Turla Indicators of Compromise

github.com/eset/malware-ioc/tree/master/turla

eset

eset/malware-ioc

Indicators of Compromises (IOC) of our various investigations

14 Contributors | 0 Issues | 1k Stars | 218 Forks

SHA-1 hash	Component	Compilation Time	Certificate	ESET Detection Name
35f205367e2e5f8a121925bbae6ff07626b526a7	Gazer loader x32	05/02/2002 17:36:10	admin@solidloop.org valid from 14/10/2015 to 14/10/2016	Win32/Turla.CC
b151cd7c4f9e53a8dcbdeb7ce61ccdd146eb68ab	Gazer loader x32	05/02/2002 17:36:10	admin@solidloop.org valid from 14/10/2015 to 14/10/2016	Win32/Turla.CC
e40bb5beec5678537e8fe537f872b2ad6b77e08a	Gazer loader x32	05/02/2002 17:36:10	admin@solidloop.org valid from 14/10/2015 to 14/10/2016	Win32/Turla.CC
522e5f02c06ad215c9d0c23c5a6a523d34ae4e91	Gazer loader x64	05/02/2002 17:36:26	admin@solidloop.org valid from 14/10/2015 to 14/10/2016	Win64/Turla.AA
c380038a57ffb8c064851b898f630312fabcbba7	Gazer loader x64	05/02/2002 17:36:26	admin@solidloop.org valid from 14/10/2015 to 14/10/2016	Win64/Turla.AA
267f144d771b4e2832798485108decd505cb824a	Gazer loader x64	05/02/2002 17:36:26	admin@solidloop.org valid from 14/10/2015 to 14/10/2016	Win64/Turla.AA
52f6d09cccdbc38d66c184521e7ccf6b28c4b4d9	Gazer loader x32	04/10/2002 18:31:37	admin@solidloop.org valid from 14/10/2015 to 14/10/2016	Win32/Turla.CC

SHA-1 hash	Component	Compilation Time	Certificate	ESET Detection Name
475c59744accb09724dae610763b7284646ab63f	Gazer loader x32	04/10/2002 18:31:37	admin@solidloop.org valid from 14/10/2015 to 14/10/2016	Win32/Turla.CC
22542a3245d52b7bcdb3eaef5b8b2693f451f497	Gazer loader x32	04/10/2002 18:31:37	admin@solidloop.org valid from 14/10/2015 to 14/10/2016	Win32/Turla.CC
2b9faa8b0fcadac710c7b2b93d492ff1028b5291	Gazer loader x64	04/10/2002 18:34:18	admin@solidloop.org valid from 14/10/2015 to 14/10/2016	Win64/Turla.AA
e05ab6978c17724b7c874f44f8a6cbfb1c56418d	Gazer loader x64	04/10/2002 18:34:18	admin@solidloop.org valid from 14/10/2015 to 14/10/2016	Win64/Turla.AA
6dec3438d212b67356200bbac5ec7fa41c716d86	Gazer loader x64	04/10/2002 18:34:18	admin@solidloop.org valid from 14/10/2015 to 14/10/2016	Win64/Turla.AA
b548863df838069455a76d2a63327434c02d0d9d	Gazer loader x64	09/01/2016 19:30:10	not signed	Win64/Turla.AA
c3e6511377dfe85a34e19b33575870dda8884c3c	Gazer loader x64	06/02/2016 19:29:15	admin@ultimatecomsup.biz valid from 16/12/2015 to 16/12/2017	Win64/Turla.AA
9ff4f59ca26388c37d0b1f0e0b22322d926e294a	Gazer loader x64	16/02/2016 16:00:44	admin@ultimatecomsup.biz valid from 16/12/2015 to 16/12/2017	Win64/Turla.AA
029aa51549d0b9222db49a53d2604d79ad1c1e59	Gazer loader x64	18/02/2016 15:29:58	admin@ultimatecomsup.biz valid from 16/12/2015 to 16/12/2017	Win64/Turla.AA
cecc70f2b2d50269191336219a8f893d45f5e979	Gazer loader x64	01/01/2017 08:39:30	admin@ultimatecomsup.biz valid from 16/12/2015 to 16/12/2017	Win64/Turla.AG
7fac4fc130637afab31c56ce0a01e555d5dea40d	Gazer loader x64	11/06/2017 23:43:51	admin@ultimatecomsup.biz valid from 16/12/2015 to 16/12/2017	Win64/Turla.AD
5838A51426CA6095B1C92B87E1BE22276C21A044	Gazer loader x32	19/06/2017 01:28:51	admin@ultimatecomsup.biz valid from 16/12/2015 to 16/12/2017	Win32/Turla.CF
3944253F6B7019EED496FAD756F4651BE0E282B4	Gazer loader x64	19/06/2017 01:30:00	admin@ultimatecomsup.biz valid from 16/12/2015 to 16/12/2017	Win64/Turla.AD
228da957a9ed661e17e00efba8e923fd17fae054	Gazer orchestrator x32	05/02/2002 17:31:28	not signed	Win32/Turla.CF

