BLACKSWAN CYBERSECURITY

THREAT ADVISORY

March 19, 2024

DarkGate Malware Exploiting Recent Microsoft Zero-Day

SUMMARY

The DarkGate malware operation has been leveraging a previously addressed vulnerability related to Windows Defender SmartScreen (CVE-2024-21412), which enables the circumvention of security protocols and facilitates the automatic installation of counterfeit software installers. Windows Defender SmartScreen typically alerts users when attempting to execute unknown files.

TECHNICAL DETAILS

Exploiting the recently patched vulnerability in Windows Defender SmartScreen (CVE-2024-21412), attackers use a technique involving Windows Internet shortcuts (.url files) to automatically execute malicious software on the host. By creating a chain of URL files, with the final link leading to an SMB share that automatically executes the file stored in the remote location. Microsoft addressed this vulnerability in mid-February'24, after seeing exploitation by the Water Hydra hacking group as a zero-day exploit to deploy DarkMe malware. Now, the DarkGate operators are leveraging this flaw to enhance their infection rates on specific systems.

The attack mechanism begins with a malicious email containing a PDF attachment with links that use open redirects from Google DoubleClick Digital Marketing services to evade email security checks. Clicking on these links redirects victims to a compromised web server hosting an internet shortcut file (.url), that then links to a second shortcut file hosted on an attacker-controlled WebDAV server. The exploitation of the CVE-2024-21412 flaw occurs as a file on the victim's device. These MSI files mimic legitimate software from reputable sources like NVIDIA, Apple iTunes, or Notion.one Windows Shortcut opens another on a remote server, triggering the automatic execution of a malicious MSI.

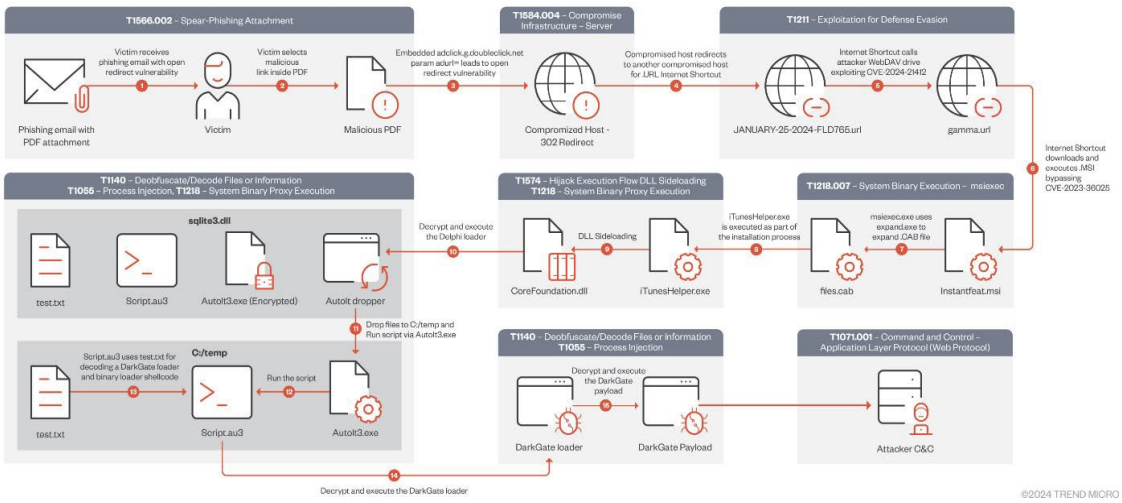

Fig. 1 - Attack Chain from TrendMicro

Once the MSI installer is executed, another flaw involving DLL sideloading with "libcef.dll" and a loader named "sqlite3.dll" is exploited, allowing decryption and execution of the DarkGate malware payload. This malware, identified as version 6.1.7 in the ongoing campaign, introduces XOR-encrypted configurations and new options, offering enhanced command and control (C2) capabilities. These configurations give operators the ability to adjust operational tactics and evasion techniques, including enabling startup persistence and specifying minimum system resource requirements to evade analysis environments.

Upon activation, DarkGate version 6.1.7 can conduct various malicious activities, including data theft, fetching additional payloads, injecting them into running processes, performing keylogging, and providing attackers with real-time remote access. This campaign underscores the evolving sophistication of malware distribution tactics and the imperative for robust cybersecurity measures to counter such threats effectively.

INDICATORS OF COMPROMISE (IoCs)

HASHES:

