Apr 15 2024

NETMANAGEIT

Intelligence Report

Renewed Espionage Campaign Targets Southern Asia, Possibly India

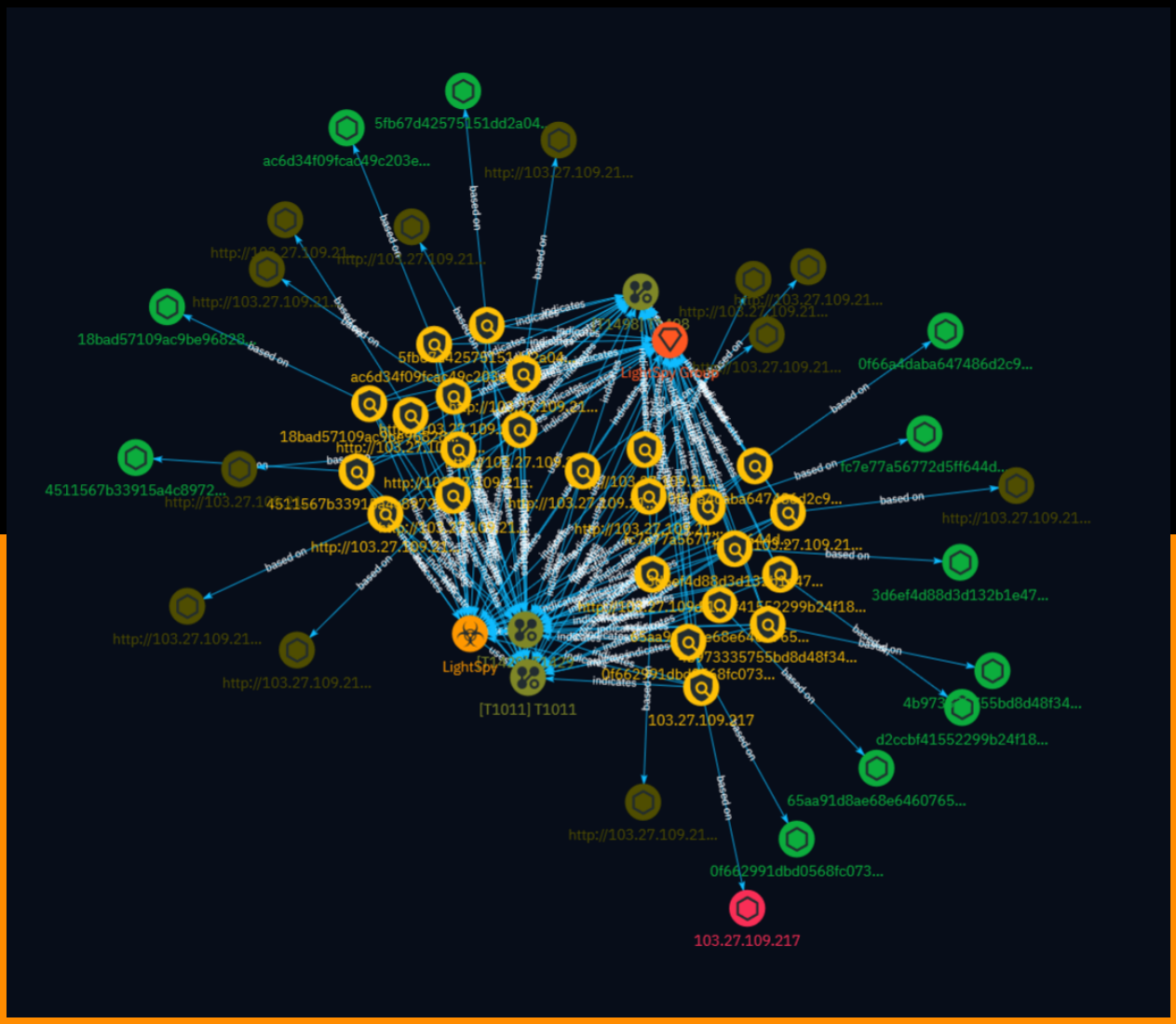

Table of contents

Overview

- Description 4
- Confidence 4
- Content 5

Entities

- Indicator 6
- Malware 18
- Intrusion-Set 19
- Attack-Pattern 20

Observables

- Url 23
- StixFile 24
- IPv4-Addr 25

External References

- External References 26

Overview

Description

This report analyzes the resurgence of the LightSpy mobile espionage campaign, targeting individuals in Southern Asia, likely India. LightSpy is an advanced iOS implant with comprehensive surveillance capabilities, including data exfiltration, audio recording, and potential device control. Evidence suggests the threat actors are Chinese speakers, raising concerns about potential state-sponsored activity. The campaign employs sophisticated techniques like certificate pinning to evade detection.

Confidence

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

100 / 100

Content

N/A

Indicator

Name

http://103.27.109.217:52202/963852741/mac/plugins/f99fcea4aba03364

Description

- **Unsafe:** False - **Server:** N/A - **Domain Rank:** 0 - **DNS Valid:** False - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': 'N/A', 'timestamp': None, 'iso': None} - **IPQS: Domain:** 103.27.109.217 - **IPQS: IP Address:** N/A

Pattern Type

stix

Pattern

[url:value = 'http://103.27.109.217:52202/963852741/mac/plugins/f99fcea4aba03364']

Name

http://103.27.109.217:52202/963852741/mac/plugins/7e3211e5a00d2783

Description

- **Unsafe:** False - **Server:** N/A - **Domain Rank:** 0 - **DNS Valid:** False - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': 'N/

A', 'timestamp': None, 'iso': None} - **IPQS: Domain:** 103.27.109.217 - **IPQS: IP Address:** N/A

Pattern Type

stix

Pattern

