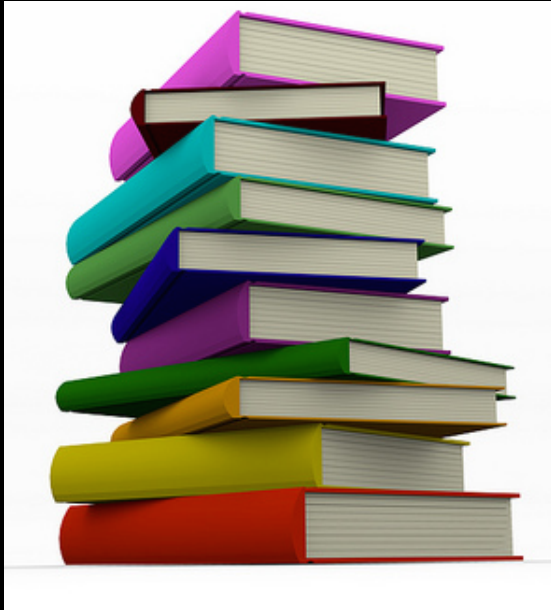


DNS Traffic Monitoring

Dave Piscitello

VP Security and ICT Coordination,
ICANN

Domain Names



*ICANN coordinates
the administration
of global
identifier systems*

Domain names provide user friendly identification of hosts

- Latin script (A-Z, 0-9, hyphen)
e.g., **www.google.it**
- *Internationalized Domain Names* accommodate non-Latin languages or scripts
e.g., **водка.рф**

What can I do with a domain name?

An engineer's answer

- Assign user friendly names to a computer (server) that hosts *Internet applications*:
- Web, blog, file server, email, IP telephony

A businessman's answer

- Create a merchant or other commercial online presence
- Join a commodities market: buy, sell, auction domain names
- Run a commercial service

A government official's answer

- Provide services for public interest

A criminal's answer

- Misuse, exploit or disrupt public or business services

Criminal or Malicious Domain Registrations

Domains registered by criminals for

- Counterfeit goods
- Data exfiltration
- Exploit attacks
- Illegal pharma
- Infrastructure (crime name resolution)
- Malware C&C
- Malware distribution (drive-by pages)
- Phishing
- Scams (419, reshipping, stranded traveler...)



