Surveying the DNS Threat Landscape
by Rod Rasmussen and Paul Vixie

Executive summary
Strong enterprise security in 2013 requires a multilayered Internet strategy that includes the monitoring of network behavior as well as solutions in software and hardware. Today’s Internet criminals are using the Domain Name System (DNS) to adapt attack vectors, and any robust security strategy should address DNS monitoring in order to secure assets and protect growth plans.

Understanding how threat intelligence works is critical to developing or improving robust network security policies. This white paper on DNS security presents an overview of the origin and evolution of threat vectors using the DNS, and it includes expert recommendations to help C-suite and IT decision makers define comprehensive policies and practices to secure an extended enterprise network.

Surveying the DNS threat landscape
In what may be looked back upon as the halcyon days of the Internet, the late 20th century was a time when you could treat malware as an infection, curing individual computers and inoculating against reinfection with antivirus signatures and firewall settings.

Today, a more accurate metaphor for Internet attacks may be multiple fronts in a cold war turning hot. The targets are multinational corporations and nation states—citizens and customers have become collateral damage. For criminal entities, exfiltration of intellectual property and sensitive data for profit has become the primary objective.

The 2012 Data Breach Investigations Report (Verizon, 2012) refers to the year in review as “a recounting of the many facets of corporate data theft.” The report records 855 data breach incidents in 2011 and many, many millions of compromised records.

- 79% of victims were targets of opportunity
- 96% of attacks were not highly difficult
- 94% of all data compromised involved servers
- 85% of breaches took weeks or more to discover
- 92% of breaches avoidable through simple or intermediate controls

These statistics make it abundantly clear that there are no silver bullets when dealing with enterprise security. A variety of technology solutions—in software and hardware, on the corporate network and in the open space of the Internet—are required to create a multilayered robust strategy to secure assets and protect growth plans as well as users.

If deploying an antivirus solution is the frontend tactic of your security strategy, then monitoring the DNS should be your backend tactic. The DNS is a bellwether for malicious activity, and both enterprise and government security experts are increasingly focused on this attack vector. Security experts estimate that over 80% of all malware takes advantage of the open framework of the DNS to facilitate activity, and 5% uses the DNS exclusively for communications (Harris, April 2012). Recent hacks have compromised the domain accounts of such high-profile companies as UPS, The Register, The Daily Telegraph, and National Geographic, allowing attackers to make unauthorized changes to DNS records and redirect visitors to third-party sites.

The cyber “bad guys” of today are well-organized and well-funded, with professional development resources and sometimes the backing of nation-states. They are using the DNS to adapt attack vectors and update botnets in real time, and atypical spikes in DNS traffic indicate that the popularity of this malware tactic is growing.

As client antivirus and network security measures are logical partners in any multi-layered enterprise security strategy, addressing vulnerabilities posed through the DNS is critical to that strategy in 2013 and beyond. The first step in developing a proactive strategy is getting a clear view of the DNS threat landscape. Learning to differentiate between normal and abnormal DNS traffic patterns can help you make the Domain Name System part of your intrusion detection system.

This white paper surveys the origin and evolution of the threat vectors that use the DNS in order to provide enterprise with threat intelligence and the means to develop or improve network security policies. As you begin to think about DNS security, ask yourself these questions:

Do I trust that the agent responding to my DNS query is the real owner of that domain?
Do I trust that the answer I’m getting back is the one the real owner intended to send?
How the DNS became a threat vector

Since the early 1980s, the Domain Name System has been translating human-friendly Internet domain names such as “www.example.com” into 32-bit Internet Protocol (IP) addresses (e.g., 172.10.254.1) in order to locate computers and route data worldwide. To use a popular analogy, the DNS works as the “telephone directory” of the Internet.

The design of the DNS is based on trust—that people and organizations on the Internet are who they say they are. At the time that the Domain Name System was conceived, there was little reason to foresee that the Internet’s evolution into an integral part of our everyday lives would create a fertile ground for illegal activities.

The Domain Name System uses authoritative name servers which are designated for each domain, an architecture that distributes the responsibility for assigning domain names and mapping them to IP addresses. This distributed system is designed for fault tolerance and speed by avoiding the need for traffic to go continuously to a centralized registry. The DNS can update and distribute name records quickly, allowing a domain’s IP location on the Internet to change without affecting human users, who simply continue to use the same domain name.

Moving out a level hierarchically, the Domain Name System uses caching, or recursive, name servers to improve efficiency and reduce the Internet traffic handling DNS queries. Using the phone book analogy, caching name servers work like “contact lists” of common or frequently dialed numbers. Caching servers use a recursive algorithm to contact the authoritative name servers of the target domain to resolve a query. The caching server stores DNS results, allowing new queries to be resolved faster than going through the full recursive query every time. To keep data communication moving efficiently, cached query results are designed to time out after a period of time called the “time-to-live” (TTL).

