File Name	Log entry	Log ID	Timestamp	Event Type	Action	Username	Target Path/File
Corrupt.vlog	!!MALFORMED!!DATA!! 0xXYZ[ts:BADTIMESTAMP]|EVNT:???	0xXYZ : not a valid	[ts:BADTIMESTAMP] : not valid or corrupted	EVNT:??? : missing	-	-	-
Session_1.vlog	0x0[ts:7716948]|EVNT:XR-EXEC!@RUN_usr:tara4=>/usr/lib/xrun.conf	0x0	7716948	XR-EXEC	RUN	tara4	/usr/lib/xrun.conf
	0x1[ts:7716950]|EVNT:XR-LOG!@OPN_usr:odinX=>/opt/secure.shd	0x1	7716950	XR-LOG	OPN	odinX	/opt/secure.shd
	0x2[ts:7716952]|EVNT:XR-CONN!@IP:224.43.154.138	0x2	7716952	XR-CONN	CONN (Connection Established)	—	224.43.154.138 (IP)
	0x3[ts:7716954]|EVNT:XR-DEL!@DEL_usr:tara4=>/tmp/init.sock	0x3	7716954	XR-DEL	DEL	tara4	/tmp/init.sock
	0x4[ts:7716956]|EVNT:XR-DEL!@DEL_usr:odinX=>/bin/xz	0x4	7716956	XR-DEL	DEL	odinX	/bin/xz
	0x5[ts:7716958]|EVNT:XR-EXEC!@RUN_usr:xav23=>/bin/xz	0x5	7716958	XR-EXEC	RUN	xav23	/bin/xz
	0x6[ts:7716960]|EVNT:XR-CONN!@IP:13.213.192.184	0x6	7716960	XR-CONN	CONN	—	13.213.192.184 (IP)
	0x7[ts:7716962]|EVNT:XR-FILE!@MOD_usr:xav23=>/etc/passwd	0x7	7716962	XR-FILE	MOD	xav23	/etc/passwd
	0x8[ts:7716964]|EVNT:XR-EXEC!@RUN_usr:mira01=>/usr/lib/xrun.conf	0x8	7716964	XR-EXEC	RUN	mira01	/usr/lib/xrun.conf
	0x9[ts:7716966]|EVNT:XR-CONN!@IP:189.11.80.156	0x9	7716966	XR-CONN	CONN	—	189.11.80.156 (IP)
	0xA[ts:7716968]|EVNT:XR-LOG!@OPN_usr:odinX=>/bin/xz	0xA	7716968	XR-LOG	OPN	odinX	/bin/xz
	0xB[ts:7716970]|EVNT:XR-FILE!@MOD_usr:neo99=>/etc/passwd	0xB	7716970	XR-FILE	MOD	neo99	/etc/passwd
	0xC[ts:7716972]|EVNT:XR-FILE!@MOD_usr:xav23=>/usr/lib/xrun.conf	0xC	7716972	XR-FILE	MOD	xav23	/usr/lib/xrun.conf
	0xD[ts:7716974]|EVNT:XR-SHDW!@KILL_proc:pid4027	0xD	7716974	XR-SHDW	KILL	—	pid4027
	0xE[ts:7716976]|EVNT:XR-LOG!@OPN_usr:xav23=>/etc/passwd	0xE	7716976	XR-LOG	OPN	xav23	/etc/passwd
	0xF[ts:7716978]|EVNT:XR-FILE!@MOD_usr:tara4=>/usr/lib/xrun.conf	0xF	7716978	XR-FILE	MOD	tara4	/usr/lib/xrun.conf
	0x10[ts:7716980]|EVNT:XR-EXEC!@RUN_usr:tara4=>/usr/lib/xrun.conf	0x10	7716980	XR-EXEC	RUN	tara4	/usr/lib/xrun.conf
	0x11[ts:7716982]|EVNT:XR-EXEC!@RUN_usr:mira01=>/bin/xz	0x11	7716982	XR-EXEC	RUN	mira01	/bin/xz
	0x12[ts:7716984]|EVNT:XR-EXEC!@RUN_usr:xav23=>/etc/passwd	0x12	7716984	XR-EXEC	RUN	xav23	/etc/passwd
	0x13[ts:7716986]|EVNT:XR-SHDW!@KILL_proc:pid5520	0x13	7716986	XR-SHDW	KILL	—	pid5520
	0x14[ts:7716988]|EVNT:XR-CONN!@IP:205.104.47.81	0x14	7716988	XR-CONN	CONN	—	205.104.47.81 (IP)
	0x15[ts:7716990]|EVNT:XR-SHDW!@KILL_proc:pid5626	0x15	7716990	XR-SHDW	KILL	—	pid5626
	0x16[ts:7716992]|EVNT:XR-FILE!@MOD_usr:xav23=>/etc/passwd	0x16	7716992	XR-FILE	MOD	xav23	/etc/passwd
	0x17[ts:7716994]|EVNT:XR-FILE!@MOD_usr:odinX=>/usr/lib/xrun.conf	0x17	7716994	XR-FILE	MOD	odinX	/usr/lib/xrun.conf
	0x18[ts:7716996]|EVNT:XR-CONN!@IP:219.192.55.249	0x18	7716996	XR-CONN	CONN	—	219.192.55.249 (IP)
	0x19[ts:7716998]|EVNT:XR-SHDW!@KILL_proc:pid3513	0x19	7716998	XR-SHDW	KILL	—	pid3513
	0x1A[ts:7717000]|EVNT:XR-CONN!@IP:104.124.103.65	0x1A	7717000	XR-CONN	CONN	—	104.124.103.65 (IP)
	0x1B[ts:7717002]|EVNT:XR-CONN!@IP:24.252.18.16	0x1B	7717002	XR-CONN	CONN	—	24.252.18.16 (IP)
	0x1C[ts:7717004]|EVNT:XR-DEL!@DEL_usr:tara4=>/usr/lib/xrun.conf	0x1C	7717004	XR-DEL	DEL	tara4	/usr/lib/xrun.conf
