TREND MICRO | research

Mirai Botnet Exploit Weaponized to Attack IoT Devices via CVE-2020-5902

Appendix

Indicators of Compromise (IoCs)

URL	Description
78.142.18.20	C&C server
79.124.8.24	Disease vector

Figure 1. URLs

SHA256	Description	Detection Name
acb930a41abdc4b055e2e3806aad85068be8d85e0e0610be35e784bfd7cf5b0e	fetch.sh	Trojan.SH.MIRAI.BOI
007254539d542563b4c4b66cee57cd1a49b5d4701d43f83db908f198aaf48229		Backdoor.Linux.BASHLITE.SMJC
af5cceefa2292b47042df22983d65c34fb57ff0f52fe4135738c53079b699fd1	sora.arm7	
b2fe976028bf9b9b6f78c9461fd9e6389f41e357691226be7c64a8f6e01b3cf9		
191cda060fa0e34cc46c616d1308df8914d8fe53c5ce3dc232bec56467adccc9		
03254e6240c35f7d787ca5175ffc36818185e62bdfc4d88d5b342451a747156d		Backdoor.Linux.MIRAI.VWIUP
b02b5f8a1e0cd51f9fef2383ab2c9362b83ebab7bbdb46c9191355363f809f2e		Backdoor.Linux.BASHLITE.SMJC
b22d772c4d825548f5d4f306be460f242e45065632fefdde7a37f2725eb8e770		
b70e3766271993388db3fee403556ec5011afb4b1a5a1e3e0803fce0c2592738		
b9e281aec5d8acbcc39939da7c5c4fd2538af924f110142de026b4b58e2dfc7c		
df6aa4092e9dc5de0371673e4fb2dc282aab74bbee388638f41fb48d55eed64f		
f835db2dfe3fbe29ea63cbe83644f2b3b12c00f8ef304f403398c8a10d2d7a87		
232bd7a7beada597ce71f1607a8d58238b4f878babaf0a167573e976c681c521		
23a70da6677e77308d763d03340adf2321e547007b98e424933aec3cb456ea61		
267600324455dcc91f395e87920a0431c31b1218eeb3b639521b350c9a6968b8		
46589461d1a2c2cda790032d5e7bd4c1b9f3a68113915f985abe1fa7d6c4f7d6		
4fd5e82c2e94a246e01afcc0d01f9595d2b7ab86252b05c26d6d0e7bf45e9876		

5a4d5a6066ce47671e29f698ff7e4566d9b9b8677808ba61200683f325d7921e		
556286fdef3600253f006f10eca18c3840377c72419e6ac2690116ee589e8be9		
6226c32ec5b3bdace911cec2c14676fbf4c51d5e6a183c1183d980a581d8207c		
6888a5d35be8fbbdab5ef3fbe9afc6ac6d9866028cc37258b60fbc5c79c3c58f		
9b2629e5167d24654b03bba97c4e2c829ba59946542b843801f9b13e7cd5f9f9		
af2eae10f700b8d004ce9c097f2a17e9edc3c2251d25ef658abf761975e07cee		Backdoor.Linux.MIRAI.VWIUP
a364513adc7103c95ee20580d8014369bc3321831ec567b0f7a342c9b517d1cc		
c97d08c7a8c4465e1d6ef5da385ff670505477a4feb0a376230e3100da5e687a		
de3d0a766b7dba822ed95b637968203b68759e73aed6d904455e94a45882b493		
fd70873b5a9b06f0d02af878d426094bdf6e3553833f5319bbb4dd7da0725db5		
f44ffa1041d89852588c1952fd7d4c82cf581c6cd70060b29eea4d15170b4398		
f891113e672325b494af13f05081668eb916589daf5cf962f130e2cf3a95cbe9		
15a5e8359e2451a49a922a004dc7e488077419b96c7b9da87822768e22df2236		
159efac3fa13178f51f0da9fff3d3df914191cf15d1717f4a5efaaeb3cc7bde7		
190dee3fcc4dd16b87674177ab25ed590b0c3a9b7d5f4a9a7258d314558a678a		
22e925219f1b8db8f81809abf8c904ca52ee9f78b88e2d1a03872db465670b06		
7d253e84fea4349307177aced6dc3c1b20cc96239cf2ff2274cb0bd52ae5a77d		
ad683393be8c09609588c67b9b978294b01fe04fa4dbca92eba8b360792361ec	sora.arm5	Trojan.Linux.MIRAI.SMNM1
dda2e6e5599a2e16dc0f0fce5579992a841063f1a71b7da9444aa92585f46245		
4c926ee55c6e3d1f881080c4b61734f3e7cf96124d8cb2c1fe33c8e8d8754a04	sora.arm5	
41f90b23dbc330f586c0bf5c6643d00fbd8e215d1222c1f156390a1d93d7d853	sora.arm5	

