Dec 14 2023

NETMANAGEIT

Intelligence Report

Gaza Cybergang | Unified Front Targeting Hamas Opposition

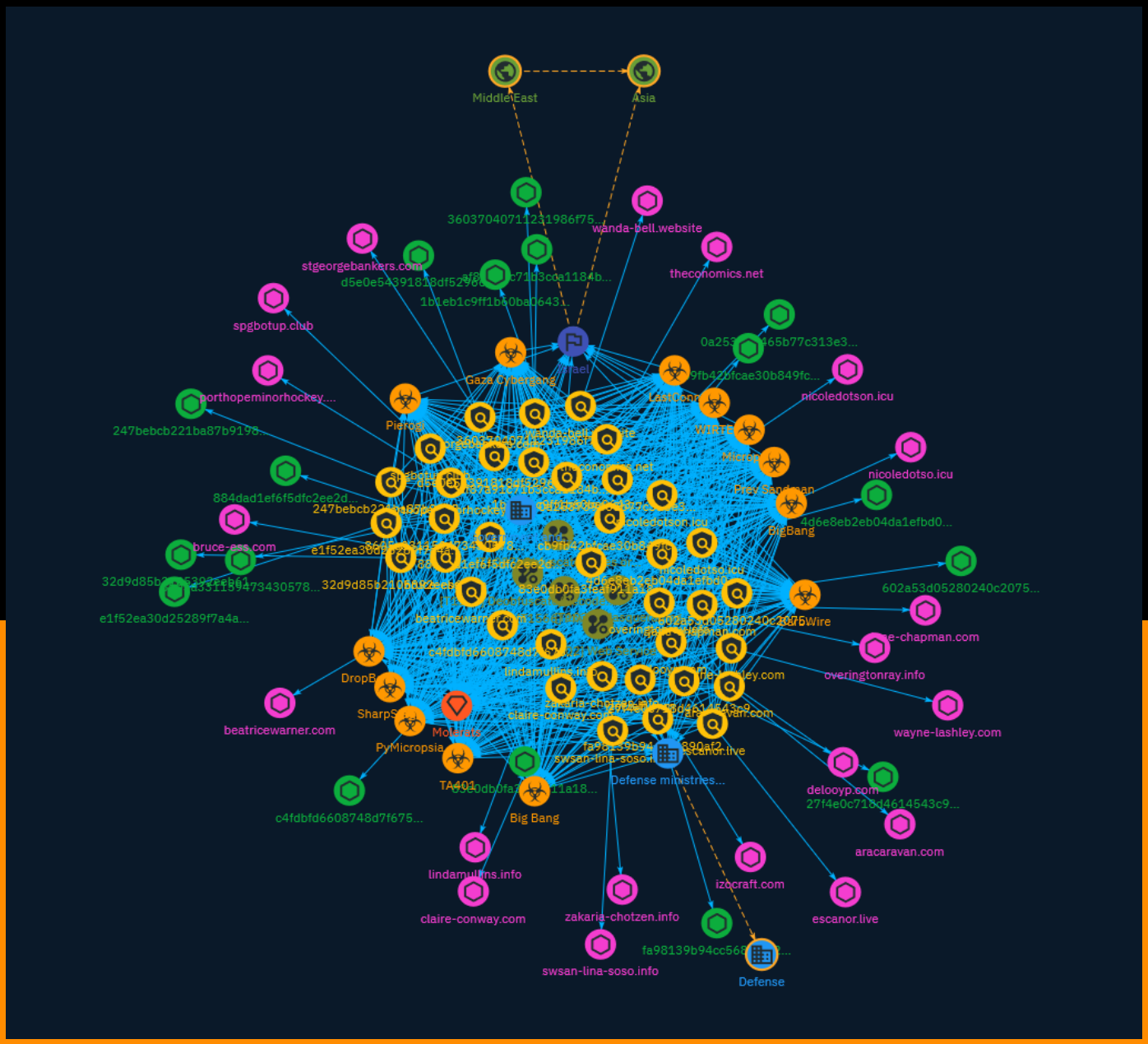

Table of contents

Overview

Entities

Observables

External References

Overview

Description

Analysis of Gaza Cybergang, a suspected Hamas-aligned cyber-espionage group, highlights new links between the group and a lesser-known Middle Eastern threat group.

Confidence

This value represents the confidence in the correctness of the data contained within this report.

