Indicator of compromise (IoC) of Transparent Tribe

Short Description:

Transparent Tribe (also known as PROJECTM and MYTHIC LEOPARD) is a very prolific group that is well-known in the cybersecurity industry for its massive espionage campaigns. The APT group Transparent Tribe is mounting an ongoing cyberespionage campaign, researchers said, which is aimed at military and diplomatic targets around the world.

Transparent Tribe mainly relies on both spear phishing and watering hole attacks to gain its foothold on victims. The phishing email is either a malicious macro document or an rtf file exploiting vulnerability, such as CVE-2012-0158, CVE-2017-0199. The attacker used watering hole websites for deliver a remote access Trojan (RAT) dubbed «MSIL/Crimson RAT». The RAT allowed attackers to steal data from infected devices, log keystrokes and capture screenshots. In the past, the group has also deployed different types of RATs, such as BreachRAT, PeepyRAT, DarkComet, Luminosity RAT, and njRAT**.**

Indicator of compromise (IoC) in computer forensics is an artifact observed on a network or in an operating system that, with high confidence, indicates a computer intrusion.

Indicator type	Indicator
FileHash-SHA256	876939aa0aa157aa2581b74ddfc4cf03893cede542ade22a2d9ac70e2fef1656
FileHash-SHA256	20da161f0174d2867d2a296d4e2a8ebd2f0c513165de6f2a6f455abcecf78f2a
FileHash-SHA256	b67d764c981a298fa2bb14ca7faffc68ec30ad34380ad8a92911b2350104e748
FileHash-SHA256	0ee399769a6e6e6d444a819ff0ca564ae584760baba93eff766926b1effe0010
FileHash-SHA256	45838a7e4bd340cb86d6b39beba5b64b162a7925cd7f1214c02bdcf304db81a3
FileHash-SHA256	d2cc95b72c3e72b3888e9fa35f6fe0563f9dbbd08b76d0c3546065ceca3c5961
FileHash-SHA256	1dea5c3fd77956115521e97309e5c07e220229acb142c920db996a85c018ca0e
FileHash-SHA256	e4d1f8ff1282ac60adc0134aec2420aa652250ac8ddafe866e56d2fab165a132
FileHash-SHA256	bfc20b00bb5b9223db2b631061d6a5d8ba989fc5572323737a7019b9013eb89c
FileHash-SHA256	b29691ac40b8bbb12b13e84641ad20583d1387ca356850aa7b5e76b0f6c76806
FileHash-SHA256	c9cdd5a5b0701a4d311e0264f5bcec49fa500dde81ff8dbaa081be032b0c0446
FileHash-SHA256	1bf6dc9af6dd730120f598d02f139f5a7776993afe29679f83a3d2fda3599736
FileHash-SHA256	93f2358f631d4bf5a1f16b40c5bb9479dbda492d6e96c2fd9760854d219faab1

