TrendLabs

# Malicious Edge and Chrome Extension Used to Deliver Backdoor

## Appendix

TrendLabs Security Intelligence Blog
Jaromir Horejsi, Joseph C. Chen, and Loseway Lu
Cyber Safety Solutions (CSS) Team
May 2018

# Indicators of Compromise (IoCs)

## Related command-and-control (C&C) domains:

- knigi[.]xyz
- ads-letter[.]info

## Related malicious files (SHA-256):

- f41a97b902936b0675f8f2a19508b58340dee263d49838c3445ca83016001f60 (TROJ_SPYSIVIT.A)
- JavaApp.jar - b6ecaf0737bc29645615372899fc53a7dfb43e8fa952deffff6e566f68265a2d (JAVA_ SPYSIVIT.A)

## Related JavaScript files (SHA-256):

| Hash | Trend Micro Detection |
|---|---|
| 07939c7dcfbe3250e58a8c0c597124cebc1cfe9a81f54f0c697780cbba3777e2 | JS_DLOADR.AUSUIX |
| 2ceed0a392b879aad03ee048dc23eee530415bb679842f3e73f0530c005f34fa | |
| eee12f9d4f58cc9949adc880c6625aa1d03b46ddca2891e5c70f70df32852ade | |
| b905f26b03303cd79f0700710e116d396e7e1f1570dadf86dd4c1d530b505cb2 | JS_STARTER.GLR |
| 1a460650a9ce9c4a152a665eb55d40a78e2e6f32d57de983b56e772e113bd08c | |
| 2de1fa8f3a4dda1902c4759833b5225f24da396afeabfa1e44bbcf615df512ce | JS_INFOSTEAL.AUSSB |

## Related delivery documents detected as W2KM_DLOADR.UHAOEEE (SHA-256):

| Hash |
| --- |
| 7d762456b617d46de77ea5f94048d78549565d3ed8cd99aab62114a80de2706b |
| 811b213ef890eeda167ffb238e2f7b2e7c380200ae75c56fee9b30fde2b1ec26 |
| 8388c5283ba42b68d5b9cd66978ebe9cee6b172f91b0f30fd70503518327192c |
| c1bc1d327fceae8d10d27638f06715534cd414328a7ccf09812d82e616fddf6a |
| c63e3bf13fb38090f96c2774f05a823756ba383abb9849ea6f5efb1a5588903e |
| e6298886e9e3fd0daa1dff80db486da0fd2650365eb29a08e563ec018e9a8d57 |
| eb98e2c8397dffe682ef962678f1cbc83c979827332f5ae7bd11699431c2860f |
| efc712bc6b974c30acec42830df619f9330c41995a3db217a868c09ed7180840 |
| 2bdfe1756a215211fd4d52c04fed5fcb53402e03f4aec3d852d3227d944a4142 |

## Related delivery documents detected as W2KM_DLOADR.AOEEE (SHA-256):

| Hash |
| --- |
| fee455b794ccd11a30acc865ca9b4effe5092697942d66785d6b2d135e245fa5 |
| 01667c18e9510c10349c7c0b38cc36e29c78c1ad89b213ba2b14bba30b861171 |
| 01c1911aa1f4eedf30ca794d5980738fbe68a1113daeb298a28749f207a9f73f |
| 03d185f903513916dcf4decfe6d65c7bfffb6b918a9adee9db32322bbee80aa1 |
| 04280afc1c2e1eb84010264b71f9b4e4459b2b8922e93501364a08a22543ca4b |
| 08466882cc32a5b52ebd58b2c82123dd0b76a29c13b0fbd7c1880d0b4b0a6ee6 |
| 0c82ecdb051ecfd1ae7949b8a82a9fd16644f3c1908d9f1e30dcf7a607163c21 |
| 115cc582bd0999c1569421519a1bf252c8c7d4a9e426818510d8e2ba9fba8a49 |
| 1162134c00371c4a78691b3655014d4f01fa9fd69e6fcf83e6907bb4c70ce9f6 |
| 1271d40e9ed8d6ac188c2201b3180eb6e81e4c3b35a6ed1c28120b249bbb5304 |
| 143f2774ef4adb06c0ebc6e90c62d405340ed945bdc8104b037f43812b860df1 |
| 188ca0a4f73b515237f20c1e30f87622a54c8295a0fcddbbdbae7c32ea8fea17 |
| 196c4a76433599e31d92f6c1e9934042946aa4b0da383d34794764d9d7e85b56 |

