DNS Sinkhole
SANSFire 2011

Guy Bruneau, GSE
Incident Handler

Hello and welcome to this SANS@Night presentation on DNS Sinkhole. My name Guy Bruneau and I'm a Senior Security Consultant with IPSS Inc. in Ottawa, Ontario, Canada.

My talk is going to cover the benefits and drawback of a DNS Sinkhole and how it can help to add another security layer in your organization to help detect and prevent access to known malicious domains.

I have made available a copy of the ISO I used to setup my DNS Sinkhole, feel free to take a copy and try it out.

So, please sit back and follow along. If you have any questions, don't hesitate to ask.

My contact at the ISC is gbruneau@isc.sans.edu

Overview

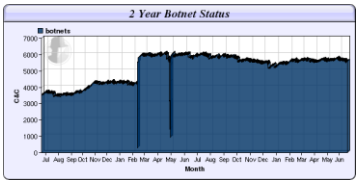
- Challenges
- Taking Control of host/domains
- Sinkhole with Bind or PowerDNS
- Sinkhole 32/64-bit ISO
- Demo
- Summary

ISC Survey June 2011

This page is intentionally left blank.

The Challenges

- Golden age of Bots
- Bots are a moving target
  - Fast flux
  - Domain hard coded in malware
- Clients under targeted attacks
  - Endless inbound spam targeting users
  - Target users to exploit applications (i.e. Adobe reader)
  - Advanced Persistent Threat (APT)
- Malware to clients = race condition
- End game is always $$$



July 2009 – June 2011
http://www.shadowserver.org/wiki/pmwiki.php/Stats/BotnetCharts

The Challenges

It is the Golden age of malware and Bots. Bots are everywhere exploiting and making money for whoever control them. Whether they are leased or custom built, the owner is constantly working at avoiding detection. More targeted attacks are commonly seen to lure people to open well crafted files or click on malicious link which in turn install malicious code that can remain undetected for days, weeks or months in the form of Advanced Persistent Threat (APT)[1] . This form of compromise is used to gain access to information from Governments, company doing cutting edge research or defence to name a few.

The common application under attack in the past year was Adobe (PDF documents) which quite often included targeted attacks against high profile targets (CEO, CFO, secretaries, etc).

1. http://en.wikipedia.org/wiki/Advanced_Persistent_Threat
2. http://itlaw.wikia.com/wiki/Botnet
3. http://searchsecuritychannel.techtarget.com/generic/0,295582,sid97_gci1278447,00.html
4. http://blog.mandiant.com/archives/730

Sinkhole Types

- Types
  - Darknet
    - Usually controlled by ISP
    - Routed, allocated IP space in which no active services
    - Collect data about anomalous network traffic
    - Often mass scanners, malware looking for new victims, or misconfigured hosts
  - Honeynet
    - Collect data from pre-configured services
  - DNS

Sinkhole Types

"Sink Holes are the network equivalent of a honey pot."[1] ISPs have been using sinkhole for several years to help protect their customers by diverting attacks and detect anomalous activity. However, the customer uses a sinkhole to collect various kind of threat their network is facing to help prevent them.

Darknet can be used for intelligence gathering and it is usually a portion of a allocated IP space without any valid services simply used to collect data. Because it isn't providing any valid services, valid traffic should not be trying to contact these address. Collecting the data attempting to communicate with these IP can be quite valuable. The traffic is quite often mass scanners, malware looking for new victims, misconfigured hosts, etc.

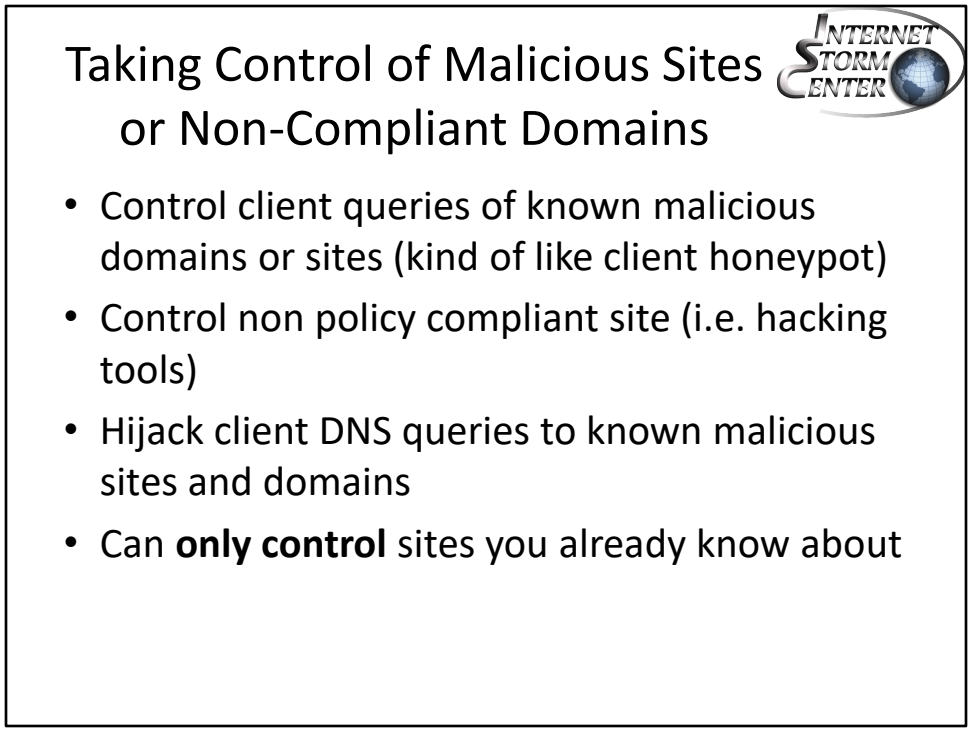
With a DNS sinkhole, you take charge of your DNS infrastructure by redirecting all domains considered malicious before the request is forward outside the corporate network. The corporate client sends its DNS request through the DNS sinkhole and gets vetted before it leaves the corporate network.

