

DNS Traffic Monitoring

Dave Piscitello
VP Security, ICANN

Modern malware use domain names and DNS

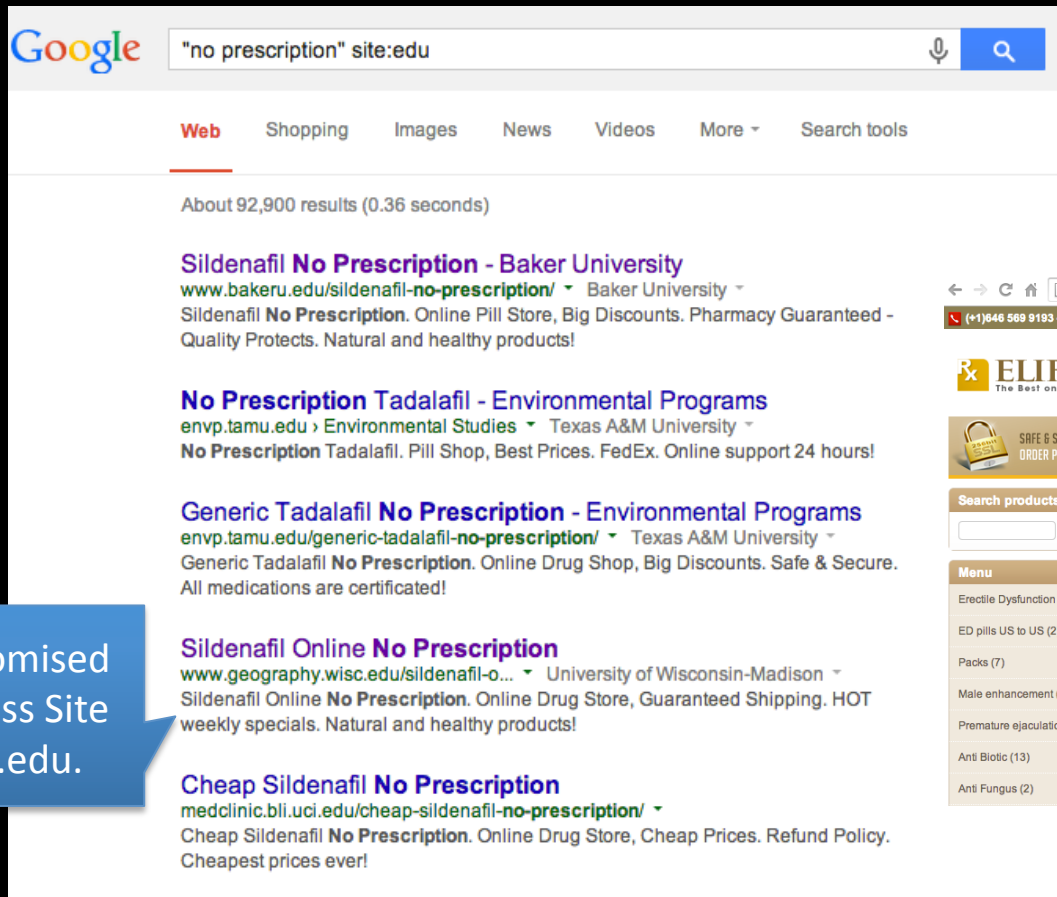
Malicious registrations in spam, phishing URLs



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

Modern malware use domain names and DNS

Compromised web sites or mail exchanges



A screenshot of a Google search results page. The search bar contains the text "no prescription" site:edu. The results show several links to university websites offering "No Prescription" versions of Sildenafil and Tadalafil. The links are from Baker University, Texas A&M University, and the University of Wisconsin-Madison. Each result includes a brief description of the service, such as "Online Pill Store, Big Discounts. Pharmacy Guaranteed - Quality Protects. Natural and healthy products!" and "Online Drug Store, Guaranteed Shipping. HOT weekly specials. Natural and healthy products!"

Sildenafil No Prescription - Baker University
www.bakeru.edu/sildenafil-no-prescription/ Baker University
Sildenafil **No Prescription**. Online Pill Store, Big Discounts. Pharmacy Guaranteed - Quality Protects. Natural and healthy products!

No Prescription Tadalafil - Environmental Programs
envp.tamu.edu Environmental Studies Texas A&M University
No Prescription Tadalafil. Pill Shop, Best Prices. FedEx. Online support 24 hours!

Generic Tadalafil No Prescription - Environmental Programs
envp.tamu.edu/generic-tadalafil-no-prescription/ Texas A&M University
Generic Tadalafil **No Prescription**. Online Drug Shop, Big Discounts. Safe & Secure. All medications are certified!

Sildenafil Online No Prescription
www.geography.wisc.edu/sildenafil-o... University of Wisconsin-Madison
Sildenafil Online **No Prescription**. Online Drug Store, Guaranteed Shipping. HOT weekly specials. Natural and healthy products!

