Targeted Takedowns: Minimizing Collateral Damage Using Passive DNS

Dr. Paul Vixie, CEO, Farsight Security, Inc.

UBM Tech

Today's Agenda

I. Introduction

II. Passive DNS

III. Using Passive DNS to Avoid Takedowns

IV. "Paul! I'm Not a LEO or Cybercrime Investigator. Why Does This Matter To Me?"

V. Consider Contributing Passive DNS Data

VI. Summary

I. Introduction

About Dr. Paul Vixie

- CEO and Chairman of the Board of Farsight Security, Inc.
- Testified before Senate Judiciary Committee on "Taking Down Botnets“ in 2014
- Designed, implemented and deployed several DNS protocol extensions and applications including BIND → BIND8
- Founded the first anti-spam company, MAPS (for “Mail Abuse Prevention System”), a California nonprofit.
- Founded the Internet Software Consortium (ISC)
- PhD from Keio University in work related to the DNS and DNSSEC
- Inducted into the Internet Hall of Fame in 2014.

- **Badness on the Internet is *Real*: Law enforcement officers (and other anti-cybercrime investigators) are very busy people.**
- LEOs are expected to vigorously enforce laws against:

  - ✓ Online child abuse material
  - ✓ Extremists using the Internet to foment terroristic attacks
  - ✓ DDoS attacks, including DDoS attacks against control systems and other critical infrastructure
  - ✓ Phishing, carding, and other attacks targeting PII
  - ✓ Malware authors and botnet operators
  - ✓ Spammers and scammers
  - ✓ Online merchants of highly addictive drugs (sold w/o a Rx)
  - ✓ Internet sellers of shoddy knock-off merchandise, etc.

- **The public is being hurt online, and their complaints are part of what motivates LEOs.** The Internet Crime Complaint Center (IC3), a joint activity of the FBI and the National White Collar Crime Center (NWCC), reported* that in 2014 they received

  "269,422 complaints with an adjusted dollar loss of $800,492,073."

- Federal, state, and local **LEOs are all under pressure to work these incidents.** They want to take effective action; they want to make a difference.

* https://www.ic3.gov/media/annualreport/2014_IC3Report.pdf

- While the public demands action against surging cybercrime, they want it done in a **very professional and precisely-targeted way= No Collateral Damage**

- A classic hypothetical example of a takedown causing collateral damage:

  *Seizure of a **shared physical server**, thereby taking down a targeted illegal criminal operation, but **ALSO** taking down innocent/uninvolved 3rd parties also using that same system.*

- Seizure of a shared physical server is, of course, not the only way an operation might cause collateral damage.

- **Collateral damage can also result from**:
  - Takedown of a shared **domain name**
  - Blackholing/sinkholing of a shared **IP address**
  - Blocking shared **name servers** used by diverse domains
  - Arranging for upstream transit providers to cease routing **an entire downstream autonomous system** (or arranging for peers to stop peering with that AS)

- **Collateral damage to 3rd parties even has the potential to dwarf the direct harm that's being targeted for remediation.**

- In July 2014, a provider impacted by a non-LEO takedown noted that, "In all, some 1.8 million customers are still offline, which translates to more than 4 million domains." That's a **LOT!**

- To avoid collateral damage, a basic standard of care is needed.
- **LEOs (and private sector investigators) need to carefully check the domains, IPs, and/or name servers they're targeting for takedown, BEFORE taking action against them.**
- If collateral damage is a potential consequence of the planned action, that risk must be carefully assessed and considered.
- Please note that I am NOT advocating a "zero" collateral damage threshold. Sometimes, *de minimis* levels of collateral damage may be unavoidable, and accepted (that's a managerial decision, and one that should be made on an informed basis).

Incomplete List of MAJOR Landmines

- Internet infrastructure
- Registries and registrars
- Crypto infrastructure (such as CRL and OCSP servers)
- 3rd-party authoritative DNS or recursive resolver providers
- Even one widely-used ("Alexa 500") domain (Google, Facebook)
- DDoS mitigation/reverse-proxy sites (such as CloudFlare)
- Major URL shortener sites
- Major NTP (time synchronization) sites
- Some major advertising/ad metrics sites
- Many unique 2nd-level domains in a range (shared hosting range?)
- Large numbers of diverse MX records on an IP (outsourced email?)
- Gov/mil/major corps/edu's/etc. (these guys will all deal with abusers)
- Domains/IPs of known anti-abuse orgs/security companies (sinkholes)

- We'll just talk about a few of the **Landmine** categories.

