THREAT CURE
RE-ARCHITECT YOUR THREAT LANDSCAPE

ThreatCure

Cyber Threat Advisory

AridSpy

Threat Actor Malware

CATEGORY

Malware

SEVERITY

High

Platforms

Windows

IMPACT

- Cyber Espionage
- Data Exfiltration
- Credential Theft
- Persistence & Evasion
- Network Compromise

Description

AridSpy

Security researchers uncovered an espionage campaign by the Arid Viper APT group distributing a multistage Android spyware named AridSpy. The malware is spread via trojanized applications masquerading as legitimate messaging and governmental apps, primarily targeting users in Egypt and Palestine.

Over the past three months, nearly 40,000 attack attempts have been blocked, with over 113,000 unique victims impacted globally. The objective of these campaigns is to steal sensitive information, establish remote access, and execute unauthorized operations on compromised systems.

Key Findings:

- Multistage Android malware (AridSpy) deployed via five dedicated malicious websites.
- Malware embedded into trojanized apps impersonating messaging, job, and governmental services.
- Avoids detection by downloading first- and second-stage payloads from C&C servers.
- Spyware capabilities: Data exfiltration, keylogging, call recording, location tracking, and capturing messages from apps like WhatsApp & Facebook Messenger.
- Attributed to: Arid Viper (APT-C-23, Desert Falcons, and Two-tailed Scorpion).

Indicator of Compromise

SHA-1

29814eacb12b53efcda496485765a30c3c2b589e
2f0895fa9e1a404da46f56ab13c131de1a0eac1e
300fb7a0597519b99b6120d16666be9b29ee5508
31ba9425007d17745bb6b44c85042dcbd15fe837
46bfcb28cde424d0d11e5772c2683391b0f1491a
4f58d69c53685365a4b6df70eca6fa203e6ba674
532876649c027ebaea56604fbcd7ce909a8aa4e3
5476d52ab6f982bb29ba2ace0074e77523f9f655
55c9c7a53c9468d365743f155b2af7e189586822
5a238ade0b402c3dbef7c82406649f27ae6b479a
600442488eb9536c821188dfad9d59e987ff7a56
6f68e8645b4b88d7608310b7736749368398914a
793177ffe60030fefbe6a17361b266980f151fa4
893dae5ded7eb0a35e84867e62cbbb7e831aac97
9c1c02a387b0aa59b09962f18e4873699d732019
9d9696bc552dc5dbb4d925d0fb04f77018deef50
a610a05d6087bc1493e505fd4c1e4ef4b29697e3
a8937d38cc8edb9b2dfb1e6e1c5cad6f63ae0ecc
a8e0b6fda4bc1bd93d2a0bc30e18c65eb7f07dec
aacb4e5f9e6b516b52d0008f2e5f58c60b46610b
ae8d4853377f4a553ecad0c84398ef9dc8735072
b9835174a9a4445dc4d5ff572a79c54f234120bf
c0f4592df97073fb5021e2acee0a3763b8fbaf76
c1c5a00b22e7d12e8a41d5d8fbe625ecb218fa7c

SHA-256

7551f1af1e8a6b8cd6d646dce88a5d605af49c86872a8b2c1d87c45f9aa755df
6bb93220660780e0640738e5b2b1ecf859ad8f28485f19380f482e7ffb160067
a91a0fb4b84fff52ec7057b5dcb29264397989a0a7adc91eb3143d88182fd4d7
750751fb2462bdbebaf627c1c603fe0f123d2a9df52957a0d1f7fe57f68e9e22
1b6113f2faf070d078a643d77f09d4ca65410cf944a89530549fc1bebdb88c8c
4d59945c7cf47cae3012807686bc999ba68e4cb1dad057ead89089e503284d40
cd373fcbe222e7ce78eb64bcb0a1db82ac2a610959b6659b297e19c092727191
29d69efcf3f6646eb6e0185f3937db040f18b2a15322fee98db57b090c4e2a17
095b7fe96e4d48d1d04a3db601bb4d82be26da4ef86e6bd33df3b460dc291f75
dfe173f42da87da3df23521015043cc2aab67d10ee58301760459de4b52c155f
fe2bd91daae371afd7594cdc9c526b965b6b42060b0331f57ed7a29866557e18
3df47aa731e289e0c60cc8be37b063e5c6263c19d80b9b14b0ba854c66c7e87b
a412e5c53ae06edb9c1bf3116dc4be020f8fdb6a3edc5d4c06d75dd5eff203bf
c8a94429c42772f7bad0d6f2f37fa8de6ddc94dfb7d35b2582f1c45df093294e
416ead3c0d55728a9320372631172360a8856384ecf34052800aedc144794f49
895e5f2000362ae65a73892c349c9da3aec915b471b9a24246bd1ae8478f7bff
57fb9daf70417c3cbe390ac44979437c33802a049f7ab2d0e9b69f53763028c5
77e393ac50e0f501ebd5c6428153a300baf2b46495df015546d08a1e8b06e6b5
9ac2461b646b908e2019da6ab127de64e88a38a26b92c5e3370797e14e279c97
d81af889dfcac4ef6ef9d7c8ccacbdfebf2db079e84d0fcd74d770ebe6a95e75
519fefb414cd55faa209ae73421c802a2e167f122be1aa2d651b9d18e54adc3f
79ad78df99205e8674ad39a5b51480c32134e95738488282c1bceee12c286aa7
3f282c9497b67bba4744d861f9364f1890bdf89d9ea2b629eac8f320e016dc91
535c9a506d76a9c50b139e5f6192fc277284cbc29878fe4d6ceab7f2b709ad2f

MD5

8d63b2693bcb322ff0fb1ed0499fcb51

148138755607cfd7890bd0c811e5c03d

1af692828f5d67da599c3860552047aa

c448a041090e4282fa181b0f28430756

88d31a0f90843c2953929fe7888babc6

7a2a253b5bc59553d6eaae3cb4dcad83

c9e7afaeedab57749110989397816d9e

9d20eea731a302354ad489d0530a12f7

73f1d9c133a9bdf7a772f30b9690c35c

85b2ea8e003e7e5e4c7a2b886405939d

05629a89e5b3ca850a9092af54a4a662

18594bddc89177e4775f3ea0f0b465d8

8f1a866e4be6b4f0d344c9a6a89f64f0

c27ccfcf5617f88bf06a375f5f0a2f24

c94597060e80b8c8184e7ec9bacca346

3bb245dad6df6bda951c268f4c936d3c

3cdf8346c4f57780dbc404567150cfe9

aa970360b447b25d95f3dc6f21f711a7

5fa835a5b2a83b063aba96a603796f4b

e71d2369f777c38984df3d9aa404942c

96245b0035323f29636d87cb1e536597

850bcb71ff066c4df76b5a9c5249ed9a

1df1e215c99a147a81dfc7d47a5838cd

210cff9a5b0a43835c6ea65bb0b5cd26

Remediation

-
- Implement **Zero Trust Security Architecture** to limit access based on device health and user authentication.
- **Train employees on phishing & social engineering to prevent future infections.**
- **Block all IOCs on your XDR, MDR and other security tools.**

ThreatCure

Cyber Threat Advisory

Secure your byte world

AridSpy

Threat Actor Malware

Get Started Today

For more information about the ThreatCure ShieldOps Platform
or to schedule a demo, please contact:

- Website: www.threatcure.net
- Email: info@threatcure.net

THREAT CURE
RE-ARCHITECT YOUR THREAT LANDSCAPE