Infoblox®
CONTROL YOUR NETWORK

WHITEPAPER

How a DNS Firewall Helps in the Battle against Advanced Persistent Threat and Similar Malware

How a DNS Firewall Helps in the Battle against Advanced Persistent Threat and Similar Malware

As more and more information becomes available and is stored in electronic form, Advanced Persistent Threat (APT) actors will focus increasingly on breaching those networks and systems on which such data treasuries can be found. The definition breaks down into "advanced," meaning that intelligence is gathered beforehand about the target, while "persistent" refers to consistent monitoring and interaction of the target organization in order to achieve the goal. The "threat" is that the actors are well-backed financially, are motivated and organized, and have intentionality and capability with specific objectives.

These targeted attacks are more purposeful, resourceful and sophisticated than others experienced in the recent past. Though the incidence of these types of attacks is, as yet, small in comparison with the more familiar, automated or commoditized, broadly targeted electronic assaults, Advanced Persistent Threats can pose a much more serious menace to you and your valuable information.

The Infoblox DNS Firewall can play a critical role in reducing the risk of data loss (or other damage) from Advanced Persistent Threat (APT) attacks, whether these are made for commercial criminal reasons or are driven by states/state-supported actors. While we acknowledge that there is no single "magic bullet" to protect against all such attacks, proper implementation of the Infoblox DNS Firewall will help to:

- Reduce the risk of initial infection
- Limit the spread of the infection
- Impede data exfiltration, and
- Result in earlier detection of APTs and thereby remove the "persistent" nature of the attack

In order to explain how the Infoblox DNS Firewall helps protect against APT attacks, let's first examine the ways such attacks progress successfully from start to finish when no effective defense is in place.

The "Ideal" APT attack

When seen from the attackers' point of view, the "ideal" APT attack occurs in four discrete stages, each of which is serially dependent on the successful execution of the stage preceding it. First, the malware must infect a victim, usually in one of three ways via a forerunner. Secondly, the actual APT must be downloaded into the victim. Third, the APT must call home and decide how far, when and where to spread. Lastly, in the fourth stage, the APT seizes its prize — your valuable trove of data — and exfiltrate it by uploading it to one of its collusive servers.

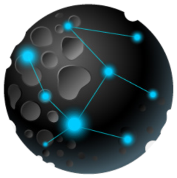
Let's look at each of these four stages in detail to see just how APTs achieve their nefarious goals.

Stage 1 – Initial infection

Generally, attackers infect an organization with their malware in one of three ways: a) by sending malware emails to persons within the organization; b) by infecting a website known to be frequented by people from the organization, commonly called a watering hole; and c) by direct physical connection.

A) Emails

Email attacks generally involve sending a plausible email that contains either an initial malware executable (embedded in, say, a PDF document) or a link to an executable on a server. The initial infection begins the moment the recipient opens the attachment or clicks on the link, assuming his system is not protected against the attack vector. Since, typically, most attacks occur on zero-day, chances are very good that his system will not be protected.



B) Watering Holes

The infection may be made directly to a specific site well-frequented by the users of the targeted organization — for example, by exploiting a particular vulnerability in a known part of the base system (e.g., joomla or wordpress) — or the infection may be encapsulated in one or more of the ads served on the site. In the latter case especially, smart attackers ensure that the malware is served only to computers whose IP addresses correspond to the external addresses of the organization in question, thereby reducing the likelihood of detection. The basic tactics of social media hacks, such as Facebook links, are essentially the same as those used in these watering hole infections, even though the context may be slightly different.

C) Physical Connections

Another effective but comparatively rare method of infection is by introducing the initial malware directly through a physical connection via a flash drive or similar device. The seminal victim is unwittingly tricked into installing the infected drive on his computer, thereby self-infecting the machine instantly. Once installed, methods of execution that work here are generally similar to the other two types. Some cases have been reported where the attacker has suborned an organization's personnel, say, one of the cleaning staff, into performing the installation intentionally.

