Hive Pro®

Threat Level

Amber

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

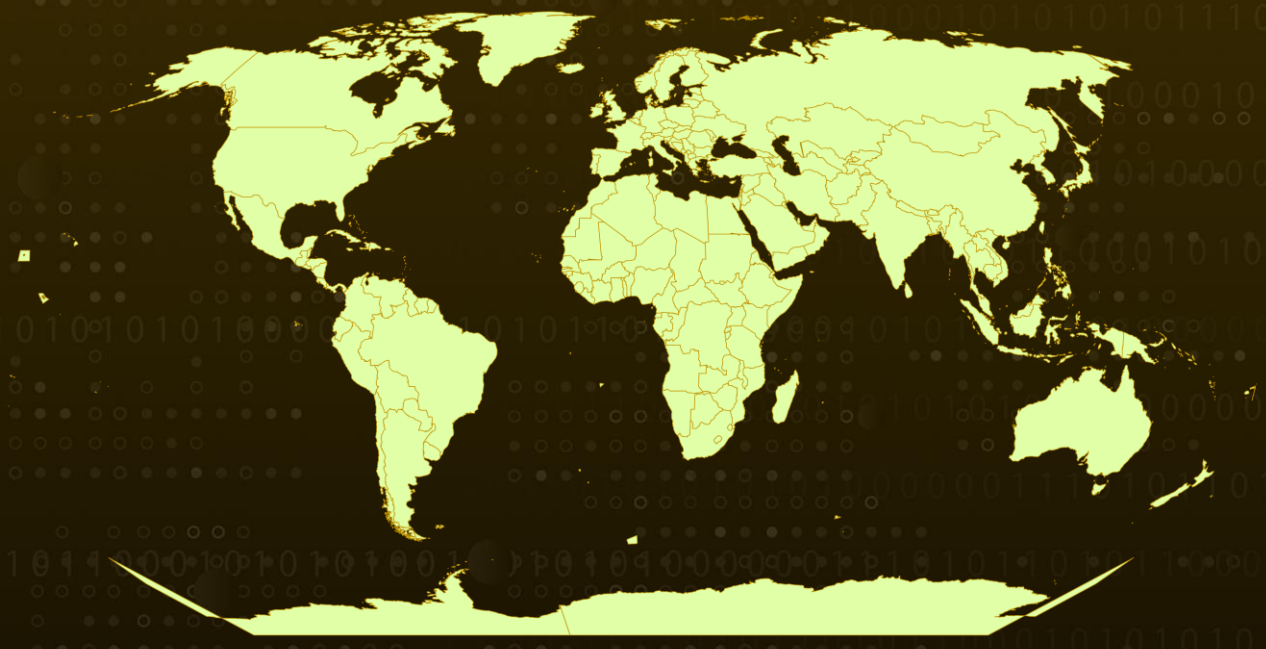
DuckTail Targets the Digital Marketers with Malicious Operations

Date of Publication	Admiralty Code	TA Number
September 7, 2023	A1	TA2023358

Summary

Attack Began: May 2023
Attack Region: Worldwide
Targated Industry: Digital Marketing and Advertising space
Affected Platform: Windows
Malware: DuckTail
Attack: DuckTail refers to an operation organized by several threat actors based in Vietnam. These threat actors not only employ common techniques but also share a common objective: to gain unauthorized access to social media business accounts, with a particular focus on those owned by digital marketers. The DuckTail malware operation is designed to steal saved session cookies from web browsers.

Attack Regions



Attack Details

#1 The DuckTail malware operation encompasses the involvement of several threat actors based in Vietnam. These threat actors share a common motivation, which is to compromise and gain access to social media business accounts, with a particular emphasis on those owned by digital marketers.

#2 The DuckTail malware is designed to steal saved social media websites session cookies, and it contains code that is specially crafted to target and compromise business accounts. This malware is commonly propagated through LinkedIn, where threat actors create fraudulent job postings to lure and recruit potential victims.

