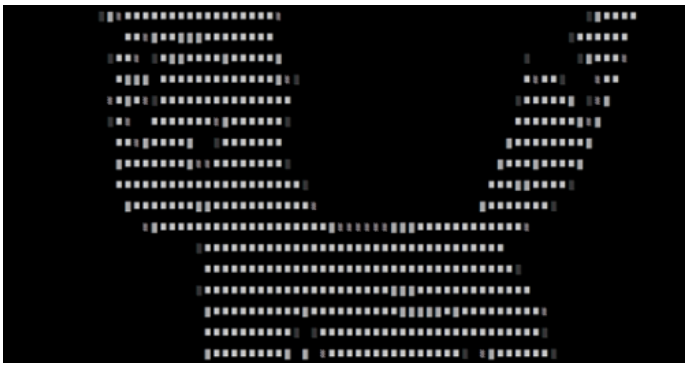
Rootkit Umbreon / Umreon - x86, ARM samples

contagiodump.blogspot.com/2018/03/rootkit-umbreon-umreon-x86-arm-samples.html




Pokémon-themed Umbreon Linux Rootkit Hits x86, ARM Systems

Research: Trend Micro

There are two packages
one is 'found in the wild' full and a set of hashes from Trend Micro (all but one file are already in the full package)

Download

Download Email me if you need the password

File information

Part one (full package)

#	File Name	Hash Value	File Size (on Disk)	Duplicate?
1	.umbreon-ascii	0B880E0F447CD5B6A8D295EFE40AFA37	6085 bytes (5.94 KiB)	
2	autoroot	1C5FAEEC3D8C50FAC589CD0ADD0765C7	281 bytes (281 bytes)	
3	CHANGELOG	A1502129706BA19667F128B44D19DC3C	11 bytes (11 bytes)	
4	cli.sh	C846143BDA087783B3DC6C244C2707DC	5682 bytes (5.55 KiB)	
5	hideports	D41D8CD98F00B204E9800998ECF8427E	0 bytes (bytes)	Yes, of file promptlog
6	install.sh	9DE30162E7A8F0279E19C2C30280FFF8	5634 bytes (5.5 KiB)	
7	Makefile	0F5B1E70ADC867DD3A22CA62644007E5	797 bytes (797 bytes)	
8	portchecker	006D162A0D0AA294C85214963A3D3145	113 bytes (113 bytes)	
9	promptlog	D41D8CD98F00B204E9800998ECF8427E	0 bytes (bytes)	
10	readlink.c	42FC7D7E2F9147AB3C18B0C4316AD3D8	1357 bytes (1.33 KiB)	
11	ReadMe.txt	B7172B364BF5FB8B5C30FF528F6C5125	2244 bytes (2.19 KiB)	
12	setup	694FFF4D2623CA7BB8270F5124493F37	332 bytes (332 bytes)	