489fc54886d20e31c9e9e099712bfb85e63ae1633a17840a956f0b1f6559621d	sora.arm5	
616ca0c082553a61f8fda6a248129dc540ff51561b4495d41951f35b1c6d5788	sora.arm5	
7127c35dc0e8edc31bba08dda487dd496b82d596054d0361060aafac4ec0023a		
81feb98ef2ed4d99c6a0d48f8b6ae17b4bc137fa0ef0c0cb5f66ea1b4416a69a		
9a8ac8c6e3898a4c5112ce5c83a3a1b775b8287360120ed9ee62131d61171450		
037859323285e0bbbc054f43b642c48f2826924149cb1c494cbbf1fc8707f942	sora.arm5	
0423e9059fe3a60c889c9dbf0a91e2a68671f5e19da17b03804666569c7e1697		
45bce22f91e2116f2334fe9899fbf6f157847ddd840688f12498ec53b8dfeb5e		Backdoor.Linux.MIRAI.SMNM4
687f1969da1747f27a315878560fa15d99f15176e8b045255e1318e2d9b2d30f		Backdoor.Linux.MIRAI.VWIUO
355d6ccef10ded805ab247c49dffd9e316608f7a4e01e4b9020a04066b9d7c17		Backdoor.Linux.MIRAI.SMMR1
815e9af39e5e143f81f4b043c17931a055bf31f852ad91fa6627140c0370c868		
ecc1e3f8332de94d830ed97cd07867b90a405bc9cc1b8deccec51badb4a2707c	sora.sh4	Backdoor.Linux.MIRAI.VWIUQ
e71aca778ea1753973b23e6aa29d1445f93dc15e531c706b6165502d6cf0bfa4	sora.x86	
15b2ee07246684f93b996b41578ff32332f4f2a60ef3626df9dc740405e45751	sora.mpsl	
204cbad52dde24ab3df41c58021d8039910bf7ea07645e70780c2dbd66f7e90b	sora.m68k	
3f8e65988b8e2909f0ea5605f655348efb87565566808c29d136001239b7dfa9	sora.mips	
43cb46b7e87317899a80134eb107597c4e80aed150b52606565c4aa9928d5ca0		
55c4675a84c1ee40e67209dfde25a5d1c1979454ec2120047026d94f64d57744	sora.arm6	
64608b5a68867aaa21574cd11b7008c946c026dbf43c2096280e4ee033da5819		
0ca27c002e3f905dddf9083c9b2f8b3c0ba8fb0976c6a06180f623c6acc6d8ca	sora.ppc	

Figure 2. Hashes

TREND MICRO™ RESEARCH

Trend Micro, a global leader in cybersecurity, helps to make the world safe for exchanging digital information.

Trend Micro Research is powered by experts who are passionate about discovering new threats, sharing key insights, and supporting efforts to stop cybercriminals. Our global team helps identify millions of threats daily, leads the industry in vulnerability disclosures, and publishes innovative research on new threats techniques. We continually work to anticipate new threats and deliver thought-provoking research.

www.trendmicro.com