TREND MICRO | research

TA505 At It Again: Variety is the Spice of ServHelper and FlawedAmmyy

Hara Hiraoki, Jaromir Horejsi, and Loseway Lu

Indicators of Compromise (IoCs)

File name / Description	SHA256	Detection
document	d8ade980ddc546d5bcc8a30dd652f23626fc864cdda53c52a421d5648d2b1ab2	Trojan.W97M.SERVHELPER.AA
document	f6cc3a2040539caeb3ef5eb4acdc282781b31780905df182c8bd942723d1fde5	
document (fedex.doc)	54ca424715511e387a2faa1485a9758bad3cca7c42f3bdee27a1cd1d845f0512	
document	9e0a804dee94320e08ddfef46a3931d06229961289e8957ec0b46baaeaf4e808	
document	186dc9b577bdf5f3292798e0e57543a34fee0dbd3ea173ba07e8656306b31	Trojan.W97M.SERVHELPER.AB
document	19a95d757437d8823c2f0e7f21e3a12591880fdd0d2cbdbac3c7b22780ec7a54	
document	6e6ff43696447764ad5ff791840659bece2a9b1200039b4235754a0e7cf32bfe	
document	762dff522d0089fa4e398434831bc0f239e1925283ea9858a21a80e3ce010ef3	
document	781c36d3eb798c9891e7a2343bf3e7d078adfd8e19aabddb2f769f1fde14c589	
document	8598512abf2657a001410eb9596776d541620ad790387d86657d7ad309c98059	
document	971a9d57b197a1deff9db94345d70d7e2123fc7d58117e3f332fba0aa9f2842f	
document	b1841c827124933599565cb30073590a5812a65ced4f727a4155407718898db3	
document	c87798f3dfa09921a847b5a031a9996a960aac1d81ede58d87194351b8f6fc88	
document	dca31760841b7436c8f73da1568b9badc4252c4eed74386007df18c3aaf1dc06	
document	d71bcd0db6aede812d90f60706dbd9823ea415456dc2240efe4cfe3f111d662e	

document	fea4517f6ba55d81122370e617fa39dfad94a76bc9af9ac5d5d4786479235ecf	
.NET downloader	1a3a349a9208507beac1e13f13c3bf5ddfe31ed70ca635198475193d72999d2e	Trojan.Win32.SERVHELPER.B
.ISO	3d2662c430e740b664dc3d8e4b31466c8265784bc3e8cf5f2825da21bf1eea4d	
.ISO	9d6812db04dc6772a94e6b30d41623aee2cc487f3fab8020c431e33ffa77505e	
.ISO file	d62cee34e7191feb660232b892d14c757bf632d69f65062733d86ea225bfca58	
ServHelper	3ddeac428ee7fe4cf24b589391e8bdb37a78ef1cfbd43fbd53d393d532d6fc2a	Backdoor.Win32.SERVHELPER.D
ServHelper	420739dcd63ff24a439524d7da8c7c73b65617f56285b9d9c93aef579094c655	
Stelar.exe	49516f2c59b5c73512353ced9740c3988af5c023f518ccd0dc04bfc68095540b	
msi	5f27735f2750d445d879356bcff4c335e1fcfce8399dd361f716319d9d00c9c3	
ServHelper .dll	6642565f8c3dd0e7b72644ed5b762f525ed5fb51518fa77614c38cf6f4bd9bd8	
ServHelper msi	0a4a28d73724476c73523bc9d250c00810cb0154e63b7a9fcb42aa5f2e2381f9	
msi (km)	ac7a9727ebae6d5a18bb9742c2e637bbdbceb1f17b90943ee267b5b8b18124a5	
ServHelper	da8d9fb287865bb12d3459bea2cde522c15e11a7057eba712968ac559214801f	
ServHelper	e9f9b7ee13748c7734d91995d5b1b96d80f003e391a2f1e740f904981347b88a	
msi	e41f7eb6f9b7d6101c3fb2ca3c709f139090b3cedceb4da7437ab677c467be7f	Backdoor.Win32.SERVHELPER.E
ServHelper	ff25a357a30d3e222f7ed03c766c4e98a1e69c6a012ec2e9b5f6d4e602d6d559	
.LNK file, downloads msi	d857dfedf10fc480e0af5028069ae7f533ad7be0a716e431b0e6e490563686eb	Trojan.LNK.SERVHELPER.A