Criminal Abuse of Legitimate Domains

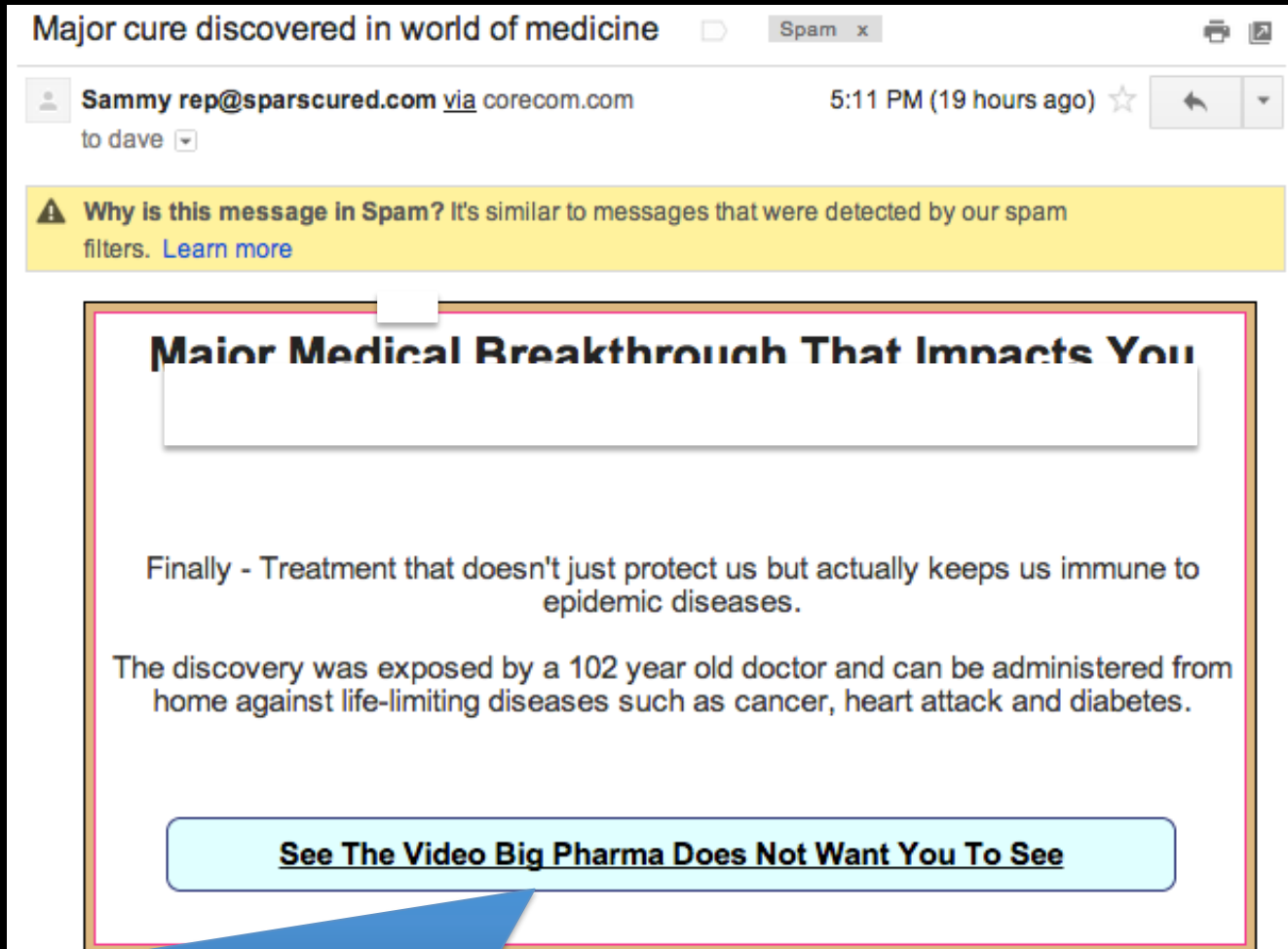


Domains compromised or hijacked by criminals or state-sponsored actors

- Host criminal DNS infrastructure
- Domain, NS, or MX Hijacking
- Hacktivism (e.g., defacement)
- Tunneling (covert communications)
- Attack obfuscation
- Host file modification (infected devices)
- Changing default resolvers (DNSChanger)
- Poisoning (resolver/ISP)
- Man in the Middle attacks (insertion, capture)

