TREND MICRO | research

Latest Spam Campaigns from TA505 Now Using New Malware Tools Gelup and FlowerPippi

Appendix

Indicators of Compromise (IoCs)

Hashes Related to TA505's Latest Spam Campaigns

SHA-256	Trend Micro Detection	Notes
32b518411ad33b1454812d7c8fe2c8e7b507d3659c7a620adf570cd3cbd12913	Backdoor.Win32.FLAWEDAMMY.AN	MSI
f07a0970cb9a1a8172a7980bf08b3bfcc7007b4d12cc207d0ad6a5a02732ace8		
d08e515044a61b2b2dad9deda564460914a9559cdfb9772babf04039d3814252		Amadey
ae46e7530fc3e51829e8939fab1dbb1958d4426598d81c5e1cf8ad8ef30bf44b	Backdoor.Win32.FLAWEDAMMY.AP	Email stealer
1e931d4b48dc12ae3e1b725471fb812486aa6dc15aa66f6803b0ca39ce5bcd9b	Backdoor.Win32.FLAWEDAMMY.SMKAT	FlawedAmmyy Downloader
9988a8e5dc49a84f1397a224e0b69a73609d40227540b1ac6eeb4f5d3475caa9		
3353f306853844c951f6332af61b804004b7759b8f56b3a62f4eeb485c793b94		MSI
b25d805a85f9d2bb611b6f6c03836ef58210af18b8421c57ce5fa31b3cb5fb10		
8034a77e0feeaada1abc5c9ccd6b7fef76fe6d01eaec63a83c37cecf2899e255		FlawedAmmyy RAT
fd76972a310d77524b47676e944e7a348f20634da5e4e295bed4ad6cfd1b83cf		MSI
1317703bfb7b0f3eeab6af67ec0fb29368ab12b06b256f6639648b85e8aa76bb		FlawedAmmyy Downloader
a1d8dfcea46dcaf2e5faab857389a6fa2bf19a29a4dbb7a31e8aecffcf468bdc		FlawedAmmyy RAT
5b589d5d3e226818a9eeb4f8294d18d1251a3a57eb3a28131fb8729e9957e5ed		FlawedAmmyy Downloader
744d44cb8b6f4d9ea547553e89152827629090701bc56c386a36264125ed81da		Amadey
7e885b76fd19fc8f9733aeecdd3789a6aeb2c2fb810bfa90a600f20805b68b71		MSI
7e885b76fd19fc8f9733aeecdd3789a6aeb2c2fb810bfa90a600f20805b68b71		
da6af8a50e2be3abd46bd24a9d125706e00b26b6721c1b28faf4eb0b2384d52e		FlawedAmmyy Downloader
744d44cb8b6f4d9ea547553e89152827629090701bc56c386a36264125ed81da		Amadey
7e885b76fd19fc8f9733aeecdd3789a6aeb2c2fb810bfa90a600f20805b68b71		MSI
526582ad66a0f96cfac8dd11841ba499a34310efbca37799d9217abe6beca88c		FlawedAmmyy RAT
3b92b542c31e879657f2b41a51ce8a347821a43feb3b4177bc242bd47833831f		