#3 DuckTail threat actors not only gain access to social media accounts but also change the password and email address associated with the compromised accounts during a takeover. This effectively locks out the legitimate owners and renders the accounts inaccessible to them.

#4 The malware was frequently distributed within an archive file, which included not only the malware executable but also various related images, documents, and video files. These file names incorporated keywords associated with brands, products, and project planning, further enhancing the ruse and illustrating the attacker's efforts to lure victims into opening the malicious content.

#5 DuckTail's malware payload is primarily delivered as a .NET executable, although this is not always the case. In some cases the Ducktail payloads are delivered as Excel add-ins or browser extensions.

#6 The compromised social media accounts are often introduced into an underground market primarily based in Vietnam. In this illicit marketplace, these accounts are bought and sold based on their perceived value.

Recommendations

Endpoint Protection: Deploy reputable endpoint protection software that includes anti-malware and behavior-based detection capabilities to identify and block suspicious activities by DuckTail. Regularly update antivirus and anti-malware software to ensure the latest threat definitions by the malware.

Multi-Factor Authentication (MFA): Implement multi-factor authentication across all user accounts to strengthen access controls. This additional layer of security reduces the risk of unauthorized access, even if passwords are compromised.

Awareness about phishing & adware: Strengthen email security measures and user awareness to combat malicious phishing campaigns, and the identification of adware to minimize the risk of successful attacks.

Potential MITRE ATT&CK TTPs

TA0002 Execution	TA0005 Defense Evasion	TA0010 Exfiltration	TA0007 Discovery
TA0001 Initial Access	T1204 User Execution	T1204.002 Malicious File	T1204.001 Malicious Link
T1567 Exfiltration Over Web Service	T1567.002 Exfiltration to Cloud Storage	T1027 Obfuscated Files or Information	T1027.001 Binary Padding
T1036 Masquerading	T1036.005 Match Legitimate Name or Location	T1070 Indicator Removal	T1070.006 Timestomp
T1566 Phishing	T1566.001 Spearphishing Attachment	T1566.002 Spearphishing Link	T1057 Process Discovery

Indicators of Compromise (IOCs)

TYPE	VALUE
SHA1	92a7ac122ab87ccfd19224b2be89fd7bbee6d0b1, C8d5b988464e7e49b932a01d3b75e192fc7a0026, 27ac50a5f2751429eed99fd4abff73c2129ba387, 2e1b5903131ad42591021919ac27beecd70c9253, Ce5f839cb8a3473330256ed72c144f689ad3c55d, B14deb48c60771fb05cddf6a16ea9fc4e56ac6be, 1b07ce1f47ba6b19087499fa4ba2e93beac227c4
SHA256	740fd780b2b45c08d1abb45cddc6d1017c9fcc6bcce54fd8415d87a80d328ff6, d93c40de3e43ec58b115e5590c98ef62de15df9b706ef6d4a06d022fa874bb48, aaf44bce6a5a2ab5b7f3f75f8238d6abe46f9fd2f2e2a2b2672ba6e52f4d5754, 4f43c031ff415fcb2f6865e98e91eaf611eb6a576acfe3250b57dc5e47a7d34f, f433fc47b9ccd66aa80196e04a4e4bf54fe3d1c689e4b5d5bcdf86017c3f8abe, a5026e7a88c3b833ee3678944d003fdfe51f86d44515c470dd2c8aa62e0fd0d2, 4759cb5a37f2c8661c3817206b4d34d65825d80526ce41461f6c11ea56289ff3, 4c546c259cbbf0daf1d0aa00d3385a1ea9e74b6fb2e3692ef44e1da27ba30abc, 71a89855974dcd69f3547632368f2ce8cfa490ee96b514d832f04cc22923f143, a6decb34e5688f543e541dbc79e6884ace29c93d7fc43716eb32204cb3c0003e, 59caef212349c6423e1fc581aaf76ab735269990bb7dc8e193e2877957c71e91, 1000d705806b940af52b54cba98261b64ed658a355e0922d64551c5acb7f1a40, 47f9122f0a25f4909795ede9bb4458495ae70fa2657745ec7c47ee172e040209, 52e295073d2114c0683d95c8d323bddc95baa5c68f8362ebcc81124a06e42672,

