Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

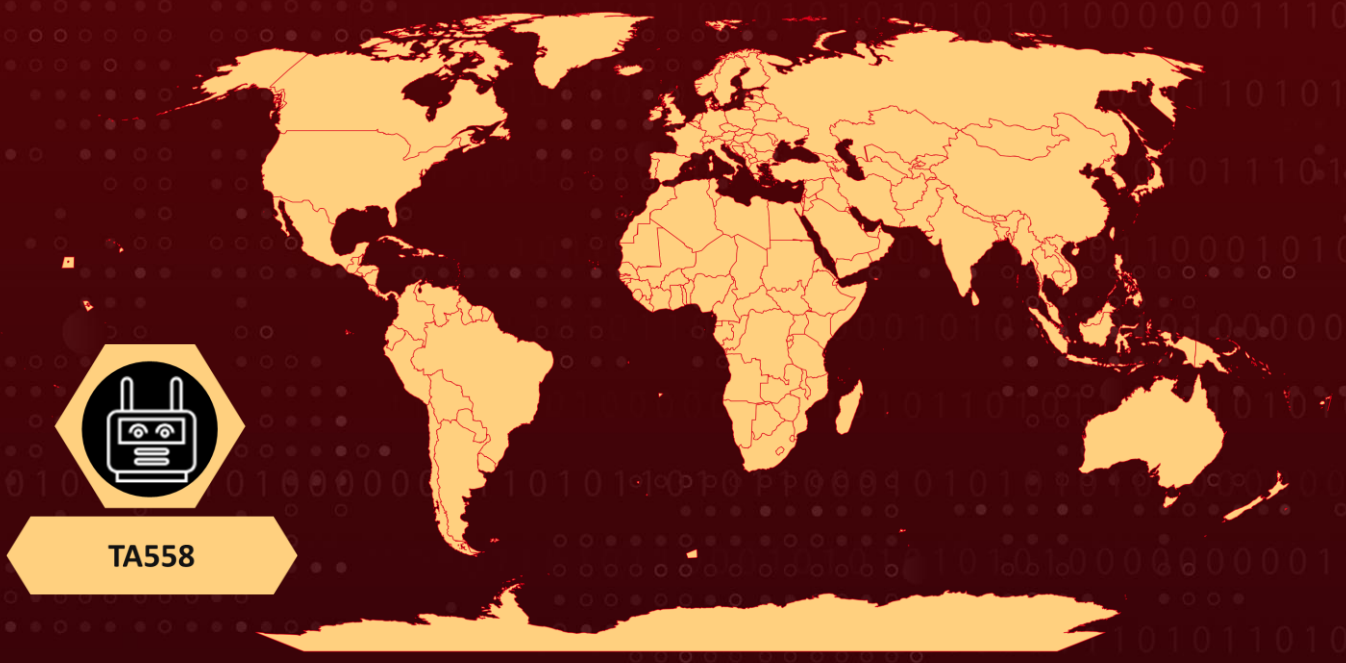
TA558's SteganoAmor Campaign Targets Organizations Worldwide

Date of Publication	Admiralty Code	TA Number
April 16, 2024	A1	TA2024149

Summary

Discovered: April 2024
Attack Region: Worldwide
Actor: TA558
Malware: AgentTesla, FormBook, Remcos, LokiBot, Formbook, Guloader, SnakeKeylogger, Xworm
Affected Industries: Industrial sector, service sector, public sector, electric power industry, counstruction, Transportation companies, Sports, Information Technology, Education, Religious organizations, Finance, Pharmaceutical industry
Campaign: SteganoAmor
Attack: The TA558 hacking group, in their recent campaign named SteganoAmor, is employing steganography to hide malicious code within images. This tactic allows them to deliver various malware tools to targeted systems. Interestingly, they are using the CVE-2017-11882 vulnerability, despite its age, as part of their attack chain.

Attack Regions



CVE

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	CISA KEV	PATCH
CVE-2017-11882	Microsoft Office Memory Corruption Vulnerability	Microsoft Office	✗	✓	✓

Attack Details

#1 TA558, a hacking group, is utilizing steganography in their recent campaign named SteganoAmor to hide malicious code within images. This tactic allows them to distribute multiple malware tools to their targeted devices. They embed RTF documents, PowerShell scripts, and VBSs with exploits inside text files and images using steganography.

#2 TA558, a cybercrime gang active since least 2018, primarily motivated by financial gain, focuses its activities on Latin American hospitality and tourism businesses. However, it has also been associated with attacks targeting organizations in North America and Western Europe.

#3 The attack begins with malicious emails containing seemingly harmless document attachments that exploit the CVE-2017-11882 vulnerability, which is a commonly targeted Microsoft Office Equation Editor flaw fixed in 2017. These attachments trigger a request to a specific URL. Upon receiving the server response, an RTF document is downloaded. When opened, it executes and retrieves a VBS script.

#4 This script then sends a request to paste[.]ee to obtain the next payload. Subsequently, it downloads and decodes an encoded malicious string hidden within an image using steganography. This string contains a Base64-encoded next-stage payload concealed within the image. A PowerShell code embedded within the script retrieves the final payload, which is hidden inside a text file and encoded in a reversed Base64 format.

