DNS Sinkholing for the Downstream Consumer

Capstone Project Draft

Marymount University

Author Note

MARYMOUNT HONOR PLEDGE

I agree to uphold the principles of honor set forth by this community in the Marymount University mission statement and the Academic Integrity Policy and Community Conduct Code, to defend these principles against abuse or misuse, and to abide by the regulations of Marymount University.

Abstract

Domain Name System (DNS) is the process by which systems translate a url or domain into an IP address. The reason for this system is rather simple, without it networked or connected devices would not know how to get from our browsers to google.com and its associated webservers for example. The intent of this paper is to examine how leveraging DNS sinkholing to protect the downstream consumer could be an effective means of limiting the propagation of malware. DNS sinkholing is the process of dropping requests from users trying visit potentially malicious websites which could lead to a reduction in the cyber-crime and compromise.

Table of Contents

THIS PAGE IS LEFT BLANK INTENTIONALLY

DNS Sinkholing for the Downstream Consumer

During the 21st century the proliferation of internet usage and connected devices has led to a global problem that impacts nearly every global citizen; the lack of proper counter-measures for internet users. The rapid advancement of enterprise cyber security solutions has been nearly unbounded. This yielded benefits for corporations and governments, however, little has been done to remedy the massive security problems the individual consumer faces. This project aims to highlight and test the effectiveness of leveraging DNS sinkholing at the consumer level.

What is DNS?

DNS is an acronym for Domain Name system. Domain names are the human-readable website addresses we use every day (HTG). DNS is the mechanism by which translation from human-readable domains to computer readable IP addresses occurs. Needless to say without DNS a government, corporation, or household would cease to have Internet access in any meaningful form.

Sinkholing

DNS sinkholing implementation and use is described by the SANS Institute as:

"By intercepting outbound DNS requests attempting to access known malicious domains, such as botnets, spyware, and fake antivirus, an organization can control the response and prevent organization computers from connecting to these domains." (Bruneau)

When an end-user enters Marymount.edu, DNS translates that domain into 198.91.36.196, the IP address for one of Marymount's webservers. This allows for a seamless interaction between the end-user and underlying technology connecting them to a specified domain. DNS Sinkholing is the process of altering what domains can be resolved. It should be noted that at an enterprise scale, there are a variety of methods to control DNS, however, this

paper will focus on the individual host and/or end-user (DNS-BH). Most individual Internet users by default will use their Internet Service Provider's (ISP) DNS servers (Cisco). This simply means that a host system and its user have very little protection from resolving to malicious domains. ISPs do not focus on including sinkholing customer's traffic as their primary function is deliver connectivity, not security.

Hypothesis

The re-configuration of a host's assigned DNS server to one that has sinkholing capabilities will provide at least a fifty percent decrease in malicious content distribution onto the end users host machine.

Public Use

In today's world of complex threats, cyber crime, spear phishing, cyber espionage, the list of cyber threat vectors is nearly endless. The nominal safeguards in place for the down stream consumer are so inferior that unless significant measures are taken, not to near in the future every internet user will have been impacted by some form of malicious content or compromise.

By leveraging DNS sinkholing technology via browser plugins or reconfigurations the vast majority of avoidable cyber threats could be mitigated. That mitigation would include the down stream consumer something in today's market place is non-existent (OpenDNS).

Project Objectives

The intent of this project is to achieve three goals:

1. Assess effectiveness of DNS sinkholing for an individual host through the capture of metrics as a means of testing the validity of aforementioned hypothesis.
2. Outline testing methodology, technical resources, and results of this project.

3. Identify open-source services available to down-stream consumers that can enhance their security posture at no cost.

Faculty Support

Dr. Diane Murphy will provide faculty and technical oversight throughout the project lifecycle. The reasoning behind a partnership with Dr. Murphy is primarily based upon her incredible depth of knowledge and experience within cyber security and related fields. Dr. Murphy's time and diligence have been paramount to my success at this university.

