Indicators of Compromise (IOCs)

Type Indicator
E-mail Subject ATTN: Invoice_J-<8-digits>
Attachment Filename invoice_J-<8-digits>.doc/ Rechnung-54-110090.xls

Malicious Command and Control Servers

C2 109.234.38.35
C2 173.214.183.81
C2 193.124.181.169
C2 195.154.241.208
C2 195.64.154.14
C2 46.4.239.76
C2 66.133.129.5
C2 86.104.134.144
C2 91.195.12.185
C2 iynus[.]net
C2 www[.]iglobali.com
C2 www[.]jesusdenazaret.com.ve
C2 www[.]southlife.church
C2 www[.]villaggio.airwave.at
URL hxxp://vjwmpxseu.fr/main.php
URL hxxp://jywdohhfkypg.de/main.php
URL hxxp://blydeylrayu.it/main.php
URL hxxp://obvpxgcohmpsou.it/main.php
URL hxxp://cqvgwp.uk/main.php
URL hxxp://tdxgp.eu/main.php
URL hxxp://109.234.38.35/main.php
URL hxxp://uxvvm.us/main.php
URL hxxp://wblejsfob.pw/main.php
URL hxxp://kqlxtqptsmys.in/main.php
URL hxxp://pvwinlrmwvccuo.eu/main.php

SHA256 ee6abe4a9530b78e997d9c28394356216778eaf2d46aa3503999e7d6bfbefe90
SHA256 5466fb6309bfe0bbbb109af3ccfa0c67305c3464b0fdffcec6eda7fcb774757e
SHA256 add7794c4d70fd49c96c11dc924c6b65c4459d6295331414b40768867dab0350
SHA256 e7277e4aa4905168f6890c6b7b80515030806db46b7ec41a8afa33d6dda231dc
SHA256 6e2a597d8c6b4ebc6474c4a96bce61340a1a66b7e8e33cdf42f3e34cef1a94fe
SHA256 76bcba80045b043e8e69f7a2a92bc8879e7b13e29d50f10b41c11bd114a288ae
SHA256 e37cb6cb2d39e3ceeb946e4a55890cd278a0ba3d541c0d18a22a0bf84c1dcadb
SHA256 18f7150992020e369dbc2aa32fdec2e3003d782716a79be654b9e4eecff0113a
SHA256 c9bfb22f9655e53dacbce66c4bfba1e5b42250f0b41973c1e4433f285ed73d79
SHA256 41a7bfe77c89b3c151f0e847e44e8f58d63ed82a8ad370bc679c29d89a20a657
SHA256 1833ea2138d21962d6f47def5d01cbec299eb6deb89fe729fd5b80c0f603a766
SHA256 03da53e5fe550a1914179d5102479771651d4fa8797f46df3e4f66a05fa64bd6
SHA256 338f15ac0d07db13e1f291c53aa004f46d994ee5bacd2787c0d536284b465f9e
SHA256 1d8cc4e8416b5ac16864583e8bb0d8f8d8ad4b32de7de111067c38da0cfc57b1
SHA256 abdbc74907d7670a65b5a4cc8c08da751cc837a11d1abb43e3ddaa932bdbf60c
SHA256 8877b9a036b76495d9f4add16d56c8819d12a92cd32ae0e4c06be4faa719a991
SHA256 4ae1f9229bfb5385949a4dfe0ac89a49d785646389be556f90ad5d29e5ecc35f
SHA256 b10733a1aa02d973d00bd780c7f1a7d1e71fd50155f2cfecfb2a8f1662aa1cd5
SHA256 8a248e85579cde3e0e8e20f254ec2c15ce063f580084be2dca1f8e725ae7f148
SHA256 11206eb0cfa0df32ef0b4d2cd2a704be11cbd6e6bc6a2d83eaf0ddf977d76ac5
SHA256 521d2885aec43104e3903988f23e42a2543682556afc51bff44bb939c74eb421
SHA256 3d84dd3f392eadaf3916c3f71cf98606c25f48feaad60b74af7196171aade0a7
SHA256 17c3d74e3c0645edb4b5145335b342d2929c92dff856cca1a5e79fa5d935fec2
SHA256 329197ec2fffb6365adee8b7302912c8ef0f7550f63c92887d2cfae432a15df4
SHA256 f81d543f5144fe8dc1d0bb84625ed298867d9b34f805c7d26ce26f37d325467a
SHA256 5843c22f9e27cd8a217114b21ccc706dafe40f626dc9fcef0000a7f79b2aad66
SHA256 d0df113d589fe481bc045bda948ace1f2b9c43b4bd0652f00b0fbb096a2fb39c
SHA256 a6189f9796f1c782b95eb6e0bc030e8d1de924efdafff8e329876b09b2b5173f
SHA256 f3712d591fbf403d23eed006d5c5bb5b94e13360920a04095968d1a914bc3ff8