1. http://www.arbornetworks.com/dmdocuments/Sinkhole_Tutorial_June03.pdf

Regaining Control

"Scientists study the world as it is; engineers create the world that has never been." -- von Karman

This page is intentionally left blank.

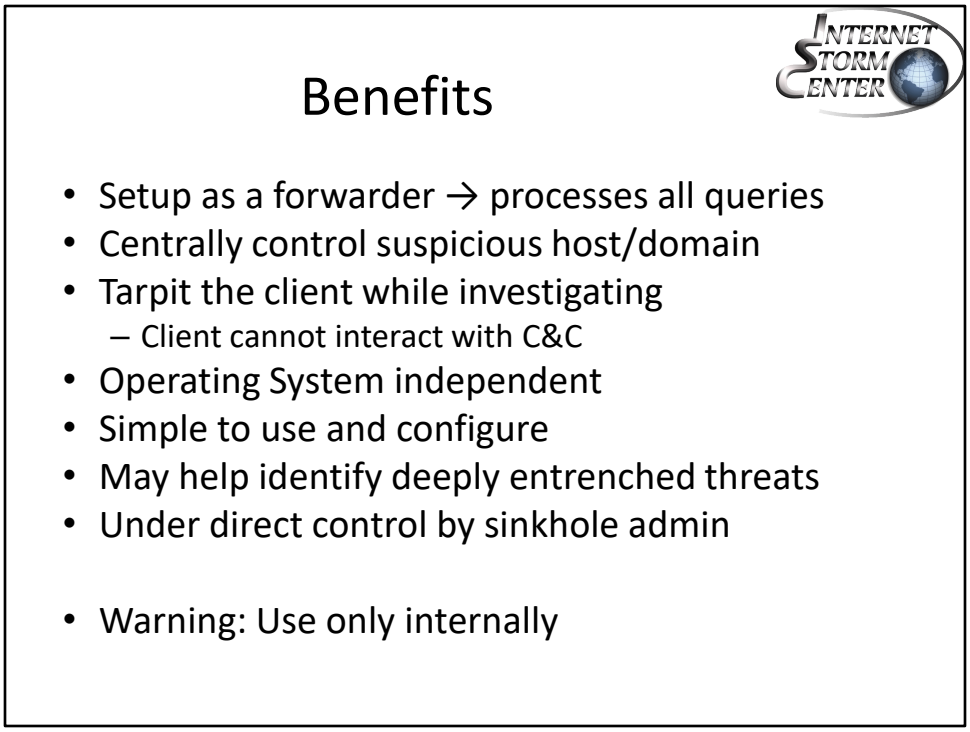


Taking Control of Malicious Sites or Suspicious Domains

Security teams are dealing daily with malware that force a client to download suspicious files from sites that we often want to prevent access. It is common for bots to use evading techniques such as fast flux to avoid being blocked by constantly changing their IP(s). However, a website name is often hard coded in malware to permit the client to download updates or upload the data it collects. This is where a DNS sinkhole can be used to find these hosts.

The primary purpose of a DNS Sinkhole is to take control of a known malicious domain before it gets a chance of leaving you network to resolve the malicious domain`s IP address(es). This can only be accomplished with known domain names (bot, spyware, malware, etc). There exist several sites on the Internet that maintain lists of known domain name hosting malware.

The sinkhole can also be used to take control of known sites that do not meet corporate policy. For example, your corporate policy stipulates that while using corporate computers you are not to access social sites. Most organizations will enforce this policy using a Unified Threat Management (UTM) device. However, another option is to create a DNS Sinkhole list and add them to the sinkhole. Redirect the client to a policy page indicating the site is blocked in accordance with corporate policy.



Benefits

Some of the most important benefit of using a DNS sinkhole in an organization is central control of suspicious domains (direct threat to the enterprise) as well as domains that do not met the enterprise's Acceptable User Policy (AUP). The other is being operating system (OS) independent. For example, It can be use to prevent access to Peer-to-Peer (P2P) sites or hacking tools (potential liability), radio and TV stations (waste bandwidth), etc.

By adding a domain to the DNS sinkhole, the client is held in a tarpit (put on hold) while analysts can find out why the client was redirected to the sinkhole. This presentation will show that configuring a DNS sinkhole is a fairly simple process to setup.

Warning: I recommend setting up a sinkhole for internal use only. A DNS sinkhole is normally used to control internal assets.

Drawback

- Host file maintenance is impractical
- Could potentially sinkhole valid site/domain
- Does not detect malware
- New sites may take time to be sinkhole
- Cannot control hard coded IP based malware
  - i.e. external DNS server hard coded in malware bypass sinkhole
  - IP address hard coded vs. domain name

Drawback

There has been some talk about maintaining some of the sites directly on the host in the hosts file. This maybe feasible on a small network but it would be to static and incapable of immediately adapting to a new threat. If a new domain needs to be added to the sinkhole, it is impractical to push that new information to all the hosts. However, adding that new domain to the corporate DNS sinkhole, it immediately take effect and provide protection to all the hosts in the network.

The most important issue that can potentially happen is to put a valid site or entire domain in the sinkhole that prevents corporate users of doing business with an enterprise. It is important to evaluate the site or domain before adding it, because it could have disastrous consequences (i.e. lost of revenue) and you could be looking for other employment.

A DNS Sinkhole does not actually detect malware but it alerts on the fact the computer might be already compromised and attempting to reach a C&C server or update the malware and on a more serious note, data exfiltration.

When a new site or domain gets added to the sinkhole, it may still resolves to its original IP address because of the Time-to-Live (TTL) assigned to its record.