#	File Name	Hash Value	File Size (on Disk)	Duplicate?
13	spytty.sh	0AB776FA8A0FBED2EF26C9933C32E97C	1011 bytes (1011 bytes)	Yes, of file spytty.sh
14	umbreon.c	91706EF9717176DBB59A0F77FE95241C	1007 bytes (1007 bytes)	
15	access.c	7C0A86A27B322E63C3C29121788998B8	713 bytes (713 bytes)	
16	audit.c	A2B2812C80C93C9375BFB0D7BFCEFD5B	1434 bytes (1.4 KiB)	
17	chown.c	FF9B679C7AB3F57CFBBB852A13A350B2	2870 bytes (2.8 KiB)	
18	config.h	980DEE60956A916AFC9D2997043D4887	967 bytes (967 bytes)	
19	config.h.dist	980DEE60956A916AFC9D2997043D4887	967 bytes (967 bytes)	Yes, of file config.h
20	dirs.c	46B20CC7DA2BDB9ECE65E36A4F987ABC	3639 bytes (3.55 KiB)	
21	dlsym.c	796DA079CC7E4BD7F6293136604DC07B	4088 bytes (3.99 KiB)	
22	exec.c	1935ED453FB83A0A538224AFAAC71B21	4033 bytes (3.94 KiB)	
23	getpath.h	588603EF387EB617668B00EAFDAEA393	183 bytes (183 bytes)	
24	getprocname.h	F5781A9E267ED849FD4D2F5F3DFB8077	805 bytes (805 bytes)	
25	includes.h	F4797AE4B2D5B3B252E0456020F58E59	629 bytes (629 bytes)	
26	kill.c	C4BD132FC2FFBC84EA5103ABE6DC023D	555 bytes (555 bytes)	
27	links.c	898D73E1AC14DE657316F084AADA58A0	2274 bytes (2.22 KiB)	
28	local-door.c	76FC3E9E2758BAF48E1E9B442DB98BF8	501 bytes (501 bytes)	
29	lpcap.h	EA6822B23FE02041BE506ED1A182E5CB	1690 bytes (1.65 KiB)	
30	maps.c	9BCD90BEA8D9F9F6270CF2017F9974E2	1100 bytes (1.07 KiB)	
31	misc.h	1F9FCC5D84633931CDD77B32DB1D50D0	2728 bytes (2.66 KiB)	
32	netstat.c	00CF3F7E7EA92E7A954282021DD72DC4	1113 bytes (1.09 KiB)	
33	open.c	F7EE88A523AD2477FF8EC17C9DCD7C02	8594 bytes (8.39 KiB)	
34	pam.c	7A947FDC0264947B2D293E1F4D69684A	2010 bytes (1.96 KiB)	
35	pam_private.h	2C60F925842CEB42FFD639E7C763C7B0	12480 bytes (12.19 KiB)	
36	pam_vprompt.c	017FB0F736A0BC65431A25E1A9D393FE	3826 bytes (3.74 KiB)	
37	passwd.c	A0D183BBE86D05E3782B5B24E2C96413	2364 bytes (2.31 KiB)	
38	pcap.c	FF911CA192B111BD0D9368AFACA03C46	1295 bytes (1.26 KiB)	
39	procstat.c	7B14E97649CD767C256D4CD6E4F8D452	398 bytes (398 bytes)	
40	procstatus.c	72ED74C03F4FAB0C1B801687BE200F06	3303 bytes (3.23 KiB)	
41	readwrite.c	C068ED372DEAF8E87D0133EAC0A274A8	2710 bytes (2.65 KiB)	
42	rename.c	C36BE9C01FEADE2EF4D5EA03BD2B3C05	535 bytes (535 bytes)	
43	setgid.c	5C023259F2C244193BDA394E2C0B8313	667 bytes (667 bytes)	
44	sha256.h	003D805D919B4EC621B800C6C239BAE0	545 bytes (545 bytes)	
45	socket.c	348AEF06AFA259BFC4E943715DB5A00B	579 bytes (579 bytes)	
46	stat.c	E510EE1F78BD349E02F47A7EB001B0E3	7627 bytes (7.45 KiB)	
47	syslog.c	7CD3273E09A6C08451DD598A0F18B570	1497 bytes (1.46 KiB)	
48	umbreon.h	F76CAC6D564DEACFC6319FA167375BA5	4316 bytes (4.21 KiB)	
49	unhide-funcs.c	1A9F62B04319DA84EF71A1B091434C64	4729 bytes (4.62 KiB)	
50	cryptpass.py	2EA92D6EC59D85474ED7A91C8518E7EC	192 bytes (192 bytes)	

