Stop Attackers from Using DNS Against You

The Domain Name System (DNS) is one of the core foundations of the internet. Every user and device in your network uses DNS to translate domain names to IP addresses, meaning it is impossible to run your business without it. Yet, DNS is often overlooked by organizations as a critical threat vector, making it an extremely tempting target for attackers. With the evolution of today's DNS-layer threats, it is more important than ever for organizations to have a solution that can secure their DNS traffic and prevent the latest attacks using DNS.

While many organizations rightfully invest significant time and resources into protecting web and email attack vectors, many security professionals don't realize the ease and prevalence of DNS abuse by attackers. In fact, many security teams don't inspect DNS traffic for threats because they assume queries sent over DNS protocol and port 53 are benign. Other organizations don't inspect DNS traffic because the sheer volume of that traffic is overwhelming, and looking for a sign of something malicious in that traffic is like looking for a needle in a haystack. This takes a great deal of time and resources—often too great an investment for organizations, especially those that assume DNS does not pose a significant threat.

DNS is a massive and often overlooked attack surface that requires the same scrutiny and protection given to web and email. It can be used for malware delivery, command and control (C2), or data exfiltration. Adversaries take advantage of the ubiquitous nature of DNS to abuse it at multiple points of an attack. According to the Palo Alto Networks Unit 42 Threat Research team, almost 85% of malware abuses DNS for malicious activity. Attackers establish reliable command channels that are difficult to take down or identify since DNS is such a reliable way to maintain a connection to DNS servers. As adversaries increasingly automate their attacks, it becomes almost impossible to secure your DNS traffic if you do not have the right solution in place.

At the same time, many security teams lack visibility into DNS traffic and how threats abuse DNS to maintain control of infected devices. Security teams are under pressure to enforce consistent protections for millions of new malicious domains while keeping up with advanced tactics like DNS tunneling and strategically aged domains. In addition to how prevalent and easy it is to abuse DNS, the sheer rate and volume of new malicious domains are enormous, and static signatures cannot be created quickly enough to keep up. If a system gets infected, networking and security teams struggle to quickly identify that system and address the infection. By then, malware may have already spread, or data may have already been stolen.

85%

of malware abuses DNS for malicious activity

– Unit 42 research on DNS traffic

Top Three Attacks Using DNS

DNS is your network's first line of defense against modern threats, and it is critical to understand how adversaries abuse it to carry out attacks. Here are the top three ways cybercriminals abuse DNS to mask their C2 activity so they can deliver additional malware or steal data.

Malware Using DNS for C2

This is one of the most typical ways attackers take advantage of DNS. Attackers use common network protocols, including DNS, to spread malicious code. Malware can be sent to users through online ads, malicious URLs in emails, or other means. Once a user's computer is infected, the system sends a DNS request back to the attacker's control server. In this way, the infected computer becomes a bot the attacker can control. The malware can then steal personal or financial data and spread very quickly by issuing instructions to scan the network for other computers.

Recently, the hacker group WINDSHIFT launched a cyberattack that used DNS for C2 against government departments and critical infrastructure in the Middle East. To learn the technical details and timeline, read Unit 42's research on the WINDSHIFT attacks.

Malware Using Domain Generation Algorithms

Effective and growing quickly, domain generation algorithms (DGAs) randomly generate large numbers of slightly different domain names. A DGA can, for instance, create thousands of domains in a day that are each a slight variation of www[.]bigbadguys[.]com. Attackers developed DGAs so that malware can generate these domains and use them for C2. Unit 42 has observed that 18% of malware uses DGAs to automatically create thousands of C2 domains every day—of which attackers may use one—so that defenders can't block them. Malicious domains controlled by attackers enable rapid movement of C2 channels from point to point, bypassing traditional security controls like block lists or web reputation filtering. Infected computers contact some of these new domain names to receive commands and updates. A key aspect of DGAs is that, even though thousands of domains can be generated in short order, not all of them need to be registered.

DGAs offer an effective means for attackers to hide the locations of their C2 centers, which they use for financial fraud, identity theft, and other malicious activities. To learn more about DGAs, read Unit 42's DGA threat brief.

