

# Fake Bank App Phishes Credentials, Locks Users Out

Appendix

**TrendLabs Security Intelligence Blog**

**May 2016**

#### TREND MICRO LEGAL DISCLAIMER

The information provided herein is for general information and educational purposes only. It is not intended and should not be construed to constitute legal advice. The information contained herein may not be applicable to all situations and may not reflect the most current situation. Nothing contained herein should be relied on or acted upon without the benefit of legal advice based on the particular facts and circumstances presented and nothing herein should be construed otherwise. Trend Micro reserves the right to modify the contents of this document at any time without prior notice.

Translations of any material into other languages are intended solely as a convenience. Translation accuracy is not guaranteed nor implied. If any questions arise related to the accuracy of a translation, please refer to the original language official version of the document. Any discrepancies or differences created in the translation are not binding and have no legal effect for compliance or enforcement purposes.

Although Trend Micro uses reasonable efforts to include accurate and up-to-date information herein, Trend Micro makes no warranties or representations of any kind as to its accuracy, currency, or completeness. You agree that access to and use of and reliance on this document and the content thereof is at your own risk. Trend Micro disclaims all warranties of any kind, express or implied. Neither Trend Micro nor any party involved in creating, producing, or delivering this document shall be liable for any consequence, loss, or damage, including direct, indirect, special, consequential, loss of business profits, or special damages, whatsoever arising out of access to, use of, or inability to use, or in connection with the use of this document, or any errors or omissions in the content thereof. Use of this information constitutes acceptance for use in an "as is" condition.

## File hash (SHA1):

Detection	SHA1
ANDROIDOS_FANTA.AXB	Fanta v.1.0 (First emerged on December 11, 2015)
	0ef7bc8f6ab7264e70ecd3b04486d3d34bde2532
	Fanta v.1.1 (First emerged on January 03, 2016)
	ff844a8bb40da72b5c9f3a8c3cda7c9d051921e6
	83e56809b1662be002f4e1c4bcd3aef90d060d8f
	7c3f693d0b0ea6c6fdbb078e56d7e71ffaf648b8
	9e36414341e4dbaa113980f7d900e0ac4baa4103
	21266e72c8becbb439cb6d77f174b5eccefa2769
	f53332b0f1b01d0dd282346c4e69da964edd137d
	9887af7e945ef3491880ae66fb6b07a2796a6ce2
	714f062e798dca9a136b9a7c408846be90b3cb45
	7f870ea901428317013e65053d55535ee5e2e047
	ad6154bec63f5fae6f948aa6697cd087b4b1f60c
	eb655deda3a33d829a4dd617358c10d029a4b0f0
	4728cdc4d652f6e7682d660cb72e21479e9183a2
	Fanta v.2.1 (First emerged on February 04, 2016)
	3065ebd6658a50262869277ff29b03dd621ca1c6
	45293e19012648ebb25d84ad259c097f6dad7c5c
	8b9af9362e0f8e789aecf0f906642239941e4055
	5359d2f33fb072609d589b054fbe9bf0ba14fbfd
	23549741658e6b1d52654691f974b01e7eca5f24

Detection	SHA1
	Fanta v.2.2 (First emerged on March 23, 2016)
	a2895b80515fbc7c1b9eea3d39a214fc777bdbb2
	052db48b8d0a1f67198263c712141477cdc09d79
	7636c2e2892eb4996245c163b728ca867171a75f
	c5898a64afd1a2e21b0898ac8df68b996ac200cf
	c2fbf01ed6e8b348a831fda0f7c3509b29a2fee8
	4d258a710bab46600dcd56aeb3080cc86c90c03b
	a339ed5597b09745503a4b716e408789ef9f8338
	14ee027b4df5c4031f6b78b3baa5602aaeb34e5f
	f3c1fd573943c0481991a1aeeddf74fda84490c5
	6c2fb05fa6d7083fbb5587c226c37e05466f9573
	7be86ac234a1dce5063f45bca341337c3cadc450
	1cbb0919441ae19b3b9fccd6d31e737036f74f90
	1600e2773a9bfa80478facc3107f75e115ff8876
	d46d478ee483d481806ffdd7122e2de9ac8467de
	e625902b39dfa649f0cd732e9680226b2113ab6
	ad65e9f83739d3f79976d634ac9532ebc9957629
	e6fe44b2f20aff67eadecfaa85ef729834b3fb13
	afd36fc8ed8a432a44695d29faba440558a3af24
	50c62996453422c438dc1282e646f30233ce6e6e
	9f931499765e85954d468fb63072a29a7e193ff7
	d770bae185476523649a5768b7bbe7f7605656ab

