36cfffe1e	BKDR_DELF.XXVR
49cf46406477bf58f6cf2ec75bf6eb8370579b9d53f9d7f2896642010a494d00	BKDR_DELF.XXVR
4ac870ef498441034054b1c0226ab079568e1c45bd8895e621598c9023318e66	BKDR_DELF.XXVR
4fd25d2c9e97d23d3b2ace30ee534643dfc0b03ada2e976e185832d3b8c0e32d	BKDR_DELF.XXVR
55216ef475ea7efcee26da19c11a842e4b124611fb3db787bfada2ebc9b39794	BKDR_DELF.XXVR
565de1908528707d44be5e6beac37456c2424035202d9272c175a1b96db19cdc	BKDR_DELF.XXVR
605a80c8b7305ad1d6815bfe2035128c8dd06e8333d8b3cba9ed68caa4aa0c17	BKDR_DELF.XXVR
6874e3b191c047695fb4b020160604b85953a067ceec795410d5fda22994db95	BKDR_DELF.XXVR
6cee1781b3acddea76959b0fc3c0058938da9ed4facc9c12c742633bf2dc5ca2	BKDR_DELF.XXVR
79dc0dd74e445f1aa1f7000150e3d6daeb5aff0bbb05e7aa79f761ffe88df0c1	BKDR_DELF.XXVR
80f02104726ff8f78db3ef70c2b641c373ec36abfd5d457219648b6edf71a521	BKDR_DELF.XXVR
8256fc98e05684569992a93318f519649d381081534e03b39263b071dd6e14c0	BKDR_DELF.XXVR
94e1916e880eedc02b8c61557926a77d7555f3f7a0131c390cdb4e98a23ff1f0	BKDR_DELF.XXVR
a493f1940a017e6ed6933f7831c11fffb59cda0bec7b3458641b83f738658d84	BKDR_DELF.XXVR
a7950c25bdbe103b3f0071bc35e90c28b06eea043b2175222674675945e7be22	BKDR_DELF.XXVR
a8165cd1897fb079969647c6de10c2489e5b8822e0f9f5643f855d4e5746353e	BKDR_DELF.XXVR
b1172084ba179d97c93f5e31ab6d0756f0fd7036020f021a11f6303b35049461	BKDR_DELF.XXVR
bd7f33c1566f56b1bce2f59e983b60d79e2e2de80ea9cd6dffe613005ab2e817	BKDR_DELF.XXVR

c0003222f997908c4552f32f95bd3fedfa4b3c9fc780ee363a7894c68ba0d4dd	BKDR_DELF.XXVR
c6c0ca3ca838b6ab857a1b22cc66ad568af96a3368c3c99598e63c4e4e6c85cb	BKDR_DELF.XXVR
f43ea2db9e79a819901c6ebb2a7cabbdddf4b3d12ccea985604d391facccbd32	BKDR_DELF.XXVR
f5fcbc63546dbce989d61895cc51f00efcf7a0241971350d749e70b0a3365d55	BKDR_DELF.XXVR
ff184e204f40b2f917c517a2abf92da20a96026e02ba4fbfa405d5c72ab96050	BKDR_DELF.XXVR
Droppers	
abe889fd02a7e107c990d2a3b909d5f82be6f4d12cee67c01d15e73843cc9a73	TROJ_DELF.XXXK
0f6138395d5ded2c2e123efe75427f3d81fd85c98ad6e5a6fe14e43744494f62	TROJ_DELF.XXXK
11596b82b8f0f4abb7998fc1f81c2205f5fdb23817c2963d4fbec247750552ee	TROJ_DELF.XXXK
211ee91911200049af80f8308a0d254f7640c5d1f802ad36f6970c148a4a9890	TROJ_DELF.XXXK
26f1b419a5f9b2f8a853429ecee78ad2aeba271fc8fc00ca2a97e818c562e991	Mal_OtorunN
2e4f4e707831e9e7884744200621c6fcd88ed26dadcc15361acd2f249943306c	TROJ_DELF.XXXK
45ae4149fed22a01a4f96fe176c90745d2b96f30717122695c6d7f6eeabb01f9	TROJ_DELF.XXXK
5206ecdb558dceacb204f11ce7fe03b5ff682f8a51468060ddeca35241b9e14d	TROJ_DELF.XXXK
54667597fc00e78c598f8e925c4c093b11bcd5a9f9644528aaccd73433e6154b	TROJ_DELF.XXXK
5bebe3986c2dcb5f50ea5d34c564c24ad3bbc132e648f1d009757a0d69c87e52	TROJ_DELF.XXXK
60c1b45113484d97e3a0d56959ac6d010e945d28a266ed52abc20159f9a9a48a	TROJ_DELF.XXXK
68f3baddf4f24eadaf715dc27d01456a2d5a3d1f116a9fe5f1ccb77ade585241	TROJ_DELF.XXXK
6e0144f57aa20557b7ec2b3a05fecb74d45169ed740055fa36f7678c418065d7	Mal_OtorunN
724ad018fb6cda26f65c3f9878715e6b4a32f07ab8ced1331c7fc1db3164135b	Mal_OtorunN

