DARKReading

MAY 2023

Sponsored by

infoblox

Everything You Need to Know About DNS Attacks (But Were Afraid to Ask)

It's important to understand DNS, potential attacks against it, and the tools and techniques required to defend DNS infrastructure.

INSIDE:

Brought to you by
informa
tech

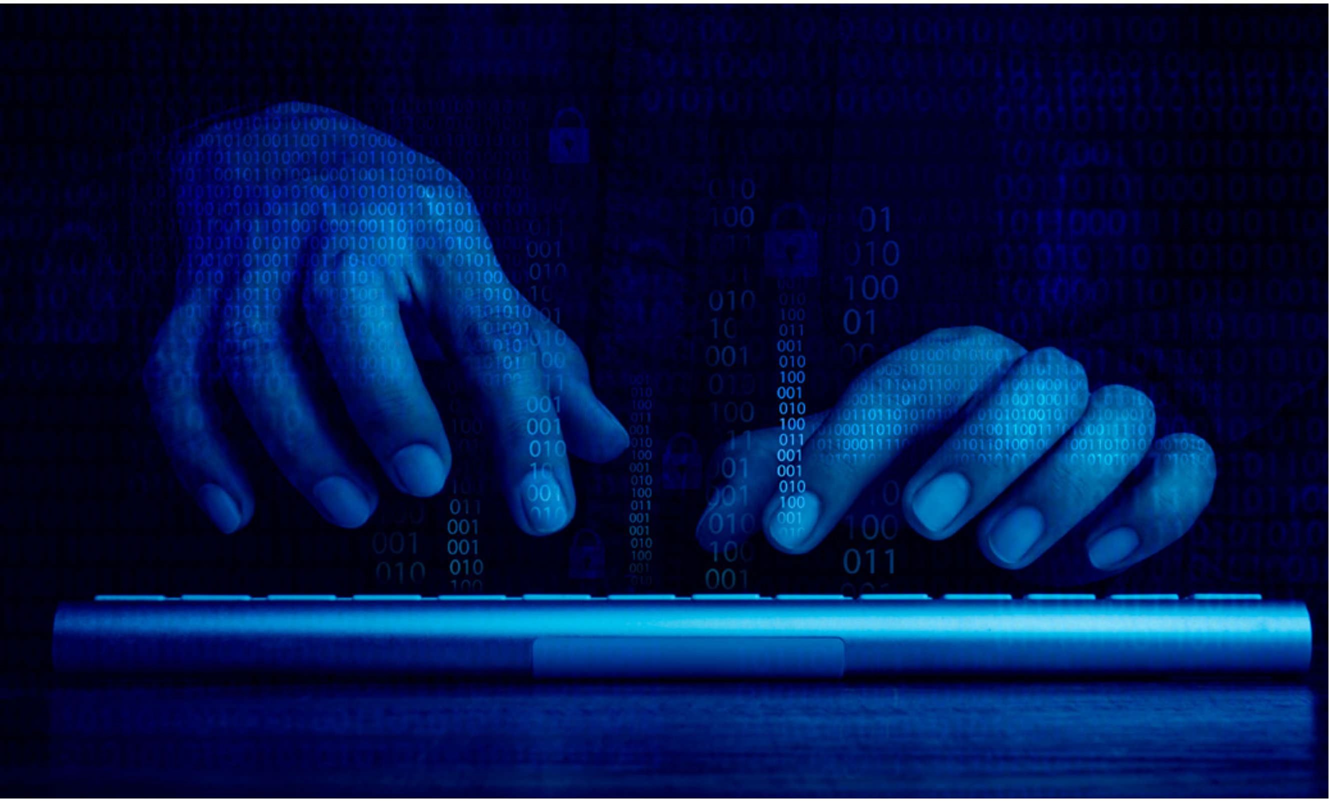
Next

FEATURE

Everything You Need to Know About DNS Attacks (But Were Afraid to Ask)

It’s important to understand DNS, potential attacks against it, and the tools and techniques required to defend DNS infrastructure.

By Ericka Chickowski, Contributing Writer, Dark Reading



Domain Name Service (DNS) is a critical part of any organization’s digital infrastructure, but it’s also one of the least understood. DNS is simple to use, but many security teams struggle to protect DNS because of the sheer complexity and diversity of attacks against it.

“Traditionally, DNS is seen as a simple service working in the background. Oftentimes, nobody takes notice, and nobody wants to touch it,” says Ivan Ristic, chief scientist for Red Sift and a veteran expert in securing network protocols. “Like all infrastructure, it is only acknowledged if it doesn’t work.”

DNS is designed to be invisible to business professionals, most IT stakeholders, and even many security professionals, but DNS’s threat surface is anything but simple. Adversaries are taking advantage and lodging extremely ingenious, multifaceted, and voluminous attacks against DNS. And they’re causing a great deal of damage and costing companies a lot of money. DNS attacks are on the rise, and the cost of a successful DNS attack can exceed more than $1 million. Enterprise organizations cannot afford to discount the importance of investing in DNS-specific security measures.

The DNS Security Awareness Problem

Often described as the “phonebook” of the Internet, DNS effectively takes the domain name of the entity a user is trying to connect to, looks up the IP address of the entity, and connects the user to resources at that IP. As organizations’ IP addresses change, DNS looks up the new numbers. DNS works behind the scenes to ensure that users can trust that they are connecting to the right resources.

DNS is great when it works, but its downfall from a cybersecurity perspective is that it depends on an “implied implicit trust,” says Steve Benton, vice president of threat research at Anomali. Things go wrong when an attacker can subvert that process and either deny the use of DNS to legitimate users or services or, worse, manipulate and falsify the DNS lookup response, he explains.

“Once the attacker is controlling the communication, you see the criminal and malicious opportunities are almost boundless,” Benton says.

