

Rootkit Umbreon / Umreon - x86, ARM samples

Archived: 2026-04-05 22:26:51 UTC

1.umbreon-ascii0B880E0F447CD5B6A8D295EFE40AFA376085 bytes (5.94 KiB)
2autoroot1C5FAEEC3D8C50FAC589CD0ADD0765C7281 bytes (281 bytes)
3CHANGELOGA1502129706BA19667F128B44D19DC3C11 bytes (11 bytes)
4cli.shC846143BDA087783B3DC6C244C2707DC5682 bytes (5.55 KiB)
5hideportsD41D8CD98F00B204E9800998ECF8427E0 bytes (bytes)Yes, of file promptlog
6install.sh9DE30162E7A8F0279E19C2C30280FFF85634 bytes (5.5 KiB)
7Makefile0F5B1E70ADC867DD3A22CA62644007E5797 bytes (797 bytes)
8portchecker006D162A0D0AA294C85214963A3D3145113 bytes (113 bytes)
9promptlogD41D8CD98F00B204E9800998ECF8427E0 bytes (bytes)
10readlink.c42FC7D7E2F9147AB3C18B0C4316AD3D81357 bytes (1.33 KiB)
11ReadMe.txtB7172B364BF5FB8B5C30FF528F6C51252244 bytes (2.19 KiB)
12setup694FFF4D2623CA7BB8270F5124493F37332 bytes (332 bytes)
13spytty.sh0AB776FA8A0FBED2EF26C9933C32E97C1011 bytes (1011 bytes)Yes, of file spytty.sh
14umbreon.c91706EF9717176DBB59A0F77FE95241C1007 bytes (1007 bytes)
15access.c7C0A86A27B322E63C3C29121788998B8713 bytes (713 bytes)
16audit.cA2B2812C80C93C9375BFB0D7BFCEFD5B1434 bytes (1.4 KiB)
17chown.cFF9B679C7AB3F57CFBBB852A13A350B22870 bytes (2.8 KiB)
18config.h980DEE60956A916AFC9D2997043D4887967 bytes (967 bytes)
19config.h.dist980DEE60956A916AFC9D2997043D4887967 bytes (967 bytes)Yes, of file config.h
20dirs.c46B20CC7DA2BDB9ECE65E36A4F987ABC3639 bytes (3.55 KiB)
21dlsym.c796DA079CC7E4BD7F6293136604DC07B4088 bytes (3.99 KiB)
22exec.c1935ED453FB83A0A538224AFAAC71B214033 bytes (3.94 KiB)
23getpath.h588603EF387EB617668B00EAFDAEA393183 bytes (183 bytes)
24getprocname.hF5781A9E267ED849FD4D2F5F3DFB8077805 bytes (805 bytes)
25includes.hF4797AE4B2D5B3B252E0456020F58E59629 bytes (629 bytes)
26kill.cC4BD132FC2FFBC84EA5103ABE6DC023D555 bytes (555 bytes)
27links.c898D73E1AC14DE657316F084AADA58A02274 bytes (2.22 KiB) 28local-
door.c76FC3E9E2758BAF48E1E9B442DB98BF8501 bytes (501 bytes)
29lpcap.hEA6822B23FE02041BE506ED1A182E5CB1690 bytes (1.65 KiB)
30maps.c9BCD90BEA8D9F9F6270CF2017F9974E21100 bytes (1.07 KiB)
31misc.h1F9FCC5D84633931CDD77B32DB1D50D02728 bytes (2.66 KiB)
32netstat.c00CF3F7E7EA92E7A954282021DD72DC41113 bytes (1.09 KiB)
33open.cF7EE88A523AD2477FF8EC17C9DCD7C028594 bytes (8.39 KiB)
34pam.c7A947FDC0264947B2D293E1F4D69684A2010 bytes (1.96 KiB)
35pam_private.h2C60F925842CEB42FFD639E7C763C7B012480 bytes (12.19 KiB)
36pam_vprompt.c017FB0F736A0BC65431A25E1A9D393FE3826 bytes (3.74 KiB)
37passwd.cA0D183BBE86D05E3782B5B24E2C964132364 bytes (2.31 KiB)

38pcap.cFF911CA192B111BD0D9368AFACA03C461295 bytes (1.26 KiB)
39procstat.c7B14E97649CD767C256D4CD6E4F8D452398 bytes (398 bytes)
40procstatus.c72ED74C03F4FAB0C1B801687BE200F063303 bytes (3.23 KiB)
41readwrite.cC068ED372DEAF8E87D0133EAC0A274A82710 bytes (2.65 KiB)
42rename.cC36BE9C01FEADE2EF4D5EA03BD2B3C05535 bytes (535 bytes)
43setgid.c5C023259F2C244193BDA394E2C0B8313667 bytes (667 bytes)
44sha256.h003D805D919B4EC621B800C6C239BAE0545 bytes (545 bytes)
45socket.c348AEF06AFA259BFC4E943715DB5A00B579 bytes (579 bytes)
46stat.cE510EE1F78BD349E02F47A7EB001B0E37627 bytes (7.45 KiB)
47syslog.c7CD3273E09A6C08451DD598A0F18B5701497 bytes (1.46 KiB)
48umbreon.hF76CAC6D564DEACFC6319FA167375BA54316 bytes (4.21 KiB) 49unhide-
funcs.c1A9F62B04319DA84EF71A1B091434C644729 bytes (4.62 KiB)
50cryptpass.py2EA92D6EC59D85474ED7A91C8518E7EC192 bytes (192 bytes)
51environment.sh70F467FE218E128258D7356B7CE328F11086 bytes (1.06 KiB) 52espeon-
connect.shA574C885C450FCA048E79AD6937FED2E247 bytes (247 bytes) 53espeon-
shell9EEF7E7E3C1BEE2F8591A088244BE0CB2167 bytes (2.12 KiB)
54espeon.c499FF5CF81C2624B0C3B0B7E9C6D980D14899 bytes (14.55 KiB)
55listen.sh69DA525AEA227BE9E4B8D59ACFF4D717209 bytes (209 bytes)
56spytty.sh0AB776FA8A0FBED2EF26C9933C32E97C1011 bytes (1011 bytes) 57ssh-
hidden.shAE54F343FE974302F0D31776B72D0987127 bytes (127 bytes)
58unfuck.c457B6E90C7FA42A7C46D464FBB1D68E2384 bytes (384 bytes) 59unhide-
self.pyB982597CEB7274617F286CA80864F499986 bytes (986 bytes)
60listen.shF5BD197F34E3D0BD8EA28B182CCE7270233 bytes (233 bytes)

Source: <http://contagiodump.blogspot.com/2018/03/rootkit-umbreon-umreon-x86-arm-samples.html>