Attacks using DNS are effective and growing. Malware using domain generation algorithms (DGA) has grown **124%** year over year

– Unit 42 research on domain generation algorithms

DNS Tunneling

This technique, increasingly used by advanced persistent threat (APT) actors, lets attackers encode their payloads in small chunks within DNS requests to bypass security controls. Advanced attackers use DNS tunneling to hide data theft or C2 in standard DNS traffic. Once a victim's device is compromised, the infected device sends a request within the DNS traffic. The DNS server is instructed to connect to the cybercriminals' server, establishing a channel through which to steal and transmit data. With DNS tunneling, DNS requests pass through the normal DNS server, inside and outside a company's firewall. However, tunneled data hidden in the DNS requests go unnoticed. Attackers, including the threat group OilRig, have used DNS tunneling extensively in recent years.

Why Current Security Approaches Fail

Traditional security solutions cannot prevent modern DNS-layer attacks for several reasons. To begin with, it is difficult to address the many ways attackers can use DNS to compromise an organization. Many organizations focus solely on protecting their DNS infrastructure—and rightfully so. If DNS goes down, they can no longer access the internet. What they don't focus on is the hidden threat—attackers using the traffic within DNS to carry out attacks. Some organizations do nothing at all to secure their DNS traffic, leaving it wide open for attackers. Many organizations don't have DNS monitoring and instead only block malicious domains, essentially doing nothing to address malware that abuses DNS.

Other security teams take a block listing approach to block attacks that use DNS by relying on static block lists of known malicious threats that prevent known bad domains. However, as malware's use of DGA grows, the effectiveness of blocking known malicious domains alone becomes more limited. Using a list of randomly generated domains for C2 can overwhelm the signature capability of legacy tools and traditional security approaches. A limited set of signatures simply cannot scale to meet the growing threat of DNS-based attacks.

Additionally, relying on static lists limits the amount of context defenders can access to fully understand the attacks against their network. Although threat intelligence feeds are regularly updated with indicators or artifacts derived from a source outside the organization, daily, or even hourly updates are too slow to keep up with the massive amount of DNS data. The sheer volume of DNS data means defenders simply lack the visibility and resources to perform a deep inspection of their DNS traffic. With traditional approaches, security teams don't have the resources to be proactive or scale their DNS security.

Some organizations use standalone point products to address threats to their DNS. These tools may adequately address specific facets of DNS security, but even "best-in-class" technologies come with limitations. For instance, these tools often require changes to DNS infrastructure if they are to work effectively. Disparate products also create silos of threat intelligence and data that may not work with other areas of an organization's security structure. As a result, overwhelmed teams drown in uncoordinated data from independent tools. Multiple tools become more things to own and manage, adding complexity and draining already limited resources.

Unit 42 Threat Research on the SolarStorm Supply Chain Attack

In December of 2020, SolarWinds, a company that provides IT management and tools and services for network and infrastructure monitoring to over 33,000 customers worldwide, was a victim of a supply chain attack on their SolarWinds Orion® software. This attack involved malicious code being infiltrated within the legitimate IT performance and statistics monitoring software, Orion, and affected over 18,000 customers around the world. Attackers were able to gain access to customer networks, systems, and data, allowing them to tunnel malware and steal sensitive information.

In order to carry out this attack, the threat actors of this campaign registered domains in 2019 and left them dormant for over a year before using them in their attack. By leaving these domains dormant, they were able to bypass reputation-based checking done by security vendors. During this dormant phase, the SUNBURST trojan periodically contacted its C2 domain to report status and receive commands. When the C2 domain was finally activated, the majority of burst DNS requests were for new subdomains. The trojan dynamically constructed these hostnames with DGAs to tunnel sensitive data out of the victim's network. Get the full details of the SolarStorm supply chain attack from Unit 42's blog post.

Stop Attackers from Using DNS Against You

With the Palo Alto Networks DNS Security subscription, you can secure your DNS traffic and protect your organization from the latest attacks using DNS.

Security Data and Lots of It

You need massive quantities of real-world security data, either data you've collected yourself or gathered through threat intelligence or cyberthreat alliances. With data from a large and expanding intelligence-sharing community, your protection will continue to grow.

Predictive Analytics and Machine Learning

Organizations today need a solution that can analyze real-world threat data in order to prevent today's most sophisticated DNS-based attacks in real time. And without these analytics, it is impossible to predict highly dynamic malicious domains. DNS Security uses predictive analytics to apply machine learning-based protections that can predict never-before-seen domains and prevent dynamic DNS-layer threat techniques, all in real time. Behavioral analytics can also help security teams determine a baseline of activity, understand general patterns, and find what is normal. When your security team sees signals that require action, they will be able to assess how manual or automated that action should be, allowing them to better prioritize time and resources.