Protecting DNS from the highly variable types of attacks waged against it can be extremely complex and involve a lot of moving parts. These demands, coupled with the perceived simplicity of DNS, can lead to a mismatch in expectations and resources that can leave DNS architecture wide open to attack. With so many other priorities on the cybersecurity road map — from firewalling and segmentation to vulnerability management and application security — DNS keeps getting moved down the priority list, explains Alex Spivakovsky, vice president of research at Pentera, a penetration testing firm.

“With so much to worry about, [cybersecurity pros] have other priorities that take precedence,” he says.

Many times, too, organizations make the flawed assumption that their other security investments will automatically mitigate DNS risks.

“Most organizations protect other traffic layers, including Web and email, and assume DNS traffic is inherently protected. But it is not,” says Mark Sangster, chief of strategy for Adlumin, a security operations center (SOC) platform provider and managed detection and response firm. “In fact, DNS attacks are one of the most common tactics criminals use to infiltrate organizations with malware or conduct reconnaissance.”

> “DNS is great when it works, but its downfall from a cybersecurity perspective is that it depends on an “implied implicit trust,” says Anomali’s Steve Benton.

According to the 2022 Global DNS Threat Report, 88% of organizations have reported one or more DNS attacks on their business in the last year. When successful, the cost of a DNS attack averages about $942,000, the report states.

The volume and variety of attacks stems from the fact that attackers are aware of a pervasive lack of DNS hygiene or security controls, says Andrew Douglas, a Deloitte Risk & Financial Advisory managing director in cybersecurity who also leads the firm’s US attack surface management team.

“Since some organizations treat DNS security as a lower-level issue, likely permitted through apathy more than anything, adversaries bide their time and watch as deprioritized DNS systems drift away from secure states over time,” Douglas says.

Understanding the DNS Threat Environment

Before tackling what it will take to overcome the DNS security awareness gap, it’s crucial to understand the attacks at hand, Pentera’s Spivakovsky says.

“Ultimately, spending money and resources on DNS security solutions, without understanding the vectors that expose you to risk, is not effective,” he says. “You need to understand how a hacker can exploit DNS, and from there you can start to build effective security protocols

that will actually hinder them."

While not an exhaustive list, the following are five of the most common or impactful DNS attack techniques cited by experts.

Denial of Service

As with many other communication protocols, attackers love to abuse DNS to carry out denial-of-service (DoS) and distributed denial-of-service (DDoS) attacks. Flood attacks are among the most disruptive direct attacks against DNS infrastructure. Flood attacks pummel DNS with so many requests that an organization depending on the DNS service literally cannot operate, Benton says.

"This can be inconvenient at best and potentially catastrophic in the extreme when business and supporting systems cannot talk to one another," he says.

Of the DDoS subclasses targeting DNS, one of the most dangerous is called the DNS water torture attack, also referred to as a pseudo-random subdomain (PRSD) attack.

"DNS water-torture attacks were first made well known by a botnet called Mirai and are denial-of-service attacks that target authoritative DNS servers. An authoritative DNS server is the server that the resolver talks to in order to get answers for a domain and is typically run by the owner of a domain," explains Mark Dehus, director of information security and threat intelligence for Lumen Technologies. Dehys says water-torture attacks were most notably used in the 2016 attack against DynDNS and have since become part of attackers' common playbooks. "This attack creates a significant load on the authoritative DNS server and prevents it from serving legitimate requests," he adds.

In addition, organizations' own DNS infrastructure can be used as part of broader attack against other organizations. With DNS amplification attacks like water torture, attackers send a flood of DNS requests to different public DNS resolvers whose single return address is the victim's infrastructure.

"It's like calling up a few hundred pizza restaurants, requesting pizza delivered to a victim's address, and the poor victim is left with a mess to sort out," Dehus explains. "While this attack may not negatively impact the DNS infrastructure itself, it enables threats to leverage the DNS infrastructure to knock victims off the Internet.

DNS Cache Poisoning

Another very common attack that enterprises struggle with is DNS cache poisoning, used by attackers to spoof DNS. This attack enables cybercriminals to redirect users or systems looking up legitimate sites to different and malicious IP addresses.

"The challenging part of this type of attack is that, often, the user does not recognize that there is an issue as the site that they are redirected to has been made to look very similar to the site they were attempting to visit," says George Jones, CISO at managed detection and response (MDR) cybersecurity solutions provider Critical Start. "What makes this challenging is that most users do not verify IP addresses of the sites they are visiting and, if they are not diligent, can become a victim of compromised data."

DNS Hijacking

Another path to spoofing is DNS hijacking.

"DNS hijacking attacks redirect users to malicious sites by changing the DNS records of a domain," says Anthony James, vice president of product solutions at Infoblox. "These attacks can be initiated by compromising the DNS registrar or using social engineering to obtain credentials. Defending against DNS hijacking is difficult."

More than 90% of malware use DNS to progress an attack at some point in the life cycle.

Often, these attacks are combined with other advanced techniques to carry out some very nasty attacks, particularly those used by advanced persistent threat (APT) groups.

"I've seen interesting attacks occur due to malicious actors abusing DNS," says Craig Jones, vice president of security operations at Ontinue, an MDR provider. "The worst attack was against a compromised firewall along with DNS hijacking to collect credentials and to redirect users to pro-Chinese propaganda. These techniques have been used extensively by APT groups controlling network infrastructure."

DNS Tunneling

DNS tunneling attacks leverage DNS infrastructure for outbound communications.