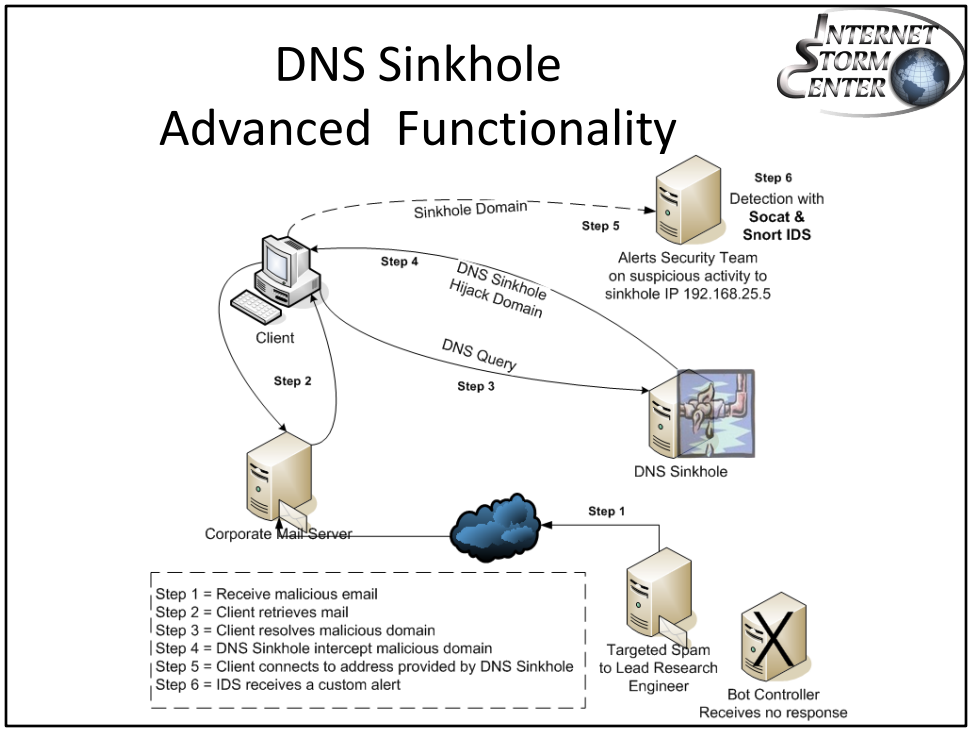
Commercial Offering

- Commercial and cloud-based
  - Do not typically allow customers to view the complete host/domain repository
  - This information is a competitive differentiator
- Free consumer-level services
  - Norton DNS (free service)
  - ClearCloud (free service ends 1 Sep)
  - OpenDNS (one free and two paid offering)

Commercial Offering

Several vendors have started offering various levels of services to block malicious sites, some are free and other cost money. Some vendors will allow you to detect which client when to what site when blocked by their offering but other free services block the site without knowing why it was blocked and what it was attempting to GET or PUSH. This could be a real problem if one of your partner or client is inadvertently added to a sinkhole block list and you have no way of removing them from it. If you decide to go with a paid service, make sure you have the ability to contact your provider to be able to remove or add a site. The longer it takes to remove it from the list to more costly it could be to the bottom line.

1. http://www.nortondns.com
2. http://www.clearclouddns.com
3. http://www.opendns.com



Sinkhole Flow

A corporate site DNS Sinkhole works quite differently than a Darknet or Honeypot Sinkhole. The main difference is the fact the site does not allow the domain to be resolve by the domain owner. Instead, the DNS Sinkhole hijacks the DNS request and provides a response with an IP you control. It provides time to gather the data you need to find which client may have been redirected to a known malicious site or is already compromised because they are attempting to connect to a known C&C server.

However, if your DNS sinkhole sites on the Internet (for example, an ISP) and anyone can resolve it, it is possible for the bot herder to check against your DNS list if the domain has been sinkhole. It is important the answer you provide doesn't leave your network.

Here is an example of a client being redirected to the sinkhole after attempting to open a document containing hidden malicious code. Another scenario is enticing the user to click on a malicious link to download malware.

Step 1 = Receive malicious email
Step 2 = Client retrieves mail
Step 3 = Client resolves malicious domain
Step 4 = DNS Sinkhole hijack malicious domain
Step 5 = Client connects to address provided by DNS Sinkhole
Step 6 = IDS receives a custom alert