#5 Multiple attack chain variations that delivered a wide range of malware families were discovered, such as AgentTesla, FormBook, Remcos, LokiBot, Guloader, Snake Keylogger, and XWorm, were identified. The group utilizes compromised FTP and SMTP servers for C2 and phishing purposes.

#6 AgentTesla operates as a keylogger and credential stealer, capturing sensitive information. FormBook functions as an infostealer, harvesting credentials from web browsers and capturing screenshots. Remcos enables remote management of compromised machines, while LokiBot focuses on collecting data related to applications. Guloader is responsible for distributing secondary payloads, while Snake Keylogger logs keystrokes and captures clipboard data. Lastly, XWorm acts as a RAT, providing remote control over the infected computer.

#7 The TA558 group is using steganography to spread malware through attack chains, posing a significant challenge to detection, particularly with compromised SMTP servers. Companies should diligently monitor network traffic and investigate suspicious activity, even from seemingly legitimate services.

Recommendations

Remain Vigilant: It is essential to remain cautious. Be wary of clicking on suspicious links or visiting untrusted websites, as they may contain malicious content. Exercise caution when opening emails or messages from unknown sources, as they could be part of phishing attempts.

Robust Endpoint Security: Deploy advanced endpoint security solutions that include real-time malware detection and behavioral analysis. Regularly update antivirus and anti-malware software to ensure the latest threat definitions are in place. A multi-layered approach to endpoint security can prevent malwares from infiltrating the network through vulnerable endpoints and can detect and block malicious activities effectively.

Implement Behavioral Analysis: Deploy advanced security solutions that employ behavioral analysis and anomaly detection to identify unusual patterns of activity indicative of malware presence. This proactive approach can help catch sophisticated threats before they fully compromise your systems.

Email Security Measures: Employ robust email security solutions to detect and block malicious attachments and links. Consider using advanced threat protection (ATP) and email filtering technologies to prevent the delivery of emails containing malicious content.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	TA0001 Initial Access	TA0002 Execution	TA0005 Defense Evasion
TA0006 Credential Access	TA0007 Discovery	TA0009 Collection	TA0011 Command and Control
T1588 Obtain Capabilities	T1588.006 Vulnerabilities	T1566 Phishing	T1566.001 Spearphishing Attachment
T1027 Obfuscated Files or Information	T1027.003 Steganography	T1059 Command and Scripting Interpreter	T1059.005 Visual Basic
T1059.001 PowerShell	T1132 Data Encoding	T1132.001 Standard Encoding	T1071 Application Layer Protocol

T1071.002 File Transfer Protocols	**T1217** Browser Information Discovery	**T1056** Input Capture	**T1125** Video Capture
T1123 Audio Capture	**T1033** System Owner/User Discovery	**T1555** Credentials from Password Stores	**T1204** User Execution
T1204.003 Malicious Image			

Indicators of Compromise (IOCs)

TYPE	VALUE
IPv4	3[.]145[.]88[.]189, 23[.]94[.]206[.]107, 23[.]94[.]236[.]203, 23[.]94[.]239[.]93, 23[.]94[.]239[.]119, 23[.]95[.]60[.]74, 23[.]95[.]122[.]104, 23[.]95[.]235[.]10, 23[.]95[.]235[.]35, 23[.]95[.]235[.]86, 45[.]32[.]86[.]119, 45[.]74[.]19[.]84, 45[.]227[.]161[.]55, 46[.]27[.]49[.]180, 50[.]3[.]182[.]140, 66[.]175[.]208[.]79, 66[.]228[.]43[.]8, 70[.]34[.]197[.]128, 70[.]34[.]220[.]238, 72[.]14[.]187[.]87, 83[.]137[.]157[.]51, 94[.]156[.]65[.]225, 94[.]156[.]69[.]17, 103[.]27[.]132[.]200, 103[.]29[.]3[.]200, 103[.]67[.]162[.]213, 103[.]133[.]104[.]112, 103[.]183[.]114[.]5, 103[.]186[.]65[.]80, 103[.]198[.]26[.]111, 103[.]237[.]87[.]56, 104[.]247[.]204[.]205,

TYPE	VALUE
IPv4	107[.]172[.]61[.]136, 107[.]173[.]4[.]5, 107[.]173[.]4[.]15, 107[.]173[.]229[.]146, 107[.]174[.]138[.]160, 107[.]175[.]3[.]22, 107[.]175[.]31[.]187, 107[.]175[.]92[.]68, 107[.]175[.]113[.]202, 107[.]175[.]113[.]204, 107[.]175[.]113[.]216, 141[.]98[.]10[.]56, 147[.]124[.]214[.]183, 147[.]185[.]243[.]107, 149[.]28[.]109[.]84, 149[.]248[.]54[.]207, 154[.]38[.]188[.]98, 158[.]220[.]80[.]156, 167[.]86[.]86[.]15, 170[.]75[.]146[.]119, 172[.]86[.]76[.]208, 172[.]202[.]120[.]36, 172[.]232[.]8[.]161, 172[.]232[.]163[.]207, 172[.]232[.]170[.]236, 172[.]232[.]172[.]53, 172[.]232[.]189[.]7, 172[.]233[.]129[.]114, 172[.]233[.]130[.]11, 172[.]234[.]249[.]47, 172[.]245[.]163[.]139, 172[.]245[.]185[.]30, 172[.]245[.]208[.]3, 172[.]245[.]208[.]19, 172[.]245[.]208[.]28, 172[.]245[.]208[.]34, 172[.]245[.]208[.]126, 172[.]245[.]214[.]91, 185[.]254[.]37[.]80, 188[.]127[.]231[.]198, 188[.]127[.]249[.]32, 192[.]3[.]95[.]131, 192[.]3[.]95[.]135, 192[.]3[.]95[.]216, 192[.]3[.]108[.]47, 192[.]3[.]179[.]133,

