TECH BRIEF

Trend Micro Research

TREND MICRO

TgToxic Malware's Automated Framework Targets Southeast Asia Android Users

Appendix: Indicators of Compromise (IOCs)

Trend Micro Research

Indicators of Compromise (IOCs)

Hashes

SHA256	App ID	Label	Detection
000e84b8409035689d698c1273c215891095af7fb4a3708e46ba140f6a52b22c	10239	Coinbase Pro	AndroidOS_TgToxic
01615ea6b2590e6d508dba0ed7bd8e8a25ca75f2b026068c49606e2ee00ac450	10252	Shopee	AndroidOS_TgToxic
01cc0e25562153fa2d13666c87a54e1198163861ad0db2db4c9d9cb11820d984	10215	eporner	AndroidOS_TgToxic
020b294f417b847dc7d3be0630bf68e7a7befb506b56231cb85e13cf0d7d3c41	10216	1UBuy	AndroidOS_TgToxic
03dece0a6397a304d3fddedd1e69a074fa3f4fbf4cf37122437a6d69b12c9da5	10211	Seeks	AndroidOS_TgToxic
0548566d15b036be1d65e9ddcbff37663457659b9fba0e549a0a29fe67003fa2	10269	GASO	AndroidOS_TgToxic
0769917a7e705795603eb5e65e3bef216926da552cef8aadbb1da0fee5babceb	10223	Seeks	AndroidOS_TgToxic
0d79b5b899a3fc97944af0af2d7482506de6a5bec602478fce494b76f356779b	10209	KakaoTalk	AndroidOS_TgToxic
0ef7297896febdfd36e1ecca2df3093685d16805d02df3f049639de798bd126a	10253	Snapchat	AndroidOS_TgToxic
10a1a2b12b4f0efbdeec5b9b05bd6a7843b0edbd8e39d891738f601a43befed3	10229	Storm Gain	AndroidOS_TgToxic
11ce4b40040874199fca2718ca47dd77505ad46d68cebcdee8b32d42551fc349	10220	Viber	AndroidOS_TgToxic
14ab067d7f3c111cb6c9b262df283ac0101c2baaa53d2a3306f7e86cb7d05c87	10220	Snapchat	AndroidOS_TgToxic
169832b5f576ee0ca3724ffcc1c63f8d8f30daf38abd30121f4d2cae31ac3baa	10256	YOUNOW	AndroidOS_TgToxic
21e6a699b58dc20e84f4aa9a39b2adadaa81712a5d697b2d1c42faea4f981738	10253	Sweet meet	AndroidOS_TgToxic
255ebe0a8354ded9b6a91fc40b60bfeb036479af31c3a1d0ada3375d2ccc10d0	10235	Sweetheart	AndroidOS_TgToxic
26c3e6c0c4c145fa9c0852d4e48e60c7ba273774bf63873b6621f15b2aaea875	10215	eporner	AndroidOS_TgToxic
27a739d802e34dace763ff8ccb685b176632d9f552ae2e9fe6a900b6379269da	10212	Seeks	AndroidOS_TgToxic
2a38cb44855c7e18eaeb6e6b26effb865dbd2dee5029130a459ad673e6033c31	16800	Sweetheart	AndroidOS_TgToxic
2b794b1501f419cdf7a8a469f7aa4bf16aae50d0906d4b7b0d5c2a3ab32d5b30	18801	HiLive	AndroidOS_TgToxic
2d0145493ff634b9a1430bdd0c7e6a6abe6f853609086c07d2bcfbec4d0abe5f	10239	Stripchat	AndroidOS_TgToxic
314521e0f247a1fc7264fa69f0f325e73d4e102ecf510b89aae4a06b0c6ae366	10225	Snapchat	AndroidOS_TgToxic
32c1cba4b2147929bdcfffba91f25bd578338c41206963e509c66a463ea20d03	10239	Coinbase Pro	AndroidOS_TgToxic
43fcffe4cfc1003579b7f28f4fdfe825dab68bd5de3cabf8cbe2f5087fb651c4	10213	Lelive	AndroidOS_TgToxic
4a8ebd71981d48c0e1ddad42475673be7f9d88007ce495c971367b8a6c868a87	10282	Thai Red Cross	AndroidOS_TgToxic

