Securing DNS Against Emerging Threats: A Hybrid Approach

This paper looks at the impact of mobility and new attack vectors on DNS-related risk and outlines use cases for securing DNS services more effectively. It also examines the use of a hybrid model of on-premises and cloud-based services to improve the security posture of organizations.

Copyright SANS Institute
Author Retains Full Rights
As key Internet infrastructure elements, Domain Name System (DNS) services have been essential to enabling the mission-critical Internet for businesses, governments and consumers. Cyber criminals and attackers have recognized this, making protecting the availability and integrity of DNS services critical. Insecure DNS services can be used by attackers to impersonate a business and route customer traffic to malicious sites, which can then steal usernames, passwords, account information and valuable intellectual property.

In recent years, attackers have also begun to subvert DNS services to provide hard-to-detect paths to inject malware into business systems and exfiltrate data from compromised PCs and servers. These advanced attacks take advantage of weaknesses in the DNS protocol and in the requirement to allow DNS communications to work through enterprise firewalls and other standard security controls.

Basic security hygiene and DNS best-practice architectures can be applied to raise the overall security level of an organization. Addressing these new threats, however, requires monitoring of DNS communications, the ability to recognize unusual or malicious activity and informing the broader security ecosystem to protect against lateral movement of threats. In addition, increased mobility of employees and contractors means that protecting and monitoring DNS services on premises is not sufficient; visibility needs to be extended out to protect the mobile workforce.

This paper looks at the impact of mobility and new attack vectors on DNS-related risk and outlines use cases for securing DNS services more effectively. It also examines the use of a hybrid model of on-premises and cloud-based services to improve the security posture of organizations.
By providing ubiquitous connectivity among employee PCs, data center servers and Internet-based servers, the early use of the Internet enabled businesses to more rapidly research, develop and target new products and services. As consumers began to connect home PCs to the Internet, that connectivity extended out to reaching customers in their homes.

Advances in wireless Internet connectivity in the early 2000s showed the promise of mobile Internet access, and by 2008, laptop sales exceeded desktop PC sales.¹ That same year, the iPhone showed the most rapid penetration of any new technology, and sales of smartphones surpassed PCs by 2012, with annual sales of tablets exceeding PCs.² ³ See Figure 1.

² “Tablets to Top Laptops this Year, All PCs in 2015,” www.pcmag.com/article2/0,2817,2419532,00.asp
The increased use of laptops, mobile devices and home PCs by employees highlights the business demand for mobility. IDC forecasts that by 2020, more than 70 percent of the workforce will be primarily mobile. Businesses have seen clear benefits in cost savings and increased innovation by enabling mobility.

Along with those benefits, however, mobility has brought new risks. Employee-owned laptops and home PCs, as well as mobile devices, are heterogeneous, change rapidly, and invariably bring along the use of external cloud services. Data from a 2017 study published by Skyhigh networks shows that the average enterprise today has dozens of business-approved cloud services in use, and many have discovered hundreds of unsanctioned cloud services. The “connect from anywhere” aspect of cloud services has served as another accelerant of the business demand for mobility.

Mobility and the use of cloud services is breaking long-established IT processes for administration and control of resources and services, and most security processes and controls have been affected. Over the years, we have learned that every time new technologies reach the user, IT is forced to adapt and support those new technologies. To secure the use of new technologies, security delivery also has to evolve.

Because mobility and the use of cloud services involve the use of external DNS services, delivery mechanisms for DNS security and visibility into DNS services to detect attacks and breaches will have to adapt to these potential paths to infiltration and attacks.

---

The security, integrity and reliability of Internet commerce and communication depend on underlying DNS services. Advanced targeted attacks often focus on DNS services either directly or as part of a broader attack campaign.

Successful attacks against DNS services in the past fell into three major categories: denial of service (DoS), DNS hijacking and man in the middle.

DNS services can also present vulnerabilities that enable data exfiltration attacks to succeed. Methods to exploit these vulnerabilities have been demonstrated as far back as 2007, and in recent years, they have been used in several real-world breaches.