document	19a6a7faffb4532316fd7de0b805d9f587cbb322300972baa8ef7a78f9a41e8d	Trojan.O97M.DEDEX.SMNH
document	9f0e6c82f18ee8adc7581746ed62f28af9f115cd1a763410976ce6dbc9ba1d90	
document	ac416e3da3d33e098846950f51b9cd9d4d6eb47e785f2c07d7de43214f27046e	
document	d905d5fa262a604f8efaea5c463c2b69a8b857c01e077d7a23753a066a456061	
document	3ed62579abcacf90f6ca7020834a02ce278cad384ef09cf39ec10c73f3abd891	Trojan.X97M.DEDEX.AFJY
document	6568dac193729270df3ee6974d55c84e7f26435c641542ea4b45a0e07e7fb065	
document	72505580cb5304ab09659f30721b0a67ad44ad9218c3dc77c231668d088bd5e9	
document	8022e43af191157e7691362ab1ad98fdcf99ff968b54a7a87febd0de5c3b1dc9	
document	8cc61af273af7dd2e10e34c2cfca5b4e857408eddefacde14c95b215209b6dba	
document	03a660faa186d44b50bdf428b535f38fc73e5fc1ccddb5c878597f780b25b8e8	
document	dc5fca5794ad3dddde92b00e2996f53290bb1bc8823468efd2aa8b009a9946a7	
document	faf05fd957b1805a545601aed940d90e2764caf2681580d15105627e010b17d7	
document	60431edef1154bb832f78bcbd7eb414778cbd1880cc06c959354916d95a3fa20	Trojan.X97M.SERVHELPER.AA
document	862913bc218df4f23e853d21ae410fb208991453b4db2b56372bea527e57f1ce	
document	d5b8de1b4c278a3c2726a8e732e647ae11eedadd1513ad51e84955d1e36af2e6	
ServHelper	56177ebe737d456f0dd502a80565c769ca2bd03893cf59976fd85c2a731b74d9	Backdoor.Win32.SERVHELPER.D

.dll downloader	4064ff7e06367b2431d371ddd1e97f659ec7f3c050229350725c91d6fffff835	Trojan.Win32.FLAWEDAMMYY.AB
.dll downloader	7fc8af6637dbf4591cb6df5ca396b7e4ff4e0d4706074523740573616b53ad12	
document	19afa4a3b01133847e1e3db551fd071e12f17b48fd1bb192a9d804a2701220a8	Trojan.W97M.FLAWEDAMMY.AD
document	287f2218c313a7cbaf693712c3ed6a5d9f00f2d0767bba27cc8b7b1ae8f6d96d	
document	20798550470b6649ea521428e95fae1efd9e1662a4d10e94fd06cfdc5be114a5	
document	2d9e03bfcb47241f298aa3cd98eeeafb339b60f0c474dcb85342f0e76f59c6e7	
document	3fbb90ce01a548955b3e2fbda4de3b5a83f6ad1db846d19256df994777f8c524	
document	68ec8b125811ca2d383ebf83ba180b65f77e9e47f83bdf35df252e1df76545e7	
document	6f2a2fcc2ea772435124f8bf4bf403eb14112757fece0a00a2727002c83055ee	
document	8ac14102d374699308703d4a5d50043a52930e63b81bade406eba4c5687271f2	
document	058b462cfcece79e7e6c77a3bf37c1f1e34c4d2238af47cdea379e69895903e7	
document	adbab063abafa6e3773274b2095b688a44b71a93a1dc16069c86b86730b0d6f7	
document	ba0adf6d839f9a29360d33ec834738abae31348dec60b59e044135454ee2c961	
document	e179d0e5cde00e30fe63d2a29dc9892a2806b245671f385a4c2e2543add72e47	
document	ea1311a458f8070daaf1fef363ea1b00acfaea097c1c6c4519478197ec36ac36	
document	eebddefe6200d95c3e48d7f3257064fce6bdfe6d01695b7e0e3aa21a523f0ccc	