| Hash |
| --- |
| 19ac272a42c94795ee21b3da9d20a3188c7a4140e0bf39f96478043a33bd89451e0f14212c9eb4951d0527c84479e18e1d4d73f0fdbdf4f19fccbc3cbdc95332 |
| 1f76022fa8af8158aabb84705a6edf8438616a6f5bc588ca0cae6b01109defd6 |
| 2200504d21d0f532d472a1e54977543f01246f93a72faf1170875dea310b8249 |
| 229eb3f67a973f73567743bd22b7926de9e0308f9c44df6c6001e3edcf5f041d |
| 22efd83624844f67057bcf30714d574904eb8eb8f2b6b73fa29730abd06ec3fe |
| 25abceb853292846804fdff82ad2e1b83899cc38b572aef4eb06eff89adbbf7d |
| 271962daf0d241d4dab2062660daaf1ca824bd8070ea59da0e00b9fbe76d1e28 |
| 2e6d0b96e8e4296a46fa1fc368769dd56e4a6ad5d0f56064c8035a5f8da9b834 |
| 3095b43e5dfc175d1b857504401f8cbd0ace26613e1180aeaeb80b530ab9922e |
| 32bca91711f25932fad821647e5b33813de286460631e0a0d864f99b0507f686 |
| 33915fc4bc8b0e8d9bbc0691ec3224409d2ee2b1d76e2b36d058a8c1ce23723c |
| 34955c905aed4b10cd7c1b626cdeb15f6225606a666922a9ec8b42b5c0f9c61a |
| 403877aaf08028c09b963fc2ace678c87f00a47962e62f8b517c0b073e2f1b67 |
| 47affa93008d19273fd76b55cd2d327b85022a88b68493a8af8e230808b6dd69 |
| 4c2a2572b0f0d215bd9453e3eba8d59d9f25ea834c67961609b22935355967a1 |
| 5466a3532ce06f9562c85b7cbb3015e91b978897ebcdf7de6eecc9b964fc71af |
| 54f0b1628a3340c0a0e305bd565d00a5f06e9d24c2f4223cd2440695d318cb71 |
| 56bb6fe3377b0f62966fbdf93fcc1714642c1833f159c2214e0a440371c4a605 |
| 5cef6da58665c3a5243648118658a62f78871a1e86bd81156e5b92842eba6376 |
| 5ede6bca52193727b2e625523b69ebe5f7793431955845097fe5ac030378a033 |
| 6063f92e573ae88cfce709dc031e4fcbe26229a10052c5b26e62669b140fb8d0 |
| 638fff5fd23505ac6681fdc8502ff8ea566faef76111f62d174f814bd8e15882 |
| 741c0da0f15b2ca91459db440f81120e8e49df2a394056c5b7ca4b76f3ce888f |
| 747e8b9033710daffa573363d5973162292cf1835abe4892a1410247af762462 |
| 76eab0271776d65f818c3ee812772d89725f1e19c1b67ad0295825bd3bbd5b1c |
| 7a12312698876a39b4872b0573d9300031d13d9113cd3b19dffbc3a82da9814a |
| 7cbebd47984d8a5abebd8e14cf71a15b38b5bd989996f4cf781edc1cc655d560 |
| 7ffca7fa6cb683f59402c532b418581128b1dc3f0371cfed96ab0331fe955a5c |
| 82f1b1bdcac86c1727829687cecbd36ac46419f864c3b9ce1fcb968420ed76da |
| 83f477245f84c4dd257b342b1cc38699d3011fc5dee3bff08b55d4add5217385 |
| 87fea3e122a490f7a789709f0e702ba655048f9b02281aec925a44bf35f147dc |
| 89027d8cb997bc3f8e41a1f42c53d8a56affd1e775c561e42634aa8b2402ad8f |

