BOUNCING GOLF

HAWK BASE
HOME FOR APT RESEARCHERS

AXIAL

A SURVEY ON BOUNCING GOLF :ABOUT , WEAPON OF CHOICE , TECHNIQUES & ENGAGEMENTS

-NERDS OF AX1AL

I. INTRODUCTION

Trend micro uncovered a cyberespionage campaign targeting Middle Eastern countries. They named this campaign “Bouncing Golf” based on the malware’s code in the package named “golf.” The malware involved, which Trend Micro detects as AndroidOS_GolfSpy.HRX, is notable for its wide range of cyberespionage capabilities.

II. TARGETS

Security researchers at Trend Micro have spotted a cyberespionage campaign, dubbed ‘Bouncing Golf, that is targeting Android users in Middle Eastern countries.

III. METHODS USED

Attackers distributed the malware in tainted legitimate applications that are hosted on websites advertised on social media. The tainted applications pose as communication, news, lifestyle, book, and reference apps that are commonly used in the Middle East.
The repackaged applications are embedded with malicious code, which can be found in the com.golf package. These repackaged apps pose as communication, news, lifestyle, book, and reference apps popularly used in the Middle East. The GolfSpy malware embedded in the apps is hardcoded with an internal name used by the attacker.

IV. CAMPAIGNS

- June 2019 : The malware involved, which Trend Micro detects as AndroidOS_GolfSpy.HRX, is notable for its wide range of cyberespionage capabilities. Malicious codes are embedded in apps that the operators repackaged from legitimate applications. Monitoring the command and control (C&C) servers used by Bouncing Golf, Trend micro so far observed more than 660 Android devices infected with GolfSpy. Much of the information being stolen appear to be military-related.

AX1AL

V. IOCS

SHA 256	C2's
00e82927b20d2db5bdfc6bff77f6841d0e59af80adce3f86f90277669159e5f3	185[.]183[.]99[.]116
01cebc3a542b08c7f818540d826c7717b7354552c20ff897e9cdbddeaabe92f	190[.]2[.]130[.]53
0593167d6e7f63c8401c4393f999de2b889078ddaa3713a0d0277b953b7b1c9	194[.]187[.]249[.]134
0801d88fa8a3cf0569e2b388ec74ed3ff71e1edaf173e99c78edf86cf3aba6f6	212[.]8[.]248[.]179
09649ca5ea3efb312b6fde47fb3e0e260f762caec2c81f663fb5489eb630ae15	54[.]38[.]51[.]159
0ad4930bbbf510a4b71379a5415a22dc15f2210c872494e128b875fa114d598	82[.]211[.]31[.]181
1024c9bc5bb77c274aa28502f280470a25d27d99657a4cc9b15e194a677fb5c	84[.]234[.]96[.]167
10e7ef263a62b3bde0047bc5870f1791781d32f399dc0e15f1fac8076d52d9f7	androidsmedia[.]com
146fd6f27df73bcdf9a245ed429047c8d279fd635cf8db63f3039a9b47fd5363	androidssystem[.]com
18b9f74dba23030272ae87a4612813317fe3c8ab8bef8ca643c7fd8b0c2ce7dd	mediadownload[.]space
1abd66b4b608735e760537103849b64aaa56a118b80bdc02c2d23ef20087ee57	mediamobilereg[.]com
208d3af2924585fae89228705bb5e1a0695ab3ad9ccedc4fa5f5234c38b36bba	secandroid[.]com
22df35ef54e8381ab7be67dfd4f781c8b9eef3a80499e5261d0b9f2d4e7b8e91	sharpion[.]org
24c3c9c8d4174da861ca852af2de65d72c8f63e5d8f70c88e10c170256743da1	shileyfetwell[.]com
2d76d929c6e9a2e45caaca7706ff3a0cfebcac4a8c711d44d586eb4bc121eeed	

VI. References / Sources

https://www.trendmicro.com/en_us/research/19/f/mobile-cyberespionage-campaign-bouncing-golf-affects-middle-east.html

https://documents.trendmicro.com/assets/appendix-mobile-cyberespionage-campaign-bouncing-golf-affects-middle-east.pdf