NXDOMAIN is where it’s at!

Using DNS Poisoning as another layer in your Security Onion to enhance your on-line Privacy & Security

thomas.delrue@fundamental-software.net
Conclusion

- When on-line, you are being followed, all the time!
- But you can do things about that
  - Don’t be a passive surfer
- Add multiple layers of defense for any on-line activities
  - Think about an onion, each layer is a wall of defense
  - And make sure that as they cut through the layers, you give them something to cry about!
- DNS Poisoning is a great additional layer in your onion
What this is not...

- This is not about protecting you from Governmental Surveillance
  - If you’ve got a government looking for you, then you ought to be in hiding, not here!
- This is not the one thing you should do that will solve everything
  - What am I, buzzfeed or something?

But this is...

- This is about protecting you against Corporate Surveillance
- This is about giving you back control over who you (don’t) share information with when on-line
- This is one of the multiple things you can do to solve a bigger problem!
A few First Principles

- Privacy
  - the right to be left alone
  - the option to limit the access others have to one's personal information
  - secrecy, or the option to conceal any information from others
  - control over others' use of information about oneself
  - states of privacy: solitude, intimacy, anonymity, and reserve
  - a necessary precondition for the development and preservation of person-hood & autonomy
  - a necessity for a working democracy
  - self-identity and personal growth
  - protection of intimate relationships

- Your private information is valuable
  - There’s a multi-national, multi-billion dollar industry based on this premise

- Fundamentally, I am not against advertising
  - I am against tracking
  - Almost all advertisements just happen to be a subset of trackers.
Something To Consider

“Over the last 16 months, as I’ve debated this issue around the world, every single time somebody has said to me, “I don’t really worry about invasions of privacy because I don’t have anything to hide.” I always say the same thing to them. I get out a pen, I write down my email address. I say, “Here’s my email address. What I want you to do when you get home is email me the passwords to all of your email accounts, not just the nice, respectable work one in your name, but all of them, because I want to be able to just troll through what it is you’re doing on-line, read what I want to read and publish whatever I find interesting. After all, if you’re not a bad person, if you’re doing nothing wrong, you should have nothing to hide.” Not a single person has taken me up on that offer.”

Glenn Greenwald in Why privacy matters – TED Talk (Oct 2014)
Oh, you disagree?

• That’s perfectly fine, but put your money where your mouth is!

• At the end of the session, please share with the group:
  – *All of your on-line account information* so that we may access it anytime at our leisure
    • Don’t forget your financial accounts, your transactions are particularly interesting to me
  – A frequent update of your full communications
    • With whom and what about, using which device
  – 24/7 updates on your location and your associations
  – *All of your pictures* (geo-tagged please, including picture meta-data)
    • This includes your children, your pets, your acquaintances, everything
  – I want it **ALL**!
  – And I will share this with whomever I choose without telling you
  – Et cetera

• You get the point!
The Problem: The Police was Right

*Every breath you take, every move you make…*

*Every bond you break, every step you take…*

*I’ll be watching you!*

*Every single day and every word you say…*

*Every game you play, every night you stay…*

*I’ll be watching you!*

*Oh, can’t you see? You belong to me!*

…

(The Police, Every Breath You Take, Synchronicity [20 May 1983])

- Everything you do on-line is watched, recorded, processed, stored forever, played back at will, used to find your weaknesses, whatever they are, and to figure out which of your buttons need pushing
- This is all turned into data that will be used against you
  - *Never* in your favor!
Cui Bono?

- Sell you trinkets: parting you from your money
- But some is more nefarious:
  - Parting you from *even more* of your money (dynamic pricing, price elasticity, surge pricing [e.g. TicketMaster, Amazon, Uber - literally just the first hits for any of these terms])
  - Preventing you from parting yourself from your money
    - Credit: cf. "How facebook can affect your credit score"
    - Health, car, ... insurance, etc.
      - The insurance industry becomes a savings account instead of an insurance pool
  - Making you see even more ads in other places you go
    - Because then we learn even more about you
  - More and more, the end result is: Computer says "No!"
    - Why? "Because of ‘data’…"
Cui Bono?

