TREND MICRO | research

Back-to-Back Campaigns: Neko, Mirai, and Bashlite Malware Variants Use Various Exploits to Target Several Routers, Devices

Augusto Remillano II and Jakub Urbanec

Indicators of Compromise (IoCs)

Bashlite variant Ayedz

SHA-256 Hash	Detection Name
16ebe7836ce650db686ca62d62901b771788d8ef78b7ba0a10aa73e68a710dd5	Backdoor.Linux.BASHLITE.SMJC8
2efae6727d3f5a4a2e7b88ef1e657f6a6e2e6e1c08af0746205dc3c7afe4094d	
8e592655cef0dc4a1a209b6f8909a95e2bbf421ecf8312a3b4d07960fb906a5f	
abea038f41b83f00e61e829df39c4b85453335cb9a70619702a6b9834bc7d591	
a2c8e598e340cc7cc27b4c045129abd9b04ddd3a592c0c41ae5c82f777b59b30	Backdoor.Linux.BASHLITE.SMJC4
416dada9ab2ae2f160363965540d5776dc2fb4e086064d97d95a11c4a90c67cd	Backdoor.Linux.BASHLITE.SMJC
55355482d12b60136fde3f5d76b2686337e4bab5248e79cf3a6b2d652a290240	
b382dce55bbc08b0f5ac7bbb231e55bb65f07e795cd6d382d9bb01b293ef2233	
355df8452d6853cbf3ed44f82967d353b709b4bd04afb96de4c4a51471c0771d	
6df1610476044ab8c3e615ddaf66e51cfe5f4a3436f37ad15fa4f6583e83fe63	

c81cbf35dbbe2502b32ce02cc55c307b6036d9d10f7d7a0a6da127592caeaf0a f1571b3c47ab0aeff1e8094f2e1a1da604c6867409b8509ef90333ca1e9775e1	

Related URLs, IP Addresses, and Domains

- *167[.]71[.]7[.]231*

Mirai variant Asher

SHA-256 Hash	Detection Name
8cbcc1af312511ebaaba24a075333835e0ac4c4754072233bccadbb996d84048	
754285c82042ca8326be39988fceb39882d301fbcd3533ce31704027c445f72c	
5df2af777ba958b7180b71fc365595141582d8604eba7c70f635a38139503439	
7ca9af2d71719134aa7cf8ca37d9fe35f4b20f2e5d6721e1d57f6e570e845669	
86717399a76d07b72733abb2c88cefe2d2a8c3c451d758f7c8b5249ab21b9e26	
b3434897b35c52551329a2f8e322d1fc1be618959794d6f4bff299c7e1ce2324	
a9a5262048664843edf9e2bc405f06949cb9354ab20f5efb23dd2800c0dd4681	Backdoor.Linux.MIRAI.SMMR1

ebc2bb1901112c9f957855b25091c21f55a4c7d5f95b3d918f85c1924c8d31b0	
c3626284fb68b6bf76d212441d88a5a30ae5d98b13a63b9e7358efc8c1c42215	

Related URLs, IP Addresses, and Domains

- *104[.]168[.]215[.]139*
- *104.168.215.139/poo*
- *Cnc[.]rapeme[.]fun*
- *Scan[.]rapeme[.]fun*

Neko

SHA-256 Hash	Detection Name
30d429d048a4f6ec86f48b4cd0955e0003b832213694cfa121b95e4c429d7980	Backdoor.Linux.NEKO.AC
86aa444a10c9c0c33a8f94ad71fd9d2b985e2e624872cd1c351aeaa7a4d6645f	
329f507ceb4ed9d6a6cb5ba5e9bc6a863ef2fd12235f6ed5d46fe3ebc04cf337	Backdoor.Linux.NEKO.AB

