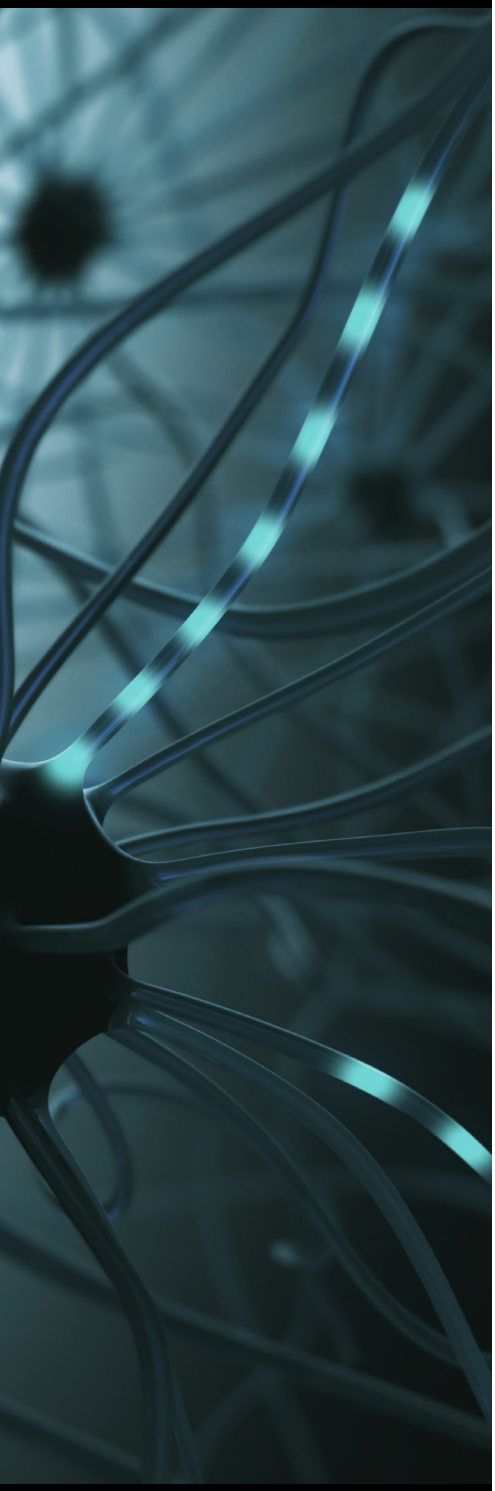
efficient iP®

White Paper



Enhancing Threat Intelligence Services for Holistic Network Security

Zero trust philosophy demands end-to-end security for today's complex networks. To do this properly requires massive amounts of data to be treated, so threat intelligence has become essential, both on domain names and in the context of the enterprise.

Outline:

In today's ever-evolving threat environment, managing security across a company's IT infrastructure is a mighty task. Increasing network complexity, together with the extreme diversity and growth of menaces, is making it extremely hard for security managers to identify suspicious activity. It is essential therefore that companies stay aware of the threat landscape, by making use of high-quality threat intelligence as part of their overall network security strategy. This threat intelligence needs to provide protection for two main purposes: 1. For global users 2. For enterprise services.

Mainly, using intelligence from external sources only brings advantages for widespread menaces at internet scale. So to protect internal networks, it really needs to be complemented with behavioral threat detection solutions in the context of the enterprise. DNS is ideally placed to provide this - being a key component of any infrastructure and having unique visibility over network activity. This makes DNS the first line of defense for any network, in addition bringing detection capability of malicious zero-day attacks, and predictive security functionality. Such protection is invaluable, considering the rapid growth in domain names being created - over 350 million exist today, with approximately 8 million new ones being registered each year[1].

Hence the near-real-time threat information offered by DNS simply must be utilized to help enhance detection and mitigation capabilities of any SOC (Security Operations Center). This sharing of information between resources is key for improving the network security ecosystem, in order to provide holistic protection from menaces.

1 *Verisign's 2018 report on the global domain name system industry*

Threat Landscape Today

Number of Domains Exploding, Threats Dynamic and Evolving

DNS is a critical network foundation, providing routing to every app & service. As such, it's a powerful indicator of network activity, so should be made use of to detect suspicious behaviors, including data exfiltration and C&C (command and control). However, complexity is increasing dramatically, as millions of new domains are being created every year - often with the help of Demand Generation Algorithms (DGAs) - due to generic TLDs multiplying the number of domains possible. Added to this is the constant threat of these domains being diverted, websites infected or corrupted, and IP addresses hijacked. All this put together means it's now become very challenging to determine which domains are suspicious, and which are not.