document	f1eca0a4c944cbad2cf683389f39d94fb666d9ed0442769c4fb8d75153a7902e	
document	f23f39b2090f38e7adb36dc0738385500e7945c351bcd57e7e5bc7b5f1cd1c0b	
document	f51b305eb32dca589e656b4e30e76fa5cc47d96994e19b11f7748477bc9de8a0	
msi	515a3cbc1117d5df84b72ba7dfa14719d81e0b97a01ddcd483ccb60e1a34cee2	Backdoor.Win32.FLAWEDAMMY.AQ
.DLL FlawedAmmyy downloader	12edbdbd0bb2f813e9aac9cfabc7fe9de8b39a0a90f79f3fc6324f49a6f333fa	
msi	44ddb11cb29b9e9a9641ae451e4778d208c944cd5f766e0c45682c94c0aa1d46	
.DLL FlawedAmmyy downloader	ad320839e01df160c5feb0e89131521719a65ab11c952f33e03d802ecee3f51f	
FlawedAmmyy	8d4761a4a43813a529bcda234d1c0c147f6d855ee3520b4934abdc5d42d3ed48	Backdoor.Win32.FLAWEDAMMY.AR
document	3530b085f7de6d275ed7ac948ece7a463393a55f6c371456b9dc4c6f0da01f8c	Backdoor.Win32.FLAWEDAMMY.ENC
document	3c4d5743d39f32ed72603e59e3760013b82e4cfd50c1fc43ca6b1b1c27b5ae48	
FlawedAmmyy (encrypted)	8d7b6772037101285afd097ac7819ac1dc7de89d215915d0686daad94d75b330	
FlawedAmmyy (encrypted)	09915830d2a710408c3b96fc3a0cd8c10d6a2b1bcb1d781d4703c80a263d2084	
document	2883d66257e92b48d0c8da0e50323db520d2223f873d4a16aa067fcd7186424e	Trojan.W97M.FLAWEDAMMYY.PUQ
document	20c92ce1e26055a6608dce2d6897ebe5b213272bd5bc682b73699876794f23d4	

document	367eba13a53bcbce1665bcdc24c011574e0d8bc736e0cb46081111aa11e99164	
document	37c721796e4337deace23bf25d09bfe4d0f090a8f45227b1416c8ba14654b1cf	
document	308ee586ada3bf313c87683678f8b07e360c16fef1d826681acc7f839b5d87c6	
document	4991cbfe921e5e0e26819e4ed4b313873e0bd817cdb56d017959dfde577a24af	
document	4bdc8e660ff4fb05e5b6c0a2dd70c537817f46ac3270d779fdddc8e459829c08	
document	535cbd2b37fa8e7766145f94aa5a6c44cbf952a238a46540e00b3349dc63e770	
document	6c7e8d87e389b1844a2e3282e0b80295cd117ac5d5302cc56bb9e0b1df5bd85b	
document	71b713e0581d90f7e7fed3158e341edcaf15216a7532a40ab5ae581e610faffb	
document	775bfbb33bce476084b469a8e71a6706f3f3961eef34fd12d1fedbccd0526926	
document	81a1331ba0c2b4545622da1996385dd170bcc9cb20eef5fd22641d4bd4fdcf43	
document	81d5d7174f9281db31609c5754d20c4dd523308b4f8ee2209244dc4197491ec2	
document	889a572946d517befe52430e6aad2007516c3dcdc69a9d2f3cbc931e2ca1b1cf	
document	8f9dde0b337ccf89e93e0975a05d5238beda08ba8823a61f895f9742e012eea1	
document	957f37a154fe18875fba6ea25793f1a2c7e389749aa472a84a8fecf92cca9d74	
document	96e55033184869fdb3038e0658cf2dd78f057cb570c4f391e510ffb1b75ca468	
document	9b61232c98c75e73973873a96d95570c09a85e369aae506e894a6b295ce0fb1f	