"Once a hacker has injected malware into your organization, what they need is a reliable channel to communicate with the malware and exfiltrate data they discover. During a tunneling attack, hackers take advantage of DNS to create this communication channel," says Pentera's Spivakovsky. "[The DNS communications channels] appear like legitimate traffic, allowing them to bypass most traditional firewalls. This type of attack leaves a very small footprint, as it appears legitimate to defenses, making it difficult to identify and prevent."

"Attackers can use DNS to communicate with infected systems, deliver malware payloads, or download additional malware components," says Infoblox's James, noting that there are many kinds of DNS-based malware tools. "Recent reports state that more than 90% of malware use DNS to progress an attack at some point in the life cycle."

Dangling DNS

Another increasingly common attack is called dangling DNS, a subdomain takeover that can be used to gain control of a slice of an organization's DNS infrastructure.

These attacks are piggybacking on the rise of cloud computing, says Red Sift's Ristic, who explains that a dangling DNS attack starts after a victim organization points its subdomain to a resource on a cloud provider and decommissions the cloud resource but still leaves the subdomain open and pointing to a nonexistent resource. Ristic's firm found that within one segment of the financial services vertical, some 60% of firms had a dangling DNS issue.

"Unfortunately, it is relatively easy for an attacker to recreate such a resource at the cloud platform, subsequently obtaining access to all traffic to the subdomain," Ristic says. "This allows an attacker access to internal cookies and enables lateral movement in the victim's organization.

Critical Start's Jones explains it's also yet another path to impersonate the brand.

"Due to the fact that the original owner no longer has authority over the domain name, an attacker can use it to acquire the trust of unwary users in order to steal sensitive data or carry out other illegal operations," he says. "They use it to send specific phishing emails or point users to a website they control."

Effective DNS Hardening Measures and Controls

Due to the DNS security awareness gap and the resulting lack of resources dedicated to DNS-specific security, DNS cyber readiness remains shaky at many organizations. To stop attacks on DNS, some organizations simply "pull the plug" on DNS or other infrastructure, according to the 2022 Global DNS Report. In the face of an attack, nearly one in five organizations either shuts down the DNS server or service or disables applications. And 25% say they go so far as to shut down all or part of their network infrastructure.

But it doesn't have to be that way. Security experts say organizations can more efficiently and effectively prepare for these attacks by shoring up security hygiene around DNS infrastructure. Organizations can use protocols like DNSSEC (Domain Name System Security Extensions) and controls like DNS firewalls. They can also systematically layer monitoring and DNS-specific controls into their programs. It's not necessarily an easy or simple process, but it is possible to make incremental improvements that will result in a more complete DNS defense strategy.

"No single measure will provide any organization total protection from a DNS attack, due to DNS's pervasive use in most organizations and the decades of research and exploitation of DNS systems by adversaries," says Deloitte's Douglas. "But there are ways to optimize security controls to make your organization less of a target and to help minimize negative impacts if your organization is victimized."

> At the most fundamental level, organizations need to be more methodical and systematic about how they manage their DNS registrations.

Hardening

At the most fundamental level, organizations need to be more methodical and systematic about how they manage their DNS registrations, experts agree.

"Organizations need to care about their own domain registrations," says Anomali's Benton. Organizations that can't be bothered to register domains and potential domains that can be used by indirect DNS lookalike attacks (such as typosquatting and homoglyph attacks) "have no business being on the Internet," he adds.

Similarly, organizations need to be regularly reviewing their DNS records, says Brad Liggett, US director of cybersecurity for Cybersixgill.

"Regular review of DNS configuration and zone records is mandatory. Even if DNS is outsourced to a provider, it's best to ensure records are kept up to date," he says.

Benton agrees. Failing to tidy up at the end of the life cycle of a piece of DNS infrastructure is a recipe for creating security blind spots that aren't maintained or monitored and are "ripe for exploitation," he says.

Liggett also recommends organizations think about how they employ wildcard DNS records, which make it easier to generate subdomains on the fly and are frequently used in development and test environments. Liggett isn't a fan of DNS wildcards, and he says that clamping down on the practice is a good way to limit exposure to things like dangling DNS attacks and to stymie attacker reconnaissance.

"While one might argue that in a dynamic environment [DNS wildcards are] a necessity, this will often result in unintended consequences," he says. "In my view, allowing teams to put test and QA environments out in the open gives attackers with malicious intent the ability to map out naming conventions and build architecture maps of the targeted organization."

DNS configuration is also crucial. Indeed, when it comes to protecting DNS servers, all the security basics apply. Organizations should regularly patch DNS servers, for example, and bolster policy and enforcement around open resolvers, which are a common target for amplification attacks. Open resolvers are recursive DNS servers that respond to any query from any source address, says Gary Sockrider, director of security solutions for Netscout.

Open resolvers "are often placed into service unwittingly by admins putting generic servers on the Internet for hosting or other purposes without understanding the need to either disable the DNS functionality or secure it," he explains. "Identifying and remediating open resolvers is not only relatively simple and inexpensive, but also contributes to a safer environment for everyone."

Finally, don't skimp on security policy and controls around DNS administrative tooling. Benton says DNS and its administration should be treated as one of the highest "privileged user" activities in the organization. This means accounts need to be tied to an individual, with strict enforcement of role-based access and visible monitoring and auditing capabilities baked in.

DNSSEC

The use of DNSSEC, developed more than 20 years ago to remedy some of the inherent security design flaws in DNS, is still lagging due to complexity and resource constraints around deploying and maintaining the infrastructure using the protocol. The Asia-Pacific Network Information Center, which tracks global DNSSEC validation rates, notes that only 31% of servers worldwide use the protocol. Increasing use of the protocol could help organizations make a dent in the risk of attacks like DNS hijacking and cache poisoning, according to Douglas.

"To prevent DNS spoofing attacks, organizations can implement DNSSEC to restrict the scope of systems served by DNS systems wherever possible and to monitor DNS system use as part of broader cyber risk management efforts," he explains.

