AKAMAI WHITE PAPER

How Securing Recursive DNS Proactively Protects Your Network

Akamai

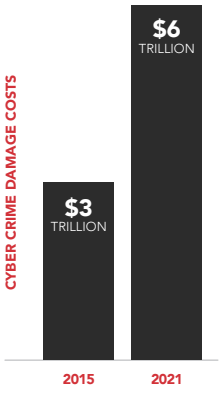
Executive Summary

With high-profile security attacks occurring every day, organizations are more concerned than ever with cyber security. Many are going well beyond anti-virus protection and firewalls to adopt multiple layers of security such as intruder prevention systems, sandboxing, and secure web gateways. Yet most IT departments fail to protect the recursive Domain Name System (DNS). This oversight leaves valuable data and personal information on their networks wide open to attack by malicious actors.

But recursive DNS (rDNS) doesn't have to be a vulnerability. Recursive DNS security solutions that serve as an effective security checkpoint are available to stop these types of attacks in their tracks and proactively protect end-user devices and the network.

This white paper details how recursive DNS security solutions block malware attacks at critical junctures. Using these recursive DNS security solutions, organizations benefit not only from improved security, but also simplified security administration and enhanced security performance.

Your Recursive DNS Is Putting Your Enterprise at Risk

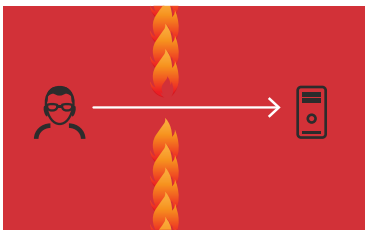


Security threats are persistent and growing. Worldwide cyber crime damage costs are expected to reach $6 trillion annually by 2021, up from $3 trillion in 2015.[1] Losses from global ransomware alone are expected to exceed $5 billion in 2017, up from $325 million in 2015 — a 15x increase in two years.[2]

With cyber criminals using many attack vectors, companies today typically address these threats using multiple layers of security. These include next-generation firewalls, secure web gateways, sandboxing, intruder prevention systems, endpoint anti-virus, and more. Yet despite these safeguards, malicious actors continue to find ways to breach a company's security by exploiting gaps in these multiple layers of security.

One common weakness that many of today's threats exploit is recursive DNS (rDNS). Malicious actors target rDNS because it is:

- **Ubiquitous —** DNS translates human-readable domain names (e.g., www.mydomain.com) into machine-understandable IP addresses. DNS is the core protocol used to perform requests of every kind on the Internet — from web browsing to email to online retail to cloud computing. Whenever an end user makes a request and the IP address is not already in cache, a recursive DNS server looks for it.
- **Open —** DNS is designed only to resolve requests. Because it does not evaluate whether the resource it is connecting to is good or bad, users can inadvertently connect to malicious domains.
- **Unprotected —** Firewalls don't typically inspect DNS port 53, which DNS servers use to listen for queries from DNS clients. Nor do most IT teams make protecting DNS communications a priority. Because IT organizations don't implement security solutions that automate protection, the only way to monitor DNS ports is manually. High traffic volumes mean manual monitoring is time consuming and inefficient. And because companies have limited sampling of their own DNS traffic, it is difficult to spot problems or identify trends that indicate irregularities.



Without DNS-based protection, most organizations don't monitor queries over their DNS infrastructure. And the DNS resolution process doesn't prevent users from arriving at or connecting to domains that place requests to known malicious locations. Companies expose themselves to the risk of malware that infiltrates corporate networks to steal user credentials, data, or intellectual property, as well as ransomware infections that prevent companies from accessing their data unless they pay a hefty ransom.

Why You Need a Recursive DNS Security Layer to Protect the Enterprise

Recursive DNS is often a security weakness that can be exploited. But it has the potential to be an effective security checkpoint where attacks can be halted before they have a chance to establish inroads on the network.

As mentioned in the previous section, DNS resolvers perform one core function. They take a human-readable domain name and find the corresponding IP address of the server where the resource is located. That means nearly every Internet request relies on a DNS resolver. The resolver will either find the IP address in cache or will use a recursive DNS server to search through a hierarchy of DNS nameservers and authoritative DNS servers that track all the information about a specific domain or subdomain.

Instead of resolving all DNS queries blindly, an organization can forward these requests to a third-party service that acts as the DNS server. This service can check the domain names against a frequently updated list of known malicious domains, apply its own intelligence, and administer policies that prevent requests from proceeding to malicious domains, minimizing the chance of infection.