· 27c66ded5befaf70b02bfa994a1e7fda76ad5c231ffe566315a04ef6d4744332

· 18db09f15aaf7d143ebd3671d742b487b04ba23a731ccbf7c914693809915b71

· 6dd0002c7ae9b4eb6d89bb41c7194402abcdf36d28ed2293f97e8540220f5965

· 3b05791686e46bfb1b2a385bfd901cb37c2bb8fa0df549fc110915334eeabc6f

· 210d93018826d16957b3acc4a5737e3f87d803ac0264790295815ba27bccef14

· 8AFEDE48832E1D92D76943687278D0781B44B341D6B0D3ABFDEEA025A18473D1

· B9AD4D86A0F379C117FA0BF2551FBF8B6EDBC3ECFA2DC20636261D5CFC06E211

· 4E1FD759CDE248FCC78C22A89DA3083D83BFFC1051DC5C9209037B45E8DC1234

· a05b15e03101c18bc6dbaf44ca5b399d6d79a069fa1be1e2e11bec5cb5f4488d

· 12A7B3BC1C5C61A43E03FDB807463497B2CE54B3321BED5276AED9392BF128DD

· e91730008e0fc7b971e492d0000fea6674a7ee00475ff5f847960dbad3a1588f

· 8DE0395077EF6ED27B8C248C94DA35471206C0707D4069AC6D09DC9D4666E93E

· FD654D05A7124BFCCD117BA172B7C75BF4A2DA6D37111F7F21C3B6D946BC7241

· 154e500d569d8752ce17ca1c809ef08c4596869be054e158abd8e0242e88f64e

· 019714f77d024fc2039e6735b81273dac6524c8622c18d0ec35d8fd196a49286

· 5075bdf160c4be0802402de6ada4b8b6c6d36d3d31848d96e3c7a57d893dc3b6

· 237D1BCA6E056DF5BB16A1216A434634109478F882D3B1D58344C801D184F95D

· C9B23DA159F7E9CE54BDE81627FE5B9F51B3CC09DE738486DB9772C046FEEC23

· 4d34049dbe1823e4eafcc569bcbdd3742747fdee8ef9e71506c141385648dc3c

· FB3D83A155D8C24CCFC953800A7D147311FE1DEC14F7CFDB2B1F4815676111F0

· 77fd9bb8e28306fd40106d64faa6f9cd7e1332da2b9f9b339c9ecac239f445f3

· 4db21255797d2d9b447e95c2f8d016bc76c895c04d31806bba3ddcc3623f8f5b

· 474fbd180a26139e8013595adedc0ce2bb434677ae667093f86d4a59b11c7045

· 4D2A2DB08F8EAB9F94F2CF3D77584366E7235B58701B2EA59D57FD908605898E

· 71f69ab13b4d443256bf965efc336acb1e5107bc10f98dd7cf06f1a528cdefbd

· cdb88489701e69174b37bcd4539f99fe004a1a0bf7f6386c9d3823f23990ca15

· a53be1e2a6f17a5f4c22ac6fcd24fd70e04cd2c768ed83e84155e37b2a14bcbd

· 0d8e71a8d7717e0b0b39081fa434d09eb30fef3a691cf5ee0445d788e35f25ec

· fffa96bbcf4e075c3c1af00d88c598b01683d411ff81a88ac654f98d21deb1b5

· 522a39bdab216d5ed39bc7943c942a791eff60560a469efeccca68424d8264c5

· 52c2f6083c6d11543a39e977120c79e1c7f541b624f2405b9c5113df902993f7

· 3b953ef40eede72755e5562996fb6854b031440ac535f2f16e86bfdcf1e85132

· 3706cd2883baa6e9ea31962e6118bdb6609237912c567148fe2a16904bda7256

· d9a6857c59852e9ecd3aa4f07266de3c6ef6bf2ed01641893481cd41cd2be763

· 22EE095FA9456F878CFAFF8F2A4871EC550C4E9EE538975C1BBC7086CDE15EDE

· 1efbfb8f9e441370bb3f3a316fea237564eefebbf4ba33cccdae5f853c86a7b0

· 3c130dd5bfba46230e49a87522411f716c4ef5ce8ff3c60ef450c5c5c2e75f45

· CAA3D32AC52E5651DE060842A645BB981BC35F4EE53B64E7A2F13CA65CA596F2

· C94ECE5425C10E57C88C13DC731907F033BA534817DAE326A1C8B4A92FB8E4C6

· a7f67553858634adf30080cfedf6a0c45a15d7933f98d6cd88c3ac1bf7714b56

· 7BFACB09BB3B16C5E8F6CD83DCF7FC28FBDFAA298B589AAD1EFAF3B9777C1DFF

· 84cb3a9bf9275eaf647c62bb97a65ce21c986f9319cccaa1b444ca2cab1e719d

· 8826eb70de19f0bde0925ea53e0e33510e5414658ceaf5afacb6c1fb180d9745

· f736083c6618dc0b9ce5ff33abfca8729a96756dadc76dd83dc55164af74feee

· 0916dd821cf0fb4af8e75ac07b7ae95ce57181a15c15b1bc33394dc71da14eb7

· 2EF25CFD20F5F57F8D12327084D9A679E85A7FC6918090EDAA532FCF346A4437

· e5e94056346367f7a8cf31fd7a2a47b4004623f1c8b74cb8f5d6ae110bef134a

· F8B27DF7DA307D0D58E1B971B8080AF872A3125E229BDCBDFB95C64E8542C9DC

· 97C6D302415978C1E3B6E336F213FC4A66C814F489604E27D277CFD259342FE0

· 6e07dc1d87c0c00f57c823d53a864a1135179f212a13df676f05644aae7c4184

· F099A415E6A07121787B07889689127D63E88B459A9977EE8616FF6D26B8958F

· f0e2a74f75656efa763626e26565fbbfc1b024e96bff124a8f0ed34bc190d6b8

· 0f60919d6fc810b602c70eafeb55ddf0dc0f72f8c23162a76148647f65cddc7d

· ebf7736ea183efe5d523f0854acf99293f27c7fb4f13de2b307d3ee02df04ec3

· de69281050c18627c8e75a3f4cdf933db77ace2a8dd13ef753f61ad6e0a405ad

· cfe0d7d43b613ddf6e63d2dd414b96f505b958cdafae22031966703df4b882d8

· 8097e6eaafb37ff845adf84041f7c6f3bd48f2911097911cac0f6b2582bec38c