4ea7c192cbdff0cffd8bf29aa19b9b6eb05e79c6dd1f90c8e6d03384c115b9b7	10207	Flirty Live	AndroidOS_TgToxic
599163b1c7628ca6971ee161e1376cb60ba75d62cff99b242f3eeec365bf6556	10235	Snapchat	AndroidOS_TgToxic
59b1b8aa0b6c027116a7e7d48ed7129402bd308b015fa7b89d00c5aa8d09d567	10265	Private Space	AndroidOS_TgToxic
62cd2720590023f60e1ec7276c8024a378f8e0190565c21eed03b47197553388	10209	Snapchat	AndroidOS_TgToxic
65c219ec188db941c66dc4f8a0917cded23682d710b0e89eada6bf3a8e917089	10260	VJOB	AndroidOS_TgToxic
677291429c4a2d8fc03795752fd32d9d94296a381942e5f0ed21d7eab37ae9b3	10220	Bumble	AndroidOS_TgToxic
68b967e0f96462873d7d5d77bfa7d895067882605b4d3a20f19572ee463e58e1	10255	Authenticator	AndroidOS_TgToxic
6a684902c4db6c804bde9f04e42185750fdc9f9ab6675385e42114dd1c51c275	10220	Snapchat	AndroidOS_TgToxic
6ba235a7538b220e62448e01aa20d189195c1667ef0beeef470843224ed70996	10263	Authenticator	AndroidOS_TgToxic
6f4e0366d95b02dc59b15d89201bde9baa0181b10c5f7de7b97cc6b075faeb96	10220	Snapchat	AndroidOS_TgToxic
6fa0c6b3e55ae87417eac523bb32ed3a8ac6f9683a70cef6f748a8765cc6eed7	10216	1UBuy	AndroidOS_TgToxic
6fa6a4ec95f1ba0063f7060d84b6ba507665150a5c30566ef19d9ea36673bd24	10218	lelive	AndroidOS_TgToxic
71e1280d6667fa0143a1e7932a9e1bb21938f52f565096eac4652da18c0edea6	10209	Snapchat	AndroidOS_TgToxic
79840344a231efa3f7b720e3526129129c6b068b982ea904ed11bb0865d31920	10266	성인 중계실	AndroidOS_TgToxic
84c6112d8cc2d2aec61a8611270ca9dbde11f252f34be614ab26024b77cdee9b	10262	near	AndroidOS_TgToxic
88f62ce8a3547a01b103dc973aefedbaeb0088ac328918ae3f5b60a51183492f	10222	Seeks	AndroidOS_TgToxic
8df9866138dbcf4e777b7f3606489733089bb13b405bff1df4e5dadc13e0c041	10239	Coinbase Pro	AndroidOS_TgToxic
93d412d799d61f0eb71fcc79e7592472f2f2ebbe9b3b657862e0fbd6961ba59c	10281	YYY	AndroidOS_TgToxic
98c7bfb823a912aacbd05904436a6a066144d4c7cccfb561f645c52775fd8347	10288	Skype	AndroidOS_TgToxic
9db60895407c5da8fd8949c50b099c758a42afc1d30448d0b79fec8e6223c169	10259	Signal	AndroidOS_TgToxic
9edf96755f3d148e04985c4377bc49dff8270cc1626d8777bc05c53fe9707274	10258	STRIPCHAT	AndroidOS_TgToxic
a010b3b9befa9b507d17fc99b38c7522016be4371f30a9cc615e9173f18e50ce	10236	Temu	AndroidOS_TgToxic
a09dabe974dcf4630d749e55a5e56a0824ce4047a44407921f9dbd1334821fc0	10209	Snapchat	AndroidOS_TgToxic
a26b0dea3e1663e823bd2287eb5b99811c0e3357c1a632112b534d4e74c963af	10213	Core Science	AndroidOS_TgToxic
a5d6b99e465d0fc22730301188a48090f7aac81796d02319421d969deb5d0857	10209	Snapchat	AndroidOS_TgToxic
a636a288c31cbbb5de9553d9a3aae73d302d7322c1b94854a583b2761ae5cb23	10238	Spiritone	AndroidOS_TgToxic
a85924f646dd74f918d65ada1e4cf3fd755c2dd4f14a6c8447a5a9ba5476aa2d	10215	eporner	AndroidOS_TgToxic