Dr. Murphy has been working in technology related fields since the 1980s, having attained a Doctorate, founded two companies, and most recently serves as a professor and the Chair for Marymount University's Department of Information Technology (Marymount University).

Project Plan

Resources

For this project, a single Windows 7 computer will be used. The computer is a standard personal machine that has been reformatted to factory condition with all current system updates installed. VMBox will be used to create two separate hosts for testing purposes. Host 1 and 2 will be exact clones of each other, with identical *hardware* and operating systems (OS). Each host is running on Ubuntu 12.04 with Mozilla Firefox used for web browsing.

An ASUS AC1900 router with 180mbps connectivity serves as the router for the project. The ASUS AC1900 is connected to a Netgear modem and provided internet connectivity by a Tier 1 ISP. All of the resources for this project are standard personal use and intended to ensure the veracity of the test.

Configuration

Two separate hosts during testing:

Host 1 using standard ISP provided DNS. This host has no alterations or additions to the basic Ubuntu OS nor modification of its routing. Connectivity will be available via Ethernet cable direct to the router.

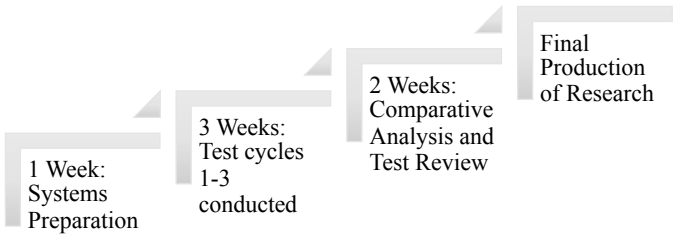
Host 2 configured to use a DNS resolver that provides sinkholing capabilities.

The DNS resolver for this project will be OpenDNS (Cisco). The DNS will be configured with 208.67.222.222 and 208.67.220.220 as the primary and backup DNS (Cisco).

Malicious Domains

The identification of malicious domains to include both phishing and malware will be provided via third party threat vendors (DNS-BH). The selected domains have been validated malicious via multi-source reporting and proven active within twelve hours of the first test. Due to the source and nature of the derivation of the threat intelligence no further information will be provided. Each test will use the same malicious domains selected, to ensure integrity and value of the DNS resolver.

Timeline



The timeline for this project is visually depicted above. During week one the systems needed for the testing will be configured and staged. A test cycle will be conducted each week for a total of three weeks. Following the completion of testing analysis and validation of the

results will occur. Once all post-test analysis is completed the results will be compiled and presented via academic format.

Test Phases

Phase 1: The ASUS AC1900 is configured to capture netflow from the hosts.

Phase 2: Each host will visit 25 distinct known good domains.

Phase 3: Each host will also visit 25 known malicious domains.

Phase 4: The ratio of dropped and or accepted DNS requests will be collected during test cycle via excel on the Windows 7 computer.

Testing Cycle

1. The test will be run 3 separate times.

2. Each test will include 25 benign and malicious domains.

3. Results will be compiled during each test and then compared in a final assessment to validate the hypothesis.

4. During testing both hosts will have mirror image internet traffic as a control to ensure the efficacy of the testing.

Key Indicators

There are three key metrics that will be captured:

