Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ACTOR REPORT

Desert Dexter: 900 Reasons to Beware of Its Expanding Reach

Date of Publication	Admiralty code	TA Number
March 20, 2025	A1	TA2025086

Summary

Active Since: September 2024
Threat Actor: Desert Dexter
Malware: AsyncRAT
Targeted Countries: Libya, Saudi Arabia, Egypt, Turkey, United Arab Emirates, Qatar, Tunisia, Russia, Akrotiri and Dhekelia, Bahrain, Cyprus, Iran, Iraq, Israel, Jordan, Kuwait, Lebanon, Oman, Palestine, Syria, Yemen, Algeria, Morocco, Sudan, Western Sahara
Targeted Industries: Oil production, Construction, Information Technology, Agriculture

Actor Map

Desert Dexter

Powered by Bing
© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, Open Places, OpenStreetMap, Overture Maps Fundation, TomTom, Zenrin

Actor Details

#1

Since September 2024, a Libya-linked threat actor known as Desert Dexter has been orchestrating a sophisticated cyber-espionage campaign targeting the Middle East and North Africa. By exploiting social media as its primary attack vector, the group distributes a modified version of the AsyncRAT malware, embedding it within deceptive advertisements and fake news groups.

#2

This operation has compromised approximately ***900 victims*** across multiple countries, with *Libya*, *Saudi Arabia*, *Egypt*, *Turkey*, the *United Arab Emirates*, *Qatar*, and *Tunisia* being the most affected. The attackers utilize legitimate file-sharing platforms and Telegram channels to host the malware.

#3

Unsuspecting users are lured into downloading malicious RAR archives, often through links embedded in social media ads or messages circulated within Telegram groups. These archives contain BAT or JavaScript files, which, when executed, initiate a PowerShell script designed to deploy the malware.

#4

Notably, the JavaScript files include comments written in Arabic, potentially hinting at the threat actor’s regional ties. As the attack progresses, the PowerShell script systematically disables security-related .NET services that could interfere with the malware's execution. It also manipulates the system registry to establish persistence, ensuring the malware remains active after reboots.

#5

To further its objectives, the modified AsyncRAT variant employs a customized IdSender module that scans browsers for two-factor authentication extensions and cryptocurrency wallets. Additionally, it uses a custom-built reflective loader in C# to inject malicious code into the infected system, strengthening its foothold.

#6

Desert Dexter's tools are relatively simple, but their strategic use of Facebook ads, combined with legitimate services and references to ongoing geopolitical events, has resulted in the widespread infection of numerous devices.

Actor Group

NAME	ORIGIN	TARGET COUNTRIES	TARGET INDUSTRIES
Desert Dexter	Libya	Libya, Saudi Arabia, Egypt, Turkey, United Arab Emirates, Qatar, Tunisia, Russia, Akrotiri and Dhekelia, Bahrain, Cyprus, Iran, Iraq, Israel, Jordan, Kuwait, Lebanon, Oman, Palestine, Syria, Yemen, Algeria, Morocco, Sudan, Western Sahara	Oil production, Construction, Information Technology, Agriculture
	MOTIVE		
	Information Theft, Espionage, Financial Gain		

Recommendations

Verify Sources Before Clicking: Avoid clicking on links from unknown or suspicious social media ads, news groups, or Telegram channels. Double-check URLs for legitimacy and use tools like URL scanners to detect malicious sites.

Implement Network Segmentation and Robust Access Controls: Isolate critical infrastructure and sensitive data from general user networks using network segmentation. Enforce strict access control lists (ACLs) to regulate traffic flow between segments, minimizing the potential for lateral movement during a security breach.

Implement Application Whitelisting: Use application whitelisting to allow only pre-approved applications to execute on critical systems. This can prevent unauthorized or malicious software from running, minimizing the risk of malware infection.

Enforce Secure Configuration Baselines with Continuous Monitoring: Implement standardized secure configurations across all systems, particularly those exposed to the internet. Leverage continuous monitoring solutions to ensure compliance, promptly detecting and alerting any deviations from established security policies.

