CIO
BUSINESS TECHNOLOGY LEADERSHIP
JULY 15, 2015 | CIO.COM

Why you need to care more about DNS

There's one key part of your network infrastructure that you're probably not monitoring, even though it keeps you connected, can tell you a lot about what's happening inside your business – and is an increasing source of attacks. DNS isn't just for domain names any more.

By Mary Branscombe

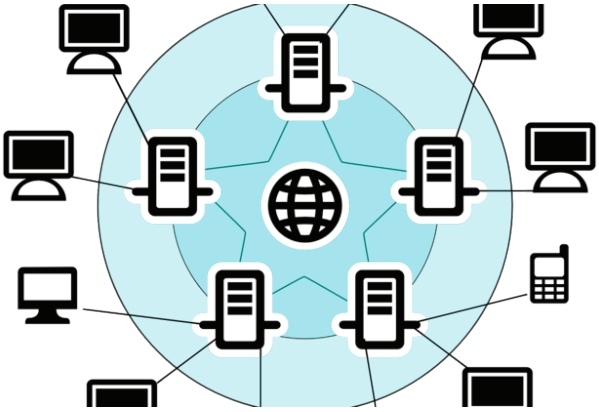
When you say Domain Name System (DNS), you might think, naturally enough, of domain names and the technical details of running your Internet connection. You might be concerned about denial of service attacks on your website, or someone hijacking and defacing it.

While those certainly matter, DNS isn't just for looking up Web URLs any more; it's used by software to check licences, by video services to get around firewalls and, all too often, by hackers stealing data out from your business. Plus, your employees may be gaily adding free DNS services to their devices that, at the very least, mean you're not in full control of your network configuration. It's a fundamental part of your infrastructure that's key to business productivity, as well as a major avenue of attack, and you probably have very little idea of what's going on.

DNS is the most ubiquitous protocol on the Internet, but it's also probably the most ignored. Data Leak Protection (DLP) systems that check protocols used by email, web browsers, peer-to-peer software and even Tor, often neglect DNS. "Nobody looks much at DNS packets, even though DNS underlies everything," says Cloudmark CTO Neil Cook. "There's a lot of DLP done on web and email but DNS is sitting there, wide open."

Data lost in the Sally Beauty breach last year was exfiltrated in packets disguised as DNS queries, but Cook points out some unexpected though legitimate uses; "Sophos uses DNS tunnelling to get signatures; we even use it for licensing."

A number of vendors are starting to offer DNS tools, from Infoblox's appliances to OpenDNS' secure DNS service; Palo Alto Networks is starting to offer DNS inspection services, U.K. domain registry Nominet has just launched its Turing DNS visualisation tool to help businesses spot anomalies in their DNS traffic, and Cloudmark analyzes patterns of DNS behavior to help detect links in email going to sites that host malware. There are also any number of plugins for common monitoring tools that will give you basic visibility of what's going on.



Few businesses do any monitoring of their DNS traffic despite it being the source of many attacks. It's not just the malware that runs on Point of Sale systems, capturing customer credit cards in attacks like those on Sally Beauty, Home Depot and Target, that uses DNS tunnelling. DNS is the most ubiquitous command and control channel for malware, as well as being used to get data stolen by malware from your business.

"DNS is frequently used as a conduit to surreptitiously tunnel data in and out of the company," says Cricket Liu, the chief DNS architect at Infoblox, "and the reason people who write malware are using DNS to tunnel out this traffic is because it's so poorly monitored, most people have no idea what kind of queries are going over their DNS infrastructure."

There's also the problem of people using DNS to bypass network security controls; that might be employees avoiding network restrictions, security policies or content filtering, or it might be attackers avoiding detection.

DNS attacks are a widespread problem

In a recent Vanson Bourne study of U.S. and U.K. businesses, 75 percent said they'd suffered a DNS attack (including denial of service and DNS hijacking as well as data theft through DNS), with 49 percent having experienced an attack during 2014. Worryingly, 44 percent said it was hard to justify investments in DNS security because senior management didn't recognize the issue.

That's because they think of DNS as a utility, suggests Nominet CTO Simon McCalla. "For most CIOs, DNS is something that happens in the background and isn't a high priority for them. As long as it works, they're happy. However, what most of them don't realize is that there is a wealth of information inside their DNS that tells them what is going on within their network internally."

