TECHNICAL APPENDIX

The indicators of compromise (IOCs) for **JAKU** can be found below. This is by no means an exhaustive list.

COMMAND-AND-CONTROL IP ADDRESSES

27.254.44.207
27.254.96.222
43.252.36.195
101.99.68.5
202.142.223.144
202.150.220.93

COMMAND-AND-CONTROL DOMAINS

bbsbox.strangled.net
benz.strangled.net
benz.wikaba.com
blog3.serveblog.net
boardchk.strangled.net
browny.ddns.net
combiz.user32.com
cometome.yourtrap.com
comix.mornor.com
cpanel.epismile.com.sg
cpanel.hash-tech.com
cpanel.roborobo.com.sg
cpanel244-webmail.newmediaexpress.com
cutemini.sexidude.com
decrypt.dnsd.info
decrypt.effers.com
decrypt.info.tm
dns53.ignorelist.com
file2.strangled.net
forum.bbsindex.com
forum.serveblog.net
ftp.mornor.com
mail.mailserverthai.com
mail.mornor.com
mailserverthai.com
minicooper.chickenkiller.com
minicooper.ddns.com
mob-adv.com
mor1.vps-leo.com
mor2.vps-roc.com
mornor.com
mornor.net
movie.flnet.org

movieadd.mooo.com
myforum.info.tm
ns1.thefince.com
ns2.thefince.com
pic.ezua.com
pic.zzux.com
pic3.mooo.com
sign.neon.org
sweetbrowny.mooo.com
torent.dnsd.info
torrent.dtdns.net
torrent.gotgeeks.com
torrent.serveblog.net
torrent1.coza.ro
torrent1.flnet.org
torrent3.bbsindex.com
torrentfiles.ddns.net
webmail.mailserverthai.com
winchk.bbsindex.com
www.bbsupdates.comxa.com
www.comix.mornor.com
www.mailserverthai.com
www.mob-adv.com
www.mornor.com
www.thefince.com

FIRST STAGE TORRENT INFECTED SOFTWARE

7e37bfbb3524361f06ff35ca82894eb95dad0be8
9bf3da2d2bd9306335ffd4a34dfa34400ff3ab7c
cfc60bdc35cc7d653fbd11b77522a890b1e04ff0
384b766477c67806c8faeef37f49beac8f46f8ae
9a2cc9384dc8b0b0d814d8df476cd3ae3665b390
e8c4b31b5b278a6c596818d0211cd017df1b730e
ba3f05bc02dffc7a1f857974bffd2cb99247b5af
eac5cd3410a33728260498bfcc15b5600a7efc90

FIRST STAGE MALWARE

5d2f372ace971267c28916ae4cb732aa105fc3b9
6b5ca84806966db8a8fc4ab4f84974f140a516a7
8feb968a996cdbebe27cf7dfafb1a51be15e7a3a
b305b998d44a319295f66785236735a00996aa36
407cff590a4492f375dc0e9fb41fd7705a482d03
1e1a440ae29d400afa951ed000b4e8010683892f

SECOND STAGE FAKE PNG PAYLOADS

ea3cfdc0b704b92918007c94d87d28e58d58e435
893706c71636bfe29ff72327a8b64db77d9a5460
36580913c831199e087b308958370ab477c8f64e
65d704604f21ffb3432378c468e3b02e54551209
ff3b413123b770c10d904bf0ef42662e4af9146f
54a15ea36d15699acda1f95e0c0ba2ec2c34d818

SECOND STAGE R2D3 MALWARE

da30c1a588e19d18a3e4b6878e3033ff2ef062cd
d2d2c2dca6ae4b7e0da167ae127b68c49efaa070

SECOND STAGE C3PRO MALWARE

c28bdea5e823cbca16d22a318ff29a338fcf0379

SECOND STAGE VIRUS INFECTOR MALWARE

bc6b34789c16487768d879b25ae8e94b416f0003

SECOND STAGE CLEAN UP MALWARE

cdcfb53b6cf8c92aebf98f6c78f92483194d9b9c