#	File Name	Hash Value	File Size (on Disk)	Duplicate?
51	environment.sh	70F467FE218E128258D7356B7CE328F1	1086 bytes (1.06 KiB)	
52	espeon-connect.sh	A574C885C450FCA048E79AD6937FED2E	247 bytes (247 bytes)	
53	espeon-shell	9EEF7E7E3C1BEE2F8591A088244BE0CB	2167 bytes (2.12 KiB)	
54	espeon.c	499FF5CF81C2624B0C3B0B7E9C6D980D	14899 bytes (14.55 KiB)	
55	listen.sh	69DA525AEA227BE9E4B8D59ACFF4D717	209 bytes (209 bytes)	
56	spytty.sh	0AB776FA8A0FBED2EF26C9933C32E97C	1011 bytes (1011 bytes)	
57	ssh-hidden.sh	AE54F343FE974302F0D31776B72D0987	127 bytes (127 bytes)	
58	unfuck.c	457B6E90C7FA42A7C46D464FBF1D68E2	384 bytes (384 bytes)	
59	unhide-self.py	B982597CEB7274617F286CA80864F499	986 bytes (986 bytes)	
60	listen.sh	F5BD197F34E3D0BD8EA28B182CCE7270	233 bytes (233 bytes)	

part 2 (those listed in the Trend Micro article)

#	File Name	Hash Value	File Size (on Disk)
1	015a84eb1d18beb310e7aeeceab8b84776078935c45924b3a10aa884a93e28ac	A47E38464754289C0F4A55ED7BB55648	9375 bytes (9.16 KiB)
2	0751cf716ea9bc18e78eb2a82cc9ea0cac73d70a7a74c91740c95312c8a9d53a	F9BA2429EAE5471ACDE820102C5B8159	7512 bytes (7.34 KiB)
3	0a4d5ffb1407d409a55f1aed5c5286d4f31fe17bc99eabff64aa1498c5482a5f	0AB776FA8A0FBED2EF26C9933C32E97C	1011 bytes (1011 bytes)
4	0ce8c09bb6ce433fb8b388c369d7491953cf9bb5426a7bee752150118616d8ff	B982597CEB7274617F286CA80864F499	986 bytes (986 bytes)
5	122417853c1eb1868e429cacc499ef75cfc018b87da87b1f61bff53e9b8e8670	9EEF7E7E3C1BEE2F8591A088244BE0CB	2167 bytes (2.12 KiB)
6	409c90ecd56e9abcb9f290063ec7783ecbe125c321af3f8ba5dcbde6e15ac64a	B4746BB5E697F23A5842ABCAED36C914	6149 bytes (6 KiB)
7	4fc4b5dab105e03f03ba3ec301bab9e2d37f17a431dee7f2e5a8dfadcca4c234	D0D97899131C29B3EC9AE89A6D49A23E	65160 bytes (63.63 KiB)
8	8752d16e32a611763eee97da6528734751153ac1699c4693c84b6e9e4fb08784	E7E82D29DFB1FC484ED277C702187818	55564 bytes (54.26 KiB)
9	991179b6ba7d4aeabdf463118e4a2984276401368f4ab842ad8a5b8b73088522	2B1863ACDC0068ED5D50590CF792DF05	7664 bytes (7.48 KiB)

#	File Name	Hash Value	File Size (on Disk)
10	a378b85f8f41de164832d27ebf7006370c1fb8eda23bb09a3586ed29b5dbdddf	A977F68C59040E40A822C384D1CEDEB6	176 bytes (176 bytes)
11	aa24deb830a2b1aa694e580c5efb24f979d6c5d861b56354a6acb1ad0cf9809b	DF320ED7EE6CCF9F979AEFE451877FFC	26 bytes (26 bytes)
12	acfb014304b6f2cff00c668a9a2a3a9cbb6f24db6d074a8914dd69b43afa4525	84D552B5D22E40BDA23E6587B1BC532D	6852 bytes (6.69 KiB)
13	c80d19f6f3372f4cc6e75ae1af54e8727b54b51aaf2794fedd3a1aa463140480	087DD79515D37F7ADA78FF5793A42B7B	11184 bytes (10.92 KiB)
14	e9bce46584acbf59a779d1565687964991d7033d63c06bddabcfc4375c5f1853	BBEB18C0C3E038747C78FCAB3E0444E3	71940 bytes (70.25 KiB)