Implement Robust Data Loss Prevention (DLP) Controls: Deploy DLP solutions to monitor, control, and prevent unauthorized data exfiltration. Configure DLP policies to restrict sensitive data transfer, especially over email and cloud storage, and monitor for unusual data movement.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	TA0001 Initial Access	TA0002 Execution	TA0003 Persistence
TA0005 Defense Evasion	TA0009 Collection	TA0011 Command and Control	TA0010 Exfiltration
TA0040 Impact	T1585 Establish Accounts	T1585.001 Social Media Accounts	T1588 Obtain Capabilities
T1588.001 Malware	T1608 Stage Capabilities	T1608.001 Upload Malware	T1608.006 SEO Poisoning
T1566 Phishing	T1566.002 Spearphishing Link	T1204 User Execution	T1204.002 Malicious File
T1059 Command and Scripting Interpreter	T1059.001 PowerShell	T1059.003 Windows Command Shell	T1059.005 Visual Basic
T1059.007 JavaScript	T1547 Boot or Logon Autostart Execution	T1547.001 Registry Run Keys / Startup Folder	T1140 Deobfuscate/Decode Files or Information
T1620 Reflective Code Loading	T1056 Input Capture	T1056.001 Keylogging	T1074 Data Staged
T1074.001 Local Data Staging	T1113 Screen Capture	T1568 Dynamic Resolution	T1571 Non-Standard Port
T1020 Automated Exfiltration	T1020.001 Traffic Duplication	T1657 Financial Theft	T1036 Masquerading
T1070.004 File Deletion	T1070 Indicator Removal	T1055 Process Injection	T1105 Ingress Tool Transfer

Indicator of Compromise (IOCs)

TYPE	VALUE
URLs	hxxps[:]//files[.]fm/f/yqsvtu99kn, hxxps[:]//files[.]fm/u/y5dys7zp96, hxxps[:]//files[.]fm/f/t5pp6hv9w4, hxxps[:]//files[.]fm/f/9xxadwws3e, hxxps[:]//files[.]fm/f/jp4nmyz3e7, hxxps[:]//files[.]fm/f/62yub4t3xu, hxxps[:]//files[.]fm/f/3mtfufs9uu, hxxps[:]//files[.]fm/f/z945eq5r6d, hxxps[:]//files[.]fm/f/ykxqvg9zt4, hxxps[:]//files[.]fm/f/9kqrkq4wqu, hxxps[:]//files[.]fm/f/3npt84t4fn, hxxps[:]//files[.]fm/f/ux28ecfzvj, hxxps[:]//files[.]fm/f/nyxwvypjw9, hxxps[:]//files[.]fm/f/9hk7x9ppcg, hxxps[:]//files[.]fm/f/h5ufvb4xpc, hxxps[:]//files[.]fm/f/b4tvte22sv, hxxps[:]//files[.]fm/f/gdezxx73br, hxxps[:]//files[.]fm/f/wjmn8b82ge, hxxps[:]//files[.]fm/f/cjvc28m3j5, hxxps[:]//files[.]fm/f/2fwuanhk3t, hxxps[:]//files[.]fm/f/ts8hzkrmm9, hxxps[:]//files[.]fm/f/w89z65su8e, hxxps[:]//files[.]fm/f/v9dmzyk6ch, hxxps[:]//files[.]fm/f/54fvu5sr4x, hxxps[:]//files[.]fm/f/cg3yjvgtem, hxxps[:]//files[.]fm/f/n553v7ycsa, hxxps[:]//files[.]fm/f/evtg4qmz4f, hxxps[:]//files[.]fm/f/fgcnsf7r8v, hxxps[:]//files[.]fm/f/2fvbg9vr5r, hxxps[:]//files[.]fm/f/2deytc9v4n, hxxps[:]//files[.]fm/f/bp4jshj9yy, hxxps[:]//files[.]fm/f/fkgns7tc3g, hxxps[:]//files[.]fm/f/er3v3jte6c, hxxps[:]//files[.]fm/f/2eu98w8ghm, hxxps[:]//files[.]fm/f/w2269c2s3n, hxxps[:]//files[.]fm/f/pwkjge962n, hxxps[:]//t[.]me/NwesWaten, hxxps[:]//t[.]me/VoiceAE2024, hxxps[:]//t[.]me/ListNames1, hxxps[:]//t[.]me/News2025News, hxxps[:]//t[.]me/AlainNwes, hxxps[:]//t[.]me/UeaNwes,

