2019 Global DNS Threat Report
Understanding the Critical Role of DNS in Network Security Strategy

June 2019

Authors:
Romain Fouchereau, Research Manager, IDC
Konstantin Rychkov, Research Manager, IDC CEMA

IDC #EUR145072419

An IDC InfoBrief sponsored by efficient iP™
Executive Summary

Many high-profile breaches and publicized security issues in enterprises have been widely exposed in recent years, demonstrating that traditional security products are no longer adequate and will not provide business continuity or data protection in a rapidly changing environment. The IT security threat landscape is continually evolving. Digital transformation is being driven by the fast adoption of cloud services, and there are major changes linked to the regulatory upheaval we have seen with the enforcement of GDPR, among other privacy initiatives. DNS is a primary target for cyberattacks, causing business damage in terms of downtime and financial loss, as it remains one of the critical elements in delivering IT services.

82% Companies that experienced a DNS attack

9.45 Average number of attacks per company

$1.07M Average damage cost

63% Companies that suffered application downtime

Source: IDC DNS Survey 2019 n= 900

DNS is more than ever a central network foundation, enabling all clients to access every app. Any DNS performance impact has major business implications.

At the same time, the fact that most traffic first goes through a DNS resolution gives it unique visibility over legitimate and malicious network activity. This is being widely recognized by businesses, who are starting to leverage DNS for their security strategy via threat intelligence, policy control and automation.

DNS is fast becoming the guardian of networks!

David Williamson, CEO, EfficientIP
DNS Threat Landscape is Dangerously Diverse

The number of companies that suffered DNS-based attacks has again increased, growing 5% over 2018, and reaching an alarming 82%.

By nature, DNS is an open service to the network, and its mission-critical role for routing application access makes it a primary attack vector and target for hackers. The spectrum of DNS attacks illustrates this fact; compared to last year, it is much broader as the percentage of each attack type suffered has significantly increased, from volumetric to low signal attacks.

Top DNS-based attacks suffered

- DNS phishing: 47% (2019), 36% (2018)
- DDoS attacks: 30% (2019), 20% (2018)
- DNS tunneling: 24% (2019), 20% (2018)

Source: IDC DNS Survey 2019 n=900

Average number of DNS attacks

2019: 9.45 up from 7.08 attacks in 2018
Impacts and Costs of DNS Attacks

2018 saw a strong increase in how organizations were impacted by DNS attacks. Worryingly, both in-house and cloud applications were damaged, with growth of over 100% for in-house application downtime, making it now the most prevalent damage suffered.

DNS attacks are moving away from pure brute-force to more sophisticated attacks acting from the internal network. This will force organizations to use intelligent mitigation tools to cope with insider threats.

Impact Statistics

<table>
<thead>
<tr>
<th>Impact</th>
<th>2019</th>
<th>2018</th>
</tr>
</thead>
<tbody>
<tr>
<td>In-house application downtime</td>
<td>63%</td>
<td>31%</td>
</tr>
<tr>
<td>Compromised website</td>
<td>45%</td>
<td>33%</td>
</tr>
<tr>
<td>Sensitive information stolen</td>
<td>13%</td>
<td>22%</td>
</tr>
<tr>
<td>Brand damage</td>
<td>26%</td>
<td>23%</td>
</tr>
<tr>
<td>Loss of business</td>
<td>27%</td>
<td>22%</td>
</tr>
</tbody>
</table>

Average cost per attack continues to increase (+49%):

- **2019**: $1.07M
- **2018**: $715k

Source: IDC DNS Survey 2019 n=900
State of DNS Defenses

Given the level of damage suffered, awareness of the critical importance of DNS security must improve:

Conventional security solutions such as secure web gateway, next-generation firewall, data loss prevention (DLP), and intrusion prevention systems (IPS) are not designed to ensure DNS service availability and integrity.