The DNS protocol uses stateless messaging for a DNS client to submit queries to an external server and receive external replies from that server. These queries and replies can contain up to 512 octets of data, and there is no message-level security enforced in standard DNS services. This combination provides an easy-to-exploit path whereby attacks can subvert DNS services for both malware updating and data exfiltration.

A typical DNS exfiltration attack scenario is represented in Figure 2.

---

**Figure 2. Typical Exfiltration Attack Scenario**

Tools such as DNSCAT\(^2\) have long been available to enable this scenario. DNS tunneling has been seen for several years in active threats (FeederBot, Moto 2011\(^8\)), and detection of its use has been increasing as security monitoring of HTTP flows has increased. A few recent DNS attacks drive home the severity of the problem and point to underlying vulnerabilities in DNS security:

- **Multigrain PoS.**\(^9\) Because they handle credit card data and are frequently poorly protected, point of sale (PoS) systems are frequently targeted by data exfiltration attacks. NewPosThings is a malware family first seen attacking PoS systems in 2014, using standard HTTP techniques for command and control communication and data exfiltration. Multigrain PoS is a variant that uses DNS tunneling to perform those functions while evading detection.

- **Wekby pisloader.**\(^10\) The hacker group known as Wekby has launched many attacks against healthcare organizations over the past few years using phishing at the front end and HTTP for exfiltration. More recently, attacks attributed to Wekby have used malware known as pisloader that uses DNS tunneling for command and control and exfiltration.

- **FrameworkPOS (2014).**\(^11\) In 2014, Home Depot suffered a large breach that was caused by malware dubbed FrameworkPOS, which targeted credit data in Home Depot’s PoS systems. FrameworkPOS later evolved in 2016 to use DNS tunneling techniques for data exfiltration.

**Closing the Gap**

SANS estimates that more than 80 percent of cybersecurity incidents exploit known vulnerabilities. Gartner estimates 99 percent\(^12\), and Verizon agrees.\(^13\)

The critical success factor for avoiding or minimizing business damage due to cyber attacks is reducing the attacker’s ability to exploit the vulnerabilities and more quickly detecting when attacks are starting. Those same factors apply to attacks that focus on exploiting DNS services or using them as part of attack command and control communications. Successful security programs have been able to prioritize security resources around increasing the ability to prevent more targeted attacks and more rapidly and accurately detect those that could not be prevented.

---

A proven starting point for prioritizing security improvements is the Critical Security Controls framework, coordinated by the Center for Internet Security (CIS), which represents a broad security community consensus of the security controls most effective for avoiding or stopping real-world threats. Version 6.1 of the CIS Controls was released in August 2016.

Figure 3 shows a summary of the various sections.

![Center for Internet Security Critical Security Controls Framework](image)

Figure 3. Center for Internet Security Critical Security Controls Framework

Although all of the controls are appropriate for an effective, efficient security program, the following sections discuss those that have the most direct applicability to DNS services and how they can be applied. Where possible, enterprises should address all of the referenced controls to keep DNS services secure and reliable. Where resources are limited, the CIS Controls should be implemented in the order presented.

---

14 [www.cisecurity.org/critical-controls.cfm](http://www.cisecurity.org/critical-controls.cfm)

Critical Controls 1, 2, 3, 11—Inventory and Secure Configurations

Vital to keeping an enterprise’s DNS services secured is identifying the DNS-related software in use (resolvers, servers, etc.), ensuring it is up to current patch levels and configured to best security practices. For example, in 2016, BIND software had 11 security advisories that required patching or configuration checking.16

DNS services may be delivered from PCs, servers and network equipment, or may involve external parties, such as ISPs. Keeping enterprise DNS services secure requires that all servers, routers and firewalls running DNS services are configured correctly and not compromised. This can be a complex undertaking and often drives enterprises to move to dedicated, hardened DNS architectures, which are scalable, highly available, more secure and simpler to configure and manage. Alternatively, some enterprises move to managed DNS services, thereby outsourcing the configuration management effort. Even if an organization moves to managed DNS services, having some on-premises DNS infrastructure can help with availability if the managed DNS provider suffers a distributed DoS (DDoS) attack, as happened recently in the Mirai attacks against Dyn DNS in 2016.

