Uncovering the Inner Workings of EyePyramid

Appendix

TrendLabs Security Intelligence Blog
Forward-Looking Threat Research (FTR) Team

January 2017

Evolution of EyePyramid

The following table lists the various properties of EyePyramid-related samples over years.

Year	# of Samples	C&C/Dropzone Related Strings	Notable Email Addresses	Notable MailBee Keys	Sample Hashes	gmail.it	Env. Info	Eye Pyramid	Spy Works	File Name	Compiler	Protection
2010	1	hxxp://guess515.fastmail.fm/files/config/ hxxp://guess515.fastmail.fm/files/config hxxp://guess515.fastmail.fm/files/bin/ hxxp://guess515.fastmail.fm/files/bin/ghk hxxp://guess515.fastmail.fm/files/obj/decepk hxxp://guess515.fastmail.fm/files/bin/run hxxp://guess515.fastmail.fm/files/replace/ hxxp://guess515.fastmail.fm/files/jobs hxxp://guess515.fastmail.fm/files/replace hxxp://guess515.fastmail.fm/files/fail hxxp://guess515.fastmail.fm/files/obj hxxp://guess515.fastmail.fm/files/obj/tasks hxxp://guess515.fastmail.fm/files/bin	tip848[@]gmail.com **deliver[@]hostpenta.com.xml** **archive[@]hostpenta.com.xml** tim11235[@]gmail.com guess515[@]fastmail.fm dude626[@]gmail.com octo424[@]gmail.com plars575[@]gmail.com purge626[@]gmail.com	MN600-D8102F401003102110C5114F1F18-0E8C	3a451f1e2f64b7f4fe3c4f48366014142e22093a16b15601e0f98bc27364bd57			\Work\EyePyramid*		run.exe	2	Skater/ Dotfuscator

Year	# of Samples	C&C/Dropzone Related Strings	Notable Email Addresses	Notable MailBee Keys	Sample Hashes	gmail.it	Env. Info	Eye Pyramid	Spy Works	File Name	Compiler	Protection
2010	2	hxxp://guess515.fastmail.fm/files/jobs/44dc7eceb2719abfaac5b2c684d05c35 hxxp://guess515.fastmail.fm/files/jobs/3261cc389d6ef8f0a8c6a6212829effd hxxp://guess515.fastmail.fm/files/ghk hxxp://guess515.fastmail.fm/files/configuration/ hxxp://guess515.fastmail.fm/files/tasks hxxp://guess515.fastmail.fm/files/decepk hxxp://guess515.fastmail.fm/files/replace/ hxxp://guess515.fastmail.fm/files/replace hxxp://guess515.fastmail.fm/files/jobs hxxp://guess515.fastmail.fm/files/run	purge626[@]googlemail.com tip848[@]gmail.com tim11235[@]gmail.com guess515[@]fastmail.fm tim11235[@]googlemail.com purge626[@]gmail.com octo424[@]gmail.com plars575[@]gmail.com dude626[@]gmail.com	MN600-D8102F40100310211 0C5114F1F18-0E8C	47a157ea41f9b93c956f0d8a78060dc044ed415c7bb0f1d8b337428660f60767cf159475586e5ff2aa699ede860b9fc2b906158562437873990 7d26d1f916d30					run.exe	2	Skater/ Dotfuscator
2012	1	ftp[:]//ftp1.storegate.com/home/jiwoku375 hxxps://webdav1.storegate.com/jiwoku375/home/jiwoku375 hxxp://webdav1.storegate.com/jiwoku375/home/jiwoku375 ftp1[.]storegate.com/home/jiwoku375		MN600-D8102F40100310211 0C5114F1F18-0E8C	4be22645fa65d7dbb173a51ce9ed6509c600c61df8ed4a131d66d9745a707510					run.exe	2	Skater/ Dotfuscator
2012	2	ftp[:]//ftp1.storegate.com/home/jiwoku375 hxxps://webdav1.storegate.com/jiwoku375/home/jiwoku375 hxxp://webdav1.storegate.com/jiwoku375/home/jiwoku375 ftp1.storegate.com/home/jiwoku375		MN600-D8102F40100310211 0C5114F1F18-0E8C	3dcb22f5428d2161167663ccf13ab0ada0066d05401789daffe64c0cb1398a500ed387453442d53d65a5b402243fb8f50ae7605196d1bc90595ed0e9c6143f5d				Spy Works	ghk.exe	2	Skater/ Dotfuscator
2013	1	ftp[:]//ftp1.storegate.com/home/jiwoku375 hxxps://webdav1.storegate.com/jiwoku375/home/jiwoku375 hxxp://webdav1.storegate.com/jiwoku375/home/jiwoku375 ftp1.storegate.com/home/jiwoku375		MN600-D8102F40100310211 0C5114F1F18-0E8C	e17c71a427cf5c9026aac00c6631ba4438da5f3b52e96655193ededd4ffd00ee					ghk.exe	3.5	Skater/ Dotfuscator