SHA256	6e797da70db98e1f8fb5a7cf794b8a8e90549e8915f4d04f510690ae23aeb505, 25b427a06608ebfc48c778829427a732c17986c64345acf35e92d03ccb126b8f, d3633c2372b67db37b11de741bfa676a425322c5208b8396c62983aed88d2bcc, 600a498e55512723074b6f5a952ffd38b249c30117e9eaafcccda4fd1a0c1e75, e74f131d1e5ed725383ee5b89ec1216c642fbd77928dafd991b406a7f59251b6, 469bcbd18e2b5d4ca15f449d43c13656758503fcc4042a05721ef5f3c35345e2, dec248f011c1f945f590bb5aeefbbcb41bdaa6c665625a594f8b315f014ea4bb, e8d5af5ebff12d0cbb8b1cd70f149a8234b993facc32b3808fc7db94f2bf80a9, 7952eb4832bfe5155e2f37abb68d552ed8f2f426715f2bc65eae5a69f1f28d87, 7c6b1a349ad96d8368e1f9742992f764a7de32e9c078709372210a88a721c532, 7eb994eaa7be9dcfb37bdfd7c8bec1dc8b90e3ec4aa86de6e6125c97eeb64426, af75e8c1f3229868d41b141165714c56baf38f3f49c8c014c4fa18bc934720bf, 6688e027e837f8e86dbbe40e2e663e72a1b7e977ae25d1157ecd8793d947f0c7, 7d15d3cdc41cc0c3452a538ed3bf8e0dbc9a0cbd4bbca453a293287e240dfff8, b83059cc733ad4af37a15a24222b09be3ee02af3964bc62ae5de6354cd85f65b, 61953e2d6e80fca18173bd3ce695274c5a25db449ac32addd8ee5b0ac29efa02, f17d2acb4c1bd0332b3c0cdba83001b82fd96d62d5bf829ae1e409902195b038, 1092ab1743ca59c29bee69d73918ee78e2195fafa232a16ba790429d39dc9083, 1e6ff886f386afbbcf8dc175bd1fbdfd8079448f1cb5a546352d7065c5fa5e7b, a81cbb9871f692350bf21d07b9acc233268df233b79c311a482d9783eb9bd539, d7f4372daf2729c956ce63e0ba2b7149f1bae03da7fbae486bbcfb0bda0f8d70, 3f9300d5d84482010bce08e9cc7b0a5b605086dc4143e8470e9e23ef14f0c27f,