SHA-256	Trend Micro Detection	Notes
43029bb89b0c7203743f75cc46f137041304b0e253fb0f7e58b3eb27e7928b5a	Backdoor.Win32.FLAWEDAMMY.SMKAT	FlawedAmmyy Downloader
bc7a23485a8c10672ebc7c998687fe837ab296e01fbf36fde08a8ce013ff67be		MSI
19d8993c742fc1a7c651ab3dba4d8c7f5e142a8421e22dd0c20c2db2d5dccffd		
cb114123ca1c33071cf6241c3e5054a39b6f735d374491da0b33dfdaa1f7ea22		FlawedAmmyy Downloader
cbea31ca496945a22c1ddb992f3954056060e764d6599f1725ce3f3293b30934		MSI
5075f2381e2bdf01104da1b4d28a7806b4cbe90d7a3726a565e2a8fadbf09ab0		FlawedAmmyy Downloader
c2c6f548fe6832c84c8ab45288363b78959d6dda2dd926100c5885de14c4708b		FlawedAmmyy RAT
163a485bdeb03b6d5f9ad97f0b5292a38844ed86e8185e44e151dc5df4f7a272		FlawedAmmyy
4e26c3b4710ef97462a74baa0c9dd78524655f7aa9371570b8c3a270b5111f47	Backdoor.Win32.FLAWEDAMMYY.END	FlawedAmmyy Downloader
d0ebd37bd6a4d1760210d251130c3cd8ed239161e65b78f54366720daca954bc		
4996c6994768eb2fb9e37efdf2993a8a41927f0bfaaa0c094923da51529b5ecf		MSI
f34ff23255ecc38fd660042df1723a44f066011dd875f1c89e41457dd5131db1		FlawedAmmyy RAT
e12c906b60bbb7fe15ad8aaa4029d36679b9707e8c0dc494ef5cf31a973b1693		MSI
b07340bd812ac1d6bab85b1b49c4e935f100b17d59da632533c8ddd361529f10		FlawedAmmyy Downloader
c3d03d9f9b132d1a326ad37d4046ad7b44b93785d20f2c41e950e63f7b316210	Backdoor.Win32.FLOWERPIPPI.A	FlowerPippi
4022ee8ea5880443aad6650f0a88821c841b9b823d4882afccb6d08a7daa9a1b		
39eaba807eaeed6f3ed79e3237c70a492fbce871a98a79c551bdfda240a4e4b2		
d4ad423482621e32a8b9477a7adba1374a51c07b1c0049b6f11cea1ff2cfcffa		
17d11b9e324faf3b1a53d8fdb002508fc0b6236472d762822d9b550c690b2623	Backdoor.Win32.SERVHELPER.B	NSIS / ServHelper
517119d4d9ae8f0b7e2ae6b6b9adc1f0546118660ee1e71afd9e7c1bb8d4c691	TROJ_FRS.VSNW11F19	HTML
955c3c04762858f1a779d51d6a288158feed69f0f20e0b0a0f254ea36b168555	Trojan.HTML.DEDEX.A	
b2ab1a485306bb25f75ad94f334ea5ad829b4d6339324575e04d3d6a18ff8b3f	Trojan.HTML.DLOADR.VWD	
9c0e8ab53fcea4c41d1887c99f12cadbd2dfa4934554bcc2ef179e4f59b7f986	Trojan.HTML.DLOADR.VWEA	