Year	# of Samples	C&C/Dropzone Related Strings	Notable Email Addresses	Notable MailBee Keys	Sample Hashes	gmail.it	Env. Info	Eye Pyramid	Spy Works	File Name	Compiler	Protection
2013	2	ftp[:]//ftp1.storegate.com/home/jiwoku375 hxxps://webdav1.storegate.com/jiwoku375/home/jiwoku375 hxxp://webdav1.storegate.com/jiwoku375/home/jiwoku375 ftp1.storegate.com/home/jiwoku375		MN600-D8102F401003102110C5114F1F18-0E8C	6085e8b4ee1b2977a4513d202ec04dea0ac378fbe8bf914f81e50f85be03fd5676c1519243dbd5d56a59cffcc5f95bdaf5c561759388d8a1395c04c527f8b092	Binary and Source				ghk.exe	3.5	Skater/ Dotfuscator
2014	5	hxxps://webdav.hidrive.strato.com/users/oncole3991 hxxp://webdav.hidrive.strato.com/users/oncole3991	almeria.recupero[@]gmail.com mariangelatreglia[@]libero.it avv.angelonimilano[@]tiscali.it cadiz.recupero[@]gmail.com	MN600-D8102F401003102110C5114F1F18-0E8C	7fcae3924409ec5b6338d2eb71dd4644d124b72ffd6995c9252dd477e0041c912a8a15b41d0713db9ddc5ad895cb9a08023d42057d98e0dcd96cfbee80146d8e	Source				ghk.exe	4.5	Skater/ Dotfuscator
2014	2	hxxps://webdav.hidrive.strato.com/users/oncole3991 hxxp://webdav.hidrive.strato.com/users/oncole3991	almeria.recupero[@]gmail.com mariangelatreglia[@]libero.it avv.angelonimilano[@]tiscali.it cadiz.recupero[@]gmail.com	MN600-D8102F401003102110C5114F1F18-0E8C	0af665d7d81871474039f08d96ba067d5a0bd5a95088009ea7344d23a27ca824871e65e7b80b32501b9890a7044dcc64fb1b0936a17d0fa0d50bb10b2550d3dd	Source				stkr.exe	4.5	Skater/ Dotfuscator
2014	1	ftp[:]//ftp1.storegate.com/home/jiwoku375 hxxps://webdav1.storegate.com/jiwoku375/home/jiwoku375 hxxp://webdav1.storegate.com/jiwoku375/home/jiwoku375 ftp1.storegate.com/home/jiwoku375		MN600-D8102F401003102110C5114F1F18-0E8C	31ef142400853070edc4261e0b35875fd6e294fd30e56ee1040bca233e3e7234	Binary and Source				run.exe	3.5	Skater/ Dotfuscator
2014	1	hxxps://webdav.hidrive.strato.com/users/oncole3991 hxxp://webdav.hidrive.strato.com/users/oncole3991	almeria.recupero[@]gmail.com mariangelatreglia[@]libero.it avv.angelonimilano[@]tiscali.it cadiz.recupero[@]gmail.com	MN600-D8102F401003102110C5114F1F18-0E8C	e2d5512fe82b6e4b6bfdeb93f49adbdcc719e833a3e7e56d95f98022e12615f9	Source	:\projects\vs2005*			vmgr.exe	4.5	Skater/ Dotfuscator

Year	# of Samples	C&C/Dropzone Related Strings	Notable Email Addresses	Notable MailBee Keys	Sample Hashes	gmail.it	Env. Info	Eye Pyramid	Spy Works	File Name	Compiler	Protection
2014	1	hxxps://webdav.hidrive.strato.com/users/oncole3991 hxxp://webdav.hidrive.strato.com/users/oncole3991 hxxp://webdav1.storegate.com/enzevu888/home/enzevu888 hxxps://webdav1.storegate.com/enzevu888/home/enzevu888		MN600-D8102F401003102110C5114F1F18-0E8C	580cf6d6f5ea248f968806605f57e440014661351593b3cf3d4dc5369a594472	Binary and Source				Carrier.exe	3.5	Skater/ Dotfuscator
2014	148	hxxps://webdav.hidrive.strato.com/users/oncole3991 hxxp://webdav.hidrive.strato.com/users/oncole3991 hxxp://webdav.cloudme.com/imin1399/xios hxxps://webdav.cloudme.com/imin1399/xios	almeria.recupero[@]gmail.com mariangelatreglia[@]libero.it avv.angelonimilano[@]tiscali.it cadiz.recupero[@]gmail.com	MN600-D8102F401003102110C5114F1F18-0E8C	6a624e266f9656f3bb684b88bf027ac2d229aac98e26accbe4bd415306fa7482e71783d9f572c2d11772a48c174b05a1871a684f6ca153e28ff67483fb3ce344	Source				crrr.exe	4.5	Skater/ Dotfuscator