15 / 100

Content

N/A

Attack-Pattern

Name
Masquerading
ID
T1036
Description
Adversaries may attempt to manipulate features of their artifacts to make them appear legitimate or benign to users and/or security tools. Masquerading occurs when the name or location of an object, legitimate or malicious, is manipulated or abused for the sake of evading defenses and observation. This may include manipulating file metadata, tricking users into misidentifying the file type, and giving legitimate task or service names. Renaming abusable system utilities to evade security monitoring is also a form of [Masquerading](https://attack.mitre.org/techniques/T1036).(Citation: LOLBAS Main Site) Masquerading may also include the use of [Proxy](https://attack.mitre.org/techniques/T1090) or VPNs to disguise IP addresses, which can allow adversaries to blend in with normal network traffic and bypass conditional access policies or anti-abuse protections.
Name
Phishing
ID
T1566

Description

Adversaries may send phishing messages to gain access to victim systems. All forms of phishing are electronically delivered social engineering. Phishing can be targeted, known as spearphishing. In spearphishing, a specific individual, company, or industry will be targeted by the adversary. More generally, adversaries can conduct non-targeted phishing, such as in mass malware spam campaigns. Adversaries may send victims emails containing malicious attachments or links, typically to execute malicious code on victim systems. Phishing may also be conducted via third-party services, like social media platforms. Phishing may also involve social engineering techniques, such as posing as a trusted source, as well as evasive techniques such as removing or manipulating emails or metadata/headers from compromised accounts being abused to send messages (e.g., [Email Hiding Rules](https://attack.mitre.org/techniques/T1564/008)).(Citation: Microsoft OAuth Spam 2022)(Citation: Palo Alto Unit 42 VBA Infostealer 2014) Another way to accomplish this is by forging or spoofing(Citation: Proofpoint-spoof) the identity of the sender which can be used to fool both the human recipient as well as automated security tools.(Citation: cyberproof-double-bounce) Victims may also receive phishing messages that instruct them to call a phone number where they are directed to visit a malicious URL, download malware,(Citation: sygnia Luna Month)(Citation: CISA Remote Monitoring and Management Software) or install adversary-accessible remote management tools onto their computer (i.e., [User Execution](https://attack.mitre.org/techniques/T1204)).(Citation: Unit42 Luna Moth)

Name

Obfuscated Files or Information

ID

T1027

Description

Adversaries may attempt to make an executable or file difficult to discover or analyze by encrypting, encoding, or otherwise obfuscating its contents on the system or in transit. This is common behavior that can be used across different platforms and the network to evade defenses. Payloads may be compressed, archived, or encrypted in order to avoid detection. These payloads may be used during Initial Access or later to mitigate detection. Sometimes a user's action may be required to open and [Deobfuscate/Decode Files or Information](https://attack.mitre.org/techniques/T1140) for [User Execution](https://

attack.mitre.org/techniques/T1204). The user may also be required to input a password to open a password protected compressed/encrypted file that was provided by the adversary. (Citation: Volexity PowerDuke November 2016) Adversaries may also use compressed or archived scripts, such as JavaScript. Portions of files can also be encoded to hide the plain-text strings that would otherwise help defenders with discovery. (Citation: Linux/Cdorked.A We Live Security Analysis) Payloads may also be split into separate, seemingly benign files that only reveal malicious functionality when reassembled. (Citation: Carbon Black Obfuscation Sept 2016) Adversaries may also abuse [Command Obfuscation](https://attack.mitre.org/techniques/T1027/010) to obscure commands executed from payloads or directly via [Command and Scripting Interpreter](https://attack.mitre.org/techniques/T1059). Environment variables, aliases, characters, and other platform/language specific semantics can be used to evade signature based detections and application control mechanisms. (Citation: FireEye Obfuscation June 2017) (Citation: FireEye Revoke-Obfuscation July 2017)(Citation: PaloAlto EncodedCommand March 2017)

Name

Web Service

ID

T1102

Description

Adversaries may use an existing, legitimate external Web service as a means for relaying data to/from a compromised system. Popular websites and social media acting as a mechanism for C2 may give a significant amount of cover due to the likelihood that hosts within a network are already communicating with them prior to a compromise. Using common services, such as those offered by Google or Twitter, makes it easier for adversaries to hide in expected noise. Web service providers commonly use SSL/TLS encryption, giving adversaries an added level of protection. Use of Web services may also protect back-end C2 infrastructure from discovery through malware binary analysis while also enabling operational resiliency (since this infrastructure may be dynamically changed).