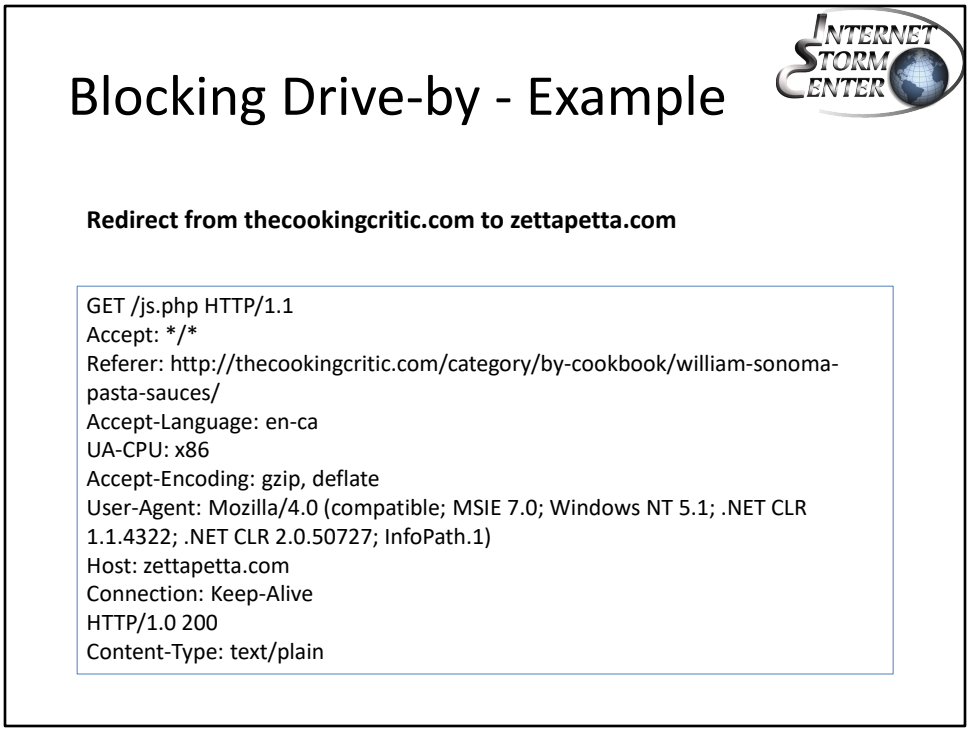
Scalability and Performance

- Using BIND or PowerDNS
  - Inexpensive, effective, scalable and easy to maintain
- Easily scale to thousand of users
- Multiple redundant servers
  - High availability and performance
- Single server with 1 GB RAM
  - Good performance with 20,000+ domains

Scalability and Performance

Loading a DNS sinkhole server with over 20,000 sinkhole domains using either Bind or PowerDNS for its DNS service, can easily provide good performance. It is a good idea to use 2 or more DNS sinkhole for high availability and improve performance.

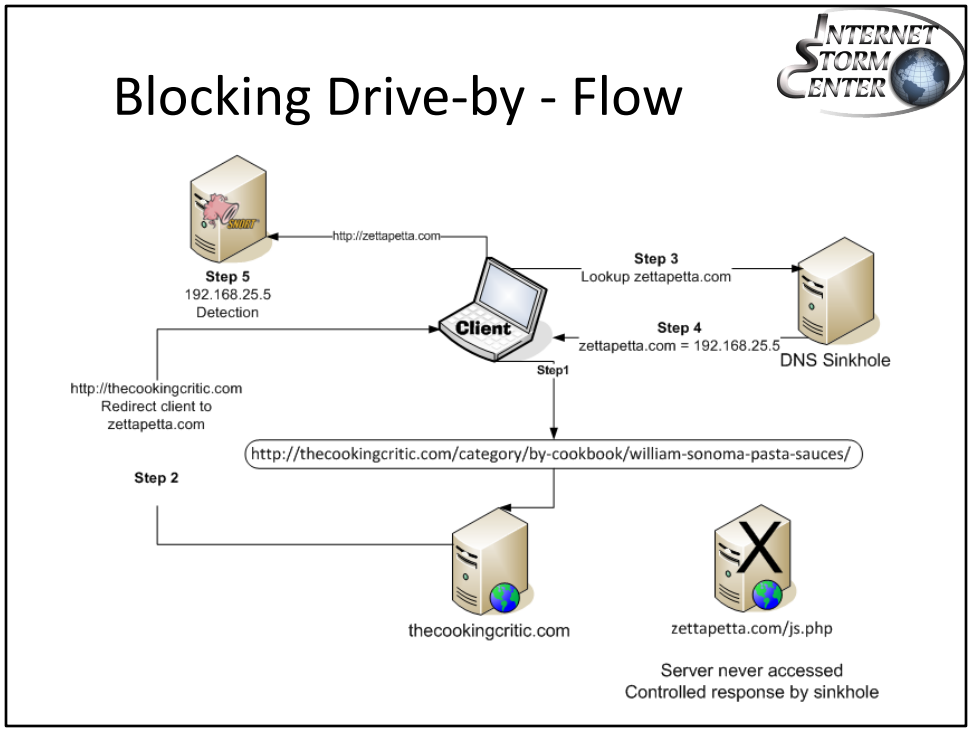
This method is inexpensive, effective and can easily scale to provide a solid service to several thousand hosts in a network.



Blocking Drive-by – Example

This example shows a client accessing `http://thecookingcritic.com` on a specific page looking at William Sonoma's pasta sauce recipes. However, on that page, unknown to the user, there is a Referer tag which attempts to get the browser to initiate a new session with `zettapetta.com`. Because the domain `zettapetta.com` is in the DNS Sinkhole list, a custom IP address is assigned to this domain to redirect the client to the internal sinkhole site to detect it activity in near realtime.

The next page shows each step in the process that eventually prevents the client from leaving the corporate network (act as an IPS) and alert the security team if a custom IDS signature has been created to alert each time a client connects to the sinkhole. The process provides Prevention and Detection.