Critical Security Control 8—Malware Defense

DNS servers should be protected from being used by malicious executables that are part of advanced targeted attacks. Whitelisting software can be run on DNS servers to make sure unapproved software cannot be installed. Another option is to use DNS as a control point to detect malware and cyberattacks early, prevent progression of malware through the cyber kill chain and protect against lateral movement of threats.

Many attacks use DNS services at several stages of the cyber kill chain as they attempt to insert targeted malware for initiating data breaches or locking up data for ransom. Critical Security Control 8 points out in sub-control 6: “Enable domain name system (DNS) query logging to detect Hostname lookup for known malicious C2 (command and control) domains.” This log data can be used as an early indication of a malware problem. Because mobile employees will be using external cloud-based services, such monitoring needs to be extended to support those services as well.

As mentioned earlier, malicious tunneling over DNS protocols is increasingly used as malware insertion and data exfiltration channels by advanced targeted attacks. DNS communications should be monitored to detect evidence of misuse. In addition, network context and data gathered can be shared with the broader security ecosystem for threat prioritization and faster remediation. Using DNS for malware defense means customers get a solution without the need for endpoint agents, which is important to consider when trying to secure IoT devices.

16 www.cvedetails.com/vulnerability-list/vendor_id-64/product_id-144/year-2016/ISC-Bind.html
Critical Security Control 12—Boundary Defense

To limit the attack aperture, internal DNS servers should be located behind next-generation firewalls and intrusion prevention systems that provide DNS-aware filtering capabilities. Another option is to put DNS servers in network segments protected by firewalls that focus on DNS protocols. This is a necessary precaution, but it does not provide complete security because advanced targeted attacks often compromise user PCs or laptops and then launch the next stage of an attack from inside the firewall.

DNS services also need protection from DDoS attacks (see Figure 4). DDoS attacks essentially have unlimited bandwidth, so it is impossible to simply oversize or overprovision a DNS server. Nor is simple DDoS protection that relies on rate limiting effective against modern DDoS attacks, because these kinds of attacks now also mix in resource starvation attacks that use low bit rate, specially crafted packets to force a server to run complex processes, causing the server to bog down or crash.

DNS appliances should be installed behind boundary defenses that limit the attack aperture, but also must include updatable capabilities for protecting themselves against evolving attacks that get through such perimeter defenses. Maintaining DNS integrity is essential to prevent DNS hijacking, which can compromise boundary defenses—as was seen in the Syrian Electronic Army attack. It is also important to deploy scalable and highly available architecture for DDoS resiliency and have visibility into any infrastructure vulnerability that could compromise its integrity. If using managed DNS services, complementing them with on-premises self-protecting DNS servers can help the services to stay up and running even under attack.

Figure 4. DDoS Attack Scenario
Critical Security Control 13—Data Protection

As detailed above, advanced targeted threats use DNS communications as a means for both inserting malware and for exfiltrating sensitive data. CSC is focused on protecting critical business information: “The processes and tools used to prevent data exfiltration, mitigate the effects of exfiltrated data, and ensure the privacy and integrity of sensitive information.”

Sub-controls 13.6, 13.7 and 13.8 focus on monitoring network traffic to detect and block unauthorized export of sensitive information.

Further, using behavioral analytics on DNS queries can help detect zero-day data exfiltration techniques that don’t necessarily send data to known malicious destinations.

Critical Security Control 20—Penetration Testing

As discussed previously, attackers often target DNS services for disruption and compromise. They often exploit multiple vulnerabilities (in both software and people) to launch complex, multistage campaigns. Penetration testing processes and tools essentially act as “attackers in a box” and use those same techniques to see whether sensitive information can be breached or business services disrupted.