· 09586fda9605e3839de24236cce2a798051a5cf4c572ad43661fc24373ed1a9b

· 3035FB3598EF2DFCE3E0472C44A6C53A7C0E18B451CA58D8AD6DEF288D890CA3

· 4588a83fbb440f4a91fbe20166fd49973635339da7a9e0ffcfabace612c7b675

· 3D58662993744A99720B70F0F5EB9676B88CFB2280C7890166255C277C1D1223

· c16ee2fee125dcdcad256517f87e5f04188db9e67d695fbcc838afe22d50456c

· 421bfeac5b236a8f0692e95b601cfc1f17f9eba3f6eb6d0e32794fb0d8028c90

· 8bfa5e42f5996f0f61a7b087eef9b73ec73079b6f36ad322d007dba066f352bc

· f23d9b0a9faa6293a1fcb1647808cb3b5d3bde2fb49e02882b035eb40bafd159

· 8310F9B7636E8E7272229888A5E36E5E51A1E601968A6AEE76D42ABE2F60DAA9

· ee4da58848a99a991293cce2d7634b4acf003442d28617c5dfb33c33757c5cc4

· cbf78bcd4918f2519b5c18708ae44b6334dc86d2f521f57331ebffc9d413d7fd

· 69a5de0f76141b926cccd42906f5eab02cd220493a614241cad7f51b5203ba36

· f70ea26928739a824c133e2a700088cba03e67b886f58078b6bab5bc2c6b8efa

· B81B896B67A7786EC06F259516496A57880E52A42E9282CF8786D0CFAD44F1AF

· 9dc2e970291fb23b769b33e12eb10b0aee96bac0437c12ecb221854feaed7250

· 9c71b3dd94329b2649fd36ccd5f0df919126284883543cff573e103076ce3506

· 5B85E1FEE47BC43122549B3C4C3B524541BE261042FA1A46C53BC23FEA9515BB

· 8ebdaebacda151ae2d5328053e9b92ac51ac5e358b94987b30770f351f611bac

· 9E6861AC7AA15474D2D00AFD67B2FDEC473CF67A13116FDDECF1495088E853BA

· 952e3debfd70d9c17ac98153cbc82b16edde12a25fb4251141ccb47fb9af6442

· e7e1701200b4dcde43a3c7b1ca0d0a464aa6fb3ee9b41044322d3101219408b4

· 2233322D30D35F1FB4205DD15E4AF94AC8E12AFC4669AE708EB232D28B3A4BA4

· 34eb7add5e6712f891858edd02ce1b757a7823e4cb7aad10cce0aeeb3f95d7af

· 1E53CF4BC67D3E52DA57D035B7522B42B5C7E2C56DD2CDF308F2760858BEB8AE

· 78B3702F5C0F7EFDF4598A2284CF3C7B3B51A6AE93A001029290BCC6A97BDC0A

· e5a9f2bbcb8626273d4294e3882aeda82bf14c636b76f2b6b22c51e0f594b2b1

· 4E003F6E8DAB88C9A1A95114C4F877B09552B45939BD069DF7690AE5DABA080F

· 429ff495ec7aaf30c4b4e4955ac31e102d28a5a681a56b0dd3afc3adb961c049

· 73a2627a68783cb4c7ca31691650625d3fb869b288aaf8e728b8030308af3368

· 93216c79101225abed1dfebf96cc26185ffb4232555bdcd22e1b88829282570f

· aa38a265cb7549ab60754df13c7bfeabdf94cdae1399160196b9f9fa17660744

· e4a971ef5331af68fa1982fbfe3394295d9bc0877d8ffb5ffd3068bb28601b5e

· 07440467F2F703E1C983DADCD57FE1F439866C0FB77EF3A29B9578F14B3C1730

· 2890222D2FDD14695E6DA012DD9267EB5F7F5F5258954560E6948203A5360A62

· 5f08c3944bcce381718c010a7c02c8d68279ee48d06a873710f3805d30a18ecf

· 0ff9edbf1596983cd81288be1fb6cc48ce562f4e0998b0f8285e661d44170b87

· 5075BDF160C4BE0802402DE6ADA4B8B6C6D36D3D31848D96E3C7A57D893DC3B6

· ce8cae98d9d48bdfa7b4c82c0b77a58db69ea79e22a9c56cd19944231a1dfe60

· 3b121eace7be5a6a6539fd0e11e7fe3e6baa39f589346707389008abd02ce341

· 4fff97d8e49b1f7cd246ed5eab2d240f5c4593015f20299e997dca4a8393a5a4

· 18D87C514FF25F817EAC613C5F2AD39B21B6E04B6DA6DBE8291F04549DA2C290

· 370c3f47b68ebc1034e7ac5644bd81b3cce15086a9cb005f1ed1960c0caf1934

· 6d0a906f3764e755d50412c58e70868db223da4a4a6ce1770f27dd9042a869bc

· 0f0efb305b6e540eb852774ae9584cc4b17a52bd8b58396937eff737690ba279

· 097fc545f5ff633010087cee9877d46cf6b8b0ad5a1cea4a806422f90f75b5c6

· 08adeadccb3d6bfa15887938f51ecdc0c851076a5b6c2a0e0eb0d7abdfcf2f9c

· 6a623c14640b37043a88bccebd644b064438eb42554e533bde92f5c0912729d5

· dda674fa0e22996523c50e39b29b84957b39c33e3bff4dd738341e2c93c96aad

· 1E3BDDD68B9DBDF728AFA28A29DB324B21D71FA145E6EFFF8D44B46F3637D9F4

· 814b4a99e0592abb948dc857b085141f06b969ebe7a738da29d88cbd9e276622

· 897b2676fdb5da61acd06b21f74b5afb1c332838c22c1ba070ec41e23bc297c8

· 79831c653ebd81093024ba5c4fef1bd33d3279b2a679e53f7872cedbae994317

· 8ea323ea2cbc99bf435f54b5da888f484250cc5458aadd16b015ec14d8d55f92

· baa8ed7251e9406d80072ca81023f16644650beaa25edc0082fa99ac28fb7acb

· 9BFE77CF0BA2DECDFF5A40401596273CBD7C8F072F4D1793007251DBB909F289

· ea673e0e6986e41a73c19dd2a9cfde3d2d4186ef52c23c1253dde2d54faca7b3

· 7cfe87d2dae654414493525445889bf8426b55d5d5674ee4e7de676598057d86