Controls and Monitoring

In addition to hardening measures, organizations should consider DNS-specific tooling. This includes enforcement tools like DNS firewalls, which filter and block malicious DNS requests; DNS sinkholes, which send DNS requests for malicious domains to honeypots for further analysis;

and DNS monitoring and analytics platforms, which offer better visibility into DNS traffic and provide real-time alerts and reporting that can speed detection and recovery from attacks, says Infoblox's James.

That monitoring and filtering capability is a must-have in today's DNS threat environment, says Abhinav Singh, a security researcher at Normalyze, who explains that the former feeds the latter: Good filtering is only possible with monitoring that can help an organization establish baselines of what normal activity looks like.

"Monitoring and filtering can never be completely done in a single day or year. It's a continuous learning and improvement process," Singh says. "You can do a good job of filtering out rogue DNS traffic only when you have strong monitoring practices around DNS built over the years. So, the sooner you start, the more knowledge you'll capture about your DNS infrastructure."

Strategic DNS investment can be especially useful in the shift to cloud-native infrastructure.

Some experts, including Benton, maintain that DNS security is best managed by a third party.

"The best 'tool' is to actually switch to a large cloud provider of DNS. Sounds like I'm saying to security teams to throw the towel in on this one — that's not what I mean," he says. "Smart security teams use intelligence and attack vector knowledge to assess the threat and risk to their organization and make informed build/buy decisions. This is one of them, and, honestly, given the business criticality of DNS and the evolving threat landscape, it's one to buy, not build."

Using DNS Visibility as a Security Tool

Investing in strong DNS monitoring and visibility capabilities can help security teams get a handle on not only DNS attacks but also a whole host of security incidents across the entire IT infrastructure.

Strategic DNS investment can be especially useful in the shift to cloud-native infrastructure. Traditionally, security incident response teams have long viewed network flow data as their go-to tool for tracking attacker behavior, says David Ratner, CEO of threat intelligence firm Hyas. However, NetFlow has becomes less effective as organizations move traffic to the cloud, he says. Security teams can't rely on netflow data as much as they used to.

"Administrators and security teams can regain visibility into their own networks with DNS telemetry," Ratner says. "It is easier and cheaper to monitor than flow data and can identify unknown, anomalous, or malicious domains based on threat intelligence data."

Organizations can increase ROI when data collected from DNS monitoring tools is also served to incident responders through SIEM (security information and event management) and other SOC tooling. This is definitely a growth opportunity for most organizations: 75% of organizations collect DNS traffic data, according to IDC, but only 23% of that telemetry is sent to SIEM platforms.

Ideally, security teams should also be looking for tooling that effectively contextualizes DNS data with other important data flows, says James. For example, DNS detection and response tools leverage what's called DDI data — a combination of DNS, DHCP, and IPAM data streams.

"This contextual data can save your security team hours of hunting through log files to associate an IP with

a user and a particular incident of compromise," says James, who adds that pairing this data with threat intelligence enriches the streams with timely information about malicious hostnames, domains, and IP addresses.

"The lack of adequate knowledge and awareness around DNS attacks is a limiting factor across these teams — and they may not see the issues in the same way — so a lack of unity and cohesion can arise," he says. "The root can be skills-based but also a factor of limited security resources spread too thinly across everything they have to master for their organization."

> All the tooling and controls in the world aren't worth a hill of beans without the resources and expertise available to run it all.

Recommendation: Build a Team

Finally, organizations need to remember that all the tooling and controls in the world aren't worth a hill of beans without the resources and expertise available to run it all.

"Organizations should have SMEs [subject matter experts] who understand the network-level implementation of security best practices that can form the stepping stones for long-term success against complex DNS or network-based attacks," Singh says.

One of the most common challenges that organizations face is that DNS security touches so many IT specialties, including networking and DevOps, according to Benton. Organizations should therefore consider creating cross-disciplinary teams and looking for opportunities for DNS experts to share their knowledge with stakeholders among these teams.

About the Author: *Ericka Chickowski specializes in coverage of information technology and business innovation. She has focused on information security for the better part of a decade and regularly writes about the security industry as a contributor to Dark Reading.*

3 Ways Attackers Bypass Cloud Security

At Black Hat Europe, a security researcher details the main evasion techniques attackers are currently using in the cloud.

By Kelly Jackson Higgins, Editor-in-Chief, Dark Reading

BLACK HAT EUROPE 2022 – London - CoinStomp. Watchdog. Denonia.

These cyberattack campaigns are among the most prolific threats today targeting cloud systems — and their ability to evade detection should serve as a cautionary tale of potential threats to come, according to a security researcher at Black Hat Europe.

"Recent cloud-focused malware campaigns have demonstrated that adversary groups have intimate knowledge of cloud technologies and their security mechanisms. And not only that, they are using that to their advantage," said Matt Muir, threat intelligence engineer for Cado Security, who shared details on those three campaigns his team has studied.

While the three attack campaigns are all about cryptomining at this point, some of their techniques could be used for more nefarious purposes. And for the most part, these and other attacks Muir's team has seen are exploiting misconfigured cloud settings and other mistakes. That for the most part means defending against them lands in the cloud customer camp, according to Muir.

"Realistically for these kinds of attacks, it has more to do with the user than the [cloud] service provider," Muir tells Dark Reading. "They are very opportunistic. The majority of attacks we see have more to do with mistakes" by the cloud customer.

Perhaps the most interesting development with these attacks is that they are now targeting serverless computing and containers, he said. "The ease of which cloud resources can be compromised has made the cloud an easy target," he said in his presentation, "Real-World Detection Evasion Techniques in the Cloud."