[url:value = 'http://103.27.109.217:52202/963852741/mac/plugins/7e3211e5a00d2783']

Name

http://103.27.109.217:52202/963852741/mac/plugins/70a5ecc118536683

Description

- **Unsafe:** False - **Server:** N/A - **Domain Rank:** 0 - **DNS Valid:** False - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': 'N/A', 'timestamp': None, 'iso': None} - **IPQS: Domain:** 103.27.109.217 - **IPQS: IP Address:** N/A

Pattern Type

stix

Pattern

[url:value = 'http://103.27.109.217:52202/963852741/mac/plugins/70a5ecc118536683']

Name

http://103.27.109.217:52202/963852741/mac/plugins/4d29ee714380cd29

Description

- **Unsafe:** False - **Server:** N/A - **Domain Rank:** 0 - **DNS Valid:** False - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': 'N/A', 'timestamp': None, 'iso': None} - **IPQS: Domain:** 103.27.109.217 - **IPQS: IP Address:** N/A

Pattern Type

stix

Pattern

[url:value = 'http://103.27.109.217:52202/963852741/mac/plugins/4d29ee714380cd29']

Name

http://103.27.109.217:52202/963852741/mac/plugins/6a0e40740cb52a1c

Description

- **Unsafe:** False - **Server:** N/A - **Domain Rank:** 0 - **DNS Valid:** False - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': 'N/A', 'timestamp': None, 'iso': None} - **IPQS: Domain:** 103.27.109.217 - **IPQS: IP Address:** N/A

Pattern Type

stix

Pattern

[url:value = 'http://103.27.109.217:52202/963852741/mac/plugins/6a0e40740cb52a1c']

Name

http://103.27.109.217:52202/963852741/mac/plugins/484c8be6af1675b7

Description

- **Unsafe:** False - **Server:** N/A - **Domain Rank:** 0 - **DNS Valid:** False - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': 'N/A', 'timestamp': None, 'iso': None} - **IPQS: Domain:** 103.27.109.217 - **IPQS: IP Address:** N/A

Pattern Type

stix

Pattern

[url:value = 'http://103.27.109.217:52202/963852741/mac/plugins/484c8be6af1675b7']

