TrendLabs

ChessMaster Makes its Move: A Look into the Campaign's Cyberespionage Arsenal

Appendix

TrendLabs Security Intelligence Blog

Benson Sy, CH Lei, and Kawabata Kohei

July 2017

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.

Hashes Related to ChessMaster (SHA-256):

SHA-256	Detection
ae6b45a92384f6e43672e617c53a44225e2944d66c1ffb074694526386074145	BKDR_CHCHES.NAK
2c71eb5c781daa43047fa6e3d85d51a061aa1dfa41feb338e0d4139a6dfd6910	BKDR_CHCHES.NAM
e7c617e162c2ae173c3581b4e08d752dc421336e1e55d879642717b75745d49c	BKDR_CHCHES.NAO
6605b27e95f5c3c8012e4a75d1861786fb749b9a712a5f4871adbad81addb59e	BKDR_CHCHES.SM2
c885a4f5c066b00e9d4de8cc0f5463f27ce49869519db8cfdc7a9ae19cdce4f0	BKDR_CHCHES.SM2
efa0b414a831cbf724d1c67808b7483dec22a981ae670947793d114048f88057	BKDR_CHCHES.SM2
fadf362a52dcf884f0d41ce3df9eaa9bb30227afda50c0e0657c096baff501f0	BKDR_CHCHES.SM2
4ff6a97d06e2e843755be8697f3324be36e1ebeb280bb45724962ce4b6710297	BKDR_CHCHES.SMZJEA-A
75ef6ea0265d2629c920a6a1c0d1dd91d3c0eda86445c7d67ebb9b30e35a2a9f	BKDR_CHCHES.SMZJEA-A
590d5e0858893951e22e392a7dad76b30765c8fd139ca288efeead9b86836237	BKDR_CHCHES.SMZKDJ-B
2965c1b6ab9d1601752cb4aa26d64a444b0a535b1a190a70d5ce935be3f91699	BKDR_CHCHES.SMZKDJ-C
4521a74337a8b454f9b80c7d9e57b4c9580567f84e513d9a3ce763275c55e691	BKDR_CHCHES.SMZKDJ-C
c21eaadf9ffc62ca4673e27e06c16447f103c0cf7acd8db6ac5c8bd17805e39d	BKDR_CHCHES.SMZKDJ-C
cb0c8681a407a76f8c0fd2512197aafad8120aa62e5c871c29d1fd2a102bc628	BKDR_CHCHES.SMZKDJ-C
d26dae0d8e5c23ec35e8b9cf126cded45b8096fc07560ad1c06585357921eeed	BKDR_CHCHES.SMZKDJ-C
e6ecb146f469d243945ad8a5451ba1129c5b190f7d50c64580dbad4b8246f88e	BKDR_CHCHES.SMZKDJ-C
94813a9097833ca793a02a33d06cf78ff25558e516527aa8cfde7b7f62cdc9d9	BKDR_CHCHES.SMZLEC-A
ae30e854a2fb49da770666df78db3983cd3a83774a0fe19d0f98a9ca450d1bd3	BKDR_CHCHES.SMZLEC-A
2933bd208993fb7ec76ae3f55d2e7959c0a79d89f134430c6a798e82ebd94636	BKDR_CHCHES.YO
316e89d866d5c710530c2103f183d86c31e9a90d55e2ebc2dda94f112f3bdb6d	BKDR_CHCHES.ZJDK-A
e90064884190b14a6621c18d1f9719a37b9e5f98506e28ff0636438e3282098b	BKDR_CHCHES.ZJDK-A

SHA-256	Detection
72d7bcc54520a7d8929eeec78e2b2297a9094fa001483f86cddb7cf1b81704ff	BKDR_CHCHES.ZJEH
e88f5bf4be37e0dc90ba1a06a2d47faaeea9047fec07c17c2a76f9f7ab98acf0	BKDR_CHCHES.ZLDK-B
759e405351e6de779757695cc6fb1bce3cc6e3bb3ee4d24778d0cb2070091681	BKDR_PLUGX.BHS
2ddcb1dc466e22388485118bcf3089014348881c4d315aca452c6bb44b6c7bee	BKDR_PLUGX.JKK
f6ba0007038805fdc9e92ccbfed5f4cc681723bb548cc83a4b34f754f3356974	BKDR_PLUGX.ZKEG-A
1ac2134ef1ca208b3d236b387a8d3256ce6fccc0419947b77a9b671b6eba52bf	BKDR_REDFLOWER.ZBEE-A
c082d5bc76eb8375a90b622474da760bd499ae8371c16cc31085be2940b0bafb	BKDR_REDFLOWER.ZBEE-A
f9f2b38e11402b56fe05127bf0e688d74bb6e55834b93b7a0f6c61174670177a	BKDR_TINYX.ZKEG
5961861d2b9f50d05055814e6bfd1c6291b30719f8a4d02d4cf80c2e87753fa1	TROJ_BLOCKER.ASK
9a6692690c03ec33c758cb5648be1ed886ff039e6b72f1c43b23fbd9c342ce8c	TROJ_FAKEMS.USPO
58a7670111087243516b601c5f070f7de0db5411febe0a878783fdc17c969a59	TROJ_INJECTR.ZJDK-A
b20ce00a6864225f05de6407fac80ddb83cd0aec00ada438c1e354cdd0d7d5df	TROJ_INJECTR.ZJDK-C
f251485a62e104dfd8629dc4d2dfd572ebd0ab554602d682a28682876a47e773	TROJ_INJECTR.ZJDK-D
19aa5019f3c00211182b2a80dd9675721dac7cfb31d174436d3b8ec9f97d898b	TROJ_INJECTR.ZKDJ-A
5c6c2370090d68d2d3120cec62984767ae0fc93766939d159a2f4c482f58ae5b	TROJ_INJECTR.ZKDJ-B
312dc69dd6ea16842d6e58cd7fd98ba4d28eefeb4fd4c4d198fac4eee76f93c3	TROJ_INJECTR.ZKDJ-C
bc2f07066c624663b0a6f71cb965009d4d9b480213de51809cdc454ca55f1a91	TROJ_INJECTR.ZLDK-A
fd6a956a7708708cddff78c8505c7db73d7c4e961da8a3c00cc5a51171a92b7b	TROJ_PASTEAL.JV
73794263b657632805c8c3907e2f20a9743d8c9b83aa3e21629eccc5de02b1ca	TROJ_PASTEAL.JV
45d804f35266b26bf63e3d616715fc593931e33aa07feba5ad6875609692efa2	TROJ_PLUGX.DUKPT

Command and Control (C&C) Servers Related to ChessMaster:

Domains
area[.]wthelpdesk[.]com
dick[.]ccfchrist[.]com
fiveavmersi[.]websegoo[.]net
fukuoka[.]cloud-maste[.]com
kawasak[.]cloud-maste[.]com
kawasaki[.]unhamj[.]com
messagea[.]emailfound[.]info
sakai[.]unhamj[.]com
scorpion[.]poulsenv[.]com
shrimp[.]bdoncloud[.]com
trout[.]belowto[.]com
whale[.]toshste[.]com
zebra[.]wthelpdesk[.]com

TREND MICRO™

Securing Your Journey to the Cloud

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.

Created by:

TrendLabs

Global Technical Support & R&D Center of TREND MICRO