zunal.com

Reducing Malicious Activities With Domain Interdiction

WebQuest Description: Provides and overview of Internet-based spearfishing attacks and how a consolidated effort between global DNS providers can be used to help reduce malicious Internet activities.
Grade Level: College / Adult
Curriculum: Technology

Keywords: spearfishing, callback, sinkhole
Published On:
Last Modified: 2013-11-02 13:58:34
WebQuest URL: http://zunal.com/webquest.php?w=218487

Introduction

The term "spear-phishing" is used when describing a cyber attack done by sending an email that contains either a malicious link or attachment to a victim over the Internet. Once the victim either opens the attachment or clicks on the embedded link, their machine can become compromised; enabling the attacker to perform follow-on exploitation activities against the victim such as installing keylogger software, document exfiltration, and other malicious activities (TrendMicro, 2012).&nbsp;One of the key indicators of a compromised machine are domain name server (DNS) requests sent from the victim to a public DNS server such as Google. Victims will send DNS requests to resolve the IP address of a malicious domain name of the attackers software, which will then enable connectivity between the malicious domain and the victim's computer. This WebQuest will discuss the concept of bringing together multiple public DNS providers in an effort to reduce the ability for malicious programs to properly resolve the IP addresses of malicious domains.&nbsp;

Tasks

The viewer will understand how their computer resolves a domain name to a publicly routable IP address and how DNS relates to an infected host machine. To accomplish this, the viewer will be walked through the process of DNS and a high-level overview of routing data over the Internet. An understanding of the DNS process coupled with information on how some malicious programs communicate to their attacker will better position the viewer to identify and mitigate malicious connections from their machine.&nbsp;

Process

DNS ProcessIn order to better understand how a computer resolves a domain name to a public IP address, the viewer will now go over a step-by-step process of how this works.&nbsp;1) User enters a domain name in the browser to the site he/she desires to navigate to.&nbsp;2) The user's device will send a DNS request to a public DNS server such as Google.&nbsp;3) The Google DNS server will respond back with an IP address that correlates to the domain name.&nbsp;4) The user's device will then route packets to the IP address provided by Google.5) The user sees on his/her screen the requested domain webpage.&nbsp;This process enables a device to communicate over the Internet with the user only needing to remember domain names vice strings of numerical IP addresses, which would be difficult for a human to accurately keep track of.&nbsp;Malicious Software & DNSNow that we understand how a user's device resolves a domain to an IP address. We can now describe how malicious software uses this same process in order to communicate with an attacker's command & control (C2) infrastructure.&nbsp;The process below would happen behind-the-scenes, without the user's knowledge.&nbsp;1) A user unknowingly clicks a link or opens an attachment which installs malicious software onto the device.2) The software attempts to contact the attacker's C2 infrastructure by sending a DNS request to Google for a predetermined malicious domain. &nbsp;3) The Google DNS server responds back with the appropriate IP address of the domain.&nbsp;4) The software establish's contact with the C2 network and awaits further guidance from the attacker.&nbsp;Coordinated "Domain Sinkholing"Currently, some public DNS servers will provide an incorrect IP address to a DNS request if the domain in question was flagged as being malicious. The incorrect IP address will be sent back to the device, which will inhibit it from making connection to the attacker's C2 infrastructure (Sancho & Link, 2012). This process is commonly referred to as "sinkholing the domain."There is no current process &nbsp;in place to globally share malicious domain names and provide a consolidated effort to sinkhole these domains, across the majority of the most common DNS servers. The establishment of a global coordination center that assisted public DNS providers with the ability to track, identify, and sinkhole these malicious domains would help reduce cyber activity.

Conclusion

As the world continues to become more reliant on the Internet for personal communication and global trade, the threat of cyber crime activity has increased dramatically. This includes world intelligence organizations, cyber criminals looking to steal personal information, and for-fun malicious actors operating around the world. Our communications and knowledge of Internet-based threats needs to become broader and more technical in order to safely traverse the global domain.&nbsp;To do this, users need to be able to understand possible attack vectors used by cyber actors and better understand how our devices connect to global infrastructure.

Additionally, users must be able to conduct their own analysis on their devices, even at a high-level, to ensure their systems haven't been compromised. A key component of this analysis is from looking at DNS requests sent from a user's device to a public DNS server.&nbsp;"In a mock phishing scenario conducted between March and May, the New York CSCIC sent spoofed e-mails to about 10,000 employees across five state agencies, trying to trick users into surrendering their passwords. More than 75% of the recipients opened the e-mail, 17% followed the link, and 15% attempted to enter their passwords." (Jaikumar, 2005).In this WebQuest, we walked the viewer through the DNS process and provided a high-level overview of how a spearfishing attack could be conducted. This will better enable the user to understand normal DNS requests to those from malicious software. It also provided a recommendation of a global, coordinated effort that could be done by public DNS servers to help combat cyber activities.&nbsp;

Evaluation

Frequently Asked QuestionsQ) What is one of the most common methods for a person's computer to become infected with malicious software?A) One of the most prevalent ways personal computers become compromised is by unknowingly clicking on a link or opening an email attachment that will exploit vulnerabilities in the victim's computer. This is called a "spearfishing" attack and is conducted by state-sponsored intelligence organizations, international criminals, along with other cyber actors operating over the Internet.&nbsp;Q) Is there a way to identify suspicious connections my computer makes to the Internet?A) Yes, a user can monitor both "inbound" and "outbound" traffic on their computer to identify either IP addresses and/or domains that are unfamiliar to the user. While many connections are normal (such as those to security product vendors, social media accounts, etc), others may be malicious or warrant further investigation with Internet searches. Many security firms now publish technical information relating to malicious programs that may help diagnose a user's Internet connections.&nbsp;Q) What can a person do to help protect their computers from a spear-phishing attack?A) Multiple things can be done to protect a user's device from an attacker. This can include keeping all software updated with the latest patches, running a reputable security product, and being very caution when clicking on links or opening email attachments. It should be noted that an attacker can spoof the "sender's email address" when delivering a spearfishing email to a victim. Therefore, any link or attachment that seems unusual from a known sender should be validated (maybe by a phone call to the person) before opening or clicking on a link.&nbsp;Q) What can be done on a large scale to help reduce malicious activities that occur over the Internet?A) A major initiative could be undertaken by the global community to establish and share information related to malicious domain names and prohibit public DNS servers from resolving these domains. This would make a malicious program unable to communicate with its attacker's command & control infrastructure. &nbsp;Many DNS providers currently do this process, called a "sinkholed" domain, however; the effort is not done on a global scale to a large percentage of the public DNS servers.&nbsp;

Category and Score					Score
				Total Score	

Teacher Page

Standards

Credits
Student: Justin C. Watts
Professor: Robert B. Lipton
Date of Submission: 11/2/2013
Course: TLMN623 9040

Purpose and Title of Submission: WebQuest

Certification of Authorship (CoA): I hereby certify that I am the author of this document and that any assistance I received in its preparation is fully acknowledged and disclosed in the document. I have also cited all sources from which I obtained data, ideas, or words that are copied directly or paraphrased in the document. Sources are properly credited according to accepted standards for professional publications. I also certify that this paper was prepared by me for this purpose.

Student's Signature: Justin C. Watts
Other