

# Mac Malware MacStealer Spreads as Fake P2E Apps

Indicators of Compromise (IOCs)

## Indicators of Compromise (IoCs)

### Command and control (C&C) servers

- [http\[://\]185\[.\]241\[.\]208\[.\]138:3000](http://185[.]241[.]208[.]138:3000)
- [mac\[.\]cracked23\[.\]site](http://mac[.]cracked23[.]site)
- [cracked23\[.\]site](http://cracked23[.]site)
- [worldofcreatures\[.\]io](http://worldofcreatures[.]io)
  - [https\[://\]play-impulseflow\[.\]com/impulse.dmg](https://play-impulseflow[.]com/impulse.dmg)
  - [https\[://\]www.dropbox\[.\]com/s/dl/43yd3of7dml3iri/Pure%20Land%20Launcher.dmg](https://www.dropbox[.]com/s/dl/43yd3of7dml3iri/Pure%20Land%20Launcher.dmg)
  - [https\[://\]worldofcreatures\[.\]io/download/LauncherMacOs.dmg](https://worldofcreatures[.]io/download/LauncherMacOs.dmg)

.dmg files SHA256	First stage Mach-O (loader) SHA256	Second stage Mach-O (payload) SHA256	Filename	Detections	Additional notes
02e1d9ea3a0c16106d173b0e6349a18a9aea facc38650e359cfe1ee 2298aaa45	5a584c1f13272755fb c379c21235d07e6a5 9b2b59fd90f5e945b b856117a2e75	7eed5a8f486aaba39 48307f165a636df83 857ab6cea21b8fd5e 0ff758bb134b3	Impulse. dmg	TrojanSpy.MacOS .CypypwdStealer.A	hxxps[://]play- impulseflow[.]com/im pulse.dmg
263c27deb22b61bef2 b79603c4753ef307ac d1f056dbc34b7bad32 07bafd1059	3c575ed9183ffc9d64 a8d5c7a098dff3c464 c5a45298e43788bcd 5287bf69cab	821ecdae151ed78e b4792d40a7787127 927900a763f3249b3 1f37d7b67b5e1e5	PearlLan dLaunche r.dmg	TrojanSpy.MacOS .CypypwdStealer.A	
2c4cb2b85fb27bf17a 198e8b6c8f3861754f 63db345103f9747086 8ef9884939	3e1ce689e6cf5c6d3e 0a5dc7957f8815e22 8950a23442c847e19 db4fc4f80a93	acef9f3f215335462e 2e2e4bacbe6c52e48 e764e7174fe46966e 29902f6a1890	anaxyn- arm.dmg	TrojanSpy.MacOS .CypypwdStealer.A	
35c9ac8792c5e38b3e 6de1374db56558233 35cb2037a95632bbe8 839d27fc236			Launcher MacOs.d mg	TrojanSpy.MacOS .CypypwdStealer.A	damaged
3e6bf7cfff924a541fdd 3179f6008205dd9b8b 0846fc39d4ae8898ce d1946e33	b0fe18e3b6f9904088 8f35ed278a739712af 23c3f7e7d3573ab41 5557d1de3c4	e51416f12f8c60e75 93bef8b9fc55e0499 0aa047ad7e8abc22 b511e7eb7586f6	RyzexLau ncher.dm g	TrojanSpy.MacOS .CypypwdStealer.A	
41c9d96073a3e90a1d 68d8ce025427329f55 b79a03c6c0564812a5 aca8915fff	ae8bf7cc0d3cf89f63 5884f1cf1c30f26a00 ed523f20e45da6406 e843dfbe349	d61666b49ef700cbd 59c744bf5fca2e850 be55a52f415102cf3 ea1c1c2db18d4	Mysteria nLaunche r.dmg	TrojanSpy.MacOS .CypypwdStealer.A	
5031aa79912fb23bcb e2209e015974fccb4b 9e9334a9e8801833f0 7bd3a5ccfc	865bd36460cb65342 30b2f5e625318b945 1f267b1ade46ea7ba 247c93fd12da8	f14dd83e60b8ca6d5 2e667ed85adafa9b8 49df33e428b005b05 b7c6732de526a	Pure Land Launcher. dmg	TrojanSpy.MacOS .CypypwdStealer.A	hxxps://www.dropb ox[.]com/s/dl/43yd3of 7dml3iri/Pure%20Lan d%20Launcher.dmg
5a58cba07000edc516 6c33629f70ceedcc722 939dc21142dcccc71b 2baaceaf2	32249354e01525161 8707a9c79cba60d55 d46cd3fad4dc91005 791414862df06	61f3cd0a7c8191745 080aa7b2e0695c3a5 7327f1f226d9fc7a4b e3cee14a2375	official agreemen t with the galleryCR EATIVA20 23 .dmg	TrojanSpy.MacOS .CypypwdStealer.A	