· f1c3eabcb797507944b757643cba34f5bb7ed2bf493f73dd43c4b1513a7c41f0

· C301CA1BB6D643BACBE814C9F43E8B3BA8C9351ECA5C9CF5834FC5740743B5E6

· 6EC4AEA4894D55CB309D396D74B826466D086921B3AF67C2A24FE5238F71B863

· 6973269a92d3447bcfe683db5c3ac69d20992cb39b58990342029cd0f54feb75

· de2816192691352a3d7f8e3b64552b2244c8c9437e223e2840bd7dd77213a5ac

· 6B7D5B7B647ED232AD25AA1A33597F4C75A5FE78B657378FC00DE3987CC7C1E7

· 72b4c69e07ab5cd3975fb0deb6ac46a73b88581386fd9a7e8ac3ac55a43f84cd

· 72fe2b9da5b0f6a19c5c983857b92bbdff4ffca6261d0dc6a71b1ba3e84a6d6b

· F7524F192F897D6166284EE8BC1CAA16335B4D097BCB686F1247C10BEF208762

· 8224e52c7b03b7287c43a545a8889a1a57ac9de3d75ff7effaf8d1966c42132f

· 087FF871A8D10CB876601850D8C2BC976AC213EDEDDA4FCC29056639F0888074

· 76fb51b5a059403e86ebfd733fe24e26b80af9919db2b5c482e3bceb8bc47178

· 37647FD7D25EFCAEA277CC0A5DF5BCF502D32312D16809D4FD2B86EEBCFE1A5B

· fc6ab939f5f2d6f12cb1edbe2babd5b180d8d036fc0b37a77f784d1c52162112

· A851B843640CF2AE413BEC04AEA0DAF580E5CC73D53CD8789AE1D1D5476695CF

· 811a57437bbcd7c0b1e0d7f29acf2403f3295b76f086e19085a8b8c994eda260

· 8e591717ec1ac52d0dee2a1783325b8b5f8aa7f0f9f4d576acd83a6cd357bad4

· 74c69940f96ccad21c7bfa75d6ee8dec4a78b16e0a32abe104d24c2076a574d5

· c900d84786405d5e834894416f20b78d2105ddd4fa88c015cc1fe18e5b1d4c91

· 2798FB13C7B43C643D5EA87EE8934ED5BC5A6E6FB54A190D8F72166F0DD02124

· a62999864a35b612153daf4a4185916a6877e820cadb807c55d48e397571423e

· 16197A321FC7B0A2A311E689621FE4A7CD50FDCB2D163973A31E4FD6352232D7

· 952adea6ba0359839498c2f4ce4f27a62b38e42a47d10c91d37ea2e37b90379f

· F75E5E1905D8DE78F99F28710DCF9774C3D5D876DD3C1CCBE49E18A6B47AAD2B

· 3706CD2883BAA6E9EA31962E6118BDB6609237912C567148FE2A16904BDA7256

· 8d116edc989d8799eb60d06bc756b4b25598e9366be05235a3f6b1158bcf8e08

· ab36a0c302c66da8d983e13e538bdd6e5eb536bd712be6e72583612377be5b8e

· 8100929a607e0ff92bfc6c6c2d7f9da0833a2318e28e4c4536996ba27d0852cc

· dd49562418564204ddd32d8dfa5863abe4dde11426652d93cc57aee0c2321119

· 2f06ba8855a654f47fbdf6b12c1a99e67e6d003ff23443f92c1f467f32f98fe3

· 6570F12A91BC387E6FCF9E9489EEBB9876E0552D88E3D1BFA94624A5DA0C511D

· c79e75ebdbe79a92c803367bab8524e576288cf67c39ea7168247bb3f1671840

· D79D3D48100CC6E32E0749F1A93B482CCF67380A3F32286D87D842AB1736C8FA

· 60e0bc861c9d3f7295f752f4aff76b0b912e50a4cc771e4578d116b08de46d63

· cf5d6c68811f37d9ae1a9cc62abc1987fdd8900d271fdaa01d4a84853d7db10d

· C5D23B65550EB6F72BE2129B0D585F36CF8042076F003D231EB2003F54E6A838

· F9B12B914595CCC1FFBE61E542BD831B3487DF4C6183A82D3C6C942334034C9D

· 9734CA4B48E229C7F2FF7AEC6B8C111D530E46A9DCBC28433BF8ED0A1E2A3E53

· 58cd93a04edc27960c8476f83ceb1cc974dceee45be092af8f47064f4271d229

· 79c8b9a9dec4516b7a6efb97f34dd6cba2cd5417fa06855f0d4def10c8c6d766

· DF0A6D50EC73F05E3D92C5F58FB3A0315C7B2B77D521BD65DE0A289EA1C5B6B6

· 73f9e415baeb063b708cdb071ddf15082393c21cb63f3ad48ec76b10a83dc4c9

· B628EB5E768F0F157137D64FF41B3B991C56B745B3BADFFDE99B2F25A503337B

· 691f7f1ed05fc3c1109b1b8b43791a43261e073eb4013572de20b95f2e4ecad1

· 7CDB07238C8CC903E13E689D4DE1129F5FB3B647E4A1C1E98C5A0E8516184ED1

· 36f37080271b81394b03a84f0fcf2717da127f8d8adfa31721067616d4043143

· 8e12fc5aa85d6953ee731203e945ccacc4ded6a8aa9752c7331dcc17da501eae

· 529d3eccf1000887f5e35b3eb8e732066b819201f37651d1ccca41d5cc2c1513

· 6D50CDAF103349ACA0177F3D6A52AE38A43BA2FC5EDDDD76B3B914ABAFECD321

· fce452bcf10414ece8eee6451cf52b39211eb65ecaa02a15bc5809c8236369a4

· CFE0D7D43B613DDF6E63D2DD414B96F505B958CDAFAE22031966703DF4B882D8

· 0c5514d1a7f47cf876873ea461df0b00810f3d52c1788835db532168516bb9a0

· f7102d06ded68bddf3c93992ccdc41182629cb5a363ec999114fccc1a526c49d

· 64D0FC47FD77EB300942602A912EA9403960ACD4F2ED33A8E325594BF700D65F

· BC694C165646842697DB370A7688753A08BED7803AA9AAAF626E54AD77B3B0FE

· bc5886f4228e2795dab87a83e7bb6d834828821226d5e6e9b7a6785aa4a803ce