DoH, It's a Cryptominer

Denonia malware targets AWS Lambda serverless environments in the cloud. "We believe it's the first publicly disclosed malware sample to target serverless environments," Muir said. While the campaign itself is about cryptomining, the attackers employ some advanced command and control methods that indicate they're well-studied in cloud technology.

The Denonia attackers employ a protocol that implements DNS over HTTPS (aka DoH), which sends DNS queries over HTTPS to DoH-based resolver servers. That gives the attackers a way to hide within encrypted traffic such that AWS can't view their malicious DNS lookups. "It's not the first malware making use of DoH, but it certainly isn't a common occurrence," Muir said. "This prevents the malware to trigger an alert" with AWS.

The attackers also appeared to have tossed in more diversions to distract or confuse security analysts, thousands of lines of user agent HTTPS request strings.

"At first we thought it might be a botnet or DDoS ... but in our analysis it was not actually used by malware" and instead was a way to pad the binary in order to evade endpoint detection and response (EDR) tools and malware analysis, he said.

More Cryptojacking With CoinStomp and Watchdog

CoinStomp is cloud-native malware targeting cloud security providers in Asia for cryptojacking purposes. Its main modus operandi is timestamp manipulation as an anti-forensics technique, as well as removing system cryptographic policies. It also uses a C2 family based on a dev/TCP reverse shell to blend into cloud systems' Unix environments.

Watchdog, meanwhile, has been around since 2019 and is one of the more prominent cloud-focused threat groups, Muir noted. "They are opportunistic in exploiting cloud misconfiguration, [detecting those mistakes] by mass scanning."

The attackers also rely on old-school steganography to evade detection, hiding their malware behind image files.

"We're at an interesting point in cloud malware research," Muir concluded. "Campaigns still are lacking somewhat in technicality, which is good news for defenders."

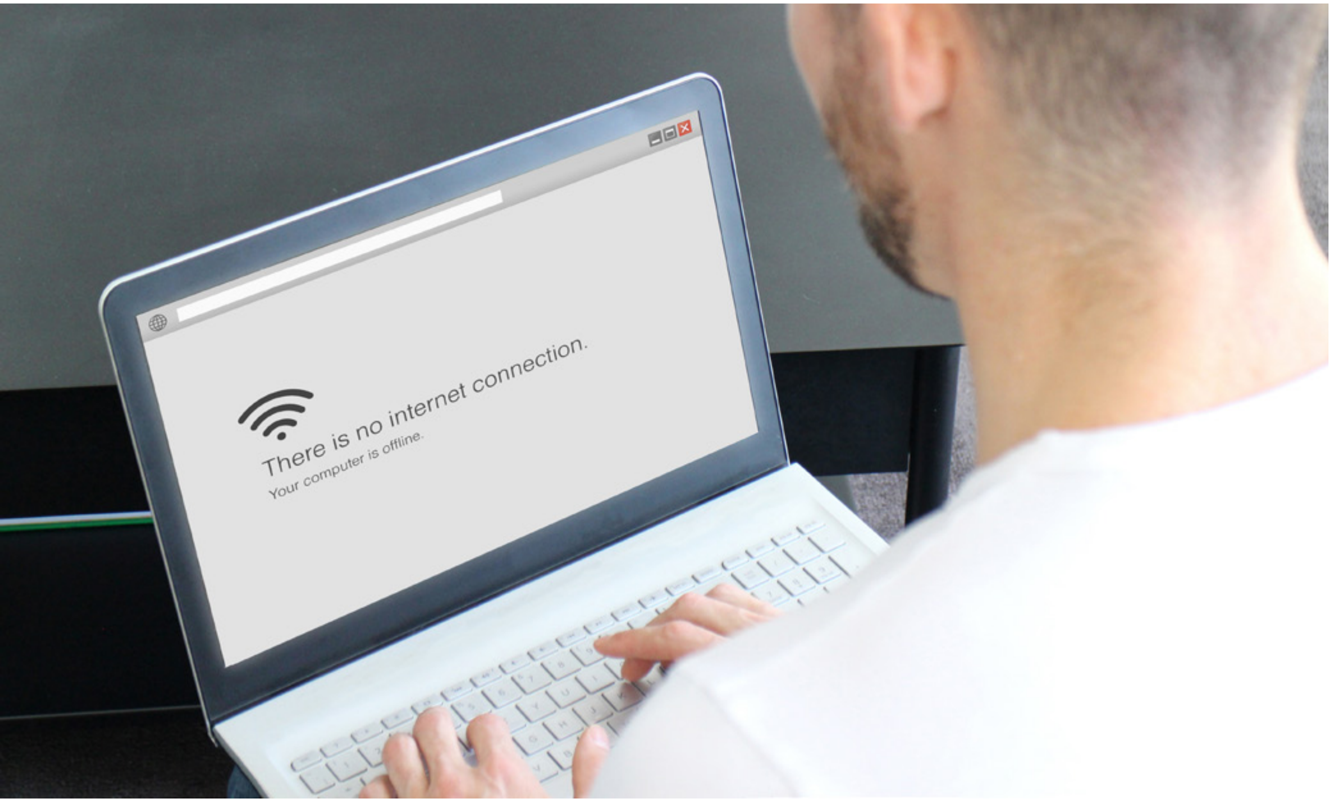
But there's more to come. "Threat actors are becoming more sophisticated" and likely will move from cryptomining to more damaging attacks, according to Muir.

About the Author: ***Kelly Jackson Higgins is an award-winning veteran technology and business journalist with more than two decades of experience in reporting and editing for various publications, including Network Computing, Secure Enterprise Magazine, Virginia Business magazine, and other major media properties.***

Report: Air-Gapped Networks Vulnerable to DNS Attacks

Common mistakes in network configuration can jeopardize the security of highly protected assets and allow attackers to steal critical data from the enterprise.