The threats themselves are dynamic, and constantly evolving. Tens of millions [2] of new malware are created every year - with the majority of them using DNS - forcing companies to find best methods to stay aware of the threat landscape. While categorizing these threats using Indicators of Compromise (IoC's) helps prioritize countermeasure action, it's also important to contextualize them, in order to make the remediation process as efficient and as accurate as possible.

Understanding Threat Intelligence

What is Threat Intelligence?

Simply put, threat intelligence is the knowledge of a threat's capabilities, resources, motives and goals. Threat intelligence enables companies to identify their adversaries, allowing them to carry out decisive action - taking policies into consideration - for defending better their network-based assets. Gartner notes that this knowledge helps organizations make informed decisions on how to respond and react to a particular threat.

Intelligence can be obtained from two sources: external and internal.

External sources are usually built using data collection, AI, and ML (machine learning). However, they can vary tremendously in terms of their "quality". Commercial sources include threat intelligence feeds, structured data reports (e.g. STIX), unstructured reports (e.g. PDF and Word documents), and emails from sharing groups. Whatever you use, it's advisable to make sure the information is complete, accurate and up-to-date.

But simply relying only on external sources is insufficient. Advanced threat intelligence needs to integrate internal sources for granular threat detection in the context of the enterprise, and not only at the Internet scale. Without this second level of analysis, emergent and Advanced Persistent Threats (APT) will go unnoticed. Proactive security needs predictive security!

Global intelligence will unfortunately provide limited protection for your enterprise, in particular against low-signal and targeted attacks. Intelligence truly relevant to your organization can therefore really only come from your own network.