document	9ccfb0e7b241d19b6822aaf58c3cad7308fba3316a600fb86cf37790cd9dbed5	
document	0476abd6fcba4104411740d3cbdad963d450c90081ad04f10934566871a65d3e	
document	b11fc8a157d2b10ef0ca97fe85850c9a557f28d28030c40c80e9648b98ac0aa7	
document	c758f8e3b006fb6ededa345e664ffeea348ace28a45d4967c4fd5305fb45c4f3	
document	f76662e05d060ec72d53e293dc7ddcab7ec118b8023cb1048581750eddb3b6e3	
	2524c10586cbcc8a54d1dfa3f7b131d119f57647e174dd55fb5bbb52f90ffeaf	Backdoor.Win32.FLAWEDAMMY.SMA
FlawedAmmyy	516e584913dee110e15b8b61bff92b0c6766b1157e4b5a8af8f07a8779af6230	
FlawedAmmyy	81cfc3d1055b96f40cd67bdcfdc5a60c3dc041948199dfed00641bfc48fdf053	
FlawedAmmyy	b9affdbb9d73da22e2e410d71b044f1b2f4376d7dbcdc03a4ea7ee3f5cdc9c1b	
FlawedAmmyy	c2cc59c6fd471678b34cf51055a59462a178ec95a5b6b424f464c6611e8bd22a	
	26b42a42f63e64942185a1e4150285dcaa2d75e6fd03c3df9b38f6d6b3c57f8a	Backdoor.Win32.FLAWEDAMMY.SMKAT
	443c90cdfe96a9ac6b696146a947d51742af3346e0c126f9d061756ea01017c2	
FlawedAmmyy downloader	460ba8a7b169af5033e7e4cdfcd7e69c2a54a53a9e6da8187cc97263f740110c	
	64a56627bf8fb75fc5cfcce44ca4e217d64d75c60e9a3c57a626d3eeb39b1c81	
	9e1f799562db2713aa52eb135b1f3d92d685d1f35da3dea29a25e862807acb8e	
	b47091051f8bd4d585cd39a7e16a1000afa82e2ddb5867c6653e20648cbf064b	

	bba2b10dd79660b6624b679fb0719e0a06ea8d6d852f9a69db22bffce15a05b9	
FlawedAmmyy downloader	c4fd77adea4ddebf40568ba71d8799d3acc92ece99abc813df650dce9c2d0f58	
	e0191d89a73281eacc65afa8d705327763c7e93bb535928eaa30498313a8c791	
	f23e455f70d7ca801a3b8f090da9761355c6d5492cfadd6aaf5c1bcc8f9f87a3	
FlawedAmmyy	fdfc7743946af381c08481451653dc3b1a6bbfc7abe2af2f90debc914f47166f	
	5ccb1e6bebaace8a3db7e34ea55a3b2fdf5e8f0b06c2cac640620fa71c852194	Trojan.LNK.FLAWEDAMMY.A
	3a79c6de1954d53bce81924e0bd2cbd5906005b2a87458320ca4c72fbd5c6f54	Trojan.Win32.FLAWEDAMMY.DLDR
	6a30c5ac83594b05a5cf418850afb4ae088f58517319cd8f70ef348bf7934708	
	9dab3bd4f4f6bf966e07eb9f76f20b9bc54b9a56eca0df273a8665d46c3e9184	
	1fc750d20a737e46f696d7fb121fd677db352e3129b53d081425de124a194231	Trojan.Win32.FLAWEDAMMY.ISO
	5a34c19528ac5dd3fabed9b097d17859baa646af139ed1b2d9bbc4c4388ea04a	
	83c6f349f4954ada3d9227832e56326668f0a667b4e11d0e1f532694013a3180	
	a9931fa6e0d0300099b2e212758df226c97deb7e168874a286e54922a5b98822	
	cb36503c08506fca731f0624fda1f7462b7f0f025a408596db1207d82174796a	
	23a5d6caa3b822f57d51e051763535b1536e0db0d2987b9905706d0949d13cba	Trojan.X97M.DLOADR.TBFD
	27261f0ad7e276667a8266dcbfaeabc062ac9243425de9568baab7af26635675	