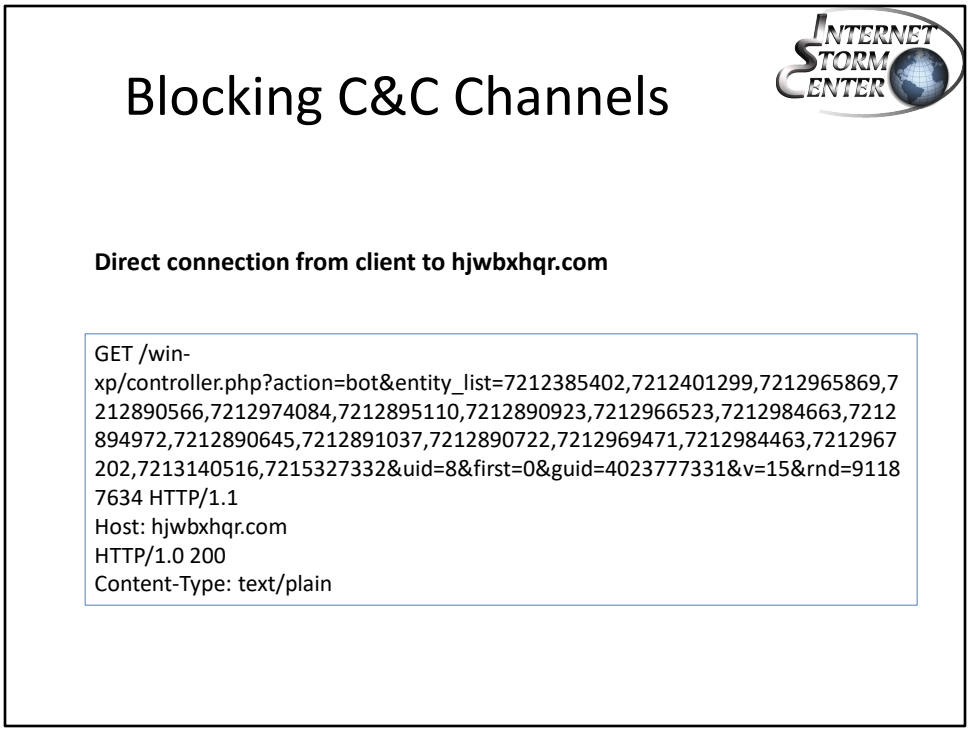


Blocking Drive-by - Flow

This example is based on the example in the previous page. Each steps of the process are described below. The main point to take away from this is the fact the client is not aware the site `zettapetta.com` is blocked unless you include a warning banner. However, if you have included and IDS signature to alert and capture the payload of the Referer, you can find out the site, whether it is a GET or a POST and the string associated with it. The other benefit, if the client is compromised (i.e. by a bot), that counter will keep going up each time the client attempts to contact the sinkhole site.

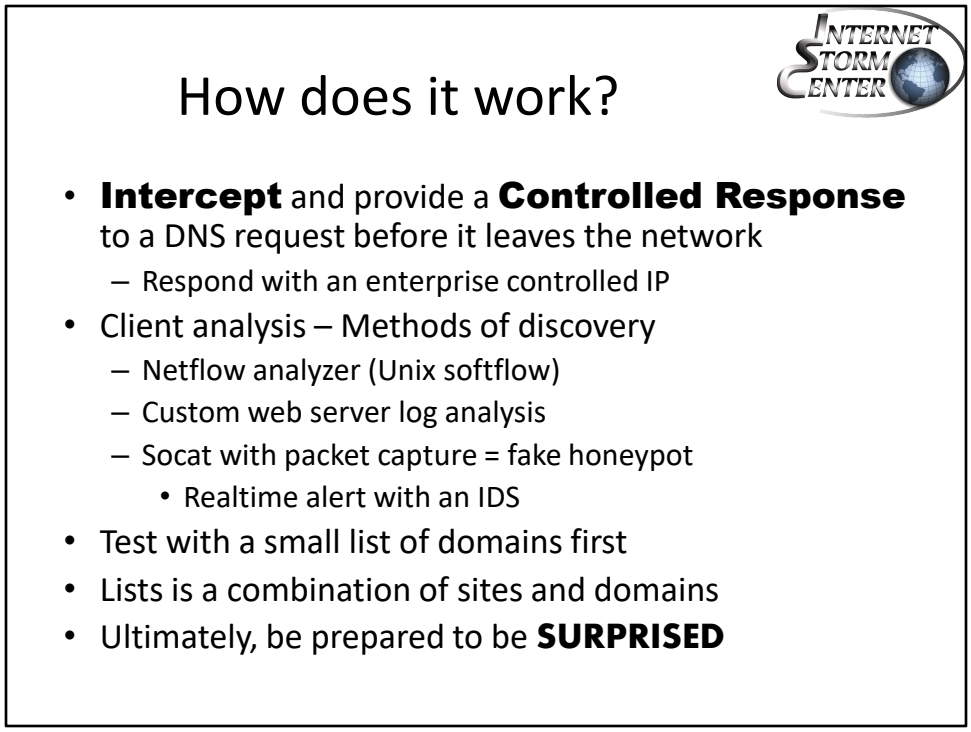
Step-by-Step

Step 1 – Client access site http://thecookingcritic.com site and get the correct IP
Step 2 – The web page from site http://thecookingcritic.com has a `Referer` which attempts to get the browser to initiate a new session with `zettapetta.com`
Step 3 – Client sends a DNS request to the DNS server that is also a DNS Sinkhole for IP resolution
Step 4 – DNS Server responds with and IP address of 192.168.25.5 because it is suspicious site and server provides a controlled response
Step 5 – Client attempt to access http://zettapetta.com and get redirected to the sinkhole which also acts as and IDS to detect the client and site it attempted to access



Blocking C&C Channels

This second example shows a compromised client attempting to connect directly to the C&C. It is clear by looking at this sinkhole event the client is compromised (i.e. controller.php?action=bot&entity_list) and attempting to report to the C&C controller.



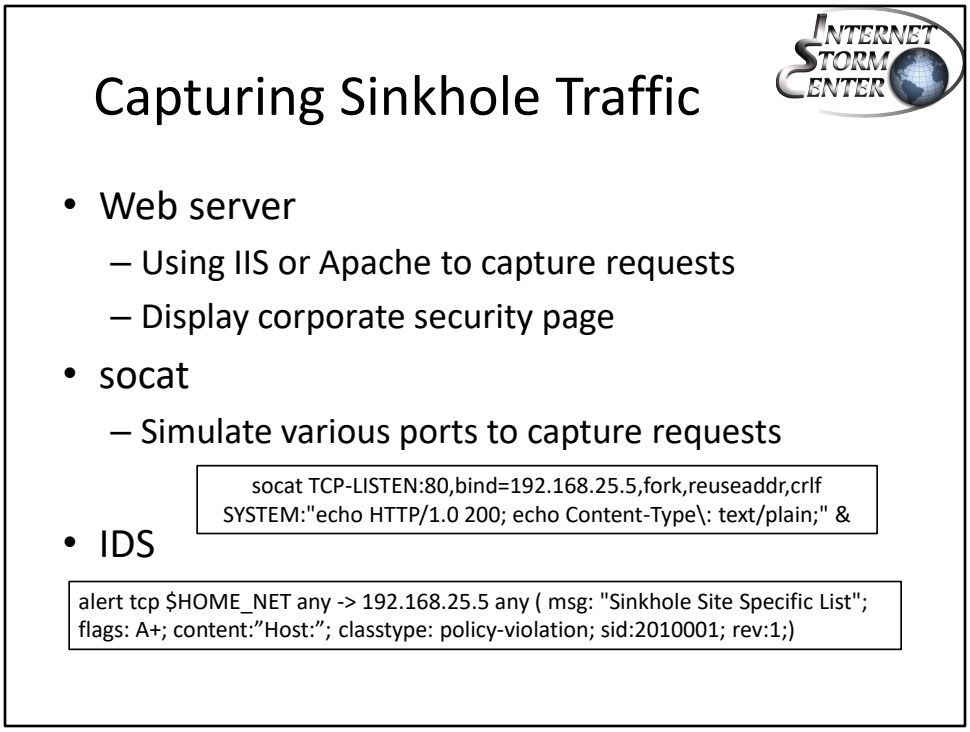
How does it work?

