Linux Platform

SHA-256

003f4431743b69894b5d7988e53a37a7bad0b9cfe4248153e477b572af081786 - Backdoor.Linux.HELLOBOT.B
0f67c729100cb4872d56830ef5907448eddb9a34dac14f8ff62aece5d947c0a0 - Backdoor.Linux.HELLOBOT.B
11edea24abac633b9e7b8aae0965cd9cb56834a32d73d8bfe4fd1c009755f640 - Backdoor.Linux.HELLOBOT.B
18698365a4ba96d1a918f61b988291fc9eed80615518a72826b0bb92c6c90a06
1901008555ebe8cbd511f9e9dac40d59286556a46a372532bc124cfe231d9689 - Backdoor.Linux.HELLOBOT.B
2dd033d67ebed75bc5a2de24835bfd2440df98e4f3dc946b385cad6992e1aafe - Backdoor.Linux.HELLOBOT.B
466bfc2f13ca97dc805f6d48d28a8a1b96d250f919b3e9cc8d55b88bf24c3ecc - Backdoor.Linux.HELLOBOT.B
51371a402a13a4cdff55c79d52f2e560c46ca72ce7b4edf9ae55a721448a4512 - Backdoor.Linux.HELLOBOT.B
575d44db142d2ef2e280ecfafeacd4eb9e6562102426032080584e769086d774 - Backdoor.Linux.HELLOBOT.B
5bf94e591b100f7006d10197008675f3db3862e8bbef6e88107063cb6c858122 - Backdoor.Linux.HELLOBOT.B
68196d13e1e5e900eb6cffdbf5517c564905440fe76b0197ff44a505b4f48c13 - Backdoor.Linux.HELLOBOT.B
69fa10bf283474ca53295e0a7eff2fc07373092c1031581b748dce8aef7b6aea - Backdoor.Linux.HELLOBOT.B
6cc526fb8cd43f38011b46a2c0aea9905bd1ba554d2c4df950b370a95d0eda8d - Backdoor.Linux.HELLOBOT.B
70c3fd8ac880ffab91db3c81456639f226cf9a7ec8a851ad72406d7ddcc629d9 - Backdoor.Linux.HELLOBOT.B
778ee62d1df9f7bf5183e1d2f95ec4036bf5be80074ca333f4d4e85bee937c1c - Backdoor.Linux.HELLOBOT.B
79b8b383c848bbf940111eca00ddc47a0e8e9ac74ac006077cecb925a971d618 - Backdoor.Linux.HELLOBOT.B
79efad9e9b272a2cea0d328a881c7f6a1933b41a7d1468549dfc60c83a31037f - Backdoor.Linux.HELLOBOT.B
8388c17ce29399175c60bf689358e033eb03a696007e5856725bd0c205629436 -

Backdoor.Linux.HELLOBOT.B
951c97fa34c0f84d85ab7b9879860444f57e58d685156abe3d2a9a2f502fae7d -
Backdoor.Linux.HELLOBOT.B
960459363583458fa220540eb84cb73af157b03f835b4bf34b986ee4c3afe704 -
Trojan.Linux.XNOTE.A
9f40d4d53222e229a58c20473abaef7c0648c19fd0f13eb0f9ec841ed18f6ff3 -
Trojan.Linux.XNOTE.A
a5047dfc3e89935b982c4b5df91b56ae5e9d0bb557f84ef791352e54ab0077c2 -
Trojan.Linux.XNOTE.A
a7776eb4512d08e594854215aead32c4480091a7ca14870b793c290f1e36cfdb -
Trojan.Linux.XNOTE.A
b26ec8e98e05dc54779c1c91a9cf31aa40d757569074346548facdddd79c02fb -
Trojan.Linux.XNOTE.A
b33fb600d46309bafd31d3b056bbba816f5bac0f1024e774530f6c4320d3c5c2 -
Trojan.Linux.XNOTE.A
bc7e80232e28c680a585c3cc1125fb10862d338e5a4b94cdfdfb954df451621d -
Trojan.Unix.TOBOXHELL.A
c718d73ffbc182c2799f3999326486c93cd59d1e04b9676edf955a1324522a2c -
Trojan.Unix.TOBOXHELL.A
ca23b21cfd1fff75c3acec4c74020cfe013393983b997b3a7178f2e969b4a7bf -
Trojan.Linux.PATPOOTY.AA
d890db7136f72fa367aff0d1550f04034232a2fa3d97bae3a6516e3d5dcad056 -
Trojan.Linux.PATPOOTY.AA
e74632e3f010bce10de73b34f4dee68054207d7b12b1a0cf1820ce833e1b5991 -
Trojan.Linux.PATPOOTY.AA
eadd6ea80e727f78e91093097b4297a88a59100fcc19299b5ce4b5280db27cdc -
Trojan.Linux.PATPOOTY.AA
ebb8985880e911db8a498e20a269a00c07dbcfde2d077e88fe4b9d78a4deed7e -
Trojan.Linux.PATPOOTY.AA
ec42e1562fab95d0fbc86b3980cc392e368b50a4a150a2258d4293e4de1bc730 -
Trojan.Linux.PATPOOTY.AA
f646eb1685da341ccb3c1d5e4a14ae93f3271a84232708ee7234b44d4a834251 -
Trojan.Linux.PATPOOTY.AA
fb5434ff3030214c672226c52bc6883bf55c3129a5ee9b78ef5b2c773f8a1101 -
Trojan.Linux.PATPOOTY.AA
fd0f0841c8502dc03689ebb64dd9764e3772fc91400d1d2c9e81530bf5ad0b0f -
Trojan.Linux.REKOOBE.A

In-the-wild URLs

http://42[.]200.181.116/java

http://d[.]github.wiki/dust/amazon-hk

C&C

1.googie[.]ph:10050
1.googie[.]ph:1723
1.googie[.]ph:443
139[.]5.202[.]82:443
2.googie[.]ph:1723
2.googie[.]ph:443
3.googie[.]ph:5432
bos.github[.]wiki:443
darknet.rootkit[.]tools:8443
dust.github[.]wiki
gb.googie[.]ph:443
hkdust[.]github.wiki
linux[.]daj8.me:80
linux[.]shopingchina.net:80
linux[.]wy01.com:443
linux[.]wy01.vip
linux1[.]shopingchina.net:80
rootkit[.]tools
rootkit[.]tools:443
yabo[.]googie.ph:443