DNS Attacks on the Rise: How to Defend Networks with a DNS Record History Resource

Posted on March 4, 2020

As attacks targeting the Domain Name System (DNS) continue to gain traction, they put forth the critical need for DNS security. Traditional solutions are not always adequate to mitigate the risks that DNS threats pose and typically do not guarantee DNS availability and integrity.

A reactive approach to the said threats, which include distributed denial-of-service (DDoS) attacks, can negatively impact organizations. Application downtime and business shutdowns as countermeasures reduce sales and revenue. Efforts to fix DNS security issues take up time and resources, too, which could also lead to even greater financial losses.

In light of these aspects, this post delves into the latest trends in the DNS threat landscape and what they mean to organizations. It also explains why the DNS is a lucrative attack target. But most importantly, it shows why resources like DNS Database Download are important for every company that does business online.

The Current DNS Threat Landscape Makes Knowing Your DNS Record History More Relevant

At present, the average cost of damage caused by DNS-based attacks stands at $1.07 million, which shows a 49% increase from last year's number. Aside from staggering financial losses, the affected companies also lost customer trust due to brand and reputation damage.

To illustrate this, we scoured the Web for the latest DNS threat trends and here's what we found:

- **DNS attacks have grown in sophistication:** Today's DNS-based attacks are no longer limited to distributed denial-of-service (DDoS) attacks and DNS flooding where attackers use up the target network's bandwidth by sending terabytes of requests from bots to render its site inaccessible. On top of taking sites offline, a recent DNS-based attack also enabled the perpetrators of the Sea Turtle campaign to infiltrate target networks and move laterally within them to steal troves of confidential data. An in-depth investigation into what was initially

thought to be just another domain hijacking attack revealed that the campaign was, in fact, state-sponsored and took advantage of poorly secured DNS infrastructures to take over government, telecommunications, and domain registrar networks, among others.

- **DNS attacks have become more common:** Apart from gaining sophistication, DNS threats have also grown in volume. According to the 2020 Global DNS Threat Report, there was an average of 9.5 DNS attacks faced by organizations in the past 12 months (vs. 9.45 the year before), with impacts among which in-house application and cloud service downtime.

- **DNS attacks targeted financial service providers most in 2018:** The same survey revealed that 82% of the 1,000 companies surveyed suffered a DNS attack. Most of the victims were financial service providers, but organizations from other industries were not bypassed either. Among the victims, government institutions suffered data leakages as a consequence, while manufacturers had to shut down business-critical applications to remedy the issues.

Why Does the DNS Make Such a Lucrative Attack Target?

The DNS is considered mission-critical to conducting business online. Without it, mapping a domain name to a specific IP address won't be possible. In simpler terms, potential visitors won't be able to access your sites.

When your DNS infrastructure is compromised, attackers can easily redirect web traffic that should go to your site to their own specially crafted malicious sites. They can also intercept email communications directed to your network to gather as much confidential information as they would want to. In some cases, they go to the extent of infiltrating your name servers and basically take over your site.

Security researchers opine that the best approach to dealing with DNS threats and similar attacks is to gather DNS data to serve as threat intelligence that would allow organizations to prevent threats from occurring proactively. That is where access to a comprehensive DNS database will come in handy, as it could shed light and provide detailed information about interacting domains' overall integrity.

Can Knowing Your DNS Record History Help?

The DNS threat trends above show that attacks are not likely to stop anytime soon. That is a given when attackers realize that those do work. Organizations can fight back, however, by knowing all there is to know about DNS record history:

- Use DNS Database Download to perform DNS-related searches based on your domains' activity logs to see potential attack areas and weak points.
- Gather important insights about your and business partners' DNS infrastructure by looking at your and their DNS record history.
- Make sure that all of your DNS records point to the right IP addresses and have not been misconfigured to redirect to malicious systems.
-

Our DNS record history database contains detailed information on 1 billion domains and 2 billion hostnames. With it, you can quickly uncover anomalies in your DNS infrastructure (i.e., misconfigurations and the like) that may help discover hidden attackers. You can also use it to check if a DNS server that is communicating with your network has been compromised or used for attacks in the past. If that's the case, red-flagging it for further investigation is a good idea.

If you want to know more about the DNS Database Download, feel free to contact us anytime at support@whoisxmlapi.com.