	0x1D[ts:7717006]|EVNT:XR-FILE!@MOD_usr:neo99=>/opt/secure.shd	0x1D	7717006	XR-FILE	MOD	neo99	/opt/secure.shd
	0x1E[ts:7717008]|EVNT:XR-LOG!@OPN_usr:odinX=>/bin/xz	0x1E	7717008	XR-LOG	OPN	odinX	/bin/xz
	0x1F[ts:7717010]|EVNT:XR-LOG!@OPN_usr:tara4=>/usr/lib/xrun.conf	0x1F	7717010	XR-LOG	OPN	tara4	/usr/lib/xrun.conf
	0x20[ts:7717012]|EVNT:XR-DEL!@DEL_usr:mira01=>/tmp/init.sock	0x20	7717012	XR-DEL	DEL	mira01	/tmp/init.sock
	0x21[ts:7717014]|EVNT:XR-SHDW!@KILL_proc:pid5307	0x21	7717014	XR-SHDW	KILL	—	pid5307
	0x22[ts:7717016]|EVNT:XR-DEL!@DEL_usr:odinX=>/etc/passwd	0x22	7717016	XR-DEL	DEL	odinX	/etc/passwd
	0x23[ts:7717018]|EVNT:XR-DEL!@DEL_usr:neo99=>/opt/secure.shd	0x23	7717018	XR-DEL	DEL	neo99	/opt/secure.shd
	0x24[ts:7717020]|EVNT:XR-EXEC!@RUN_usr:mira01=>/bin/xz	0x24	7717020	XR-EXEC	RUN	mira01	/bin/xz
	0x25[ts:7717022]|EVNT:XR-EXEC!@RUN_usr:xav23=>/usr/lib/xrun.conf	0x25	7717022	XR-EXEC	RUN	xav23	/usr/lib/xrun.conf
	0x26[ts:7717024]|EVNT:XR-FILE!@MOD_usr:odinX=>/tmp/init.sock	0x26	7717024	XR-FILE	MOD	odinX	/tmp/init.sock
	0x27[ts:7717026]|EVNT:XR-CONN!@IP:131.110.180.152	0x27	7717026	XR-CONN	CONN	—	131.110.180.152 (IP)
	0x28[ts:7717028]|EVNT:XR-DEL!@DEL_usr:mira01=>/etc/passwd	0x28	7717028	XR-DEL	DEL	mira01	/etc/passwd
	0x29[ts:7717030]|EVNT:XR-EXEC!@RUN_usr:odinX=>/opt/secure.shd	0x29	7717030	XR-EXEC	RUN	odinX	/opt/secure.shd
	0x2A[ts:7717032]|EVNT:XR-EXEC!@RUN_usr:mira01=>/bin/xz	0x2A	7717032	XR-EXEC	RUN	mira01	/bin/xz
	0x2B[ts:7717034]|EVNT:XR-CONN!@IP:137.146.86.102	0x2B	7717034	XR-CONN	CONN	—	137.146.86.102 (IP)
	0x2C[ts:7717036]|EVNT:XR-FILE!@MOD_usr:tara4=>/usr/lib/xrun.conf	0x2C	7717036	XR-FILE	MOD	tara4	/usr/lib/xrun.conf
	0x2D[ts:7717038]|EVNT:XR-FILE!@MOD_usr:tara4=>/etc/passwd	0x2D	7717038	XR-FILE	MOD	tara4	/etc/passwd
	0x2E[ts:7717040]|EVNT:XR-LOG!@OPN_usr:mira01=>/opt/secure.shd	0x2E	7717040	XR-LOG	OPN	mira01	/opt/secure.shd
	0x2F[ts:7717042]|EVNT:XR-FILE!@MOD_usr:tara4=>/bin/xz	0x2F	7717042	XR-FILE	MOD	tara4	/bin/xz
	0x30[ts:7717044]|EVNT:XR-SHDW!@KILL_proc:pid3508	0x30	7717044	XR-SHDW	KILL	—	pid3508
	0x31[ts:7717046]|EVNT:XR-LOG!@OPN_usr:mira01=>/etc/passwd	0x31	7717046	XR-LOG	OPN	mira01	/etc/passwd

session_2.vlog	0x0[ts:7664148]|EVNT:XR-CONN!@IP:39.62.133.75	0x0	7664148	XR-CONN	CONN	—	39.62.133.75 (IP)
	0x1[ts:7664150]|EVNT:XR-EXEC!@RUN_usr:odinX=>/tmp/init.sock	0x1	7664150	XR-EXEC	RUN	odinX	/tmp/init.sock
	0x2[ts:7664152]|EVNT:XR-FILE!@MOD_usr:mira01=>/etc/passwd	0x2	7664152	XR-FILE	MOD	mira01	/etc/passwd
	0x3[ts:7664154]|EVNT:XR-DEL!@DEL_usr:neo99=>/usr/lib/xrun.conf	0x3	7664154	XR-DEL	DEL	neo99	/usr/lib/xrun.conf
	0x4[ts:7664156]|EVNT:XR-FILE!@MOD_usr:odinX=>/tmp/init.sock	0x4	7664156	XR-FILE	MOD	odinX	/tmp/init.sock
	0x5[ts:7664158]|EVNT:XR-EXEC!@RUN_usr:odinX=>/opt/secure.shd	0x5	7664158	XR-EXEC	RUN	odinX	/opt/secure.shd
	0x6[ts:7664160]|EVNT:XR-CONN!@IP:236.9.201.102	0x6	7664160	XR-CONN	CONN	—	236.9.201.102 (IP)
	0x7[ts:7664162]|EVNT:XR-CONN!@IP:147.242.164.155	0x7	7664162	XR-CONN	CONN	—	147.242.164.155 (IP)
	0x8[ts:7664164]|EVNT:XR-LOG!@OPN_usr:xav23=>/usr/lib/xrun.conf	0x8	7664164	XR-LOG	OPN	xav23	/usr/lib/xrun.conf
	0x9[ts:7664166]|EVNT:XR-SHDW!@KILL_proc:pid9182	0x9	7664166	XR-SHDW	KILL	—	pid9182