SHA-256	Trend Micro Detection	Notes
531cfa6a35d94624903f498bfcd43fc0df89937fd1891221a8d6303f44dfd191	Trojan.HTML.DLOADR.VWEB	HTML
648bee316a490ea2cc1831a9b3de91252e1fe1d5ac13d04b35bbe09103c201bb	Trojan.HTML.DLOADR.VWEC	
105df91a08857c2e66ea64e899e8ee5702423d213cc372ba035d6e9003ee43c0	Trojan.HTML.DLOADR.VWED	
1b2a92c230fd944ef553f46e4d5576c622c37d2fc5a23aacd327424b0578d586		
ba175e84c6f519570f22d084e12e9bf749aa73bc322643788b622eda5ce636cd	Trojan.HTML.DLOADR.VWEE	
3c1cb96996ae865fc2ba9c9b89fd4b1faf38fb1cdcd39f6de8641c0498247579		
cbfd13caa5f8301c9e0000b39b147cc79d83b03c41aacf3aedfcb9fbde71ef8f		
9e0ba57890bca06af9f92e7e520804a8c1d53445fe21859517362ba0fadb8a2c		
cbd8490b8cb50ff0d7dfa5a4c94e9856daa093a0cfaf4a28d3e2d1dd1c7e2a11		
da1ae3da119271163353b68a5bce6dae96f15208c27549680056bcdf4f227fdc	Trojan.HTML.FLAWEDAMMY.AA	
5bc0cb4909f66436dee7db6d51ac0347865e2841598b7399d26d3932249b9b95	Trojan.HTML.FLAWEDAMMY.F	
769988272bef7c201e328e9609d3e465b6f90c82d01b8cc0415b590d6f2f1379	Trojan.HTML.FLAWEDAMMYY.E	
502a73c776d5c46b94f880f6d27702c0bd0ed14c297a9412b1986b1d9ee7bc57		
e72a88c8b388ebf51bb6a43813e9d39ab12e18468c81af7e8eaa4a0903a43453	Trojan.HTML.MALINK.FASFE	
f6c15547ae8187155e00902bccbe655babd8fd92f7e1dff45ed119750a43a64f	Trojan.HTML.PHISH.TIAOOHGS	
a62a8f18cb563332171b0bcd6b646aeac19594186413ffadeff69e925bcec058		
6ebdd60d46c454c463cd6c9aa487a226ac0b505684e1882208c6ded91e9cb36f	Trojan.HTML.REDIR.WVEHXO	
4a05aa6a5667598f93a5a5089bf110f52a0f7c6fc510db2bbcccccf789565090	Trojan.W97M.DLOADER.PUP	Excel VBA Macro
0bab91b3290a63c14f2bcc134e89c47b520f8e09d97d1771ec2c2506dce0a57e		Doc VBA Macro
10f163f27391c8a9cae6676af2871604b34fbc0cff548b086cd5d1cfe1007949		
b2e35df4e3b4317cbc35001897c6cd53d428416b03639bb65933e3ce1f160fa2	Trojan.W97M.FLAWEDAMMY.AA	Doc Macro
0fe745b26efe3c4d82389d10c43e5755a30e1a794d920a807915313f049048eb		
34ef6ca151453369a321fee1a17450808b40bd35b6fa16de79742d88e382c31b	Trojan.W97M.FLAWEDAMMY.AB	Doc VBA Macro

SHA-256	Trend Micro Detection	Notes
09cfcc51dd91c7e16f8936f9f47842276974e0d5fe993566911e031b37e98d63	Trojan.W97M.FLAWEDAMMY.AB	Doc VBA Macro
50d5cd656ba4061b85e048667bb9720ad0ad309116c591c3158726a165d83bae		
5c361bab21f7db6a58f23c6db38d88b35943544687bd8c643031add429ed135d	Trojan.W97M.FLAWEDAMMY.AC	
fcfaa5a008448be96b273ca3d59e28d4a0b20156909da676520dc5103d15ad77	Trojan.Win32.DELF.AKT	ServHelper
0617ddb1b7e7ab86159bc7be01c86c50a9d7a57db0914486c496e277c10b19ae	Trojan.Win32.DLOADR.AUSUQE	Amadey
5e1e97fc52d2a0eed9272dc4b5603d2a5c142326cc3fb8fa22fb70902e9d056e	Trojan.Win32.FLAWEDAMMYY.AA	FlawedAmmyy Downloader
bb5054f0ec4e6980f65fb9329a0b5acec1ed936053c3ef0938b5fa02a9daf7ee	Trojan.Win32.GELUP.A	Gelup
f3b2d2d16ee2b16fe5c288f9cccb2b2ade13475ed902fda49fdb36493515332e		
1f2be0267a715b6537e14dc8150b32e5cd48bd2642889f89912ec3d1a4bfe1ea	Trojan.X97M.DLOADER.PUP	Excel VBA Macro
65ddf99b086091548237f563f39e7b9752f9e4f0d4d59ef50068cc7ab852097b	Trojan.X97M.DLOADR.JHLZ	Excel Macro
6bfe268c3725cbb75a10f998f019c297e46d09ca9e6222b852d746a5cf522673		
0ca16e3bbff4db92f13797cced761ad59b08d0f6d1489dd24124afbd060c9811		
45aee15c3da9bea29f189e8440ca4f0db7af2ed03b3173b203037c1d282e64b7		
ff0ef9cda2216faa837aeec4c69b5cb77712557746fddc1939b032db910a6efd		
71207a001ee28a5c517d7dfc1567825a1f7c23ab17813712d09fbed2b139206d		Excel 4.0
524b71a88312eaf5953eb839e9d43c8a51d3ff8c9753a837efa34cdb6f3d9cd8		HTML
4094e075b1a9523f76b451071c2df62c345e6fea65c1813758a4154f5688390d	Trojan.X97M.DLOADR.JHMA	Excel 4.0
df3268cf0b904734819cebf7cc10a3955992edb6d596fc432f0e44c79184f2b3		Excel Macro
d8e569dec9850e2b034f99d78cc78fb3b3fad0ab724f890cf65e7110fef3ce4f		
9a1cde5e4e066932debff522b48144ddcf9507955b618cd99815853a230a0ebe	Trojan.X97M.DLOADR.JHMB	Excel VBA Macro
412a76221b95352ff08b86f569ed99599a7cd6ebacc24ccbdd770a7b24b121c7		
a13669d5f8f5d5b67f72b1e5e83e9eaa28ad3e23a9757f2484ce7f5878af2251	Trojan.X97M.DONOFF.AI	Excel 4.0
4708ef059434d195c3eb2e7d01188ee42bccb4219a7aa2d12b0e7ac90544439d	Trojan.X97M.FLAWEDAMMY.SM	Excel Macro