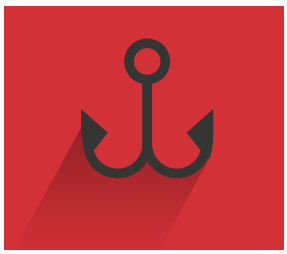
Using a third-party recursive DNS security solution, rDNS becomes a "DNS firewall" that protects the enterprise before an infection can occur. Instead of being a vulnerable security liability that can be exploited, recursive DNS becomes a valuable security asset that proactively protects the network.

How Recursive DNS Security Works

How does rDNS security protect against cyber attacks?

Let's look at how malware attacks that exploit recursive DNS typically play out and how recursive DNS security can thwart these attacks every step of the way.

Blocking Malware Delivery



All recursive DNS exploits begin when malware finds its way onto an end user's machine or connected device. Proactive recursive DNS security can stop many of these attacks.

An end-user machine or connected device can become infected with malware through a variety of tactics. Phishing and spear phishing attacks — where a user downloads a malicious attachment or is prompted to click an embedded link — are the most common malware delivery mechanisms, according to a recent report from Verizon.[3] But malware can also gain access to a user's machine through a malicious download or an infected USB key. A user might also browse to a compromised domain directly, or click on a malicious ad or link on a page where they are already browsing.

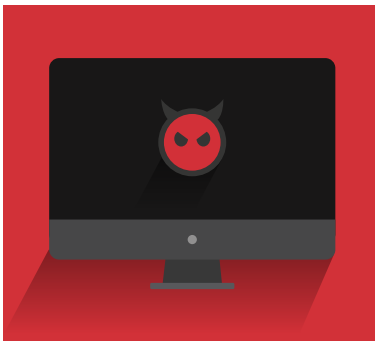
If a domain delivers malware, recursive DNS security intelligence proactively blocks users from accessing that domain.

Detecting Command and Control (CnC)

Of course, not every malware threat comes from a link. As we mentioned in the previous section, malware can make it onto the device through an attachment in an email or through a USB key. Recursive DNS security can help in these situations as well.

Once malware finds itself on a user's machine, its next step is usually to connect with its command and control (CnC, also known as C2 or C&C) server to send back intelligence about the device on which it is installed, such as an unpatched operating system or application vulnerabilities. The CnC server can then instruct the malware to download remote access tools, additional software components, or updates that exploit the unpatched vulnerabilities on the compromised device. In this case, recursive DNS security proactively prevents access to the CnC server and therefore the download of this additional malware.

If CnC servers do succeed in gaining access to end-user machines on the target network, they can issue commands to the compromised systems. These actions can be as simple as continually sending out beacons that keep an inventory of compromised systems, or they can take malicious action such as remotely controlling the machine, exfiltrating data, or installing ransomware on endpoint devices.



A recursive DNS security solution can also detect these actions. The rDNS security solution examines the communications traffic between a compromised endpoint and the CnC server. If necessary, it can send traffic for analysis via machine learning to detect suspicious traffic patterns. This security intelligence can also incorporate learning from attacks that others have experienced by accessing threat data from various vendors and information-sharing partners. The ability to access multiple threat databases allows the solution to benefit from a vastly greater information set than it can develop on its own. When the recursive DNS security solution identifies suspicious behavior patterns indicative of command and control, it alerts security teams.

Additionally, once a machine on the network is compromised, the attacker will often attempt to move laterally within the target network to additional hosts. This ensures that if one infected system is detected, the attacker continues to maintain access. Or the attacker can create a bot network of zombie devices that participate in attacks unbeknownst to the machine's owner. Recursive DNS security jumps into the fray here, too. Once again, by analyzing network traffic patterns, rDNS security can detect attempts by the newly infected systems to communicate with the command and control servers and prevent these machines from contacting the CnC infrastructure.

Thwarting DGAs (Domain Generation Algorithms) and Fast Fluxing

Network security teams and hackers play a never-ending game of cat and mouse — and recursive DNS security helps the cats gain the upper paw.

Hackers are well aware that network detection techniques can easily discover a predefined list of malicious domain names and then block them or shut them down, severing the links between the infected device and the CnC server. In response, hackers have come up with several techniques to prevent security teams from finding and closing these links, including DGAs and fast flux.

DGAs generate a large number of domain names that can be used as rendezvous points with their command and control servers. The only way to block these domain names with a firewall blacklist would be to reverse engineer the algorithm used to generate the domain names. In addition, DGAs can regenerate domain names frequently. Attackers simply set up the CnC server briefly to allow infected machines to call home, then shut it down and reinstate it again as the need arises.