1. Number of resolutions to malicious domains by each host to include any re-directs.

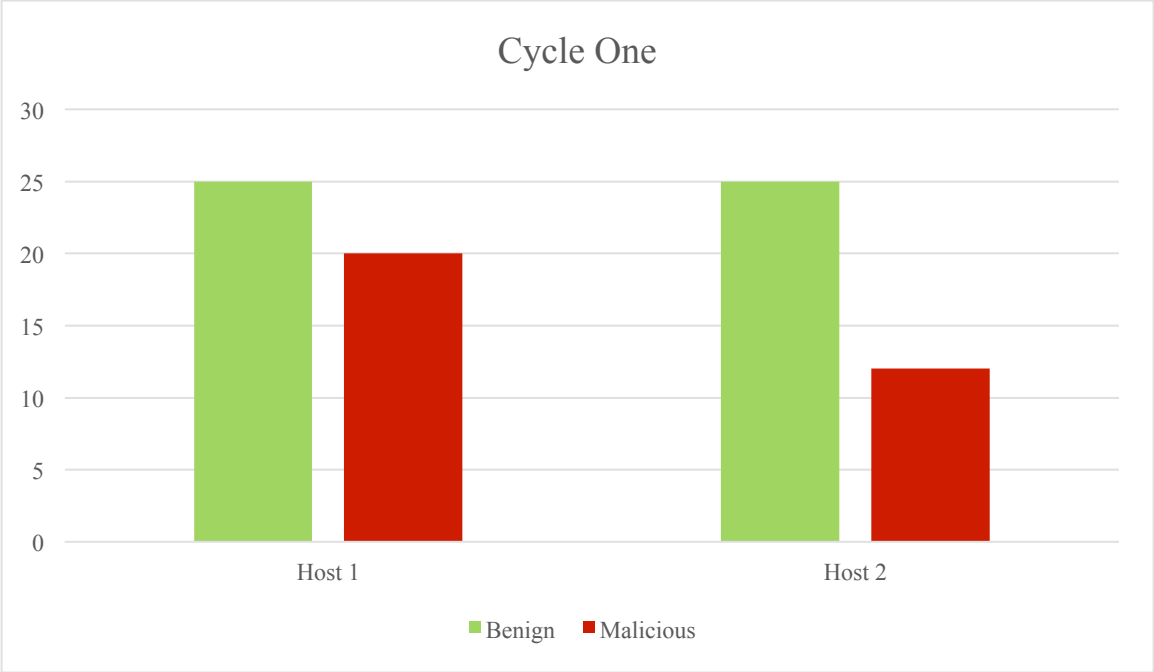
2. Number of failures to access known good domains by each host.

3. Status of malicious and benign domains; Ex: are the domains live?

Project Details

The project has yielded mixed results. Primarily, DNS sinkholing via third party resolver, proved to be effective at mitigating known bad threats at a higher rate than using the standard ISP DNS.

Results Test 1:



At first glance it appears that using a third part DNS resolver had a positive impact. During testing, several more effective means of mitigating malicious traffic become apparent. The primary issue with using an external DNS resolver it was a narrow means of protection. For example, when resolving directly to an IP address it had no means of redirecting the traffic. To further complicate the matter, all of the direct payload domains (ex: malware.com/bad.exe) were successfully resolved, resulting in compromise of the host. The primary value appeared to be derived from phishing protection. While protection against phishing sites that entice users to enter credentials is useful, it by no means was impressive.

Throughout the first test, warnings from the Mozilla browser had to be ignored to ensure that the DNS resolver would redirect and drop the connection attempt. This led to a very simple conclusion, browser based security measures are highly effective and had far more value than the DNS resolver as they protected the user at the application layer. Even more troubling was the ASUS AC1900, which has built in malware defense provided by TrendMicro. Those features had to be forcibly turned off to ensure the test was even possible. When left on, nearly all the traffic was dropped by the router and a splash page stating the site was malicious thus no connection was established would populate. The last aspect that led to near complete discrediting of DNS sinkholing as a standalone security counter-measure was the inability of the resolver to prevent against downloading of malicious content. After several compromises, an anti-virus was installed which identified all malicious content downloaded in addition to a variety of security options including secure DNS resoloution.

Another interesting aspect to the test, was the enabling of a VPN, which would actually circumvent the routers protections and alter the DNS resolution of the host (GRC). The reason for this was due to the OpenVPN configuration which forced all traffic including DNS through the VPN server, thus eliminating the use of OpenDNS outright.

From an overall perspective, it is clear that using and a third party DNS resolver provides some added security, however, there are a variety of means to achieve better security. At this stage of testing, a more comprehensive look at host based security is required.