· 03a40539f0ad693acb57c8dc7453d185a4d0976c4dba2c1de56bd43e0892654b

· b16251ac78b661937e98799d27c331d5c0d80e8e267da4f75047158ac61cc787

· 8738866be2f39ac05df243bbe2c82dfc6c125643cc5c75e5f199701fbacc90c9

· 0D8878CCA08903777888B3681F90E4A07C7AEF7D9600A67DFA985844D4BF5EDA

· 1E5385399BD1A8D6D531B820DA88D0B217B863EC2E7100E1533E64605FADD898

· 2663e66088753a99f331b9f3a6ee23807a96d6d6fd3df47578b4a69eeb342adb

· a4dd677885647bf091e1e4943c5349e3b66d6364542aadf6905205e4b572f544

· 7bd04eb149ce6efb4470a66ed228375ad9a1d8355d9e4ce68bae7226527b122d

· eb3dfd03f0a882d286ca3ebad884cb513c7f42085b8b2a1a52315d231eae1f9a

· c6433b04483bef0219467a3fc58a5859e57b2ca41eb713023fcbfda8f45e7506

· 5d7f212b4f581ccaecfeaba1c1d3c6aedc76356c362bd6737daa4ec6a834a5b1

· 8b6c6c007efa8e1a7da241564142f8a8a934dcce451c7e522cdd86292e81ead7

· 72a53cf0020911b0267f1be66fad768b5baa979b2f0945452896c3e7d47d7369

· 697046df70499620a5d72d0afdca2f6a795303e2399bcdcd28a44dd0ce3dcd23

· f84145edc0c57ac9ba6b4eab365c2e79ef74da860098e0a7a8b224116c38abd1

· db34f90a2aa2f37cb18fca54972b8574d1582f6ea0ef51f5d452551cbf36a28a

· 171bfffa8b8f9bdfbcb8d59dce33f5689fd4b6d6b198b2986eb65ec44cdb3443

· a838ed47fd3a5fa4b21c83d1fe2ddc1e736634d6e5baaae9112ec48760c3f5a5

· a52f3fc87b7c383a12fd8439fed29e57bdbf85dae2fbc09b3931815183a01768

· 22b5dce4881004cd5491a450ccd459dc4790f28e8dfd9765e040b51003cccab8

· 43ED3E85A7F0C80A9B532C11853A30A39A570B57F9E61703426BD6F25C30DBAB

· cec7a486b713490d937b9c3f8737da954b8dd188beab63302949b42332971044

· 35ae3a7c161fa67520cf9ba04878d8965f998e08f3402b141acd236b53ba6af3

· C105894E55C27E224B68ECF2E7F87978A0655584FDC870CE9C848A39B7E0AE89

· fdd30f479b2af0bc856ab7fbf128724d688d358fb7a3d4161bf07f5d35cb9ab6

· daf9da77300ea5a32dc143eaf12c3bb6bd4c4876f13facfd7fd5982cba1a0731

· e8da78f9024083cf6a382548e9c38814669ee5ba8e51ec43b43e8140243c6cb3

· 18157A08BDEC511B1510272658E23FE2342AD41DA8BB3CDAF12E557EEFDBF474

· 8263f13e3f0c03bc3917bd7aae0e3e42b0be10ccc6ecfb1188c9f6feb042d44b

· BB111DDFEBEA4F314060C665E2B5F58FC2C3478C2C3FE03198D72A23AC546473

· d1c084cdcdd7672904790fddfa751780774d8170ac97ad457a7ac7c5caefe817

· cd077900d5fc72a03e6247cfb02ce3f4f42c7e6384fd9f4ce248dd012936dfe4

· c95530bc11cfd8ef072f99afc640ee1f972ec62e36188dd0dbb6e1df8b7ac19b

· bd7c59b9a903c079b195f00395013635ddd996cb34e24e395765f2255312e96d

· dbc54deb6684b4825cfd97a620abd431ede7c3095ecfac3897b0551e9bcb57d8

· de797af0a3d8ceafc75328b4ad5a5ec61692c43a19527db63735f285b5409fc4

· 70026BAEB568EC2BB17ABFF67DC8022B12F0DD6E8787C82D81B26EFD577E6D84

· 7496609398d4282a1f42adb38614804192d9bf11025d92895eeafaf05fe303e1

· b2304293937cc02831291056f7ea72e5a2546b2e9fb87e4d6985203eb55901f7

· 0522678e81a18303b2e93c3bd7a0e9f19e784a7c935eaf98db19e91a3a8f7166

· 0EA0A41E404D59F1B342D46D32AC21FBF3A6E005FFFBEF178E509EAC2B55F307

· eff77b8c6e9960b8928f7b4280a34ed4b7660d34585ee129a01f2acddfa66969

· 96ca146b6bb95de35f61289c2725f979a2957ce54761aff5f37726a85f2f9e77

· 10864e706a8c593767c6cdfc6c5892e422707b33250b845b60338f0d5cfa6c37

· e3d0328e947d418f01528a6e40ba13f0fdbc3307c539931501d59fd9d4f58a16

· 46C5ED90E3D6B8BC85AE369AA87BA75A12EED6A7CFA8EDEB497E5EC7F7C75D9E

· 10335e3afc5d9867a124680fe12767d53c7bb181c748129f42e22f77c5a6c205

· DF0495D6E1CF50B0A24BB27A53525B317DB9947B1208E95301BF72758A7FD78C

· 5AEE3BA5ACC947091F9E0837AAAF2D3F81FCA38AA5A9EE9A65925D69296FEE75

· de91a5b9b49ae33afc4e87f71604af8848d7bbc500a71c1ebe78d3ebb9365b51

· c77da2d7f50cb01181dffa8942289ad04e57f0e38d8b2ee05a4ac11dbbc483f9

· a2f4dcba192607e2a8889f46a7ca20c8676ac15bccd55097d3983240371e71ec

· 663326B44B1FAF8E7E7192C1D69959803A2FA02870A7756FCD2745D9BD91E02E

· ea39a1add9c174b88fe8e116fc89aac2ddb64ef91dd7c449aed99acaafc52c33

· 4088a7f6662a6104c785126b69f1e588260bad1df2db507140b5974f30a464a1

· 2890222d2fdd14695e6da012dd9267eb5f7f5f5258954560e6948203a5360a62

· ea8f893c080159a423c9122b239ec389939e4c3c1f218bdee16dde744e08188f