SHA256 348c92b47a27fbf427d1093f09ef662dbd11846ca1f3e8cf9ba2dda8008f9c4f
SHA256 1083fd1d0a02d36582b78fdba4478e75401f7ec37359f6d8142426f8f3523328
SHA256 2e1305b440274e1f4340a10180709b83f5aad182963d6f6594613e71b309d7d5
SHA256 e6079af75b4a06f6ce95cb95d3de3b8af89afbf7722a64a6f7b04f3c643024b2
SHA256 dca90037836376ce5634f277ee21e779462b6faaff83ade1ba36f75fc0bc255b
SHA256 5fc15b920f00f427350987ae192b9baf2eb0fecfc662985fb612e8ebc60f9b30
SHA256 0c38c96617436fadf66852e48365def3e00b297c7f160617768bebd09f15658d
SHA256 13bd70822009e07f1d0549e96b8a4aec0ade07bea2c28d42d782bacc11259cf5
SHA256 9b5653a986529c2eebc429387f3dea52ea167ccb259b6f57491d14ea4b86627e
SHA256 55645af2a4c54c6c1141b7261ca598d2e250a5a1b51731920cf7c09264c4c160
SHA256 1c5c1c287cd6151da44571b8cfae526b0b6e6d09faaa6723fdd040cb595b9fd0
SHA256 89b732003c08f0f1c2f8a0412b1c2f0efc216ae0204103326571e1831e28b09e
SHA256 711147bfafee1b3f71b0c8e9d00bb139401c207ca5518e2c02a6b0a7367cc9c2
SHA256 53e91bbc1de973265ef3366201a70bce385951f805d2d9ebc9ab5f2d7627b7d3
SHA256 f56655bfbd1be9eab245dc283b7c71991881a845f3caf8fb930f7baabae51059
SHA256 555fb717902e671c26848ee80788769a1c88ac00c9f8440250f9936632597bc8
SHA256 a5b2d0f5367bebd70137e0ebf3286d80434789e95aca488ffd8391905dd98fd9
SHA256 da21dbe14f408ddb3de2e57fb77fd94e8615cb6cce5b7c541b8fe4e309b7fb6c
SHA256 fd5c0d976292b233328ea085f101bbef9c6cae2007d275a5e6e07149d86c7968
SHA256 7c3651cb149cb5f9a4db6b64e412fcd23977f5c083bdfd3ee8c7bbf929e20b4d
SHA256 7b39dfb32220e3f653ce8ec124a3f1541230c158533ea4b799e766bb1f77b96f
SHA256 e77aec1984755d69692487acbf1ce4743726714ffe9168610a49e05723e891cd
SHA256 0661bd8cefcc41bba4322077b6ab96d49054074c6aa2a917acf87ff815d53e49
SHA256 5bae6d580e1e16d29233f7164ce6aadfabcbd562b9137e92997e4ad3854926fd
SHA256 ec9ac36b8ef41ecda870ed41297592a34e3250db821c8d518701c0e486c9379f
SHA256 1c8ebb27ad656d720c854a476d6f0e1de4288e9f2a4c60ae35bb7020dedf5239
SHA256 db3bc157f8f6bda96c63d2ba40c74e7bfd4d451d87eaa8ed02ce9ee692098d15
SHA256 9cc592720e4d859f7cd2995587e1f724133ff3008164261ea7fb7e3269ac597a
SHA256 c866dcfa95c50443ed5e0b4d2c0b63c1443ad330cb7d384370a244c6f58ce8a5
SHA256 2dbfd8f5e20168a52dadf694fc9e63c8f09356dae60fd79e00897dc094a48cb6