TYPE	VALUE
URLs	hxxps[:]//t[.]me/Al0Saa/, hxxps[:]//t[.]me/TheNwes2025, hxxps[:]//t[.]me/LibyaPrees, hxxps[:]//t[.]me/TheLensLy, hxxps[:]//t[.]me/TheLensNwes, hxxps[:]//t[.]me/NwesLibya, hxxps[:]//t[.]me/TVAlmasar, hxxps[:]//t[.]me/LaamNwes, hxxps[:]//t[.]me/NwesLibya2025, hxxps[:]//t[.]me/NewsStepAgency, hxxps[:]//t[.]me/AlhurraTVNwes, hxxps[:]//t[.]me/alwasatLY, hxxps[:]//t[.]me/AlmasarNewsTV, hxxps[:]//t[.]me/TheLibyaObserver, hxxps[:]//t[.]me/News2025Nwes, hxxps[:]//t[.]me/AlhurraTV2025, hxxps[:]//t[.]me/SkyNwes2025, hxxps[:]//t[.]me/StepNews2025, hxxps[:]//t[.]me/WatenNews1, hxxps[:]//t[.]me/SkyNewsBreaking, hxxps[:]//t[.]me/AlhurraTv2025, hxxps[:]//t[.]me/NwesLaam, hxxps[:]//t[.]me/AlmasarTVnews, hxxps[:]//t[.]me/News2025Breaking, hxxps[:]//t[.]me/NewsBreaking2025, hxxps[:]//t[.]me/TimeIsraelNEWS, hxxps[:]//t[.]me/VoiceQatar, hxxps[:]//t[.]me/ListNameAE, hxxps[:]//t[.]me/ListNameNwes, hxxps[:]//t[.]me/ListNamesSaudi
Domains	sexzsex1[.]ddnsfree[.]com, lovlysexy[.]freeddns[.]org, dick2024[.]ddnsfree[.]com, pdflove[.]ddnsfree[.]com, ohsexoh[.]freeddns[.]org, sex2024[.]freeddns[.]org, fuck1up[.]freeddns[.]org, ducksex[.]ddnsfree[.]com
MD5	c18828769cf0ee4159b0f73bcb1febb5, 075fdf5c8b4409c1f39d175f4941c5da, 7eda3a423372b7d39da6fb01d2a681d6, f20f5bf86c65ad5d7d8e04f50e0fdd6a, 7d6aa05580c83825c688211f1e71b72a, 45801650db5dbc718c6bc5cace4832af, cdc521cfab18cf6b0b72c87e9018120b,