The first thing it does it takes control of the malicious domain by responding with an IP address controlled by the enterprise, redirecting the client to a sinkhole address under its control. This IP can be a web server or a Linux server using Socat listening on a series of common ports used by malware. This is used to capture the initial exchange with a sniffer of your choice (Sguil, tcpdump, etc).

Another option is to write an IDS signature for each sinkhole IP. This is used to detect each time a client is redirected to one of the sinkhole IP, to assist in the detection of potentially compromised clients.

Netflow is another option to find out who is connecting to the sinkhole. However, you won't be able to find the domain with this method but you will be able to build statistics on the number of hosts redirected to the sinkhole over a period of time. You can capture netflow traffic with a Linux server using softflow[1]. Send the traffic to a Netflow analyzer such as ManageEngine NetFlowAnalyzer [2] to view the collected data.

1. http://www.mindrot.org/projects/softflowd/
2. http://www.manageengine.com/products/netflow/download.html



Capturing Sinkhole Traffic

There are various ways to capture sinkhole traffic including web servers but this has limitation as you would need to set it up to listen to TCP 80, 8000, 8080 (to name a few).

However, using SOcket CAT (socat), it is easy to setup various services to simulate something like a web as well as others if needed. Socat can be used to capture which website the client attempted to connect too and the IDS event indicate which client was redirected to the DNS sinkhole. This socat configuration example, emulate the 3-way handshake and using a sniffer or a custom IDS signature, provides the ability to capture the domain the client wants to connect too. http://www.dest-unreach.org/socat/

Wit a simple IDS signature, you can use an IDS to capture the traffic from any clients redirected to the sinkhole. If you are using Sguil for your Snort IDS framework, it will capture the full packet stream which you can carve after it triggered, to find out the sinkhole domain name. This is quite useful to investigate which client is potentially infected with malware or if it was a simple redirect. If your counter keeps increasing at regular intervals, the client has most likely been compromised and is trying to contact the Command & Control (C&C). This should be investigated and may have to be rebuild using a clean media.

Sinkhole - Bind or PowerDNS

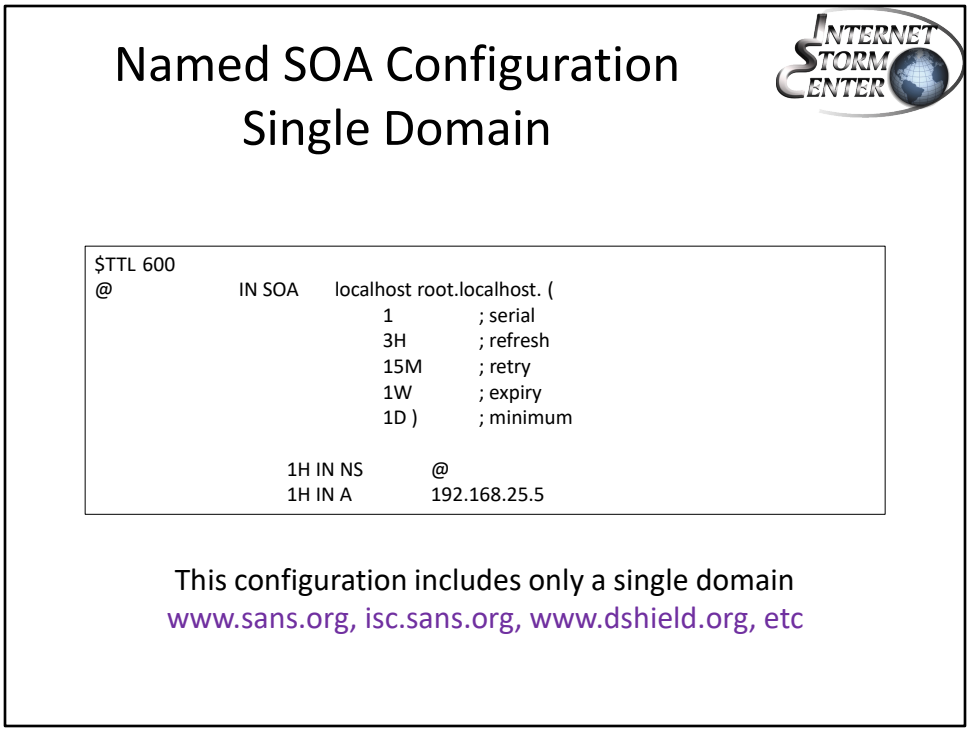
- Bind
  - Easy to setup
  - Command line driven or with Webmin access
- PowerDNS
  - All domains stored in MySQL database
  - Domain records can be accessed via browser
  - Built-in statistical server
- Populating Sinkhole List
  - sinkhole_parser.sh script

Sinkhole – Bind or PowerDNS

Out of the two available options, the Bind setup is the easiest. Using the sinkhole_parser.sh script, it is easy to download the sinkhole domain list and load that list into Bind to immediately start controlling suspicious domains. The same script is used to load that list in the PowerDNS database.