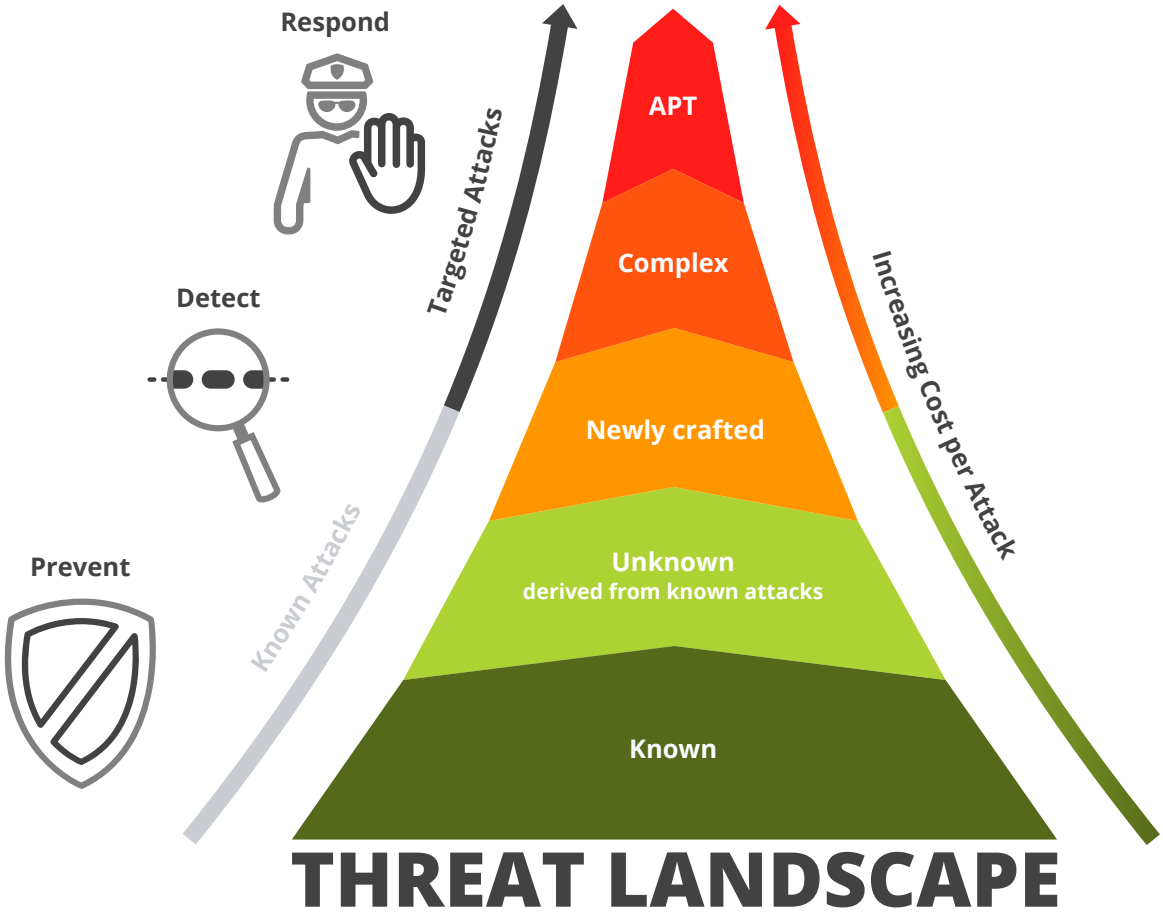
---

2 MacAfee Threat Report 2017

Why is Threat Intelligence Important?

Tactics, techniques, and procedures (TTP) used by cybercriminals are becoming more and more sophisticated, outpacing stand-alone security solutions, and so allowing them to bypass uncoordinated defenses. Adversaries are often state-sponsored groups or organized criminals, who have the tools, training, time and resources to breach most conventional network defense systems. Often, they rely heavily on APTs to help maintain rogue access to compromised networks/resources, allowing them to carry out multi-year campaigns targeting valuable, sensitive data.

When it comes to threats, if you're only in "reactive-mode", you're constantly playing catch-up. So to give your organization a fighting chance of defeating ever-changing threats, your security program needs to be led by threat intelligence. This starts with a holistic view of the threat landscape, followed by constant harvesting and processing of knowledge about threat actors. The only way to reduce the chances of success of an adversary is by knowing the who, what, when, where, and how of their actions. That's why threat intelligence needs to be brought in.



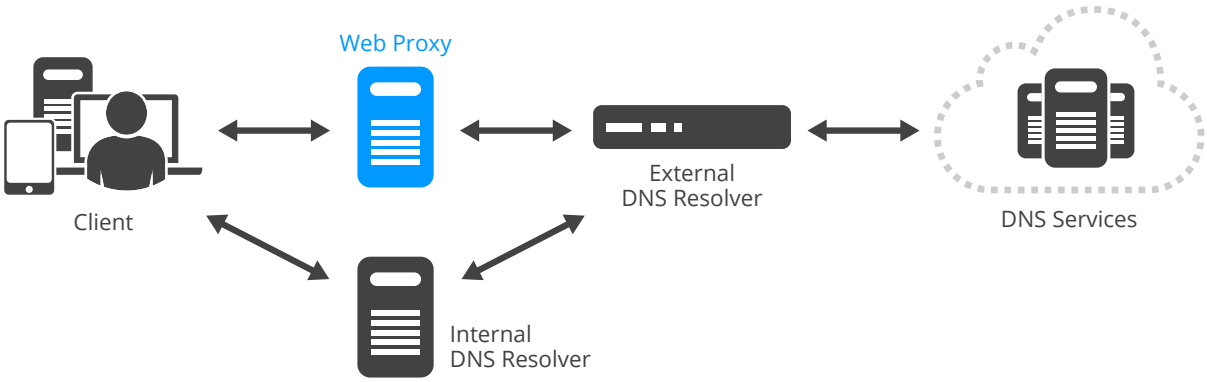
Threat categories, impact and security measures

Existing DNS Threat Protection Solutions

Various solutions are already in place today at many organizations to help protect connected assets and resources. Amongst these are anti-virus, web proxies including filtering, Next-gen Firewalls, and DNS RPZ, which are all great tools, but have important limitations. The good news is that it is possible to leverage them to help provide more complete, effective protection.

Proxies/Web Filtering

Proxy servers are able to control requests relayed in one or both directions, applying appropriate filtering policies. But some devices, such as those used for IoT projects, do not support proxy configuration and cannot therefore be forced to use them. Also, when using applications such as VoIP or ERP, the client often accesses external DNS via the internal resolver, thus totally avoiding the proxy.