SHA-256	Trend Micro Detection	Notes
edaee521bf4d85a08748119d38d905ef1fd101f63f977f9a2111a280773b3655	Trojan.X97M.FLAWEDAMMY.SM	Excel VBA Macro
15301f69844ff2bdcf77dab4bc3cc604a1ba19460eda5c2cdab077fe7624d287		
55110e9d4b69f35fbc1c41c21c54ffb556e261fdeb2fa5da7ddd2b4fabed3827		
a092bd3894ef02b6b4c9ec7112befad2791b0b907b3510f90b4fcf2ef8d23450		
5f701d503f9e4fb31fcc5c251f9e647e6dcf266d0635ca4b6b856b50942bd78a		
c05f5f4559ce43fbcefdcbf76c7a9e71db4db97afe45786b5c7e924aa130fcfb		
1ea33acdfd21085c06a97d0ff240a55de8fb2496900bd6fd0e03247d107e80ca	Trojan.X97M.FLAWEDAMMYY.C	Excel Macro
b35e2f1010f2f0203f414437362f44044254e62c11895ad0b7561e22d41c8e15		Excel VBA Macro
5e3243428001552bdf3873d7bdbde0303d67253c5ec43dc5951ce5de939087a9		Excel VBA Macro
ff6f9f3006945512678c8f8148345ea75468cbb5a2e7f82f470db3d2382f9007		
7dfc8de60b4e192cb0d6d5479b18715597164ccdce433021aac5af4ce017aee8		
a9ec81179948798b21929d56ac0e8883fd30bf6ac17f6e9dcbf9c85bbc4a3be7		
6311fda702418ed9e24b3d554296ea847d884c602316ca6f7a3544b44cb17221	Trojan.X97M.FLAWEDAMMYY.D	
8621fa54946096ed38aee5cbcc068c0620416a05c17328a527673e808847850d		
eb3792fc83cd65823bc466e7253caf12064826b058230666d2ed51542ac59275		
f21039af47e7660bf8ef002dfcdb0c0f779210482ee1778ab7e7f51e8233e35c		
0e91e6e17f8c8e2f1ae29e13f116c8611cb7679607695eed355025295fb1999a		
01163d0223a353014d14347e1ed2f2873df3ed441d3b91652c045309ba171df5	Trojan.XF.DEDEX.L	Excel 4.0
11a9ae4896f5568c43d697a6e2949746d2c6cef8a35beabbd96e03bb9e8de521	Trojan.XF.DEDEX.M	
56db1f67c467094b0386b7790cb12efb6f2de5cbbb2ed1f8f63a8bb698b4e26b	Trojan.XF.DEDEX.SMNH3	
a9e508392956bdab0d7ccaaf423569d645af43154ba5d9213864328aa28662f9		
c402673cfc7d3012789efdcc0ea865273aa18cf1ffd4e2364959b97b352f85e5		
ecf19496fcbde3c92aa37000ba6e87f26f19d6d753c958830b7f411d39eecc07		

