MalOrbot
An Android malware to bridge mixes in Tor

Evangelos Mitakidis*, Dimitrios Taketzis*, Alexandros Fakis*, Georgios Kambourakis*
*Information and Communication Systems Department
University of the Aegean, Greece

***Abstract*—**

I. Introduction

One of the most widely used anonymous communication systems is Tor. It is used to provide anonymity service to users. Many researchers are trying various attacks on its protocol to discover ways to deanonymize its users. In this paper, we show a new stealthy approach to attack Tor, which enables attackers to deanonymize users instantly. In this approach, the attacker is in control of one or more specially configured exit node(s). In addition, using social engineering techniques, a user-side android malware is planted on the tor user's smart device. Its purpose is to inject user identifying information on every request that goes through Tor. When the malicious exit node receives the request with the injected information, there will be instant deanonymization.

A. Subsection Heading Here

Subsection text here.

1) Subsubsection Heading Here: Subsubsection text here.

II. Conclusion

The conclusion goes here.

Acknowledgment

The authors would like to thank...

References

[1] H. Kopka and P. W. Daly, *A Guide to LaTeX*, 3rd ed. Harlow, England: Addison-Wesley, 1999.