- **Internet Infrastructure**: For example, even an incomplete list of Internet infrastructure would certainly include:

  -- Sites in the root hints file:
  http://www.internic.net/domain/named.root

  -- Sites in the root zone file ("TLDs"):
  http://www.internic.net/domain/root.zone

  -- Sites in the list of effective top-level domains, see:
  https://publicsuffix.org/list/public_suffix_list.dat

- By way of example (again, rather than as an exhaustive list):

  -- Sites related to the ICANN list of **registries and registrars**:

  https://www.icann.org/resources/pages/listing-2012-02-25-en
  (that file *has* been updated since the date reflected in the URL)

  http://www.internic.net/origin.html

  -- Equivalent sites for ccTLDs, as documented in the ccTLD root zone database, see

  http://www.iana.org/domains/root/db

Examples of Crypto Infrastructure

- Especially as more and more sites are deploying TLS by default, certificate validation means that OCSP responders and CRL servers have become operationally critical.

- OCSP responders and CRL servers verify that a certificate, as used in setting up a secure ("https") session hasn't been revoked.

- If a site's cert provider's OCSP responder or CRL server aren't available, attempts to access those secure sites will stall, at least if OCSP and/or CRL validation is required by the user's browser. You may want to see: https://www.imperialviolet.org/2014/04/19/revchecking.html

The "Human Shield" Model

- *De minimis* levels of good content on a site cannot "immunize" large swaths of bad content against takedowns.

- Why? Well, if even a single good (but not critical) site was enough to protect an IP against takedown, many bad guys would adopt a "human shield" hosting model -- perhaps having an IP with thousands of bad domains all used for awful purposes, plus one site donated for use for a local animal shelter.

- Sorry -- one carefully-arranged token good domain won't be enough to give your online cesspool immunity.

'What If We Only Have A Few Bad Sites?'

- Takedowns are normally a solution of last resort, and providers who deal with their own abusive customers don't tend to become the target of takedown efforts (or blocklisting by anti-spam outfits and other reputation data service providers).

- Having an abuse and/or security department, and
  -- Proactively monitoring your online assets for problems, and
  -- Acting on verifiable reports you receive from third parties
  will ensure that your operations are unlikely to ever be targeted for takedowns. Remember, takedowns are normally used strictly as a last resort, when a site is unreachable/uncooperative (or actively colluding with bad guy customers).

Documenting Customer Blocks

- The other thing that can ensure innocents are less likely to get tangled up in takedowns is **accurate, up-to-date documentation:** use SWIP or rwhois to clearly delineate dedicated customer blocks, or to call out shared hosting ranges.

- If a customer has a disjointed series of blocks rather than one single contiguous block, make it possible for concerned parties to easily find ALL those related blocks -- perhaps by referring to one master block that contains pointers to all additional related netblocks. Doing so will tend to reduce the likelihood of blanket actions against larger covering prefixes. Provide contact details for each customer as part of documenting those assignments/allocations, too.

II. Passive DNS

What *Is* Passive DNS?

- Passive DNS uses empirically observed DNS queries, captured by sensors, as the basis for synthesizing DNS relationships and answering questions that regular DNS simply can't. E.G.:

  -- Passive DNS can tell us all the fully qualified domain names that have been seen under given base domain name
  -- Passive DNS can tell us all the domains that have been seen on a particular IP address, or in a particular IP address range
  -- Passive DNS can report all the domains that have been seen using a given authoritative name server

- These are useful things to know if you want to avoid shooting yourself in the foot when seizing domains or blocking IPs.

Defensive Use of Passive DNS

- Passive DNS is normally used by investigators to enhance existing threat intel -- such as a known-bad domain name, an abused IP address, or a suspicious name server.

- Today, we're talking about using Passive DNS defensively, to ensure that an intentional takedown won't result in collateral damage.

- As a result, Passive DNS is used to watch out for unexpected pockets of goodness, e.g. innocent 3rd-party domains, etc.