783bcf19e34d58d00ba135369a57fe31cec22d027fc8d87b073a28a7c1a4e9d8	TROJ_DELF.XXXK
7d566e2ad6d41bf16e3b7fdb0ad36f351dad59a6841b59153962f70907ddc768	TROJ_DELF.XXXK
801137138d8b4a44dc84944018c285d13f61887746f440c65a9f604c46b16ce9	TROJ_DELF.XXXK
85e839b45088bd2ff0ea184634e567fb1e3b7f86caf8a7c0e839218906da4c0d	TROJ_DELF.XXXK
9e9389f4a1e025ed6549aa4e2ff73f6e5710d74acacf392c607cf824d4640123	Mal_OtorunN
9ea71ba619e521f6525c72de25a6f510c6b5ed047cbf24eb3494806e4d767979	TROJ_DELF.XXXK
a3bd44c5e03200b74168f576666f0031bf64072e16205a6edfe3116b4eac7cb9	TROJ_DELF.XXXK
a69f3c5bd2e22aa8d830252386a689b28bbe5834fcfe675293707531e5fc4a07	TROJ_DELF.XXXK
be12ec7094ab85adb98f9199fa88113ceb8c98e1e80b46a0d00abc74efb96e29	TROJ_DELF.XXXK
c3f20c24057c4911199e17a30a9ad67d3cd6c831bd2fce0a4b542d7a9370278f	TROJ_DELF.XXXK
d7dcd1453121f9f2f0fbb2eae9fd4828be263afa617ac3baf34ec9910da1d623	TROJ_DELF.XXXK
dc4fa0f51999ff73135f3d97fa01f5a4ce846facdcddf5d51fd59f9111684620	TROJ_DELF.XXXK
ddf2520224381c653119908f0dceb154138b0724fa8307ef95629429576024e7	TROJ_DELF.XXXK
efd5168f6ce4c94792e003d249e8af165e888d61bc5db36237cbc5a24534f268	VBS_DELF.PTR
VB backdoors	
d92037764fbd8a2dab9577b43e9a007af77859e38b67175fec6b7484efccea28	BKDR_DELF.XXVR
01bca9ae7b7d5ac5913f7272254b09de2dcecb0ff0fee7f6b6e7767ed979fec5	BKDR_DELF.XXVR
04082c8d6c81d7f5cc1509ffb3fa90648a00081e939230a963d94e72ba1e4362	BKDR_DELF.XXVR
041b1df3684c2c37b55cb3bebce37e11e9273259deae50f303fb344fb28065ec	BKDR_DELF.XXVR
0ab0af32f1d5b1bc505b7f623f4b099e16364f25604a67ffcf550d7556352d18	BKDR_DELF.XXVR

