An Analysis of the BabLock (aka Rorschach) Ransomware

SHA1 File name Detection name
3dd98117802d1992066188402ff63411f5a38c51 log.dll Trojan.Win64.DARKLOADER.YACE1
a571b70c6303e9144ed8a169bb0322e80226bcc5 log.dll
Trojan.Win64.DARKLOADER.SMYACE1
5953d721de1716fca88fa6472504dfde11ee3899 log.dll (N/A)
Trojan.Win64.DARKLOADER.SMYACE1
a8745ee6756e9288d88cc0a648c1ec06545f660e log.dll (N/A)
Trojan.Win64.DARKLOADER.SMYACE1
d39a35fefa9afb0ca1cfa19bcacae54b254d02ce log.dll (N/A)
Trojan.Win64.DARKLOADER.SMYACE1
48e3dc8b02426c433b4cc121b487110845a657cc ccl110u.dll
Trojan.Win64.DARKLOADER.YACE1
8ecaf752c5a9e57f496c951321415ca7ba470db6 ccL110U.dll
Trojan.Win64.DARKLOADER.YMCHAT
b8b21937d161363be05d3e7c43b9f3dbe11f807d ccL110U.dll (N/A)
Trojan.Win64.DARKLOADER.SMYACE1
e77b4b69ac5480f063c0cfc427536bac32cd7f88 libexpa.dll
Trojan.Win64.DARKLOADER.YMCHAT
88e3a57c8d8919aed0200c04b19e08660ca3262e libexpa.dll
Trojan.Win64.DARKLOADER.YMCHAT
8ef6d55e6ef2427c79f9a6ed5a3ecd1421fc75a9 libexpa.dll (N/A)
Trojan.Win64.DARKLOADER.SMYACE1
88e3a57c8d8919aed0200c04b19e08660ca3262e winutils.dll
Trojan.Win64.DARKLOADER.YADCGT
d50afee5b441e068439d74641a0a48311c0dfe8d fssync.dll (N/A)
Trojan.Win64.DARKLOADER.SMYACE1
e5c54ea9c51edba2c89da11e8bcf2ebd3f7869b4 1.bat (N/A) N/A
edc9f4eded2c57dee14595a2fba6aa3a98ff7b45 config.ini
Ransom.Win64.LOCKBIT.THFOABB.enc
4a8d3392b96092d766a9e05a7d92d990688b0ced config.ini
Ransom.Win64.LOCKBIT.YADCK.enc
24925b6b77fce4406da3002e52e464dd64eed407 config.ini
Ransom.Win64.LOCKBIT.THGOGBB.enc
4b430cf6c653b105654245964aae82665969fc02 config.ini

Ransom.Win64.LOCKBIT.THGOGBB.enc
72aa372424cf784c39674f78b89b9c1d3d9fd83c config.ini
Ransom.Win64.LOCKBIT.THGOGBB.enc
4a8d3392b96092d766a9e05a7d92d990688b0ced config.ini
Ransom.Win64.LOCKBIT.THGOGBB.enc
f2d340f0f9149896d49c76ac36f456c1ee8441fe config.ini (N/A) N/A
3af8e6446e77700a89d0777bb56bc1e172246339 config.ini (N/A) N/A
0c57807b967b79b10072d64565a8d5e7f428b63d 1.exe (N/A)
Troj.Win32.Gen.XXBM100FF015
28132fc26b567a517daa0d7b5ad8376af5ca885c 2.dll TrojanSpy.Win64.MIMIKATZ.YMCHAT
95c4130f6adb7eed6fbfdc0ce8394f4bbb66ab26 scvhost.exe (N/A)
HackTool.Win64.Chisel.SM.go
8e55377990128a9c3ba61a663a8540a8c56f8a54 svchost.exe HackTool.Win64.Kerbrute.SM
3ca3b27d7ab11331b3521cf9d86292473d7d02fa scvhost.exe
HackTool.Win64.CHISEL.YACE1T.go
97c3e38781848d9a15fc0bad0ab114c081a80b72 scvhost.exe (N/A)
Troj.Win32.Gen.XXBM100FF015
443e7cfb3956975708dd6b2ea74e9fe2f3d03bf8 f.exe (N/A) Troj.Win32.Gen.XXBM100FF015
7b5bf0930f60b6980a5f44db1357882e93e18dab f.exe (N/A)
Troj.Win32.Gen.XXBM100FF015
bb2a3404ec8baaadb353d5e41d384c800eaca6a3 f.exe (N/A)
Troj.Win32.Gen.XXBM100FF015
8347947476fb90799cb237008db7e34aaff2f8a2 f.exe (N/A) Troj.Win32.Gen.XXBM100FF015
d9c37fb4a69e05e2b74ee8080f04dd0683977482 f.exe (N/A)
Troj.Win32.Gen.XXBM100FF015
f3b984faeb58ad5ac862c7ca45cababaa78111b7 f.exe (N/A)
Troj.Win32.Gen.XXBM100FF015
700e3ce6cccdf0ab538d68ec53640c1b37866781 f.exe (N/A)
Troj.Win32.Gen.XXBM100FF015
be691f4a2aa619c31358e0159e07adf4b4ccd68a f.exe (N/A)
Troj.Win32.Gen.XXBM100FF015
45db28b53c615653734aa0bb1eb33fd46440843e f.exe (N/A)
Troj.Win32.Gen.XXBM100FF015
d02cc623ffedcea20330ebc5fdde9c24bd6e89d6 f.exe (N/A) Troj.Win32.Gen.XXBM100FF015
236e4f1bc6bf27e93a50fd9add6f12f2e49cc942 f.exe (N/A) Troj.Win32.Gen.XXBM100FF015
49c0a3595d0a314f105a9918181c57191c607026 f.exe (N/A)
Troj.Win32.Gen.XXBM100FF015
1ebba3accd925bc281fcc068c47483d99174c8bd f.exe (N/A)
Troj.Win32.Gen.XXBM100FF015
7ed2bd87d81f5243a1e0d07265bcf485c7d074ae f.exe (N/A)
Troj.Win32.Gen.XXBM100FF015
f18387dce0536aa8da897ac092f7812b0ff1f986 f.exe (N/A) Troj.Win32.Gen.XXBM100FF015

e936fcb964c206545dd8270d2cfaec963ac81dec f.exe (N/A)
Troj.Win32.Gen.XXBM100FF015
ee5b60d2b44df59e8c630b4d5ea9a87042022492 f.exe (N/A)
Troj.Win32.Gen.XXBM100FF015
c5199ceb7c69deca1a746f3a07dad096c148495a f.exe (N/A)
Troj.Win32.Gen.XXBM100FF015
443e7cfb3956975708dd6b2ea74e9fe2f3d03bf8 f.exe (N/A) Troj.Win32.Gen.XXBM100FF015