Modern malware use domain names and DNS

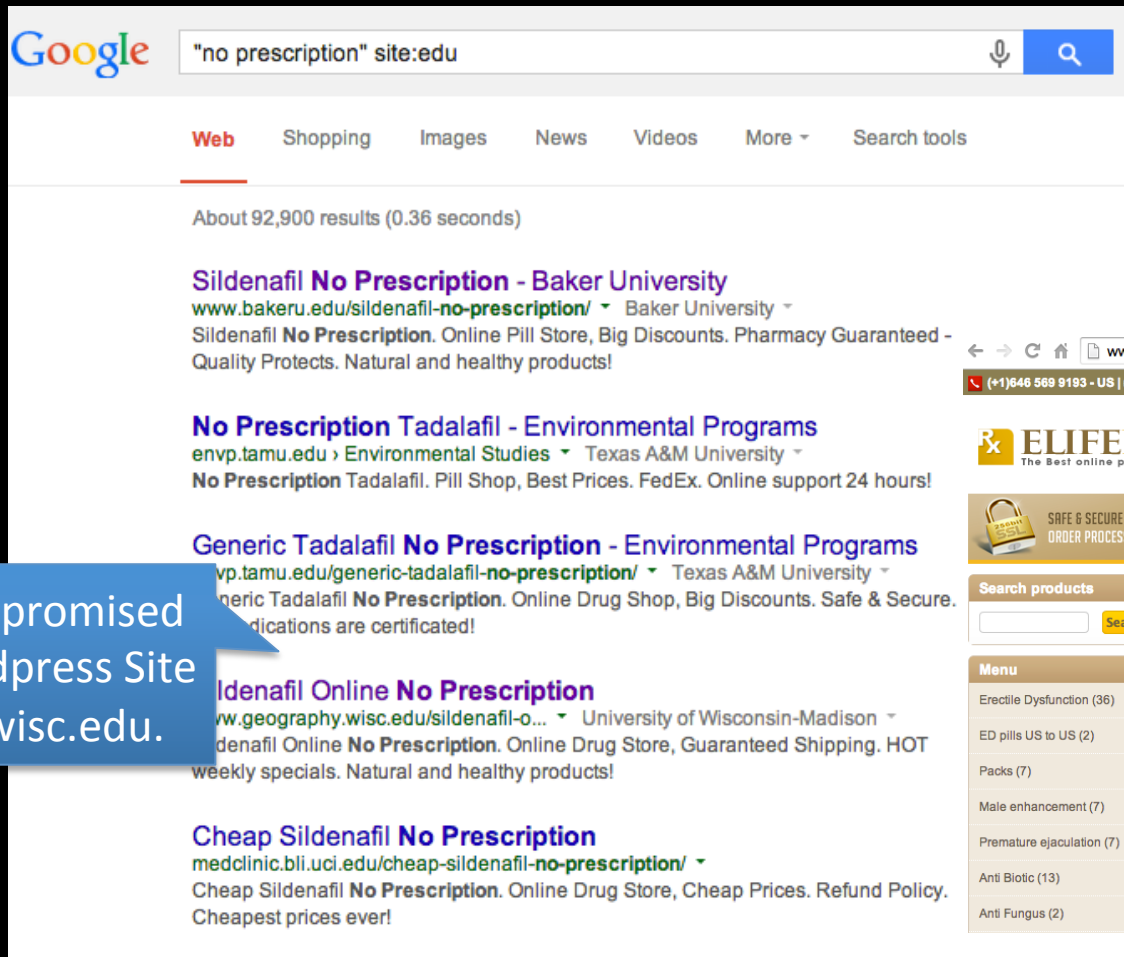
Maliciously registered domains are common in spam, phishing URLs