· 1EA0E878E276481A6FAEAF016EC89231957B02CB55C3DD68F035B82E072E784B

· C92D4927D6E5D4B7FCC989D384A92862FC88B1970C4C01DEBFEA770ED02D59E7

· 21e89038cbfb3e90ef7bd0f7115de19a4eb81907f881153e7f43896a3c704139

· BD54882ADC69FEE47D160D5245F8E78D787AC84BF0DAA64D0FA03DE5F48F4D7E

· 8e16d1403b8faea9ad07f105735b6b8973fc22a914ff64365cc2d3917e88d641

· 5e9f9643c2762af1e70c675baa1a0bdc8569ba66c29343783506aeb43e6cf5e3

· 4BA483FDE18E3600085E94315C389973F1B34738DAD95611D8007892A2F70F54

· 008BBBFF530DAF5D53663A32F1355CC787EB14C485EE74EE03F7F33993DB33F3

· e15955057ffc7d77bca1ad9cb25323af9bf1897a59a5de2935408cecc60d9257

· 72AB2445AD73CEB4C6CA84D166D5CB01478752BFACDA2366E560706B77B8D920

· 699dbe66ce536373123ca04819ffd5373fe6eb342511cc90bae6636822bdbc60

· E05A7B47A4DDF8E85C1DD406FCF62D4CD3DE7208212A6D0E9360C06E1ACFC1BF

· 62b3951ada0420181ab4ca937270c00a56cd18a1abfe40071899fa29fccc4b92

· 2fe932361571199fe36565c0c71d4029ffcf22b44e61eadb7b3daf2b034ea861

· 2934aa4a67ebc93cdb76386d64627786479eed29223c89920fa02399bf1fbc9d

· 37034f91de33daa486f169d16d8be4a0c14cdeb31e760deda8b70eeb69bc8835

· EF5AD9C437B21E836673A08FABE4FDD2A26B050B724525D5C225335DAB26DFE7

· b518136fa3638d8fa4469a2df4cbc93d20a96f7f47abee972cf32258b1b38553

· cfea9125ca9e7cc2a24ad7c2d2d4020d6a7dbe57fdd1c536144861e0ad9ee06f

· 4D045A1B78D5FEF7CB9A893900EE0D286A7ED170CB35ACCB16FEFAAFF5539B97

· 30a4c977022561b721ac99429689efd881089308f208b744d711c3ecfb6bf365

· 11e7a00771278ad3931332c4cf062e8ca01a70ffd11d5e89e3e428d30faf572c

· 6b4a0d877c2097591256a80b5547a02bd95ec24a8d9aaca881fbe728f2453a71

· 9C30732E6D23A7B81FEE0037DD8CA089B6FF5E5EAA9E41F2978B52DBC55EF165

· 80B22764A857512DA9BF80D39B92B4C8A4CB258E55806EABF84C01127ED6C06D

· bb1921ca562d22d3f76c93ba390256216f47ef6fa32c8bf9b140e907e6471695

· b692ff8a44bebfcc88c2988db48c6d8294ef1cd2de08390a7a7fb9ffe26ccd63

· b578da1e149637b9a9d30ff264d1033aa3350d404cd173bb314ff05dd124a2a6

· 3debe4ce2ae86ef609aef86ba67dab2ab08eea4e3c5211ea349e8959de011f46

· d65c32e7f1c9ee5ea5f08911a360575c12bca545fdebca3e0e4c7b142ce79edd

· 2dfb642eb63b813205a6382f25deee8ba8727b7f4d4120ab1fb2fad42f7b47e9

· f55aedfa7be17fd9b69b3fdb1e4b864df0911ee6d69f7f222fe806c7e321f09b

· 00de24dff6de0a2fdfa3c83150c4aa38c292d6dd9f5fa55ee2c857a82f879443

· 1e53cf4bc67d3e52da57d035b7522b42b5c7e2c56dd2cdf308f2760858beb8ae

· 2186ff1e26c311636972be67136135bb4ffb78f65619f110419b83f1374c555a

· 8532a45e21a24ab863581ae7f24f4531c33edfb7a51500227ee8a6553bb4bd84

· 749ea9b55273ed8051960ba0aa0a31721a1cd1fecbbb253da3322df745aa40e2

· 8ccd538a5cc46278409e736a26db8c9d6c57452021be1ffab26a85b3229083f1

· 5C5764049A7C82E868C9E93C99F996EFDF90C7746ADE49C12AA47644650BF6CB

· 1c73dae4a75c01a64709dc2dd602c072457118689fe863990022b40d523b2004

· 23c2744610736f5ea8e9b390e3b3cc800c98b661b8362bd2da3eee2f62fb51f9

· bd3df66ddce687239ed1b4c2664899a842277d0ddf520892ff01a6d47730395b

· 18b4c0f61fd753646ae4b75d1835df351ee9b18500f7a0671934c926b1476355

· 805C7DAEB376520828028A8C534984F8A268942253AA332DFE7066A0DA669F46

· 1927c89e8514cc8d7516d4513331a6c461d00547d107ffb7985742c46806f8f5

· f8dff2241f7caa824b1a83b70e8505371ad203927eafead0344c0bd86204544e

· e2d26a1e9d2ac16329c2b488866595961c068154af348bf777efbd637bc68c2e

· E9B65B8F156750E62F742680FD1E476CEBF2491DC191D9C4480597F3EAFCDB83

· 6C9E0FAE988F29598BDEBF2C3744083A22F444E7E91F48E63349E1268794E84D

· 695c8089eb0a2dbbd8d43f3fe703816aaef82a4a4730a3d6e76712dbaa57773e

· 7DCA7E080134492DB1E121E6F8CBAE6F65B4C9621940DE5D4AD9CAF71DF72DD9

· E38B88B3FCD72AD804AC1B10887A3426EDC0ED15A136E804A1F85941C7C8E62C

· ed8ff09ee7c0b9ff801c90d130d8d553c9a3482c8861251b5e0b70e4cbc55d86

· 72FE2B9DA5B0F6A19C5C983857B92BBDFF4FFCA6261D0DC6A71B1BA3E84A6D6B

· 9c30732e6d23a7b81fee0037dd8ca089b6ff5e5eaa9e41f2978b52dbc55ef165

· d35a34fd18d0b6b81b8f4ce82a08562eb2555a71ea67d547e62749b435e86d7e

· 95625d2437a53736cd1acbf5f83be50691834b0c7a2c1988f3865118ef52af24