Year	# of Samples	C&C/Dropzone Related Strings	Notable Email Addresses	Notable MailBee Keys	Sample Hashes	gmail.it	Env. Info	Eye Pyramid	Spy Works	File Name	Compiler	Protection
2014	12	hxxps://webdav.hidrive.strato.com/users/oncole3991 hxxp://webdav.cloudme.com/imin1399/xios hxxp://webdav1.storegate.com/oldi4006/home/oldi4006 hxxps://webdav1.storegate.com/oldi4006/home/oldi4006 hxxp://webdav1.storegate.com/uwiq175/home/uwiq175 hxxps://webdav1.storegate.com/enzevu888/home/enzevu888 hxxps://webdav1.storegate.com/ordu1337/home/ordu1337 hxxp://webdav1.storegate.com/oqokul68646/home/oqokul68646 hxxp://webdav1.storegate.com/enzevu888/home/enzevu888 hxxps://webdav.cloudme.com/imin1399/xios hxxps://webdav1.storegate.com/uwiq175/home/uwiq175 hxxp://webdav.hidrive.strato.com/users/oncole3991 hxxp://webdav1.storegate.com/ordu1337/home/ordu1337 hxxps://webdav1.storegate.com/oqokul68646/home/oqokul68646	almeria.recupero[@]gmail.com mariangelatreglia[@]libero.it cadiz.recupero[@]gmail.com	MN600-D8102F401003102110C5114F1F18-0E8C	faeb185c0d2048fce0597b899047d4c222d31c5f94ea94d19dcfe788e5dd3da8906624aec0b63d5a6f1c8f0fa4386af02365508cbe9c12498ee60432984bdc9c	Source				crrr.exe	3.5	Skater/ Dotfuscator
2014	1	hxxps://webdav.hidrive.strato.com/users/oncole3991 hxxp://webdav.hidrive.strato.com/users/oncole3991	almeria.recupero[@]gmail.com mariangelatreglia[@]libero.it avv.angelonimilano[@]tiscali.it cadiz.recupero[@]gmail.com	MN600-D8102F401003102110C5114F1F18-0E8C	137846f698de9b30fe0fb81af20f175f36cf7c6297e3f920996e607cf80f518a	Source		\Work\EyePyramid*		mfkr.exe	4.5	Skater/ Dotfuscator

Year	# of Samples	C&C/Dropzone Related Strings	Notable Email Addresses	Notable MailBee Keys	Sample Hashes	gmail.it	Env. Info	Eye Pyramid	Spy Works	File Name	Compiler	Protection
2014	2	hxxps://webdav.hidrive.strato.com/users/oncole3991 hxxp://webdav.hidrive.strato.com/users/oncole3991 hxxp://webdav1.storegate.com/enzevu888/home/enzevu888 hxxps://webdav1.storegate.com/enzevu888/home/enzevu888		MN600-D8102F401003102110C5114F1F18-0E8C	55c9a611103f43070ba186fe70d0253ec1ff21f644d8ae92f9b02b4a1f4c0ea1f9bf0244a99437213bbb8dd3ff1ca2995a519e9fccf1409566460becc9062e2d	Binary and Source				crrr.exe	3.5	Skater/ Dotfuscator
2014	12	hxxps://webdav.hidrive.strato.com/users/oncole3991 hxxp://webdav.hidrive.strato.com/users/oncole3991	almeria.recupero[@]gmail.com mariangelatreglia[@]libero.it avv.angelonimilano[@]tiscali.it cadiz.recupero[@]gmail.com	MN600-D8102F401003102110C5114F1F18-0E8C	9c3d491033f8c9452e70bb37caaa9c49573515e2e5cf7af5615fd78ec90cfce80970e403b26e10159639532190a4125f4ddc4e4575d7b98e9be98a7037ff8ebb	Source				run.exe	4.5	Skater/ Dotfuscator
2015	2	hxxps://webdav.hidrive.strato.com/users/oncole3991 hxxp://webdav.hidrive.strato.com/users/oncole3991	almeria.recupero[@]gmail.com mariangelatreglia[@]libero.it avv.angelonimilano[@]tiscali.it cadiz.recupero[@]gmail.com	MN600-D8102F401003102110C5114F1F18-0E8C	51a96dad0bba7a89431afe04e7eb73b7e6186dc28ae2cfc125989785c859e9e2a0c25021e04b95cc4af1e001109ef559834c4a343b085d2ebb16d0a495179f70	Source				run.exe	4.5	Skater/ Dotfuscator
2015	1	hxxps://webdav.hidrive.strato.com/users/oncole3991 hxxp://webdav.hidrive.strato.com/users/oncole3991	rinomorbegno[@]tiscali.it almeria.recupero[@]gmail.com mariangelatreglia[@]libero.it cadiz.recupero[@]gmail.com antonio_francione[@]alice.it	MN600-D8102F401003102110C5114F1F18-0E8C	590f43c66ec69b9534c893acbb2fce7f1780fe5ac0e7fca7462db1600ad91f38	Source	:\projects\vs2005*			vmgr.exe	4.5	Skater/ Dotfuscator