Stage 2 – Download the Real APT

In almost all cases, no matter the method used for infection, the first key action the initial malware performs is to download the real APT from a remote server. This real APT will be far more capable of carrying the malicious intent to fruition than will the initial infection, whose primary function is expressly to exploit known zero-day vulnerabilities.

Stage 3 – Spread and Call Home

Once downloaded and installed, the first thing the APT will do — assuming the initial malware has not already done so — is disable any antivirus or similar software running on the now infected computer. Unfortunately, this minor but key task is usually not at all difficult. Then the APT will typically gather some preliminary data from its computer victim and any connected LAN, and will then contact a Command & Control (C&C) server to discover what to do next.

The C&C instructions may involve anything across a wide range of options — from a simple "remove yourself" to a virulent command to "aggressively scan for other vulnerable devices" — but in many cases the APT will simply be told to remain in place, quietly gathering data, and to ask periodically for further instructions. In those cases where the C&C instructs the APT to spread the infection, the APT will frequently attach a zero-day exploit to files that its victim touches or edits rather than noisily look for open/vulnerable computers. However, if the controllers are able to establish real-time two-way communication with the APT, the controllers can use clues gathered from the user's own files to identify the most promising avenues for further infection and can then instruct the APT to become more aggressive.

As the APT spreads, the initial device may act as a proxy for other infected devices if it turns out that they do not afford direct external access. However, in most cases, each newly infected device will first attempt to call home directly to the C&C and will only use the proxy if, for some reason, it cannot connect to the C&C.

Stage 4 – Data Exfiltration

A successful APT may identify terabytes of data that the attackers will want to see. In some cases, the APT will simply export these data via the same C&C servers from which they received instructions, but in many cases the bandwidth and storage capacities of the intermediate servers may be insufficient to transmit the data in a timely fashion. Moreover, the more steps involved in transferring the data, the more likely that someone will notice. Consequently, the APT is far more apt to contact a different server directly, essentially a "dropbox," for the purpose of uploading all the data.

The impact of a DNS firewall

A DNS firewall can block, either temporarily or permanently, any of the stages noted in the description of an ideal attack. One of the key weapons in the defense arsenal is the fact that the bad guys on the Internet trust relatively few intermediate servers and networks. Consequently, these collusive servers and networks tend to get reused over and over again. Going back to the same well time and again heightens the chances that some, or all, of the server infrastructure used by the attackers can be "discovered and categorized" and, therefore, blocked. This infrastructure-specific insight gives a DNS firewall its strength and the ability to thwart APTs and similar malware.

How the Infoblox DNS Firewall works

Simply put, the Infoblox DNS Firewall does its job by checking both the domain names it is requested to resolve and the IP addresses it returns against a list of currently identified malicious domains and IP addresses. This means that while lookups to benign sites like www.google.com are returned unchanged, lookups to domains that harbor malware or which are currently hosted on IP addresses known to harbor malware return an error (NXDOMAIN by default) instead of an answer. Infoblox compiles the list of current malicious locations from a variety of sources, ranging from publicly available data to proprietary data that is made available selectively. This critical list changes frequently, and Infoblox is careful to age out locations that are no longer malicious and compare all listed sites and IP addresses against the most current white-lists in order to eliminate false-positives. The scrubbed and refreshed lists are routinely transferred to the Infoblox DNS Firewall via standard DNS zone transfers, and the overall technical standard we use to implement the blocking is called Response Policy Zone.

Why list-checking blocks APTs

Attackers employ DNS because the ability to redirect contact from a server that has been taken down is so useful to them. Fastflux botnets and related attack mechanisms utilize DNS to keep the involved hosts in a state of constant change in order to reduce the chance that a single takedown will impact the entire net. In most cases, APT malware just uses the DNS configuration provided to the computer it is infecting to minimize its chance of being detected. Blocking or alerting access attempts to other non-standard DNS servers is a simple rule that can be placed into SEIMs, IDSes and the like, and thus the APT will try to avoid generating such alerts by using the configured DNS servers. As a result, any DNS server running the Infoblox DNS Firewall is able to see every DNS lookup the malware makes. This awareness enables the DNS firewall to determine easily which attempts to block.