A typical external penetration test will expose potential paths that attacks could use to affect an enterprise’s DNS services. That test will also reveal ways attackers might exploit an enterprise’s DNS resources to launch attacks within its firewall or against other companies. The DNSCAT2 tool or equivalent can be used as part of penetration testing to test the ability to detect DNS tunneling attacks.

More modern penetration testing adds “inside out” penetration testing, in which an internal PC is compromised (perhaps through compromised DNS services) and the testing demonstrates potential impacts. All penetration testing plans should include DNS services as targets and as services to be used in the simulated attack.
The impact of mobility and the growth of DNS tunneling as part of advanced targeted attacks requires enterprises to adapt their security architectures, processes and controls to maintain needed DNS security levels. The optimal approach will depend on the particular use case and business environment. Two common scenarios are addressed here: 1) protecting headquarters operations, and 2) adding branch office and mobile/remote employees to the mix.

### Use Cases

#### Protecting Headquarters

To assure reliability and integrity, DNS services used at headquarters locations should be deployed and maintained following the CIS Controls addressed in the previous section. Organizational staffing, expertise and governance constraints (especially at branches) should be evaluated to determine whether in-house software-based DNS services, an appliance-based approach or external DNS services will provide the most effective and efficient way to deliver secure DNS services.

To address DNS tunneling risks and detect when sensitive data is being exfiltrated, DNS server activity and both client and server DNS network communications should be monitored and analyzed using behavioral models to detect malicious or suspicious activity. To detect known malware effectively, highly verified and curated threat intelligence to provide reputation information should be used while doing DNS lookups, ensuring that communications to known bad sites are blocked.

To protect against lateral movement of threats and accelerate remediation, malicious hit information, network context and data from DNS, DHCP and IPAM services can be shared with the broader security ecosystem.

#### Mobile Workforce

Employees using laptops and tablets from external locations bring another level of complexity. The growth in the number of employees working from remote and multiple locations and not necessarily using VPNs has meant that the majority of the mobile workforce could be exposed to cyber attacks, malware and data theft. The demand for speed and mobility has caused most organizations to abandon back-hauling all mobile user Internet traffic through corporate Internet points of presence. This means that mobile user DNS traffic is generally not visible to corporate security monitoring.

There are three approaches to maintaining DNS security in the mobile environment:

1. **Mobile client-side monitoring.** Agent software on the mobile device can reroute DNS traffic to a cloud-based DNS security solution that can monitor client-side behavior to detect malicious or suspicious DNS activity. This approach can provide the highest level of visibility and control but requires that an agent be installed and maintained on all devices.

2. **Proxy approaches.** Where an agent cannot be installed on mobile devices, configuration settings on mobile devices can be set to proxy mobile device traffic through services often called cloud access security brokers (CASB). CASB services can monitor HTTP Internet traffic from mobile devices, but other protocols are not widely supported. To complement CASB solutions, a DNS proxy solution can also be implemented. This reroutes DNS queries to a cloud-based DNS security solution with identifying client information to monitor and block suspicious activity.

3. **Both of the above.** Using both client agent and proxy approaches can provide coverage across a variety of devices and external services. Both approaches need to be integrated with threat intelligence to assure detection of DNS tunneling and other advanced targeted threats.

With a hybrid approach of using on-premises DNS security together with a cloud-delivered DNS security solution, organizations can protect not just their users within the corporate network, but also their mobile workforce and branch offices.
Conclusion

Without proper consideration in an enterprise’s security plans, DNS provides an easy point of entry for disruption and unauthorized information access and exfiltration. Sophisticated cybercriminals and other attackers continue to develop new attack tactics and techniques to exploit weaknesses in DNS services. The increasing demand to support mobile business and a mobile workforce have been opening up additional attack vectors.