Name

http://103.27.109.217:52202/963852741/mac/plugins/2e351c7b4de4d3b1

Description

- **Unsafe:** False - **Server:** - **Domain Rank:** 0 - **DNS Valid:** False - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': 'N/A', 'timestamp': None, 'iso': None} - **IPQS: Domain:** 103.27.109.217 - **IPQS: IP Address:** N/A

Pattern Type

stix

Pattern

[url:value = 'http://103.27.109.217:52202/963852741/mac/plugins/2e351c7b4de4d3b1']

Name

http://103.27.109.217:52202/963852741/mac/plugins/26f7d6b449f01571

Description

- **Unsafe:** False - **Server:** N/A - **Domain Rank:** 0 - **DNS Valid:** False - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': 'N/A', 'timestamp': None, 'iso': None} - **IPQS: Domain:** 103.27.109.217 - **IPQS: IP Address:** N/A

Pattern Type

stix

Pattern

[url:value = 'http://103.27.109.217:52202/963852741/mac/plugins/26f7d6b449f01571']

Name

http://103.27.109.217:52202/963852741/mac/plugins/0c377d6b6b074d16

Description

- **Unsafe:** False - **Server:** N/A - **Domain Rank:** 0 - **DNS Valid:** False - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': 'N/A', 'timestamp': None, 'iso': None} - **IPQS: Domain:** 103.27.109.217 - **IPQS: IP Address:** N/A

Pattern Type

stix

Pattern

[url:value = 'http://103.27.109.217:52202/963852741/mac/plugins/0c377d6b6b074d16']

Name

http://103.27.109.217:52202/963852741/mac/plugins/0408ece5a667ec06

Description

- **Unsafe:** False - **Server:** N/A - **Domain Rank:** 0 - **DNS Valid:** False - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': 'N/A', 'timestamp': None, 'iso': None} - **IPQS: Domain:** 103.27.109.217 - **IPQS: IP Address:** N/A

Pattern Type

stix

Pattern

[url:value = 'http://103.27.109.217:52202/963852741/mac/plugins/0408ece5a667ec06']

Name

http://103.27.109.217:52202/963852741/mac/C40F0D27

Pattern Type

stix

Pattern

[url:value = 'http://103.27.109.217:52202/963852741/mac/C40F0D27']

Name

fc7e77a56772d5ff644da143718ee7dbaf7a1da37cceb446580cd5efb96a9835

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'fc7e77a56772d5ff644da143718ee7dbaf7a1da37cceb446580cd5efb96a9835']

Name

ac6d34f09fcac49c203e860da00bbbe97290d5466295ab0650265be242d692a6

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'ac6d34f09fcac49c203e860da00bbbe97290d5466295ab0650265be242d692a6']

Name

d2ccbf41552299b24f186f905c846fb20b9f76ed94773677703f75189b838f63

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'd2ccbf41552299b24f186f905c846fb20b9f76ed94773677703f75189b838f63']

Name

65aa91d8ae68e64607652cad89dab3273cf5cd3551c2c1fda2a7b90aed2b3883

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '65aa91d8ae68e64607652cad89dab3273cf5cd3551c2c1fda2a7b90aed2b3883']

Name

5fb67d42575151dd2a04d7dda7bd9331651c270d0f4426acd422b26a711156b5

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '5fb67d42575151dd2a04d7dda7bd9331651c270d0f4426acd422b26a711156b5']

Name

4b973335755bd8d48f34081b6d1bea9ed18ac1f68879d4b0a9211bbab8fa5ff4

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '4b973335755bd8d48f34081b6d1bea9ed18ac1f68879d4b0a9211bbab8fa5ff4']

Name

4511567b33915a4c8972ef16e5d7de89de5c6dffe18231528a1d93bfc9acc59f

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '4511567b33915a4c8972ef16e5d7de89de5c6dffe18231528a1d93bfc9acc59f']