TYPE	VALUE
IPv4	192[.]3[.]179[.]162, 192[.]3[.]241[.]235, 192[.]99[.]190[.]119, 192[.]210[.]214[.]26, 193[.]56[.]255[.]218, 198[.]12[.]81[.]138, 198[.]12[.]81[.]158, 198[.]12[.]89[.]23, 198[.]12[.]91[.]244, 198[.]23[.]156[.]251, 198[.]46[.]173[.]145, 198[.]46[.]174[.]147, 198[.]46[.]176[.]159, 198[.]46[.]176[.]175, 198[.]74[.]57[.]54, 207[.]32[.]219[.]82
Domain	uploaddeimagens[.]com[.]br, wallpapercave[.]com, imageupload[.]io, 2s[.]gg, i8[.]ae, tt[.]vg, ye[.]pe, dik[.]si, qly[.]ai, tau[.]id, uri[.]ac, rdre[.]me, shlx[.]us, shtu[.]be, ssur[.]cc, toss[.]is, tyny[.]to, tt22[.]in, l-to[.]com, paste[.]ee, r2u[.]site, urlsh[.]us, qr-in[.]com, ur8ly[.]com
SHA1	08b7d3b19ee002fc1977170c94f26a412dcd3787, 6469e6950a845c31765412b16a2031ca48212a88, c764d6470cf3932ce3a13d5c05b14e9a236ff0fa, 8bd40194c741c9ac9ee50c348981edca15a5519d, acd3b796d5665ded2feec9405348375507fa7a61,

TYPE	VALUE
SHA1	3d687920329bcad5a1ff5cd32388ce9a370a975a, 63e27b152f8a608192ea0509af3399d7a51cd80d, c1ad7328fcf745c1656f3a541c66608da754ed92, 11e713bb72de9814062ae2009aa373cfa7fe125a, 0fdf6f2916881c99ae4f00fb927f1a5571da2d65, 79357ccab662489ed1e9c301f30371dd10701656, 8a47f46ab9f3ed5fd132cd8f30ece15e6c47cf21, efc18a43109a3973d974d696bb9847c33addfee5, 1ae33c13e5504b73f62189e04a7960c20e74c7ad, ca00c8e4cb09165da43d9501d7a28d7c31077eaa, b900e45999942e6d61db42cd65f820e9957f0f52, c0da7f205c769131e0433af452945c7e632218ec, a95943f311ec9e2e5e157ced3daac28beb31cc6f, a660ab84283b72f7a371aa806092800a0af1c134, 6d6d1889835319c81e546728d4ec6f965ece85f0, 4670088158f0d0bfbedd79d98b7a86ebec1a73ec, 99c47d4ff4ce4c17ba415aff15ed49b19b0417a4, 3dc1b480a400ec2596340b11d44e86509941891f, 2551b7d13ca515024c3201144341679a20a2f055, 8fae5af8e828901f63a82a7efa7e57e504fcc5df, f22817ca641b30ddd80c05a6168169dc1d838af8, c697255e7e2869253181d285a957d486847f137b, d1e47e0b12747b4c26ad0fd2003c67ab7c89b5b9, 0e59baeb2575c53881793d0d856795a8d4b4d69f, d56940deb34bc057e9cb8b476ff6e4095e7628b9, 21235976eaa20ba5d0341e7a1c75ad63ea4f5619, ae4ae9eb5045fb7b8c56224ebae0f0c2ca75744e, aed52a2c473bbe5272636d738b2e214c601b3079, bed64cc6b8f0f4f632209515fe693800e0ef3e5d, ca381306bd0da25fd26d35577a6585bb966ca8b8, 6be0d19b811da758233951f95e483f8e76b5efb5, 8ee3339859aac5f0a5becc1a2a034ee571a39c3d, 9f819597d49283b719342b271d55d0a25b993801, 0cbbaee2d968b9eae700fcc0347d686ce2d50714, 6c722d7ffc2e84ce49f4caca61536da6ea7e1bf5, e256b7c4d8310c13da7e56740f635ef935b6898b, 2ec0c7b9f96470969e2c11e6a97c392dce336939, 81ad675d6b2951c0d83fa917527644cb033d9d39, 9d77828cf50c7821abfb904dc355e01708321867, 9afb0392b4e44553d1e0bbb48ae166348ce91171, f4633dc2650f5ec00d99e50509144fdcf7c46aff, 41cb257e0b7c5a34ada21e5de69da73d1c4f3a5c, 09b61023395bd39f43ab7af66bb3beb0661b32c8, 8f573a4bc456cb24fad63c30bbb6babeb7737c84, 7fe26286388d4a497115dbac01060df29c0d203b, b6aecee4e29989615304b460cb13d64ac60b5203,