However, several ways exist to help mitigate the problems caused by DNS vulnerabilities and actually use DNS services and data as an asset in the security chain. Awareness is the first step toward implementing a more secure enterprise, followed by ensuring “basic DNS security hygiene,” as demonstrated by the Critical Security Controls. From that secure foundation, enterprise security managers can effectively and efficiently provide secure solutions for new business demands such as mobility and IoT.
John Pescatore joined SANS as director of emerging technologies in January 2013 after more than 13 years as lead security analyst for Gartner, 11 years with GTA, and service with both the National Security Administration, where he designed secure voice systems, and the U.S. Secret Service, where he developed secure communications and voice systems “and the occasional ballistic armor installation.” John has testified before Congress about cyber security, was named one of the 15 most influential people in security in 2008 and remains an NSA-certified cryptologic engineer.

SANS would like to thank this paper’s sponsor:
<table>
<thead>
<tr>
<th>Event Name</th>
<th>City, Country</th>
<th>Start Date - End Date</th>
<th>Location Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>SANS Munich December 2017</td>
<td>Munich, DE</td>
<td>Dec 04, 2017 - Dec 09, 2017</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Austin Winter 2017</td>
<td>Austin, TXUS</td>
<td>Dec 04, 2017 - Dec 09, 2017</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Bangalore 2017</td>
<td>Bangalore, IN</td>
<td>Dec 11, 2017 - Dec 16, 2017</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS SEC460: Enterprise Threat Beta</td>
<td>San Diego, CAUS</td>
<td>Jan 08, 2018 - Jan 13, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Security East 2018</td>
<td>New Orleans, LAUS</td>
<td>Jan 08, 2018 - Jan 13, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>Northern VA Winter - Reston 2018</td>
<td>Reston, VAUS</td>
<td>Jan 15, 2018 - Jan 20, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Amsterdam January 2018</td>
<td>Amsterdam, NL</td>
<td>Jan 15, 2018 - Jan 20, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Dubai 2018</td>
<td>Dubai, AE</td>
<td>Jan 27, 2018 - Feb 01, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Las Vegas 2018</td>
<td>Las Vegas, NVUS</td>
<td>Jan 28, 2018 - Feb 02, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Miami 2018</td>
<td>Miami, FLUS</td>
<td>Jan 29, 2018 - Feb 03, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>Cyber Threat Intelligence Summit &amp; Training 2018</td>
<td>Bethesda, MDUS</td>
<td>Jan 29, 2018 - Feb 05, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS London February 2018</td>
<td>London, GB</td>
<td>Feb 05, 2018 - Feb 10, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Scottsdale 2018</td>
<td>Scottsdale, AZUS</td>
<td>Feb 05, 2018 - Feb 10, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Southern California- Anaheim 2018</td>
<td>Anaheim, CAUS</td>
<td>Feb 12, 2018 - Feb 17, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Secure India 2018</td>
<td>Bangalore, IN</td>
<td>Feb 12, 2018 - Feb 17, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Dallas 2018</td>
<td>Dallas, TXUS</td>
<td>Feb 19, 2018 - Feb 24, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>Cloud Security Summit &amp; Training 2018</td>
<td>San Diego, CAUS</td>
<td>Feb 19, 2018 - Feb 26, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Brussels February 2018</td>
<td>Brussels, BE</td>
<td>Feb 19, 2018 - Feb 24, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Secure Japan 2018</td>
<td>Tokyo, JP</td>
<td>Feb 19, 2018 - Mar 03, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS New York City Winter 2018</td>
<td>New York, NYUS</td>
<td>Feb 26, 2018 - Mar 03, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>Cyber Threat Summit 2018</td>
<td>London, GB</td>
<td>Feb 27, 2018 - Feb 28, 2018</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS Khobar 2017</td>
<td>OnlineSA</td>
<td>Dec 02, 2017 - Dec 07, 2017</td>
<td>Live Event</td>
</tr>
<tr>
<td>SANS OnDemand</td>
<td>Books &amp; MP3s OnlyUS</td>
<td>Anytime</td>
<td>Self Paced</td>
</tr>
</tbody>
</table>

Last Updated: November 29th, 2017