TYPE	VALUE
MD5	1946b638e4e2c0f5fdc371a9e9c01bc1, a7f582c808f39659a53feecef6c3ebfe, 238f84f74dd3367c1068d31f025eb05e, 30fd61ec57dec347989030caaf0ec6e0, 294c8b3bc2c198795b20efa684c35b65, 013ecb281bf4f5c25e7823d522895cdb, e0415f4d3d8122214a3098ec6baa8dc6, 195f42f7e6cc6416da279446c9fd10ee, 6276af8151adad9b2e248faccae43d83, a400fe79f7d615e35550a8a15cbc31a9, 261d067103910dcdb5a966a9d6cbf917, 50301fc5d522055e29b2122958263acc, 64ddb41e380281a2440eb93af06c2fe7, 1a50f670c9d8a0c6ed60a26423f38c6c, 1b4e81246bc9bdcfa554d5c2343cde4b, 27dc626f052cde7ca5c99e09ba2c3bc5, f5c257cf1b96459ad985de4ee778e995, 4b667f53cd0abb72a05e1d16dacb094c, a2e1a80759ff915c795823c511e3e4e2, 65e4b959ba44711fa63f9a7fefe32c24, 3fbc9d18f8e94a0b5b1e39134be7c153, dcabbd8c5904e246164411eb63730b76, f77a293d7128c66a2d18b48af317280c, d13ea3bf14a05e4aa8d3f3aca89fe327, bc78a149c773196e9b7af9f2fef260e4, bb997e1a845b20dd5c9ebc18ac716af2, 11c6a227402d19f926adf61fdb6de824, 7dfa0cc4f95933e169f38ca80a99c86d, 97fbbb9968f5739a0cd7aadc1a1e254d, 5eac13e41e72e235d9f0e303f36220a5, 7ef04955085db9621d592575b825a0e8, e59107b5d4866ab8f87c7f4561fb0d97, 1e0ca1718e360353953eb1994fe901fc, 4527c576f1af0580c8d96ac23c8f761c, b7a1f3c523644788977f45b1539d3d52, 33b6c435bdbbec12ae8cba21eb6d105f
SHA1	3ace4c356fd2a7d359e59263d81de9a138da3eeb, 755649612fb6b8d31165dd729d6044e62a5a2c99, 767ff3096314e9a83177724b9fe9d2f04e8feae7, e5a2d21fff7ebc448e6cc58f4b10427f82033841, e1650405a2061dec28d8cb770964902028d0cf4a, 246e5dbb718afdd6be95fda076724bcdca484e1d, 7e3d8f52eaf5b17693a0ca98fa837d3349a35a4f, 5c7903ebe2cb97475e5505a3116464423c614706, 2d27b137a1136cb96a746de8fff7d51dd5c014a8,

TYPE	VALUE
SHA1	ca13c7619f5fbac8ab0153ced50f1929f512b1eb, e03b8fc93f8a7366adf3dcc482147f6fed1c4bb3, 1a2afb6af4b54fc266d4a66f848afcb990ce237e, 17f77c83a6dfa7f2a6ed5c65a3671434b4851950, 90f7996a7c2278c6fa1fba93c3ede85c94680106, 537bea04526fe7f01f84ea765fa6a89fcc51d9bf, 66c8f50c0150e3c538a14608da68c7d928bb3d85, d88d5110ebe30c8ad3fd215a4bd85388c6113076, 626e7394e9efb8b8496768d87de8d9288a0021d3, 905592e41e54e1d971390cbbd99e9ead72efd834, 089e077bdba26833b848fac22a13d744aeb0b770, 763068d2c6a7771584126956cc8fca76f5d8ee6c, 04533e810bd33936c596e7cfd30a36ba7204de39, 2bc44b1968fe3063310aea0ae3e7f56ccd826b1a, c67cd9c5412a076b742e88f939dae496bdadba6d, be57121278042b33d0cda331c8ae0d3bcf8e76c9, 946345327b619ccd2609fff063a5ad23ec55730f, f4bb8280e17617d6e0332776e2b197d51f76f0e1, be9a946fae242ff3b59ed41e0847338dfc90c58f, 0f5c254b6ae8acb1dfadc7e4422e0c275b6a43ce, 519fc698d92f19f569dc7a129a9baac483cff8d3, 7330d8a5ca8f8dc85657c3ec54fc4ff51b5cc004, 1333eb3ffe1dbd5efe7e2f2d70501ce715e833ff, 77d340f6f6e6f25c412ec866664ffcf3144ca0d9, 4d5fb4a91875a8403c9894774635c4619e4659b1, 103d0125a56947ffa1783a46a14ceda30b6cea89, 76dda9bd72ef8a5a642a007b3074f922dc98d012, a4b114b05eef3e9cb4109d8e76f27c8ed554d3ee, 3ca892dceb68af13273e8877fde7776f043cb7e8, 39e904a06737e019fde4f47d1b13c264a76d3edc, 7002f6f240ae07d4b4b4f7db7bcc889117abb4ef, dac3bf00eeb34c9c1d9dca63973f2e04da045383, 56bf9295b40a78534913a37095ff0abd8e8894ef, 41d43dc4ec1187e6120f26158e074e39475b0815
SHA256	1791d00fbe569489f48cf5e56b9a2a9b71d3c17096df4982668f51d512b820c5, 1d9a6edc55a547b9e522b3dd7f40aebc3f1c4761070294cc56e328800569fc45, 630c9ae8b4cbbe71c78bdc6f7da81a7d5de00cd7d8157021fd0aec870248c9eb, b2e678427428898f46899140fea44fcad52acf5a614427981d357b23d5f77607, df07b378a833528cca8012ec0bd65f06372ccf23262b9930c246d8758cef342a,