Detection	SHA1
	de585c41b3236ed3bf29298a0732876a947be47f
	ca5680a4ee9d0b6847fe20f297a98d3539fdaf2b
	017730f4cc127d98678ae814f19017e8db0562fe
	312c111d3e6cddfa7f8f782525d792de0776ec72
	1d5774c06e483e1ba4160d63334385178ae42162
	514152082315816e91049b3da6f95ea376555445
	c5d00409f39082ae782fcdeb127f28d172556efa
	ed73b2fe3f5f726f029961434a8c599a91011564
	17561eb2a0e07b5f5361994e952ea4b79cc90c4f
	c3c3d3f3636005cc2d4e2d258baf9c1ef63f23a4
	c971e8425a2f3616222ab1af552e4ab45fc8ab99
	ea9a4b41c7a93238ae5c0f3d46fd22acca2818ea
	2c77aab581983c33eefa65d867f03e54d3105611
	0a2c68c40453625eb2676023b97894e621c4af23
	f36dd6a0858dfbefd860a81eb76a07e7bf01a6f6
	93bb6b7934080541985a7bdf0efe34136c1650d3
	f3f8bd1f7edcee5c60b303eabd1b9591b7264c07
	31eba30c1b7120eaa23ba23f7dce3bf5f41d5f4a
	5b135f6d815c8c089860f04ed335c143a41dc1f3
	Fanta v.2.3 (First emerged on April 13, 2016)
	ef15f1705b83c575cc8aa716d4695c073c23b5cf
	6fd9c0c65ee41b2e46a246af0dd93b72460c0089

Detection	SHA1
	5dd722c5fce53c8c26adf522641e5facfe976bc7
	91b59ab5bfa7366a6eada67103d9598ccf1cfdc5
	571b5082341e75d908fbe5c7a8db6dff8a67e650
	a1587f10849162156591be75e705d586aa8ec74d
	2ea844e8cfed19d76e114e4d43bea70671b7d413
	12d57ed44d4de42fbb06be091d964d9af5c5e8e3
	00f74e3435e2845667ae05be94c4bfb5f3a3f31e
	9fd0480fa11fe7760311f6775d4dcaa6b94ba792
	30dfc598d7c3e60d12695f5827f6507f6c1feeaa
	20eaa48d86129febdfee80b0cccd484fe589a2bf
	410c995ebd564a1010ed12108f53cbb2a495d7b4
	388c84df0a057321f5bd6dfa9a8f66e6f95d2779
	856823203a29b767d473bd6c850ed0296cc41a52
	c74f2aef00c80cabee05631886705ccdaeb935de
	e8f84ad2731e303659f9864323fd814412033bc1
	a08a1e3ab778c5a83f017fdc22db181ee1c906e9
	d1c5f6889a09cb05bfec4045a50d73f5f5fe7783
	d553185a2f581e4b71ad80924f4d2e2d7d19bb97
	dcabc0dd585bb4d918ab6b7b062d50c222e94709
Ransom_CRYPTICH.EN	78fcacf076eb0540ab0079e3b04bc515643ed10e
VBS_RAMNIT.SMC	f49cc6dae2576c2a5eab3034c644d1c396e8a90d
WORM_CRIDEX.NU	de06a520ddfbeb972c29dac995422c7e91b00424

<b>Detection</b>	<b>SHA1</b>
VBS_ZBOT.YUYAPA	7524e300c17e8b96aca6ec09c345424fc4aedce4
HTML_MALPHISH.VVVM	b8ff0570024fe488252d917732be75431c1d76ff
	c27055b9b75569205a1cafae8762acd2f05da712

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](http://www.trendmicro.com).

©2016 by Trend Micro, Incorporated. All rights reserved. Trend Micro and the Trend Micro t-ball logo are trademarks or registered trademarks of Trend Micro, Incorporated. All other product or company names may be trademarks or registered trademarks of their owners.



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