Even with Web Proxy, DNS is still used

In addition, having a proxy does not prevent DNS being manipulated for malicious purposes. Generally, web proxies themselves are not designed to provide DNS security mechanisms. The few that do are quickly undermined by the attacker, as the mechanisms prove to be limited and simple: maximum FQDN size, and maximum subdomain size, are the most commonly seen available options. So menaces can go unnoticed, in particular data exfiltration. The logical step is therefore to combine proxies with specialized DNS security, protecting end clients as a result. This DNS security enforces existing security levels provided by the proxy - by filling the hole left by this protocol.

As DNS Security is very complementary to proxies, it complies perfectly with the common ideology of network security being about making all pieces of the network security ecosystem working together.

Next-Gen Firewalls (NGFW)

NGFWs leverage DPI (Deep Packet Inspection) technology to detect threats with various methods including pattern matching, data encoding, signature identification and heuristic analysis.

However, their restricted visibility over transactions means they have weak traffic analysis capacity for threat detection. NGFWs also suffer from behavioral-based threat detection capacity being limited to packet frequency, request entropy, and payload.

This means that abnormal use of cache by clients cannot be detected, resulting in, for example, data exfiltration over DNS queries going unnoticed.

DNS Filtering/RPZ

DNS filtering is a technique of blocking access to certain websites, webpages, or IP addresses. If a particular webpage or IP address is known to be malicious, the request to access the site will be blocked. Instead of connecting to the website, the user will be directed to a local IP address that will display a block page explaining that the site cannot be accessed.

DNS filtering adds an extra security system prior to the web proxy being reached. It offloads the workload for the proxy by optimizing feeders and architecture (thus eventually bringing down operating costs), and increases security by focusing on threats hidden in URLs based on legitimate domain names.

DNS Response Policy Zones (RPZ) provide a highly valuable first line of defense and an effective approach to stop ransomware, phishing and malware infections earlier, identifying already infected devices faster and mitigating data exfiltration attempts through known malicious domains and IPs. In summary, RPZ blocks attempts to reach malicious targets.

How Should DNS Threat Intelligence be Built and Applied

For effective handling of threats, the two key parameters relate to: 1) How data is collected 2) How the information is used. Quality feeds, providing information relevant to your particular enterprise, are mandatory for achieving both of these.

Make Use of High-Quality Feeds

Select an External Feed

One of the most important considerations is choosing a high-quality external feed. Whilst it obviously needs to cover a comprehensive list of domains/IPs, the actual size of feed is less relevant for influencing quality of the information provided. What's more important is accuracy, which relies on the feed being updated regularly. Due to the dynamic environment it works in, regular cleaning of the feed is absolutely necessary.

Important criteria which help define a high-quality feed include:

- feed updated every few minutes
- worldwide coverage of malicious domains
- global collection of traffic with analysis on a per-client basis
- use of machine learning and predictive analytics
- control of spam and malware
- effectiveness against hard-to-detect phishing and botnets domains
- efficient handling of false positives

A good example of a high-quality feed is SURBL, which has one of the most comprehensive and accurate list of 'current, active' bad domains - over 800,000 as of today. The feed is updated every 1 to 2 minutes, offering near-real-time threat intelligence.

Construct Your Own Internal Feed

For internal feeds, what's most important is the capability to collect a maximum amount of data related to activity on your network (alerts, logs, traffic flow), in order to recognize behavior associated with threats. With this in mind, the ideal "tool" for helping you build your own threat intelligence is the DNS itself.

"detection of zero-day malicious domains is mandatory"

Due to the fact that threats are constantly evolving and becoming more and more discrete and targeted, there is a need for context-aware behavioral threat detection. DNS offers this, bringing with it predictive security capability. Take for example an advanced DNS security solution which has detected a data exfiltration attempt - the detection can lead to knowledge of the domain associated with this menace, meaning that other network security components can be alerted to immediately block the non-categorized domain. Consequently, zero-day malicious domain detection becomes automatically included in the overall threat intelligence strategy.

Because of DNS's major role in the attack schema (91% of malware use DNS, according to Cisco's 2016 Threat Report), it is undoubtedly crucial to implement an advanced DNS analytics solution as part of the essential tooling of any SOC.

Combine External and Internal Feeds to Enhance your Threat Intelligence solution

Aggregating information from external feeds and internal feed obviously provides the most complete threat detection capability. It emphasizes the fact that DNS is both at the forefront of your threat intelligence solution, as well as being a major contributor to the overall security of your network.