TYPE	VALUE
SHA256	24f2877c5a47480f7873d8ae0c3f85ad16a3e656a058a92f38d358eb37cdc48f, 704eabc86b2b3e7bc008059b59ceee8282847b08eb888c576b9105d0bd8f3c83, 8593a6c8fe6c98fd8c4d9b947e58066fd25bda10454da3f59b527a02795639e2, b9d613cf9ff332a3269223ed553e9806038de764f89abfe6f7f9cfe7595ad7a9, d8b2ea2b8e256df386b1a55a1aabdb1ec8a96f6b7f13ab41d0641da8386d24e6, 260a773be1ad179da987b22a87abf2eaac93fdf26c4e37b053f1ab2bbf1add82, b7341efc8e08b5243091c23fd4775cf5b3b6227d7e15baf8ad9ed79cba74709d, 5f3e6175c93e9f070f35d6c10c995b92264a06987af335a85d47fd8825562c3a, 6a117f3ba96c3ff1ac073f90e648a45ffb3f86566144ba526a17ff46d31d679f, 6f38b9d1db71631887f8a0cc241c2d3e74237ed30c4e46a26cf92d6702860795, 8e509cfc8711b0828cbdbac0e40a81628129015952d7011052068311c1e63063, e61e533b6a88e899bf008d751725b2e3c52bf6871c80ce41ef4c520f7e4bf663, f2225e97cb7f79fd2759117581a365300897860586aa12f3197def215ce3ef2a, 3014d48f6f667b6a6130b1ec2821073057c45a03f329ea6cecafc84784dd2252, 31d36f325ba63cf9e08cf7c0c08099089206cb9de556549491a6874e7f9101c7, 323fc0987bb2bc7d2f8aa1d6cb6db4901330b2874f01722ae5586ced09bba4fd, 4a3a95d68d85136618ab6f07674fb6ebd4a8e2fc373b5f5f9e0245d87ad9dfe3, 6eebe78eaeed5994a575baa50964ee98edc0fbf03f23620aef0d76910754132f, 79434f9046555e2d4233f903af2bd99834d0b1f4e2abde2ed8a1aa095bdb24c3, b1aa718183fa5059da99b9b5955b660dc495db375cf75e1d6731061e6492c408, d20d221d0b3a49133e9d50509380b2017913254918235 3ea97acad47bd25a137, d931dba26eee7bdc532111f006ec7973176f6b6b5dda4d23ea3fa700ccc8aef0,