- And then there’s the very nefarious:
  - It all started with trying to sell you things, and then it hit that slippery slope
  - Censoring through e.g. the search bubble: hiding things from you
    - Also, pages without ads get shifted down, because they don’t make us money!
  - Influencing through echo chambers: telling you what you already know
  - Behavior prediction & modification
    - Crush dissent & purge dissenters before they become “a problem”

- The Internet has become the Panopticon
  - From penology: a prison in which the prisoner doesn’t know when they are being watched but in which a prisoner could be watched at any given time
  - The purpose of a Panopticon is to force a behavior change
  - People who know they are being watched, but not when they are being watched, behave as if they are watched all the time
  - But instead of being watched occasionally, you *are* watched *always*
Who’s doing the watching?

• A person in an unmarked car following your every move and watching you 24/7 is considered creepy or requires a warrant, but replace this with an ever-expanding army of faceless, all-seeing machines that pry into everything you do on-line and that follow you everywhere you go on-line and suddenly everyone thinks that this is just dandy.
  – “But but… the ads are relevant now” - That’s a pretty low bar for ‘benefit’ you got there...

• Back in the day, there was the guy in a trench-coat with a newspaper, shadowing
  – These guys are expensive, they have faces you can remember, they’re relatively visible (don’t kid yourself, they are, cf. the Panopticon)
  – You better be very important for us to dedicate this resource to you

• Today, there are armies of faceless machines, following you everywhere and anywhere when you touch the Internet in any way, shape or form
  – They’re cheap, they have no faces, they’re easier to hide
  – You’re most certainly not important to us, which is why we’re not excluding you from being captured
  – It’s cheaper to capture everything and anything instead of capturing only what we want or need
Are you a criminal?

• What do we do with people who get out of prison?
  – Tag ‘em: put an ankle brace on them so we know where they are, where they have been and where they are going at all times
  – Make it mandatory to report in every so often with their parole officer
  – So you can take steps when they do something they shouldn’t be doing

• Are you a criminal?
  – If not, then why are you tagged when you are on-line?
    • Trackers
    • Telemetry
    • Analytics
    • Cookies
    • Content Delivery Networks
    • E-mail images & click-through links
    • Et cetera

• Why are you being treated like a criminal?
You don’t believe you’re being tracked? (2011)
You don’t believe you’re being tracked? (2012)
You don’t believe you’re being tracked? (2014)
You don’t believe you’re being tracked (2015)
But what if...?

- What if you could be on-line without being tracked?
- What if you could open up your internet pipe?
- What if you could get back control?
- What if you could eliminate some of these security risks?
- What if you could set a policy and enforce compliance?
Enhancing On-Line Privacy through Request Blocking

• Prevent your devices from talking to X or Y
  – This is the equivalent of telling your kids “Don’t talk to strangers”.

• What you don’t request, is stuff you don’t have to download
  – Don’t clog up your Internet pipe/artery

• Do you know how reputable each and every host you connect with is?

• Do you inspect every piece of code that your machine downloads before executing it?
  – What about images or documents booby-trapped with zero-days?

From a security point of view: not blocking outbound requests is really the equivalent of running random binaries from the Internet.
Arguments in favor of blocking requests

- **Privacy**
  - ‘nuff said before

- **Speed**
  - I’m paying for this bandwidth, not you. It’s mine and I will allocate it the way I please

- **Security**
  - Advertising networks are being used as malware delivery vectors
    - Combine this with Google CustomerMatch for Spear Phishing, it’s super effective!
  - Do NOT run stuff you download from the Internet!
    - zero-days, javascript

- **Control**
  - It’s my machine and I decide where it goes and who it talks to (i.e. “We don’t talk to that side of the family” or “Don’t talk to strangers”)