Fast fluxing prevents IP-based access control lists from working by taking advantage of the fact that DNS allows an administrator to register a number of IP addresses to a single host name for purposes of load balancing. Fast flux can be used to hide phishing and malware delivery sites behind an ever-changing network of compromised hosts acting as proxies.

Recursive DNS security detects both DGA and fast fluxing. Instead of looking at domain names, the rDNS security solution's machine learning can evaluate DNS traffic patterns to a given site from a large number of users across the Internet to identify suspicious patterns of behavior. For example, the enterprise threat protection system can examine billions of DNS requests a day and can see that multiple people are using a domain — and that the domains they access keep changing. The system uses machine learning behavioral analysis in a similar manner to identify fast fluxing.

Preventing Data Exfiltration

Unlike the strong protections found on protocols such as HTTP, SMTP, and FTP, DNS port 53 is often unprotected. Recursive DNS security fills this gap.

Once a machine is compromised, CnC servers often use port 53 to exfiltrate sensitive data in a process called DNS tunneling. In tunneling, cyber criminals use DNS to smuggle data out of the enterprise. Criminals break up the data into small chunks, hide these in a DNS query, and send the queries to a "rogue" authoritative DNS server that they control remotely. This rogue server receives, unencodes, and reassembles the stolen information.

The rDNS security solution detects data exfiltration by looking at the DNS traffic patterns. For example, it might see large numbers of sequential requests to the same domain at fixed time intervals. It can then take steps to correct that problem.

Benefits

Using an rDNS security solution, organizations can achieve a wide range of benefits:

Significantly Improve Security Defenses and Close DNS Security Gaps

Recursive DNS security solutions proactively block DNS requests to malware drop-sites, malware CnC servers, and ransomware sites, as well as prevent DNS data exfiltration by taking advantage of unique and up-to-date threat intelligence that improves security defenses and closes DNS security gaps.

Secure All Ports and Protocols

In general, secure web gateways only look at port 80 (HTTP traffic) or port 443 (HTTPS traffic). Because all traffic uses DNS regardless of protocol, and malware exploits this blind spot, a recursive DNS security solution secures all ports and protocols.

Stop Attacks Early, Before IP Connection

Because recursive DNS security detects threats before any IP connection is made, blocking happens early and further away from the network perimeter. Ideally, this is where blocking should occur. If you try to kill activity later in the cycle, the costs of investigation and remediation rise.

Reduce Alert Noise

One of the problems that IT security teams face is that they get too many alerts. It becomes difficult and time consuming to determine which alerts are real and which are false positives. By mitigating more attacks at the DNS level, organizations see fewer events that need to be addressed by other security systems on the network, making the IT security team's job more manageable.

Leverage Existing Threat Intelligence

A company may already have access to threat intelligence or have a threat intelligence program. By incorporating this threat intelligence into the recursive DNS security solution, companies can increase ROI on their existing solutions.

Improve HTTPS Performance

Today, more than 70% of global Internet traffic is encrypted[4] — and more is being encrypted each day. As a result, encrypted traffic will become the "go to" way of distributing malware and executing cyber attacks. Inspecting encrypted traffic is very processor intensive because it requires organizations to decrypt and inspect the SSL traffic. By using recursive DNS security to block suspicious DNS traffic, you reduce the amount of HTTPS traffic that needs to be inspected.

Set Up Easily

A 100% cloud-based recursive DNS security solution can be configured and deployed in minutes without the need to set up and maintain hardware to protect all locations.

Conclusion

Your enterprise security is only as strong as its weakest link. For many organizations, recursive DNS is a gaping security hole that cyber criminals are only too happy to exploit.

By deploying a recursive DNS security solution, your organization can close your DNS security gaps and significantly improve your security defenses. Not only do recursive DNS security solutions secure all ports and protocols, they block DNS requests to malware drop-sites, ransomware sites, and malware CnC. Because this blocking occurs farther away from the network perimeter, it reduces the cost of remediation. These solutions even simplify security management by reducing false alarms and improve HTTPS performance by reducing the amount of HTTPS traffic that needs to be inspected.

For more information on recursive DNS security, visit akamai.com/etp.

Sources

1) http://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/

2) http://www.csoonline.com/article/3197582/leadership-management/ransomware-damages-rise-15x-in-2-years-to-hit-5-billion-in-2017.html

3) http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017/

4) https://www.sandvine.com/pr/2016/2/11/sandvine-70-of-global-internet-traffic-will-be-encrypted-in-2016.html