Name

http://103.27.109.217:52202/963852741/mac/macversion.json

Description

- **Unsafe:** False - **Server:** N/A - **Domain Rank:** 0 - **DNS Valid:** False - **Parking:** False - **Spamming:** False - **Malware:** False - **Phishing:** False - **Suspicious:** True - **Adult:** False - **Category:** N/A - **Domain Age:** {'human': 'N/A', 'timestamp': None, 'iso': None} - **IPQS: Domain:** 103.27.109.217 - **IPQS: IP Address:** N/A

Pattern Type

stix

Pattern

[url:value = 'http://103.27.109.217:52202/963852741/mac/macversion.json']

Name

3d6ef4d88d3d132b1e479cf211c9f8422997bfcaa72e55e9cc5d985fd2939e6d

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '3d6ef4d88d3d132b1e479cf211c9f8422997bfcaa72e55e9cc5d985fd2939e6d']

Name

18bad57109ac9be968280ea27ae3112858e8bc18c3aec02565f4c199a7295f3a

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '18bad57109ac9be968280ea27ae3112858e8bc18c3aec02565f4c199a7295f3a']

Name

0f66a4daba647486d2c9d838592cba298df2dbf38f2008b6571af8a562bc306c

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '0f66a4daba647486d2c9d838592cba298df2dbf38f2008b6571af8a562bc306c']

Name

0f662991dbd0568fc073b592f46e60b081eedf0c18313f2c3789e8e3f7cb8144

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '0f662991dbd0568fc073b592f46e60b081eedf0c18313f2c3789e8e3f7cb8144']

Name

103.27.109.217

Description

- **Zip Code:** N/A - **ISP:** Topway Global - **ASN:** 132883 - **Organization:** Topway Global - **Is Crawler:** False - **Timezone:** Asia/Hong_Kong - **Mobile:** False - **Host:** 103.27.109.217 - **Proxy:** True - **VPN:** False - **TOR:** False - **Active VPN:** False - **Active TOR:** False - **Recent Abuse:** False - **Bot Status:** False - **Connection Type:** Premium required. - **Abuse Velocity:** Premium required. - **Country Code:** HK - **Region:** Hong Kong - **City:** Hong Kong - **Latitude:** 22.28000069 - **Longitude:** 114.15000153

Pattern Type

stix
Pattern
[ipv4-addr:value = '103.27.109.217']

Malware

Name
LightSpy

Intrusion-Set

Name
LightSpy Group

Attack-Pattern

Name
T1429
ID
T1429
Description
Adversaries may capture audio to collect information by leveraging standard operating system APIs of a mobile device. Examples of audio information adversaries may target include user conversations, surroundings, phone calls, or other sensitive information. Android and iOS, by default, require that applications request device microphone access from the user. On Android devices, applications must hold the `RECORD_AUDIO` permission to access the microphone or the `CAPTURE_AUDIO_OUTPUT` permission to access audio output. Because Android does not allow third-party applications to hold the `CAPTURE_AUDIO_OUTPUT` permission by default, only privileged applications, such as those distributed by Google or the device vendor, can access audio output.(Citation: Android Permissions) However, adversaries may be able to gain this access after successfully elevating their privileges. With the `CAPTURE_AUDIO_OUTPUT` permission, adversaries may pass the `MediaRecorder.AudioSource.VOICE_CALL` constant to `MediaRecorder.setAudioOutput`, allowing capture of both voice call uplink and downlink. (Citation: Manifest.permission) On iOS devices, applications must include the `NSMicrophoneUsageDescription` key in their `Info.plist` file to access the microphone. (Citation: Requesting Auth-Media Capture)
Name
T1498