6bef4ec59e2d0e5b55 1361dba3027d05c66 9176255bce9eb7d74c 920983dc55f	ed8ff35a869325b1af 568852155bb2d6722 1cbdb7baa69e5d3 682c3963ebe5	2abc380ad22c47db 0035df1f0e6e00a7fa bcb5d4afd913e2474 478ea11ea6a63	SecretCas ino.dmg	TrojanSpy.MacOS .CypypwdStealer.A	
7bb7b51494c60401c8 535baaa30cddb1c41c 436e778092f30db526 0c42cc70f6	8b33a47dde03b45f4 922bac240d167646c 4370acfe75c3e2d9d 9dccc80fded35	b517455fb54f757cfb 6ba3bf7f1da1eb018 2c42c2d8958ba6c4f 76bf73a7594b	toncap.d mg	TrojanSpy.MacOS .CypypwdStealer.A	
8863f14b7e3fd4d129 af2e5851e815b31a31 17380c5c018803ed85 67dae8f41b	81e6421e9a579bf90 78c2e6c36aa4a89fae a37b0eeda96f37034 4dd6070e1803	977cf1a74467e72b7 fd9434bebd9e171a4 5b520ade960771b3 1f3bd5e9e4a5aa	Mysteria nLaunche r.dmg	TrojanSpy.MacOS .CypypwdStealer.A	
8a3c482f4548ce600e 031983e5477941cc64 20b4617d17169bdba 82651e191db	225789b60987a54c7 c57089ce47af664de9 50c66ce8c7fdc89d8b 7ed3aac8d87	1b0684ab02071f8b b03967866596efcea 92a48e49f8b1013a6 301653f7687e74	rinom.d mg	TrojanSpy.MacOS .CypypwdStealer.A	
8ea33c34647578b79d d8bb7dcf01a8ad1c79 e7ada3fd61aca397ed 0a2ac57276	5e8f37420efb738a82 0e70b55a6b6a66922 2f03e4a8a408a7d43 06b3257e12ff	15d1afca780e2ea6ff ec8c4862a3401e003 b5e79ce5f9076b4ee a4ab599bc4ce	Launcher MacOs.d mg	TrojanSpy.MacOS .CypypwdStealer.A	hxxps[:]//worldofcrea tures[.]io/download/L auncherMacOs.dmg
9506831d18b895d63 58ef54f2d41002ca2b 3fbbf2841b28c49bbc a5b14933d32	cc3c44e8ce241f42cc 1b5e387eecd3b0943 959361fbf32af4dc33 45c087e775d	a270150d23ded2c8f de6124ce5fd605369 13fc84259922ddb74 0b9a67fb89041	adobepat ch2023.d mg	TrojanSpy.MacOS .CypypwdStealer.A	
a4ccd8283e2b8c9087 fd8c820f75e6d5201f9 8ebff7fb0a51130947b 03a3a8bf	edd0b28ef28bc3898 4aa01dca253be58f7 e266754640ad41962 d7d7c990b87cc	df71b5c99052b63de 167f9c22b3cf6ded5 13ed6d1e1c74eff7af 8cf9e4692714	Magical World Launcher BETA.dmg ALMV.dm g Installer.d mg	TrojanSpy.MacOS .CypypwdStealer.A	
c4cb0af59293c2baec7 1612af0561addbba80 7ddec474315e1c04c1 bf5b3b14a	d9b0e0f85f4f2e68f4 6af23d369b877db04 dfb21ca53a4694109 87afdaf68b29	e01eec798a326a1e0 beb767cdd0f185e19 361871de82e23568 042e9fc6128bb6	(MacOS) CONCEPT A3 full menu with dishes and translatio ns to English.d mg mutant playersclu b brief.dmg	TrojanSpy.MacOS .CypypwdStealer.A	
f79850569cac857d0df 033d03ff4433400713 e1600b569cbe1a5d6f 0d0c279db	a79929aeeccb05548 ba7a15a1b60b64e95 f448a6222e0741a62 2181b78c2f100	1153fca0b395b3f21 9a6ec7ecfc33f522e7 b8fc6676ecb1e40d1 827f43ad22be	toncap.d mg	TrojanSpy.MacOS .CypypwdStealer.A	

Table 1. MacStealer's (original sample) indicators of compromise



Trend Micro, a global cybersecurity leader, helps make the world safe for exchanging digital information. Fueled by decades of security expertise, global threat research, and continuous innovation, our unified cybersecurity platform protects hundreds of thousands of organizations and millions of individuals across clouds, networks, devices, and endpoints.

With 7,000 employees across 56 countries, and the world's most advanced global threat research and intelligence, Trend Micro enables organizations to simplify and secure their connected world.

[TrendMicro.com](https://www.trendmicro.com)