SHA-256	Trend Micro Detection	Notes
a088b80280f841f2c793dd0a75970ba70d2322eac57778a407d16f899fa53951	Trojan.XF.DEDEX.SMNH3	Excel 4.0
e91feb6dac52ce29aad52daa369cb80e6e118f17427c3abcd03366cefb04ecd9		
55951ac49f5792d8c1bfb0072db56895ab5b290b531ed8803b809b62e1f4f3cb		
751a31e4705a4d0ccf08590ba4a1a50096651b6a045a6f5462716cff4d224c82		
518998b37f6e9f1f7fb102503272d0a3e4a3e37500985a8cdb1d495078e22951		

Domains and URLs Related to TA505's Latest Spam Campaigns

Domain/URL	Notes
hxxp://bigpresense[.]top:80/es/es[.]php	C&C Server
hxxp://shortag[.]icu/docs/s[.]php	
tcp://185[.]106[.]122[.]120:80	
tcp://185[.]117[.]89[.]139:80	
tcp://185[.]117[.]89[.]145:80	
hxxp://handous[.]net/ppk/index[.]php	C&C Server (Amadey)
hxxp://safegross[.]com/ppk/index[.]php	
tcp://169[.]239[.]128[.]186:80	C&C Server (FlawedAmmyy RAT)
tcp://185[.]117[.]89[.]145:80	FlawedAmmyy
hxxp://179[.]43[.]147[.]77/01[.]dat	FlawedAmmyy Downloader
hxxp://54[.]38[.]127[.]28/02[.]dat	
hxxp://54[.]38[.]127[.]28/02[.]dat	
hxxp://109[.]94[.]209[.]178/02[.]dat	FlawedAmmyy RAT
hxxp://176[.]105[.]252[.]168/01[.]dat	
tcp://185[.]117[.]89[.]145:80/	

Domain/URL	Notes
hxxp://149[.]5[.]209[.]70/02m	Malicious Doc VBA Macro
hxxp://195[.]123[.]245[.]185/04m	
dp45320398[.]lolipop[.]jp/20[.]06[.]2019_418[.]64[.]doc	Malicious Download URL
dp45320398[.]lolipop[.]jp/20[.]06[.]2019_705[.]12[.]doc	
hxxp://185[.]176[.]221[.]103/01[.]dat	
huseyinyucel[.]com[.]tr/20[.]06[.]2019_781[.]08[.]xls	
hxxp://109[.]94[.]209[.]178/r3	
hxxp://149[.]5[.]209[.]70/02m	
hxxp://169[.]239[.]129[.]60/k1	
hxxp://169[.]239[.]129[.]61/k1	
hxxp://176[.]105[.]252[.]168/r1	
hxxp://179[.]43[.]147[.]77/01[.]dat	
hxxp://179[.]43[.]147[.]77/p2	
hxxp://179[.]43[.]147[.]77/pm1	
hxxp://179[.]43[.]147[.]77/pm2	
hxxp://185[.]140[.]248[.]17/01[.]dat	
hxxp://185[.]140[.]248[.]17/lt1	
hxxp://185[.]140[.]248[.]17/lt2	
hxxp://185[.]140[.]248[.]17/ltm1	
hxxp://185[.]140[.]248[.]17/ltm2	
hxxp://185[.]176[.]221[.]103/m1	
hxxp://185[.]176[.]221[.]103/m2	
hxxp://185[.]176[.]221[.]103/w1	
hxxp://185[.]176[.]221[.]103/w2	
hxxp://195[.]123[.]245[.]185/04	
hxxp://195[.]123[.]245[.]185/04m	
hxxp://54[.]38[.]127[.]28/02[.]dat	

