TrendLabs

Confucius Update: New Tools and Techniques, Further Connections with Patchwork

Appendix

TrendLabs Security Intelligence Blog
Daniel Lunghi and Jaromir Horejsi
Cyber Safety Solutions (CSS) Team
May 2018

Indicators of Comptomise (IoCs):

Hash (SHA-256)	Detection
FuddiDuniya APK:	
467c587ccff90bf8b4fff77aa88392640fcca75656cfb8bb9fb4c0e935edb525	AndroidOS_ConfuSpy.HRX
Philions 1.0.3 APK :	
b2a3b46498abdec68e82b85f01fc8d96ada56bb9a9a9d294eab8441e17484a79	AndroidOS_ConfuSpy.HRX
Philions 1.0.4 APK:	
ccb03e6b26ba9039f0a098231495072dd5fcca587d2f3aa7d51f84419b349c91	AndroidOS_ConfuSpy.HRX
Philions Windows malicious installers	
e95c6ebc4737d2dc3fa3a29df456322fc19bd4e85373008b580cfc042037b9bf	TSPY_CONFSTEAL.C
d2676976c12581ea3954804e7831a8a11019cddfb2a6e91dcac3d3299600aa15	TSPY_CONFSTEAL.C
84312d3b0760540ead06151d0d9dec9ed674afca615ee4caa47155abf51b93a0	TSPY_CONFSTEAL.C
batch2exe dropper	
03265294358b7edb7a8b689474e9791d30a4d6fc47f9caadbc0fc064abc447ae	TROJ_DELFDROP.B
.NET downloader	
e425b6bbf5d74f3f4b442a8b9b083629a89a616645eb3507e59292afabf181d2	TSPY_CONFSTEAL.C
4d369817cc80d25f0f483b9d66633cbb33de6fe8c3e248a3abc9548f30d97b0f	TSPY_CONFSTEAL.C
Delphi second stage filestealer	
5c2dd8fadf9f0bb60513f693b188a704583bb68da5572442d6c742ba0c8989c0 (94 chars substitution table)	TROJ_DELF.XXWZ
Malicious delivery documents	
cb8fa89b2664155e4fb60bf33024bc6d4b1d658abbec250a2a13b3d2e337ad86	TROJ_DELFDROP.B
780e56adc4a71c46892fe30b269a8d879a8fad0f885ac90dd1605d2510c5172a	TROJ_DELFDROP.B
7be2628f1cfba974979208cace745561e0403c639df8e87238938c8afae30788	TROJ_DELFDROP.B
ffe9b86bbc2298ba003796bd18283fb4fba78962ae5aefd213a78b3494fd5708	TROJ_DELFDROP.B

72895802000d4eb9b9c850b8360f8489e14e120cc3ecc25aae6a86c46469d79d	TROJ_DELFDROP.B
b8bc0be5b8778f1813fc20c8984cc8d902d41df3f1a67f4e33a73ec577ad20cb	TROJ_DELF.XXWZ
b56be15f2d31a64e3fdff5461a2c72eb7f18743cd3711e2574b85e5d71fb64f3	TROJ_DELFDROP.B
627c2b722ea28fdd9558dd62e0938908bded7aa16a7649af87f88f1fef0fc44f	TROJ_DELFDROP.B
7747440bc9aa779ef0b7e925f029ebf1a4b0d8f40baf01b21606c891b61d10da	TROJ_DELFDROP.B
Python file stealer	
52be00915bd34d552f2c37000b99e1c5921521dcac96dcb76c3ff4050af170ea	TSPY_CONFSTEAL.C
Delphi file stealers	
d971842441c83c1bba05742d124620f5741bb5d5da9ffb31f06efa4bbdcf04ee (94 chars substitution table)	TSPY_CONFSTEAL.A
5c2dd8fadf9f0bb60513f693b188a704583bb68da5572442d6c742ba0c8989c0 (94 chars substitution table)	TROJ_DELF.XXWZ
Delphi backdoors	
29844b8125bb408f2c95754303f8b201ba754950111151bb3405740ebb5dae30 (bit flip)	TROJ_DELF.XXWZ
ff73e549a1d761c8e323e60d96aa31c0733aa4933243064c668c11eba3143f77 (bit flip)	TROJ_DELF.XXWZ
32425dc129d5b4cf6483e267907365ba5ad87c082d536e190f1d46f6a70b3ec8 (bit flip)	TROJ_DELF.XXWZ
3fad24c3a572e93764ca528cc025b19928682e8ed05f4fec4adac5dadb9c7127 (XOR-based)	TROJ_DLOADR.AUSUIN
97c6dc02eaa6b8ce8d46460d5d94f57ceb4f355626d1cd3ddaf6dccea81d75e2 (XOR-based)	TROJ_DELMOFU.A
cea94b50159f940df6ef1b7a1dd0fffd1ea45ce6aa86696f1441826029980984 (94 chars substitution table)	TROJ_DELF.XXWZ
2d1ae38f918293599bee7df30185084e767a447c0f89ac42ca79dbaa828ce1b1 (94 chars substitution table)	TROJ_DELF.XXWZ
147a44b7d1011aa553cbc4fec0aa13c051c6a6f882318cebbe52acc65a1af011 (94 chars substitution table)	TROJ_DELF.XXWZ
Patchwork	
Malicious delivery documents	
4c704849972882b81e398f14357c35546f513928aafb687f0e36f18438077055	TROJ_RELSLODR.AU
885ca96b477e09edbb20e979a422597b56d72ce1435551a43d30aa9024d9e2ec	TROJ_EXPLOYT.TIDAIBF
d486ed118a425d902044fb7a84267e92b49169c24051ee9de41327ee5e6ac7c2	TROJ_CVE20152545.CAP
fd8394b2ff9cd00380dc2b5a870e15183f1dc3bd82ca6ee58f055b44074	TROJ_MDROP.YYSRM