hxxp://grill.s[redacted]scured.com/cure17213154296cr-t2123501true612246174

Malware also abuse legitimate domain names

Compromised web sites often redirect to criminal domains



Redirects to
www.rx-elife.com/



Advanced uses of Domains and DNS

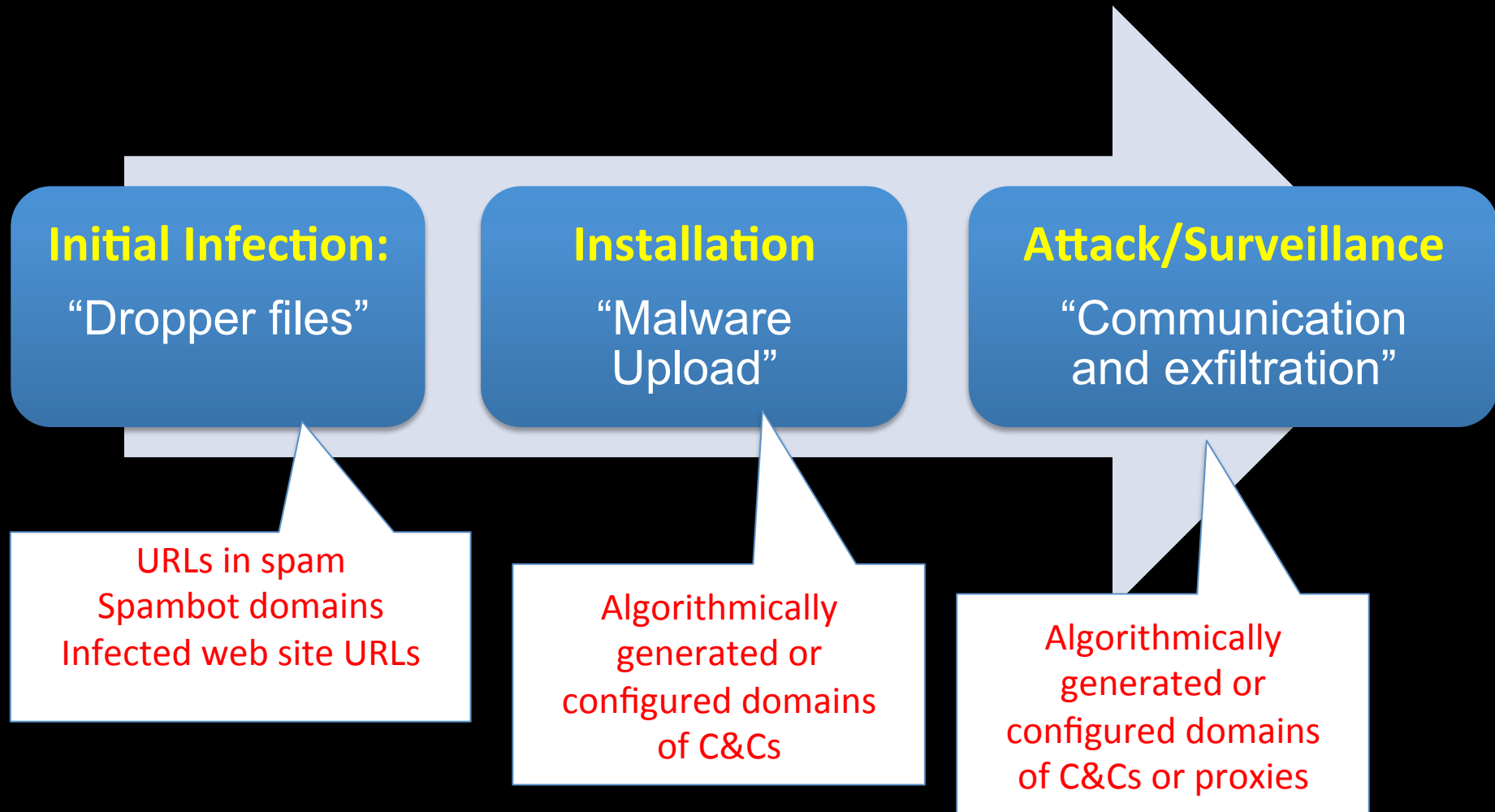
Criminals register domains to identify

- botnet command and control hosts
- proxies for fast flux or MITM hosts
- name servers of malicious domains

Over the course of the malware's life cycle...

Tens, hundreds, sometimes, thousands *per day*...

DNS is used by malware at different times for different purposes



But...DNS is a public directory service

Fundamental characteristics of DNS information

- You cannot copyright it: it's meant to be copied
- If you keep it confidential no one can find you
- DNS data are mostly temporal
 - Names are registered not owned
 - Addresses are registered or allocated not owned
 - DNS data and even some addresses have *lifetimes*
- You can't prevent others from collecting it
- Criminals can't stop us from monitoring the DNS

What are you looking for? Why?

DNS QUERY TRAFFIC	SYMPTOM OF
Spoofed source addresses Unauthorized source addresses Queries that use TCP High query volume	DDOS
Malformed queries or queries with suspicious composition	Vulnerability Exploitation Attack or incorrectly operating device
Queries to suspicious or unauthorized resolvers	C&C communications/exfiltration

What are you looking for? Why?