Security countermeasures are based on workaround

- **60%** shut down processes & connections
- **56%** disabled some/all affected apps
- **53%** shut down the business server

DNS security practices must move from reactive to proactive

DNS analytics usage is evolving from threat remediation to predictive security

- **64%** use DNS analytics to detect compromised devices
- **35%** augment threat intelligence with internal analytics on DNS traffic
- **53%** find high value in machine learning for the detection of malicious domains

Only **64%** of companies estimate DNS security is critical for business
No Industry is Spared From DNS Attack Disruption

- **MANUFACTURING**: In-house application downtime the highest at 70%
- **FINANCIAL SERVICES**: Most targeted industry with 88% of respondents attacked last year
- **RETAIL**: Experienced highest cloud service downtime at 45%, with the most business loss at 35%
- **TELECOM AND MEDIA**: Experienced the highest amount of brand damage at 34%
- **HEALTHCARE**: 50% of organizations were impacted by a compromised website
- **EDUCATION**: Most subject to phishing attacks at 55%
- **GOVERNMENT**: Highest occurrence of sensitive information stolen at 19%
- **UTILITIES**: Cost of attack highest with 25% of attacks costing over $1.1 million
Data Privacy & Compliance, One Year After GDPR

24% of organizations were victims of DNS tunneling last year

GDPR regulation has been in force since May 2018. Important investments have been made by organizations in all countries, notably to strengthen network security defenses. As part of a security technology strategy, DNS traffic monitoring analysis is considered one of the most effective ways to protect data confidentiality.

Organizations see a positive impact from GDPR legislation, feeling it will sustain the need to deploy stronger security defenses. Ongoing data privacy compliance initiatives strategies in other countries (CLOUD Act, NISD, PDPA, etc.) will also benefit.

Action considered most effective to protect data confidentiality

- Better monitoring and analyzing of DNS traffic: 29%
- Securing network endpoint: 32%
- Additional firewalls: 22%

GDPR Impacts

- Network security upgrade and innovation: 79%
- Heightened consumer trust: 64%
- Education of employees on data privacy: 81%
Network & Information Systems Directive

As one initiative to increase Europe's preparedness to ward off cyber incidents and to achieve consistent protection against cyberattacks across all member states, the EU adopted the Network and Information Security (NIS) Directive in August 2016.

The NIS Directive is focused on the protection of essential services and digital services such as online marketplaces, online search engines, and cloud computing services.

The initiative has a broad focus on protecting infrastructure, including physical assets, and there is a primary emphasis on resilience, incident management, and business continuity management.

DNS is critical to ensure service continuity. Faulty or ineffective DNS services can negatively affect the perception of any organization (from clients, partners or employees), impact your ecommerce applications, resulting in lost revenue, and ruin a brand image: 63% of organizations suffered app downtime as a direct result of a DNS attack last year.

When under DNS attack, utilizing adaptive countermeasures designed to ensure DNS service availability and integrity are required; disaster recovery and avoiding single points of failure must be part of the mitigation process and security best practices, as current countermeasures such as disabling all apps or shutting down servers will no longer be suitable.
Digital transformation leads to a dramatic increase in network complexity and security risks, driven by the proliferation of devices, hybrid cloud, and multicloud deployments, and mobility.

To face these challenges, perimeter network security is evolving to become zero-trust strategy. The new architecture pattern relies on the fact that there are no longer trusted and untrusted zones, perimeters, devices, and users. Everything is untrusted — by default.

A zero-trust strategy requires moving from macro-segments to micro-segments that could be as small as a single client, resource, or server. It implies collecting telemetry data to get in-depth visibility on end-point behavior to detect threats at the most granular level. It also needs advanced automation through a software defined network (SDN) in order to provision micro-segments to connect end-points and activate associated filtering security policies.

DNS security, fueled by threat intelligence and network automation, is key to a successful zero-trust strategy.

17% of companies run on zero-trust architecture already, with 48% planning as part of security strategy.

Only an average of 14% collect DNS logs and correlate them through machine learning.