116315d211261df94da3d834c324f65b368025c009f7e387564f6cd23fbbc08c	BKDR_DELF.XXVR
1378f07bb8f64214d219f9487faa539c811aa65343a4d7bb3db79bc94878f4a2	BKDR_DELF.XXVR
1755ce13e1cfafebeef2568fc6fb271d7ae68b379280c77068de714b5b7f4f91	BKDR_DELF.XXVR
2819700088787eea566f2c70457a5b334f3246119585d039f45e27fba6c5d6fc	BKDR_DELF.XXVR
2a3228c5923e32f79c2cbdade14d0e8c79d55b9532f3a3c83b359b1913979ff8	BKDR_DELF.XXVR
32a939274de1d9577e14b3b991fbaab75a2cdd3380d10eada7cc3a743307367e	BKDR_DELF.XXVR
3ea4414259502bac22bd0bffa5735e4a4f03b85c576057eecc1d6fc5ea11bb22	BKDR_DELF.XXVR
4e32c59307f34560903ed4622d20860d43ee37ba01b349ebefcb9ae30b74c64b	BKDR_DELF.XXVR
4f3a100d5dd86ead436911223b323175ce0d0f2c678018a2b27d4545625f9740	BKDR_DELF.XXVR
5f2250b46514d4b3f99f3a66cfff97a60e6185e4bbd13ee4b824d97efc0604d8	BKDR_DELF.XXVR
69055236df30a32f08fd4bd20b4c550d25fd1812b26999325743f36c3ad1cf5c	BKDR_DELF.XXVR
6f362bc439ce09c7dcb0ac5cce84b81914b9dd1e9969cae8b570ade3af1cea3d	BKDR_DELF.XXVR
7af0e7c16435ffb30372bd9b86277ae95c6136301789f8e4724c752dbeb9f77e	BKDR_DELF.XXVR
7de73e02a560b9764ab6e3925d03f2a4412cf2b5dd81880865e8a74a62289eab	BKDR_DELF.XXVR
816a272e95f223eaf31e8830e054e0711cb868684c0d0569a52c2abfd0ad28bb	BKDR_DELF.XXVR
8a95841bd088a6e8985e378a14a559a7a192142e7970d2ef3f109b9696ca0e4f	BKDR_DELF.XXVR
910e9e24ba94045ba2ab2beb13d5ad81b7849fb2a314b0b943c8d574b93ebd34	BKDR_DELF.XXVR
913d5c82a9ba2b3a6c42bac93fbd79ed748c1ed4d7b3ff19f97ae770433c7e73	BKDR_DELF.XXVR
9c8c3ce88f8d99207a68405a6d67dec108e58cbf26de5be3130158e96e570b72	BKDR_DELF.XXVR

bd8bc9544c36c1ad681faff0b025274178ad045928beddfaf91841b344a5715b	BKDR_DELF.XXVR
d53ba4cb902eec9d3b7629a6c59704d66a7b4ce14484ceff4237b50f7d165fc4	BKDR_DELF.XXVR
d89654bfd5091e78ab76089feb07f5e48e128ca71b43e743d33bf6ab97dab336	BKDR_DELF.XXVR
e492f301734d6694974086129f66c8afd6368c6540f08c91fb33dd9003da08d8	BKDR_DELF.XXVR
e8ca99bd810ae24fd5a196d30fc41efcf58be8ca2c56f05c4eba48f97a61ef49	BKDR_DELF.XXVR
Malicious documents	
335fa41bff0aabd07b23ac84d4a0eb16e95dce2426220eac0fb8a4c02f05b23f	TROJ_CVE201712824.A
434d34c0502910c562f5c6840694737a2c82a8c44004fa58c7c457b08aac17bd	Mal_CVE20170199-2
47c8b680caaff83c000565a0649ee1419834329afd58505d8459ecac325a7f32	TROJ_CVE20152545.CR
552077169995dba6295c2f61aeda8baa7129176af133b2174b720a628498a085	TROJ_CVE201712824.A
6d981475f453589178f4fb56ffbb579cfa081d77bc2018aacb5097a2455b39ff	TROJ_CVE20178570.DBU
6f73f81ce78588279454c9a2c0188c8386f665ce1d62139a8874270866388c8b	TROJ_CVE20120158.MVZ
7bc9bc2b34a8055601fe52e01b0d4ca0d32ee62287f88b1b6b0d87e8e7ef7759	TROJ_CVE201712824.A
7ef9b59cb57193fb62039602596723189fcdb5986590ca4e55edb1d0034f2faf	TROJ_CVE201712824.A
a577079c23fb59ca552211dd118214c32dd5fcf0a49962c6dec02df8779ce15d	TROJ_CVE201712824.A
b33956a1a0a77023d4ffd4fc2f80650d83fe2da7e174792c840527a8a6271904	TROJ_CVE201712824.A
c33a349c74a7b15833169189cfc31fdb9c7bf25212a113ce363fbca4bd13bd1d	TROJ_CVE201711882.HGH
d1880adc559a52bfccc50f875eab81d8a9f18ecea55f3554168ac06a1315c712	TROJ_MALINK.ASR
eea8cc1d819e44fbd5715d746597afac1e47647bcedce4f748cba17306ea2043	TROJ_CVE20178570.DBU