DNS RESPONSE TRAFFIC	SYMPTOM OF
Suspicious length, especially in association with high volume	DDOS Amplification
Suspicious composition	
Incorrect responses for your domains	Cache poisoning, Covert channel
Short TTLs	Domain account hijacking, DNS response modification
High Name Error volume	Possible fast flux indicator
DNS on non-standard, unauthorized ports	Infected hosts cannot reach C&Cs C&C communications, exfiltration

DNS misuse leaves a trail

- Certain malware change host configurations or resolver data
 - DNSChanger malware
 - Compromised broadband routers/modems
 - Cache poisoners
- You can track others by examining network traffic



<https://www.flickr.com/photos/reway2007/>

Where to look

- Host (device) or resolver configuration
- DNS query and response traffic on networks
- Resolver and authority logs
- Event logs
 - Hosts, Security Systems, Network elements
 - Applications (clients or servers)
- Passive DNS replication (sensor networks)

How to Look (Packet Capture)

- Traffic analyzers

- Create/borrow DNS filters for PCAP files generated using Wireshark or other packet capture software

<http://ask.wireshark.org/questions/7914/how-to-identify-any-rogue-dns-requests-using-wireshark>

- Intrusion Detection Systems

- DNS rules for snort, suricata, Bro

<http://blog.kaffenews.com/2010/03/04/detecting-malware-infections-with-snort-dns-monitoring/>







<http://www.bro.org/search.html?q=dns>

How to Look (Firewalls)

Create Internet firewall rules for

- Antispoofing
- Egress traffic filtering
- Allow DNS to authorized resolvers, deny all other

Enable logging, event notifications

	Source	Destination	Service	Interface	Direction	Action	Time	Options
0	 linux-static  net-192.168.1.0	Any	Any	 eth0	 Inbound	 Deny	Any	

www.fwbuilder.org/4.0/docs/users_guide5/anti-spoofing-rules.shtml

→ Firewall Best Practices - Egress Traffic Filtering

Too many network administrators think only to protect private network resources from external attacks when assessing security threats. Today's landscape is littered with threats that emanate from malware-infected endpoints. Attackers can use these to collect and forward sensitive information from your network, to attack or spam other networks. Companies large and small are better served when network administrators are equally concerned with threats that are associated with outbound connections. In this column, I discuss ways organizations can improve their risk profile and be better 'netizens by implementing *egress traffic filtering*.

Filter Egress Traffic to Protect Yourself

If you don't restrict the services that hosts in your internal networks can access, malware that will inevitably find its way onto some of your hosts may exfiltrate data to a location that an attacker controls. Data exfiltration could be unintentional, i.e., an insider might incorrectly attach sensitive information an email message to upload it to a document sharing service. Exfiltration can result from configuration error: NetBIOS, DNS, or other service traffic that leaks from your trusted networks may be captured or exploited by external parties. Exfiltration can also be malicious, the result of hosts having been infected with an advanced persistent threat (APT).

Irrespective of the cause, data exfiltration is a threat you can't mitigate without egress traffic enforcement, and one you can't readily detect if you don't log and monitor traffic behavior associated with permitted and prohibited services.

Filter Egress Traffic to Do No Harm to Others

In the most lax of configurations – and sadly, in many default configurations – a firewall or router may treat as valid and forward traffic it receives from any source address. Fred Avolio calls this "The Nefarious Any". Such configurations are green fields for attacks that leverage forged source IP addresses (IP spoofing). Compromised or unauthorized hosts that gain access to your local networks often use IP spoofing to attack (DDoS) other networks, to store child abuse or other illegal material, or to conduct spam or phishing campaigns. This is problem enough in NAT environments: in poorly implemented router configurations, especially where you have multiple access points to the Internet, your organization can inadvertently behave as a transit network for forged, malicious traffic emanating from other organizations.

securityskeptic.com/the-security-skeptic/firewall-best-practices-egress-traffic-filtering.html

How to Look (IPS)

NextGen firewall/IPS features

- Sonicwall, Palo Alto, Checkpoint, cisco, others

The screenshot displays the SonicWALL Network Security Appliance configuration interface. The top navigation bar includes the SonicWALL logo, the text "Network Security Appliance", and links for "Wizards", "Help", and "Logout". The main content area is titled "Mode: Configuration" and shows a list of IPS rules. A red box highlights the left sidebar menu items 37 through 43, which correspond to the rules listed in the main table.