	0xA[ts:7664168]|EVNT:XR-LOG!@OPN_usr:neo99=>/usr/lib/xrun.conf	0xA	7664168	XR-LOG	OPN	neo99	/usr/lib/xrun.conf
	0xB[ts:7664170]|EVNT:XR-DEL!@DEL_usr:odinX=>/bin/xz	0xB	7664170	XR-DEL	DEL	odinX	/bin/xz
	0xC[ts:7664172]|EVNT:XR-DEL!@DEL_usr:mira01=>/tmp/init.sock	0xC	7664172	XR-DEL	DEL	mira01	/tmp/init.sock
	0xD[ts:7664174]|EVNT:XR-DEL!@DEL_usr:tara4=>/bin/xz	0xD	7664174	XR-DEL	DEL	tara4	/bin/xz
	0xE[ts:7664176]|EVNT:XR-DEL!@DEL_usr:xav23=>/etc/passwd	0xE	7664176	XR-DEL	DEL	xav23	/etc/passwd
	0xF[ts:7664178]|EVNT:XR-LOG!@OPN_usr:mira01=>/usr/lib/xrun.conf	0xF	7664178	XR-LOG	OPN	mira01	/usr/lib/xrun.conf
	0x10[ts:7664180]|EVNT:XR-CONN!@IP:133.202.249.92	0x10	7664180	XR-CONN	CONN	—	133.202.249.92 (IP)
	0x11[ts:7664182]|EVNT:XR-DEL!@DEL_usr:xav23=>/tmp/init.sock	0x11	7664182	XR-DEL	DEL	xav23	/tmp/init.sock
	0x12[ts:7664184]|EVNT:XR-CONN!@IP:199.40.234.167	0x12	7664184	XR-CONN	CONN	—	199.40.234.167 (IP)
	0x13[ts:7664186]|EVNT:XR-FILE!@MOD_usr:tara4=>/opt/secure.shd	0x13	7664186	XR-FILE	MOD	tara4	/opt/secure.shd
	0x14[ts:7664188]|EVNT:XR-CONN!@IP:78.50.247.114	0x14	7664188	XR-CONN	CONN	—	78.50.247.114 (IP)
	0x15[ts:7664190]|EVNT:XR-EXEC!@RUN_usr:neo99=>/usr/lib/xrun.conf	0x15	7664190	XR-EXEC	RUN	neo99	/usr/lib/xrun.conf
	0x16[ts:7664192]|EVNT:XR-EXEC!@RUN_usr:odinX=>/bin/xz	0x16	7664192	XR-EXEC	RUN	odinX	/bin/xz
	0x17[ts:7664194]|EVNT:XR-DEL!@DEL_usr:neo99=>/bin/xz	0x17	7664194	XR-DEL	DEL	neo99	/bin/xz
	0x18[ts:7664196]|EVNT:XR-SHDW!@KILL_proc:pid6274	0x18	7664196	XR-SHDW	KILL	—	pid6274
	0x19[ts:7664198]|EVNT:XR-LOG!@OPN_usr:xav23=>/etc/passwd	0x19	7664198	XR-LOG	OPN	xav23	/etc/passwd
	0x1A[ts:7664200]|EVNT:XR-LOG!@OPN_usr:mira01=>/bin/xz	0x1A	7664200	XR-LOG	OPN	mira01	/bin/xz
	0x1B[ts:7664202]|EVNT:XR-DEL!@DEL_usr:odinX=>/etc/passwd	0x1B	7664202	XR-DEL	DEL	odinX	/etc/passwd
	0x1C[ts:7664204]|EVNT:XR-LOG!@OPN_usr:neo99=>/etc/passwd	0x1C	7664204	XR-LOG	OPN	neo99	/etc/passwd
	0x1D[ts:7664206]|EVNT:XR-FILE!@MOD_usr:odinX=>/usr/lib/xrun.conf	0x1D	7664206	XR-FILE	MOD	odinX	/usr/lib/xrun.conf
	0x1E[ts:7664208]|EVNT:XR-DEL!@DEL_usr:mira01=>/bin/xz	0x1E	7664208	XR-DEL	DEL	mira01	/bin/xz
	0x1F[ts:7664210]|EVNT:XR-CONN!@IP:227.194.38.114	0x1F	7664210	XR-CONN	CONN	—	227.194.38.114 (IP)
	0x20[ts:7664212]|EVNT:XR-LOG!@OPN_usr:neo99=>/etc/passwd	0x20	7664212	XR-LOG	OPN	neo99	/etc/passwd
	0x21[ts:7664214]|EVNT:XR-CONN!@IP:218.60.93.170	0x21	7664214	XR-CONN	CONN	—	218.60.93.170 (IP)
	0x22[ts:7664216]|EVNT:XR-CONN!@IP:55.7.142.145	0x22	7664216	XR-CONN	CONN	—	55.7.142.145 (IP)
	0x23[ts:7664218]|EVNT:XR-SHDW!@KILL_proc:pid3211	0x23	7664218	XR-SHDW	KILL	—	pid3211
	0x24[ts:7664220]|EVNT:XR-CONN!@IP:189.132.8.12	0x24	7664220	XR-CONN	CONN	—	189.132.8.12 (IP)
	0x25[ts:7664222]|EVNT:XR-SHDW!@KILL_proc:pid4528	0x25	7664222	XR-SHDW	KILL	—	pid4528
	0x26[ts:7664224]|EVNT:XR-FILE!@MOD_usr:xav23=>/tmp/init.sock	0x26	7664224	XR-FILE	MOD	xav23	/tmp/init.sock
	0x27[ts:7664226]|EVNT:XR-EXEC!@RUN_usr:odinX=>/etc/passwd	0x27	7664226	XR-EXEC	RUN	odinX	/etc/passwd
	0x28[ts:7664228]|EVNT:XR-DEL!@DEL_usr:neo99=>/bin/xz	0x28	7664228	XR-DEL	DEL	neo99	/bin/xz
	0x29[ts:7664230]|EVNT:XR-EXEC!@RUN_usr:xav23=>/bin/xz	0x29	7664230	XR-EXEC	RUN	xav23	/bin/xz
	0x2A[ts:7664232]|EVNT:XR-EXEC!@RUN_usr:mira01=>/usr/lib/xrun.conf	0x2A	7664232	XR-EXEC	RUN	mira01	/usr/lib/xrun.conf