Related Command-and-Control (C&C) Servers
http://ambicluster[.]com/aoc[.]php
http://ambicluster[.]com/sampler657dsadsadgt6[.]php
http://classmunch[.]com/rest7987987rewrew[.]php
http://voidplask[.]com/singleton[.]php
http://voidplask[.]com/reque79797dsfds[.]php
http://lepze[.]com/webseries[.]php
http://conioz[.]com/wertyuio9876tyghtyu[.]php
http://ringatomic[.]com/xmsyn[.]php
http://conioz[.]com/hrserialeoiuwtogtf[.]php
http://crazeprint[.]com/Commentallezvous/FrappadingueAvoir[.]php
http://hikevalt[.]com/Visual/stud[.]php
http://upgrade9[.]com/roadrash/team[.]php
http://scan8t[.]com/delta/deltafile[.]php
http://scan8t[.]com/pulm/scrub[.]php
http://work4m[.]com/engine/mkfile[.]php
http://scan8t[.]com/silo/strength[.]php
http://scan8t[.]com/encourage/spring[.]php
http://scan8t[.]com/encourage/spring[.]php
http://work4m[.]com/suffer/catfile[.]php
http://scan8t[.]com/pulm/links[.]php
http://analogbiz[.]com/pause/break[.]php
http://logicvisor[.]com/WTzFMQbzfmjehThulJnhyA/ntfsfilesystem[.]php
http://logicvisor[.]com/vwVKKGnSmfRguGEuGjGmcja/fatfilesystem[.]php
http://logstrick[.]com/Million167786gg/original678tyhghg[.]php
http://logicvisor[.]com/Scroll454656capsyt/standard567tyr[.]php
http://logicvisor[.]com/LIEZhJGpwVfRlLCcbzrdPlb/rootfilesystem[.]php
http://logstrick[.]com/Bos24hhgihkgch987987f/modified7687shdf0990[.]php
http://logicvisor[.]com/BoiUiNqDvkAbaoSlakfKj/filedirectorysystem[.]php
http://relaybg[.]com/estateertret76576fewr/Maxcvhfdmin8797fds[.]php
http://digivx[.]com/trick6878ftomfe/Reo768768jhjkh7687[.]php

http://i3mode[.]com/dbExpressversion/db87987Administrator[.]php
http://digitizet[.]com/express54354view/docc7686gg154po[.]php
http://digivx[.]com/trick6878ftomfe/Reo768768jhjkh7687[.]php
http://scrollayer[.]com/equation3343tweywd/linear87987987ytre[.]php
http://errorfeedback[.]com/MarkQuality455/developerbuild[.]php
http://computesystem[.]com/scrol89r74gfeflock/electro686876fsdfs[.]php
http://qutonium[.]com/Bingfdkshfljsafljsaf/spiraldquiyqwiudff[.]php
http://buffdrops[.]com/wing/wingfile[.]php
http://sysknox[.]com/invert8uiusaokikdpkswer/redsad6876dsadas[.]php
http://redopro[.]com/severe7fsfdsdfsdfsdf/several45yutuuttffds[.]php
http://computesystem[.]com/region878777yygyg/tide6565fffffd66t6gg[.]php
http://scrollayer[.]com/request6876klgd/prior8658768djsfjds[.]php
http://by4mode[.]com/rsdgbukhifndfjdn/gfvbjkjfvhbdfdn[.]php
http://zonafield[.]com/sdfkjxlik42w2kd/dfdsikj453ldfb[.]php
http://portstake[.]com/fvfbdfbvfhvdh/dfbvdfbvfydfv[.]php
http://portstake[.]com/fvhbfdjvdfhvb/vfgvdhfvdhvhdb[.]php
http://sysknox[.]com/gvfbhfdvb/yrffgrgfgh[.]php
http://redopro[.]com/uygruhutfhg/fhgvfjbhg[.]php
http://redopro[.]com/fgsfhngvd/gdcfdhsvgfh[.]php
http://redopro[.]com/vfyggvfdu/bvufdhvfvfh[.]php
http://scrollayer[.]com/dfhgbhjf/yfghfdgjh[.]php
http://capsnit[.]com/gfhfdjghf/fdghfjghfdj[.]php
http://redopro[.]com/dhdvbdvbc/rtfygtdfdfgv[.]php
http://sysknox[.]com/ytyhtfightf/sdfgsdhggfds[.]php
http://sysknox[.]com/dfhjfdvjfdvjdf/fgjdfgdfkgdkjg[.]php
http://capsnit[.]com/fyudvhfjdhvdfj/erhdgvkjdfhgvjkdf[.]php
http://yetsyn[.]com/dfghhughfhjtighj/gfihighrtgirjtf[.]php
http://yetsyn[.]com/rgtreugreugh/rugofdgiiofjh[.]php
http://yetsyn[.]com/udghdfhgkfdgj/rergthghdfjh[.]php
http://lepze[.]com/bandwidth567ad/sky79asdastracker[.]php
http://lepze[.]com/bandwidth567ad/sky79asdastracker[.]php

