

We offer free Secure Recursive DNS - blueAPACHE

Canonical: <https://www.blueapache.com/blog/blueapache-offers-free-recursive-dns-internet>

Details:

2016

We extend Internet offering to include free secure recursive DNS services with integrated blacklisting for all emPOWER Internet customers. The rapid rise in sophisticated threats like zero-day malware, Trojans and advanced persistent threats makes cybersecurity a daunting challenge for both individuals and businesses. In their simplest form, many scams rely on the poor security habits of users, such as clicking on links or attachments in spam emails, to succeed. According to the Internet Security Threat Report published earlier this year by Symantec Corporation, on average, each business user sent and received 42 emails each day, with spam accounting for more than half of inbound business email traffic in 2015. As regularly mentioned (including in our recent PayPal Scam news), tricking users into visiting a malicious domain by clicking on spam emails is a common approach used by criminals to launch targeted and personalised phishing and malware attacks against organisations. There are also numerous instances of legitimate websites that have been hacked and, unknown to its administrators, malicious code embedded into it. These compromised websites act as effective bait for victims who might believe that they are visiting a trusted website, but in reality, are allowing cyber criminals to send malicious code directly to visitor's computers. Despite extensive use of network security measures, the reported number of successful breaches has continued to rise. Enterprise security today can no longer rely solely upon the old cornerstones of traditional firewalls, built-in security tools or anti-malware software. Instead, organisations need a broad-based, holistic and resilient approach to cyber security.

We offer emPOWER secure recursive DNS service at no cost

In our continued effort to proactively respond to today's constantly evolving threat landscape, we have expanded our Internet offering to include emPOWER secure recursive DNS. It is different from industry standard recursive DNS thanks to the integrated site blacklisting that automatically blocks known malicious sites. This service is offered to existing emPOWER Internet customers for free . It is also offered free to all new emPOWER Internet customers.

"We wanted all of our emPOWER Internet clients to benefit from the extra security our recursive DNS brings" said James Hendry, General Manager Commercial within our business. "Integrating blacklisting adds to our service costs, but offering it as a free upgrade reinforces our commitment to securing our clients. If it helps only one customer avoid downtime caused by ransomware or malware, the investment we are absorbing will be easily justified". While recursive DNS is not a standalone security solution by itself, integrating blacklisting adds another layer to existing solutions including email security, next-generation firewalls, end point security and zero trust networks, to create a stronger and more scalable security posture. Email security provides the first level of protection by filtering emails sent and received at the network / internet perimeter, and blocking incoming threats such as spam, phishing attacks, viruses, malware and malicious links. The secure recursive DNS service offers the next level of protection, blocking access to known malicious links should an email make its way to a user. How it works The secure recursive DNS service acts as a gatekeeper between your organisation and the outside world by blocking access to malicious domains and preventing users from inadvertently compromising the security of your data and systems. Built into the emPOWER secure recursive DNS service is a lookup filter that utilises a real-time database (also called the Domain Block List or DBL) of

malicious domains. The DBL is a database of spam payload URLs, spam sources and senders, known spammers and spam gangs, and virus and malware-related sites that are typically found in spam messages. This database is maintained by a dedicated team of specialists who constantly analyse and update it with malicious domains identified from around the world. It can be queried in real-time to recognise, tag and block domains that have previously been identified as being malicious. If an emPOWER Internet user clicks on a link or tries to browse to a website that appears on the DBL, they will see the blueAPACHE block page, instead of the domain they are trying to access. Most ransomware including Cryptolocker , are launched using malicious links that direct users to a compromised website. The ransomware are typically programmed to 'talk' back to the attackers by looking up the domain name for its Command and Control (C&C) server. However, if the domain name appears on the DBL, the recursive DNS service is able to block the malware from communicating with its C&C server, rendering it useless. In summary, emPOWER secure recursive DNS service is a simple addition to secure your users' Internet experience by blocking unsafe sites. Simple, effective and free. It is an additional element in a multi-pronged, multi-layered approach to security that can lead your organisation to a more reliable, stringent level of protection against targeted, phishing and other advanced malware attacks. If you would like secure recursive DNS added to your emPOWER Internet, contact our account team .

Reading this historical announcement

This 2016 article describes the DNS-filtering service and availability announced at that time. DNS filtering was presented as an additional security layer alongside email, firewall and endpoint controls. The article does not establish the service's current availability, implementation or pricing; contact our account team to confirm those details for your Internet service.

What service did the 2016 announcement offer to emPOWER Internet customers?

The 2016 announcement offered secure recursive DNS with integrated site blacklisting free to existing and new emPOWER Internet customers. Contact us to confirm current availability and terms.

How is your secure recursive DNS different from industry standard recursive DNS?

It is different from industry standard recursive DNS because it has integrated site blacklisting that automatically blocks known malicious sites.

Who commented on the launch of the free secure recursive DNS service, and what did they say?

James Hendry, General Manager Commercial within our business, said, "We wanted all of our emPOWER Internet clients to benefit from the extra security our recursive DNS brings," and added, "Integrating blacklisting adds to our service costs, but offering it as a free upgrade reinforces our commitment to securing our clients. If it helps only one customer avoid downtime caused by ransomware or malware, the investment we are absorbing will be easily justified."

How did the 2016 article describe the service working?

The 2016 article described a lookup filter using a Domain Block List of known malicious domains, maintained by specialists and queried in real time. Confirm the current service implementation

separately.

What happens if an emPOWER Internet user tries to access a site on the Domain Block List (DBL)?

If a user clicks on a link or tries to browse to a website that appears on the DBL, they will see the blueAPACHE block page instead of the domain they are trying to access.

How does the recursive DNS service help against ransomware like Cryptolocker?

The article described blocking communications to known malicious command-and-control domains listed on the Domain Block List. This is an additional control; it does not guarantee that ransomware is prevented or rendered harmless.

Why did you expand your Internet offering with secure recursive DNS in 2016?

We expanded our Internet offering to proactively respond to the constantly evolving threat landscape of sophisticated cyber threats like zero-day malware, Trojans, and advanced persistent threats, recognizing that a broad-based, holistic and resilient approach to cyber security is needed beyond traditional firewalls and anti-malware tools.

Is the secure recursive DNS service meant to be a standalone security solution?

No, recursive DNS is not a standalone security solution by itself; integrating blacklisting adds another layer to existing solutions such as email security, next-generation firewalls, end point security, and zero trust networks to create a stronger, more scalable security posture.

How can a customer get secure recursive DNS added to their emPOWER Internet service?

Contact our account team to confirm whether secure recursive DNS is available for your service and what its current scope and terms are.