5 MUST-ASK DNS QUESTIONS

Almost every action taken on the Internet begins with a Domain Name System (DNS) request that translates domain names to IP addresses. While DNS makes the Internet fast and efficient, and significantly more navigable for humans, it is inherently ripe for exploit due to its open and ubiquitous nature. DNS itself has no intelligence and, as a result, will resolve requests for both benign and malicious domains.

Cyber criminals are capitalizing on this vulnerability in recursive DNS to launch damaging malware and ransomware campaigns, phishing attacks, and data exfiltration against companies. As your users, devices, applications, and data continue to move outside of the traditional enterprise perimeter and zone of control, your attack surfaces will only expand.

So, how are you proactively protecting your network from these targeted threats? Many businesses are turning to a zero trust security strategy to "verify, but never trust" all users and devices. This is an especially relevant approach as we examine the inherent risk that users and devices pose through outbound DNS requests. Here are five things to ask yourself to determine if you need a DNS security strategy.

1 How many requests does your recursive DNS resolve per day?

One device makes several thousand queries per day; now multiply that by every user and device on your network. It's difficult to view this data in aggregate as the volume often prohibits entry into a security information and event management (SIEM) system. There is simply too much good and too little bad traffic to warrant adding DNS logs into a SIEM. Moreover, exporting logs and cutting in data from multiple sources is onerous. Even if you overcome these aggregation issues, you're viewing thousands (or millions) of hostnames with no context. While too much data is a problem, too little data is worse as you're deriving insights in a vacuum.

2 What does irregular DNS traffic look like?

Well, do you have a benchmark for regular, healthy DNS traffic? Given the number and variety of DNS requests on your network — originating from laptops, mobile phones, desktops, tablets, printers, and guest Wi-Fi, not to mention all of the "smart" connected devices — it's difficult to know what constitutes normal day in and day out. Additionally, it is often far too time consuming and arduous to dig through the data to identify which devices on your network are making requests.

This is an important piece of information however, as device type can be a key indicator that something has gone awry. While a laptop making thousands of recursive DNS queries per day should not raise alarm, your building's HVAC system sending that many requests should certainly be investigated further. But only if you can first identify the HVAC as the source of these superfluous requests. As the number of connected devices (Internet of Things) climbs — projected to reach 20.4 billion in 2020[1] — your exposure will only increase.

Even if you allocate resources to constantly monitor and dissect your DNS logs, or something appears hugely amiss, by which time it's probably too late, it's highly unlikely you'll identify and mitigate an intrusion before it inflicts damage. This is because your company's sample size is too small to identify Internet-wide trends and threats, which is why many employ a cloud service. The more traffic and intelligence you view in aggregate, the easier it becomes to flag irregular DNS traffic; you must understand global trends and patterns to efficiently and consistently identify threats.

3 Do you know that recursive DNS can be used to exfiltrate data from your enterprise?

Targeted threats continue to evolve as companies and individuals react to attacks. Increasingly, cyber criminals are using recursive DNS to penetrate security perimeters, honing in on the infrastructure's innate vulnerabilities. Once a device on your network is infected, the vast majority of malware will send a request back to its command and control (CnC) server for further instructions. As DNS traffic is necessarily unfiltered and open, these malicious queries will go unchecked, bypassing all network-level security.

Through this DNS tunneling, bad actors can exfiltrate financial records, social security numbers, credit card information, intellectual property, and other sensitive data. These data packets are encrypted, compressed, chopped, and then transmitted using various techniques to avoid detection such as slow drip, IP spoofing, domain generation algorithms (DGAs), and fast flux. You'll be none the wiser about this breach if you rely solely on network-level security.

Understanding this innate vulnerability becomes even more vital when you consider the growing mobility of today's workforce. As employees, vendors, partners, and suppliers move outside the traditional network perimeter, increasingly working from home, coffee shops, airports, hotels, conferences, and more, their devices are most likely connecting to unsecured networks. All it takes is one compromised device reconnecting to your corporate network to unleash malware that facilitates data exfiltration across the enterprise.

4 Can you apply policy to block malicious activity across your entire company in seconds?

Identifying a bad domain or IP address is challenging, but it's only half of mitigating a targeted threat. Once an attack or vulnerability is pinpointed, IT teams have the unenviable task of implementing a defense plan, quickly and company-wide. Without a cloud-based solution, this might involve numerous unwieldy software updates and hardware installations. These directives also require effective and timely communication from HQ, and are then contingent upon 100% compliance by all branches, employees, and devices on your network.

That's a lot of room for error, and hours — if not days — of exposure. Alternatively, a cloud-based solution allows for configuration and deployment in minutes with no hardware or software. It can be managed from anywhere, pushed everywhere, and enforced unilaterally almost instantaneously.

5 Is DNS part of your layered security system?

You can't afford for it not to be. Seventy percent of organizations had a security incident that negatively impacted their business in 2016,[2] and the number of data breaches grew by 30% in 2017.[3] The mean time from a breach to identification is more than six months[4] and the average cost is $18 million, including damage to brand reputation.[5]

As every web request from the enterprise begins with DNS, it's the perfect control point to secure company-wide visibility into web requests and apply security policy. And since this validation happens before the IP connection is made, threats are stopped earlier in the security kill chain and further away from an enterprise's perimeter. Recursive DNS is an often forgotten attack vector, but with ever-evolving malware and growing financial incentives for hackers, you must reinforce this vulnerable back door.

Proactive Targeted Threat Protection in the Cloud

Proactively protecting your recursive DNS from targeted threats is imperative, and incorporating a cloud solution like Akamai's Enterprise Threat Protector into your security stack is now easier than ever. It is quick to configure, easily scalable, and simple to deploy with no hardware or software, and zero downtime. The cloud portal allows agile central management and enforcement of unified policies in minutes, and the dashboard provides drill-down into DNS traffic, threat events, and Acceptable Use Policy (AUP) activities.

Enterprise Threat Protector easily integrates with other security products and reporting tools, allowing companies to maximize their investments across all layers of their defense-in-depth strategy. Powered by real-time intelligence from Akamai's Cloud Security Intelligence and insights gleaned from managing 30% of global web traffic via Akamai's Intelligent Platform, Enterprise Threat Protector provides near-instantaneous protection for companies and their employees.

SOURCES

1. http://www.gartner.com/newsroom/id/3598917
2. **RSA Cybersecurity Poverty Index 2016,** https://www.rsa.com/en-us/resources/rsa-cybersecurity-poverty-index-2016
3. http://247wallst.com/technology-3/2017/06/22/2017-data-breaches-nearly-30-higher-than-2016s-record-pace
4. **Ponemon Institute: 2016 Cost of Data Breach Study,** https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=SEL03094WWEN
5. **Ponemon Institute: The Economic Impact of Advanced Persistent Threats**