SHA256 78e9558a9762cf778a3ba9ba61e0ec73e8d81c22d0945e56ea75d197c512883a
SHA256 708bae89b1866c85243f02b011d4d1e9585305845bf7a4df4430927cd5af8c27
SHA256 7c9c451a3a3bded9aad02297f611e425b3649e629e4c5e24a7ccb7928babb006
SHA256 069464563ca340ef167b29b55797bbb63792c00700a867437fdd9f640e99aa09
SHA256 cba9de885f30b627d9c30079a22956e61cd1b03d10ec972ef9c90f8d23cff8aa
SHA256 1f126aabbf32507f4385fe335b46fbb46234b2c25909ed6884ed664a5c93d0f9
SHA256 1bad53ce984f652bc03ecb96fad5746357968c2fdccdea82995231f1099773e4
SHA256 62a19c7a08db69a45ecf009955e6d8aa441079dea06770af1a953b681a0d81a2
SHA256 1450fa0c4f5973ebf3efa06fb03259105065baba29690362014926583bc85f48
SHA256 d6772478ab901d81514b0d04852380932ee214b364dff246c3f91963d9ec6927
SHA256 ec9bfe9c9d44437c04209269fcd26815dc99416722bb4f4a4a2049bc41c63cc6
SHA256 acf01ba44f916a8f82f76c0b91021fd79d4968e3aa312fb77904a9757058b5ac
SHA256 d69b7f196fa8a2298e261333d4794ac34a8a4503c26750c3d5a012b2b7b327f5
SHA256 134ef8198282652fb98e4174deda4d105db53c54d50039a2c0f6eb283eed8a1b
SHA256 50c2b1f4b32fcd43fa9871f51f72d2b227eab1a3e5d04159d326a22e56305dc8
SHA256 e5aecadf8f132b64384bba0f1ffbf317637eed11398a0d6ef789b1dc10db4cb1
SHA256 87068696c0291fe976f62afb23ff2720d53dfd638a6953c0d0867d9ad4ea451a
SHA256 c7ab7c65e65cdc13bbb991403c1338c556500472114ba79bb31356eecabd0089
SHA256 eaa4d072b1eb53b2dae7d5396e67c03e523fe05f76f793c991119463b1f8522c
SHA256 3eb1e97e1bd96b919170c0439307a326aa28acc84b1f644e81e17d24794b9b57
SHA256 2059727c6447781b2dc2e4c51c126bc0b7f05b9c23b3edf365332d90c078b7f6
SHA256 d9de8ff8c82baeeab0e1e355f9f5025547ba40cb8d95e9cad9dc25ffdb690057
SHA256 915be79a2330c1fcb9e0cf392913986dbe9bf7a404cdf88a65ae148586b162d5
SHA256 5549b000fd38a2634adbe956d46f7bb649eda8efd768ef8919a703378885186b
SHA256 bc98c8b22461a2c2631b2feec399208fdc4ecd1cd2229066c2f385caa958daa3
SHA256 83279bbeb581892ccee9cfa7d37b73674d55380d55d78123781b3c38a2d8ffe0
SHA256 f519f99c9b49cf730cb092d83350002fb0d90fd705c86ed306c36f38fd6af10a
SHA256 50a2235f356d59269b98f1d6420afa257651b33e9d9af5af56ab777c331dc6dd
SHA256 d7d23b516041299868eb67a814e22064a05f06283a673a186e24d184521fa33e
SHA256 8545aa956982bf6f5763058cbde3f8c92e1dcbfb699a7248969ef12bb59a615c