ID

T1498

Description

Adversaries may perform Network Denial of Service (DoS) attacks to degrade or block the availability of targeted resources to users. Network DoS can be performed by exhausting the network bandwidth services rely on. Example resources include specific websites, email services, DNS, and web-based applications. Adversaries have been observed conducting network DoS attacks for political purposes(Citation: FireEye OpPoisonedHandover February 2016) and to support other malicious activities, including distraction(Citation: FSISAC FraudNetDoS September 2012), hacktivism, and extortion. (Citation: Symantec DDoS October 2014) A Network DoS will occur when the bandwidth capacity of the network connection to a system is exhausted due to the volume of malicious traffic directed at the resource or the network connections and network devices the resource relies on. For example, an adversary may send 10Gbps of traffic to a server that is hosted by a network with a 1Gbps connection to the internet. This traffic can be generated by a single system or multiple systems spread across the internet, which is commonly referred to as a distributed DoS (DDoS). To perform Network DoS attacks several aspects apply to multiple methods, including IP address spoofing, and botnets.
Adversaries may use the original IP address of an attacking system, or spoof the source IP address to make the attack traffic more difficult to trace back to the attacking system or to enable reflection. This can increase the difficulty defenders have in defending against the attack by reducing or eliminating the effectiveness of filtering by the source address on network defense devices. For DoS attacks targeting the hosting system directly, see [Endpoint Denial of Service](https://attack.mitre.org/techniques/T1499).

Name

T1011

ID

T1011

Description

Adversaries may attempt to exfiltrate data over a different network medium than the command and control channel. If the command and control network is a wired Internet connection, the exfiltration may occur, for example, over a WiFi connection, modem, cellular data connection, Bluetooth, or another radio frequency (RF) channel. Adversaries may choose to do this if they have sufficient access or proximity, and the connection might not be secured or defended as well as the primary Internet-connected channel because it is not routed through the same enterprise network.

Url

Value
http://103.27.109.217:52202/963852741/mac/plugins/f99fcea4aba03364
http://103.27.109.217:52202/963852741/mac/plugins/7e3211e5a00d2783
http://103.27.109.217:52202/963852741/mac/plugins/70a5ecc118536683
http://103.27.109.217:52202/963852741/mac/plugins/6a0e40740cb52a1c
http://103.27.109.217:52202/963852741/mac/plugins/4d29ee714380cd29
http://103.27.109.217:52202/963852741/mac/plugins/484c8be6af1675b7
http://103.27.109.217:52202/963852741/mac/plugins/2e351c7b4de4d3b1
http://103.27.109.217:52202/963852741/mac/plugins/26f7d6b449f01571
http://103.27.109.217:52202/963852741/mac/plugins/0c377d6b6b074d16
http://103.27.109.217:52202/963852741/mac/plugins/0408ece5a667ec06
http://103.27.109.217:52202/963852741/mac/macversion.json
http://103.27.109.217:52202/963852741/mac/C40F0D27

StixFile

Value
fc7e77a56772d5ff644da143718ee7dbaf7a1da37cceb446580cd5efb96a9835
d2ccbf41552299b24f186f905c846fb20b9f76ed94773677703f75189b838f63
ac6d34f09fcac49c203e860da00bbbe97290d5466295ab0650265be242d692a6
65aa91d8ae68e64607652cad89dab3273cf5cd3551c2c1fda2a7b90aed2b3883
5fb67d42575151dd2a04d7dda7bd9331651c270d0f4426acd422b26a711156b5
4b973335755bd8d48f34081b6d1bea9ed18ac1f68879d4b0a9211bbab8fa5ff4
4511567b33915a4c8972ef16e5d7de89de5c6dffe18231528a1d93bfc9acc59f
3d6ef4d88d3d132b1e479cf211c9f8422997bfcaa72e55e9cc5d985fd2939e6d
18bad57109ac9be968280ea27ae3112858e8bc18c3aec02565f4c199a7295f3a
0f66a4daba647486d2c9d838592cba298df2dbf38f2008b6571af8a562bc306c
0f662991dbd0568fc073b592f46e60b081eedf0c18313f2c3789e8e3f7cb8144

IPv4-Addr

Value
103.27.109.217

External References

- https://blogs.blackberry.com/en/2024/04/lightspy-returns-renewed-espionage-campaign-targets-southern-asia-possibly-india
- https://otx.alienvault.com/pulse/661ce8bfefbeb41610234efa