Indicator type	Indicator
FileHash-SHA256	e38ff03d54d40f4e10292d7cbd614f26f3af13d01ded95dc7c363b317a5d6dd4
FileHash-SHA256	e7dbf1eacfbd73576b0e410099898e4c7e2d51d76fe3095314dee1b54860bf4f
FileHash-SHA256	567b82c892f10a5cc6d0286c5777e7462cec7182eba81db7dd7de53d1e8d3274
FileHash-SHA256	a22f6dc3eb0001c2be76d261721a1c1f419e15f6b5bfff95c5b8a5f633ce1956
FileHash-SHA256	fadc0fe0714d9e95904ccaaf16d895ac71c1337e92b8eb51258fed9fb8fb4620
FileHash-SHA256	72aa69be5cd46220e1509c040ceb6e3cbb3c676a6c464a811370d688f45f26ec
FileHash-SHA256	2e103dd8eda4750fd5fe99c0c5fbc987ae7712bea7c08db4db240e85a0ee1bbf
FileHash-SHA256	1d806466896998a6c4ac962d6e5381fe704670e3fd912db98e13c2a5482b9a7e
FileHash-SHA256	cee88ffae63cd95e4f9f7008a86a8d7818a47b62608d28a70bbe8d73c6d2b042
FileHash-SHA256	0283c0f02307adc4ee46c0382df4b5d7b4eb80114fbaf5cb7fe5412f027d165e
FileHash-SHA256	4a25e48b8cf515f4cdd6711a69ccc875429dcc32007adb133fb25d63e53e2ac6
FileHash-SHA256	58643719af0f271b87c51665c2e8c904db70155b8c6f514d6e5f44c0828a4a53
FileHash-SHA256	6c9c6966ce269bbcab164aca3c3f0231af1f7b26a18e5abc927b2ccdd9499368
FileHash-SHA256	1cb726eab6f36af73e6b0ed97223d8f063f8209d2c25bed39f010b4043b2b8a1
FileHash-SHA256	ccbe720fd059610227d478578a5a4019c96885de8fd3e83984f9c1c5fe850ad6
FileHash-SHA256	c598f7956b1d0d6514ade39df05c9fcad70f970957c980d15f6d019e5ca04df6
FileHash-SHA256	81ca347465f28d093a27caf3d83fe5c4fb50c5e48cfd851a06784d431fa8c2cf
FileHash-SHA256	2aa160726037e80384672e89968ab4d2bd3b7f5ca3dfa1b9c1ecc4d1647a63f0
FileHash-SHA256	c4a75a64f19bd594b4bb283452d0a98b6e6e86566e24d820bfb7b403e72f84e2
FileHash-SHA256	1d09e91d72c86216f559760da0f07acdc0cff8c0649c6e1782db1f20dcc7e48f
FileHash-SHA256	b0279cc1fde7b18c0632585ea0bb48c3f3140d0a4ff4ccb3b35eaee27c12751d
FileHash-SHA256	234defc7e28089ce81141907ceb16f3c80b12b6c19a4516d97f049ec66af633d
FileHash-SHA256	709d548a42500b15db4b171711a31a2ab227f508f60d4cde670b2b9081ce56af

Indicator type	Indicator
FileHash-SHA256	a866800a90a404feb4a96813c487bfd7114a5ec521516eba8c0178fb3f08f74a
FileHash-SHA256	38a5e825577b51eefe4c571d29b34713b4fd2a2b09a013df4803110d5ce553e8
FileHash-SHA256	8c6aff2224fdd54615ef99d32a6134c961b6d7d576b6ff94f6b228eb8af855af
FileHash-SHA256	0a6d33bdc0b70a45626211393d67566e1c9ebfff020f7ff1ef23dc93ede0c27a
FileHash-SHA256	26ca6af15ff8273733a6a386a482357256ac4373a8641e486fb646bc9c525afa
FileHash-SHA256	fb761a2da4841f8739d33a682c5f2f39a033c7ba16430ce5785f7d51ab5d1537
FileHash-SHA256	7ead6660510aa9a7e58094f05a8655df23fe680b57d51141e6e6d124c9a678d1
FileHash-SHA256	36c9022b8d2260b360dc9390c146636a97aa984cdf5176036cd4e444840216f8
FileHash-SHA256	8b11db3a20f447b31cfc6a6af626c037b8f77ed0f96f7210f9d58a21f83e6eda
FileHash-SHA256	dd0762fc58acb30f75b0a2a14dbef2ccda553ea9dde08a180c60cd4113e1a506
FileHash-SHA256	1a2cf862d210f6d0b85fbf71974f3e1fbe1d637e2ef81f511ea64b55ed2423c7
FileHash-SHA256	029feed08a935ba7ec5186c3ea8ae7114910ba95011395f9a097bf2b069da342
FileHash-SHA256	5bc838b11eadb3fec80a7e6bb46183b868096d8c2e499bedd9c976f3d70d41b1
FileHash-SHA256	92e9ceedf28c99f90f8892aec9d2fa413ff0f4f17c5b0316d05871e95993c3fa
FileHash-SHA256	f889d2358eec85212659b0d273e5e892e610e114c990bfde93c9d607d85f58b0
FileHash-SHA256	7b722c66602e53d173163537fa66056a78e3043bfdddcb6fc06f31f1f7f25ed8
FileHash-SHA256	1e36dc2d6ca94e14dc7acc7c183d1cca3e05d6f01813c9a1918ef99f9caae693
FileHash-SHA256	70e2236e467d2b453e6c412d32d0bd0ab256603e50339b644d064de18dbcb539
FileHash-SHA256	c2e4f6d9c6afd91e6f85d2bc96c6096346bbcbadd6e1ba7192a9b226b17e67d8
FileHash-SHA256	27af16554281f3dd773e76768f13b099b41624bec5ab0405a09c26595a49e80e
FileHash-SHA256	87e5ab38b3e2bb5f63fd40d97a225f9dedb724b07038521ee4766a233f718ca2
FileHash-SHA256	cb136924562c2e70a5e3039ea3cd6713f4bd980df2795f6cdbc67d3364b5e79b
FileHash-SHA256	9d7edfa9834f4c5b5b35c04c7906993c330fc0a29382a69f9601793211ccf253