	0x2B[ts:7664234]|EVNT:XR-FILE!@MOD_usr:xav23=>/usr/lib/xrun.conf	0x2B	7664234	XR-FILE	MOD	xav23	/usr/lib/xrun.conf
	0x2C[ts:7664236]|EVNT:XR-EXEC!@RUN_usr:xav23=>/opt/secure.shd	0x2C	7664236	XR-EXEC	RUN	xav23	/opt/secure.shd
	0x2D[ts:7664238]|EVNT:XR-EXEC!@RUN_usr:neo99=>/bin/xz	0x2D	7664238	XR-EXEC	RUN	neo99	/bin/xz
	0x2E[ts:7664240]|EVNT:XR-DEL!@DEL_usr:odinX=>/bin/xz	0x2E	7664240	XR-DEL	DEL	odinX	/bin/xz
	0x2F[ts:7664242]|EVNT:XR-EXEC!@RUN_usr:neo99=>/bin/xz	0x2F	7664242	XR-EXEC	RUN	neo99	/bin/xz
	0x30[ts:7664244]|EVNT:XR-EXEC!@RUN_usr:neo99=>/etc/passwd	0x30	7664244	XR-EXEC	RUN	neo99	/etc/passwd
	0x31[ts:7664246]|EVNT:XR-FILE!@MOD_usr:tara4=>/etc/passwd	0x31	7664246	XR-FILE	MOD	tara4	/etc/passwd
	0x0[ts:7622003]|EVNT:XR-LOG!@OPN_usr:mira01=>/opt/secure.shd	0x0	7622003	XR-LOG	OPN	mira01	/opt/secure.shd
	0x1[ts:7622005]|EVNT:XR-SHDW!@KILL_proc:pid5139	0x1	7622005	XR-SHDW	KILL	—	pid5139

session_3.vlog	0x2[ts:7622007]|EVNT:XR-DEL!@DEL_usr:tara4=>/opt/secure.shd	0x2	7622007	XR-DEL	DEL	tara4	/opt/secure.shd
	0x3[ts:7622009]|EVNT:XR-CONN!@IP:118.13.190.31	0x3	7622009	XR-CONN	CONN	—	118.13.190.31 (IP)
	0x4[ts:7622011]|EVNT:XR-EXEC!@RUN_usr:mira01=>/tmp/init.sock	0x4	7622011	XR-EXEC	RUN	mira01	/tmp/init.sock
	0x5[ts:7622013]|EVNT:XR-CONN!@IP:157.21.64.173	0x5	7622013	XR-CONN	CONN	—	157.21.64.173 (IP)
	0x6[ts:7622015]|EVNT:XR-FILE!@MOD_usr:mira01=>/usr/lib/xrun.conf	0x6	7622015	XR-FILE	MOD	mira01	/usr/lib/xrun.conf
	0x7[ts:7622017]|EVNT:XR-EXEC!@RUN_usr:neo99=>/usr/lib/xrun.conf	0x7	7622017	XR-EXEC	RUN	neo99	/usr/lib/xrun.conf
	0x8[ts:7622019]|EVNT:XR-CONN!@IP:235.238.129.67	0x8	7622019	XR-CONN	CONN	—	235.238.129.67 (IP)
	0x9[ts:7622021]|EVNT:XR-EXEC!@RUN_usr:mira01=>/bin/xz	0x9	7622021	XR-EXEC	RUN	mira01	/bin/xz
	0xA[ts:7622023]|EVNT:XR-EXEC!@RUN_usr:mira01=>/opt/secure.shd	0xA	7622023	XR-EXEC	RUN	mira01	/opt/secure.shd
	0xB[ts:7622025]|EVNT:XR-LOG!@OPN_usr:odinX=>/tmp/init.sock	0xB	7622025	XR-LOG	OPN	odinX	/tmp/init.sock
	0xC[ts:7622027]|EVNT:XR-CONN!@IP:65.139.59.139	0xC	7622027	XR-CONN	CONN	—	65.139.59.139 (IP)
	0xD[ts:7622029]|EVNT:XR-SHDW!@KILL_proc:pid8855	0xD	7622029	XR-SHDW	KILL	—	pid8855
	0xE[ts:7622031]|EVNT:XR-FILE!@MOD_usr:tara4=>/tmp/init.sock	0xE	7622031	XR-FILE	MOD	tara4	/tmp/init.sock
	0xF[ts:7622033]|EVNT:XR-SHDW!@KILL_proc:pid3553	0xF	7622033	XR-SHDW	KILL	—	pid3553
	0x10[ts:7622035]|EVNT:XR-EXEC!@RUN_usr:tara4=>/etc/passwd	0x10	7622035	XR-EXEC	RUN	tara4	/etc/passwd
	0x11[ts:7622037]|EVNT:XR-DEL!@DEL_usr:xav23=>/bin/xz	0x11	7622037	XR-DEL	DEL	xav23	/bin/xz
	0x12[ts:7622039]|EVNT:XR-EXEC!@RUN_usr:xav23=>/opt/secure.shd	0x12	7622039	XR-EXEC	RUN	xav23	/opt/secure.shd
	0x13[ts:7622041]|EVNT:XR-FILE!@MOD_usr:odinX=>/usr/lib/xrun.conf	0x13	7622041	XR-FILE	MOD	odinX	/usr/lib/xrun.conf
	0x14[ts:7622043]|EVNT:XR-CONN!@IP:47.158.48.20	0x14	7622043	XR-CONN	CONN	—	47.158.48.20 (IP)
	0x15[ts:7622045]|EVNT:XR-EXEC!@RUN_usr:mira01=>/etc/passwd	0x15	7622045	XR-EXEC	RUN	mira01	/etc/passwd
	0x16[ts:7622047]|EVNT:XR-CONN!@IP:48.168.181.180	0x16	7622047	XR-CONN	CONN	—	48.168.181.180 (IP)
	0x17[ts:7622049]|EVNT:XR-FILE!@MOD_usr:odinX=>/usr/lib/xrun.conf	0x17	7622049	XR-FILE	MOD	odinX	/usr/lib/xrun.conf