ad41768a22bdbb1612012793f29a73bab8c9f65e362ec9be7704a35c7199d48c	10223	Seeks	AndroidOS_TgToxic
b09c0572d470728f56d81d919de34eb72b978e8b0a01bfb557ab949b125b96be	10268	Moneta Markets	AndroidOS_TgToxic
b1546668f3ff35d7b509a8dc2dcb014891c814c34cfd1c5273c502636830a328	10280	1U BUY	AndroidOS_TgToxic
b36707eb435d5651bbf95ebb04024c32c757e535cdc59d8168d8a4628ac797aa	10221	Stripchat	AndroidOS_TgToxic
b611bb8d8617be791d45b9d9c47aae07820064e5ae659e129de005e8ed3f4fe7	10082	紓困	AndroidOS_TgToxic
b638e21da12d84673fc5be049f35d64848fc01008c2a866b9dc568d21616b5b2	10251	Flower dating	AndroidOS_TgToxic
bf1b2dbbf756501148b500a7714ec57c53b38375ff9d6eee4da9089f538e1a03	10220	Snapchat	AndroidOS_TgToxic
c1c7d5449849344a7a1786501820c1f5d629349a228818ad08b6b566a8878232	10220	Bumble	AndroidOS_TgToxic
c42ebd46610bbbb2327e27f48d9eec685d0f7b543ff36c9c376b38dfedf2ebb9	10207	LiveMe+	AndroidOS_TgToxic
c4b56d3566a7a670331482f5d851bcd25281fb66b924630994a2cbc7ebb41cd6	10261	Walmart	AndroidOS_TgToxic
d5de951f26f8cd8fb25100a3edd777d5ed3cae7756a1bec2af81a28dc53afbd6	10207	Flirty Live	AndroidOS_TgToxic
d887267dd40e47dbea8b3911e888e4da637598b095c388d9477957f77a6851ad	10212	Seeks	AndroidOS_TgToxic
d9c08cd79d16c35456c0c3f5ee4e57f34cfbdf0ea8769902358c45f278b7f52f	10232	Snapchat	AndroidOS_TgToxic
da14372d16a99fa6c4870182c41b3b0149be78f146bc5fd3384b3bc2186bdd59	10207	Seeks	AndroidOS_TgToxic
dbacbce478e87b4f93efdf1a40d045ab3dd6e337aaca8f05e4bb9ed6ce9943e7	10201	紓困	AndroidOS_TgToxic
de40a43629da3006547f57896f9a0417432b0c33ae03f1a9f2d7cca035c87d28	10216	1UBuy	AndroidOS_TgToxic
e2d9519337c6ede76c69e8a6e80479192bab7628c417fa0d227ff30cb362102e	10222	Seeks	AndroidOS_TgToxic
e5f1b4cc77b51c44564262de7e97cae36d84fe872db09b2ac9dfead71f2b4b98	10218	lelive	AndroidOS_TgToxic
e775c1bcc9f661845338d9e4c2249bd626a0fafb12bc9a88b0a4a4a90765c89d	10215	eporner	AndroidOS_TgToxic
eacac489a1fad1b2cabdcfa2aa7e3ab9893fc4edab15d71dd5e883d180b6e838	10218	夜色	AndroidOS_TgToxic
f0815f8fd98af572898a8a141c7830abf1e9a983d0e5bccd78251013a90b658c	10208	Moli	AndroidOS_TgToxic
f0815f8fd98af572898a8a141c7830abf1e9a983d0e5bccd78251013a90b658c	10208	Seeks	AndroidOS_TgToxic
463c2ea20c86dbc0052a6f99a271b4eeba5c9050d11b55a4a0ad13331fdb851b	10290	Skype	AndroidOS_TgToxic

Table 1. TgToxic hashes, Android app IDs, app labels, and Trend Micro detection names

URLs

URLs	Description
api.tw1988[.link	Command and control (C&C) server
de.jsp[.lol	Command and control (C&C) server
eu.ja7[.site	Command and control (C&C) server
hk1.jsp[.lol	Command and control (C&C) server
kr.ja7[.site	Command and control (C&C) server
kr.jsp[.lol	Command and control (C&C) server
sa.ja7[.site	Command and control (C&C) server
sa.jsp[.lol	Command and control (C&C) server
sg.ja7[.site	Command and control (C&C) server
sg5.ja7[.site	Command and control (C&C) server
test.gv2[.lol	Command and control (C&C) server
test.ja7[.site	Command and control (C&C) server
test.tw1988[.link	Command and control (C&C) server
us.ja7[.site	Command and control (C&C) server
uss.advertearn[.xyz	Command and control (C&C) server
hk.advertearn[.xyz	Command and control (C&C) server
ru.advertearn[.xyz	Command and control (C&C) server
usn.advertearn[.xyz	Command and control (C&C) server
usn.advertearn[.xyz	Command and control (C&C) server
eu.advertearn[.xyz	Command and control (C&C) server
kr.advertearn[.xyz	Command and control (C&C) server
sg.advertearn[.xyz	Command and control (C&C) server
au.advertearn[.xyz	Command and control (C&C) server
za.advertearn[.xyz	Command and control (C&C) server
sa.advertearn[.xyz	Command and control (C&C) server
arp[.lol	Malware delivery
asc[.lol	Malware delivery
avbgg[.com	Malware delivery
bb1[.lol	Malware delivery
bbk[.lol	Malware delivery
bf5[.lol	Malware delivery
bf5[.lol	Malware delivery
bf5[.one	Malware delivery
bf5[.xyz	Malware delivery
bmq[.lol	Malware delivery
bn3[.lol	Malware delivery
bnq[.lol	Malware delivery
bo6[.lol	Malware delivery

