IDC
Analyze the Future

IDC TECHNOLOGY SPOTLIGHT

Stopping Data Exfiltration and Malware Spread Through DNS

January 2018

By Robert Ayoub

Sponsored by Infoblox

Recent research from IDC predicts worldwide spending on security-related hardware, software, and services will reach $119.9 billion in 2021. Despite the overall increase in spending (over 10% from 2017), significant breaches are reported nearly every day from trusted brands. The resulting loss and impact on companies and individuals alike are substantial, and IDC expects that lost business will become a more tangible factor over time. Organizations must adapt and shift their defensive techniques in ways that can detect threats early and protect against data exfiltration. While many organizations utilize pattern matching and other traditional approaches to aid in detecting data theft, this control has proven to be inadequate when faced with multiple pathway scenarios used by modern attackers. This paper examines the use of Domain Name System (DNS) as one such pathway for data exfiltration and describes best approaches to protect against advanced malware and data exfiltration. It also looks at the role of DNS vendor Infoblox in addressing this strategically important challenge.

Introduction

A recent IDC survey of 2,500 consumers found that over three-quarters of respondents would be willing to switch providers if their data was lost to criminals.[1] CEOs, board members, and everyday end users will continue to seek ways to improve security despite the overwhelming size and scope of these breaches, which have become a common occurrence.

It's clear that we cannot halt the progression of overarching industry trends, which affect the way data is handled. Digital transformation (DX) is occurring, and organizations that do not embrace DX will be left behind. Securing the digital transformation is a key challenge for organizations that now must face a whole new set of challenges, including:

- Increased attack surface and constantly evolving attack techniques
- Visibility into new machines and services — especially difficult in virtual, cloud, and distributed environments
- Gaps in security exploited by bad actors

A 2016 IDC survey of security channel partners asked the question "What are the top attacks your customer networks are facing?" The top responses included "attacks designed to leak data" (phishing, ransomware, and spyware were also top answers). A different 2016 IDC survey asked CISOs what was keeping them up at night; unsurprisingly, the top responses were also related to data loss. However, despite increased spending on IT security over the past several years, data exfiltration remains a key challenge for even the largest organizations. The Equifax breach, in particular, illustrated that even the most trusted stewards of data had become prime targets.

[1] *Measuring U.S. Data Security and Privacy Sentiment: An IDC Special Report* (IDC #US42238617, January 2017)

While continued investment in traditional security products and controls is warranted, IDC also believes that organizations should examine the potential for other components in their infrastructure to aid in detecting and preventing against attacks, especially attacks that target the most sensitive data trusted by the organization. DNS is an often-overlooked infrastructure component, with most DNS services trusted to open source products. By considering a purpose-built, secure DNS product or service, organizations may patch significant gaps in their security infrastructure and gain additional visibility and protection that they are currently missing across the entire network.

Trends

Part of the challenge for enterprises has been to properly evaluate the number of toolsets on the market today. Ensuring that new investments can be augmented as opposed to relying on forklift upgrades every few years may also result in significant pressure from the board of directors. A secure DNS platform vendor can help organizations respond to these challenges by incorporating features that support the changing trends in security.

Malware continues to be more difficult to keep out of networks, with organizations often losing significant amounts of data before an attack is discovered

Ransomware attacks have proven to be extremely successful against large and small organizations alike. WannaCry and NotPetya made headlines for their ability to spread among a larger number of organizations in a very short time frame. While many organizations have refreshed their network security products over the past few years, only a few organizations are taking advantage of new advanced technologies. IDC believes that organizations will look to purchase advanced subscription licenses and services to battle ransomware.

Organizations expect their security devices to interoperate with each other and share threat data

Security can no longer simply focus on a single gateway, or a single set of machines; instead, it must be present whenever data or users are. For organizations that are deploying products or services, security is becoming a constant, inherent process, not simply an afterthought or the addition of a single process. A secure DNS solution must be able to provide correlation and context across a wider variety of vendors and environments than ever before.

DNS is being leveraged more often as part of the security infrastructure

While DNS is a core piece of the infrastructure, its ability to play a proactive part in the security of an organization is frequently overlooked. However, more and more vendors are becoming aware of the potential for DNS to provide greater visibility into the network and to help in the early detection of malware.

Solution and Best Practices

There are many benefits that come from moving DNS to a dedicated, well-supported secure product or service. Like other security product areas — firewall, security information and event management (SIEM), email, or web — DNS security adds another layer of protection to the enterprise. By implementing a secure DNS platform, an enterprise should be able to see several benefits such as detecting malware activity early before it spreads, blocking DNS data exfiltration, and keeping sensitive data safe and efficiencies gained by the security team by using data coming from core network services (e.g., DNS, DHCP, and IPAM data) to help the security team prioritize its response. These core services are providing data that, when properly analyzed and correlated with threat intelligence, will show evidence of an attack.

Instant visibility with context into devices and hosts within the organization

Enterprises cannot protect what they cannot see. It is imperative to discover all devices (on-premises, virtual, and in the cloud) and to have visibility into network topology (every IP address, switch port, and VLAN). Core network services such as DNS and DHCP see all the traffic passing across the network, although most of these products in the enterprise are not designed to convert that data into context, which helps prioritize critical threats in an IT environment.

