HACKER PERSONAS

A Deeper Look Into Cybercrime

CARBONITE an opentext company | WEBROOT an opentext company

THE INFILTRATOR

Infiltrators rely on virtual back doors and unprotected points of entry to slip through hidden cracks. Hiding in the shadows, this type of cybercriminal lurks, watches and waits for the opportunity to invade systems. DNS (Domain Name System), which is considered a trusted protocol, is especially vulnerable. Once the criminal redirects internet traffic to malicious websites or takes control of servers, the damage is inevitable. But thanks to modern technology and security awareness training, damage can be mitigated quickly.

DNS is an Unlocked Back Door

One of the most common methods of infiltration includes internet-based attacks, such as Denial of Service (DoS), Distributed Denial of Service (DDoS) and DNS poisoning. By default, DNS traffic is unencrypted, allowing internet service providers and other third parties to monitor website requests, surveil browsing habits, and even duplicate web servers to redirect traffic. However, cybercriminals can also use legal DNS traffic surveillance to their advantage. There are several examples that show the vulnerabilities of DNS:

Amazon Web Services (AWS) DDoS Attack
Amazon reportedly mitigated the largest known DDoS attack in history, stopping a 2.3 terabit-per-second (Tbps) threat. The attack hit the Amazon Route 53 DNS web service, impacting all AWS services as well as thousands of Amazon customers.[1]

GitHub DDoS Attack
Prior to the AWS attack, the largest verifiable DDoS attack on record (1.3 Tbps) targeted the web development platform GitHub. Hackers used amplification to affect the database's caching system, flooding servers with spoofed requests.[2]

The Mirai Krebs DDoS Attack
The blog of cybersecurity expert Brian Krebs was assaulted by a DDoS attack in excess of 620 Gbps, which was three times bigger than any previous attack on the site. The source was the Mirai botnet made up of 600,000 compromised IoT devices.[3]

> MSPs can benefit from deploying DNS protection solutions that support DNS-over-HTTPS, especially for employees working remotely on unsecured devices.
>
> **Grayson Milbourne,** Webroot

DISRUPTION IS COSTLY

There are several types of infiltration attacks that utilize flaws in internet security to cause disruption or damage. A DoS or DDoS attack is designed to disrupt normal web traffic or make a website unavailable in some way, often used to leverage ransoms from victims.

Network flooding is a type of DDoS attack that floods DNS servers with high volumes of traffic, making the service temporarily unavailable. While not always associated with ransoms or specific financial loss, flooding and other DNS attacks can cause serious disruption to businesses of all sizes.

Even short website or network outages can increase downtime. According to Gartner, the average cost of IT downtime is $5,600 per minute.[4]

DNS Attacks Are a Threat to All Businesses

The goal of DDoS and other infiltration-based attacks varies, but disruption and financial gain are desired outcomes for infiltrators. In some cases, criminals may launch a DDoS attack on a specific business to demand a ransom payment or another action, like providing access to a network or third party, in order to restore service. They can also be launched by a rival business to discredit the victim's service and damage their reputation with customers. Around 82% of organizations have faced a DNS attack at some point, and the average cost per attack is now $1.07 million.[5]

Stopping Infiltrators with DNS-over-HTTPS

To protect against DDoS and other DNS attacks, ISPs like Google and Mozilla have been working to encrypt and secure the Domain Name System.[5] In 2018, DNS-over-HTTPS (commonly known as DoH) was proposed as the standard protocol for encrypting DNS requests. It works by preventing infiltrators from accessing the information and, in some cases, making it difficult to tell the difference between a DNS request and other HTTPS traffic.

This encryption ensures that no one can tamper with a web page while you're viewing it or spy on your browsing behavior. For example, if you connect to a website, a network operator like your ISP or a public Wi-Fi hotspot can only see the domain name of the site you're reading, not the IP address itself. This keeps your browsing secure and prevents access to cybercriminals attempting to spoof the site or launch an attack.

However, DoH isn't perfect. If all DNS requests are encrypted, then admins can lose considerable visibility and control in terms of web filtering security. When applications are capable of making DNS requests independently, it defeats the value of web filtering by circumventing the in-place protections. To correctly leverage the advantages of DoH, it's important to use the right DNS protection.

An effective solution should encrypt and manage the DNS requests for the entire system, and then securely relay these requests via DoH. This way, administrators retain control of the DNS while users benefit from the additional security.

HOW TO PROTECT YOUR BUSINESS

- Work with your ISP to monitor any heavy traffic to your website
- Ensure your server capacity can handle heavy traffic spikes to prevent downtime
- Update and patch your firewalls and network security programs
- Encourage customers and employees to increase security on personal IoT devices
- Develop an incident response plan in case of a DDoS attack
- Use DNS protection and leverage professional DDoS mitigation services

Protect against DNS attacks with Webroot DNS Web Filtering!

START MY FREE TRIAL

1 ZDNet, "AWS said it mitigated a 2.3 Tbps DDoS attack, the largest ever."
2 GitHub, "February 28th DDoS incident report."
3 KrebsOnSecurity, "KrebsOnSecurity Hit With Record DDoS."
4 The 20, "The Cost of IT Downtime."
5 EfficientIP, "IDC 2019 Global Threat Report"
6 Encrypted-DNS.org, "Encrypted DNS Deployment Initiative."

About Carbonite and Webroot
Carbonite and Webroot, OpenText companies, harness the cloud and artificial intelligence to provide comprehensive cyber resilience solutions for businesses, individuals, and managed service providers. Cyber resilience means being able to stay up and running, even in the face of cyberattacks and data loss. That's why we've combined forces to provide endpoint protection, network protection, security awareness training, and data backup and disaster recovery solutions, as well as threat intelligence services used by market leading technology providers worldwide. Leveraging the power of machine learning to help protect millions of businesses and individuals, we secure the connected world. Carbonite and Webroot operate globally across North America, Europe, Australia, and Asia. Discover cyber resilience at carbonite.com and webroot.com.