Indicator type	Indicator
FileHash-SHA256	43d469f38545b63389712eba636e87ad483308eb6ce609c1117a2fdddcefe1a2
FileHash-SHA256	a8d8a56cda7e29dd64cf28b2bdad19e8dcbf78e5900cf9ca53f952e9fd2452eb
FileHash-SHA256	0196bc9ac3db6f02cfa97323c8fce6cc7318b8f8fadb3e73bdf7971b3c541964
FileHash-SHA256	0ade4e834f34ed7693ebbe0354c668a6cb9821de581beaf1f3faae08150bd60d
FileHash-SHA256	23577ceb59f606ae17d9bdabaccefcb53dc2bac19619ce8a2d3d18ecb84bcacd
FileHash-SHA256	2ad362e25989b0b1911310345da90473df9053190737c456494b0c26613c8d1f
FileHash-SHA256	47bed59051a727911b050c2922874ae817e05860e4eee83b323f9feab710bf5c
FileHash-SHA256	553502bfe265a7e75a1d2202776fd816cabccfcdb200cc180dc507f4d45668d2
FileHash-SHA256	5a425372fac8e62d4b5d5be8054967eabe1e41894bcb8c10e431dd2e06203ca0
FileHash-SHA256	84aa777badab889d066e3a57c6a3d2096bc978c01499ea3dd8dd65fe44a3c98f
FileHash-SHA256	926d3f258fe2278bd1d220fafb33f246f9db9014204337f05a25d072bb644b6d
FileHash-SHA256	a9d9d7f6dd297af2bb3165ad0bfe3bbb88969393a3534bd33ef9aad062aefd05
FileHash-SHA256	b85536589c79648a10868b58075d7896ec09bbde43f9c4bad95ed82a200652bc
FileHash-SHA256	ec85e270c5cb159255a3178117197d275a6a90295fd31248b397dc03bcc4f3e4
URL	hxxp://email.gov.in.maildrive.email/?att=1581914657
URL	hxxp://email.gov.in.maildrive.email/?att=1579160420
hostname	email.gov.in.maildrive.email
domain	newsbizupdates.net
domain	uronlinestores.net
URL	hxxp://212.8.240.221:80/server/upload.php
URL	hxxp://www.tryanotherhorse.com
URL	hxxp://tryanotherhorse.com/config.txt
URL	hxxp://sharingmymedia.com/files/7All-Selected-list.xls
URL	hxxp://212.8.240.221:5987
URL	hxxp://sharemydrives.com/files/Laptop/wifeexchange.exe
URL	hxxp://sharingmymedia.com/files/Criteria-of-Army-Officers.doc
URL	hxxp://sharemydrives.com/files/Mobile/Desi-Porn.apk
hostname	www.tryanotherhorse.com
domain	fincruitconsulting.in
URL	hxxp://144.91.65.100:6102
URL	hxxp://mfahost.ddns.net/classical/