Here's how the Infoblox DNS Firewall detects and stops APT attacks in each of the four stages:

Stage 1 – Initial infection

A DNS firewall can detect and block both email and watering hole attempts at infection, but in cases of physical connection, say, via a flash drive, clearly the DNS firewall will not be able to block this introduction of malware directly at the moment of infection. A DNS firewall may well stop mail delivery if the mail server is set to use Sender Policy Framework (SPF) and other similar mitigation techniques. Also, in cases where the malware is initially downloaded because the victim clicked on a link or visits an infected site in some way, the chances are quite high that the Infoblox DNS Firewall will block at least one link in the chain that leads to the initial exploit.

The chain is present because an attacker is rarely willing to allow his carefully crafted zero-day APT to be stored on computers outside his control due to the chance of discovery. So typically the initial browser visit is redirected one or more times before ending up at the server that drops the exploit. Even if the final dropper server is unknown, the chances are quite high that at least one of the intermediate servers will be a known malware supplier and, thus, will be on the list as an entity to which the DNS firewall should block a lookup. Without the complete chain, the initial exploit will not be downloaded.

Stage 2 – Download the Real APT

Even in cases where the exploit is introduced directly, the download of the real APT is another chance for the DNS firewall to block the attack. As with the exploit download described above, the chances are high that a server in the download chain will be known. In fact, it's quite likely that the attackers will reuse the DNS server employed to resolve the server name, and that IP address or domain name will be blocked by the DNS firewall.

Stage 3 – Spread and Call Home

As in Stage 2, the call home servers, the domain names used to resolve them or the name servers used to resolve their names may be known to the DNS firewall. The APT may also have a backup non-DNS-based call home method, but assuming that the DNS firewall logs are examined regularly for anomalies, the initial (failed) lookup using DNS will identify the infected device and allow for remediation. This failsafe mechanism dramatically reduces the persistence — and, thus, the danger and very nature — of the APT.

Moreover, DNS logs can help identify not just the initial infection but also the infected devices, as each one of these is likely to make similar DNS lookups in an attempt to call home.

Stage 4 – Data Exfiltration

The servers used in the data exfiltration stage are less likely to be shared with other attackers, which could make them difficult to detect and identify. However, they are quite likely to be hosted overseas, and often they are located in countries with lax enforcement of Internet behavior. If the DNS firewall is provided with geographic filters that block such countries, then any attempt to use DNS resolution in those countries is blocked and exfiltration is stopped. As with Stage 3, it is possible that a fallback, non-DNS-based method of contacting the dropbox server will exist, but again, it is highly likely that the first contact attempt will use DNS and, thus, the failure can be logged. Although this identification is late in the process, if the DNS firewall logs are examined regularly, there is a chance that the exfiltration can be interrupted in mid-upload, even if it is not fully prevented.

Summary

The Infoblox DNS Firewall is not a magic bullet that will stop all APTs, however it will block many of the initial infections by blocking the initial dropper and the download of the full APT. It will also quickly identify (if not block) subsequent attempts to call home. Should that effort fail because the collusive server infrastructure is not known, the DNS Firewall will subsequently identify infected computers by their attempts to call home for instructions. While this step does not stop the infection directly, it does allow for a timely response that ensures the threat is no longer "persistent," even if it is advanced. Finally the geographic blocking abilities mean that the Infoblox DNS Firewall will impede and alert any ensuing data exfiltration stages that might begin to be executed.

All told, stage by stage, the Infoblox DNS Firewall can play a critical role in reducing the risk of data loss or other damage due to Advanced Persistent Threat, and is currently the best available defense against this new and highly worrisome cyber danger.

CORPORATE HEADQUARTERS:

+1.408.986.4000

+1.866.463.6256

(toll-free, U.S. and Canada)

info@infoblox.com

www.infoblox.com

EMEA HEADQUARTERS:

+32.3.259.04.30

info-emea@infoblox.com

APAC HEADQUARTERS:

+852.3793.3428

sales-apac@infoblox.com