- **Compliance**
  - “We don’t want anyone accessing domain D1 or D2 for business reason R”: uspto.gov
Arguments against Request Blocking

• Never any valid ones

• But here are some of the most common I keep hearing
  - “You are taking away my funding” or “The Internet relies on advertising to run”
    • No, I’m not and no, it’s doesn’t
    • I pay for what I use on-line: e-mail, news, contribute to communities in time and money
    • GoFundMe, Patreon or others if you want to ask for people’s support or money
  - How much bandwidth is this really using after all?
    • 40-60% of your bandwidth actually
    • Literally 40 to 60% of all your bandwidth is being eaten up by this crap
Arguments against Request Blocking (cont)

• And some others:
  – How bad is it really if Google/FB/... knows that you visit X or Y
    • The “Like” or “+1” button is everywhere
    • If you like being under surveillance, that’s your choice
    • I also never agreed to (for instance) FB’s terms of service. I have never given them permission to track me, yet they maintain a Ghost Profile of me
  – Telemetry is to make the product better
    • Not all telemetry is telemetry: Windows 10 for example
    • The product is you
    • “better” means “more willing to give us more of their money”
  – What do you have to hide?
    • See above, but it boils down to: a whole freakin’ lot, and it’s none of your business to make any decision about it!
Preventing Tracking: Browser Add-ons

• Two main types
  
  – **Ad Blockers**
    • Some don’t work, they still request the data and then *hide* it
    • “Acceptable Advertising” is a scam (AdBlock Plus, I’m look at you!)
    • Useless arms race: Ad Blocker detection script → Ad Blocker detection-detection scripts → etc.
    • Really? We’ll trust Google to build a functional ad-blocker for Chrome?

  – **Request Blockers (e.g. μMatrix)**
    • These generally work better than ad-blockers but...
    • Hard to set up
    • Easy to get wrong
    • Can be frustrating to get started because everything appears broken, people abandon them quickly
Preventing Tracking: Browser Add-ons (cont.)

- Not all add-ons are available in all browsers (e.g. Firefox, Chrome [& Opera or Vivaldi], Safari)
- No way to enforce compliance
- No way to manage
- No way to report
- No way to control what it does
- Browser deprecation is something to consider (FF57: XPCOM & XUL needing to become WebExtensions)
- Not something your Nan can do on her own
  - And do you really want to be managing that for her?
Preventing Tracking: 
Browser Add-ons (cont)

It only work in *this* browser

It only work in *this* profile of *this* browser

It only work in *this* profile of *this* browser in *this* user account

It only work in *this* profile of *this* browser in *this* user account on *this* device
Preventing Tracking: Hosts File

- Needs to be done on every individual machine
- Low level of manageability
  - Sync hosts files across all your assets
- Needs root: good luck with phones, iPads, guest’s machines
- Exact hosts only
  - It’s a cat and mouse game: www.domain.com → www1.domain.com
  - Can’t say “don’t talk to anything under domain.com”
- I ended up with hosts files over 50MB, merged from multiple sources
  - There is a perceivable slowing down and increased memory use
  - When things go wrong, grep and sed are your only friends but I really shouldn’t have to be friends with them for this...
Preventing Tracking: Tor & Privoxy

- Do not run non-standard extensions in the tor browser
  - Do **NOT** run non-standard extensions in the tor browser!
    - Because if you depend on the TBB for anonymity, it is a way to identify you!
  - This includes Ad or Request Blockers
    - It comes with NoScript though – but it is ill-configured (turn off ‘allow scripts of top level’)
  - Tor is ‘slower’ and not blocking stuff will make it even more slow

- Many CDNs block tor exist-nodes (Google & CloudFlare for instance)
  - The CAPTCHA CloudFlare uses comes from Google *facepalm*!
  - Don’t get me started on CAPTCHA’s… I don’t like being part of the free labor Google gets for training its neural nets/AI

- Privoxy is a proxy server, so for all intents and purposes, HTTP(S) only
  - A valuable thing to set up though if you also want to strip out stuff from HTTP requests
  - Privoxy is a great extra layer in your Onion of Protection but something for another talk
Which solutions have you tried?
Preventing Tracking through DNS Poisoning

- So I started thinking: What if I could tell you “That domain doesn’t exist”/NXDOMAIN instead of the actual IP when you request ‘dumb stuff’?

