TURNING DNS FROM SECURITY TARGET TO SECURITY TOOL

Cricket Liu

Chief DNS Architect
Infoblox
@cricketondns
DNS is Complicit in All Kinds of Malicious Activity
Most Malware Uses DNS in Attacks

- 91.30% Uses DNS
- 8.70% Who knows--host tables?
Most Organizations Don’t Monitor DNS

- You betcha!
- I would prefer not to know
How DNS Is (Ab)Used

- Bad guys register brand-new domain name
  - With no negative reputation
- Bad guys mount phishing campaign, luring the unsuspecting to a website using the new domain name
  - Visitors are infected through a variety of means
Malware wakes on the corporate network, inside the firewall

The malware wants to communicate with a command-and-control (C&C) server

It rendezvous with a C&C server by looking up
- A compiled-in list of domain names
- Domain names generated by a Domain Generation Algorithm (DGA)

...until it gets an answer
How DNS Is (Ab)Used: Tunneling

- But most corporate networks no longer permit direct communication from arbitrary internal hosts to the Internet.
  - Many require that common protocols (e.g., HTTP, HTTP-S) run through proxies.
- So many species of malware fall back to using DNS to tunnel communication to and from C&C servers.
DNS Tunneling

- Tunneling data surreptitiously into or out of a network using DNS as a vector
  - This is often effective because
    - DNS is generally allowed into and out of an organization (e.g., you can look up Internet domain names from inside the network)
    - DNS queries and responses are usually poorly monitored
  - Can be used
    - As a command and control channel for a botnet
    - To download new code to existing malware
    - To exfiltrate data from the internal network to a drop server
DNS Tunneling Example: Infiltration

S: [infected host] Q: 0.[id].hacker.org/TXT ?
D: [infected host] A: 0.[id].hacker.org TXT “0.[base-64-encoded data]”
0.[id].hacker.org TXT “1.[base-64-encoded data]”
...
DNS Tunneling Example: Exfiltration

S: [infected host] Q: 0.[base-32-encoded data].[id].hacker.org/A ?
D: [infected host] A: NXDOMAIN
S: [infected host] Q: 1.[base-32-encoded data].[id].hacker.org/A ?
D: [infected host] A: NXDOMAIN
Enough!

- Through all of the abuse, DNS servers have been blindly complicit
- DNS security has traditionally concentrated on
  - Securing DNS transactions (queries, updates, zone transfers)
  - Protecting the authenticity and integrity of zone data (e.g., DNSSEC)
- Finally, after nearly three decades of this, we’d had enough
Actual Photograph of Paul Publishing His Blog
Enter Response Policy Zones

- In 2010, Paul Vixie writes “Taking Back the DNS,” introducing Response Policy Zones, or RPZs

- RPZs reuse
  - DNS zones as containers for resolution policy
  - DNS records as a mechanism for expressing policy

- Policies can
  - Trigger based on domain name in a query or an answer
  - Trigger based on an IP address in an answer
  - Return errors or static data in place of answers
RPZ “Feeds”

- Since RPZs are zones, you can distribute RPZ policies quickly and efficiently
  - “Subscribers” configure their DNS servers as secondaries for RPZ zones
    - Transferring those zones from “publishers”
  - Publishers can send NOTIFY messages when policies change
  - Subscribers can request IXFRs to get just the changes

- Organizations traditionally in the DNS blocklist business now make their reputational data available via RPZ because it’s efficient and easy to consume
How Response Policy Zones Work

Infected client

Local recursive name server

Query for malicious domain name

Error or redirect

RPZ data via zone transfer

Log

Master name server (run by RPZ feed provider)
Enter Passive DNS

- Invented by Florian Weimer in 2004
- Essentially "DNS telemetry"
  - A record of responses seen by recursive DNS servers and a timestamp
    - Referrals
    - Answers
    - Errors
Passive DNS

Root name servers -> com name servers -> example.com name servers

Recursive name server

Passive DNS database

pDNS replication
Passive DNS Databases

- Databases of collected passive DNS data are invaluable for detecting malicious or suspicious activity
  - Fast fluxing
  - Domain Generation Algorithms
  - DNS tunneling
  - Cache poisoning
  - Unauthorized access to cloud services
  - ...and much more
Closing the Loop

Analytics Cloud

RPZ

Passive DNS replication

Customer 1

Customer 2

... Customer 9000
Case Study: Farsight’s NOD Feed

- Farsight Security uses their passive DNS database to create an RPZ of domain names “newly observed” on the Internet
  - Say less than 30 minutes old

- Turns out an enormous percentage of brand-new domain names are malicious
  - Registered, used for malicious activity (e.g., a phishing campaign) and then discarded

- Blocking access to them will thwart much badness

- And the opportunity cost is minimal
How to Apply What You’ve Learned Today

- Check whether your DNS servers already support Response Policy Zones
  - If not, consider making RPZ support a requirement when you upgrade your DNS servers

- Determine whether one or more RPZs might be useful to you

- Plumb these RPZs into your DNS servers and send RPZ logs to your SIEM

- Think about collecting your passive DNS data and mining it