SHA256	e2a343dfa801882625c264f944f89665319ea9b3a2793ec47a02bb4a126f5e15, 8cf5a4d0b6848604c338ad2d8bde8ceab2e86fff0d65e777bc574025f26bad73, 994039645f60d5fc9621cb10826b7583c83667827c195b3fa9d875a8ee50b170, c9c5409e6327f2f443dfa3cb6ffa527b291a34a572c14e93b65205fd305f4ff1, 83126452e240cdebbfaabeda58dcb4ea68f1e9836596e6032119592b4057ca4e, 7395aa619010fee65ef640f46023be5732188df36079e13f023aa2dc69602e21, a09f560a1ddbc7c60695d5651cff0ae0f0911399cb5146bb531caccb4d14089e, 34392151e58955b0bd7eb70a90499127ec5810a8488c2ae5bd4da1f9167a7762, 9d24436f652abe1df6319fbfa0a5468f1061e280d41fb00a60265d6c2aa7871d, 8c87c2d7f3932fa6661daf8fbf058ab4b721d0d6fe0849da30ae695b61d3ddc2, f47a002d93df2190e47e7026663bea34ea0299a4afe2810b8cb45b51bf330a8b, 6578a3dfaa2c59443b02581c0097e8c356babcb388c4ab48ef651c90c262e9e7, 4a56e4a753a5fa615aec4f80eb842ea2f089bd439e93ecf406f8433e97b659e8, a8196b3995bfbc62ec073dd35377a5412db30e9070ab72743694ceaddd2495c, 958ff188086e33caf119347ef7d81a99716e83bc688ed1ada1ad25feab7088b9, 697307235b627a33f4308a14dda9c1f33e38c9efb572026320bca453f6301b0a, b0968ac6489e7f2122ef2deafbc5a5f5968451918a8023c7aa8ded7171264ba4, 625b5b3f5bc9e1fce5486812051b187975210a46bc2d9a712e9ef9ae5c68f09c, d6c18d9efcbb6ce7292c4d6bdba70a64acca10561b66fd88e9e47cb9c7b63392, 4089277eff9f088684f53697c2f5615dcf4c940c1693d9d8c85a7de47dce7161, ce1f6a00bf9f79ffe879c2e7ef40166ecacbe6a17a382544648f0f25c5c4177b, 2c9824d0faff9a0485c36546ac7884697d1773bd221c2586ae9ddb0e54208731,

SHA256	a99fa349faabd5773816c53a11b67a7be95f277b622ebe93c1ca3625500b8384, 1fcbf708854f7ebf93726d5dd08c08648e84aee0a33a618a29c7e50df09e12d5, cd8b9cc35064b76df01ba5ce7536fd8b60dc773e32889ceca95f586112b6f3c5, 044eba497f9259d18a3ea593de3fc39c6123805ce485cf4a193083f9e0b74bb7, e81db61004834afb0dbf47db128942e3353774764466fb9269e88a553e6dfc33, ee5dcf9b070e19b87842e5c9ce3548bb1507e41d7aad272ae697afcd9f3ab7c2, 7af6cbfd7d1e7fe2f8c8c0382ee43860ec2cbe25ca845588981263ff8144f236, a30548fa4058d1309d4d75dd2dc36a492c503168f4d1c2f6c52cce57069629cc, fc8c250c2346e5440e249942eb8fe7c8b9b7d8d013f275c5fae2ae142ac50171, 8db1a51d514811057d29ddda85858f52303999cebdeae25f88d05a39594afd3a, f7c015d65d4966936927ae5241ead77c9d167d749e97667a571d7439e652ffa3, a3c5cd4f1afbe10de154bf3f669479496ff2e93da660a849ff41c29d5f118a4a, 9ef977e0403f9dff5cebe3935402d7a776ca3c9a79618e4d6992d3754051f603, d6c7c6a9098769b015802a278eb81bc7b72b08c5e18534ac71f01394a95c1f28, 647793166e03397bb1c30f0935330bcabc9f2f0f4ba8d7a821fc145237d96b2f, ddb7c9d4da1bc5534cda685bf3ac3e6ee56dd8605504da1e6c7a1fda5fd24ee2, 300358895c7895c14949c80d7b4ef6fa50ec5027e65e4578d503c39f2bd6618e, e4bf8cfc1035f51020ff033b9366dd1fefef8ae5664e2fde6798831399c51d1d, c1e65ebb05c500b5ade389a2f880e9116b74b24782d9ea13955adab087194b43, 4874878056cebe9627bbf44a3bc977315d6e14492af855319103b99103241c5f, d26b0baa30cc13df88eca57ce22f651a744cf5683b8b62121b4292e1005527f7, d5939fc12c88264cb28ac867767e5492aa145f0499aeaaa83cdaca8b15da07ee, 507376fa684f17508a195426d933e0e2ef92028d5956ed66cba825b6ce61df8e, c2c7347339cbb5975205df81cfa89e8c23c59f97e56a81fbd2c178a78def23df,