We will see a bit later how the script download and parse the list ready for use.

This presentation is based on Unix Bind and Unix PowerDNS. There is an example on how to set up a DNS Sinkhole using Windows 2003 or later using PowerShell 2.0+. This example is written by Jason Fossen the Windows SANS Instructor and should provide the same result. The configuration example is available at: http://www.sans.org/windows-security/2010/08/31/windows-dns-server-blackhole-blacklist

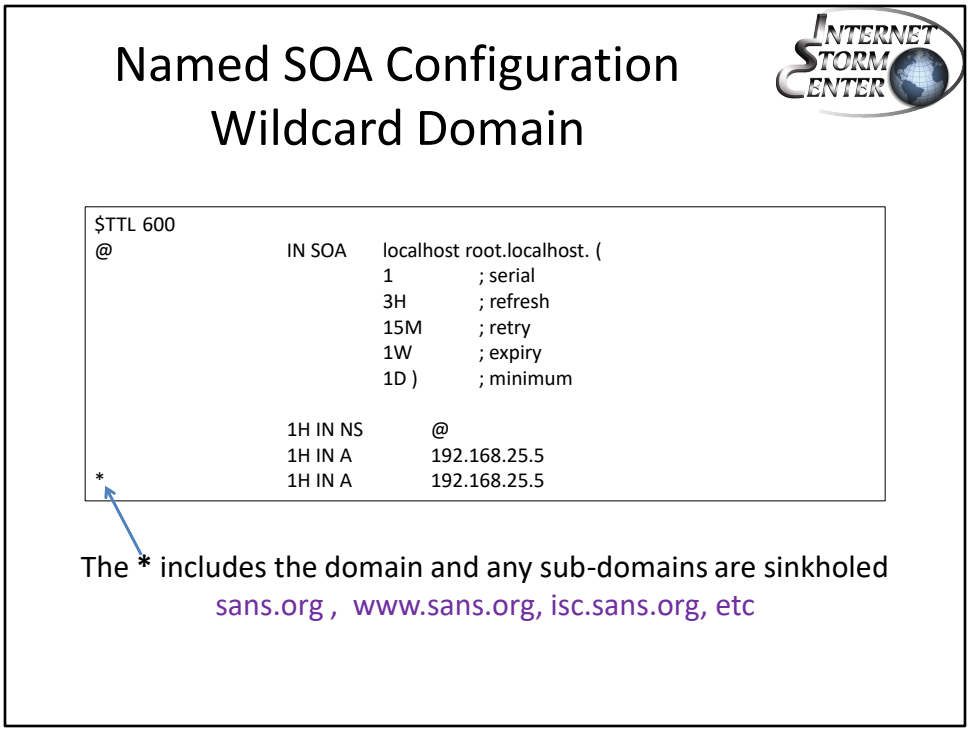


Named SOA Configuration Single Domain

Two method exist to sinkhole a domain: this method presented here sinkhole just the domain listed in the DNS table. We will see on the next slide by adding a second A record, we can sinkhole an entire domain.

In this example, if we enter www.sans.org as a record in our sinkhole, then we will be hijacking this domain an give it an response with an IP address of 192.168.25.253 to prevent a corporate client to reach its true address (66.35.45.201). If a client request to connect to www.sans.org, the answer the client will get is IP 192.168.25.253 vs. 66.35.45.201. This way we can find out through whatever means you decide to use (a few were listed earlier) which client attempted to reach www.sans.org was redirected to the sinkhole and investigate if this was a redirected or the client has been compromised and attempting to contact a C&C server (as an example).

This method hijack a single domain only.

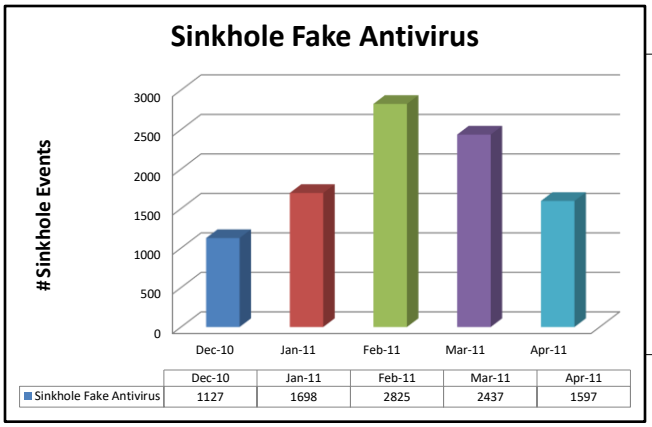


Named SOA Configuration Wildcard Domain

The second method is the addition of a second A record with a wildcard using a start (*). Both A records are needed to ensure the entire domain and sub-domains are included. So, if the domain entered as a record is sans.org, this will include www.sans.org, isc.sans.org, testing.sans.org, etc. It is all inclusive!

Warning: Be careful before you wildcard an entire domain because no one in your organization will be able to reach either the root domain and any sub-domains. Depending of the domain, this can include a few hosts to several hundred.

