


Untangling the Patchwork Cyberespionage Group

Appendix




TrendLabs Security Intelligence Blog
Daniel Lunghi, Jaromir Horejsi, and Cedric Pernet
Cyber Safety Solutions Team
December 2017
Updated as of October 9, 2018

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.



Indicators of Compromise (IoCs)

Hashes related to malware used by Patchwork (SHA256):

Hash	Trend Micro Detection
6535696186395b02608f16d86ce9b918e45012a217c11352b9d2904bf6a30c6c	BAT_DLOADER.AUSYSB
ab70ef16e625291df6dc33903ec23dbc7b505c25e2e894bfbfd0110550d7664e	BKDR_SCADPRV.G
647b7a619b3ef6fa76b3e710a3f20b78a0a8ab6299b9245a893052d7b94b62fa	
f1a45adcf907e660ec848c6086e28c9863b7b70d0d38417dd05a4261973c955a	BKDR_XRAT.JCT
92be93ec4cbe76182404af0b180871fbbfa3c7b34e4df6745bcde480b8b4b3b	BKDR_XRAT.KVJ
684523927a468ed5abea8f6c0d3dc01210ec38aa4e0a533abc75dc891d3b0400	
a34d60d00ac67e8ccce6c5b969e86e969272af2e2479e17b5bfd0b25650504c4	
e5af968a8eca77ac64862db3f6c92d7d64db24a999d0ded30f272f2a220cdb70	
260fa4d0680272feb537aac722466e58eb26c5de2ac858c10d3a244655544313	TROJ_ARTIEF.EVV
d9cdaa649b7ca7b9f61121d269801dbbd68551488c8423ae3a3e95233d6ee99d	
889f1f6873a090162356109f0f3984c044094ea789028ec3e20ba2238d269160	
0aeda32f977c98c8160491358491d0ad0898dcaa3366bde60c0a3bf8541e7b3f	TROJ_DDEX.SM
de22772c655890a73c7fe13d6cff49b1a560d19df04271e4bc3adcd5402158c9	BKDR_DISMONN.A
f2c6effbbb203d5889f75b7d445f1a0f73c479e4a977fd7da3bd923f5b827762	TROJ_DLOADER.JEJOWJ
a6abfb56c25c06c5c12c08a8098f427fd0da11c5930a02ebb51ebc117ff63b1a	TROJ_DLOADR.AUSUGF
283e3e8a651b87e055944e9b132f087f88181331bec1194f354eccf085d1bfe2	TROJ_DROPDR.DAM
34399b371c44e52dbd17c6b4e46619f7c7131af20f66fd7a2c7f92c081d78276	
b6e9a1ab662304ad11ffca314fcf3d29bf7bd8cb2ff06d9b9727eaed576384b6	
bc8e469ac8515a23a3073a41099fde8420b8a40bb71abaf965c9031bd0a084e3	TROJ_FUERY.A
7535cf27ca99f8f77c8ae918ca07e8365289f27d252283444b1e6a5dd8bf087b	
10112aab7bc43c9c138aad9b75ed6a69d7305ea2f04b5cfaa14ecfcdffaa4c7a	
0345ecfb3b26acc072a3a423a9bc6aafe8750e65234e5d1f820c07cb61a2fcf	TROJ_GENOME.VIDK
145551d6ad9f6e6d825393342561407f9f663a43471bb1738f741addf4dd6d82	
e4f66bd9eb1cb01f103c9a0b0616c3b073c658c1248f0e0f6faa06a629d7b06d	TROJ_HTALINK.C
bf94a8f82f9b3ec1ad36be72a27813a661654bc5215559bf10b9eddfd49021b4	
7d6fa3046a4e558b2ef40ae0a96001a50eb3fcaed9b00e4d7bd235d1d83be01a	TROJ_MDROP.YYSOW
a0c9b6a77dd3e6738a9f5c1a6704adeef904831d29392cf2c24a5628afecf563	

