The DuneQuixote cyberespionage campaign

Date: 22nd April 2024 | Severity: High

Summary

The DuneQuixote cyberespionage campaign, first reported by Kaspersky in April 2024, has been active since at least February 2023. The campaign targets government entities in the Middle East.

Attack Vectors

- The initial dropper is a Windows x64 executable file, although there are also DLL versions of the malware sharing the same functionality. The malware is developed in C/C++ without utilizing the Standard Template Library (STL), and certain segments are coded in pure Assembler. All samples contain digital signatures, which are, however, invalid.
- Upon execution, the malware initiates a series of decoy API calls that serve no practical purpose. These calls primarily involve string comparison functions, executed without any conditional jumps.
- The malware decrypts the names of essential Windows core DLLs using a straightforward XOR decryption algorithm. It employs multiple decryption functions to decode strings, where a single function might decrypt several strings.

Indicator of compromise

INDICATOR TYPE	INDICATORS	
Domain	• e1awq1lp.commonline[.]space • mc.commonline[.]space • g1sea23g.commonline[.]space • tg1sea23g.commonline[.]space • service.userfeedsync[.]com	• commonline[.]space • telemetry.commonline[.]space • telemetry.userfeedsync[.]com • userfeedsync[.]com

File Hash	• 3cc77c18b4d1629b7658afbf4175222c • 6cfec4bdcbcf7f99535ee61a0ebae5dc • 71a8b4b8d9861bf9ac6bd4b0a60c3366 • 17119d30e632434e04d2106cf3d0b361d5c69180550e3db8ef07aa76c5e586dc • 17ffa01187ce7eef1a2e9a989d21e7b744714064 • 4324cb72875d8a62a210690221cdc3f9 • 828335d067b27444198365fac30aa6be • f1b6aa55ba3bb645d3fde78abda984f3 • 1bba771b9a32f0aada6eaee64643673a • 00130e1e7d628c8b5e2f9904ca959cd7 • 0fdbe82d2c8d52ac912d698bb8b25abc • 4f29f977e786b2f7f483b47840b9c19d • abf16e31deb669017e10e2cb8cc144c8 • 5759acc816274d38407038c091e56a5c • f151be4e882352ec42a336ca6bff7e3d • 5200fa68b6d40bb60d4f097b895516f0 • c70763510953149fb33d06bef160821c • b0e19a9fd168af2f7f6cf997992b1809 • 5a04d9067b8cb6bcb916b59dcf53bed3 • 996c4f78a13a8831742e86c052f19c20 • a0802a787537de1811a81d9182be9e7c • 91472c23ef5e8b0f8dda5fa9ae9afa94 • cf4bef8537c6397ba07de7629735eb4e • 0d740972c3dff09c13a5193d19423da1 • 5e85dc7c6969ce2270a06184a8c8e1da • 446c20567ef09819ad160537f49efe9f242d8eacde86eb662571c0be56f0a00d • 9d20cc7a02121b515fd8f16b576624ef • 2b69929e1bda591e8178134e92f3e4df5dd13330 • 258b7f20db8b927087d74a9d6214919b • cc05c7bef5cff67bc74fda2fc96ddf7b • fb2b916e44abddd943015787f6a8dc35 • 9b991229fe1f5d8ec6543b1e5ae9beb4 • a4011d2e4d3d9f9fe210448dd19c9d9a • 48c8e8cc189eef04a55ecb021f9e6111 • 450e589680e812ffb732f7e889676385 • 8dade177642a50ff101519b159d38a41aedf157df44f0a875310f7f21c2e9808 • 135abd6f35721298cc656a29492be255 • f3988b8aaaa8c6a9ec407cf5854b0e3b • db786b773cd75483a122b72fdc392af6 • 0e6072efb087ef19318a03a0509758fe9543222a • 606fdee74ad70f76618007d299adb0a4 • 72c4d9bc1b59da634949c555b2a594b1 • 3aaf7f7f0a42a1cf0a0f6c61511978d7 • 56d5589e0d6413575381b1f3c96aa245 • 7b9e85afa89670f46f884bb3bce262b0 • 84ae9222c86290bf585851191007ba23
IP	• 135.148.113[.]161 • 104.36.229[.]249

Recommendation

- Block the attached IOCs on network and use the latest Threat Intelligence data to stay aware of actual TTPs and IOCs used by threat actors.
- To protect your organization from falling victim to attacks like the one involving the DuneQuixote, implement a comprehensive, multi-layered security strategy.
- Establish and enforce strict download policies.
- Implement procedures for verifying the legitimacy of downloaded files.
- Implement execution policies to control application and script execution.
- Prevent the execution of unknown or malicious files.

NOTE: The recommended settings/controls should be implemented after due shall be tested on Pre-Prod or test environment before implementing. diligence and impact analysis.

Reference Links

- https://thehackernews.com/2024/04/hackers-target-middle-east-governments.html
- https://securelist.com/dunequixote/112425/