A network visibility tool can easily leverage DNS data to provide instant visibility with context into devices and hosts within the organization regardless of location. By constantly evaluating history and comparing data against current threat intelligence, DNS can be used to gain insight into potential hacking activity before a breach even occurs. Because of the additional visibility, an attack can be stopped much earlier during the cyber kill chain. DNS can quickly detect communication with command and control servers and can detect a breach with much more certainty than solutions that are looking for data exfiltration such as DLP.

Plugging DNS security gaps and using DNS as a choke point to disrupt malware

As mentioned previously, many DNS products and services that are widespread today are open source and are not built to be secure. In fact, many attacks leverage weaknesses in the DNS to deliver and spread malware. By choosing a secure DNS platform, customers benefit from a dedicated security solution that can boost their organization's security posture together with the other security tools they may already own.

Additionally, a secure DNS platform can act as a choke point to disrupt malware. Utilizing a platform that leverages up-to-date threat intelligence (malicious hostnames, domains, IP addresses) means that any command and control (C&C) communications to these malicious destinations can be automatically blocked at the DNS level using a DNS Firewall Response Policy Zone (RPZ). Using behavioral analytics and machine learning on live DNS queries enables advanced threats such as zero-day DNS tunneling, data exfiltration, DGA, and Fast Flux to be detected and stopped. Device remediation can occur rapidly by having the platform seamlessly share early indicators of compromise (IoCs) in real time with advanced threat detection, threat intelligence platforms (TIPs), endpoint security, network access control (NAC), and SIEM technologies.

Accelerating response by sending events data to other security tools

A secure DNS platform can also help expedite the response to an incident by automatically sending IoCs to other security tools. By providing rich alerts with context, a secure DNS platform can inform SIEM solutions and other security devices of a potential attack, provide actionable network intelligence to prioritize response, and ensure that attacks are stopped quickly and effectively.

A variety of advantages are associated with the reporting provided by a DNS platform. While some of the key benefits are security related, other benefits associated with compliance and future planning can be realized. Some of the benefits that may be achieved with advanced reporting are:

- See top malicious hits with associated context
- Identify security risks and impacted devices
- Ensure compliance with historical visibility
- Plan future requirements with predictive reporting

Considering Infoblox

Infoblox security products enable organizations to mitigate security challenges that arise from DNS-based threats. The company's secure DNS solutions combine multipronged threat detection approaches including a combination of signature, reputation, and behavioral analytics; enhanced visibility; and a unique actionable intelligence drawn from the data residing in the core of the network. Infoblox detects DNS-based data exfiltration, DGA, and Fast Flux by combining reputation, signatures, behavioral analytics/machine learning, and its threat intelligence platform.

In addition to its on-premises solution, Infoblox provides a cloud-based security service for a true hybrid integrated solution that can protect devices and users everywhere — on-premises, roaming, and in remote offices. The company has robust ecosystem integrations and open APIs that make the existing security tools work more effectively and ease security operations. Infoblox is able to integrate with NAC, endpoint security, vulnerability scanners, and SIEM solutions and supports REST API output in many formats such as STIX, JSON, XML, CSV, CEF, and RPZ. These integrations help address the challenges mentioned previously and show the company's commitment to working with other industry participants to best secure customers.

Ultimately, Infoblox provides several solutions that help organizations find and automatically disrupt device communications with detrimental internet destinations. By combining its Threat Intelligence Feed with its Threat Insight streaming analytics–based solution, Infoblox can identify devices communicating with domains associated with C&C sites and data exfiltration and use a DNS Firewall RPZ blacklist to block any communications to them. Infoblox can quickly remediate compromised devices by having a DNS Firewall seamlessly share early indicators of the compromise in real time with other solutions such as threat intelligence platforms, endpoint security, NAC, and SIEM technologies.

Challenges

While Infoblox offers a strong malware and data exfiltration solution, it still faces many challenges in the market. First and foremost, Infoblox must overcome the mindset that exists around DNS and its relation to security. DNS has not traditionally been part of the security stack, and security practitioners do not have experience or familiarity with DNS. Infoblox needs to collaborate with its networking counterparts to establish itself as a go-to vendor for organizations seeking DNS security solutions.

Second, there is a great deal of confusion about who is responsible for securing DNS. Organizations often believe it is the responsibility of the service provider or the network team. Some organizations do not believe they should be configuring DNS at all. Until the security team within the organizations is ready and willing to take a proactive approach to leveraging DNS as part of the overall security strategy, Infoblox will have to make a considerable effort to educate the market.

Conclusion

Data exfiltration is the top concern of CISOs today. While investment in solutions continues to increase, CIOs' and board members' frustration with the ability of hackers to have continued success is growing. IDC believes that organizations must expand their thinking beyond traditional security solutions and look at other components of the infrastructure that can be improved. DNS is one of the areas where a fresh look at new tools can significantly improve an organization's ability to detect and stop malware and subsequently data exfiltration.

DNS security is an emerging area, and IDC believes that DNS security will continue to grow in importance and adoption. Although there are still some challenges around ownership and acceptance among potential adopting organizations, Infoblox has a significant opportunity for success if it is able to meet these challenges and proactively educate and inform CIOs and board members who are actively seeking ways to improve.

Global Headquarters: 5 Speen Street Framingham, MA 01701 USA P.508.872.8200 F.508.935.4015 www.idc.com