Cheap Sildenafil No Prescription
medclinic.bli.uci.edu/cheap-sildenafil-no-prescription/
Cheap Sildenafil **No Prescription**. Online Drug Store, Cheap Prices. Refund Policy. Cheapest prices ever!

Compromised
WordPress Site
at wis.edu.

Redirects to
www.rx-elfe.com/



A screenshot of the ELIFERX website, which is a pharmacy. The website has a header with the ELIFERX logo and several award seals. Below the header, there are sections for "SAFE & SECURE ORDER PROCESSING", "DELIVERY GUARANTEED", "100% MONEY BACK GUARANTEE", and "HIGHEST QUALITY GENERIC DRUGS". The main content area features a search bar, a menu with categories like "Erectile Dysfunction (36)", "ED pills US to US (2)", "Packs (7)", "Male enhancement (7)", "Premature ejaculation (7)", "Anti Biotic (13)", and "Anti Fungus (2)", and a large advertisement for "Generic Viagra" featuring a couple embracing.

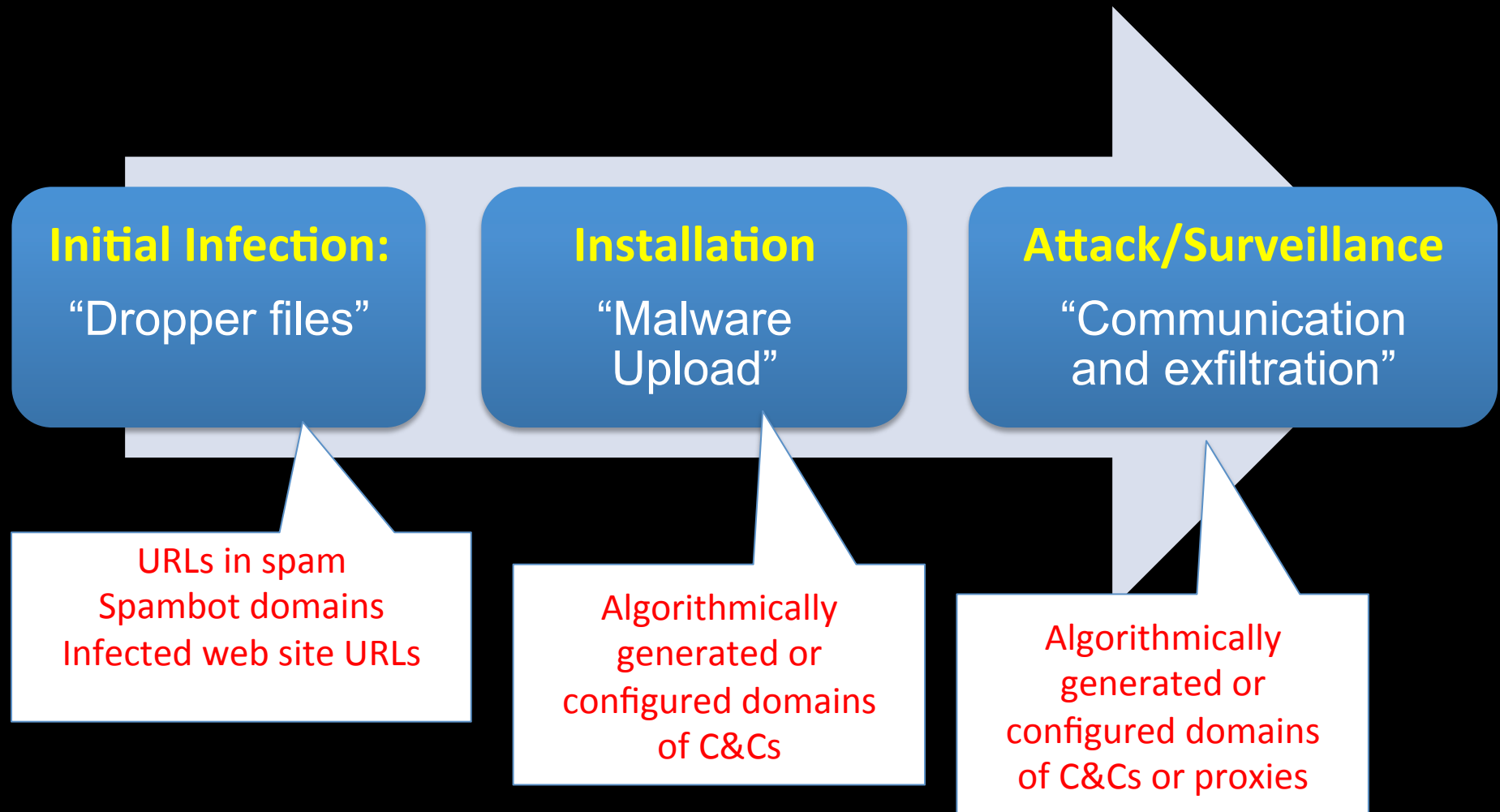
Modern malware use domain names and DNS

Other (advanced) uses: 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...