Predictive analytics are already part of the security stack for 45% of companies.

Only 14% have adopted automation in their network security policy management.
Essential Guidance

From the findings in this report, it is evident that DNS is a critical service for all businesses, and warrants purpose-built security to protect users, apps and data on your network.

Here are our top 3 recommendations:

1. **Implement internal threat intelligence to protect your enterprise data and services.**

   Using real-time DNS analytics helps detect and thwart advanced attacks such as DGA malware and zero-day malicious domains.

2. **Make use of DNS for ensuring security compliance.**

   Integrating DNS with IPAM in network security orchestration processes helps automate management of security policies, keeping them current, consistent and auditable.

3. **Leverage DNS’s unique traffic visibility in your network security ecosystem to help SOCs accelerate remediation.**

   Implementing real-time behavioral threat detection over DNS traffic allows qualified security events rather than logs to be sent to SIEMs.

---

**View the DNS Security video**
To better understand the threats, their impact and how they can be averted.

**Explore the IDC Technology Spotlight**
Dealing with DNS-Based Data Breaches to Avoid GDPR Non-Compliance.

**Receive a free DNS Security Assessment**
To qualify your security risk exposure.

For more information, contact a security expert at EfficientIP.
About EfficientIP

A Network Automation and Security Company

Enable Dynamic & Secure Communication Between Apps & Users

DNS
DHCP
IPAM

Open Ecosystem Integration

110+ COUNTRIES

Safeguard Data
Protect Users
Ensure Service Continuity

USA — Philadelphia
EMEA — Paris
APAC — Singapore

1000+ Customers Across All Industries

Extend Visibility
Accelerate Deployment
Enforce Policies

About EfficientIP
A Network Automation and Security Company

Enable Dynamic & Secure Communication Between Apps & Users

DNS
DHCP
IPAM

Open Ecosystem Integration

110+ COUNTRIES

Safeguard Data
Protect Users
Ensure Service Continuity

USA — Philadelphia
EMEA — Paris
APAC — Singapore

1000+ Customers Across All Industries

Extend Visibility
Accelerate Deployment
Enforce Policies

About EfficientIP
A Network Automation and Security Company

Enable Dynamic & Secure Communication Between Apps & Users

DNS
DHCP
IPAM

Open Ecosystem Integration

110+ COUNTRIES

Safeguard Data
Protect Users
Ensure Service Continuity

USA — Philadelphia
EMEA — Paris
APAC — Singapore

1000+ Customers Across All Industries

Extend Visibility
Accelerate Deployment
Enforce Policies
Methodology

Analysis of this Infobrief is based on a survey IDC conducted on behalf of EfficientIP of 904 organizations across the world during the first half of 2019.

Demographics:

<table>
<thead>
<tr>
<th>REGIONS</th>
<th>NUMBER OF BUSINESS SIZE SEGMENTS</th>
<th>NUMBER OF COUNTRIES</th>
<th>NUMBER OF INDUSTRY SECTORS</th>
<th>METHOD</th>
</tr>
</thead>
<tbody>
<tr>
<td>Europe</td>
<td>5</td>
<td>9</td>
<td>10</td>
<td>CAWI + CATI</td>
</tr>
<tr>
<td>North America</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Asia</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Yearly comparison was carried out like for like with a survey from 2018.

Screener requirements: companies with 500 employees or more; all industry segments with quota per region; target respondents — IT decision maker or security expert.
International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications, and consumer technology markets. IDC helps IT professionals, business executives, and the investment community make fact-based decisions on technology purchases and business strategy. More than 1,100 IDC analysts provide global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries worldwide. For 50 years, IDC has provided strategic insights to help our clients achieve their key business objectives. IDC is a subsidiary of IDG, the world's leading technology media, research, and events company.

IDC is a subsidiary of IDG, the world's leading technology media, research, and events company. Further information is available on our websites at www.idc.com