TYPE	VALUE
SHA256	da58732f8c52ededed023e7d604dd10e295ad436884b990c8f13e6660cc42b5e, f722df5995b24216d2b5b3607213e25c361eafd00ed988d130f66e93af3f8d67, fb3461c4514b421b60181102b33ac2ac683021ce57fcf7741334d6cafe68ab7f, 02ad851087bfb3a9fd7ead36727a4992de338de651fb9ff4c0269d5e2e55bce8, 1579c6bcc9fa6f3565e3b74b26b5bf1c69c0671aec6bcace3d74d80fb4371c5b, 1c8c4612142e65286f455ea64ba41e6870bf6424fe2ac587848b2b8bd89ebd3e, 61bd750ff7331471320abc06ad99b7289a5c44f417d136f8af1b7db25ac0cb35, 63c9f2a14e4edd0691ffc49e62d488077e6d6689d26e5af49fd8c392238bf1f7, a0d5afdbaa125751e238760386b08037c01d442aef37e12194b75d40dfa485c9, 2c27fad3bdeab8dab52b21562df4dbd8217a84fb2553c1f99de03d1c686137e7, 7348760bbb74159d0be1ebabe54c22f1e158780d9a76d0a73c5ed391491d563f, af5eef159cf15e82dcf062a4865562b2721b2d1abb6dc26f454ba2b0008654cf, e0bd309a63d0daf9b231e4017176f788e987255f558712f372b085c0c13085fc, 5dee2d0dd4d3eee97c372b6a8dbd3d3042d24b9483addfa9f8786617a88e268b, cca42f01a887d5261e9d389d8f82991c4a35c88eefd7e38afb90d70146ca15b0, d4f4d3196d92b306f65ba4f1f90ec73403803530a58196b48db38210e3e3047d

References

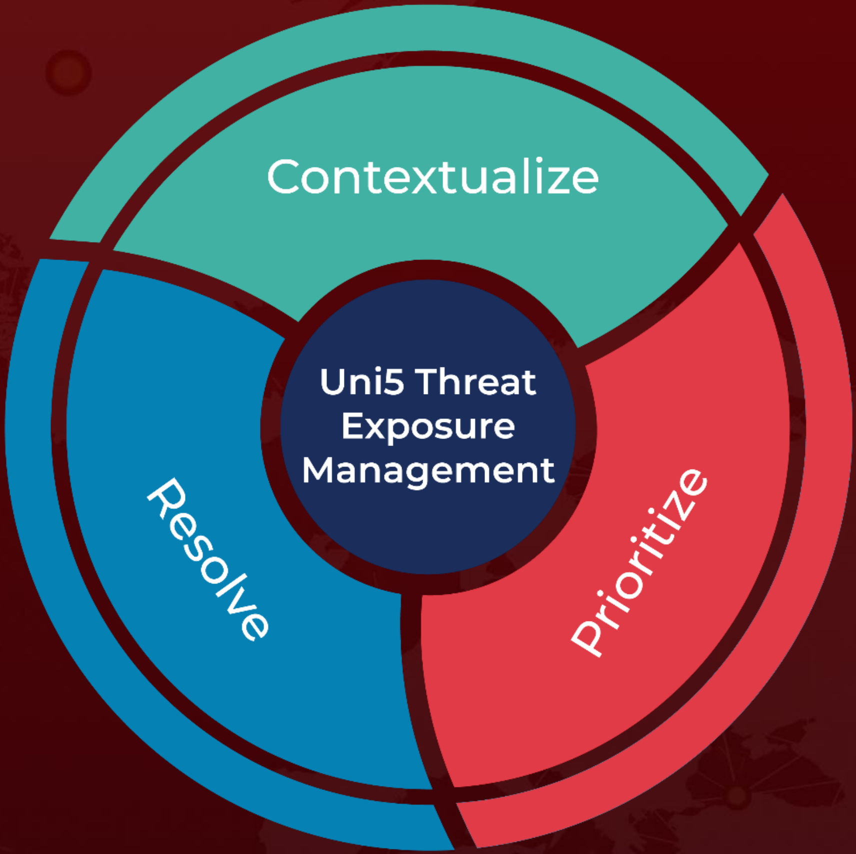
https://global.ptsecurity.com/analytics/pt-esc-threat-intelligence/desert-dexter-attacks-on-middle-eastern-countries

https://hivepro.com/threat-advisory/stealthy-asyncrat-campaign-leverages-trycloudflare-tunnels-for-evasion/

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

March 20, 2025 • 4:30 AM

More at www.hivepro.com