c7fd4	
07d5509988b1aa6f8d5203bc4b75e6d7be6acf5055831cc961a51d3e921f96bd	TROJ_CVE20152545.CAP
a67220bcf289af6a99a9760c05d197d09502c2119f62762f78523aa7cbc96ef1	TROJ_MDROPPER.AUSIC
7e0e7deb55fb6024127273620466148fc70cea5bea43457cddd38fa650b0665c	TROJ_CVE201711882.SM
e97deb1869b219dc1b93820b360c79d9d535685926ce4a46f567bc27c352ac72	TROJ_CVE201711882.SM
a67220bcf289af6a99a9760c05d197d09502c2119f62762f78523aa7cbc96ef1	TROJ_MDROPPER.AUSIC
95efb091998fee13cae08c1ae70a8edf4372362e8270d37614bc51b17cde9bbe	TROJ_CVE201711882.R
c4e3f4d812a95fd7c49e98143a5dcb8b13542e3d8a72054b3d6f844c242d8084	TROJ_CVE201711882.UHAOBGXQ
4ae1677f511ddc57784c330b1c9c6091e136ada2123ebb1ddaae7666cd075872	BKDR_XRAT.KVM
21f5514d6256a20dcf9af315ee742d6d2a5b07009b200b447c45b2e8f057361d	BKDR_XRAT.KVM
c11e2306a7926e55f4b2fcbbe7307690059572f1857724bd4aaa7974be6a4b56	BKDR_XRAT.KVL
72b3636718456d99a3d12267baa7b94d2e58a996036c2d39505e3e02ad38d94f	BKDR_XRAT.KVM
b4e6724be4764ca14060262a9b3dee20f1a72be9f5ae7f15294ffa3cd037b78b	BKDR_XRAT.KVM
119ae4ad1797b6e1a46404264de95c1e5e0bb95920926ed9740676864ebb6411	TROJ_DELF.XXMO
1ce65c338471814b69ab2779a24a3e80d1e09ab37f3f064bf9d9065541f18df1	BKDR_XRAT.KVM
2d4a460a5f165e33c695791f2803dfaf348b0cc5cd9938119856986745db0bbd	BKDR_XRAT.KVM
8204a9061f124dd83745c01bb328063712615dfc6e4179a9886ae3eba3f53633	BKDR_XRAT.KVM
cf0999f84bfcefbb789fca7bc22f2ee9cb870d9e794d177efd1acb6647e01862	BKDR_XRAT.KVL
5b76985f26c17df4897fff102a7ca66c39e8b58dc06dd367ff6aacc0616a664b	BKDR_XRAT.KVM
ce0e152ef2cb8f1e74580d632a17451b8e007719433074a614d0468bad11a8dc	BKDR_XRAT.KVM
679eec0b8f3a9bb2d85ef1f9e0220b98bb7ffb9f9a7e1a3e7c2fb45af37b4f68	BKDR_XRAT.KVL
236a245ae5b6333336a38a0c347664386866e70c043d57c85b37d15b7ecd050a	BKDR_XRAT.KVL
c2f7e50e753322249a98e2e906b3cb6e328fcb09a4cca341304fd25a742c6e37	BKDR_XRAT.KVL
a53a13a6f3aed8523710ff38a8d38f5aa9ebd9b44a25cc4967130f238f9	BKDR_XRAT.KVL