The Domain Name System is now the pivotal technology that enables all Internet transactions to occur. The DNS architecture processes billions of IP addresses for domains worldwide, and it provides name-to-IP address resolution for every type of digital content: sites, email, instant messages, transactions, file sharing and streaming multimedia, and so on.

These use requirements have evolved the DNS into an open and reliable service for resolving Internet addresses. Although the DNS doesn’t cause problems per se, its open, distributed architecture makes it a lucrative target for subterfuge. There are several points along the recursion path where DNS traffic may be intercepted or changed. A person with bad intentions can use the DNS to direct your query to the wrong web site or to intercept email. Most troubling for today’s enterprise is the fact that criminal organizations and political “hacktivists” are using the DNS to facilitate targeted attacks against corporate and government networks.

Types of DNS threats

DNS-based attacks have evolved, as the Internet itself has evolved, to be more adaptive and resilient. Attacks today are targeted at enterprise-level networks because the attack objectives have also evolved. The profile of the modern bad guy is no longer an individual mischief maker or petty spammer. Today’s attacks come from organized crime, foreign business interests and geopolitical agents provocateurs.

There are many issue and response variations between the different “flavors” of the DNS security problem. The upshot is that criminals are leveraging the strength of the DNS—its resilient, distributed architecture—for nefarious purposes, and they’re doing it in several ways.

“In transit” attacks

The more commonly known type of online malfeasance using the DNS is the “man-in-the-middle” attack—some variation of creating false content that looks real. This style of attack has become largely theoretical due to improvements in domain authentication, but it still happens. People aren’t careful enough about when and how to trust DNS results, especially those accessed over public networks where the DNS servers are more susceptible to cache poisoning.

Cache poisoning, or spoofing, is the introduction of false data into a DNS caching server that causes the server to return an incorrect IP address and divert the user to a different computer. (The flaw in DNS software that allows poisoning of the cache from outside is called the Kaminsky bug.) Botnets use a complex version of
cache poisoning by taking advantage of the “fast flux” technique in the DNS. A DNS caching server configured for fast flux means that the time to live for its cached addresses is very short, perhaps just a few minutes. Fast flux is utilized by large content distribution networks for load balancing, but criminals use fast flux DNS configurations to make their infrastructure harder to disrupt. The botnet’s command-and-control (C&C) domain cycles through botnet IP addresses so quickly, they’re nearly impossible to track.

Implementation of Domain Name System Security Extensions (DNSSEC) can largely prevent cache poisoning attacks. However, as we’ll discuss later, there’s a form of distributed denial-of-service (DDoS) attack in which the extra payload of cryptographic signatures in DNSSEC can end up amplifying the effect of the attack.

**Attacks on control of DNS record publishing**

Malicious attacks on DNS record publishing include hijacking domain owner accounts and hacking domain registrars and registries; essentially changing data where it’s published, rather than “in transit” between DNS servers and end users.

Responsibility for maintaining and updating the Internet’s master DNS records is spread among many domain name registrars worldwide. These registrars compete for the business of domain owners, and customers can move their domain records from registrar to registrar at any time. If a registrar’s supply of domain owner account passwords gets hacked, any of their customers become susceptible to domain theft.

Criminals are also hacking into certificate signing authorities and changing data so that they can gain access to secured networks. Certificate signing was developed as a way to ensure the trustworthiness of sites—that people and organizations really are who they say they are. Hacked authorities end up granting security certificates that allow imposters to prove they are a known, trusted company. (It’s worth noting that this problem is not always technological; there is little regulation on the process of certificate signing itself. The Internet is experiencing a proliferation of certificate authorities worldwide, some of them under the aegis of governments whose geopolitical interests are unfriendly to other nation-states.)

In this case, an enterprise’s DNS security may only be as strong as that of its partners. Performing due diligence in the acquisition of partner relationships and monitoring partner policies is the best defense option at this time.

**Attacks using domain generation algorithms**

In the last several years, the Domain Name System has become a “no man’s land” for botnet traffic attempting to avoid detection. After infecting a computer, bot malware has to go out to the Internet to contact its C&C domain for instructions. This observability poses a problem for criminals because they don’t want security forces to be able to track a bot back to its “mothership” and take down the C&C domain.

So in order to avoid being shut down, botnets are programmed to look up a bunch of random-seeming, gibberish DNS names. This type of malware uses a domain generation algorithm (DGA) to create randomized domain names based on a mathematical formula plus the time of day, a Twitter trending topic, or some other randomization factor. The bot is programmed to try a bunch of domain names that will only be valid on a given date.