bpa[.lol	Malware delivery
btv[.lol	Malware delivery
cc2[.lol	Malware delivery
ccv[.lol	Malware delivery
coinbasepro[.win	Malware delivery
csn[.lol	Malware delivery
de1[.lol	Malware delivery
down.tw1988[.link	Malware delivery
dt2[.lol	Malware delivery
ee9[.lol	Malware delivery
egt[.lol	Malware delivery
etv[.lol	Malware delivery
fm9[.lol	Malware delivery
ggy[.lol	Malware delivery
gh7[.in	Malware delivery
gv2[.one	Malware delivery
hd5.[lol	Malware delivery
hd8[.site	Malware delivery
hdv[.one	Malware delivery
htv[.lol	Malware delivery
ime[.lol	Malware delivery
in1[.lol	Malware delivery
itv[.lol	Malware delivery
itw[.lol	Malware delivery
ja7[.mom	Malware delivery
jit[.lol	Malware delivery
jop[.lol	Malware delivery
kgu[.lol	Malware delivery
knk[.lol	Malware delivery
mm5[.lol	Malware delivery
mtv[.lol	Malware delivery
my2[.lol	Malware delivery
ngn[.lol	Malware delivery
okv[.lol	Malware delivery
oop[.wiki	Malware delivery
oup[.lol	Malware delivery
pi2[.lol	Malware delivery
pon[.lol	Malware delivery
puk[.lol	Malware delivery
py5[.lol	Malware delivery
py5[.one	Malware delivery

req[.lol	Malware delivery
soa[.lol	Malware delivery
soh[.lol	Malware delivery
ss3[.lol	Malware delivery
st7[.fun	Malware delivery
st7[.skin	Malware delivery
stripchatapp[.info	Malware delivery
stripchatapp[.net	Malware delivery
stripchatapp[.org	Malware delivery
suw[.lol	Malware delivery
t0i[.eu	Malware delivery
th7[.site	Malware delivery
thb[.lol	Malware delivery
thk[.lol	Malware delivery
ti7[.co	Malware delivery
ti7[.eu	Malware delivery
tk6[.lol	Malware delivery
tk6[.one	Malware delivery
tnb[.lol	Malware delivery
tv7[.site	Malware delivery
ty7[.site	Malware delivery
uue[.lol	Malware delivery
uuk[.lol	Malware delivery
v1i[.eu	Malware delivery
v2r[.lol	Malware delivery
vnc[.lol	Malware delivery
waz[.lol	Malware delivery
wew[.lol	Malware delivery
wmw[.lol	Malware delivery
xx6[.lol	Malware delivery
xxr[.lol	Malware delivery
yq5[.lol	Malware delivery
zos[.lol	Malware delivery
zzq[.lol	Malware delivery
dai.fasjit[.xyz	Phishing
dygov[.com	Phishing
fggov[.com	Phishing
gb7[.site	Phishing
hd8[.lol	Phishing
kegov[.com	Phishing
kggov[.com	Phishing

m.st0[.shop	Phishing
ougov[.com	Phishing
qegov[.com	Phishing
rrgov[.com	Phishing
tw1988[.cc	Phishing
tw1988[.co	Phishing
uigov[.com	Phishing
wugov[.com	Phishing
xigov[.com	Phishing
jump.gv2[.lol	Redirect to malicious websites via App ID
jump.ja7[.site	Redirect to malicious websites via App ID
jump.tw1988[.link	Redirect to malicious websites via App ID
jump.advertearn[.xyz	Redirect to malicious websites via App ID
ja7[.skin	Website statistics of tw1988[.link

Table 2. URLs and their respective descriptions