Year	# of Samples	C&C/Dropzone Related Strings	Notable Email Addresses	Notable MailBee Keys	Sample Hashes	gmail.it	Env. Info	Eye Pyramid	Spy Works	File Name	Compiler	Protection
2015	24				383dd234d22ead747319a04847d789bcedeacd0137a51ff394bab10256ab4b8e 93c19d6e744053f4b337c9026e09c13e8d1019d535fdc21c2b1a21937e5aa76f					crrr.exe	4.5	/ConfuserEx *1
2015	15	hxxps://webdav.hidrive.strato.com/users/oncole3991 hxxp://webdav.hidrive.strato.com/users/oncole3991	antonio_francione[@]alice.it mariangelatreglia[@]libero.it almeria.recupero[@]gmail.com cadiz.recupero[@]gmail.com rinomorbegno[@]tiscali.it avv.angelonimilano[@]tiscali.it	MN600-D8102F401003102110C5114F1F18-0E8C	d910283342c7be67b03a01cac2aae5d310ac6e6d9d3572df324eb2afe0127f2fb0a718f2322a8eb15633f8d0cd72f653aab5921e3a581bf8cb8222bdd4dbb7bb	Source				crrr.exe	4.5	Skater/ Dotfuscator
2015	2	hxxps://webdav.hidrive.strato.com/users/oncole3991 hxxp://webdav.hidrive.strato.com/users/oncole3991	antonio_francione[@]alice.it mariangelatreglia[@]libero.it almeria.recupero[@]gmail.com cadiz.recupero[@]gmail.com rinomorbegno[@]tiscali.it avv.angelonimilano[@]tiscali.it	MN600-D8102F401003102110C5114F1F18-0E8C	d874fe7cd08aff55655a3e35f96c895a3cf84bfa92f482eb7d404f8feb4de130d4439954ff2a158a861946e1a223e97a46b0b55669857dcfdf5cc70e459d24cd	Source				stkr.exe	4.5	Skater/ Dotfuscator

Year	# of Samples	C&C/Dropzone Related Strings	Notable Email Addresses	Notable MailBee Keys	Sample Hashes	gmail.it	Env. Info	Eye Pyramid	Spy Works	File Name	Compiler	Protection
2015	3	hxxps://webdav.hidrive.strato.com/users/oncole3991 hxxp://webdav.hidrive.strato.com/users/oncole3991	antonio_francione[@]alice.it mariangelatreglia[@]libero.it almeria.recupero[@]gmail.com cadiz.recupero[@]gmail.com rinomorbegno[@]tiscali.it avv.angelonimilano[@]tiscali.it	MN600-D8102F401003102110C5114F1F18-0E8C	b860b98eed4f2214cfd95375caa82e1c5d1e438086220d2f08d1f86fd21a54da1012f0717543409a3dfa4418bfdcde31ecc55ef7c673a13f5dbcd131c4a0db22	Source				ghk.exe	4.5	Skater/ Dotfuscator
2016	7				6f1d9aca5cd32bc70056289854ba5afa9a5698e807bc9575f162a4d964c88504d728caa5901e8893b5ba97ef8ad58a73fec98ab9f2c93b3f3a0bc31a20eabdbd					crrr.exe	4.5	/ConfuserEx ***1**

**1: Please note that the samples packed with ConfuserEx are still being verified.*

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.

Securing Your Journey to the Cloud

10101 N. De Anza Blvd.
Cupertino, CA 95014

U.S. toll free: 1 +800.228.5651
Phone: 1 +408.257.1500
Fax: 1 +408.257.2003