SHA-1 hash	Component	Compilation Time	Certificate	ESET Detection Name
295d142a7bdced124fdcc8edfe49b9f3acceab8a	Gazer orchestrator x32	05/02/2002 17:31:28	not signed	Win32/Turla.CF
0f97f599fab7f8057424340c246d3a836c141782	Gazer orchestrator x32	05/02/2002 17:31:28	not signed	Win32/Turla.CF
dbb185e493a0fdc959763533d86d73f986409f1b	Gazer orchestrator x32	05/02/2002 17:31:28	not signed	Win32/Turla.CC
4701828dee543b994ed2578b9e0d3991f22bd827	Gazer orchestrator x64	05/02/2002 17:34:25	not signed	Win64/Turla.AA
6fd611667ba19691958b5b72673b9b802edd7ff8	Gazer orchestrator x64	05/02/2002 17:34:25	not signed	Win64/Turla.AA
fcabeb735c51e2b8eb6fb07bda8b95401d069bd8	Gazer orchestrator x64	05/02/2002 17:34:25	not signed	Win64/Turla.AA
75831df9cbcfd7bf812511148d2a0f117324a75f	Gazer orchestrator x32	04/10/2002 18:31:28	not signed	Win32/Turla.CC
bae3ae65c32838fb52a0f5ad2cde8659d2bff9f3	Gazer orchestrator x32	04/10/2002 18:31:28	not signed	Win32/Turla.CC
37ff6841419adc51eeb8756660b2fb46f3eb24ed	Gazer orchestrator x64	04/10/2002 18:33:02	not signed	Win64/Turla.AA
9e6de3577b463451b7afce24ab646ef62ad6c2bd	Gazer orchestrator x64	04/10/2002 18:33:02	not signed	Win64/Turla.AA
795c6ee27b147ff0a05c0477f70477e315916e0e	Gazer orchestrator x64	04/10/2002 18:33:02	not signed	Win64/Turla.AA
8184ad9d6bbd03e99a397f8e925fa66cfbe5cf1b	Gazer orchestrator x64	09/01/2016 19:28:29	not signed	Win64/Turla.AA
7ced96b08d7593e28fee616eccbc6338896517cf	Gazer orchestrator x64	06/02/2016 19:29:04	not signed	Win64/Turla.AA

SHA-1 hash	Component	Compilation Time	Certificate	ESET Detection Name
63c534630c2ce0070ad203f9704f1526e83ae586	Gazer orchestrator x64	06/02/2016 19:29:04	not signed	Win64/Turla.AA
23f1e3be3175d49e7b262cd88cfd517694dcba18	Gazer orchestrator x64	18/02/2016 15:29:32	not signed	Win64/Turla.AA
7a6f1486269abdc1d658db618dc3c6f2ac85a4a7	Gazer orchestrator x64	01/01/2017 08:39:19	not signed	Win64/Turla.AG
11B35320FB1CF21D2E57770D8D8B237EB4330EAA	Gazer orchestrator x64	11/06/2017 23:42:28	not signed	Win64/Turla.AD
E8A2BAD87027F2BF3ECAE477F805DE13FCCC0181	Gazer orchestrator x32	19/06/2017 01:28:21	not signed	Win32/Turla.CF
950F0B0C7701835C5FBDB6C5698A04B8AFE068E6	Gazer orchestrator x64	19/06/2017 01:29:46	not signed	Win64/Turla.AD
a5eec8c6aadf784994bf68d9d937bb7af3684d5c	Gazer comm x64	05/02/2002 17:57:07	admin@solidloop.org valid from 14/10/2015 to 14/10/2016	Win64/Turla.AH
411ef895fe8dd4e040e8bf4048f4327f917e5724	Gazer comm x32	05/02/2002 17:58:22	admin@solidloop.org valid from 14/10/2015 to 14/10/2016	Win32/Turla.CC
c1288df9022bcd2c0a217b1536dfa83928768d06	Gazer comm x32	06/02/2016 19:23:52	not signed	Win32/Turla.CC
4b6ef62d5d59f2fe7f245dd3042dc7b83e3cc923	Gazer comm x32	11/06/2017 23:44:24	not signed	Win32/Turla.CF
7f54f9f2a6909062988ae87c1337f3cf38d68d35	Gazer wiper x32	05/02/2002 17:39:07	admin@solidloop.org valid from 14/10/2015 to 14/10/2016	Win32/Turla.CL
27FA78DE705EBAA4B11C4B5FE7277F91906B3F92	Gazer wiper x32	07/04/2016 15:04:24	not signed	Win32/Turla.CL