What is Lemon Duck Attack?

By Jasper Tan

Published: 2021-08-04 · Archived: 2026-04-10 03:07:26 UTC

The following are the malicious MD5 checksums. Cybersecurity teams can scan for the following files.

SHA256:
• 0993cc228a74381773a3bb0aa36a736f5c41075fa3201bdef4215a8704e582fc
• 3295dee4429647074d6d1062b0a069256397883c2a52d16525d35a3ed2e1c73f
• 34aa230ccb2888a5c884394d9eadbd02a480f4adf99e2e065e9d3c24e136f3df
• 3cfac69313f8f54f75bd4ee61b0a2a7c601f32faeddcd8bae725505c8f345b12
• 3df23c003d62c35bd6da90df12826c1d3fdd94029bf52449ba3d89920110d5ec
• 438248f6c28c02ffde120b2573aae9e53f449e6e7536f49a640f958a22d6d3b4
• 4a2bd91d6b189e135a500d62b93088c17e6fdc7bde10ecbab5d60f57e4e63b71
• 4cc3a01b313c9e542a825af3a520ff550c886c86acd895aa58b422de6697bebf
• 4f0b9c0482595eee6d9ece0705867b2aae9e4ff68210f32b7425caca763723b9
• 56101ab0881a6a34513a949afb5a204cad06fd1034f37d6791f3ab31486ba56c
• 607654d35de12a84e812a3b475499f91b1a7849d81be79b4e622ca97f2da2e0e
• 69ce57932c3be3374e8843602df1c93e1af622fc53f3f1d9b0a75b66230a1e2e
• 737752588f32e4c1d8d20231d7ec553a1bd4a0a090b06b2a1835efa08f9707c4
• 893ddf0de722f345b675fd1ade93ee1de6f1cad034004f9165a696a4a4758c3e
• 9248c617d19410832784e15b5382cac5837e990f641f4c016cbeee8219af6bc8
• 9cf63310788e97f6e08598309cbbf19960162123e344df017b066ca8fcbed719
• 9f2fe33b1c7230ec583d7f6ad3135abcc41b5330fa5b468b1c998380d20916cd
• a70931ebb1ce4f4e7d331141ad9eba8f16f98da1b079021eeba875aff4aeaa85
• ccbca8dac5824b49ce4c28c839dddb4e4ed35098adbe9978ad609ac9867e88b7
• d110083ba7e3d115c8632ab45949fc8ecc36b835328686028ae1af7d4b56329d
• d12b6691a9141b3150e24ce7798c81d5558d5dad7ba3603d8cd532d3a14089d1
• d8b5eaae03098bead91ff620656b9cfc569e5ac1befd0f55aee4cdb39e832b09
• db093418921aae00187ae5dc6ed141c83614e6a4ec33b7bd5262b7be0e9df2cd
• dc612f5c0b115b5a13bdb9e86f89c5bfe232e5eb76a07c3c0a6d949f80af89fd
• e99228953306f91b9f5213ac305025f5caeb5f4900a5657beb3834b209ac4b69
• f517526fc57eb33edb832920b1678d52ad1c5cf9c707859551fe065727587501
• f8d388f502403f63a95c9879c806e6799efff609001701eed409a8d33e55da2f

This is the list of malicious domains which threat actors are using. Cybersecurity teams can add them to the list of blocked domains.

js88.ag	ackng.com

amynx.com	b69kq.com
bb3u9.com	cdnimages.xyz
hwqloan.com	netcatkit.com
pp6r1.com	sqlnetcat.com
zer9g.com	down.sqlnetcat.com
Zz3r0.com	t.awcna.com

• Patch operating systems and applications. Keep antivirus signatures up to date.
• Ensure endpoints are patched with this (CVE-2017-0144, CVE-2017-8464, CVE-2019-0708, CVE-2020-0796, CVE-2021-26855, CVE-2021-26857, CVE-2021-26858, CVE-2021-27065.)
• Scan emails and attachments to detect and block any suspicious malware activity.
• Implement training and processes to identify phishing via externally-sourced emails.
• Maintain offline, encrypted backups of data and regularly test backups.
• It is recommended that users Patch OS with MS-17-010 to prevent further damage/propagation.
• Advise the user to use complex passwords, especially for Local/Domain Administrators0.

Source: https://cybotsai.com/lemon-duck-attack/