990a3	
9cb4b0f1330478d7748fc1f92e3150dfcb7cf958dce302e9224c235d4b6f19ed	BKDR_XRAT.KVM
c057b3a6bb9082b6be0b57d1c07ae30bc97a97ea9740a1781a23ea7e20686a6b	BKDR_XRAT.KVM
301bd83352dde7113cc7769d918da2953a6dcfe7935a7e945ac251378873264f	BKDR_XRAT.KVM
47edd2fc695f04623ec883416dbf166a495ded54cc4af7e41ceadd1cd4449608	BKDR_XRAT.KVL
141c92659d1b126d85383ee099cbc56e3bc9832c952446bd8969bf900d4ccf4c	BKDR_XRAT.KVM
110568a2c505b72ef3957f1d2ce42ab1fb9264180ef94704ce2b9f1f0d5beffd	BKDR_XRAT.KVM
5518c1bad3dc9b63c3b34a57d96a6dad11b0c30f6ad08ce7064e65d6eeec315d	BKDR_XRAT.KVM
1e2b962a1a850808c9d071324e642d2891ea2c0b8cd48f471b1af16fa38ae399	TROJ_CVE201711882.UHAOBGXQ
Droppers	
939ac722791058d6cdf165624d7cc3a47e3c815a7bb62eb2493755ae1b3c514f	TROJ_DLOADR.CSH
2d981e468deac0ad5b47f7c55d05ea5812ddd4d539f9939cc6825ea261750533	TROJ_DLOADR.AUSULC
1eb22abc743122ce749f3d5263bf9285d2dccbc2b520b62a1b280783e87c671b	BKDR_XRAT.KVM
Delphi backdoor	
5881d307ad1b7ac72daf7ab5dd3f72a278ae4bda0a61e25f86940540250c3dce (94 chars substitution table)	TROJ_DELF.XXWO
061c155e87eaf790cc8bfa6c59ab7c1e5184df77dee4bd1c59506c9a91785b9a (bit-flip)	TROJ_DELF.XXWP
Delphi filestealer	
795ae4097aa3bd5932be4110f6bd992f46d605d4c9e3afced314454d35395a59 (XOR-based)	TROJ_DELF.XXWZ
QuasarRAT	
60d522f415c0b2bfffb2a25650e6ac975ca8976750129ac769d257bf173dcec2	BKDR_XRAT.LA
e1c837fc2399ffc3b211b422f67b4af02041f79b4eadfa8e4f1b79d8c133d714	BKDR_XRAT.KVL
5359a7bb5e7b68e61ecce8c1ca6167c88a685a1085b6005cecd5ef9c7a838af5	BKDR_XRAT.KVL
eeaa075f3e53737471e8da2f7e932e67776f2387ddef73c4208aebded98eea2b	BKDR_XRAT.KVL
81dd46a4cc1138ff7a7f12747af501b51f0ad35c5a247cb44e2296cc8fa4c886	BKDR_XRAT.KVL
Badnews	