Related URLs, IP Addresses, and Domains

- *hxxp://185.244.25.200/bins*
- *hxxp://185.244.25.200/bins/x86.neko*

Neko Kill List

- 902i13
- BzSxLxBxeY
- HOHO-LUGO7
- HOHO-U79OL
- JuYfouyf87
- NiGGeR69xd
- SO190Ij1X
- LOLKIKEEEDDE
- Ex0420
- ekjheory98e
- rzr
- EXTENDO
- scansh4
- MDMA
- fdevalvex
- scanspc
- MELTEDNINJAREALZ
- flexsonskids
- scanx86
- MISAKI-U79OL
- foAxi102kxe
- swodjwodjwoj
- MmKiy7f87l
- freecookiex86
- sysgpu
- frgege
- sysupdater
- 0DnAzepd
- NiGGeRD0nks69
- frgreu
- 0x766f6964
- NiGGeRd0nks1337
- gaft
- urasgbsigboa
- 120i3UI49
- OaF3
- geae
- vaiolmao

- 123123a
- Ofurain0n4H34D
- ggTrex
- ew
- wasads
- 1293194hjXD
- OthLaLosn
- ggt
- wget-log
- cupsddh
- 1337SoraLOADER
- SAIAKINA
- atddd
- sksapdd
- ggtq
- 1378bfp919GRB1Q2
- SAIAKUSO
- skysapdd
- ggtr
- 14Fa
- SEXSLAVE1337
- ggtt
- 1902a3u912u3u4
- haetrghbr
- 19ju3d
- SORAojkf120
- hehahejeje92
- 2U2JDJA901F91
- SlaVLav12
- helpmedaddthhhhh
- 2wgg9qphbq
- Slav3Th3seD3vices
- hzSmYZjYMQ
- 5Gbf
- sora
- SoRAxD123LOL
- iaGv
- 5aA3
- SoRAxD420LOL
- insomni
- 640277
- SoraBeReppin1337
- ipcamCache
- 66tlGg9Q
- jUYfouyf87
- 6ke3
- TOKYO3

- lyEeaXul2dULCVxh
- 93OfjHZ2z
- TY2gD6MZvKc7KU6r
- mMkiy6f87l
- A023UU4U24UIU
- TheWeeknd
- mioribitches
- A5p9
- TheWeeknds
- mnblkjpoi
- AbAd
- Tokyos
- neb
- Akiru
- U8inTz
- netstats
- Alex
- W9RCAKM20T
- newnetword
- Ayo215
- g1abc4dmo35hnp2lie0kjf
- Word
- nloads
- BAdAsV
- Wordmane
- notyakuzaa
- Belch
- Wordnets
- obp
- BigN0gg0r420
- X0102I34f
- ofhasfhiafhoi
- BzSxLxBxeY
- X19I239124UIU
- oism
- Deported
- XSHJEHHEIIHWO
- olsVNwo12
- DeportedDeported
- XkTer0GbA1
- onry0v03
- FortniteDownLOLZ
- Y0urM0mGay
- pussyfartlmaojk
- GrAcEnIgGeRaNn
- YvdGkqndCO
- qGeoRBe6BE

- GuiltyCrown
- ZEuS69
- s4beBsEQhd
- HOHO-KSNDO
- ZEuz69
- sat1234
- HOHO-LUGO7
- aj93hJ23
- scanHA
- alie293z0k2L
- scanJoshoARM
- HellInSide
- ayyyGangShit
- scanJoshoARM5
- HighFry
- b1gl
- scanJoshoARM6
- lWhPyucDbJ
- boatnetz
- scanJoshoARM7
- luYgujeIqn
- btbatrtah
- scanJoshoM68K
- JJDUHEWBBBIB
- scanJoshoMIPS
- JSDGIEVIVAVIG
- cKbVkzGOPa
- scanJoshoMPSL
- JuYfouyf87
- ccAD
- scanJoshoPPC
- KAZEN-OIU97
- chickenxings
- scanJoshoSH4
- yakuskzm8
- KAZEN-PO78H
- cleaner
- scanJoshoSPC
- KAZEN-U79OL
- dbeef
- scanJoshoX86
- yakuz4c24
- KETASHI32
- ddrwelper
- scanarm5
- zPnr6HpQj2
- Kaishi-Iz90Y