SHA256 3d08eb860a2a13e7fc36f7750a4a87cf11b994a19343234b8e0621fa951e5a38
SHA256 488947790c6aba7dff05c5f1c9ce1d24b3f9e5a0677f1695bbd6ae2bd9d48236
SHA256 d2369ae9977cbb23cfe1c63f6deb0d7fabe9ee38980831c8a636f91342f716c1
SHA256 b16ed0060bd5359fc695b965ce4c459bbe73e083094aff720837739487fd2900
SHA256 3c305696f35fe10eb27a97bb76bc737654727b33e81333c8fe73aeded98b6ca8
SHA256 cf836b6a36bffc5a4545a27cc66bc9ddfd49483500aa1f055671e40f06e34221
SHA256 66bf8957d55e0aacc3c2472ebd8966dc3370503e59d57f27ddbc1a83bcf5102a
SHA256 2114322ecc57f0fab5dd1e5b348a066fcfd7baf8ced89fcdb23df172e30a4189
SHA256 971b389bd82806942c44b48bdd0a4ac560377b7fcb5c872264796705b769414a
SHA256 8426bdde88e8e59c56ab4ff6b32dfd1080dfc0fc86980a853802e9aea1773c47
SHA256 fa3f2cf4b2f1a0393383294dae8ba20709b1ce0985b6fe8e51ccd90cb609ca6e
SHA256 20c37d343ba95aed4180d75825a06828783e924f81a1237c4a68252e0ce97f2d
SHA256 46cf36241696d4127b5d32cbde63a672d9a037d9d47bd59ae8346d83424b53c9
SHA256 892fe60e489e229eb46627241b6078a5b213a4d1840bd39cc939f90cf903a560
SHA256 4d203ae53a96b8207c81ecc0167bb06db3e67bb365639972b9ef22dafbbc189a
SHA256 a32f9eff7fca4f8b98b553b90915b28d4e11e523d36bb64b41f1793c2ed7cf94
SHA256 7f540e391b55221f7696031471b6f8d2068677a67ed8782d52a67872096d23a2
SHA256 408f10baec56c62cc4692d1ba98aa77e7847a7b6f1d3cf812dd2f51c93d580a3
SHA256 2410b7f81082b216c5edd99b4b0a22e7709b0e05b0f6961d4f93ee1a05590237
SHA256 566878276748089f6e87b20fd18bfab4018d9e33fae6e28cb87ffb43b1b80582
SHA256 0a6f1b58819fe0d5f0595be96847f9cb9722777501771d3066d1e7fd39fa3d48
SHA256 d9d3acec0620a1395dda087318de075573fa3b4352641aedc01a16a921c11b5d
SHA256 6e10b784d653ceca19a234411df7a570cb0923bef9a3fe1d91da1e8eb10306d3
SHA256 8988323e0c8b26a3cb0166104001c8d5fd818bef72b506bd03403a2c7c552e8d
SHA256 e7d7b7c8b9cba4dcfee5648f25ad0380c86398cd0b6cba59c3ee8256425d19e6
SHA256 057c1fc879ff7fed218ef3142a0f8761b2651a4c060dc7d853e5621cddc0e6f9
SHA256 ca7ea4325e6e55c504d29f0b080a5755aef771772d8c51f5016e4ce6ed88ccd0
SHA256 77ea0b407dece7f22b0b4732ec06fb0e887262d847a49b9f8cd8611a5c865af4
SHA256 5ad06eda999a9f2f28c2057ba40bd2f7b6a7cb2e1915104b2724753649e97de5
SHA256 584a2767e5881c7f91a04ca2cd78e62e9d52841eea5e0ca7fcd197553666a827