SHA256	a8850c0de9c2ff0ad440eeb299013de88940de8ad7f4076fd05ee63087d08fe8, e5a2d62ab4f8dcce7c5376378ec16bbcb5620f5ea507e74b0ac32649a2b9e52b, 0dcf3b1c16f39e375e53b2b63de1f267334a075e84aad857b3ce52dcaee73ab2, 012ec7a1553f46fd3fe28f175a3205c85f672153a6793a81cc8f6ad65085cc0c, 267874d5e9ccb484994fc20d08f8c653986e056c12cfc8e1ce7565dd6b60f5a7, 3ece0a9a92a410b8edad39bbb2aad3c155ae7f8b2a0177e116efbe29292329a9, 05aeb980d9eb1597bfde77b6969bdc7d13ff8a5f95db4112c5330f442c01f6f0, 51abe6d7196e93c4264ff508a11611b871bb1c9d96df2086efe84dd48af96cc2, 05aeb980d9eb1597bfde77b6969bdc7d13ff8a5f95db4112c5330f442c01f6f0, e5a2d62ab4f8dcce7c5376378ec16bbcb5620f5ea507e74b0ac32649a2b9e52b, c2c7347339cbb5975205df81cfa89e8c23c59f97e56a81fbd2c178a78def23df, 267874d5e9ccb484994fc20d08f8c653986e056c12cfc8e1ce7565dd6b60f5a7, 3ece0a9a92a410b8edad39bbb2aad3c155ae7f8b2a0177e116efbe29292329a9, 07d5d4721c3ed9a860dc10d25f226dd81a83602023c63310f9634b8dd704e7f8, 0dcf3b1c16f39e375e53b2b63de1f267334a075e84aad857b3ce52dcaee73ab2, 012ec7a1553f46fd3fe28f175a3205c85f672153a6793a81cc8f6ad65085cc0c, 161d081e9ba94ee1749c3192888702f6a25e8e2fb59b9d1f9d989ffc885566a6, 80160fd48ba4d174ccd1d2d8e72afc3674c1ce7c73ef18d3e372a6d68e6b3227, a8850c0de9c2ff0ad440eeb299013de88940de8ad7f4076fd05ee63087d08fe8, 8731ec7667084e649622e9f553e291b889eb0709c669545bd19f3ec0c2878687, de0a568803eb5b3d51eac593d2c9174e6fdef9a9ee11f222e5822ae3f182b5b0, a979cf0a2a44f2c23e01eb72cb72cbfadbae40bea38a3d390977d79bad610bc8, 40da0bc61a4ccf170f43981a7d908b0c3b541b1652cbb959b1ea9a87dd5944a7, d76260578caf24dbb6dd2d10c60b066d7659f5c21da8c998f34ab0f675d626d2,

SHA256	5d9b287df9b9b3f019e8d5834f117200f0651ecd0988338fb395ef1382fabc26, cd5c66a206e92be1e7eb77d5cb69c63fc2acc9ffbfcf7031713c9fddca11b3e7, f4e9feb547dcd6a233f71c7ad57a0759a584ae94a9e822a64831ed26cb32ecf4, 0241555cc3e21a658c78cbe93ab75eaa4f978a013df22852ada57652a3a57b6a, Cc5483d21c84ac73c410194205b529d6190b322b8da49577ee36ae9d8878c0c3
Domains	marketingagency[.]social, a1outreach[.]software, mangogroup[.]sale, la-roche-posay[.]click, li-ning[.]agency, li-ning[.]news, hrm[.]social, hrms[.]social, mccann[.]fyi, avalonorganics[.]work, li-ningagency[.]news, li-ningjod[.]news, ogilvy[.]social, narscosmetics[.]social, yodo1game[.]software, louisvuitton-social[.]news, luoisviitton[.]news, eucerin[.]work, guessinc[.]work, samsungagency[.]link, brandresource[.]social, recruiterofbrand[.]social, brandrecruitment[.]social, hrmmarketing[.]link, marketingmanager[.]social, recruitmentagency[.]social, marketing-project[.]social, nike-agency[.]link, recuiter[.]company, louisvuitton-agency[.]link, louisvuitton-agencyjod[.]live, mccann[.]expert, ogilvysocial[.]company, louisvuitton-hr[.]news, louisvuitton-jod[.]chat, hyundaimotorjob[.]social,