Domain/URL	Notes
hxxp://54[.]38[.]127[.]28/pm4	Malicious Download URL
hxxp://95[.]216[.]189[.]14/02[.]dat	
hxxp://95[.]216[.]189[.]14/m4	
hxxp://95[.]216[.]189[.]14/w3	
hxxp://95[.]216[.]189[.]14/w4	
hxxp://aureliostefaniniarte[.]com/11-Jun-2019_a437f673[.]xls	
hxxp://bascif[.]com/tt1	
hxxp://bascif[.]com/tt2	
hxxp://carpc[.]si/OZ00488941[.]xls	
hxxp://cdpet[.]org/20190614864789048[.]xls	
hxxp://cjsebbelov[.]dk/11-Jun-2019_b901fe43c[.]xls	
hxxp://counciloflight[.]bravepages[.]com/conto-134[.]xls	
hxxp://e-commerce-shop[.]com/11-Jun-2019_412ac541[.]xls	
hxxp://engast[.]top/rt1	
hxxp://engast[.]top/rt2	
hxxp://jbswin[.]net/rt3	
hxxp://jbswin[.]net/rt4	
hxxp://kosmetolodzy[.]com/11-Jun-2019_f963a2afe3[.]xls	
hxxp://kramerleonard[.]com/OZ74509374[.]doc	
hxxp://lancehugginsltd[.]co[.]uk/Attestation_impots[.]xls	
hxxp://lidovemilice[.]unas[.]cz/Payment-503_Copy[.]xls	
hxxp://luchies[.]com/11-Jun-2019_e762a23d[.]xls	
hxxp://makosoft[.]hu:80/out_1[.]exe	
hxxp://nanepashemet[.]com/20[.]06[.]2019_781[.]37[.]xls	
hxxp://nivans[.]pro/Attestation_impots[.]xls	
hxxp://ogallar[.]com/~inaki/I1806201980891123[.]doc	
hxxp://operasanpiox[.]bravepages[.]com/20190614890563891[.]xls	

Domain/URL	Notes
hxxp://pack301[.]bravepages[.]com/Payment-892_Copy[.]xls	Malicious Download URL
hxxp://sscvl[.]fcpages[.]com/I1806201990010667[.]doc	
hxxp://staler[.]se/I1806201911266473[.]doc	
hxxp://trictac[.]com/I1806201989006781[.]doc	
hxxp://ulda[.]com/I1806201972395014[.]xls	
hxxp://www[.]versiliaradi[.]it/conto-043[.]xls	
iluj[.]in/20[.]06[.]2019_013[.]93[.]xls	
nagomi-753[.]jp/20[.]06[.]2019_784[.]09[.]doc	
nagomi-753[.]jp/20[.]06[.]2019_800[.]77[.]doc	
nanepashemet[.]com/20[.]06[.]2019_781[.]37[.]xls	
orderlynet[.]net/r5[.]exe	
runpen[.]dothome[.]co[.]kr/20[.]06[.]2019_673[.]81[.]doc	
runpen[.]dothome[.]co[.]kr/20[.]06[.]2019_701[.]82[.]doc	
workingsolutionsrome[.]org/~terryh/20[.]06[.]2019_430[.]22[.]xls	
hxxp://engast[.]top/rt2	Malicious Excel 4.0
hxxp://jbswin[.]net/rt4	
hxxp://179[.]43[.]147[.]77/p2	Malicious Excel VBA Macro
hxxp://179[.]43[.]147[.]77/pm1	
hxxp://179[.]43[.]147[.]77/pm1	
hxxp://179[.]43[.]147[.]77/pm2	
hxxp://179[.]43[.]147[.]77/pm2	
hxxp://ogallar[.]com/~inaki/I1806201980891123[.]doc	Malicious HTML
hxxp://sscvl[.]fcpages[.]com/I1806201990010667[.]doc	
hxxp://staler[.]se/I1806201911266473[.]doc	
hxxp://trictac[.]com/I1806201989006781[.]doc	
hxxp://bigpresense[.]top:80/es/es[.]php	C&C Server

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