Name

Deobfuscate/Decode Files or Information

ID

T1140

Description

Adversaries may use [Obfuscated Files or Information](https://attack.mitre.org/techniques/T1027) to hide artifacts of an intrusion from analysis. They may require separate mechanisms to decode or deobfuscate that information depending on how they intend to use it. Methods for doing that include built-in functionality of malware or by using utilities present on the system. One such example is the use of [certutil](https://attack.mitre.org/software/S0160) to decode a remote access tool portable executable file that has been hidden inside a certificate file.(Citation: Malwarebytes Targeted Attack against Saudi Arabia) Another example is using the Windows `copy /b` command to reassemble binary fragments into a malicious payload.(Citation: Carbon Black Obfuscation Sept 2016) Sometimes a user's action may be required to open it for deobfuscation or decryption as part of [User Execution](https://attack.mitre.org/techniques/T1204). The user may also be required to input a password to open a password protected compressed/encrypted file that was provided by the adversary. (Citation: Volexity PowerDuke November 2016)

Sector

Name
Defense ministries (including the military)
Description
Includes the military and all defense related-space activities.
Name
Government and administrations
Description
Civilian government institutions and administrations of the executive and legislative branches. The diplomatic and judicial branches are not included.
Name
Defense
Description
Public and private entities involved in the conception and production of weapons and the planning and conducting of military operations.

Indicator

Name

884dad1ef6f5dfc2ee2d4e22cc64a97042637d79ce678038b5c00e56dc9241f0

Description

SHA256 of 26fe41799f66f51247095115f9f1ff5dcc56baf8

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '884dad1ef6f5dfc2ee2d4e22cc64a97042637d79ce678038b5c00e56dc9241f0']

Name

83e0db0fa3feaf911a18c1e2076cc40ba17a185e61623a9759991deeca551d8b

Description

Unknown APT SHA256 of 599cf23db2f4d3aa3e19d28c40b3605772582cae

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '83e0db0fa3feaf911a18c1e2076cc40ba17a185e61623a9759991deeca551d8b']

Name

delooyp.com

Description

Unknown malware botnet C2 domain (confidence level: 100%)

Pattern Type

stix

Pattern

[domain-name:value = 'delooyp.com']

Name

af87a91c71b3cca1184b4b1250cacec041430264d0f8ac56bde3a6b1173e84a2

Description

Delphi SHA256 of c3038d7b01813b365fd9c5fd98cd67053ed22371

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'af87a91c71b3cca1184b4b1250cacec041430264d0f8ac56bde3a6b1173e84a2']

Name

4d6e8eb2eb04da1efbd0a0fd6dddad39ead99dfcb391ef57668e4286232127f4

Description

SHA256 of 694fa6436302d55c544cfb4bc9f853d3b29888ef

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '4d6e8eb2eb04da1efbd0a0fd6dddad39ead99dfcb391ef57668e4286232127f4']

Name

zakaria-chotzen.info

Description

Unknown malware botnet C2 domain (confidence level: 100%)

Pattern Type

stix

Pattern

[domain-name:value = 'zakaria-chotzen.info']

Name

36037040711231986f7509a2aa2af74b33022defac4669fb0eb14beba7caff39

Description

AridViper SHA256 of aeeeee47becaa646789c5ee6df2a6e18f1d25228

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '36037040711231986f7509a2aa2af74b33022defac4669fb0eb14beba7caff39']

Name

wayne-lashley.com

Pattern Type

stix

Pattern

[domain-name:value = 'wayne-lashley.com']

Name

bruce-ess.com

Pattern Type

stix

Pattern

[domain-name:value = 'bruce-ess.com']

Name

cb9fb42bfcae30b849fcc210d1ac4b39a12e32c6dc9d8523fcf9883632d7135e

Description

RAR_Archive SHA256 of 60480323f0e6efa3ec08282650106820b1f35d2f

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'cb9fb42bfcae30b849fcc210d1ac4b39a12e32c6dc9d8523fcf9883632d7135e']

Name

izocraft.com

Description

Unknown malware botnet C2 domain (confidence level: 100%)

Pattern Type

stix

Pattern

[domain-name:value = 'izocraft.com']

Name

porthopeminorhockey.net

Pattern Type

stix

Pattern

[domain-name:value = 'porthopeminorhockey.net']

Name

jane-chapman.com

Pattern Type

stix

Pattern

[domain-name:value = 'jane-chapman.com']

Name

lindamullins.info

Pattern Type

stix

Pattern

[domain-name:value = 'lindamullins.info']