	0x18[ts:7622051]|EVNT:XR-EXEC!@RUN_usr:mira01=>/usr/lib/xrun.conf	0x18	7622051	XR-EXEC	RUN	mira01	/usr/lib/xrun.conf
	0x19[ts:7622053]|EVNT:XR-DEL!@DEL_usr:tara4=>/etc/passwd	0x19	7622053	XR-DEL	DEL	tara4	/etc/passwd
	0x1A[ts:7622055]|EVNT:XR-EXEC!@RUN_usr:mira01=>/tmp/init.sock	0x1A	7622055	XR-EXEC	RUN	mira01	/tmp/init.sock
	0x1B[ts:7622057]|EVNT:XR-EXEC!@RUN_usr:mira01=>/etc/passwd	0x1B	7622057	XR-EXEC	RUN	mira01	/etc/passwd
	0x1C[ts:7622059]|EVNT:XR-FILE!@MOD_usr:xav23=>/tmp/init.sock	0x1C	7622059	XR-FILE	MOD	xav23	/tmp/init.sock
	0x1D[ts:7622061]|EVNT:XR-CONN!@IP:172.139.178.68	0x1D	7622061	XR-CONN	CONN	—	172.139.178.68 (IP)
	0x1E[ts:7622063]|EVNT:XR-CONN!@IP:185.148.214.180	0x1E	7622063	XR-CONN	CONN	—	185.148.214.180 (IP)
	0x1F[ts:7622065]|EVNT:XR-LOG!@OPN_usr:tara4=>/bin/xz	0x1F	7622065	XR-LOG	OPN	tara4	/bin/xz
	0x20[ts:7622067]|EVNT:XR-CONN!@IP:218.204.0.114	0x20	7622067	XR-CONN	CONN	—	218.204.0.114 (IP)
	0x21[ts:7622069]|EVNT:XR-CONN!@IP:221.229.243.75	0x21	7622069	XR-CONN	CONN	—	221.229.243.75 (IP)
	0x22[ts:7622071]|EVNT:XR-FILE!@MOD_usr:tara4=>/bin/xz	0x22	7622071	XR-FILE	MOD	tara4	/bin/xz
	0x23[ts:7622073]|EVNT:XR-SHDW!@KILL_proc:pid8910	0x23	7622073	XR-SHDW	KILL	—	pid8910
	0x24[ts:7622075]|EVNT:XR-SHDW!@KILL_proc:pid9523	0x24	7622075	XR-SHDW	KILL	—	pid9523
	0x25[ts:7622077]|EVNT:XR-SHDW!@KILL_proc:pid2424	0x25	7622077	XR-SHDW	KILL	—	pid2424
	0x26[ts:7622079]|EVNT:XR-FILE!@MOD_usr:tara4=>/tmp/init.sock	0x26	7622079	XR-FILE	MOD	tara4	/tmp/init.sock
	0x27[ts:7622081]|EVNT:XR-EXEC!@RUN_usr:neo99=>/opt/secure.shd	0x27	7622081	XR-EXEC	RUN	neo99	/opt/secure.shd
	0x28[ts:7622083]|EVNT:XR-FILE!@MOD_usr:odinX=>/etc/passwd	0x28	7622083	XR-FILE	MOD	odinX	/etc/passwd
	0x29[ts:7622085]|EVNT:XR-FILE!@MOD_usr:tara4=>/etc/passwd	0x29	7622085	XR-FILE	MOD	tara4	/etc/passwd
	0x2A[ts:7622087]|EVNT:XR-CONN!@IP:137.58.250.177	0x2A	7622087	XR-CONN	CONN	—	137.58.250.177 (IP)
	0x2B[ts:7622089]|EVNT:XR-DEL!@DEL_usr:xav23=>/etc/passwd	0x2B	7622089	XR-DEL	DEL	xav23	/etc/passwd
	0x2C[ts:7622091]|EVNT:XR-CONN!@IP:192.98.37.158	0x2C	7622091	XR-CONN	CONN	—	192.98.37.158 (IP)
	0x2D[ts:7622093]|EVNT:XR-FILE!@MOD_usr:xav23=>/bin/xz	0x2D	7622093	XR-FILE	MOD	xav23	/bin/xz
	0x2E[ts:7622095]|EVNT:XR-CONN!@IP:10.237.180.67	0x2E	7622095	XR-CONN	CONN	—	10.237.180.67 (IP)
	0x2F[ts:7622097]|EVNT:XR-EXEC!@RUN_usr:neo99=>/usr/lib/xrun.conf	0x2F	7622097	XR-EXEC	RUN	neo99	/usr/lib/xrun.conf
	0x30[ts:7622099]|EVNT:XR-SHDW!@KILL_proc:pid6346	0x30	7622099	XR-SHDW	KILL	—	pid6346
	0x31[ts:7622101]|EVNT:XR-EXEC!@RUN_usr:mira01=>/tmp/init.sock	0x31	7622101	XR-EXEC	RUN	mira01	/tmp/init.sock
	0x0[ts:7875734]|EVNT:XR-FILE!@MOD_usr:tara4=>/bin/xz	0x0	7875734	XR-FILE	MOD	tara4	/bin/xz
	0x1[ts:7875736]|EVNT:XR-SHDW!@KILL_proc:pid9271	0x1	7875736	XR-SHDW	KILL	—	pid9271
	0x2[ts:7875738]|EVNT:XR-SHDW!@KILL_proc:pid3118	0x2	7875738	XR-SHDW	KILL	—	pid3118
	0x3[ts:7875740]|EVNT:XR-EXEC!@RUN_usr:neo99=>/tmp/init.sock	0x3	7875740	XR-EXEC	RUN	neo99	/tmp/init.sock
	0x4[ts:7875742]|EVNT:XR-LOG!@OPN_usr:neo99=>/etc/passwd	0x4	7875742	XR-LOG	OPN	neo99	/etc/passwd

session_4.vlog	0x5[ts:7875744]|EVNT:XR-SHDW!@KILL_proc:pid2822	0x5	7875744	XR-SHDW	KILL	—	pid2822