http://sysknox[.]com/ydfgfjrkghkjdfhg/grufghrjghjrvh[.]php
http://capsnit[.]com/zoom87687r6wefrfs/randomytuyt56[.]php
http://traxbin[.]com/purchase61dfdusfdsu/costnbenifit8889[.]php
http://twitck[.]com/IUHHGdjhgdfdgvfdyh/yudiqwhdikqgdigwgdujh[.]php
http://referfile[.]com/iueyriejhjhdgfueguegft/uedhehdgeudgedhgeugfytf[.]php
http://referfile[.]com/uiyeibguygeebd/uiygdjhutyjhsgxjkAg[.]php
http://twitck[.]com/jweuduxgyxhygdh/uirfwekjfhiewufifhuefguh[.]php
http://appswonder[.]info/dopqeimety/krtmfpkowqgsty[.]php
http://twitck[.]com/ytgcredaoipqwert/rtdjioqwxzdf[.]php
http://blueclickr[.]com/loekwluhekwyfktjg/kfjalfmkjffdh[.]php
http://referfile[.]com/rajdowgvdkshgdrsvv/ahrwnxdswpoh[.]php
Links to malicious documents
http://flash9v[.]com/rolls2/wingtrs[.]exe
http://flash9v[.]com/soup1/winfsrcvry[.]exe
http://flash9v[.]com/soup3/winfsrcvry[.]exe
http://source4z[.]com/torato2/wndocxsrb[.]exe
http://typehash[.]com/pad1/winmedia[.]exe ; http://typehash[.]com/lambs2/winmedia[.]exe
http://aliasway[.]com/nor3/cmdloader[.]exe
http://gigatrons[.]com/bor1/inspckge[.]exe
http://gigatrons[.]com/zing1/syscrlog[.]exe
http://bitzroid[.]com/joy3/cmdloader[.]exe
http://b4invite[.]com/aPPTx9E3Rk02/wsysservc[.]exe
http://bitzroid[.]com/jnDV99inp/cllproaxis[.]exe
http://trekicon[.]com/nw/cdesrssr[.]exe
http://xtrbuz[.]com/ov_g2/fnvndcver[.]exe
http://crowestore[.]com/dog/avg[.]exe
http://w4zone[.]com/clipart/winvc[.]exe
http://w4zone[.]com/Document/word[.]exe
http://dragb4u[.]com/video/VeenaInAction[.]avi[.]zip
http://entity4u[.]com/rolls2/winfsmod[.]exe
http://as-pn[.]info/images/Screenshot[.]zip
http://traxbin[.]com/final/yes[.]exe

http://117357700-328882259567290481[.]preview[.]editmysite[.]com/uploads/1/1/7/3/117357700/aimplb__remove_salman_nadvi_[.]rar
http://chirpck[.]com/NE/template[.]rtf
http://stringbit[.]com/ABDIN1/cllproaxis[.]exe
http://www[.]checkblink[.]com/ABDIN2/cllproaxis[.]exe"
http://yetsyn[.]com/b1/free[.]exe
http://capsnit[.]com/z[.]exe
http://chirpck[.]com/NE[.]jpg
http://32player[.]com/rims/lgfxtray
http://yetsyn[.]com/NSCN/New%20secretory%20list[.]doc
http://yetsyn[.]com/NSCN/INDO%20-%20NAGA%20ACCORD[.]doc
http://pikrpro[.]eu/DSR/21[.]06[.]2018[.]doc
http://pikrpro[.]eu/candida/AAT%20national%20assembly%20final[.]inp
http://gwesteiwr[.]com/onetwothree/Operational_Reports_June_2018[.]doc

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