SHA256 a756d84edecae5f17726ba1e59cbc3a622f84159e293a875c24bacf1038f69f1
SHA256 6d76567220652b0d03b34feafaef8b32a472bfd9d617b6eff4db5254c959bf6e
SHA256 1227d8b7e375dfaf0ff76053e3ab158c0635cb288dc1a2f083536f5fe1820ddd
SHA256 8d6be9b4df6679cc5db1750500e3e1645f885878223936670e9ce0442cd0e999
SHA256 82761eb506711dd35af4fe7b71a4e926e1bd70d4dacadd1bb3e68bcd3ef480f3
SHA256 9524daf160f35c3217df680f5676c8f177bc9a3de5b6a128d52bc46d97df96c0
SHA256 c9303f7405c88da80d94df5b11c514ce791becab02e06dfbf4796f361fb93108
SHA256 815530458a2e17fd67774a6802c49423088ddde0ae23e179cc4a608e088c276a
SHA256 66314449bc3bd2772ff062c05ba21f1aa408ce4f7ff73ad37f0f7a2388ab819e
SHA256 4b08d86ca080234c2432613e6730d06dd8c703b35ea7effc999a0e3c3b11ec48
SHA256 88718a0ff51b2e7d9e17d8796cfed1f52d78653c42e3c5dd597833ee0036d803
SHA256 feba92e398ba6da41cccffb0e6b5aacdee27fcfa4f6c3a469330be309eaad627
SHA256 73c41e29e75e998a186e6fc74b81fbc537f3b232a5d07b5621e8fd3485506b87
SHA256 06cc1531e8f912ca9e5f1e37f442d2145df6b8cdadf3d1d7abfc9dfae6bb98ab
SHA256 6d74cb6e7e93277cef4a8d62fad53d806be140aaddb89b44d9b7eb8307c5b7f5
SHA256 04e561cf760209b3bef678117366dd184f4474e4ba15ec9b95cddea4e01ade95
SHA256 6314ba359b26e05fba095ac58e3f9451243081cbc331bf60522ad69439b438c4
SHA256 2f45d682260ca936e1c577c845576eef009a7017882ed57b6a8b76f9f6b83ad6
SHA256 cc1afcf52046e08ba1314e74a852eec27211395c77f5b911de52245fae93ab3d
SHA256 97b13680d6c6e5d8fff655fe99700486cbdd097cfa9250a066d247609f85b9b9
SHA256 281d72fe63fae2e3b1b74c3953b3b4c429948d1f56c7897104754393dc0ab38f
SHA256 e2790ea81b297f0b10871b9a16d0adbb670c7ea5900d64bc1d2f65a296d87ade
SHA256 a9e663aa23a75f8574b5e10b4bea1deed22b49ed6dc451e4bb45f217811978a0
SHA256 caac78ebfdb6102c05b82a00cf1acda1797cf4dc1bcc66336286289c8a309b47
SHA256 bb85dedadd0b96084eb6c45b4a7650e33aa149f286d1272f17c56228278fe5b8
SHA256 abffa851076dd0f2d408e66d047a2d50415513a17239b2d2ece33891c9c0ad23
SHA256 9cfd1878606c41624b2e41a96eefcab6ca673d07f8e8f98ce6e86c4c8a806f5e
SHA256 3cc5d88b8a69dec6a606aa01c29789811442b2572dcc51e25aa7711e657b51f3
SHA256 e6ec5b942625bc910b3dc1c8f28940d5e5ba4f5fb89c7c189c61c3b46945f1f1
SHA256 b37f2e7dd94e441a129629d1d352b82bb4a0e9b98a1c9a188f95e6c148e6b407

SHA256 78b7b0eddc1d05cafd0202729f488daa027cac375dcd688c10fae34f65e0224e
SHA256 9b4f6d76d125524f7ac11ddc3251152ca45c79d44a4359e831ebe0ec3142b609
SHA256 5e945c1d27c9ad77a2b63ae10af46aee7d29a6a43605a9bfbf35cebbcff184d8
SHA256 2d79bf996a3f5a10f5b42c6449df14a00395390f5028dca18aa768651ed7bf62
SHA256 e8cbcdac6f39abf67c9c297203312d39f83a150277e0672a83657d38e6ef5446
SHA256 e25d15f721362c6e6110ce21c3ced554a2c8510a6c5627457688fdb397608656
SHA256 c8a7a0a8d702ce8087617a12572c00eefb92508ea6f1cfd95fe14c26107cef67
SHA256 3f8437665c6c7638e5f86d034ac2ce3367ab97533c45476e6beee8863c365ff6
SHA256 1a35563989c5528348713b0246374bb3c8d316561dc6b9bf17f2b20c88fbd178
SHA256 69afcd4b38bf84069c4f520e65ef7df31411d69819d88716cbb5e17178e5b5b0
SHA256 aef677a0a83d1ab1036fde6926e848674d7d53bf5dc3bd984c6c6d51337c4b61
SHA256 76499405dd3cea63f170813d88ab32b2716e5682b8083a94966d494b706eadc7
SHA256 acee75cd346795ceb02fc30aa822d13c4132e64fd36b5244dd822199a5a0c0a7
SHA256 4f2ae18fe003ec4dfd47255f24141b42af1b423c94a1abcbe8af337f251c8789
SHA256 3540b0720b610f93713df454af8ad1e7bd0e0eb3099d115a8cc5a9b7a85d3c50
SHA256 e95cde1e6fa2ce300bf778f3e9f17dfc6a3e499cb0081070ef5d3d15507f367b
SHA256 8c6e41a5e33749c31516b1931e129bbdaeff7f3434c4259c8842b0b9f047b6b7
SHA256 47b27cb727b1ada6c65c7bf30b57537b26080f1f5a6730be91b767427945d731
SHA256 658e17adf469ec61f1cc62a0c3932185e94f9557597dcf4714575706efd71141