ab4f86a3144642346a3a40e500ace71badc06a962758522ca13801b40e9e7f4a	TROJ_JAKYLLHYDE.A
290ac98de80154705794e96d0c6d657c948b7dff7abf25ea817585e4c923adb2	TROJ_JAKYLLHYDE.A
d909945e0188839c5b52043c1ade5951a8481d53eb5bb9564366e73f6928c907	TROJ_JAKYLLHYDE.A
bb7f7096787f9e4974baca7b8faece258464d426ce1ff749d9870f24671358b9	TROJ_JAKYLLHYDE.A
ab3ebbda6147230b70c9807047ab5bbb4481f7bb8c71955e579047d91226b5aa	TROJ_JAKYLLHYDE.A
de83af838038998474a7f3cf1ba3a146af5a5b6d1b53ac59966978ae9703fa19	TROJ_JAKYLLHYDE.A
Delphi filestealers	
1f0dabd61947b6df8a392b77a0eae33777be3caad13698aecc223b54ab4b859a (XOR-based)	TROJ_DELF.XXWZ
815466ec21c59f7704f094a0e4cfc4f817c8b98231d10fe01919b6bd60eca64e (94 chars substitution table)	TROJ_DELF.XXWZ
Delphi backdoors	
94e1916e880eedc02b8c61557926a77d7555f3f7a0131c390cdb4e98a23ff1f0 (bit-flip)	TROJ_DELF.XXWZ
6874e3b191c047695fb4b020160604b85953a067ceec795410d5fda22994db95 (bit-flip)	TROJ_DELF.XXWZ
a7950c25bdbe103b3f0071bc35e90c28b06eea043b217522267467594 5e7be22 (bit-flip)	TROJ_DELF.XXWZ
33c5867b3375ef7e879caf614e79455df26adafdbb6aad11bde23edf695b5d85 (bit-flip)	TROJ_DELF.XXWZ
3bf87393abc6344a3e0dc751c81cced760b886e2f97b319c1443636b9957f2b9 (bit-flip)	TROJ_DELF.XXWZ
1a510082dbcd23a86569c713a848100a1ea018a6f35f8fecf9bbe6a86f555ad9 (bit-flip)	TROJ_DELF.XXWZ
565de1908528707d44be5e6beac37456c2424035202d9272c175a1b96db19cdc (bit-flip)	TROJ_DELF.XXWZ
184446bcb17021c39128369e9fe3d06cd0dde430c7f2e90c945c5a3299ef7b52 (bit-flip)	TROJ_DLOADER.TICOGAS
8256fc98e05684569992a93318f519649d381081534e03b39263b071dd6e14c0 (bit-flip)	TROJ_DELF.XXWZ
4ac870ef498441034054b1c0226ab079568e1c45bd8895e621598c9023318e66 (bit-flip)	TROJ_DLOADER.TICOGAS
e93f28efc1787ed5e8763cdc0417e7d5db1c9203e484350c64860fff91dab4f5 (bit-flip)	TROJ_DLOADER.TICOGAS
408e7360b5f382d1fe90719dcbd1343c22a48bd17017ac47374e15c36cfffe1e (bit-flip)	TROJ_DLOADER.TICOGAS
229805c8c6b2c54f7e34e23dba61268a1ef89b04f9052efec292366aa86c224a (bit-flip)	TROJ_STARTER.TJBGBT
bd7f33c1566f56b1bce2f59e983b60d79e2e2de80ea9cd6dffe613005ab2e817 (bit-flip)	TROJ_DELF.XXWZ

f43ea2db9e79a819901c6ebb2a7cabbdddf4b3d12ccea985604d391faccbd32 (bit-flip)	TROJ_DLOADER.TICOGAS
c6c0ca3ca838b6ab857a1b22cc66ad568af96a3368c3c99598e63c4e4e6c85cb (bit-flip)	TROJ_DLOADER.TICOGAS
ff184e204f40b2f917c517a2abf92da20a96026e02ba4fbfa405d5c72ab96050 (bit-flip)	TROJ_DELF.XXWZ
80f02104726ff8f78db3ef70c2b641c373ec36abfd5d457219648b6edf71a521 (bit-flip)	TROJ_FAKEDMC.A
1be9579507a8b20110b740c65f1b65d920c455ab1c026cadb1a250a267c206be (bit-flip)	TROJ_DELF.XXWZ
b1172084ba179d97c93f5e31ab6d0756f0fd7036020f021a11f6303b35049461 (bit-flip)	TROJ_DELF.XXWZ
605a80c8b7305ad1d6815bfe2035128c8dd06e8333d8b3cba9ed68caa4aa0c17 (bit-flip)	TROJ_DELF.XXWZ
21ff4ee3adbe90638453f76f8922cf6ac39d0016afbddac9dd18f6db80e7ff33 (bit-flip)	TROJ_DELF.XXWZ
f558351453096e02e5fbeddc10f59f6f8e5311cefa626aa78f06ef8474997df5 (bit-flip)	TROJ_DELF.XXWZ
6cee1781b3acddea76959b0fc3c0058938da9ed4facc9c12c742633bf2dc5ca2 (bit-flip)	TROJ_DELF.XXWZ
2af07c7cee0743b9ab84eb5947d0334cb0b1dc874fa562920aafbc4ad95b12fc (bit-flip)	TROJ_DELF.XXWZ
5716509e4cdbf8ffa5fbce02b8881320cb852d98e590215455986a5604a453f7 (bit-flip)	TROJ_DELF.XXWZ