Hash	Trend Micro Detection
4fbfc64623700615410ec2caba6b931494990e1c0b210d76819edc95a8d1d8b4	TROJ_MDROP.YYSRE
e80a97b02bf9c43b8d288097caa38ab85a03ec1f8dbbc7cced1198274f60f6f6	
4c8202aa414622c84a6fe32bb0402c30de964e84dcffef452e830c6f3b6c8467	
667992e8c195664ad87fed3e715f0a52efe79a7c83f67d031c3a1affc6411e5f	
328d98944555f83357c099208c3be597f5a0af0c05a3384dfbd419822177ad08	
8a6a2027099e8a4d68f4c9931a8050b89aa587f8de47244af4ff399dfc0930a2	TROJ_MDROP.YYSRG
72d71b91ceb7dda82db0ec8ca3aba476d01b1011057ae71425e34fa31af2ee6b	
dfc469d0cca07e83e58c6266dcd6ac67c5d5dacd6c6ef2543b3ebbbf6d35a280	TROJ_SELFDEL.TT
d0d63189a28406914d9d49e8164dc716326f849cd35195ad56bb7e7ea0196ad8	TROJ_VAGGER.B
dfe0e2cad843ee66f7bad85e62accb76ae54993eb057041e6f81315a3c99d522	TROJ_VAGGER.C
f24546590ad97b60b3c99a0bcacea4e405ba3884b57393ecf47b3463c8936a45	TROJ_XRAT.JCT
801b101bc935ae3c4a8b9bf964ddc30fc5132da2271a23b9727f2b78187c62b4	
244d8dccd179a94b91e51f94be1e8ace42835b5b204e94e3f77f52dc866d8209	
ae5ecf3889c4bb1838cca1b644c16cb32e815fc1e2fd0db96aa6ca6fffbf30b6	TSPY_SKEEYAH.LNH
cf7adf8ed9b779e62f603a2f23af72671eb331e79586c46b75bd95644a62039a	
4a21f18ec5e65b77a9c826991d6c51c45001d2b013d317096fb5f1417da88d74	
7317867ee5207f6b7195930d0ec3938130cbd2dc00adc8ba0cd3eca7114f4b26	VBS_DLOADR.YYSUJ
b43bd22295f8287e5f8126712f0db11afe8b2bdaf918ed361c0d0865125a585b	W2KM_DLOADE.PUTY
0c09c662699c507c553317a909665952562bd7e2434c4a719470f672bdada700	W2KM_DLOADE.VQZTP
48b68a5ab219d7917dbe818e00ddbae889cf8655faf02639e4a3fbe4e46ef9b2	
f0766afdaf89181401b1cbcf012f8e3bf7af8dde10f11407e23ad867e1b2922a	
3dd9814aeae5530e514915c6f73125188a692d0df2e56788c4302cb63d406e03	
0cddd9288e87db957b3517ac201f2da309e782a8f127d49e1dec2c7a7312d911	
c1227e575553f06fca469d43d02eda006033e5d88acb9b516f5ba64c030772b1	TROJ_MDROP.YYSRH
72d71b91ceb7dda82db0ec8ca3aba476d01b1011057ae71425e34fa31af2ee6b	
c1227e575553f06fca469d43d02eda006033e5d88acb9b516f5ba64c030772b1	
90218e24be373a8a8a3452d5da59d551a3b1936e7c3210cc9cb83995be3d2030	TROJ_MDROP.YYSRG
647b7a619b3ef6fa76b3e710a3f20b78a0a8ab6299b9245a893052d7b94b62fa	BKDR_SCADPRV.G
47e0886ba064156d7914db02dec46fa8f497b20373c7f2d4bc8f3f13bd8fa455	BKDR_SCADPRV.I
ab608d1adb169040b6fad2029ae56c07fa8d45ee9e03f4b9dfecbce2b7d92b1d4	

Domains/URLs related to Patchwork's campaigns:

Domain/URL
hxxp://bdarmy[.]news
hxxp://brokings[.]org
hxxp://ciis[-]cn[.]net
hxxp://clep[-]cn[.]org
hxxp://cnaas[.]org
hxxp://cpcnews[-]cn[.]com
hxxp://crazywomen[-]dating[.]com
hxxp://dwnnews[.]net
hxxp://euuwebmail[.]com
hxxp://gffbzbgov[-]cn[.]org
hxxp://gloalfirepower[.]org
hxxp://googlemail[.]support
hxxp://googlmail[.]cloud
hxxp://ifenngnews[.]com
hxxp://iisd[.]org
hxxp://invitingholes[.]com
hxxp://loweinstitute[.]org
hxxp://mfagov[-]cn[.]com
hxxp://mileastday[-]cn[.]com
hxxp://militarypeoplecn[.]com
hxxp://militaryreviews[.]net
hxxp://milstar[-]cn[.]com
hxxp://neteease[.]com
hxxp://pla[-]report[.]net
hxxp://qzonecn[.]com
hxxp://randreports[.]org
hxxp://rannd[.]org

Domain/URL
hxxp://scitechrends[.]com
hxxp://servicelogin[.]center
hxxp://servicelogin[.]support
hxxp://sinamilblog[-]cn[.]org
hxxp://sinamilnews[.]com
hxxp://sinodefence[.]info
hxxp://stripshowsclub[.]com
hxxp://tecchweb[.]com
hxxp://tiexue[-]cn[.]net
hxxp://ustc[-]cn[.]org
hxxp://yahoomail[.]support
hxxp://zhiihua[.]org
hxxp://zhouangjiabing[.]com

Command-and-control IP Addresses related to Patchwork:

IP Address
93[.]115[.]94[.]202
94[.]185[.]82[.]155
94[.]242[.]249[.]203
179[.]48[.]251[.]4
209[.]58[.]183[.]33
176[.]107[.]177[.]10[:]23558
5[.]101[.]140[.]220
209[.]58[.]163[.]44
46[.]166[.]163[.]243
5[.]8[.]88[.]64



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.

©2017 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.

Created by:

TrendLabs

Global Technical Support & R&D Center of TREND MICRO