By Elizabeth Montalbano, Contributor, Dark Reading



Common misconfigurations in how Domain Name System (DNS) is implemented in an enterprise environment can put air-gapped networks and the high-value assets they are aimed at protecting at risk from external attackers, researchers have found.

Organizations using air-gapped networks that connect to DNS servers can inadvertently expose the assets to threat actors, resulting in high-impact data breaches, researchers from security firm Pentera revealed in a blog post on Dec. 8.

Attackers can use DNS as a command-and-control (C2) channel to communicate with these networks through DNS servers connected to the Internet, and thus breach them even when an organization believes the network is successfully isolated, the researchers revealed.

Air-gapped networks are segregated without access to the Internet from the common user network in a business or enterprise IT environment. They are designed this way to protect an organization's "crown jewels," the researchers wrote, using VPN, SSL VPN, or the users' network via a jump box for someone to gain access to them.

However, these networks still require DNS services, which is used to assign names to systems for network discoverability. This represents a vulnerability if DNS is not configured carefully by network administrators.

Previous Next

"Our research showcases how DNS misconfigurations can inadvertently impact the integrity of air-gapped networks," says Uriel Gabay, cyberattack researcher at Pentera.

What this means for the enterprise is that by abusing DNS, hackers have a stable communication line into an air-gapped network, allowing them to exfiltrate sensitive data while their activity appears completely legitimate to an organization's security protocols, Gabay says.

DNS as a Highly Misconfigurable Protocol

The most common mistake companies make when setting up an air-gapped network is to believe they are creating an effective air gap when they chain it to their local DNS servers, Gabay says. In many cases, these servers can be linked to public DNS servers, which means "they have unintentionally broken their own air gap."

It's important to understand how DNS works to know how attackers can navigate its complexities to break into an air gap, the researchers explained in their post.

Sending information over DNS can be done by requesting a record that the protocol handles — such as TXT, a text record, or NS, a name server record — and putting the information into the first part of the record's name, the researchers explained. Receiving information over DNS can be done by requesting a TXT record and receiving a text response back for that record.

While DNS protocol can run on TCP, it is mostly based on UDP, which does not have a built-in security mechanism — one of two key factors that come into play for an attacker to take advantage of DNS, the researchers said. There also is no control over the flow or sequence of data transmission in UDP.

Thanks to this lack of error detection in UDP, attackers can compress a payload prior to sending it and immediately decompress after sending, which can be done with any other type of encoding, such as Base64, the researchers explained.

Using DNS to Break an Air Gap

That said, there are challenges for threat actors to communicate successfully with DNS to break an air gap. DNS has restrictions on the types of characters it accepts, so not all characters can be sent; those that can't are called "bad characters," the researchers said. There also is a limit on the length of characters that can be sent.

To overcome the lack of control over data flow in DNS, threat actors can notify the server which packet should be buffered, as well as what is expected as the last package, the researchers said. A package also should not be sent until an attacker knows that the previous one successfully arrived, they said.

To avoid bad characters, attackers should apply Base64 on data sent right before sending it, while they can slice

Previous Next

data into pieces to be sent one by one to avoid the DNS character length limit, they said.

To get around a defender blocking a DNS request by blocking access to the server from which it is being sent, an attacker can generate domain names based on variables that both sides know and expect, the researchers explained.

"While the executable is not necessarily difficult, an attacker or group would need the infrastructure to continue to buy root records," they noted.

Attackers also can configure malware to generate a domain in DNS based on a date, which will allow them to constantly send new requests over DNS using a new, known root domain, the researchers said. Defending against this type of configuration "will prove challenging to organizations using static methods or even with basic anomaly detection to detect and prevent," they said.

Mitigating DNS Attacks on Air-Gapped Networks

With DNS attacks occurring more frequently than ever — with 88% of organizations reporting some type of DNS attack in 2022, according to the latest IDC Global DNS Threat Report — it's important for organizations to understand how to mitigate and defend against DNS abuse, the researchers said.

One way is to create a dedicated DNS server for the air-gapped network, Gabay tells Dark Reading. However, organizations must take care to ensure that this server is not chained to any other DNS servers that may exist in the organization, as this "will ultimately chain it to DNS servers on the Internet," he says.

Companies should also create anomaly-based detection in the network utilizing an IDS/IPS tool to monitor and identify strange DNS activities, Gabay says. Given that all enterprise environments are unique, this type of solution also will be unique to an organization, he says.

However, there are some common examples of what abnormal type of DNS behavior should be monitored, including: DNS requests to malicious domains; large amounts of DNS requests in very short period of time; and DNS requests made at strange hours. Gabay adds that organizations also should implement a SNORT rule to monitor for the length of requested DNS records.

About the Author: *Elizabeth Montalbano is a freelance writer, journalist, and therapeutic writing mentor with more than 25 years of professional experience. Her areas of expertise include technology, business, and culture.*

ANALYSIS

What CISOs Can Do About Brand Impersonation Scam Sites

Apply these four tips to proactively fight fraudulent websites that use your brand to rip people off.

By Ericka Chickowski, Contributing Writer, Dark Reading

Brand impersonation is a particularly thorny problem for CISOs. Cybercriminals piggyback off a trusted brand to push scam lures through various means to onto unsuspecting customers. They could disguise themselves as part of the organization's IT team or someone familiar to trick employees into clicking on malicious links or send a message that looks like it is coming from a legitimate source to convince the recipient the contents are real.