DNS is used by malware at different times for different purposes



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 | Cache poisoning, Covert channel |
| Incorrect responses for your domains | Domain account hijacking, DNS response modification |
| Short TTLs | Possible fast flux indicator |
| High Name Error volume | Infected hosts cannot reach C&Cs |
| DNS on non-standard, unauthorized ports | C&C communications, exfiltration |

DNS misuse leaves a trail

- Certain malware change host configuration 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
- Resolver and authority logs
- Event logs
 - Hosts, Security Systems, Network elements
 - Applications (clients or servers)
- Passive DNS

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-rogu-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 notification

→ 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

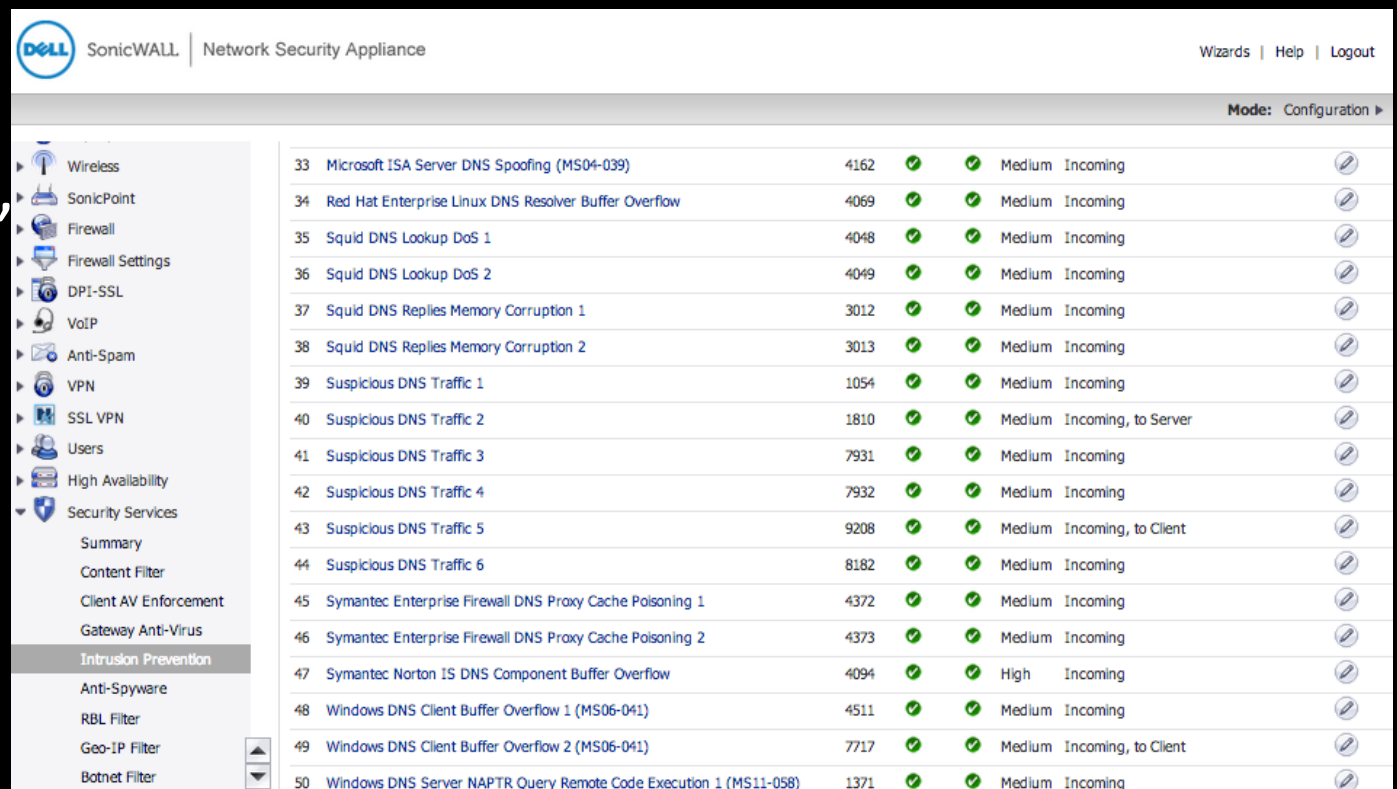
| | Source | Destination | Service | Interface | Direction | Action | Time | Options |
|---|---|-------------|---------|--|---|--|------|---|
| 0 |  linux-static  net-192.168.1.0 | Any | Any |  eth0 |  Inbound |  Deny | Any |  |

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

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 left sidebar shows the navigation menu with 'Intrusion Prevention' selected. The main area shows a list of 18 intrusion prevention rules, numbered 33 to 50. Each rule entry includes a rule number, a description, a port number, a status icon (green checkmark), a severity level, a direction, and an edit icon.

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

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

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...

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>