TYPE	VALUE
SHA1	ee9f6396934bca243adba63a593f54de69ab46b2, 0ae07c406163d69b009d6b4abc0b873e7e1b6935, eb64df19874aab134ec75baf72f8b619a7821f43, bdf6b8cf59a16f8ae9fc977b2d2507c179849eee, fc0f6892d07214ae5e43d997c38ca393491d5aba, 48439210d824fe34418bc89320fdf2ddb698fa73, bbb963fb00928aeb3c3d56dcbdb266fc141d6cda, 017bb90012dfa9fd9a6a05efd01d1d929e411039, 8c277f0f756ff225fe6862b1feca5d5ce58ffbc3, 15470ea8e47f9091f4aa5cc5f3bb4d4cd5efdc52, cb09ec0010e3e4da977888c4edff2012e30d0f24, b680651aced67b1725a7a6e44771ac919c0c5723, e9614746a051af4afe484ea5964597127b5d515f, 4e2746000367071d818c131faade4fa6d12f1893, 8eab0679cfb78fe905758bed258de9f454d6a65e, f8bf895f8f2ab82ccf8b2c0ed23f3fe8845d6fb0, c04789e8a9edea9ad9b8694bbc471460ce3d2e8f, e13e73821a0a0d3ed1e87aff00c742537de282f2, df721ea78886ba9fa47e0b4ff172cff71d3eac65, 01b1a3c676dbc370fb1916ef17f9bb0309d5b966, 7d40d330c9f2bb7016e7fb7cb1dbc6684e3c9f81, eacb7cff538195418e807c8c23a0558cbb160ec5, ad5b69f26885a229106c4542f195d710e045ff63, 5ba4479a67b26e2a8a1e4ad46f727474bb3e0768, e646247851726554f54a4b09f2288563cd623875, f70746f19efa93102f4b40e6b65166e54d722326, 4e7654e97dfa1a287587b9d65c9a6dba39158fe7, 04f2249a7ec88e7e8394c8d9deaba835e2a80dd6, abdb89981fbc623ed0dfcb14543346200600deb6, 32a0b9dadfbd452fef345d398658be1ebbcc6dc3, e29c64134a68b3d58c18491f59c62428cf315930, d30e3e26802d95f1931ecbbe5384c4ee78ee62f2, dfba0231d1991f3f4e702d44a4c90598b99a2e9b, 69963ab2e390bf35e5ff9a4c94a170f23acdf096, 99048c271e01792ef79118117e52ce68ba8c4b92, f3490a94b98e2f1f964caf90f8ca61e74619c813, de4c28fc5c4eab8c71b09830ff295b901be6a844, 1d466b66435f85871baf84e16bf476be7622dbb5, 6f4a65dd084cfcd67567da0b232226a08d6ac1bf, f048831662e209245fe3996b621f2de170199812, 3993bebae6d4c5c0b0e494472f8f3973367d7f39, f80268a58e1f1635dd9ccd6dd029dae2bf93fd58, 6ac7bcf1a0ab03f20a88b713f193803eeb092bf2, fca7d6bbbd81f136e5c24b6f78e0874e0eb0726a, 5ef1903f2f1be545a86050e3437d61ec02cfd1f9, 4db5afbf61b198629bcf58b215039c777c5ebc72,

TYPE	VALUE
SHA1	6da76b692ff1699cb723ef25abd74c9a1db27b49, 86450793957aca416e2c72733642f0b46a9de403, 1a96d14bec33dec3bbf5b8d27681fd47582b70e9, 4b1b2c297077f9a2cf927d300e642e6d0b0051db, aa2de74b5fdfd4e92bd5f8ee46b4cc2768d5b6b6, c6b323faca3427f1c7e7a28f53f998f5c11c5668, 4e005a97e144515a8c1eeea11d43ac9f16574421, 4edce7c3f0b2625b1e5c0c67c54e48f455100c8a, 94f67dc9e663ff131a07822cf6c4c8b0ace29cea, 461a92b53f3c24755689fe8a766bdd593010db80, 6ceb3a2d8a406cc33ca88ebc166f2deecf28a99d, 9d7ea472196720734d396cb1fea677c9ef32eefc, 46627b487ee37bbe389fff151c9761cdf6f2b97b, a514325d8050829352c929fe3d283db9fb290182, 5848ecc64eb9c66073c481435c28b726b9353cbd, 1e1620387907a9a3905b4bb41bdcc4bc1b0dbf46, 191e32ee0095c03ed38fb0cf656830eed585e53d, ce23e21e0db4097037a1760285f447c6f72d6cdb, 48de9f34226fd7f637e2379365be035af5c0df1a, b13a15a5bea65b711b835ce8eccd2a699a99cead, 04b12227d6b22ed562005d126cd7e3366c4fe966, 8e84857b6286bbf38b96faf1c05aa5796d412225, 4bfe6bd81502ff5bd45d17703e73e348b25dc665, 726afc25dbac5004232d28a2b83deb7603e6b375, 607a5d42b94aa5362857f893f5ff12d8fe6b7dcb, 1bdeab2b6857e99af6d67c1038e793710423607a, E60FBFF5F9387C47FA3CDF9ADFB80709F16537C5, 0722fde06e25a8c4e18e08dcc7cfba8d2be2ce47, 56222c0cc90d4a38625352f8e57f2d3016a51c9c, c202d352895b4977494c10d2942e3f5800a55d84, 5aced3fb181a459b9883b492039d9951bd378abe, a80f36aa7ee61fe48ac1e59111dc9c734b2fa885, e5002770edaf060167a45f12b3b5b2f62aeb36dc, c7ecb90deeebb50b8f42178a44cbbd4f06c1278d, 55fd9fc26380414b340aee4c605fe227f82f7380, 6d976561672a0423bc9188b695b82711db6a9d03, fb8e0e900762b9b78944f66fee54a135577c210c, 2c7885a5b28910bde36c4799ae2b2fb21513087e, 8d5d02b6394787570699267c802c3997e35f5f40, 7b709a3b7356de2d3aefa9095096af1c732c3e07, a9f256dcac6ec78bc5f00489ce45ea2c3025ada0, 536bab4cf9e397d987d4b12d0320145c49365555, 3a2b7e5f506347b9e507ff73ec9d0f236fd9f980, be46f0af75b61558145791ab831606e27ec6788b, 2e9270b03f6aede4608511c3b8a5eca93ece52a1, 46d860462c37ee8a5a5cd0497bd83ca560ec1a3e,