Rule ID	Rule Name	Port	Status	Severity	Direction	Action
33	Microsoft ISA Server DNS Spoofing (MS04-039)	4162	✓	Medium	Incoming	Block
34	Red Hat Enterprise Linux DNS Resolver Buffer Overflow	4069	✓	Medium	Incoming	Block
35	Squid DNS Lookup DoS 1	4048	✓	Medium	Incoming	Block
36	Squid DNS Lookup DoS 2	4049	✓	Medium	Incoming	Block
37	Squid DNS Replies Memory Corruption 1	3012	✓	Medium	Incoming	Block
38	Squid DNS Replies Memory Corruption 2	3013	✓	Medium	Incoming	Block
39	Suspicious DNS Traffic 1	1054	✓	Medium	Incoming	Block
40	Suspicious DNS Traffic 2	1810	✓	Medium	Incoming, to Server	Block
41	Suspicious DNS Traffic 3	7931	✓	Medium	Incoming	Block
42	Suspicious DNS Traffic 4	7932	✓	Medium	Incoming	Block
43	Suspicious DNS Traffic 5	9208	✓	Medium	Incoming, to Client	Block
44	Suspicious DNS Traffic 6	8182	✓	Medium	Incoming	Block
45	Symantec Enterprise Firewall DNS Proxy Cache Poisoning 1	4372	✓	Medium	Incoming	Block
46	Symantec Enterprise Firewall DNS Proxy Cache Poisoning 2	4373	✓	Medium	Incoming	Block
47	Symantec Norton IS DNS Component Buffer Overflow	4094	✓	High	Incoming	Block
48	Windows DNS Client Buffer Overflow 1 (MS06-041)	4511	✓	Medium	Incoming	Block
49	Windows DNS Client Buffer Overflow 2 (MS06-041)	7717	✓	Medium	Incoming, to Client	Block
50	Windows DNS Server NAPTR Query Remote Code Execution 1 (MS11-058)	1371	✓	Medium	Incoming	Block

How to look (name service)

- **DNS log analysis**
 - Analyze log data from your resolvers, authoritatives
<http://www.irongeek.com/i.php?page=videos/derbycon3/s114-another-log-to-analyze-utilizing-dns-to-discover-malware-in-your-network-nathan-magniez>
- **Add Response Policy Zones to your resolver**
 - Add zone file with known malicious domains to BIND
<https://sites.google.com/site/thingsoflittleconsequence/home/using-domain-name-service-response-policy-zones-dns-rpz-with-shallalists>
- **Passive DNS**
 - Inter-server DNS traffic captured at sensors, forwarded to collector, then analyzed
http://www.bfk.de/bfk_dnslogger.html
<https://www.dnsdb.info/>

How to Look (Commercial Grade)

- **DNS Monitoring plugins for SIEM, IT infrastructure**
 - vFabric Hyperic 4.6, Nagios, ManageEngine (lots of variations among these services)
- **DNS Monitoring services**
 - Threat intelligence + DNS (Application) Firewall Infoblox, Internet Identity, A10 Networks, others...
- **Threat intelligence platforms**
 - Cybertoolbelt, Maltego, ThreatConnect, others...

Final Comments

- DNS is essential to users
 - and to criminals as well
- Observing DNS traffic is a good way to monitor network activities
 - There are lots of ways to do this for small budgets or large
- It's also a great way to identify malicious, or criminal activity

... So why are you still reading and listening?

further reading

- **Monitor your DNS and you may just find a RAT**
<http://www.darkreading.com/attacks-breaches/monitor-dns-traffic-and-you-just-might-catch-a-rat/a/d-id/1269593>
- **5 Ways to Monitor DNS Traffic**
<http://www.darkreading.com/analytics/threat-intelligence/5-ways-to-monitor-dns-traffic-for-security-threats/a/d-id/1315868>
- **The Security Skeptic**
<http://securityskeptic.com>