Remember to "Time Fence"

- When you use passive DNS, you're querying a database. That database may go back for **many years** – for example, Farsight's DNSDB goes back to June 2010.
- However, sites that tend to matter (from a collateral damage perspective) will normally be seen by passive DNS sensors within the last **month**, or at least within the past **ninety days.**
- You typically won't want to go back further than that for collateral damage-avoidance purposes
- When you're using passive DNS for defensive purposes, your focus really needs to be on what's there **now**, or at least what's been seen in the **immediate past**. Looking too-far back may result in false positives (e.g., if a block formerly used by a good customer has bee repurposed for use by a bad one).

Passive DNS: Facts, Not Opinions

- Passive DNS gives you just the facts -- not opinions about reputation.

- It tells you what domains or IPs or name servers were seen, it doesn't tell you if they were associated with spam, or phishing, or malware, for example.

- If you need reputation data about domains that passive DNS has found, you should check with a domain reputation source.

- Examples of particularly-highly trusted sources of domain reputation data include Spamhaus and SURBL. A quick way to manually check both is via http://multirbl.valli.org/

III. Using Passive DNS to Avoid Takedowns

Example scenario

- Starting point: www.potenzmittelapotheke24[dot]de
- You may have seen this domain in email; if not, it is shown on numerous pages in less-filtered search engines such as Bing.
- Status?

  The base domain is listed by both the Spamhaus DBL and by SURBL.

Note: references to domains in this section have been intentionally "munged" by selectively replacing a dot with [dot] for the purpose of these slides

Where Does The FQDN Currently Live?

- 'A' records for www.potenzmittelapotheke24[dot]de (from dig):

  172.245.83.110
  216.170.114.3

- Reputation for those two IPs? At the time this was written:

  http://www.spamhaus.org/sbl/query/SBL262391 has 172.245.83.110 listed
  http://www.spamhaus.org/sbl/query/SBL262392 has 216.170.114.3 listed

- Nonetheless, what do we see from passive DNS for those IPs?

Checking One of The IPs

$ **dnsdb_query.py --after=2015-6-18 -i 216.170.114.3 | sort | uniq**

dns1.dnsite.in[dot]net. IN A 216.170.114.3
dns2.dnsite.in[dot]net. IN A 216.170.114.3
ns1.endorsquall[dot]com. IN A 216.170.114.3
potenzmittelapotheke24[dot]de. IN A 216.170.114.3
www.potenzmittelapotheke24[dot]de. IN A 216.170.114.3

Not very many FQDNs, and just three base domains were seen on that IP in our one month period: dnsite.in[dot]net, endorsquall[dot]com and potenzmittelapotheke24[dot]de.

We'll check the other IP, too.

Checking The Other IP

$ **dnsdb_query.py --after=2015-6-18 -i 172.245.83.110 **
| sort | uniq

dns2.dnsite.in.net. IN A 172.245.83.110
potenzmittelapotheke24.de. IN A 172.245.83.110
www.potenzmittelapotheke24.de. IN A 172.245.83.110

Nothing new there...

Is This Host "Stable" in its Hosting?

- That is, if we look back in time, what IPs have we seen www.potenzmittelapotheke24[dot]de hosted on?

  Has it lived on the same IP's "forever?"

  Or has it been moving around, hopping from one IP to another?

It Has Moved Around

;; count: 121
;; first seen: **2015-04-12** 18:32:41 -0000
;; last seen: **2015-05-15** 23:48:40 -0000
www.potenzmittelapotheke24[dot]de.
IN A **5.149.254.93**

;; count: 6
;; first seen: **2015-04-27** 02:28:58 -0000
;; last seen: **2015-04-27** 02:28:58 -0000
www.potenzmittelapotheke24[dot]de.
IN A 37.1.200.98

;; count: 558
;; first seen: **2015-04-28** 05:37:32 -0000
;; last seen: **2015-05-08** 03:46:50 -0000
www.potenzmittelapotheke24[dot]de.
IN A 37.1.204.6

;; count: 1,037
;; first seen: **2015-05-15** 23:48:39 -0000
;; last seen: **2015-05-20** 17:10:44 -0000
www.potenzmittelapotheke24[dot]de.
IN A **104.18.32.125**
www.potenzmittelapotheke24[dot]de.
IN A **104.18.33.125**

;; count: 159
;; first seen: **2015-05-18** 04:57:29 -0000
;; last seen: **2015-05-18** 21:17:07 -0000
www.potenzmittelapotheke24[dot]de.
IN A **75.127.9.148**

[etc]

Are There Other Hostnames Under That Base Domain Name?