· d6d80231325c39b421d06eb3224ed54d958c1d643d961048176f2a93eecbb524

· a97d6cb9745af75d6d019d5a81c3c2f844ee867a20ea2a4c84f1b1e960f054a5

· f432b91c9a48f98ce667b0da5a94b6f5ceca40d69f7e56d6813423a16ff3306a

· fb3d83a155d8c24ccfc953800a7d147311fe1dec14f7cfdb2b1f4815676111f0

· 787df38b2367f2f4601ef604235e78ab3c6167e8b9214cc904df10e31ad383b4

· 7f7b65326073f10129ce5474d8ffabbd822d9fd00eb5d7fedf617afc99a598c3

· 8d2ab8055accf560647c2d03e47a62453956ccc9b48c0214e966f18eb87131f6

· eb7c1aa98542309a34fbdf708522d6915af8d5753168f68c463e61a00cb724fb

· 7aa7c115e4a4fd11d4d67b8f4ca6602998bfc61231d7a2b2f24a953220a00f80

· c63a10d8a92a5348801360fb963792f3f4309d6801eee6fa63038333f6b5d830

· 3ad9151c18894372cd8add3fe20f07bb5ca6df4de6b08b225a5341b1f008cca4

· 699195B2E86918EE23109C22A9DAE9A32B19466C808A4B6C29337EB04D4C9242

· 71ceb2f9ac1dee224e90025826e8f9d49f3737e38c7270fff0edef37d062b6ba

· edee3d980f39e29a49472679d6d915f038fda1fd6e27559f432e3296e645a98c

· fd75f97997d9bffb19e3520eda7f702c7e6b2b9d9007804a7cd13c55d518ccfa

· 38ef6e6e48f23addf853c7635c9444a3278f4875c10acc146457668deacbaedf

· BAA8ED7251E9406D80072CA81023F16644650BEAA25EDC0082FA99AC28FB7ACB

· 75c65c18b853095ff15328e747103ff63ac646c0b91f982cff6f4d3d8fc0bac8

· 4311369cdccedeabe7e1d68dd6ae1ee22f9e63d8d812fd66b53227c2331e5b05

· CA8ABD64F55B402A61FA8FBC1C79A5706021561D96CA7A391CE6F4503782300B

· 1876B3A1FF2984C168BA9A4F2C6B75348B2037F9C5ED2E8513BB43BE74153F41

· abdb3783dbe5e397d57380ea6a8c2cda998a6af42c47a10f1ce3c1d2b5592a31

· cc4ca35770e4862da94087f5fad72cb488fd3674ca7b1f02b2b3e911bea7efab

· F1E2F82D5F21FB8169131FEDEE6704696451F9E28A8705FCA5C0DD6DAD151D64

· aa8f395fdf04bff4fdec0e14034f7e52c29ca403a962404d99f156012e2edc60

· d907d8c31d0fd689f76d1d8b1bf4cb74b83524a81f05ba363510bd9794ad8197

· 9f376bf136a1f68b0150936216a041c0ee3b2b3165f6d6d74a683541f0845d72

· 36e5303137ea51addf3f10554abad8989f0ec0740cfbcd81faf3e40c1bdd3b81

· d044dd2caea86fbfec6f54d5e8190a86198f6ca6522bc57f2f06d8251b72aea4

· d0987cbd70b07bc0f5b5a82c6157c5d47563d7f2c8aa123b4b0182e9182dcc83

· f8818081bdc2dbf059ae5494a06fe2893900190f27b26f7af29c8fad95ed7ab2

· 8428ac92017ef075b2da8992e29b6550b6f0c4e3282d7f5f1c84b9e234daaac8

· 1db0dc619d3be1983b65273330f390264bcc6a8b0878f0ffe1996c1ec0263e49

· bb111ddfebea4f314060c665e2b5f58fc2c3478c2c3fe03198d72a23ac546473

· A86CD95594771888B1CA6F4BF6AEAFFF8820AA6680665305520E0D2F9C0AC4FA

· 9bb7aa4615f7ca28639f1235c2d6be785b702a5bbe4617a7b55384afbfb4c7c1

· 251e70dff8eeb33393763951e995461d3050db48ea7de480613cd50435ca4d07

· 932888435c8d3da6e173eea11bd35066eb1bfb285e7454f19c15ed2ca3c3fd03

· 543a09b2873baba4b1613da24fcf4b337a2115ee2b583bea404e8043f9dfa92a

· c0a30a69aa180aed1311b1c28dcdba615cb78e828311d84386b9182910143de2

· fd4932f19ee4494bcd4ceaa5a445a74a210f3a044eb75dd3adb359dd4625c350

· c9cd44c4bd729e856a023d706f09dd0e249415e7da90d386b1439c3a0fbe6e3f

· 004dc00f66098d37167a52a7fc0814f497d30814dc00a8da7083a4765510d79a

· cfbc29604609d96e937bf09f4313e98a644a4262839e8e32cb0ce9c250ee368a

· 2524D01ECB63CF59FDC21DE03F6CD012C8CBADD74016923A69228AA6024674FE

· F4FA5B3E56077D29E3877DBC1F2C8FEB507FB4ADD72F6023DDB6AF00BAB7FCF7

· e8c53bb41b90d991af0ee2e5a7bc99473c0bc4db2cd1e683f8a513ad7d2601cf

· 7078656ed4ea736c286798b097fb65511c6dbe1b1f4df22d594b867395a213a8

· 7fc9731d88f5a0598d883589b72b666da065929b554f9d2bdd966dad29800041

· 6C7D1623CA13FB45FC6369BEE06C148121A6DF40E41307891D3D2B77D5DC3C7A

· 4fd1ae48e9470891915cfaae7b68c89ed601b75c900bf5ad06a2d5ce05579268

· bbd98779726f138b3079a3a54ca67bb5c03649130ab0d8511cdc5d3ef5140098

· b4361d177d283a5155e6e06ad673bbe314f56fee7f8c29634dfc1938381e651d

· de4e579a8a8c83c0eaa384146a5a2d2e4d1d3f32f3da8c877f1276e962e9e7f7

· 2D61625A0E63AB4491DEAB98C76AA02BA583B4C655B55C1672B74338C20E39DD

· 70f3f4df592b84eb9089b2d80ed347198dbbf5a2ea7157f8e064be3fec842c6a

· bd6e38d4e3fa8153f9400f34fdd09db3a17cb89c95167bddd3035d7ece1199ba