- Most of the ways you are being tracked rely on your machine actively reaching out to surveillance actors
  - e.g. your machine requesting a script, a pixel, an image, a cookie
  - Sometimes just brazenly trying to upload data (e.g. contacts from your phone, ‘telemetry’)

- The Internet uses DNS at a very fundamental level
  - Sure, you could use IPs, but seriously, how many people do that?

- Everything that resolves domains, goes through DNS
  - EVERYthing, not just your browser, your ‘apps’ and anything else too

- I can apply DNS onto an entire network in a single setting
Preventing Tracking through DNS Poisoning (cont.)

- Any properly-written code deals gracefully with inability to talk to a host
  - “I’ll try again later, I guess”
  - “Doesn’t exist? I guess I’ll just move on to the next thing!”

- If it doesn’t know where to go (no IP), it can’t get there!
  - And if it doesn’t get there, they don’t see me
  - Nor the payload of data that would otherwise be sent there
    - Guess who sends a lot of these with each request...

- Use normal DNS handling (i.e. “no such domain”/NXDOMAIN) against them

This is starting to sound like something that would work much better than these other things...
Enter IvyDNS

• If you can’t find something that does what you need... Build it yourself!

• So I did and it is called **IvyDNS**
  – IvyDNS uses **DNS Poisoning** to turn a successful DNS resolution into an NXDOMAIN (i.e. “that domain doesn’t exist”) for things you want to block
  – The name IvyDNS = Poison Ivy + DNS
    • It’s a pun… a bad one, but a pun nonetheless

• Built it so that I can sell it as a service too – which I do
  – It works for home users as well as for companies, scales without issues
  – But this is about why it is a good idea and how it does some of its stuff
Quid Pi-Hole?

• There is something called PiHole
  – It does a similar thing, but in a different way
• Rather limited: on/off only
• Much more complex to set up
  – Think of your nan!
• Much more complex to manage
  – Won’t somebody think of their nan?
• You’re also not going to be running a Raspberry Pi as your DNS resolver on your company’s network
  – Nor will you run the PiHole software on a full blown server! It’s not meant for that.
• But it’s got a cutesy UI with pretty pictures, I’ll give it that
• If you know what you’re doing, PiHole can most certainly be a good DNS Poisoning solution at home!
The 5 enhancements of IvyDNS

- **Enhanced Privacy**
  - **DON’T** talk to stuff that tracks you or that violates your privacy

- **Enhanced Security**
  - **DON’T** talk to stuff that is likely going to infect you

- **Enhanced Speed**
  - **DON’T** talk to stuff that eats up your bandwidth or your CPU cycles

- **Enhanced Control**
  - **DON’T** talk to stuff you don’t want to talk to

- **Enhanced Compliance**
  - **DON’T** talk to stuff your boss tells you not to talk to

All serving a single purpose: Peace of Mind
What does IvyDNS do?

- It prevents outbound or egress requests to *undesirables* by responding to DNS Queries for known bad actors with NXDOMAIN (i.e. “That domain does not exist”)

- IvyDNS maintains something I call its “Internet Intelligence”
  - A multi-factor approach
  - Other solutions stop at “who you are” (i.e. what is your domain)
  - IvyDNS’ Internet Intelligence also contains “what you do”
  - This enables blocking on categories, for example:
    - Block advertising, errr, I mean trackers, trackers…!
    - Block social networks, music streaming, video streaming, news sites, porn, CDNs, anything Belgian (*.be), etc…
  - High level of granularity:
    - e.g. “Block social networks, except for Geocities”
  - Currently IvyDNS has detailed intelligence on over 1.3 million domains
How does IvyDNS do it?