Malicious Domains and IP Addresses

Domain / IP Address
Related Command-and-Control (C&C) Servers
185[.]203[.]118[.]115
185[.]29[.]11[.]59
209[.]58[.]185[.]36:23558
94[.]156[.]35[.]204
datapeople-cn[.]com
http://46[.]165[.]207[.]108/appstore/appservice.php
http://ambicluster[.]com/aoc[.]php
http://analogbiz[.]com/pause/break[.]php
http://classmunch[.]com/rest7987987rewrew[.]php
http://computesystem[.]com/scrol89r74gfeflock/electro686876fsdfs[.]php

http://digitizet[.]com/express54354view/docc7686gg154po[.]php
http://digivx[.]com/trick6878ftomfe/Reo768768jhjkh7687[.]php
http://digivx[.]com/trick6878ftomfe/Reo768768jhjkh7687[.]php
http://ebeijingcn[.]live/templates/software[.]php
http://ebeijingcn[.]live/update/software[.]php
http://errorfeedback[.]com/MarkQuality455/developerbuild[.]php
http://i3mode[.]com/dbExpressversion/db87987Administrator[.]php
http://iexplorer[.]ddns[.]net/premium/product[.]php
http://lepze[.]com/webseries[.]php
http://logicvisor[.]com/BoiUiNqDvkAbaoSlakfKj/filedirectorysystem[.]php
http://logicvisor[.]com/LIEZhJGpwVfRlLCcbzrdPlb/rootfilesystem[.]php
http://logicvisor[.]com/Scroll454656capsyt/standard567tyr[.]php
http://logicvisor[.]com/vwVKKGnSmfRguGEuGjGmcja/fatfilesystem[.]php
http://logicvisor[.]com/WTzFMQbzfmjehThulJnhyA/ntfsfilesystem[.]php
http://logstrick[.]com/Bos24hhgihkgch987987f/modified7687shdf0990[.]php
http://logstrick[.]com/Million167786gg/original678tyhghg[.]php
http://mfone[.]net/strength[.]php
http://microdigit[.]info/microservice/micservice[.]php
http://msoffice-updater[.]ddns.net/universe/blue[.]php
http://msword-updater[.]ddns.net/pyrimon/directory[.]php
http://pcupdate.ddns[.]net/mercury/heliocentric[.]php
http://qutonium[.]com/Bingfdkshfljsafljsaf/spiraldquiyqwiudff[.]php
http://relaybg[.]com/estateertret76576fewr/Maxcvhfdmin8797fds[.]php
http://saicgovcn[.]xyz/systemdb[.]php
http://scan8t[.]com/delta/deltafile[.]php
http://scan8t[.]com/encourage/spring[.]php
http://scan8t[.]com/encourage/spring[.]php
http://scan8t[.]com/pulm/links[.]php
http://scan8t[.]com/pulm/scrub[.]php
http://scan8t[.]com/silo/strength[.]php
http://scrollayer[.]com/equation3343tweywd/linear87987987ytre[.]php
http://upgrade9[.]com/roadrash/team[.]php
http://windefendr[.]com/description[.]php

http://work4m[.]com/engine/mkfile[.]php
sastind-cn[.]org
Tautiaos[.]com
Links to malicious documents
http://www[.]nationinterests.org/index.php?f=Python_Strategy[.]docx
http://rannd[.]org/china_adiz[.]doc
http://www[.]sinamilnews[.]com/cp0000412[.]rtf
http://chinapolicyanalysis[.]org/Chinas_Arctic_Dream[.]doc
http://mail[.]ifenngnews.com/Strategic_report_EN_2018_A01[.]doc
http://mail[.]ifenngnews.com/Strategic_report_ZH_2018_A01[.]doc
http://mail[.]ifenngnews.com/8888-91-2018[.]doc
http://chinapolicyanalysis[.]org/Armed-Forces-Officers[.]doc
http://fprii[.]net/The_Four_Traps_for_China[.]doc
http://fprii[.]net/Part-I[.]doc
http://fprii[.]net/Part-II[.]doc
http://chinapolicyanalysis[.]org/Weapons_Systems_Factbook_2018_NQ[.]doc
http://fprii[.]net/Systems-CW-and-DW[.]doc
http://mail[.]ifenngnews.com/ADiCON2018[.]doc
http://www.mericcs[.]org/GPPi_MERICS_Authoritarian_Advance_2018_1Q[.]doc
http://www[.]worldpolicticsreview.com/ChineseNuclearThinking_Final[.]doc
http://planews[.]live/China_Coast_Guard[.]doc
http://tiebabaidu[.]live/CSBA6318-GBSD_QLRSO_Report[.]doc
http://mericcs[.]org/SouthChinaSea[.]doc

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