TYPE	VALUE
SHA1	545b851ca621da383063fdef12af805b1ec7925e, 19f76e04060d92ca0d7192b654ef145b3aae2311, 6bf4e708d05f086e78257126754494f2055affa0, 1a5668a22fa1eb520dc05e8bbf10c6b3a9e130bc, 77e3d99a32fc9b66467f1d7dd40dc8a71fa94ed8, 48a39ec502f24bf3e3fae5fad09f6e26ed23a736, bdf67090623133a2e966d789ac36d1f66802bdd2, 6e0a8481d276e212df18746e9ee4f92c0857a015, 1bd83ca584acf1339c9d0257ca00f36800a13464, 1cd4aa98e0a1e0ac3c7c074e90e57a2cc57af907, bf41a1fb5658b33d886ddc20b7d424c6dbd91d15, fb49751f66bbb232a6c625b1538e07a43f2a9c76, ae42a49a3b3e6c9ef20ae8ab49632e0ed44551ed, e0e4a713ea490b03bcefbcf9c39e5656d33d12c8, ba13031c90fa551ed3128a51b7d691be015f4120, 0c806d77241b6b7fba72cf608fe619db86c62194, 30ba7c406754335058fd1c59002318d5157df9ae, 5a39a8e9f872de1207e49a20b4baf2eaf156cb35, cf1a9a7997fcfda446f396cd915dc7ac4c7d878f, 761926f3ea3b5b68ac0749ff965aba15b67690d1, 4337db458d185cc465b804e57cd550cfb64dafcb, 81a784866b049d3fe7ecaeefd206e2e4efabd699, 80a8c652d5ce8253494b710dc4773e257c2b8811, 1776a2177af5eaaaa6ce615223a4e3e61667eec4, 2f98aa1d2be76cb921259157064af220ea08ac35, 7f88df3a43b850913c2d1688a4810689fd1cb772, e7e135c24dcfcec99ec2db3edc05ff7a2d4ebf49, 420de07fa1a999789d6da89e26fe7bb1fd122d12, 3f2affe56ff8af95727a64faf82ff8c99d3607ee, 1f07b17cac8d2327e1b16c3114dcec27407a3cf9, 48defa74814d2744c7cf4cd3731f6dd91484f1d2, 713c663eed7cadeb40bbbea1e56efa2829260350, 0874b04d13655d0e9e38fda43824f1a55a5e13ed, 196b0cbc196dab44d19d8252e115a8045e919ea1, 8aaa974f0e51908251b9817af5cf7072dd863172, 285e32a73738d98f26d6af0e5bc1e1fe913ba821, bb08e09e40d2f40e8fe99037b6d3cda695343ef1, 46f0e67a127ab61c667124e513bb038e09d82621, 8fa9c3cf820b0a65e1d70fe578240cd3c60eacb0, e2a05c418de34d46504e046e0341e96af2c1639a, d57c9ec3f6e103d79f37763f08ab4d400d9c88a7, a34668789a9238660453e5d8ccec13e19614bbc0, f879369a4da547c9778025ebeba3b58e28372f8e, 1045f331ac8846660f9c8f5069a91869c39c3e63, 2bfa962996354538e52a2d0b0fd42667fb22785c, da52e4ed8222a4d5a21509ce7af4bea0e04993e5,

