DNS Traffic Monitoring

Dave Piscitello
VP Security and ICT Coordination,
ICANN
Domain Names

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

ICANN coordinates the administration of global identifier systems
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 (ecrime name resolution)
- Malware C&C
- Malware distribution (drive-by pages)
- Phishing
- Scams (419, reshipping, stranded traveler...)

![Counterfeit goods example]

![Data exfiltration example]

![Exploit attacks example]

![Illegal pharma example]

![Infrastructure (ecrime name resolution) example]

![Malware C&C example]

![Malware distribution example]

![Phishing example]

![Scams example]
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

hxpx://grill.sparscured.com/cure17213154296cr-t2123501true612246174
Malware also abuse legitimate domain names

Compromised web sites often redirect to criminal domains

Compromised Wordpress Site at wisc.edu.

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

**Initial Infection:**
“Dropper files”

**Installation:**
“Malware Upload”

**Attack/Surveillance:**
“Communication and exfiltration”

- URLs in spam
  Spambot domains
  Infected web site URLs

- Algorithmically generated or configured domains of C&Cs

- Algorithmically generated or configured domains of C&Cs or proxies
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
<table>
<thead>
<tr>
<th>DNS QUERY TRAFFIC</th>
<th>SYMPTOM OF</th>
</tr>
</thead>
<tbody>
<tr>
<td>Spoofed source addresses</td>
<td>DDOS</td>
</tr>
<tr>
<td>Unauthorized source addresses</td>
<td></td>
</tr>
<tr>
<td>Queries that use TCP</td>
<td></td>
</tr>
<tr>
<td>High query volume</td>
<td></td>
</tr>
<tr>
<td>Malformed queries or queries with suspicious composition</td>
<td>Vulnerability Exploitation Attack or incorrectly operating device</td>
</tr>
<tr>
<td>Queries to suspicious or unauthorized resolvers</td>
<td>C&amp;C communications/exfiltration</td>
</tr>
<tr>
<td>DNS RESPONSE TRAFFIC</td>
<td>SYMPTOM OF</td>
</tr>
<tr>
<td>-----------------------------------------------------------</td>
<td>------------------------------------------------</td>
</tr>
<tr>
<td>Suspicious length, especially in association with high volume</td>
<td>DDOS Amplification</td>
</tr>
<tr>
<td>Suspicious composition</td>
<td>Cache poisoning, Covert channel</td>
</tr>
<tr>
<td>Incorrect responses for your domains</td>
<td>Domain account hijacking, DNS response modification</td>
</tr>
<tr>
<td>Short TTLs</td>
<td>Possible fast flux indicator</td>
</tr>
<tr>
<td>High Name Error volume</td>
<td>Infected hosts cannot reach C&amp;Cs</td>
</tr>
<tr>
<td>DNS on non-standard, unauthorized ports</td>
<td>C&amp;C communications, exfiltration</td>
</tr>
</tbody>
</table>
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
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

• Intrusion Detection Systems
  – DNS rules for snort, suricata, Bro
    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

<table>
<thead>
<tr>
<th>Source</th>
<th>Destination</th>
<th>Service</th>
<th>Interface</th>
<th>Direction</th>
<th>Action</th>
<th>Time</th>
<th>Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>linux-static</td>
<td>Any</td>
<td>Any</td>
<td>eth0</td>
<td>Inbound</td>
<td>Deny</td>
<td>Any</td>
<td></td>
</tr>
<tr>
<td>net-192.168.1.0</td>
<td>Any</td>
<td>Any</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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

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

![Screen Shot](image_url)

<table>
<thead>
<tr>
<th>Number</th>
<th>Vulnerability Description</th>
<th>Value</th>
<th>Risk Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>33</td>
<td>Microsoft ISA Server DNS Spoofing (MS04-020)</td>
<td>4152</td>
<td>Medium</td>
</tr>
<tr>
<td>34</td>
<td>Red Hat Enterprise Linux DNS Resolver Buffer Overflow</td>
<td>4039</td>
<td>Medium</td>
</tr>
<tr>
<td>35</td>
<td>Squid DNS Lookup Dos 1</td>
<td>4048</td>
<td>Medium</td>
</tr>
<tr>
<td>36</td>
<td>Squid DNS Lookup Dos 2</td>
<td>4049</td>
<td>Medium</td>
</tr>
<tr>
<td>37</td>
<td>Squid DNS Replies Memory Corruption 1</td>
<td>3012</td>
<td>Medium</td>
</tr>
<tr>
<td>38</td>
<td>Squid DNS Replies Memory Corruption 2</td>
<td>3013</td>
<td>Medium</td>
</tr>
<tr>
<td>39</td>
<td>Suspicious DNS Traffic 1</td>
<td>1064</td>
<td>Medium</td>
</tr>
<tr>
<td>40</td>
<td>Suspicious DNS Traffic 2</td>
<td>1810</td>
<td>Medium</td>
</tr>
<tr>
<td>41</td>
<td>Suspicious DNS Traffic 3</td>
<td>7911</td>
<td>Medium</td>
</tr>
<tr>
<td>42</td>
<td>Suspicious DNS Traffic 4</td>
<td>7032</td>
<td>Medium</td>
</tr>
<tr>
<td>43</td>
<td>Suspicious DNS Traffic 5</td>
<td>9208</td>
<td>Medium</td>
</tr>
<tr>
<td>44</td>
<td>Suspicious DNS Traffic 6</td>
<td>6132</td>
<td>Medium</td>
</tr>
<tr>
<td>45</td>
<td>Symanec Enterprise Firewall DNS Proxy Cache Poisoning 1</td>
<td>4097</td>
<td>Medium</td>
</tr>
<tr>
<td>46</td>
<td>Symanec Enterprise Firewall DNS Proxy Cache Poisoning 2</td>
<td>4373</td>
<td>Medium</td>
</tr>
<tr>
<td>47</td>
<td>Symanec Norton 15 DNS Component Buffer Overflow</td>
<td>4094</td>
<td>High</td>
</tr>
<tr>
<td>48</td>
<td>Windows DNS Client Buffer Overflow 1 (MS06-041)</td>
<td>4511</td>
<td>Medium</td>
</tr>
<tr>
<td>49</td>
<td>Windows DNS Client Buffer Overflow 2 (MS06-042)</td>
<td>7717</td>
<td>Medium</td>
</tr>
<tr>
<td>50</td>
<td>Windows DNS Server NAPTR Query Remote Code Execution 1 (MS11-058)</td>
<td>1371</td>
<td>Medium</td>
</tr>
</tbody>
</table>
How to look (name service)

• DNS log analysis
  – Analyze log data from your resolvers, authoritatives

• Add Response Policy Zones to your resolver
  – Add zone file with known malicious domains to BIND

• 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

• 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