A knowledge gap exists in the areas of anti-virus definition technology, firewall rules, heuristic based detection, and host-based intrusion detection. The ability to apply defense-in-depth at the host is highly complex and far more intensive than previously expected. The ability

to protect a host OS and its traffic throughout the TCP stack requires varied technology, significant configuration capability, and most importantly substantial research.

Risk Assessment

There are several risks associated with this project. Primarily, the risk is segmented into two categories; risk to tester and risk to consumer. While performing tests for this project, the host network, supporting IT infrastructure, and human capital are being put at risk of compromise. The risk stems from the intentional use of platforms to visit known domains hosting malicious content.

The risk to the consumer is centered on a false sense of security. When speaking with unsophisticated users of technology or those that lack security insight, a pervasive theme emerged; the security hoax. Users feel that if they have a solution in place like an AV they are protected from all threats and should not be cautious when using networked systems. This could not be farther from the truth. Threat vectors and actors are dynamic and relentless, this fact should leave consumers concerned, however, most think simple plug and play solutions equate to total security. When leveraging DNS sinkholing, consumers may fall victim to the above stated thought process. It is imperative should the results of these tests show substantial security value from DNS sinkholing for the downstream consumer that some form of education on the capabilities and limitations accompany the results.

Path Forward

The remaining two tests will be conducted using the controlled format outlined in the project plan. No alteration to the methodology or configurations will be used. Outside of the test cycles, a renewed focus on how DNS sinkholing can be used as part of a larger host based security strategy will become part of the research.

By expanding the scope to include gathering further information regarding implementation of sinkholing, gathering of network traffic for in-depth analysis, and lastly the use of sandboxing technology to identify the threat vectors will help provide context and enrich the projects findings.

In addition to further technical analysis, a host based defense-in-depth strategy will be included alongside the academic results. This strategy should include consumer based security products, how they interact with each other, and how they can provide value for the consumer and little to no cost.

References

1. Bambenek, J. (2015, April 6). Principles of Malware Sinkholing - Dark Reading. Retrieved October 23, 2015, from http://www.darkreading.com/partner-perspectives/general-dynamics-fidelis/principles-of-malware-sinkholing/a/d-id/1319769

2.Bruneau, G. (2010, August 7). DNS Sinkhole. Retrieved October 23, 2015, from https://www.sans.org/reading-room/whitepapers/dns/dns-sinkhole-33523

3. Cisco Aquires OpenDNS. (2015, June 30). Retrieved October 23, 2015, from http://newsroom.cisco.com/press-release-content?type=webcontent&articleId=1667697

4. Dagon, D. (2014, June 3). What We Learned from Sinkholing CryptoLocker – Ushering in an Era of Cyber Public Health - Damballa. Retrieved October 23, 2015, from https://www.damballa.com/learned-sinkholing-cryptolocker-ushering-era-cyber-public-health/

5. Dan Virgillito, D. (2014, September 8). How a DNS Sinkhole Can Protect Against Malware - InfoSec Resources. Retrieved October 23, 2015, from http://resources.infosecinstitute.com/dns-sinkhole-can-protect-malware/

6. DNS-BH – Malware Domain Blocklist. (n.d.). Retrieved October 23, 2015, from http://www.malwaredomains.com/?page_id=6#Summary

7. Dr. Diane Murphy. (2014). Retrieved October 23, 2015, from http://www.marymount.edu/Home/Contact-Us/Directory/?profileid=37

8. GRC | OpenVPN HOWTO Guide: Routing vs Bridging . (2008, February 18). Retrieved October 23, 2015, from https://www.grc.com/vpn/routing.htm

9. Home Internet Security | OpenDNS. (n.d.). Retrieved October 23, 2015, from https://www.opendns.com/home-internet-security/

10. HTG Explains: What is DNS? (n.d.). Retrieved October 23, 2015, from http://www.howtogeek.com/122845/htg-explains-what-is-dns/

11. PhishTank Statistics about phishing activity and PhishTank usage. (n.d.). Retrieved October 23, 2015, from https://www.phishtank.com/stats.php