	0x6[ts:7875746]|EVNT:XR-SHDW!@KILL_proc:pid6271	0x6	7875746	XR-SHDW	KILL	—	pid6271
	0x7[ts:7875748]|EVNT:XR-DEL!@DEL_usr:tara4=>/opt/secure.shd	0x7	7875748	XR-DEL	DEL	tara4	/opt/secure.shd
	0x8[ts:7875750]|EVNT:XR-SHDW!@KILL_proc:pid6183	0x8	7875750	XR-SHDW	KILL	—	pid6183
	0x9[ts:7875752]|EVNT:XR-FILE!@MOD_usr:odinX=>/tmp/init.sock	0x9	7875752	XR-FILE	MOD	odinX	/tmp/init.sock
	0xA[ts:7875754]|EVNT:XR-SHDW!@KILL_proc:pid7910	0xA	7875754	XR-SHDW	KILL	—	pid7910
	0xB[ts:7875756]|EVNT:XR-DEL!@DEL_usr:xav23=>/tmp/init.sock	0xB	7875756	XR-DEL	DEL	xav23	/tmp/init.sock
	0xC[ts:7875758]|EVNT:XR-LOG!@OPN_usr:odinX=>/usr/lib/xrun.conf	0xC	7875758	XR-LOG	OPN	odinX	/usr/lib/xrun.conf
	0xD[ts:7875760]|EVNT:XR-LOG!@OPN_usr:tara4=>/opt/secure.shd	0xD	7875760	XR-LOG	OPN	tara4	/opt/secure.shd
	0xE[ts:7875762]|EVNT:XR-CONN!@IP:214.122.91.151	0xE	7875762	XR-CONN	CONN	—	214.122.91.151 (IP)
	0xF[ts:7875764]|EVNT:XR-CONN!@IP:21.36.145.178	0xF	7875764	XR-CONN	CONN	—	21.36.145.178 (IP)
	0x10[ts:7875766]|EVNT:XR-EXEC!@RUN_usr:xav23=>/usr/lib/xrun.conf	0x10	7875766	XR-EXEC	RUN	xav23	/usr/lib/xrun.conf
	0x11[ts:7875768]|EVNT:XR-EXEC!@RUN_usr:odinX=>/usr/lib/xrun.conf	0x11	7875768	XR-EXEC	RUN	odinX	/usr/lib/xrun.conf
	0x12[ts:7875770]|EVNT:XR-CONN!@IP:115.143.90.97	0x12	7875770	XR-CONN	CONN	—	115.143.90.97 (IP)
	0x13[ts:7875772]|EVNT:XR-EXEC!@RUN_usr:tara4=>/bin/xz	0x13	7875772	XR-EXEC	RUN	tara4	/bin/xz
	0x14[ts:7875774]|EVNT:XR-SHDW!@KILL_proc:pid2396	0x14	7875774	XR-SHDW	KILL	—	pid2396
	0x15[ts:7875776]|EVNT:XR-LOG!@OPN_usr:tara4=>/usr/lib/xrun.conf	0x15	7875776	XR-LOG	OPN	tara4	/usr/lib/xrun.conf
	0x16[ts:7875778]|EVNT:XR-CONN!@IP:164.104.248.157	0x16	7875778	XR-CONN	CONN	—	164.104.248.157 (IP)
	0x17[ts:7875780]|EVNT:XR-SHDW!@KILL_proc:pid3558	0x17	7875780	XR-SHDW	KILL	—	pid3558
	0x18[ts:7875782]|EVNT:XR-CONN!@IP:96.154.104.132	0x18	7875782	XR-CONN	CONN	—	96.154.104.132 (IP)
	0x19[ts:7875784]|EVNT:XR-SHDW!@KILL_proc:pid2781	0x19	7875784	XR-SHDW	KILL	—	pid2781
	0x1A[ts:7875786]|EVNT:XR-EXEC!@RUN_usr:mira01=>/usr/lib/xrun.conf	0x1A	7875786	XR-EXEC	RUN	mira01	/usr/lib/xrun.conf
	0x1B[ts:7875788]|EVNT:XR-EXEC!@RUN_usr:mira01=>/etc/passwd	0x1B	7875788	XR-EXEC	RUN	mira01	/etc/passwd
	0x1C[ts:7875790]|EVNT:XR-FILE!@MOD_usr:tara4=>/usr/lib/xrun.conf	0x1C	7875790	XR-FILE	MOD	tara4	/usr/lib/xrun.conf
	0x1D[ts:7875792]|EVNT:XR-FILE!@MOD_usr:neo99=>/tmp/init.sock	0x1D	7875792	XR-FILE	MOD	neo99	/tmp/init.sock
	0x1E[ts:7875794]|EVNT:XR-LOG!@OPN_usr:neo99=>/opt/secure.shd	0x1E	7875794	XR-LOG	OPN	neo99	/opt/secure.shd
	0x1F[ts:7875796]|EVNT:XR-CONN!@IP:160.100.208.238	0x1F	7875796	XR-CONN	CONN	—	160.100.208.238 (IP)
	0x20[ts:7875798]|EVNT:XR-EXEC!@RUN_usr:odinX=>/bin/xz	0x20	7875798	XR-EXEC	RUN	odinX	/bin/xz
	0x21[ts:7875800]|EVNT:XR-SHDW!@KILL_proc:pid6159	0x21	7875800	XR-SHDW	KILL	—	pid6159
	0x22[ts:7875802]|EVNT:XR-LOG!@OPN_usr:xav23=>/opt/secure.shd	0x22	7875802	XR-LOG	OPN	xav23	/opt/secure.shd
	0x23[ts:7875804]|EVNT:XR-CONN!@IP:32.51.192.87	0x23	7875804	XR-CONN	CONN	—	32.51.192.87 (IP)
	0x24[ts:7875806]|EVNT:XR-EXEC!@RUN_usr:xav23=>/tmp/init.sock	0x24	7875806	XR-EXEC	RUN	xav23	/tmp/init.sock
	0x25[ts:7875808]|EVNT:XR-CONN!@IP:163.128.220.79	0x25	7875808	XR-CONN	CONN	—	163.128.220.79 (IP)