Name

wanda-bell.website

Pattern Type

stix

Pattern

[domain-name:value = 'wanda-bell.website']

Name

overingtonray.info

Pattern Type

stix

Pattern

[domain-name:value = 'overingtonray.info']

Name

247bebcb221ba87b9198aa8f4102b4239e63bc2bf4bb97554c96a586b8c66007

Description

SHA256 of f3e99ec389e6108e8fda6896fa28a4d7237995be

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '247bebcb221ba87b9198aa8f4102b4239e63bc2bf4bb97554c96a586b8c66007']

Name

0a253739465b77c313e3127b3969b58d08674f2fc3fea7449e6dfbba7c4deafd

Description

Win32:TrojanX-gen\ [Trj] SHA256 of 708f05d39df7e47aefc4b15cb2db9f26bc9fad5f

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '0a253739465b77c313e3127b3969b58d08674f2fc3fea7449e6dfbba7c4deafd']

Name

claire-conway.com

Pattern Type

stix

Pattern

[domain-name:value = 'claire-conway.com']

Name

d5e0e54391818df52966eabde9398d35dda1f7c66598880f87603c8d542bc6f3

Description

ALFPER:DropItOutBrowse.A2 SHA256 of ee899ae5de50fdee657e04ccd65d76da7ede7c6f

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'd5e0e54391818df52966eabde9398d35dda1f7c66598880f87603c8d542bc6f3']

Name

aracaravan.com

Pattern Type

stix

Pattern

[domain-name:value = 'aracaravan.com']

Name

32d9d85b2105392eeb6109b27eb58c7a0ea84e7804fc19cba63fffa69d63daa4

Description

SHA256 of 75a63321938463b8416d500b34a73ce543a9d54d

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '32d9d85b2105392eeb6109b27eb58c7a0ea84e7804fc19cba63fffa69d63daa4']

Name

1b1eb1c9ff1b60ba0643a80698404f9169d0006469303aa77e235ee8dd00d213

Description

SHA256 of da96a8c04edf8c39d9f9a98381d0d549d1a887e8

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '1b1eb1c9ff1b60ba0643a80698404f9169d0006469303aa77e235ee8dd00d213']

Name

swsan-lina-soso.info

Pattern Type

stix

Pattern

[domain-name:value = 'swsan-lina-soso.info']

Name

8605a33115947343057847aba7ef0cbf57265e88b080a973b59960c2dbd0a003

Description

TA401 SHA256 of 745657b4902a451c72b4aab6cf00d05895bbc02f

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '8605a33115947343057847aba7ef0cbf57265e88b080a973b59960c2dbd0a003']

Name

nicoledotso.icu

Pattern Type

stix

Pattern

[domain-name:value = 'nicoledotso.icu']

Name

c4fdbfd6608748d7f675a83f392cd923e86a6d491395a611a3d651c3385708b8

Description

SHA256 of 4dcdb7095da34b3cef73ad721d27002c5f65f47b

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'c4fdbfd6608748d7f675a83f392cd923e86a6d491395a611a3d651c3385708b8']

Name

stgeorgebankers.com

Pattern Type

stix

Pattern

[domain-name:value = 'stgeorgebankers.com']

Name

escanor.live

Pattern Type

stix

Pattern

[domain-name:value = 'escanor.live']

Name

e1f52ea30d25289f7a4a5c9d15be97c8a4dfe10eb68ac9d031edcc7275c23dbc

Description

vad_contains_network_strings SHA256 of 994ebbe444183e0d67b13f91d75b0f9bcfb011db

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'e1f52ea30d25289f7a4a5c9d15be97c8a4dfe10eb68ac9d031edcc7275c23dbc']

Name

nicoledotson.icu

Pattern Type

stix

Pattern

[domain-name:value = 'nicoledotson.icu']

Name

fa98139b94cc56890af27e6dd02deb4da64b930e801492a966e0f13103808e2f

Description

Delphi SHA256 of 19026b6eb5c1c272d33bda3eab8197bec692abab

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'fa98139b94cc56890af27e6dd02deb4da64b930e801492a966e0f13103808e2f']

Name

spgbotup.club

Pattern Type

stix

Pattern

[domain-name:value = 'spgbotup.club']

Name

602a53d05280240c2075924af5c0bb4f4d5e86b90ae92eb3e33003d60b1ea685

Description
SHA256 of 5e46151df994b7b71f58556c84eeb90de0776609
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = '602a53d05280240c2075924af5c0bb4f4d5e86b90ae92eb3e33003d60b1ea685']
Name
beatricewarner.com
Pattern Type
stix
Pattern
[domain-name:value = 'beatricewarner.com']
Name
theconomics.net
Description
TA402
Pattern Type

stix

Pattern

[domain-name:value = 'theconomics.net']