TYPE	VALUE
SHA1	61ee85005265f2e2185dd9b07c66dfeaf6e300f9, 6c90360abc9605eaa09a630217f14961c30ac70a, 252a6d49a0d9096e8c48c11d7c9a934681e55f6a, 5ae4d3a7dec17b9740d4573e8f1014769e683f79, 33939e398901764dd5ecd0cc567f0ff5a89029d9, 2b8e2c6709e2f3920941384d492cbd7b478ac3bc, 1ef621122eb75827cf3bdd33ac4055882a706c77, ea4442f03b71397eee6cb7c781646186318bf3f6, 5f46fa9c8b61706c76ef23397db2fffd0dbc2be5, 535f8a7f356fdc428af253c256980a1d6b235623, 37941431bd552ad1cd1a385c771e44fe93917f5c, bf3e3960792bab3a8e798934ac8325636eb64b93, 224279b474c067f00793befc067d71ab706a9022, 28f1eb380c9ae75e47a84561328cce81bb7c73b4, 8de492602efab51138f53cf92c4734c2a1524213, 82f2e4db4ee70c73b3a7a98aea67e20bb977135c, 4b2da628635bd8244665663c61afe7a42f3a7c7e, 84f2fd32925940e988bd1284fabd244935fb375b, f7cf182890f3321eaecbadb9d21ce31bc7f0e722, 5e45c80c1dbd31890e70d582b2dc79756914c5df, 7f5c5b019067effb512a920964e60e2d6a7e6fd4, c43574e3cba99d3553d9d57b33acb34a503a4cc9, 7d474baba37200e0c401f12d50126e5ebb6cf62b, 103dd11c34e66b826abac28381ce80eba933e2b7, 2bbfb909e4e3bb1a1518e973afec5b587b59e426, a5d786f8d9ad0fe1ffbd6a8b00950f96d82420bf, 13f3c733960aeb518e51b0883c3bae4524da64d3, 6bb2a3e292761ad2323d9371be3d18781dc68bca, 12aa02703b0f69bd6e2084405b3d1f0c06c85f84, 9293c09804ff0e14fa9112b2138f8aa1c1d7ad11, 5fb1ce62fa6753a9b217e7e9e7c5fea780b1e571, f537c9fd4ab19a1c2a65d002fb61b60f5820f8da, bbb90acce8e40e13286066a82049671f5f3c515b, a56f5c4143e1e8f56a191cb1303c2b0f7f59fd80, 5b375d9994fd22ce44ebd8e1098aa0935c090357, 89be03fc76eccc6ad6c12bbc491891833cdec9ce, b93bc9282ad4b8cf728e24148da0f1f2872e834f, 52fd4fde60876eaf8dbde9279282fdc3601bdd0c, 9b795e4f06ba04238541f68dad15a7da88ed1eb5, d5f06e5ae1d810bf265797ab1d2d6ec12989d81a, 605e8891f64f3ac8943bd40f25709869545d40f6, 43758e1db2bc0fb7fded6ec864ec20973b26251a, cec6895dd3fc1b3e7abfe0312404a3ab7e597a18, 4bcc2b5b1c3a8d5ab5f81b7f249480da91b1eccd, aed1d5b7bffec047b22152fa4cf7e601c8ba963f, 75e142060680509acade4921ea417e1d438a34fd,

TYPE	VALUE
SHA1	e2830040a42c15c3825c2ff5ed7c96f3e7a14dc1, 17cf2050e2ba38677b95ec319c4642f65d0e3b8e, 5787b635711b51cffb3399ef069f58683a18e9c8, 1396c25a417e8fb7cf4e6b72899688b9f6ea8329, d316f5418950945761c24fb92a6b8e017c53010c, 2ce30b992142e318ee9393170b8106058007eb2a, f015c46dcf09ab813f3330e2f297346ad26e7091, 53122c78ed663ad84714ba55e6690934ab05077c, 75d0ea0edc9787db1bc13fed10e916a1e46ed1bc, 3c7c28ae981200e69e86545aac468377b2179d82, a45dc186286d95acf747f9aa521fb3b39a229b07, f80549805bbdd9a62872365be4dc8aceaa71340e, 2c070e8123357f94dc0cfaf584c787c0793760c6, a6d68f4ea448e4945788d47d434e697508d3728d, 6738d1a969194359c7c7579956269d77fed8d26f, 567848dfc535f4b1c77d4d4a89bffe1e7714bb11, 7fd2bb176a7013df00bfefe308fe72ed60cfa4a3, 7a9ee7131ceb522ce6ee9da968537c472c5ca677, 954387bc240bcbb21b6c80509da81df93a2b4d3c, a058647c11af7f1f6deb655421c8a307d30aa08e, 48efdbb41f2a724b2d158b32f7aa34fb25d9c658, 8cd81d3254cc14e6ffcba4aa6f8985b75b0d996a, db48b90b3c3fbc58b90a08b74ac948c25a15c0a0, 507d6e48c7d74af7651a1af5e1d0844f45f9c263, 150f1de0e17ff66b74105bc89fd02f498c205d79, 6be0d5a7c7e43101462799bbe5f1d16a0ba2b9fc, 8c95bae113ad1f730cf4008e144d2698eda378f6, 3d432e0a884179dd31cbd3707f4109bc5f84b1ef, d48fc60229b4b3b76407e3db0791c98d4b6a53c9, a66a656c08d16f8246c252a0e1ecd2629254e346, cb210c13c9f94e0e2273cf50740a3d32b08d8fda, c9b97bd1827d06e1a0d57366c1ea9629b8166340, f5fcf4a6312e5d6b0543731e5727283ce37711c2, c7be6c8c83b1d019735464a96460c452834b54dd, 2da37d96fdde37b6b24c561bc04a8c8c88290e6e, 6c99895b6cc25610f7d882693a06f7762eac0b9b, 880cdae437a21e8d7d45be18b0135aaf32146893, 557f7ae7b7382c2bc06db09f7cb07f640332238a, 95b74f7267867cf7f538876428cff90c2430ce6d, 5301aec910164eda6b9b36ba04a51211d038786e, cc9400861fea3deee8815eb34b7f5879fd6ca3ab, a4309c6c02bb320784c5952bf900eb2cd43b6ecf, c00a137d85855be8c462f835de67201124de62a1, 0046a5cf40bafa768b5afa282b91c63dd9fddf5c, c5610449b5cf0a3171fd5ce7b2cf2886a0d7de1d, 9befcfe5eb0f5fda18fed13ac4906eae3b702387,