DNS Becomes a Critical Choke Point

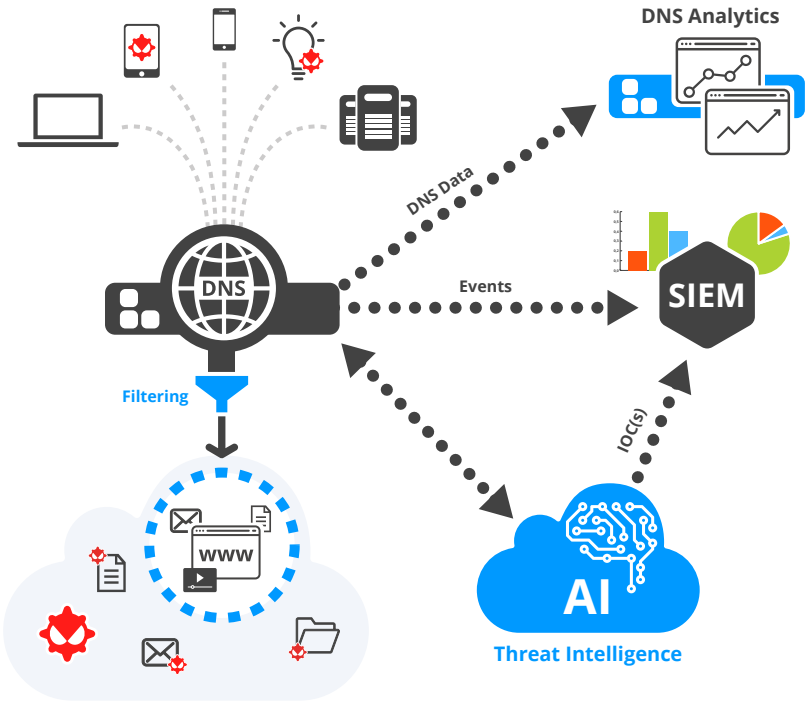
An ideal combination of DNS Analytics + DNS Firewall + external feed offers the following capabilities:

- proactively implement and manage security controls to thwart advanced attacks.
- near real-time threat intelligence for countering exfiltration. This maximizes threat response efficiency, permitting permanent blackholing of locally identified suspicious domains. The external security feed (e.g. SURBL) adds security intelligence from global traffic analysis.

Contributing to Overall Network Security

The Zero trust phenomenon means that enterprises are putting more emphasis on improving end-to-end security. But today's networks are incredibly complex. Securing them adequately demands treating huge amounts of data, so threat intelligence has become vital.

Intelligence on domains is already being worked on by many actors, making use of AI & ML. But for protecting enterprise users & discovering malware, DNS is ideally placed. It has a specific view of what activity is going on in the network, as well as having intelligence on network users, allowing context-aware analysis of DNS traffic for creating information which can be offered to SIEMs and external threat intelligence solutions to help find and isolate the suspicious clients. This global approach is absolutely necessary for helping security operations take the best course of action for mitigation



The key role of DNS for overall network security

For Actionable Intelligence, Focus on Events, Not Logs

Among the huge amount of domains in existence today, most domains are legitimate, but a lot are compromised, and many have been registered specifically for malicious purpose. Detecting those domains and their associated traffic is hard work, requiring much time, effort and specialized skills.

So subscribing to threat intelligence to maximize your chances of detecting malicious traffic is a wise choice. In addition, integrating the provided information feed with secure DNS engines, will feed your SIEM with invaluable security events.

Today's SOC personnel are becoming overwhelmed with workload required to treat data and alarms raised for potential threats. Combining a quality threat feed with DNS analytics can help you turn these mountains of data into real actionable intelligence.

Conclusion

Threat intelligence is crucial for holistic network security, in order to protect users, apps and services. Threat information can come from two complementary sources - external and internal feeds. When combined, they secure networks both at internet scale and enterprise-wide.

Internal sources are key for providing predictive security, including data exfiltration on non-categorized domains. DNS is central to the infrastructure, making it ideally placed to provide data on events from internal networks, thus is without doubt essential to the global security strategy of any company.

efficient iP®

REV: C-180816

Americas
EfficientIP Inc.
1 South Church Street
West Chester, PA 19382-USA
+1 888-228-4655

Europe
EfficientIP SAS
90 Boulevard National
92250 La Garenne Colombes-FRANCE
+33 1 75 84 88 98

Asia
EfficientIP PTE Ltd
60 Paya Lebar Road #11-47
Paya Lebar Square SINGAPORE 409051
+65 6678 7752