Case Study - FakeAV with .cc

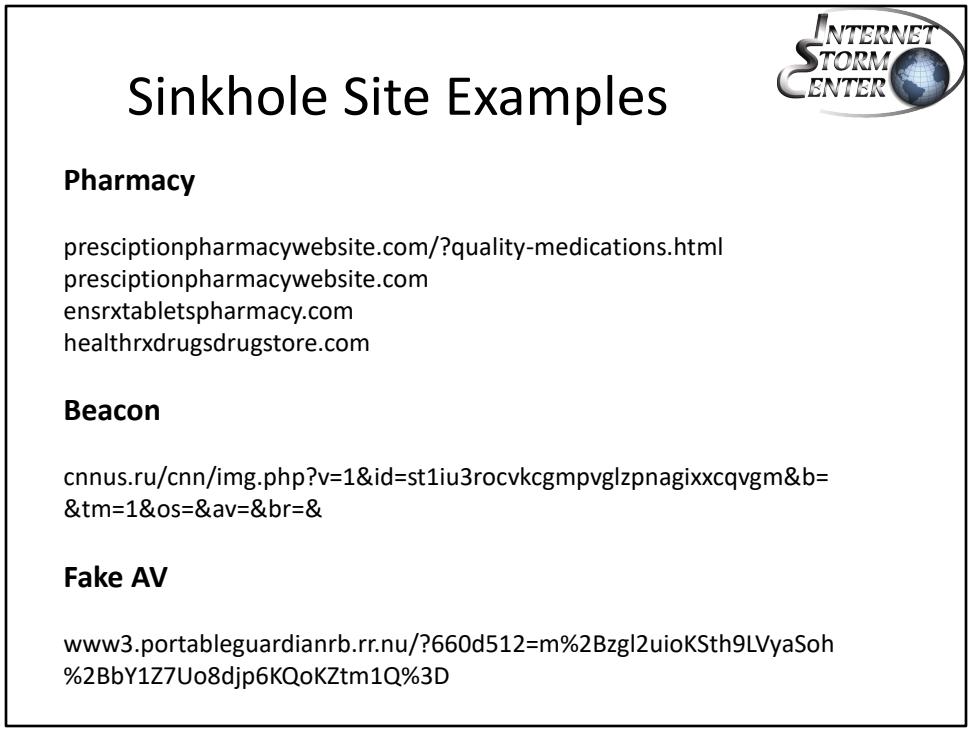


2011thebest.co.cc
av-scan2010.co.cc
av2011.co.cc
av2011best.co.cc
av2012best.co.cc
chek-pc2010.co.cc
multi-protect.co.cc
multy-protect.co.cc
protect-pc-2011.co.cc
valentine-days.co.cc

Case Study - FakeAV with .cc

This example shows Fake AV sinkhole data over a 5 months period (Dec 2010 – Apr 2011). The chart includes only a portion of the domains (co.cc) a DNS sinkhole was preventing access too. Include with the chart are some of the most popular domains seen during that 5 months period.

The list include a tell-tale domain (valentine-days.co.cc) that by now you probably realized that was used during the month of February for Valentine Day. This domain was short live but still managed to get 26 hit for that week. Some of the other domains blocked were sometime interesting (fume.co.cc, ready2view.co.cc, www.top10android.co.cc) or unreadable (lalalaldd.co.cc, x95bkbker10q6.co.cc, r--p.co.cc) no name a few.



Sinkhole Site Examples

Here are some examples of sites controlled by a DNS sinkhole. A DNS sinkhole can control various types of activity which is not necessarily malware such as Bot beacons or the download of fake antivirus software. A DNS sinkhole can control any types of domain acting as web content filtering device, blocking a Fully Qualified Domain Name (FQDN). It provides limited protection to such threats as malware, spyware, IM and inappropriate content.

How to Build a List?

Fortunately for us, there are some good list that exist out there that can be used to protect yourself. I have included 11 in the script but of course, don't forget to add your own collection from your incident cases.

Monitor who is connecting to your sinkhole and investigate. If you have assigned a different IP list to your own cases, it maybe worth investigating sooner than later which may mean the incident you previously dealt with may not be completely eradicated.

The script is written to remove duplicate domains and keep only a copy of each domain before they are added to the DND sinkhole.

If you find other domains that should be added to the sinkhole, send me an email at gbruneau@isc.sans.edu

Demo

- Sinkhole_parser.sh script
  - Download list from the Internet
  - checked_sites list to exclude valid sites
  - Test the domain list for errors
  - Activate list in Bind or PowerDNS
- PowerAdmin
  - PowerDNS interface

This page is intentionally left blank.

Summary

- DNS Sinkhole = Another defence layer
- Immediate control of known suspicious sites
- Regain control of infected client → tarpit
- OS independent
- Low maintenance

Summary

This presentation illustrated how it is possible to use Bind and PowerDNS to setup a simple, yet very effective, DNS Sinkhole to take control of domains that do not meet corporate policy. When a DNS sinkhole is deployed in a corporate network, it provides the ability to detect and regain some control of host(s) that have been compromised by malware and can also be used to prevent clients to access certain sites or domains that do not meet corporate policy. In order to add a host or domain to the sinkhole, you must know who it is and why it is breaking corporate policy.

A sinkhole is OS independent and applies to all hosts within the organization. It is low maintenance and provides another layer of security that protects your clients against known malware sites and domains.

Questions?

- Send us your logs
  - http://www.dshield.org/howto.php
- ISC Suspicious Domain List
  - http://isc.sans.edu/tools/suspicious_domains.html
- Contact us
  - http://isc.sans.org/contact.php
  - Email:handler@isc.sans.edu

- gbruneau@isc.sans.edu
- DNS Sinkhole paper available in SANS Reading room

Thanks you and I hope you found this presentation worthwhile.

Check out my OS hardened **Snort with Sguil IDS** platform and **DNS Sinkhole** ISO freely available at: http://www.whitehats.ca

References:

http://www.cert.org/archive/pdf/BotSinkhole_KrCERTCC.pdf
http://www.arbornetworks.com/dmdocuments/Sinkhole_Tutorial_June03.pdf
http://www.malwaredomains.com
http://www.askstudent.com/security/sinkholes-in-network-security-5-easy-steps-to-deploy-a-darknet/
https://zeustracker.abuse.ch/monitor.php

DNSParse Project

ISC handler Bojan Zdrnja in collaboration with Nevil Brownlee and Duane Wessels published a paper on how DNS could be used to detect unusual behaviour. The sinkhole ISO contains the DNSParse parser binary as well as a script to send the data to their project with the University of Auckland, NZ. If you wish to participate, you can contact Bojan to become part of the project.

http://www.caida.org/publications/papers/2007/dns_anomalies/dns_anomalies.pdf