| Hash |
| --- |
| 89249e57ba98274f0e2d5ebd4dfc47a7a8f256e4e5b282478f5609b11961b1d2 |
| 8a89bc4371ae026bec3df6df429141a1aa12adc1caf9dfd7f19b52452257a909 |
| 9413f18772a4a132a350f0065a06ed9342850dcc9e61337cba3b117d0bd5f999 |
| 96636b5f63e16a35574ac7c9d7a9e109f859bae46c5af1baf8fa7dc92e99fc03 |
| 99b5224c128de42923d55272e26f01b5ccfce6bcaf3df7c71ece884a2eb22154 |
| 9af7ab73a34ce5c6683a13fbe657b3d5eb4a1981fc5298e6a93222c33015c97b |
| a16ee19ac7b833488083ccc85f086dca477f6c531d55512daee347308fa46302 |
| a17f7aa9fb51f5ac76e17a56a52098f24ba406886f366a7a893f843ddd2c770b |
| a56f143fa388569e9a2f1bafdff5b4d9623ad77da98391e6eb6a193d17f7c431 |
| a5f3fa402a0286cd5f9bfe7ad8912641dd39b294035bab8fcc54a1c290cac594 |
| a81085d0623b9737293098809a46edd0d9079ecb4a24b6c0cc6ea1aab556b4f3 |
| a8162c8271e43e56421fb43ff4e44157c208d4bed238a0813ee640a4b9ba124f |
| a8ebdce501dd63d37fc7f55d87b19b41626a2ae1a8f4d32b2413e1647bcd4bf4 |
| a924f026caf2cbb7ede8152138b53d484f69fb200ff0ff305147f6d0e7099b2a |
| af296ad4ee5a22bb4a3d2ef51c2df1925e4d511562efde927922ab994aeaddc7 |
| b4207fae1503835bc432b5f509f4f3ae69d3b4ef2a7d644dda6109e2ff84a3f5 |
| b475ae620f1431fd818fa94280e9b8eed0a000e3a21a4f6b61bd1f664d5d7e0d |
| b8482d65c65c6767bafbaed3262b75aa03e9f5522cbf9cd7a1d26e53b491653c |
| c0f1a5505a855805b1de02291f2752fba5e6d003d9ed6ef0cd04300536fbc888 |
| c5efd1a69aadbb619f9c7d077d3ea31d1e1a0f1e7a591971cdb714229d943a66 |
| c6108e76e3a30ef1f9b93398be98a0085c25cee407713f3df6a757e49153738e |
| d183e36502b5f1365d273cd75ddd3ea10184a5b0472ba2fdc902f43aecd8489b |
| d4fee398dae5f7fb32f34065635d228046f798547681a6425a70fd2ecd59a909 |
| d670a056d935249377c14124f4af0c6bc85b7c6bfe0e1e385364b7e85a58ed99 |
| d85fc5a0af5cc95aa6559173a00f2b356d4829abd32ad6b915659c7b8cd9b461 |
| d8e9181273d152d0b3c14dbab254a6138c3fc398f746ba429d7ca83a383819ea |
| db0f24a4af6b88caf2f7c1c2cd752c89e8c43745e29f811add04ac5067fdb62c |
| df7e4ca830b6d65ecf8ec349d3de021f5ad43c27d0a8ef983485f0b5a1308464 |
| e02e7aa4cc0f15d6912af949beaf2c99a990d9158ec7acfc38578fe03eed9b3c |
| ef487655db642f796e4f9419d33d03cd24cdc94f253b7d5af5375863c7569a08 |
| a995756c75b4bb54b519ceccc7f2577df98a9847e8d0d75cb3b61e28e7880d2e |
| f0bc85ad1486b4b36d45cf0e154725c7de85223d3d611221e06e8bba3223158e |

| Hash |
| --- |
| f0c346c8f5d842f328e12eb42ac99c46fd8096bc8c5e31dc9266d16da08daa78 |
| f1920f2058f04e3e429ffccaf2b600c07812f53ff84684701ea04669712b55f5 |
| f1c355aa5d32bf18c700b79bf7138dc901bfce73f435faf8963d6e56b7b90c13 |
| f6ea3edfa626ef35e0590af228e5ded78ac235fb154654491fc4713eb8edf7fb |
| f7821f037aab375b9a2b691a827d83f1934b82973c99fd75891f5ad397d1ce90 |
| f9a77db9ae0542f0b229f9278ef6f82ac9abbebddf2eeb37487f047e3313a6bc |

Trend Micro Incorporated, a global leader in security software, strives to make the world safe for exchanging digital information. Our innovative solutions for consumers, businesses and governments provide layered content security to protect information on mobile devices, endpoints, gateways, servers and the cloud. All of our solutions are powered by cloud-based global threat intelligence, the Trend Micro™ Smart Protection Network™, and are supported by over 1,200 threat experts around the globe. For more information, visit www.trendmicro.com.



TREND MICRO™

Securing Your Journey to the Cloud

Created by:

TrendLabs

Global Technical Support & R&D Center of TREND MICRO