Name

27f4e0c718d4614543c95125d670f4420b1b0990a5fdb1da9e71fa3585045968

Description

SHA256 of 5fcc262197fe8e0f129acab79fd28d32b30021d7

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '27f4e0c718d4614543c95125d670f4420b1b0990a5fdb1da9e71fa3585045968']

Intrusion-Set

Name
Molerats

Description
[Molerats](https://attack.mitre.org/groups/G0021) is an Arabic-speaking, politically-motivated threat group that has been operating since 2012. The group's victims have primarily been in the Middle East, Europe, and the United States.(Citation: DustySky)(Citation: DustySky2)(Citation: Kaspersky MoleRATs April 2019)(Citation: Cybereason Molerats Dec 2020)

Country

Name
Israel

Region

Name
Asia
Name
Middle East

Malware

Name
WIRTE
Name
Big Bang
Name
Pierogi
Name
Prev Sandman
Name
PyMicropsia
Name
LastConn
Name
BarbWire

Name
DropBook
Description
[DropBook](https://attack.mitre.org/software/S0547) is a Python-based backdoor compiled with PyInstaller.(Citation: Cybereason Molerats Dec 2020)
Name
Micropsia
Description
[Micropsia](https://attack.mitre.org/software/S0339) is a remote access tool written in Delphi.(Citation: Talos Micropsia June 2017)(Citation: Radware Micropsia July 2018)
Name
TA401
Name
Gaza Cybergang
Name
BigBang
Name
SharpStage
Description

[SharpStage](https://attack.mitre.org/software/S0546) is a .NET malware with backdoor capabilities.(Citation: Cybereason Molerats Dec 2020)(Citation: BleepingComputer Molerats Dec 2020)

Domain-Name

Value
nicoledotso.icu
jane-chapman.com
escanor.live
swsan-lina-soso.info
wayne-lashley.com
beatricewarner.com
spgbotup.club
theconomics.net
porthopeminorhockey.net
zakaria-chotzen.info
stgeorgebankers.com
delooyp.com
nicoledotson.icu

claire-conway.com

izocraft.com

aracaravan.com

wanda-bell.website

lindamullins.info

bruce-ess.com

overingtonray.info

StixFile

Value
360370407112319 86f7509a2aa2af74b33022defac4669fb0eb14beba7caff39
c4fdbfd6608748d7f675a83f392cd923e86a6d491395a611a3d651c3385708b8
0a253739465b77c313e3127b3969b58d08674f2fc3fea7449e6dfbba7c4deafd
cb9fb42bfcae30b849fcc210d1ac4b39a12e32c6dc9d8523fcf9883632d7135e
e1f52ea30d25289f7a4a5c9d15be97c8a4dfe10eb68ac9d031edcc7275c23dbc
4d6e8eb2eb04da1efbd0a0fd6dddad39ead99dfcb391ef57668e4286232127f4
8605a33115947343057847aba7ef0cbf57265e88b080a973b59960c2dbd0a003
27f4e0c718d4614543c95125d670f4420b1b0990a5fdb1da9e71fa3585045968
af87a91c71b3cca1184b4b1250cacec041430264d0f8ac56bde3a6b1173e84a2
1b1eb1c9ff1b60ba0643a80698404f9169d0006469303aa77e235ee8dd00d213
884dad1ef6f5dfc2ee2d4e22cc64a97042637d79ce678038b5c00e56dc9241f0
d5e0e54391818df52966eabde9398d35dda1f7c66598880f87603c8d542bc6f3
247bebcb221ba87b9198aa8f4102b4239e63bc2bf4bb97554c96a586b8c66007

fa98139b94cc56890af27e6dd02deb4da64b930e801492a966e0f13103808e2f
83e0db0fa3feaf911a18c1e2076cc40ba17a185e61623a9759991deeca551d8b
32d9d85b2105392eeb6109b27eb58c7a0ea84e7804fc19cba63fffa69d63daa4
602a53d05280240c2075924af5c0bb4f4d5e86b90ae92eb3e33003d60b1ea685

External References

- https://otx.alienvault.com/pulse/657b6fc5f21adc5b57300979
- https://www.sentinelone.com/labs/gaza-cybergang-unified-front-targeting-hamas-opposition/