	0x26[ts:7875810]|EVNT:XR-LOG!@OPN_usr:odinX=>/opt/secure.shd	0x26	7875810	XR-LOG	OPN	odinX	/opt/secure.shd
	0x27[ts:7875812]|EVNT:XR-LOG!@OPN_usr:xav23=>/opt/secure.shd	0x27	7875812	XR-LOG	OPN	xav23	/opt/secure.shd
	0x28[ts:7875814]|EVNT:XR-LOG!@OPN_usr:mira01=>/etc/passwd	0x28	7875814	XR-LOG	OPN	mira01	/etc/passwd
	0x29[ts:7875816]|EVNT:XR-DEL!@DEL_usr:tara4=>/tmp/init.sock	0x29	7875816	XR-DEL	DEL	tara4	/tmp/init.sock
	0x2A[ts:7875818]|EVNT:XR-DEL!@DEL_usr:neo99=>/bin/xz	0x2A	7875818	XR-DEL	DEL	neo99	/bin/xz
	0x2B[ts:7875820]|EVNT:XR-CONN!@IP:143.33.249.114	0x2B	7875820	XR-CONN	CONN	—	143.33.249.114 (IP)
	0x2C[ts:7875822]|EVNT:XR-CONN!@IP:119.239.226.60	0x2C	7875822	XR-CONN	CONN	—	119.239.226.60 (IP)
	0x2D[ts:7875824]|EVNT:XR-FILE!@MOD_usr:odinX=>/usr/lib/xrun.conf	0x2D	7875824	XR-FILE	MOD	odinX	/usr/lib/xrun.conf
	0x2E[ts:7875826]|EVNT:XR-FILE!@MOD_usr:tara4=>/bin/xz	0x2E	7875826	XR-FILE	MOD	tara4	/bin/xz
	0x2F[ts:7875828]|EVNT:XR-FILE!@MOD_usr:mira01=>/opt/secure.shd	0x2F	7875828	XR-FILE	MOD	mira01	/opt/secure.shd
	0x30[ts:7875830]|EVNT:XR-LOG!@OPN_usr:neo99=>/tmp/init.sock	0x30	7875830	XR-LOG	OPN	neo99	/tmp/init.sock
	0x31[ts:7875832]|EVNT:XR-CONN!@IP:173.5.70.127	0x31	7875832	XR-CONN	CONN	—	173.5.70.127 (IP)
	0x0[ts:7928936]|EVNT:XR-DEL!@DEL_usr:neo99=>/tmp/init.sock	0x0	7928936	XR-DEL	DEL	neo99	/tmp/init.sock
	0x1[ts:7928938]|EVNT:XR-FILE!@MOD_usr:tara4=>/usr/lib/xrun.conf	0x1	7928938	XR-FILE	MOD	tara4	/usr/lib/xrun.conf
	0x2[ts:7928940]|EVNT:XR-SHDW!@KILL_proc:pid5834	0x2	7928940	XR-SHDW	KILL	—	pid5834
	0x3[ts:7928942]|EVNT:XR-CONN!@IP:172.70.145.196	0x3	7928942	XR-CONN	CONN	—	172.70.145.196
	0x4[ts:7928944]|EVNT:XR-DEL!@DEL_usr:mira01=>/etc/passwd	0x4	7928944	XR-DEL	DEL	mira01	/etc/passwd
	0x5[ts:7928946]|EVNT:XR-LOG!@OPN_usr:xav23=>/opt/secure.shd	0x5	7928946	XR-LOG	OPN	xav23	/opt/secure.shd
	0x6[ts:7928948]|EVNT:XR-LOG!@OPN_usr:xav23=>/opt/secure.shd	0x6	7928948	XR-LOG	OPN	xav23	/opt/secure.shd
	0x7[ts:7928950]|EVNT:XR-EXEC!@RUN_usr:odinX=>/opt/secure.shd	0x7	7928950	XR-EXEC	RUN	odinX	/opt/secure.shd

session_5.vlog	0x8[ts:7928952]|EVNT:XR-CONN!@IP:195.33.196.36	0x8	7928952	XR-CONN	CONN	—	195.33.196.36
	0x9[ts:7928954]|EVNT:XR-DEL!@DEL_usr:neo99=>/tmp/init.sock	0x9	7928954	XR-DEL	DEL	neo99	/tmp/init.sock
	0xA[ts:7928956]|EVNT:XR-LOG!@OPN_usr:mira01=>/usr/lib/xrun.conf	0xA	7928956	XR-LOG	OPN	mira01	/usr/lib/xrun.conf
	0xB[ts:7928958]|EVNT:XR-FILE!@MOD_usr:neo99=>/usr/lib/xrun.conf	0xB	7928958	XR-FILE	MOD	neo99	/usr/lib/xrun.conf
	0xC[ts:7928960]|EVNT:XR-FILE!@MOD_usr:tara4=>/usr/lib/xrun.conf	0xC	7928960	XR-FILE	MOD	tara4	/usr/lib/xrun.conf
	0xD[ts:7928962]|EVNT:XR-LOG!@OPN_usr:tara4=>/etc/passwd	0xD	7928962	XR-LOG	OPN	tara4	/etc/passwd
	0xE[ts:7928964]|EVNT:XR-FILE!@MOD_usr:mira01=>/usr/lib/xrun.conf	0xE	7928964	XR-FILE	MOD	mira01	/usr/lib/xrun.conf
	0xF[ts:7928966]|EVNT:XR-FILE!@MOD_usr:mira01=>/tmp/init.sock	0xF	7928966	XR-FILE	MOD	mira01	/tmp/init.sock
	0x10[ts:7928968]|EVNT:XR-EXEC!@RUN_usr:odinX=>/opt/secure.shd	0x10	7928968	XR-EXEC	RUN	odinX	/opt/secure.shd
	0x11[ts:7928970]|EVNT:XR-LOG!@OPN_usr:tara4=>/usr/lib/xrun.conf	0x11	7928970	XR-LOG	OPN	tara4	/usr/lib/xrun.conf
	0x12[ts:7928972]|EVNT:XR-DEL!@DEL_usr:xav23=>/usr/lib/xrun.conf	0x12	7928972	XR-DEL	DEL	xav23	/usr/lib/xrun.conf