- Multiple pieces of software: do one thing and do it well!
- The backbone of IvyDNS
  - The Collectors: agents crawling for (new) domain information
  - The Classifiers: agents figuring out what domains do and who they are
    - Heuristics
    - Some (limited) AI
    - WHOIS records (when available)
    - Etc…
- These are the core of it all
  - It really stands or falls with these
    - Without this, you just have a dumb DNS server
  - Hard to get right
    - ‘Right’ does not just mean ‘correct’, you also want to keep them honest and courteous as they figure things out on-line
How does IvyDNS do it? (cont)

• And then there are
  – The Cops: agents ensuring only valid customers can access the service
    • I learned about DNS Amplification Attacks the hard way
  – The Resolvers: the actual DNS servers
    • Really, this is currently just bind, but could be any DNS server
    • If it’s good enough for the root servers of the Internet, it’s good enough for me

• DNS Servers are the only things you interact with
  – Runs in the cloud, not on your machine
    • I’m currently working on enabling them to run on your premise as well
  – It’s really more of a configuration setting (DNS) on your end, it’s not a piece of software that eats up cycles
  – Fully redundant for maximum uptime (100% so far)
Effects of using IvyDNS/DNS Poisoning

- Frequent feedback: “I had no idea the Internet could be this peaceful”
- Imagine being left alone on the Internet
  - Nothing to steal your focus away from what you’re doing
  - No ads when you (or your kids) are on-line
  - Including in-app ads (because this works everywhere)
- People need the Internet to do their work
  - No mental pollution while you work (or play, I don’t care...)
- Imagine having the full 100% of your connection available to you
- Imagine no longer putting down footprints in the snow as you browse
- Enhanced security because IvyDNS knows about malware & exploits
Things you can do with DNS Poisoning you can’t otherwise do

- It catches more
  - Wholesale blocking
    - Block everything under *.domain.com or even *.be
    - Because why not…

- Compliance
  - Everyone uses your gateway/router as a DNS resolver and thus everyone falls under the rules of that DNS server for any DNS request, regardless of purpose, source...
  - **Inherited Compliance**: visitors on your network get it *automatically* without having to touch their devices
    - Just joining the network gives you protection, at home or in the office
    - Not having to touch tens or hundreds of devices is a big deal!
    - Inform & ask nicely not to circumvent
  - **Hard Compliance**: reroute traffic to non-sanctioned DNS server back to the sanctioned one (e.g. through NAT) – it’s *your* network
Things you can do with DNS
Poisoning you can’t otherwise do

● Flexibility
  – Different networks, different rules: e.g. marketing needs access to social networks, but everyone else in the office does not
    • Put them on different networks with different DNS servers, one allows social networks, the other blocks it

● Reporting
  – There’s always the one guy that doesn’t respond well to being asked nicely; figure out who it is by logging any DNS request that is not going to the right server!
  – Report on your DNS requests response rates (resolved vs blocked) to figure out anomalous behavior, which could indicate a potential infection
    • This is not a replacement for an anti-virus product!
A couple of words on IoT

- IoT: Internet of Things
- The P in “IoT” is for “Privacy”
- We went from “I’m afraid ‘they’ are trying to put us under surveillance” to “Surveillance device, order me more stuff and turn the music volume up!”
- Be careful not to undo your hard work in preserving your privacy by introducing these types of devices
- These devices are actively and explicitly violating your privacy

https://xkcd.com/1807/
Conclusion

• When on-line, you are being followed, all the time!
• But you can do things about that
  – Don’t be a passive surfer
• Add multiple layers of defense for any on-line activities
  – Think about an onion, each layer is a wall of defense
  – And make sure that as they cut through the layers, you give them something to cry about!
• DNS Poisoning is a great additional layer in your onion
Thanks

• Contact me:
  – thomas.delrue@fundamental-software.net
  – https://www.fundamental-software.net
  – https://www.fundamental-software.net/ivydns