A watershed example of the way a DGA-based attack can grow is the Conficker worm, which was first detected in 2008. The earliest variants of the worm generated around 250 domain names per day. Over several months and many rounds of one-upmanship between criminals and security authorities, the last Conficker variants generated 50,000 domain names per day, spread across many top level domains (dot-coms, country codes, and so on).

This is a very challenging attack method to combat. More DGA botnets are being created every day. Criminals can register just one domain out of the generated batch, but still create thousands of potential communication points, and they only have to get to one of them to control their botnet.

And even though most of the randomly-generated domains have names that appear to be gibberish, these domains can still cause problems for people who own real domain names. Once in a while, the algorithms happen to hit on a domain name that actually exists, an event known as a “domain collision.”
DGA botnets work on the premise that there will be enough randomized, weird domain names to keep security forces from finding and taking down the C&C domain—and that there may be some registrar or other who will allow questionable entities to register random domains without recording any type of identity information. The bad domain name essentially becomes an accountability laundering mechanism.

This problem touches on the need for policy and operational expertise among the entities that provide DNS services and resources, various Internet governing bodies, and world governments to apply order to the chaos. In the meantime, an enterprise-grade dynamic DNS firewall can be developed with the data found in IID’s ActiveTrust platform. ActiveTrust arms organizations with automated actionable intelligence about compromised hostnames and domains.

DNS tunneling

DNS tunneling is the last area of risk under the “Do you trust this domain?” question. DNS tunneling is a surreptitious way to use the framework of the Domain Name System as a tool to send other types of communication. Tunneling takes advantage of the normal DNS query/response protocol because the Domain Name System itself is never blocked. (If it were, people would lose the ability to resolve anything on the Internet.) By asking questions and getting answers over the DNS, malefactors can send and receive coded signals, similar to stenography. DNS tunneling is about hiding in plain sight, and it’s an emerging risk.

People first started experimenting with tunneling to get around Wi-Fi security (at hotels and airports, for example) so they could surf the ‘Net. Since the DNS is never blocked, people wrote software to “tunnel” their Internet connectivity over the DNS. It’s slow, but it works. Of course, it wasn’t long before people figured out that you could use the same method for distributing malware, or for getting onto a corporate or government network and exfiltrating data.

This method of exploiting DNS architecture is closely tied with the concept of the advanced persistent threat (APT). APT refers to foreign governments or rogue political organizations that have the ways and means to commit acts of cyber-espionage or cyber-sabotage against specific targets.

In the APT scenario, a cybercriminal, rogue organization, or hostile government gets access to its target’s network and, using DNS queries, takes a big file and sends it off to a foreign country where the recipients are interested in the contents. DNS tunneling works for espionage because attackers can use the slower DNS channel quietly. You don’t see it, you don’t monitor for it.

Now security experts are starting to see DNS tunneling used as a covert channel to transmit actual malicious communications in the DNS queries.

IT security teams traditionally look at unusual files and/or unusual connections rather than what’s in the DNS. Antivirus solutions and intrusion detection systems are all set up with the idea that someone is going to send you a file, or bits of files, through some port or communications channel that will then change something on your computer. But with DNS tunneling, there are no identifiable or visible malware signatures to look for, making tunneling attacks very hard to detect.

The real risk in DNS tunneling attacks is that you can’t block the DNS from being used. The best you can do is take a look at how people are using the DNS and make determinations about practices around patterns. In this area a DNS security partner solution that includes active threat monitoring, such as ActiveTrust, can help.

Reflective DNS amplification DDoS attacks

The Domain Name System is sometimes used as a tool for a different sort of online security problem, but a discussion of threats to network security via the DNS would not be complete without mentioning it. DDoS attacks using reflective DNS amplification are an immediate and growing threat area for anyone connected to the Internet.

A reflective DNS amplification DDoS attack takes advantage of the fact that criminals can spoof DNS queries to look like they’re coming from a different address; in this case, the address of the DDoS target. Then the reflective DNS amplification comes in. The
attackers send the spoofed queries to open DNS caching servers, which then query the DNS authoritative servers. The query may be something like “where is foo.example.com?” with the “foo” part being something new, so that the response to the DNS query includes additional information about “foo.” Essentially a very small query, in terms of packet size, generates a much larger packet response. The response is especially amplified if foo.example.com has a larger than usual DNS record, which domains enabled with DNSSEC do.

Do this once, no problem. But do it a million times, and you have a huge DDoS attack. The amplified packet response is reflective because it goes to the victim whose IP address was spoofed, instead of going to the true source of the query.