TYPE	VALUE
SHA1	fa05f64345f74503e8d9ee1ada145942109c8aa0, ff9d30f793f2bc5c5279f8a082b31e6d0279a2c7, 777b5a8771f9571c779b2a85a439de80a7652624, 63b4c7daf5d4f821b660cf07733f067ac87b3662, 6944ca6b892e18901352010080cee39462d2940d, 7636aaf9e6186f81da27b39031504aaf33546aea, 7eb41cac06080bf49c46725455aea2f938581ce1, a7382690fc0c843dd101b97b2b2a33d82912a88a, 35ec7d9a0a0b6914fe636ba89a3ad059ed881051, 665270dd573f8486a68b8a9082d71b21fca952ac, a11d6a33a26b9b6a13fc011def75e4265f6e777d, af14df85dd55b518030f65cdd955201133e423be, 2b923dd6f2192f284697ed6f8605ad39eb38ec5e, 202a8e9c79abf7a41a5b1e6a35df7e1f381bca4c, 9029629af55f5e3f738cde263fd665863d8af8d8, cc26334cb8f4dde326f59c6401c1543589d3f2ac, a76cf1a0546cc1afd7d00ccc5df3939f287e8f95, 62c760e98d352131474947f3be744a1336d49643, a21812ab46cea86aad67e3ec3ded5bb8c1bd812f, c57dfbcc8058d00a1f97a05947eb7554e0a13fdc, db5058617cb8f1ce5d6f9a39ff566487b7d8470b, 636d1ae335692e547fa65ecff198d853ea9ce083, 4ed925880235aff579fbe5caa7c35b3578a96634, a9e07ce56e1f9ed4e8e04a5412730c4fc61c71d3, e89d1c6f127834cd447c5a88e4e65b2e235ded47, c1d4b47f66114e33bb3f8af30aacfcf7a4fe2118, 16957a9697a8720c61ec3c91d9a06f0f1e5f729f, 17a58fd39584c3e01bf4738501ecd3b03f3f8b7e, f7de3365879a5f401a22e86fb2880778ef18fdc3, 9334c0dbba480706ebb9e91065eeb14b11412795, d99b20cfabee66b7cb8a415841f05eda84f06b76, 704ff0a28aeef3a0fe67d5d593041a8685016b13, ac1062211fd3e2d0e0cb363e484a5ed33da88fc2, bec6644f6e7272117039d14ba93e5b1b69f21cb9, 326b6bdca100671e52ed2cda567f62ad9bf06d54, 1bb64ff0cb3e579494fc9110658063cf862f40d8, 7b2a104e475234b87ade4d6ae655eb61878ab825, 6b5ae14fcd6565ae94af730636763eba7e3933c0, 7c5b91cd266c0597f2f042ee4be5ce3ac4dfa8c0, 060d5f8cfd6f692ab8cded1f97970f5e1bdefcca, 130229782a69515dc5affb15cf50e3226410dc1a, 9689f972f5bb59fe6e57123f8425e025c1242336, ba63027b7dfe880c95fa57234a98f8d1a789f3ac, 64e031bda28509528f26a64ac5d7935cf5afe426, cd023c49119fb7a6edf2cd4eae824f5ac0a0f6c6, 99f481ad361658bbe70f3adf1e558131af3fce3f,

TYPE	VALUE
SHA1	cea585a58f4e0de28dd3490ecc71e3f60035b9f0, 2c63719b47c03c0c0fac65ac4c1e36c9225d67c4, 1de1701134a5fd88a5a8abb88c8e52ea698fad31, bed8d6f6f2fe85b6e2ff123957e4fbc9a7f39152, 0f4841790d7e28b89c154b7027600264a4bf166a, dce65d2f23808451e525d76bfb3d20b2fccddd11, c571dc00092e1dc217c534ed801a7901e4f6adaa, 224f19c9eb80108d7cf3c67f0c0b70db48126fa5, 95ac8338a39675ef5b2c04d7a54221c926590e40, 897f46786d020add2b78fcf74fe889955328e6fd, 79f795aaa0051fb83cfc50be5a4ab9f761f6bc18, f7b92fe99e3d7baf94e726697b546d57f1f8cbb9, 72f7cdcec9d629632b1a6b6a4d3c876313ffa709, c8b477d80b06556dec6a97962a48ede70e858eda, 3246714299fd84b3bb530e7138e570dfcf5948ae, e2a1a5641295f5ebf01a37ac1c170ac0814bb71a, 40dd20643ba58bb81a27c3be4c37c84cc6a2ce6f, 363cbb65b86e443f24de3d4915db01208217c08c, 36a98688e0d50e0584034daa45565b75905de044, 7457a05e415855131efd3a4c1bfda45a9051a656, 6eb28adb6e8cc866f70dbbd22407f7ad0f78dd6b, 47e6fdb6b3b72501d0d6bbadf73b7ba16117de4a, 46d5d6e37c2062c8c7aef94dca143520d4be42b8, 248968f14c1706a105f86ed9da4cdb48a98535e0, b4738338f23c754a889f88a3de30fa7341b2de76, fde7e33898b73304755f1cff8578139f34246e23, 17d8ea8de47cf645f4f922a9e601e74e3705bfcf, 0bb59500525d0b45c506c7b4fab6c1d905ee3280, ca07d2d6c63dad12362bd6b5576721e3426156ae, 6855f4213dbb2b74e80ea4c299b2d94c7166590d, cb68241c564ea94f825836eb47cd282114466b19, 7fa5d3ca357cf2fb82d0b21a9303dce53642bf62, 65ca40119351f524c478a6c65c1c201c0023d439, 25373a57005f725c32bcfc0b72a06f001c375843, 761fe57c2da0aa95562369e67370748239e390db, 5d9f70fd761854f72c719aad591f8a29d70d5300, 9abd358ab00de031588bbe3d4cfbfb02beb3a00c, d3bcc82d43fd4accc211fbbba5805c5c314d9254, db2839ef38551d72f6367e7e6e44072f6b6a5e87, c328edc80f120b5b2cd71981df8b84419e565da4, 264e2ff34bb6cd54f31a3de23f9d9cd8f0b20224, 72649006fafce65ad62619a64e9e785906198986, 5c491c6625ab617f0850bcd4b567fe2d9746841b, e7ddbe6bfb647627db77b0af9e8e5cc2abe761a6, 87e7e8fd6e6b95591edde3ceefa7ca3ae3e857e6, 55f96d85611d46d948370b68dd300b0fc9042f2b,