	340964a15b5ceccd3b3c127cf03b32522a2cceccd9e8aef6cd7e54ac6672533b	
	30620d2d115079e501fc824e7dd802bfc3e001c865481a84a7a959d71017bc22	
	384e809707b593151d75d8c196b5b00019b060387da7f8c21a06c52c787e0cc9	
	0abd2cc220b3c1126dccab93e0c919511dc7156d0ab081636b601cc24fe844d3	
	0c36e65fcc09cd12f729d542344f93daadcbc0c2adb3460161a5095a5ace7d9e	
	9294997053e9fd404a4f154165cd8c210d4c35654e93412d50bdd92e4b14a96c	
	a967fb9c5e2fb3b5e9fd78eaf37f9eb1f11d15f118c993ec40d062a3aab8c131	
document	1eb6a4facd28b0a702b0a58f9a8338a6a32b709f7cf4b8b4adc6791ca5154954	Trojan.X97M.DLOADR.TIOIBEFE
document	777ae4fe2b06c018d58304a8e8748165fbfc0bf607fbf5918e2fc1a05464ce45	
document	7e198b8fc8ae4e05fdbcfab3b29de656e31e903752b9096e5979e8ce835e590e	
document	9fffa2ac1cef1e2d178fe1389667a203a2465d9e39e1e9d62384510bdab2aa40	

Related URLs, IP Addresses, and Domains

• *hxxp://109[.]94[.]209[.]91/1.b*	Disease Vector (79)
• *hxxp://109[.]94[.]209[.]91/12340.txt*	Disease Vector (79)
• *hxxp://139[.]180[.]195[.]36/p2*	Malware Accomplice
• *hxxp://139[.]180[.]195[.]36/pm2*	Malware Accomplice
• *hxxp://159[.]69[.]54[.]146/555.msi*	Download URL Malware Accomplice (78)
• *hxxp://185[.]142[.]98[.]41/2.b*	Disease Vector (79)
• *hxxp://185[.]142[.]98[.]41/3405.txt*	Disease Vector (79)

• *hxxp://185[.]17[.]122[.]220/555.msi*	Download URL Malware Accomplice (78)
• *hxxp://185[.]225[.]17[.]5/2.dat*	Disease Vector (79)
• *hxxp://185[.]225[.]17[.]5/km*	Download URL Disease Vector (79)
• *hxxp://185[.]225[.]17[.]5/r1*	Malware Accomplice (78)
• *hxxp://195[.]123[.]213[.]126/g2*	Malware Accomplice (78)
• *hxxp://195[.]123[.]245[.]185/1.dat*	Disease Vector (79)
• *hxxp://195[.]123[.]245[.]185/km*	Download URL Disease Vector (79)
• *hxxp://195[.]123[.]245[.]185/r1*	Malware Accomplice (78)
• *hxxp://27[.]102[.]102[.]235/2.b*	Disease Vector (79)
• *hxxp://27[.]102[.]102[.]235/235.msi*	Disease Vector (79)
• *hxxp://27[.]102[.]102[.]235/235.txt*	Disease Vector (79)
• *hxxp://27[.]102[.]70[.]196/1.dat*	Disease Vector (79)
• *hxxp://27[.]102[.]70[.]196/1.dat*	Disease Vector (79)
• *hxxp://27[.]102[.]70[.]196/k1*	Malware Accomplice (78)
• *hxxp://27[.]102[.]70[.]196/k1*	Malware Accomplice (78)
• *hxxp://27[.]102[.]70[.]196/k2*	Disease Vector (79)
• *hxxp://27[.]102[.]70[.]196/km1*	Disease Vector (79)
• *hxxp://27[.]102[.]70[.]196:80/km1*	Disease Vector (79)
• *hxxp://45[.]67[.]229[.]36/p2*	Malware Accomplice
• *hxxp://45[.]67[.]229[.]36/p2*	Malware Accomplice
• *hxxp://79[.]141[.]168[.]105/g1*	Malware Accomplice (78)
• *hxxp://79[.]141[.]168[.]105/g2*	Malware Accomplice (78)
• *hxxp://92[.]38[.]135[.]67/2.dat*	Disease Vector (79)
• *hxxp://92[.]38[.]135[.]67/k1*	Malware Accomplice (78), Disease Vector (79)