Domains	hyundaimotor[.]social, hyundaimotorgroup[.]social, adplexity[.]site, adplexitydesk[.]tech, fbadsguide[.]tech, affiliateguide[.]tech, newguide[.]tech, businessmanagerads[.]tech, businessmanager-update[.]info, marketing-tool[.]info, connectads[.]agency, disruptiveadvertising[.]agency, impressionagency[.]co, themars[.]social, ommmarketing[.]agency, growmemarketing[.]agency, ommmarketing[.]digital, impressiondigitals[.]agency, impressiondigital[.]info, passions[.]agency, brandstyle[.]agency, brandstyle[.]digital

References

https://www.zscaler.com/blogs/security-research/look-ducktail

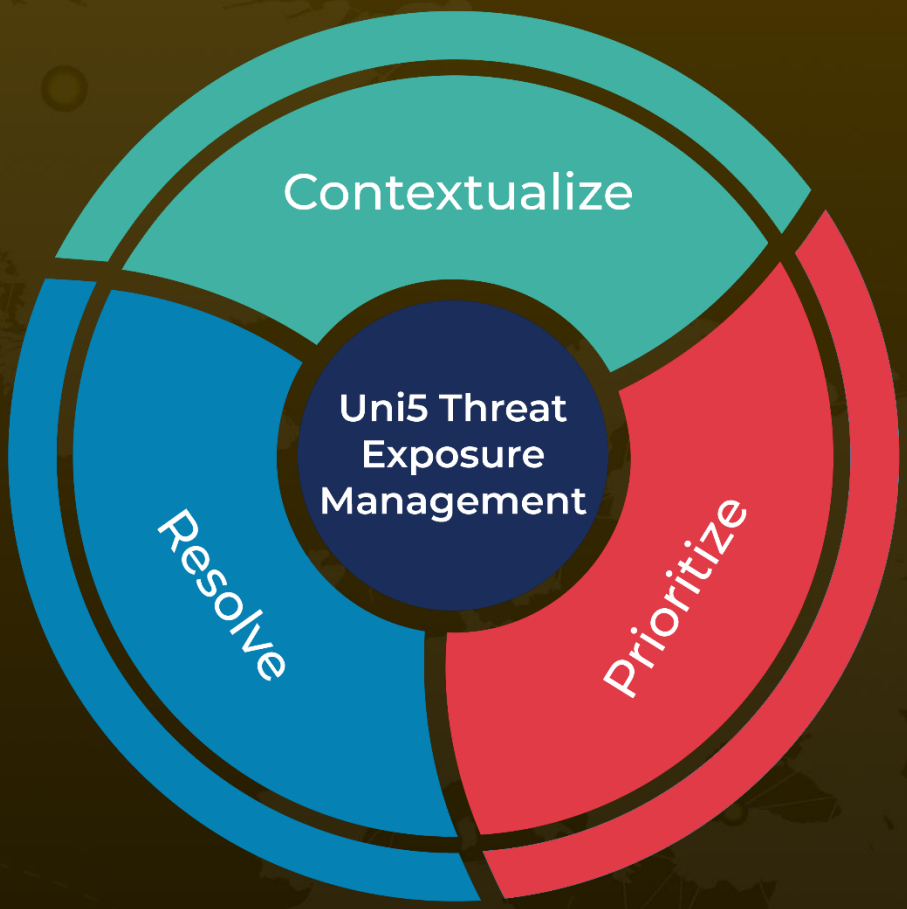
https://github.com/WithSecureLabs/iocs/blob/master/DUCKTAIL/iocs.csv

https://labs.withsecure.com/publications/ducktail

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

September 7, 2023 • 6:00 AM

More at www.hivepro.com