The whole point of a DDoS attack is resource exhaustion—it makes a legitimate Internet resource unavailable to innocent people who actually want to use it. DDoS attacks are nothing new; however, as the name implies, reflective DNS amplification makes DDoS an extraordinarily effective attack methodology. This type of attack is devastating to the target victim or victims, and it’s not easily blocked because the attack is made up of simple responses from DNS caching servers that respond to anybody. A DNS administrator can set query/response limits on an authoritative name server, but other recursive DNS name servers are open.

Massive reflective attacks are indirect to the functioning of the Domain Name System itself, but they are a major threat to all who use the Internet. Although the security community is working on the problem, an authoritative, enforceable response to reflective DNS amplification DDoS attacks does not yet exist.

**Developing DNS threat countermeasures**

The Domain Name System is, by design, open and resilient to change. For over three decades it has proven its worth as the Internet’s “phone directory,” reliably connecting ever-changing domain names with billions of IP addresses. The DNS is also a high-risk area for enterprise security in the ongoing Internet war between cybercriminals and the rest of us.

If you change DNS records in one place, they may not be changed appropriately in another. Unaware, your users may be compromising the network by opening channels with addresses they believe they can trust. And yet you can’t turn off the DNS without effectively crippling your network.

It takes careful thought and implementation to secure an extended enterprise network against data exfiltration and domain theft. As this discussion of the DNS threat landscape shows, any comprehensive DNS security strategy must include a multi-pronged approach:

<table>
<thead>
<tr>
<th><strong>Enable and monitor trust validation in your enterprise.</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Validate the digital proofs that other people are putting on their DNS content with DNSSEC. Take advantage of real-time threat intelligence in a dynamic actively monitored DNS firewall and 24/7 threat monitoring solutions provided by a DNS resolver partner.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Secure your registrar relationship.</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Know the policies and security track records of the companies who maintain your master DNS records to help guard against domain theft. Enforce best practices for your domain account password: use a strong password do not use the same password for any other purpose and change the password periodically.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Use digital proofs to secure DNS content.</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Know whom you’re “trusting” and prove that others can trust you. Crypto-authentic proofs allow other people to be certain that the DNS content purporting to come from your enterprise is the real deal.</td>
</tr>
</tbody>
</table>

Securing DNS access to your network must be an integral part of any comprehensive security strategy in the enterprise. DNS security measures are the rearguard in your security strategy—without it, your backend is exposed to those who would do you harm.

**IID aggregates widely sourced threat data and delivers actionable intelligence to facilitate the protection of users, brands and business growth. Your organization can use ActiveTrust threat intelligence to block DNS communications to malware controllers, spear phishing sites, data exfiltration drop servers and other threats.**

IID stands ready.

Call us at 1-888-239-6932
www.internetidentity.com
References


About the authors

Rod Rasmussen co-founded IID and is the company’s President and CTO. He is widely recognized as a leading expert on the abuse of the domain name system by criminals. Rasmussen serves in leadership roles in various industry groups including the FCC’s Communications Security, Reliability and Interoperability Council (FCC CSRIC), the Anti-Phishing Working Group (APWG), ICANN’s Security and Stability Advisory Committee (SSAC), the Online Trust Alliance (OTA), and the Forum of Incident Response and Security Teams (FIRST).

Dr. Paul Vixie is Chairman and Founder of ISC (Internet Systems Consortium). He served as President of MAPS, PAIX and MIBH, as CTO of Abovenet/MFN, and on the board of several for-profit and non-profit companies. He has served on the ARIN Board of Trustees since 2005, where he served as Chairman in 2008 and 2009. Vixie has been contributing to Internet protocols and UNIX systems as a protocol designer and software architect since 1980. He is considered the primary author and technical architect of BIND 8, and he hired many of the people who wrote BIND 9 (and now BIND 10). He has authored or co-authored a dozen or so RFCs, and "Sendmail: Theory and Practice" (Digital Press, 1994). He earned his Ph.D. from Keio University for work related to the Internet Domain Name System (DNS and DNSSEC).

IID enables trusted threat intelligence collaboration for enterprises and governments. The company aggregates widely sourced threat data and delivers actionable intelligence to facilitate the protection of users, brands and business growth. IID’s ActiveTrust platform enables threat intelligence sharing in a trusted environment that reaches beyond limited trust groups. ActiveTrust delivers automated threat intelligence that allows network members to maximize their most valuable resources, human capital and time, allowing companies to focus on their core business. Top financial firms, the largest government agencies, and leading e-commerce companies, social networks and ISPs leverage IID to detect and mitigate threats. For more information about IID, go to www.internetidentity.com.