Indicator type	Indicator
URL	hxxp://164.68.108.22:6102
URL	hxxp://144.91.91.236:6102
URL	hxxp://192.185.129.21:443
hostname	vmi314646.contaboserver.net
hostname	vmi268056.contaboserver.net
hostname	vmi296708.contaboserver.netnewsindia.ddns.net
hostname	vmi312537.contaboserver.net
hostname	mfahost.ddns.net
domain	afgcloud7.com
domain	attachment.biz
domain	bbmsync2727.com
domain	hussainibuilder.com
domain	knockknock-jokes.com
domain	ordering-checks.com
domain	pradahandbagsshoes.com
domain	thefriendsmedia.com
URL	hxxp://176.10.136.96:4782
URL	hxxp://178.238.228.113:7861
URL	hxxp://178.238.228.113:9001
URL	hxxp://178.238.235.143:52399
URL	hxxp://178.238.235.143:52400
URL	hxxp://178.238.235.143:8688
URL	hxxp://178.238.235.143:9001
URL	hxxp://178.238.235.143:9999
URL	hxxp://191.101.23.190:5552
URL	hxxp://193.164.131.58:10000
URL	hxxp://193.37.152.28:9990
URL	hxxp://213.136.64.119:10101
URL	hxxp://213.136.87.122:10001
URL	hxxp://5.189.137.8:1453
URL	hxxp://5.189.143.225:11114
URL	hxxp://5.189.152.147:12200
URL	hxxp://5.189.167.23:7866
URL	hxxp://5.189.167.65:12010
URL	hxxp://80.241.221.109:10000
URL	hxxp://bhai1.ddns.net:10110
URL	hxxp://bhai1.ddns.net:3050
URL	hxxp://bbmsync2727.com/upd/ss1.dll
URL	hxxp://ordering-checks.com/bbm/bbm.exe
URL	hxxp://ordering-checks.com/bzu/ordc.exe
URL	hxxp://ordering-checks.com/cum/orc.crm
URL	hxxp://ordering-checks.com/cum/ordd.exe

Indicator type	Indicator
URL	hxxp://ordering-checks.com/ord/bb1j.exe
URL	hxxp://ordering-checks.com/ord/dc1j.exe
URL	hxxp://ordering-checks.com/patch2/perfect.exe
URL	hxxp://ordering-checks.com/sms/bbms.exe
URL	hxxp://ordering-checks.com/sms/ordapr.exe
URL	hxxp://thefriendsmedia.com/est/controller.exe
URL	hxxp://ordering-checks.com/bzu/ss.exe
hostname	bhai1.ddns.net
domain	drivestransfer.com
domain	iiaonline.in
domain	larsentobro.com
hostname	micrsoft.ddns.net
hostname	yepp.ddns.net
URL	hxxp://185.183.98.182:4701
URL	hxxp://drivestransfer.com/myfiles/Dinner%20Invitation.doc/win10/Dinner%20Invitation.doc
URL	hxxp://iiaonline.in/111.jpg
URL	hxxp://iiaonline.in/111.png
URL	hxxp://iiaonline.in/9999.jpg
URL	hxxp://iiaonline.in/DefenceLogo/theta.bmp
URL	hxxp://iiaonline.in/camela.bmp
URL	hxxp://iiaonline.in/merj.bmp
URL	hxxp://iiaonline.in/sasha.jpg
URL	hxxp://iiaonline.in/timon.jpeg
URL	hxxp://larsentobro.com/mbda/goliath1.bmp
URL	hxxp://larsentobro.com/mbda/mundkol
URL	hxxp://micrsoft.ddns.net:4313
URL	hxxp://yepp.ddns.net:4315

***Note**: All **http** is replaced with **hxxp**.

External Reference related to "Transparent Tribe" threat actor:

https://securelist.com/transparent-tribe-part-1/98127/

https://securelist.com/transparent-tribe-part-2/98233/

https://www.kaspersky.com/about/press-releases/2020_a-look-into-transparent-tribe-the-prolific-espionage-campaign-after-military-and-government-related-personnel

https://www.proofpoint.com/sites/default/files/proofpoint-operation-transparent-tribe-threat-insight-en.pdf