• *hxxp://92[.]38[.]135[.]67/k1*	Malware Accomplice (78), Disease Vector (79)
• *hxxp://92[.]38[.]135[.]67/k2*	Malware Accomplice (78), Disease Vector (79)
• *hxxp://92[.]38[.]135[.]67/km1*	Malware Accomplice (78)
• *hxxp://92[.]38[.]135[.]67/km2*	Disease Vector (79)
• *hxxp://92[.]38[.]135[.]99/22.b*	Disease Vector (79)
• *hxxp://92[.]38[.]135[.]99/99.txt*	Disease Vector (79)
• *hxxp://armyoffers[.]com/docs/saz.php*	ServHelper C&C Server (91)
• *hxxp://coreapc[.]co[.]kr/25072019_8351.xls*	Ransomware (95), Malware Accomplice (78)
• *hxxp://fakers[.]co[.]jp/25072019_0963.xls*	Ransomware (95)
• *hxxp://fonetorap[.]com/docs/saz.php*	ServHelper C&C Server (91)
• *hxxp://hukumaru[.]nobody[.]jp:80/25072019_8873.xls*	Ransomware (95)
• *hxxp://korpla[.]co[.]kr/25072019_0291.xls*	Ransomware (95)
• *hxxp://krselectrical[.]co[.]uk/25072019_7230.xls*	Ransomware (95)
• *hxxp://lotmoji[.]com/docs/saz.php*	ServHelper C&C Server
• *hxxp://nonestored[.]com/docs/saz.php*	ServHelper C&C Server (91)
• *hxxp://nonestored[.]com/docs/saz.php*	C&C Server
• *hxxp://runpen[.]dothome[.]co[.]kr:80/25072019_7892.xls*	Ransomware (95)
• *hxxp://stalpina[.]com/docs/saz.php*	ServHelper C&C Server (91)
• *hxxp://stelar[.]icu/sun/s.php*	ServHelper C&C Server
• *hxxp://towerprod3[.]com/docs/saz.php*	ServHelper C&C Server
• *hxxp://www[.]fedexdocs[.]icu/fedex.doc*	Trojan-Downloader.Script.Generic

• *hxxp://www[.]fedexdocs[.]top/fedex.doc*	Trojan-Downloader.Script.Generic
• *hxxp://www[.]izu[.]co[.]jp/~saigo/25072019_1120.xls*	Ransomware (95)
• *hxxp://www[.]ma[.]mctv[.]ne[.]jp:80/%7Eblanc/25072019_4093.xls*	Ransomware (95)
• *hxxp://www[.]pa[.]airnet[.]ne[.]jp:80/%7Eishi/25072019_1390.xls*	Ransomware (95)
• *hxxps://senddocs[.]icu/stelar.exe*	Malware Accomplice
• *tcp://160[.]119[.]253[.]219:80*	C&C Server (91)
• *tcp://169[.]239[.]128[.]29:80*	FlawedAmmyy C&C Server (91)
• *tcp://169[.]239[.]128[.]36:80*	C&C Server
• *tcp://45[.]84[.]0[.]82:80*	C&C Server (91)

TREND MICRO™ RESEARCH

Trend Micro, a global leader in cybersecurity, helps to make the world safe for exchanging digital information.

Trend Micro Research is powered by experts who are passionate about discovering new threats, sharing key insights, and supporting efforts to stop cybercriminals. Our global team helps identify millions of threats daily, leads the industry in vulnerability disclosures, and publishes innovative research on new threats techniques. We continually work to anticipate new threats and deliver thought-provoking research.

www.trendmicro.com