- If we check *.potenzmittelapotheke24[dot]de do we find a lot of hostnames besides just the base domain name, its name servers, and maybe www.potenzmittelapotheke24.de?

- $ **dnsdb_query.py -r *.potenzmittelapotheke24[dot]de --json | jq .rrname --raw-output | sort | uniq**
  [one other potentially tagged hostname omitted here]
  mail.potenzmittelapotheke24[dot]de.
  ns1.potenzmittelapotheke24[dot]de.
  ns2.potenzmittelapotheke24[dot]de.
  potenzmittelapotheke24[dot]de.
  www.potenzmittelapotheke24[dot]de.

- That's not very many unique hostnames. Again, very reassuring.

What About The Name Servers?

- What name servers does www.potenzmittelapotheke24[dot]de use?

  Checking with dig, we see our domain of interest uses two name servers:

  dns1.dnsite.in[dot]net.
  dns2.dnsite.in[dot]net.

  What do we see from passive DNS for those name servers?

Checking dns1

$ **dnsdb_query -n dns1.dnsite.in[dot]net**

;; record times: **2015-07-03** 10:15:29 .. **2015-07-19** 21:11:30

;; count: 130698

potenzmittelapotheke24[dot]de. NS dns1.dnsite.in[dot]net.

;; record times: 2015-07-04 00:26:23 .. 2015-07-10 13:45:24
;; count: 378
gesundeliebe[dot]de. NS dns1.dnsite.in[dot]net. *[listed on Spamhaus DBL and SURBL]*

;; record times: 2015-07-09 21:02:03 .. 2015-07-10 23:30:26
;; count: 74
mailrusecuritystop[dot]ru. NS dns1.dnsite.in[dot]net. *[ditto]*

;; record times: 2015-07-09 22:43:05 .. 2015-07-11 00:48:31
;; count: 56
yandexrusecuritystop[dot]ru. NS dns1.dnsite.in[dot]net. *[ditto]*
[plus one additional domain]

Checking dns2

$ **dnsdb_query -n dns2.dnsite.in[dot]net**

;; record times: **2015-07-03** 10:15:29 .. **2015-07-19** 18:29:06

;; count: 130698

potenzmittelapotheke24[dot]de. NS dns2.dnsite.in[dot]net.

;; record times: 2015-07-04 00:26:23 .. 2015-07-10 13:45:24
;; count: 378
gesundeliebe[dot]de. NS dns2.dnsite.in[dot]net. *[listed on Spamhaus DBL and SURBL]*

;; record times: 2015-07-09 21:02:03 .. 2015-07-10 23:30:26
;; count: 74
mailrusecuritystop[dot]ru. NS dns2.dnsite.in[dot]net.
[ditto]
;; record times: 2015-07-09 22:43:05 .. 2015-07-11 00:48:31
;; count: 56
yandexrusecuritystop[dot]ru. NS dns2.dnsite.in[dot]net. *[ditto]*
[plus one additional domain]

Checking ns1.endorsquall[dot]com

We saw one other name server mentioned on one of our IPs of interest... what about it?

$ **dnsdb_query -n ns1.endorsquall[dot]com**
;; **zone** times: 2014-07-19 16:14:48 .. **2015-07-18** 16:15:24
;; count: 361 *[still in the zone ^^^]*
endorsquall.com. NS ns1.endorsquall.com.

;; **record** times: 2014-07-19 04:02:26 .. **2015-06-20** 13:14:37
;; count: 24195 *[but almost a month ^^^ since last seen used]*
endorsquall.com. NS ns1.endorsquall.com.
[one other record, an SOA record, omitted here]

This NS is only used by one domain, e.g., itself. Not a blocker, either.

Whew…

- Most LEOs or other investigators contemplating action against the initial domain would likely take some comfort from...