Retailers, product creators, and service providers are increasingly having to deal with brand impersonation attacks. Mimecast's "2022 State of Email Security Report" found that 90% of organizations experienced an impersonation attack over the previous 12 months. Further, the Mimecast "2021 State of Brand Protection Report" found that companies on the BrandZ Top 100 Most Valuable Global Brands 2020 list experienced a 381% rise in brand impersonation attacks over May and June 2020 compared with before the pandemic. New domains suspected of brand impersonation also rose by 366%. These impersonation attacks include not only the typical phishing or malware attacks but also fraud that sells or claims to sell products or services on behalf of the brand. These include fencing of stolen items, non-delivery scams, and counterfeit or gray market sales of product.

"[Brand impersonation] is a fraud problem and a security incident problem," says Josh Shaul, CEO of Allure Security. "People are stealing from you, and you're trying to prevent the theft."

Experts recommend that CISOs take a systematic and multidisciplinary approach to this problem. The right approach will not only require technology like automated detection, but also security leadership in helping business stakeholders to harden the brand on a number of fronts.

1. Monitor Domains

Organizations should not only be watching and monitoring the domains they own, but also their domain ecosystem, says Ihab Shraim, CTO of CSC Digital Brand Services.

"This means understanding the types of domains that are being registered around them because it's a multidimensional cyber threat," he says.

As Shraim explains, often larger enterprises manage thousands of domains, which can make it difficult to keep tabs on and effectively manage the entire portfolio.

"Companies need to devise policies and procedures to monitor and mitigate threats associated with all their domains as an integral part of their security posture," Shraim says.

He explains that they should be continuously monitoring their domains and also digital channels within search engines, marketplaces, mobile apps, social media, and email to look out not only for phishing and malware campaigns but also brand abuse, infringements, and counterfeit selling on digital channels.

"It is crucial for companies to understand how their brands are operating on the Internet," Shraim says.

2. Leverage Threat Intel

Doug Saylors, partner and co-lead of cybersecurity for global technology research and advisory firm ISG, believes that organizations should leverage threat intelligence to help them with the adjacent domains and also the tricky tactics, techniques, and procedures (TTPs) used by bad actors in their impersonation attacks.

"Organizations need to invest in threat intelligence platforms that will help identify the use of fake domains, phishing campaigns, and other technologies to defeat the TTPs used to enable brand impersonation," he says.

3. Consider Full-Cycle Brand Protection

Saylors is also a big believer in full-cycle brand protection. He recommends that companies consider these services — not just for their detection capabilities but also their expertise in mitigation.

"They should engage the services of specialty firms that deal with the full life cycle of brand protection to ensure scalability and absolute focus on reducing fraudulent ac-

tivity," he says. "These firms have advanced capability to identify fake sites, catalogs, and catalog entries and remove them through industrial-strength takedown procedures."

As organizations evaluate online brand protection companies, they've got to keep in mind that this is another cat-and-mouse game detection category, where mileage may vary based on technology and how well companies keep up with evasive behavior from the attackers.

For example, when attackers found that their scams were being discovered through image processing and logo detection, they began with simple evasive techniques like changing the image file format and then evolved to use multiple nested images and text in a single collapsed image to trip up detection, Shaul says.

"So now, unless you can compare sections of an image, which is a super hard technical problem that some of us have solved, you can't detect these things anymore," he says. "They just bypass the evolving detections that organizations are putting out there."

Another new tactic they've taken is [creating generic fake shops and evolving them into branded shops over time](), he says.

"The scammers are working hard to understand how detection is evolving in the industry, and doing things to try to evade detection as aggressively as they can," Shaul says.

4. Use Incident Responders Judiciously

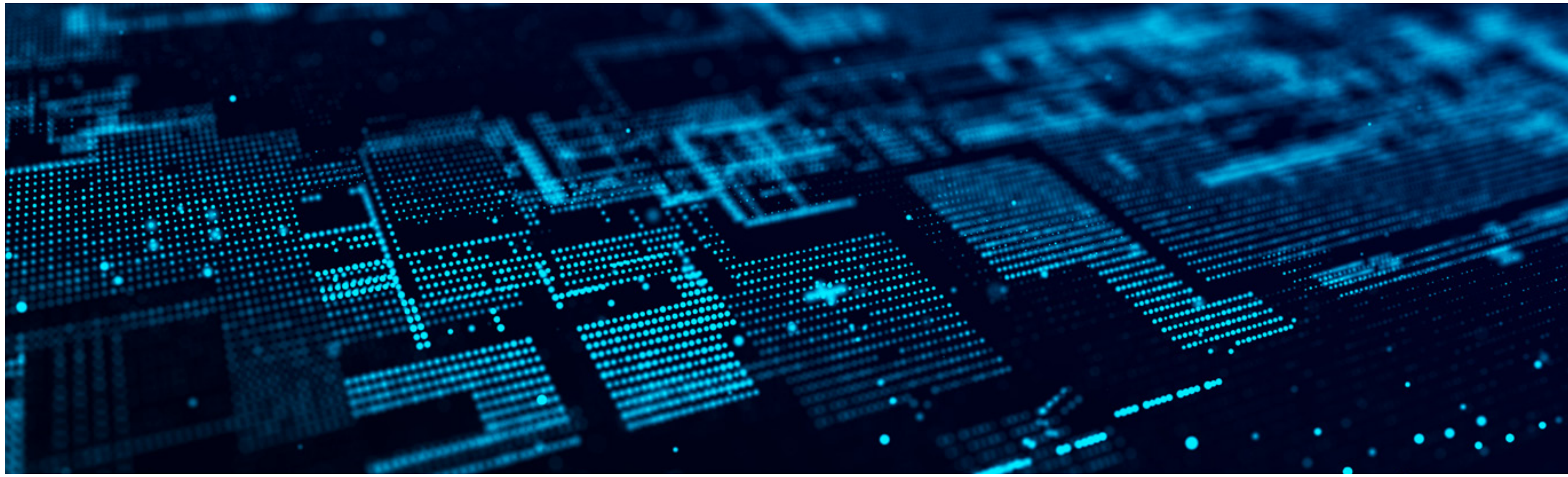
Incident responders hate handling the mitigation of brand impersonation because it is a different skill set than a lot of analysts who get into the field for fun investigative work and not to chase down registrars to do takedowns, Shaul says. Even if a company can make it fun for their responders, they have got to be careful that they're using their specialized responders in a cost-effective way.

