DNS Spoofing as a Medium for Anoymized Package Delivery

Rick Housley, Francesco Garruzzo, Michael McCarthy
Department of Electrical and Computer Engineering
Stevens Institute of Technology
Hoboken, New Jersey 07030
Email: {rhousley, fgarruzz, mmccart1}@stevens.edu

***Abstract*—The Internet consists of two principal namespaces: the domain namespace, and the Internet Protocol (IP) address space (http://tools.ietf.org/html/rfc1034). Traditionally Domain Name System (DNS) webservers are utilized as a means to traverse between these namespaces by translating domain name requests into IP addresses. As the Internet largely consists of end-users and services in need of domain name translation, DNS traffic is highly prevalent. Google's Public DNS server alone manages 70 billion requests a day (http://googleblog.blogspot.com/2012/02/google-public-dns-70-billion-requests.html).**

We present a novel method for anonymized, elusive, unidirectional messaging and package delivery using existing DNS infrastructure. Due to the pervasiveness of DNS traffic we believe that malicious content encoded within DNS packets will go unnoticed by traditional Intrusion Detection Systems (IDS) and networking analysts. The proof-of-concept presented utilizes DNS spoofing to direct DNS responses to a listening machine. The listening machine decodes messages from the DNS packet's 16-bit transaction ID.

A virtualized networked was used as the test-bench for our proof-of-concept implementation. Wireshark was used for debugging purposes as well as for ensuring the chaffy quality of the DNS requests. The final implementation consisted of a server and client. The server is capable of sending messages and files to the client while maintaining what would appear to be traditional network traffic. To ensure that the packets did not appear malicious Snort in conjunction with Snorby, a popular open-source IDS and its partner interface, were utilized. The results met our initial objectives with one shortcoming; the server-client pair only works on internal networks or with external-facing IP pairs. This is a result of Network Address Translation (NAT) acting as a firewall for non-requested packets.

I. Introduction

A. Motivation

Anonomized messaging has a number of use cases. In recent years social media has played a large role in geopolitical developments in the middle east. As a result governments have tightened their control over Internet infrastructure to quell widespread disobedience. Messaging clients that are discrete and anonymous provide security to dissenters and allow for the free dissemination of information.

Ignoring the social consequences of anonomized messaging services, malware has utilized non-traditional message exchanging techniques for quite some time to prevent detection. Simple malware has been known to communicate with Command and Control (C&C) servers via Internet Relay Chat (IRC) (http://searchsecurity.techtarget.com/feature/Command-and-control-servers-The-puppet-masters-that-govern-malware). As HTTP, HTTPS, FTP, and SSH are highly prevalent protocols, malware is also known to tunnel traffic through them. A recent news article showed that the popular website Reddit was used as a Command and Control Center by the well known iWorm (http://www.intego.com/mac-security-blog/iworm-botnet-uses-reddit-as-command-and-control-center/).

B. DNS Background

test

II. Development Process & Experimental Setup

test

III. Proof Of Concept

test

A. Features

test

B. Limitations

test

IV. Installation / Execution

test

V. Summary / Conclusions

test

VI. References

test

VII. Acknowledgements

test