Operation Emmental Revisited: Malicious Apps Lock Users Out

Appendix

TrendLabs Security Intelligence Blog

Richard Tai
January 2016

Related URLs:

- hxxp://www.pergotools[.]com/gfx/main.php
- hxxp://www.inetz[.]at/temp//main.php
- hxxp://www.inetz[.]at/man.php
- hxxp://www.itgs.biz/man.php
- hxxp://www.stranzl[.]at/includes/man.php
- hxxp://www.querummi[.]at/piwik/man.php
- hxxp://szaivert-numis[.]at/standardbilder/dll/2.php
- hxxp://losbalonazos[.]com/wp-admin/2.php
- hxxp://esser-transporte[.]at/img/common/2.php
- hxxp://fam-andres[.]at/administrator/2.php
- hxxp://gigele[.]at/includes/main.php
- hxxp://dwostasms[.]com/seta.apk
- hxxp://bomberathlete[.]com/wp-conf.php

App hashes (SHA-1):

Detection	SHA1
ANDROIDOS_FAKEBANK.HATB	a4c8fc5d6b31594823a177f98bc0f0da5273d50b
	e35a78b0648d10cd3c586b69a6862f36276a6525
	03281439f005d62e6e5fc73314c7162ae2e0ba5c
	93f96e346e9956b5e690f8c58ed130670dc303f3
	bc492b69207036bf314839b94b0bc4d98b5430ba
	fe1341a443e84a433f2d743a96b1cf1b928a6d99
	34cd1c302cb236a64d6e629a5cd8607635e5177b
	4ea1583c46b13f8fbeafc7bedbf7cfe08be05f96
	4fc7c0cf7969bfe040bf7deb14784379185c7d35
	bd63ec4b87402a49e2cb07e1920e50ad623d3954
	ef1a0799e431880a86fd6804fd5e45eab0cb803b
	54a8b9976cd2402538e598f5052ac424d6aebe53
	613f61c8c15338235fdd696dd9f08bbddf04d9fe
	15345f6c64b4801fb13c3f201d552b6a67380dd4
	df1b43fbd918836582a4cd8085efe7ec6bf40ba6
	0a47b1e2f59054e3020e1487a947e6f0c054f280
	1d9751bfd8e928e345d5063cc8b207cd351c53fa
	60485cd82e1aac9b9a0a04c6a41534a4d53ffa90
	af8e61c419908b59672a65e55c031a3866094068
	c928ffa8ffb3fea8586f1f8edbf7129a5ad584d7

Detection	SHA1
	dad368a88ef13d12f7dfdde478f8d9697dc418f5
	0ab13e470cd9b4ddb460cddd062685600c7864f4
	37d7455a8518e1628df38cad812ac1f55d978ffb
	5daf7f29ce893c7f93dd6908dd559f0689ebcd7a
	91c052d3625d6d27360ae03948d43e0209cc6ca2
	96f5e97cfc26e2c372449161b361db7f11df5646
	b3945dd815c1c662db294fcaa8c2bedb544e0ba8
	b5d38bcd6ca08fbf73314cf1b1d2f58a43cb562a
	1ede09ca64fb91cea14b2b5150115fb675583aee
	77c982474fc0d4bdbe6c951a0e658ad9658eb0e5
	b5d3af29e7d184c8ca06c173b8fb9b5465074188
	d69cf41d2a651502f14277e171d96e94b7714364
	e1f9ae0f757b9347accd91d8468a305ee38053e1
ANDROIDOS_FAKEBANK.HATZ	3cd6dd1c74174760158d20a6b6bb9f2d4221c7b8
	474a4eb03bc72335e9adbd000e3641790d7b81a8
	78973d78a821daf7b223e95ca2ae27d59ed966ab
	d373be29633376e2200e741687adea6adf9f5f3a
	01a6eb4014fb0fc234d51d8c97dc96c62b2a6676
	27642a8ee941503fd340ea3c48ff44d4c0dd6093
	33c25e15fdb41c3d1a4831dda3a524824917f0b0
	5c6538a08d89158efc2536353e97f272af039fe3
	709a522161a760c34f9b82b59cc78c62a66be8fd
	86f6ed16743eaf8de1cf3185a63b1120a1b91c88
	ad325c6158c218ba24f540ec1c290b0d5dd008e1
	cfb3ee74ff29d0258a87440f90d1e4a213bfa151
	d414fe34a9723c5e6ada8b91c44d47570b9262c4
	edf38b9fb79be1650e20c7b586a125db015e88ea
	152cc424282d562ac903e13ef0648635206704ac
	a66bf28089d7521420bbcd87a5d72e2d694d35fd
	c437463420ddceac0a4215fb62b440ccbefcde9d
	f10b315fb9d0f9573895b108edc75f0c78506277
	b801bbe4035724fe4eecc752591c0dca98b4dad7
	00fd3f105296e34eb13cfe56c48075f7be16cb5e
	540d49ff22a0024fc31f09f18aec9ce95bf36688
	94973388a1366fed32830152d14c9a3310bfc5e1
	c8d553a132aa0bd67462e2be36d1758b2217702c
	ccbe96ae3b52d5b15b782cb8583dc1e80c8b4909
	49c8c3370a29d633ae8f303b111fd130659222e2
	55e6e8e6f708650d486503af5cee1d93b425ce15
	66a284ad83bb964f61b52c268e303596d8a6ba97
	a24ef079ca40bf55be2bedf0588e6cc0e4f6ee73
	4a47397e839bb30eeb759ae1c6f103ebfa8a70fb
	73fccc6a951e6f221784332de797d17f4c75b277
	7a4a9a656e4ff864a3f76032d1d8bd661cc8a8e3