He likes to tell the story of a banking customer that had been putting this on their IR team, who turned it into a fun exercise by breaking into phishing sites that were targeting the company's brand and doing a lot of offensive security work.

"The IR guys were having a ball with it, but they realized, 'Look how much time we're spending basically just playing games with the attackers,'" he says. "They had their best people doing hard work to just clean up after scams that already happened."

He suggests that by knowing in advance that response to these sites takes a different skill set than advanced analysts have, this might be a way to break in new security ops personnel and give early-career responders some experience through a planned career path that starts with impersonation takedowns.

About the Author: *Ericka Chickowski specializes in coverage of information technology and business innovation. She has focused on information security for the better part of a decade and regularly writes about the security industry as a contributor to Dark Reading.*



Why DNS Detection and Response Is Key to Reducing Cybersecurity Risk

DNS can speed up response to threats and make security operations more productive.

By Srikrupa (Krupa) Srivatsan, Senior Director of Product Marketing, Infoblox

Protecting today's distributed networks — which may include multicloud, on-premises, edge, and IoT/OT (Internet of Things/operational technology) environments — is no simple feat. Networks are getting more complex, and attackers are getting more sophisticated and finding new ways to bypass enterprise security controls. Early detection when breaches happen and fast response to threats are more crucial than ever, enabling enterprises to reduce risk to the business and stay compliant. What's needed is a security approach that permeates all aspects of your network and can continuously monitor activity from any device, any user, anywhere.

Traditional approaches often fall short when it comes to protecting the growing attack surface and/or addressing constantly evolving cyberthreats. In addition, security operations teams are often faced with challenges around improving incident response times due to lack of easy access to contextual information.

One network infrastructure element that every network has and needs for connectivity is DNS (Domain Name System). But DNS can be more than just a protocol that connects users to websites. It can be used to detect and block a majority of threats, including ransomware, phishing, and malware command and control. DNS also can block attacks — such as domain generation algorithms, DNS-based data exfiltration, and look-alike domains — that are missed by existing security controls. Protective DNS makes DNS a great first line of defense without adding additional infrastructure elements to the network. Protective DNS has been embraced by governments around the world, including the US and UK.

But Protective DNS is only part of the solution. DNS also provides robust capabilities to speed up response to threats and make security operations much more productive, with significant time and cost savings. This is made possible by tapping into DHCP and IP Address Management (IPAM), DNS-related technologies that help provide visibility into where threats exist in the network, what devices are impacted, and which threats pose the most risk. In addition, integrating with other existing security tools for automatic downstream remediation when threats are detected can relieve some of the burden from the security teams. This greatly reduces MTTR (mean time to remediation) and provides concrete savings in time and effort.

Introducing DNS Detection and Response

Protective DNS + Visibility + Automation = DNS Detection and Response.

DNS Detection and Response is the combination of:

1. Protection at the DNS level
2. Using the visibility that DNS, DHCP, and IPAM (collectively known as DDI) data provide
3. Automating remediation through ecosystem integrations

Protecting at the DNS request/response level looks like the following:

- “Shifts left” protection by detecting and blocking threats early (92% of malware uses DNS control plane)
- Reduces security incident-related endpoint downtime by 47% per user feedback
- Reduces load on downstream security devices
- Protects all types of systems, including IoT/OT
- Protects east-west traffic and contains lateral spread in an easy and transparent way

The visibility that DNS, DHCP, and IPAM provides has been proven to reduce security operations effort by 34% by providing critical telemetry on threats. The what, when, and why of each threat is presented with deep insight, which saves manual time and effort for SecOps as they investigate a threat.

A DNS detection and response solution also helps with remediation action after an incident by integrating with other security tools — including ITSM (IT service management), NAC (network access control), and vulnerability scanners — to raise an IT ticket, knock a system off the network, or trigger a scan on the affected device. This makes the ecosystem tools more effective while allowing organizations to get better ROI from these investments.

The following list summarizes key capabilities for a robust DNS detection and response solution:

Identify

- Map DNS queries to user/device activity using IPAM (to identify what user/machine talked to any domain/IP)
- DNS-based application discovery (to identify what applications are being used and detect shadow IT)

Protective DNS

- Block phishing, ransomware, malware command and control, DGA (domain generation algorithm), and data exfiltration
- Brand protection from lookalike domain attacks
- Content filtering to block access to certain categories of content (social media, gambling, and so on)
- Protect any system anywhere, including IoT/OT
- DNSSEC (DNS Security Extensions)
- Customizable policies for granular protection

Detection

- Use of threat intelligence for detecting communications to known malicious sites
- DNS threat hunting to detect suspicious domains and emergent domains that may not be deemed malicious yet
- AI/ML analytics on DNS queries for detecting DGAs and data exfiltration

Response

- Automated remediation actions via ecosystem integration to trigger scans or quarantines, or raise IT ticket
- Sharing of DDI data to SOC tools for triage/correlation
- Easy view of impacted systems
- Context on IoCs (indicators of compromise) to prioritize threats that pose the most risk

About the Company: *Infoblox unites networking and security to deliver unmatched performance and protection. Trusted by Fortune 100 companies and emerging innovators, we provide real-time visibility and control over who and what connects to your network, so your organization runs faster and stops threats earlier. Visit infoblox.com, or follow us on LinkedIn or Twitter.*