  -- Having checked the FQDN and the IPs that it is currently using
  -- Having checked historical FQDN→IP mappings, and seeing the domain hopping around from one IP to another frequently
  -- Minimal set of hostnames under the base domain
  -- Having checked the hosts associated with the name servers and seen nothing significant there, either

- That's a lot different than just deciding to "take a chance" and "go for it." Checking passive DNS is how the pros protect the general public, and themselves, from online minefields.

IV. "Paul! I'm Not a LEO or Cybercrime Investigator. Why Does This Matter To Me?"

Know Your (Online) Neighbors

- Even if you're not an LEO or non-law enforcement investigator, passive DNS can still help protect you from collateral damage.

- For instance, average individuals with web sites may want to make an effort to "know their neighbors," checking to see who else may be sharing their IP addresses, their name servers, etc.

- If it turns out you're living in a sort of bad online neighborhood, you may want to consider potentially voting with your pocketbook, moving to a safe(r) neighborhood where you're less likely to be a potential victim of collateral damage.

- Just thinking about setting up a site? You might want to check BEFORE you sign up, thus avoiding the need for a later move...

If You're A Service Provider...

- You now know that current and prospective customers may be looking at who's located on a given IP, or a given name server.
- As a result, you may decide that you should more carefully screen incoming customers, or perhaps periodically review existing customers, to avoid *prima facie* questionable customers
- If you aren't quite ready to do that, you may at least decide to tier customer assignments, with rock-solid blue-chip security-conscious companies in one zone, and less well-self-regulated customers in a completely different higher-risk zone (naturally, price points might be different for the two zones, too).
- If even that's too much, you might at least want to limit the level of aggregation you allow to develop. For example, you might put no more than 25,000 domains on any individual name server or IP address, avoiding an "all eggs in one basket"-type scenario.

TBTTD?

- Providers could, ironically, also consider going the exact opposite direction, intentionally putting EVERYTHING on a couple name servers, thereby seeking to become "Too Big To Take Down (TBTTD)."

- That *might*... "work."

- Then again, it might attract exactly the sort of customers you DON'T want, and scare away the sort you DO want.

V. Consider Contributing Passive DNS Data

Why Bother Contributing pDNS Data?

- The quality of any passive DNS database is only as good as the data it receives. If you're a major service provider running large recursive resolvers and you're NOT contributing data to passive DNS databases, you run the risk of being underrepresented.
- If that happens, authorities may end up checking passive DNS in good faith, seeing what appears to be a "clear lane" for action, and then — in spite of checking — having a nasty surprise.
- It is worth your time to help instrument the Internet so that the online equivalent of "hospitals," "orphanages," and "museums" can be clearly seen and avoided when the authorities do whatever the authorities feel they need to do.
- Consider contributing passive DNS data to SOME passive DNS project, Farsight's or someone else's.

What About Customer Privacy?

- Any time we talk about passive monitoring of Internet traffic, the issue of end-user privacy must be considered. At Farsight, we take enduser privacy very seriously.

- I can't speak for all passive DNS efforts, but at least in Farsight's case, we intentionally collect passive DNS **above recursive resolvers** specifically in order to **avoid collecting PII.**

- This means that the queries and responses that our collectors gather all appear to come from the recursive resolver, which is typically shared by tens of thousands of users or more, rather than from any individually attributable user.

- Contribute data **and** protect the privacy your customers, too,

VI. Summary

1) Civil investigators and LEOs should balance the desire to act decisively against cyber criminals with the need to avoid doing collateral damage to innocent third parties.
2) You've learned what Passive DNS is, have seen how it works, and know it can be effectively used to assess potential takedown targets for collateral damage considerations. You also know scenarios having a high risk of collateral damage.
3) You've been reminded that collateral damage is a real thing that has occurred in the past, and at daunting scale, and you know what that potentially implies for you & your customers.
4) Finally, I also hope that you are motivated to consider contributing passive DNS data, thereby improving the quality of passive DNS data for everyone, and reducing the likelihood that collateral damage will occur in the future.

Thank you!

For more information:

- *Passive DNS for Threat Intelligence Whitepaper*: Contact sales@farsightsecurity.com
- Farsight Blog https://www.farsightsecurity.com/Blog/
- Dr. Paul Vixie: vixie@fsi.io

FARSIGHT SECURITY