	0x13[ts:7928974]|EVNT:XR-LOG!@OPN_usr:xav23=>/etc/passwd	0x13	7928974	XR-LOG	OPN	xav23	/etc/passwd
	0x14[ts:7928976]|EVNT:XR-LOG!@OPN_usr:xav23=>/usr/lib/xrun.conf	0x14	7928976	XR-LOG	OPN	xav23	/usr/lib/xrun.conf
	0x15[ts:7928978]|EVNT:XR-FILE!@MOD_usr:neo99=>/usr/lib/xrun.conf	0x15	7928978	XR-FILE	MOD	neo99	/usr/lib/xrun.conf
	0x16[ts:7928980]|EVNT:XR-CONN!@IP:162.112.39.26	0x16	7928980	XR-CONN	CONN	—	162.112.39.26
	0x17[ts:7928982]|EVNT:XR-SHDW!@KILL_proc:pid4188	0x17	7928982	XR-SHDW	KILL	—	pid4188
	0x18[ts:7928984]|EVNT:XR-FILE!@MOD_usr:xav23=>/tmp/init.sock	0x18	7928984	XR-FILE	MOD	xav23	/tmp/init.sock
	0x19[ts:7928986]|EVNT:XR-CONN!@IP:87.33.75.208	0x19	7928986	XR-CONN	CONN	—	87.33.75.208
	0x1A[ts:7928988]|EVNT:XR-DEL!@DEL_usr:odinX=>/tmp/init.sock	0x1A	7928988	XR-DEL	DEL	odinX	/tmp/init.sock
	0x1B[ts:7928990]|EVNT:XR-CONN!@IP:175.155.196.2	0x1B	7928990	XR-CONN	CONN	—	175.155.196.2
	0x1C[ts:7928992]|EVNT:XR-EXEC!@RUN_usr:tara4=>/usr/lib/xrun.conf	0x1C	7928992	XR-EXEC	RUN	tara4	/usr/lib/xrun.conf
	0x1D[ts:7928994]|EVNT:XR-SHDW!@KILL_proc:pid2128	0x1D	7928994	XR-SHDW	KILL	—	pid2128
	0x1E[ts:7928996]|EVNT:XR-CONN!@IP:54.245.247.189	0x1E	7928996	XR-CONN	CONN	—	54.245.247.189
	0x1F[ts:7928998]|EVNT:XR-FILE!@MOD_usr:xav23=>/opt/secure.shd	0x1F	7928998	XR-FILE	MOD	xav23	/opt/secure.shd
	0x20[ts:7929000]|EVNT:XR-DEL!@DEL_usr:tara4=>/usr/lib/xrun.conf	0x20	7929000	XR-DEL	DEL	tara4	/usr/lib/xrun.conf
	0x21[ts:7929002]|EVNT:XR-SHDW!@KILL_proc:pid5675	0x21	7929002	XR-SHDW	KILL	—	pid5675
	0x22[ts:7929004]|EVNT:XR-DEL!@DEL_usr:xav23=>/opt/secure.shd	0x22	7929004	XR-DEL	DEL	xav23	/opt/secure.shd
	0x23[ts:7929006]|EVNT:XR-DEL!@DEL_usr:mira01=>/tmp/init.sock	0x23	7929006	XR-DEL	DEL	mira01	/tmp/init.sock
	0x24[ts:7929008]|EVNT:XR-LOG!@OPN_usr:odinX=>/etc/passwd	0x24	7929008	XR-LOG	OPN	odinX	/etc/passwd
	0x25[ts:7929010]|EVNT:XR-EXEC!@RUN_usr:mira01=>/usr/lib/xrun.conf	0x25	7929010	XR-EXEC	RUN	mira01	/usr/lib/xrun.conf
	0x26[ts:7929012]|EVNT:XR-CONN!@IP:223.194.70.87	0x26	7929012	XR-CONN	CONN	—	223.194.70.87
	0x27[ts:7929014]|EVNT:XR-CONN!@IP:254.44.133.153	0x27	7929014	XR-CONN	CONN	—	254.44.133.153
	0x28[ts:7929016]|EVNT:XR-FILE!@MOD_usr:xav23=>/usr/lib/xrun.conf	0x28	7929016	XR-FILE	MOD	xav23	/usr/lib/xrun.conf
	0x29[ts:7929018]|EVNT:XR-CONN!@IP:249.178.178.78	0x29	7929018	XR-CONN	CONN	—	249.178.178.78
	0x2A[ts:7929020]|EVNT:XR-DEL!@DEL_usr:tara4=>/usr/lib/xrun.conf	0x2A	7929020	XR-DEL	DEL	tara4	/usr/lib/xrun.conf
	0x2B[ts:7929022]|EVNT:XR-EXEC!@RUN_usr:odinX=>/tmp/init.sock	0x2B	7929022	XR-EXEC	RUN	odinX	/tmp/init.sock
	0x2C[ts:7929024]|EVNT:XR-CONN!@IP:119.54.128.55	0x2C	7929024	XR-CONN	CONN	—	119.54.128.55
	0x2D[ts:7929026]|EVNT:XR-CONN!@IP:214.60.133.73	0x2D	7929026	XR-CONN	CONN	—	214.60.133.73
	0x2E[ts:7929028]|EVNT:XR-FILE!@MOD_usr:odinX=>/tmp/init.sock	0x2E	7929028	XR-FILE	MOD	odinX	/tmp/init.sock
	0x2F[ts:7929030]|EVNT:XR-FILE!@MOD_usr:xav23=>/usr/lib/xrun.conf	0x2F	7929030	XR-FILE	MOD	xav23	/usr/lib/xrun.conf
	0x30[ts:7929032]|EVNT:XR-SHDW!@KILL_proc:pid6011	0x30	7929032	XR-SHDW	KILL	—	pid6011
	0x31[ts:7929034]|EVNT:XR-FILE!@MOD_usr:xav23=>/etc/passwd	0x31	7929034	XR-FILE	MOD	xav23	/etc/passwd