Detection	SHA1
	c325388e22b01525907ddc555d4538222f7156dc
	ec6a680e9bb6ca7fdb5fb23b7824275380aa22a4
	a72b46a4f9eca80c27353cf19b3d2feb03ef0c3c
	146340fe6e0a5bad0ef5b04f3f6cfda6969f0303
	da4b4714d677383550d63a9b1e38428fc3d500a5
	1a7f7f683a50ee09bad366139590f2524fd5f79c
	37f63726a590ce8cb01236db544a048e0615cc95
	043428a6a09b220c7b9535e1274e5bff59d48765
	149f2ab2d3297e42400e191cf05bb3a98863bb99
	1e8ff15167aa24d0d5caa9cf1cafb3bdc7594510
	3d029dd45d4b889c52bb49e6ca0b30fb566a994e
	43b079941904c4a5182f97d099dba87c75a6a1b4
	52b4a972e457ace732a5731f1ecd2e9b96757f86
	77450004605dea77df18c3b8962103ce20fc61f8
	7bfb2fcb2db30ea28bcd8fe37a7f7c19337736c9
	80c16f62d06d4ec18a9add4f73e8e219611af152
	829fe85c34034ca92b576804ab411112ad3cf3e0
	8951f6fc42ac532fb624efa9cd265ef2c9c62e1a
	9c357cd44b573a74f283aaad6a597ac12b754289
	abe53a7ee1ed0235ede8d3335a12c416f8105118
	c256195ca9d4fe75b28eb7164602adfb59db87ab
	d23aa178283c694c1d0c22069384927162643 2df
	de2859a758249d068c449917abc73d3edf050dc3
	a2f959b4670df7960a1e0f930cc899affbe07af6
	a46818095ec7e177e9a5d4c27f9b67450662ef7b
	d4569a529bc68998be8889a9f3f8d8a314548edc
	01112af4b4c191b695221518d82182a409abf2ca
	06896d180d20d2acb6c35e5ca8b87dad368a91a7
	2a6e52d1d41a94a9b13492d30f96ceda3cbdc216
	39ff5ffe8135595f0d339ece3ac3aa65ccd322a1
	5bf052f0ba840fcc6e9fe3b50beb465f39a7ec37
	9846a5352ddcbc356c214414b45e0094c9f8fe5d
	b1596b65a057d20658e47e93018ac2beec37c59b
	b3ab7ec2054a488f05d4be1b52450049fee1f9bd
ANDROIDOS_PUXIS.AXM	3e43b3e6036f1a9ba33bad6e16b4ffb4bab8346b
	0cfb4ecf43ed4a672d297cfbab5a7dd11edf77f4
	b53f9004018537bb9f084ee1352dbaebc4a621ad
	fcb9474436f511b5ac0b7fa3959e2498975933de
	fd1536dfd9b2534c19df07c22e10e3af1f7e14c6
	7885ae006fa10ab88b6830fd44a20101efb84357
	b50ecc150a9ca97a312b3549a9854b4caf3f5013
ANDROIDOS_PUXIS.CBTA	2b2e4ec52daecee35d75d31ca58000a37439d728
	99e878362f40427a0617410b88698a79aa7aa9b9
	6727fe7581d1ddb9805efde5e55335b4a1884ae0

Detection	SHA1
	c82f0c79651e644a80e220d1e1a90697b2f08424
	c3037e258082666110cadcb6561858b36c49e4a8

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