Liu is blunter: "I'm surprised how few organizations bother to do any kind of monitoring of their DNS infrastructure. DNS doesn't get any respect, yet TCP/IP networks don't work without DNS; it's the unrecognized lynch pin." Liu insists "it's not rocket science to put in monitoring of your DNS infrastructure; there are lots of mechanisms out there for understanding what queries DNS servers are handling and their responses. And you really ought to be doing because this infrastructure is no less critical than the routing and switching infrastructure that actually moves packets across your network."

Usually, he finds demonstrating the threat is enough to get management attention. "Most CIOs – once they see how with one compromised machine on the inside of a network you can set up a bi-directional channel between that endpoint and a server on the internet – realize they need to do something about this. It's just a matter of being faced with that cold hard reality."

Tackling DNS security

First, you need to stop thinking about DNS as being about networking and just "part of the plumbing," says David Ulevitch, the CEO of OpenDNS (which Cisco is in the process of acquiring).

"It used to be network operators who ran your DNS, and they were looking at it in terms of making sure the firewall was open, and not blocking what they viewed as a critical element of connectivity as opposed to a key component of security policy, access control and auditing. But we live in a world today where every network operator has to be a security practitioner."

If you actively manage your DNS, you can apply network controls at a level employees (and attackers) can't work around. You can detect phishing attacks and malware command and control more efficiently at the DNS layer than using a web proxy or doing deep packet inspection, and you can detect it as it happens rather than days later.

"DNS is a very good early warning system," says Liu. "You can pretty much at this point assume you have infected devices on your network. DNS is a good place to set up little tripwires, so when malware and other malicious software gets on your network, you can easily detect its presence and its activity, and you can do some things to minimize the damage it does." You could even see how widespread the infection is, by looking for similar patterns of behaviour.

Services like OpenDNS and Infoblox can also look across more than your network. "It's easy to build a baseline of what normal looks like and do anomaly detection", says Ulevitch. "Suppose you're an oil and gas business in Texas and a new domain name pops up in China pointing to an IP address in Europe, and no other oil company is looking at this domain. Why should you be the guinea pig?"

You also need to monitor how common addresses are resolved on your network – hackers can try to send links to sites like Paypal to their own malicious sites – and where your external domain points to. When Tesla's website was recently redirected to a spoof page put up by hackers, who also took control of the company's Twitter account (and used it to flood a small computer repair store in Illinois with calls from people they'd fooled into believing they'd won free cars), the attackers also changed the name servers used to resolve the domain name. Monitoring their DNS might have given Tesla a heads-up that something was wrong before users started tweeting pictures of the hacked site.

At the very least, remember that DNS underpins all your online services, Ulevitch points out. "The bar is very low for improving DNS. Usually, DNS is seen as a cost enter; people don't invest in reliable enough infrastructure or high enough performance equipment so it's hard to cope with a high volume of transactions."

That doesn't only matter if you're targeted by a DNS attack. "Organizations should look at DNS performance because it will have a material impact on everything you do online. Every time you send an email or open an app you're doing DNS requests. These days, web pages are very complex and it's not uncommon to have more than 10 DNS requests to load a page. That can be a whole extra second or more, just to handle the DNS components of loading a page."

Tracking business behavior

Monitoring DNS can also give you a lot of information about what's going on across your business far beyond the network. "We live in a world where the network perimeter is becoming ephemeral and where services are easy to adopt," Ulevitch points out. "A marketing executive can sign up to Salesforce; if you're looking at the DNS you can see that. You can see how many employees are using Facebook. You can see devices showing up in your network, whether it's because they're checking a licence or doing data exfiltration. If you have a hundred offices, you can still see who is connecting devices."

That's not just PCs either, he points out; printers and televisions and IoT devices are increasingly connecting to your business network. "Do I want my TVs phoning home? If you look at the Samsung privacy policy, it says the TV has a microphone that might be listening at any time; do I really want that in the corporate boardroom? Maybe I want to apply DNS policies so my TVs can't phone home."

Infoblox's Liu agrees. "IoT devices are often not designed with a lot of security in mind. You want to make sure devices are connecting where they should be and that if someone throws something else onto your IoT network they can't access your internal network. DNS is a useful place to monitor and control that access."

And because you're already using DNS, monitoring it isn't disruptive, Ulevitch points out. "Usually in security, the reason most things aren't used is the effort needed to make sure they don't have a detrimental effect on user performance."

In fact, you need a good reason *not* to be doing this, he says. "There are fundamental best practices in security and one of them is network visibility. Not being able to see the traffic on your network means you're flying blind. Finding a way to inspect DNS traffic is a fundamental requirement of a strong security posture. To not know what's happening on your network is borderline derelict."

Mary Branscombe is a freelance journalist who has been covering technology for over two decades.