TYPE	VALUE
SHA1	6b7c0946aa8c00ea239b73eba3baafd559aa7683, 30a6538dbede15967e30c0c20bbfa6164229c7fc, 89bb7cf606ede494dab8c89282ea399418f536f7, 653c01f221326ecd6053187ed566eeaca6b75879, 6f24d08fd83320e303d0cb3b48a2ba029b783d38, df2b0241645cc410a1439f354c7421f7aecbdf4c, aa99049bcb8caaac23c7c3a9488b47435ce524ec, 53b5ab29ad6bb922960fc7614a2643b8b4277a05, 9cc536e983081790eabb19cf872dfc612e39aeb1, 69cec4e11ed336b0c5bd4d5d39ccf49c96ad7823, ba1d5792f37d858c54df890e48bdb5c438821d96, dc8a3f1164bf81c9aa872012978ecba503c0d1c2, c0f3a01777c5fb4706121e8933b7f3b67a1fef03, d46339a4aa3a51c8d61dabb10e73b726ef150265, 0e3f68bbcb8dc9bce8583e7f2f77c79a971fdd74, 1f350dd42bbf58737a3e1b3ec439bd30b3eda252, 2394740c6c354d10eeebc9437f56a46fdcd6f6bd

Patch Link

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2017-11882

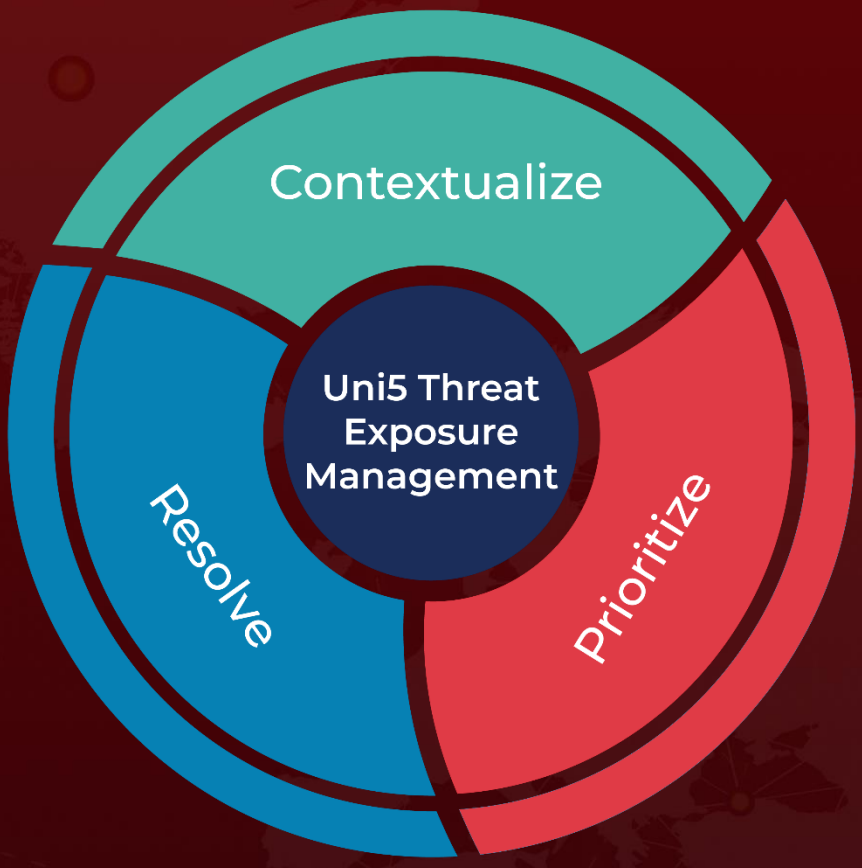
References

https://www.ptsecurity.com/ww-en/analytics/pt-esc-threat-intelligence/steganoamor-campaign-ta558-mass-attacking-companies-and-public-institutions-all-around-the-world/#id12

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

April 16, 2024 • 7:15 AM

© 2024 All Rights are Reserved by Hive Pro

More at www.hivepro.com