Severity

High

Analysis Summary

Molerats APT — also known as Moonlight, Extreme Jackal, and Gaza Hackers Team — have been active since 2012. They made headlines in 2012 when they conducted a cyberattack against Israeli government. The targeted nations expanded to include Palestine, U.S., and also the UK. Molerats is a politically motivated nation-state actor that is conducting cyber espionage using one new malware variant:

1. Nimble Mamba

NimbleMamba uses the Dropbox API for both command-and-control as well as exfiltration, suggesting its use in highly targeted intelligence collection campaigns.

Molerats use Dropbox, Google Drive, and other legitimate services to drop spyware for cyber espionage against the Middle East.

Impact

- Data Exfiltration
- Cyber Espionage
- Political and Economic Loss

Indicators of Compromise

MD5

- 0ea8f665f5e2d20e6a6e852c57264193
- 6c81f73fb99c56b90548b9769ab6a747
- 84fdcb1f23f592543381c85527c19aaa
- b726fe42c5b6c80b4f10d3542507340f
- c9a0e0c04b27276fcce552cf175b2c82
- 6dc73f2b635019724353b251f1b6f849
- fea6546e3299a31a58a3aa2a6b7060c9
- 2dcbcfac6323fc2be682ee3eb9b26d21
- 5d5b2ed283af4c9c96bc05c566bf5063
- b76f4c8c22b84600ac3cff64dadfaf8b
- bb161c7a01d218ee0cc98b4d5404d460
- 5da48e60c61a7f16e69f8163df76fac3
- 12fd3469bdc463a52c89da576aec857e
- 2a7e0463c7814465f9a78355c4754d0a
- 8598313222c41280eb42863eda8a9490
- aede654e77e92dbd77ca512e19f495b8
- 3227cc9462ffdc5fa27ae75a62d6d0d9
- 486954967e02a2e1577bd7dd91026102
- ea406ea60a05afa14f7debc67a75a472
- d99a401a4db249e973e33e9f2b51f8ad
- ade199b16607fd29c8e7288fb750ca2b
- 05854d1475cfbbcca799b3b1d03fd5af
- b8d5d8e79f1f83548f1efef7f53606da
- 1c64b27a58b016a966c654f1fdf4c155

SHA-256

- 0A777B0B981DF907E42B277C2AE6DA0D68539781DFDBB256EA4C41A5B7A9996E
- 0F0A9724ABAAF0F7AB9A55B136212F757F9929319B64314550CA594D87C8C255
- 15D390626FEA8D06ADC261E0588EC40D17B6A62A2320313073BA94809C5E0F4D
- 17FBC98AA216BEE93A14FDDEFEDCE3563A1B41095EA32FFF0F0DE6B86854A11F
- 202D1D51254EB13C64D143C387A87C5E7CE97BA3DCFD12DD202A640439A9EA3B
- 211CAA67FA9FFF89BA719CB0B711E4C86BF9AC2926BD4413BCB1106B326B4672
- 26C672B2537F8A89F2D59674F00BCFE9825796CA9B1EC51C96E5675DD586B87B
- 32643FAD3191CC5F2A3E8F0194B65505D77E3DC0703A98F66BB7DF865D9747D5
- 4AF094CD8704149D810175A192FCB1B6EA39C77085C7CF4535C03061BF7577A8
- 5AE0A582ED5D60324D6D1397BE3DEB0C704A1D77C9EF3D5F486455F99DA32E7F
- 70DDE32A57AC2E92C35D35FF9544010170E10EA914C14E7F6A45D4A0F1B4CB0B
- 760ACE17AD8AACD23699682600BD7EE319D617DC225B87AA873AD92EF5ABCB24
- 7A4C078A687E0C12ACDA81681231B823A8D59353CDB7B814D7BD50A0C136771D
- 7E122A882D625F4CCAC019EFB7BF1B1024B9E0919D205105E7E299FB1A20A326
- 8C81EB0FB49C40A1FA5474F45FF638961330FF73198DC7D537667455E5273BB8
- AED93C002574F25DABD1859F080203A2C8F332E92C80DB9AA983316695D938D3
- C34888F50BD1FC09B70FD5E0FBC333BE9D8F0AD998221CE4FBD4CB2CC0B78F6B
- C3F5F5BFE39B55FFE0343950E0A4BF0433C35679A01DAF07CE6C0CCC7D4DA9B7
- C44E13C75DFF157604934CA4D1E792B4250F7E0E9206F00E7FF367D62763D6AA
- C75C89E09F7F2DBF5DB5174EFC8710C806EF6376C6D22512B96C22A0F861735E
- D5B22843AABBBC20AF253D579FD1F098138BE85E2CFF4677F7886E8D31FF00CB
- DD43BA370D10CAA673FFDC55A265ED4A997681A0049A5AC38539F11E252A5CFB
- E32E8D881FDD250A2F72002AFBBDB9B03D02953F64D21B287715B60590CCEFE2
- EBF2423B9DE131EAB1C61AC395CBCFC2AC3B15BD9C83B96AE0A48619A4A38D0A

SHA-1

- 505c98fdc2e8d6ef7cc317339f48003b5523c04e
- 3ff45e700338eaa3f6704ec30d9552a605c92132
- cc2f96a2f4dbc4b0176bab37c22a48ebfe1bac06
- 62969b6cd78d9da829ccd3f8410cc794b3b57fea
- f24a18fa29af2c2213c3f2728e0ddff141d1d5d9
- 0dda541139a85bd4caaa58110c2bdfbd9547fa8b
- eddf2ca780b4396c0bf5ea3f13d22275fb6822fc
- adb895a23c7f7c6bbd3e97b237fee52a3d43eb8b
- e9bb52b4b24393e00bcda074d8d323f3fc5570bd
- 78c0266456e33abed00895cb05d0f9fe09b83da3
- ca00fa8110d567d5b09337d87c67bc8b6ee2db9b
- 1f2f306d6c55305bf5ab2d4b69e9acc481fdb7b5
- 7142063a6255e7982ea4e2a1b0b0d2cd1d93968b
- 2a4b20d399d61f99f7ddf389c523eb20e36a843f
- 256c631372692a1a907b04d27a735eb0905a003e
- d9fac68b6c49c485675d9141f375799d10572999
- 0e7f429a27fd09e88c8f48d6c0f95169839937a1
- 27b2fc98c91dddf002cda77da3f44cf9a05d7fba
- 970bed241c3382c09ded9f0661f955232b97fb58
- b0f2c934588feb8ea95c378aee0043147439d06d
- a1047665ed9d665f5cf066e4a9902d809e7325cf
- cda07b55beacf4a97fc310ea2d7b4e2f33d252c3
- dd4aff7fcd2634303f77c6c60792db94f8618733
- c3c8e5346e084b99cbaa69e3586af35d29612e94

Remediation

- Block all threat indicators at your respective controls.
- Always be suspicious about emails sent by unknown senders.
- Search for IOCs in your environment