Native Integration with Our Next-Generation Firewall

Because many DNS-based attacks happen so quickly, it is imperative that security teams spend less time manually responding to attacks. To stand a chance, defenders need automation. Automation can help quickly determine infected machines, automate responses, and contain threats before they spread to other areas of a network. Security teams need integrated innovations that extend the value of existing security investments without complicating operations. DNS Security seamlessly integrates with Palo Alto Networks Next-Generation Firewalls (NGFWs) and Prisma® Access, allowing you to secure your DNS traffic across all users and locations with no changes to your DNS infrastructure. This includes any DNS traffic that may go to an internet resolver or malicious DNS server.

Cloud-Based Protection

With DNS Security being built on a modular, cloud-based architecture, your DNS protections can scale infinitely and always stay up to date. These cloud-based innovations allow your security team to develop and deploy new detections in real time, stopping the latest attacks using DNS. By being in the cloud, these detections are updated instantly, meaning your security operations center (SOC) team doesn't need to worry about updating or making any changes to your software.

No Standalone Point Products

Security teams that use disparate tools struggle to keep up with the sophistication of DNS-layer attacks. These tools are poorly integrated and weren't designed for automation, meaning security teams are forced to manually stitch together insights from multiple disparate sources before taking action on threats. These products also lack the ability to share data or insights across your security stack, resulting in slower response times to threats. DNS Security allows you to maximize your operational efficiency by securing the DNS traffic across your network through a single platform. By eliminating the need for independent tools, organizations can save an average of $9.9 million per year on infrastructure costs.

Full Visibility and Context for DNS Traffic

To protect against threats over DNS, it is critical that you empower your security personnel with complete visibility and context of your DNS traffic. These insights allow security teams to better understand why a domain was blocked, and the history of that domain and easily identify malicious and benign traffic trends. By giving you full visibility and context of your DNS traffic, DNS Security can secure the DNS traffic across your entire network, including unexpected DNS resolvers and malicious servers.

Category-Based Actions

Different types of DNS-based threats require a different course of action. For example, malware may require simple blocking and alerting, while C2 requires sinkholing as well as identification, quarantining, and inspection of potentially infected endpoints. In order to prevent threats in real time and reduce risk exposure, security teams need automated responses based on DNS traffic categories to enable fine-grained control over DNS traffic. DNS Security uses machine learning capabilities to rapidly detect and categorize threats over DNS. All DNS queries are checked against our scalable cloud database in real time to determine appropriate enforcement actions.

DNS Security Best Practices

In addition to deploying the right technology, there are other best practices your organization can follow to protect your network from DNS-based threats.

Train and Educate Your Security Staff

Implement a security education and awareness program to train your staff to identify malicious threats. Encourage them to take precautions when following links to avoid installing malware. Phishing training can help them learn to recognize, avoid, and report email-based attacks.

Implement a Threat Intel Program

Understand the threat landscape and set up a threat intelligence program to be aware of the different types of threats and techniques attackers are using today. With this knowledge, you can ensure you have the right technology stack to keep your network safe.

Learn What DNS Data Can Tell You

Don't just look at DNS traffic. Collecting DNS data logs has little value unless you understand what you're looking at. By understanding the data, you can successfully prevent your organization from never-before-seen DNS-layer threats.

Don't Rely on a DNS Resolver

If a DNS server is compromised, it may feed you false responses meant to direct your traffic to other compromised systems or enable a man-in-the-middle attack.

Plan for the Risk of Remote Work

Develop a strategy for your remote workforce as they can put sensitive company data at risk. Warn them against using unsecured, free, or public Wi-Fi as adversaries can easily put themselves between employees and the connection point. Integrate multi-factor authentication and prepare for the risk of devices being lost or stolen.

Approach Network Security Holistically

Take a holistic approach to network security and ensure you have the right capabilities that can address various threat vectors in your network and can be easily integrated within your entire security stack. When evaluating vendor solutions, it's important to make direct comparisons in proof of concepts. Every environment is different, and independent vendor-neutral testing for DNS-layer security has not yet been established.

Automate Responses and Not Just Alerts

To successfully protect your organization, you need automated responses and not just alerts. The speed at which threats are carried out makes alerts and signals ineffective. By the time a threat has been identified, it may already be too late. Your security team needs to be able to automatically determine threats and quarantine potentially infected systems before more damage is done. In order to ensure your organization is following best practices and optimizing Palo Alto Networks DNS Security service, take a Best Practice Assessment.

paloalto® NETWORKS

3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com