- deexec
- scanarm6
- zdrtfxcgy
- Katrina32
- doCP3fVj
- scanarm7
- zxcfhuio
- Ksif91je39
- scanm68k
- Kuasa
- dvrhelper
- scanmips
- KuasaBinsMate
- scanmpsl
- LOLHHHOHOHBUI
- eXK20CL12Z
- nya
- mezy
- QBotBladeSPOOKY
- hikariwashere
- 0DnAzepd
- p4029x91xx
- 32uhj4gbejh
- zhr
- lzrd
- PownedSecurity69
- ggt
- .ares
- fxlyazsxhy
- jnsd9sdoila
- BzSxLxBxeY
- yourmomgaeis
- sdfjiougsioj
- Oasis
- ggtr
- SEGRJIJHFVNHSNHEIHFOS
- apep999
- KOWAI-BAdAsV
- KOWAI-SAD
- jHKipU7YI
- airdropmalware
- your_verry_fucking_gay
- Big-Bro-Bright
- sefaexec
- shirololi
- eagle.
- For-Gai-Mezy

- 0x6axNL
- cloqkisvspooky
- myth
- SwergjmioG
- KILLEJW(IU(JIWERGFJGJWJRG
- Hetrh
- APEP
- wewrthe
- luFdKssCxz
- jSDFJIjio
- OnrYoXd666
- ewrtkjoketh
- ajbdf89wu823
- AAaasrdgs
- REKAI
- WsGA4@F6F
- GhostWuzHere666
- BOGOMIPS
- sfc6aJfluY
- Demon.
- xeno-is-god
- ICY-P-0ODIJ
- gSHUIHIfh
- wrgL
- hu87VhvQPz
- dakuexecbin
- TacoBellGodYo
- loligang
- PRIVMSG
- Execution
- orbitclient
- Amnesia
- Owari
- UnHAnaAW
- DUP
- Eats8
- z3hir
- obbo
- miori
- eagle
- MASUTA
- doxxRollie
- WHOIS
- KILLATTK
- daddyl33t
- lessie.
- sora

- 1gba4cdom53nhp12ei0kfj
- 9u123448u124au814d4x10
- hax.
- yakuza
- wordminer
- v[0v
- minerword
- SinixV4
- hoho
- g0dbu7tu
- orphic
- furasshu
- horizon
- assailant
- Ares
- Kawaiihelper
- ECHOBOT
- DEMONS
- kalon
- Josho
- daddyscum
- akira.ak
- Hilix
- daku
- Tsunami
- estella
- Solar
- rift
- _-255.Net
- Cayosin
- Okami
- sysupdater
- OnrYoXd666
- Kosha
- bushido
- trojan
- shiina
- Reaper.
- Corona.
- wrgnuwrijo
- Aka
- Hari
- orage
- fibre
- galil
- stresserpw
- stresser.pw

- Tohru
- Omni
- Josho
- kawaii
- Frosti
- sxj472sz
- HU6FIZTQU
- PFF1500RG
- plzjustfuckoff
- nvitpj
- elfLoad
- mioribitches
- Amakano
- tokupdater
- /dev/netslink/
- /dev/FTWDT101_watchdog
- cum-n-go
- oblivion
- Voltage
- Votan
- .anime
- scanppc

TREND MICRO™ RESEARCH

Trend Micro, a global leader in cybersecurity, helps to make the world safe for exchanging digital information.

Trend Micro Research is powered by experts who are passionate about discovering new threats, sharing key insights, and supporting efforts to stop cybercriminals. Our global team helps identify millions of threats daily, leads the industry in vulnerability disclosures, and publishes innovative research on new threats techniques. We continually work to anticipate new threats and deliver thought-provoking research.

www.trendmicro.com