· 3ec4885e51bb83af594cdb7ab27226270e6ccf38258ca7bd3ed0b3c5ed1ae04f

· 80b22764a857512da9bf80d39b92b4c8a4cb258e55806eabf84c01127ed6c06d

· 81243E4919F17341C1EC438D55B3528F8B452A221CBE74D00D825E64AA19AEEE

· 79fa1578f06c01c187c432878f6080df7d01883eb656900907b6b437450bc8d0

· 736525350539904d19d4028dfc6be5feac95b662c0cc841bed640794cfb2e8e9

· 2cc92f98a34b82edcf67ef68d09a119cc4f57ac1e81348ce5272ecc1a25c233e

· 32133D31A507047AE10993A7F9634E3613D8B894FD07315DB266D82DD40976F9

· 19c691efd348a78c6b8b3f496a182b37db26205de206c64b573abc5af84e2e1e

· 83D419350EE663283D207204F00198A4740DC40EB4562004AA426E06FE197AEC

· 0D2FD30F5EAB419BB0D8ABDB835A6BB86D34406CCFD1BD6CEFC2BD86C2BF2CC0

· 7bfacb09bb3b16c5e8f6cd83dcf7fc28fbdfaa298b589aad1efaf3b9777c1dff

· eb16562b15abf2d0b58658b014ba5d6a7dbf34c3df7921b25ae17d58b9f5929e

· ca49f449f9fbb12f74c3ecbb5208e6f3153ee3dbdaca03630297bc0e489565bf

· 13e1f6e19b9094f56128bf5b8fd22a9283206e34d1c97cdb78f73fc2e2cb8683

· 854b116a65ed70ae7ab18be69af4bdb68078e50603e519e587f21a308d258d53

· f58eb772a3f828108025ed76fb6ac2a181b5e92d4cc0c733e097c04c83b02dc7

· fd654d05a7124bfccd117ba172b7c75bf4a2da6d37111f7f21c3b6d946bc7241

· 42ba8ae0342777573b25e5bc079a14a2e4f952aa5c585983de8f54fc6aeca83d

· f75e5e1905d8de78f99f28710dcf9774c3d5d876dd3c1ccbe49e18a6b47aad2b

· 95B45CD112424A61DE0680230D4AFFD0102CEF13A49F6AECBC819425F4827756

· b81b896b67a7786ec06f259516496a57880e52a42e9282cf8786d0cfad44f1af

IP ADDRESSES:

· 5.181.159.0

DOMAINS:

· duelmener-naturtrailpark.org

· script.au

· bizabiza.mywire.org

· streammobs.com

· selectwendormo9tres.com

· stachmentsuprimeresult.com

· pjnbadfjandkadm3kd.com

· lili19mainmasters.com

· newdomainfortesteenestle.com

· strongdomainsercgerhhost.com

· wegrowcoaching.com

· asareholdings.com

· elshoppingdelalimpieza.com.ar

· jenb128hiuedfhajduihfa.com

· projetodegente.com

· newdomainfortesteenestle.com

· aakritifitness.com

· higreens.co.in

RECOMMENDATIONS

• Ensure regular review and application of updates and patches for software and operating systems. Formal patch management process.

• Enhance email security measures by deploying advanced threat protection solutions capable of detecting and blocking malicious attachments, links, and phishing attempts.

• Educate employees about email best practices and encourage them to exercise caution when interacting with unfamiliar or suspicious emails.

• Utilize comprehensive endpoint protection solutions equipped with behavior-based detection capabilities to identify and mitigate malware threats.

• Implement endpoint security policies to enforce strict access controls and prevent unauthorized software installations.

• Deploy web filtering and content inspection technologies to monitor and control internet traffic, blocking access to malicious websites and preventing drive-by downloads.

• Consider utilizing secure web gateways and sandboxing solutions to analyze and quarantine suspicious files in a controlled environment.

• Segment network infrastructure to isolate critical systems and sensitive data from potential threats.

• Implement access controls and firewall rules to restrict unauthorized communication between network segments and limit the lateral movement of attackers.

• Implement MFA mechanisms to add an extra layer of security to user authentication processes.

• Require users to verify their identity using multiple factors, such as passwords, biometrics, or token-based authentication, before granting access to sensitive resources.

REFERENCES

• https://www.trendmicro.com/en_us/research/24/c/cve-2024-21412--darkgate-operators-exploit-microsoft-windows-sma.html

• https://www.bleepingcomputer.com/news/security/hackers-exploit-windows-smartscreen-flaw-to-drop-darkgate-malware/#google_vignette

• https://thehackernews.com/2024/03/darkgate-malware-exploits-recently.html