HYAS

OFFICE
500 - 3 FAN TAN ALLEY
VICTORIA BC V8W 3G9 CANADA

PHONE
+1 778-817-0246

EMAIL
info@hyas.com

Office of Electricity, Department of Energy (DOE)
Request for Information (RFI)

HYAS

HYAS

7 June 2021

Bid to include Protective DNS as part of the continued security of the United States Critical Electric Infrastructure

Point of Contact: Rob Kleinberg
Email: rob.kleinberg@hyas.com
Phone: (720) 450-6544
Agency: Department of Energy
Document Citation: 86 FR 21309
Page: 21309-21312
Document Number: 2021-08482

Address:
HYAS Infosec
500 - 3 Fan Tan Alley
Victoria, BC V8W 3G9 Canada

Table of Contents

Executive Summary

HYAS is pleased to respond to the Office of Electricity, Department of Energy (DOE) Request for Information (RFI). As a recommendation for the DOE we present the mandatory use of a Protective DNS solution within the United States Electrical Grid, specifically the use of HYAS Protect. HYAS has constructed what is arguably the world's most unique data lake of attacker infrastructure including unrivaled domain-based intelligence. We take a different approach as opposed to focusing on the attack we look at the attacker and their infrastructure. Our data is dynamic and ever-growing giving our clientele access to up to date and accurate adversary infrastructure to preemptively block and/or disengage with malicious infrastructure at the DNS layer.

Protective DNS services are now being recognized by the most respected agencies as a necessary part of a comprehensive security stack. These agencies include, but are not limited to the NSA, CISA, and the National Cyber Security Centre. The world has entered a new frontier of cyber threat and no stone should be left unturned. Protecting the DNS layer of the United States Electric Grid is essential.

HYAS Company Information

Founded by a team of world-renowned security researchers, analysts, and entrepreneurs, HYAS is rapidly growing with commercial and government customers. As of June, 2021 HYAS founder, Chris Davis is one of only three civilians to receive the FBI's Director Award. Chris earned this prestigious award for the exemplary work he did on bringing down the Mariposa Botnet. The leadership team is split between California and Canada, includes two PhD's and over a combined century of building companies, products, and cybersecurity: David Ratner, Ph.D (CEO), Jonathan Candee (CRO), Paul van Gool, Ph.D. (VP of Engineering), Melissa Blanchard (VP Operations and Finance) and Chris Davis (Founder & Technical Advisor).

What is Protective DNS?

The Domain Name System (DNS) is central to the operation of modern networks, translating human-readable domain names into machine-usable Internet Protocol (IP) addresses. DNS makes navigating to a website, sending an email, or making a secure shell connection easier, and is a key component of the Internet's resilience. As with many Internet protocols, DNS was not built to withstand abuse from bad actor's intent on causing harm. "Protective DNS" (PDNS) is different from earlier security-related changes to DNS in that it is envisioned as a security service – not a protocol – that analyzes DNS queries and takes action to mitigate threats, leveraging the existing DNS protocol and architecture.

-Executive Summary. *Selecting a Protective DNS Service*, NSA/CISA, 2021.
https://media.defense.gov/2021/Mar/03/2002593055/-1/-1/0/CSI_PROTECTIVE%20DNS_UOO117652-21.PDF

Addressing the Issue – RFI Question 1

"What technical assistance would States, Indian Tribes, or units of local government need to enhance their security efforts relative to the electric system?"

Virtually all malicious software uses domain names in attacks, either for payload delivery, C2, or data exfiltration. Conventional network security approaches can fail to keep up with new, rapidly evolving threat infrastructure. By combining HYAS's proprietary threat attribution knowledge, analysis of C2 communication patterns for hundreds of thousands of daily new malware samples, and proprietary multivariate algorithms, HYAS Protect provides unparalleled visibility into attackers' assets and infrastructure, which can be utilized to uniquely and definitively answer key questions for analysts, enhance existing assets in the security stack, and even provide an added and critical layer of protection. Even before a bad actor launches an attack involving communication to a malicious domain. HYAS Protect knows a domain's reputation and can provide a verdict that both enhances existing toolsets and preempts attacks, enabling a fundamentally more secure environment.

HYAS Protect is a cloud-based applications hosted in Microsoft Azure. This cloud-first approach provides the scalability, security, and flexibility to meet the US Federal Government's demanding requirements.

HYAS Protect – Protective DNS Solution

HYAS Protect is deployed as a cloud-based DNS security solution or through API integration with existing solutions. HYAS Protect combines infrastructure expertise and multi-variant communication pattern analysis to deliver reputational verdicts and actions for any domain and infrastructure, allowing enterprises to preempt attacks while proactively assessing risk in real-time. HYAS Protect can enforce security, block command and control (C2) communication used by malware, ransomware, and botnets, block phishing attacks, and deliver a high-fidelity threat signal that enhances an existing security and IT governance stack.

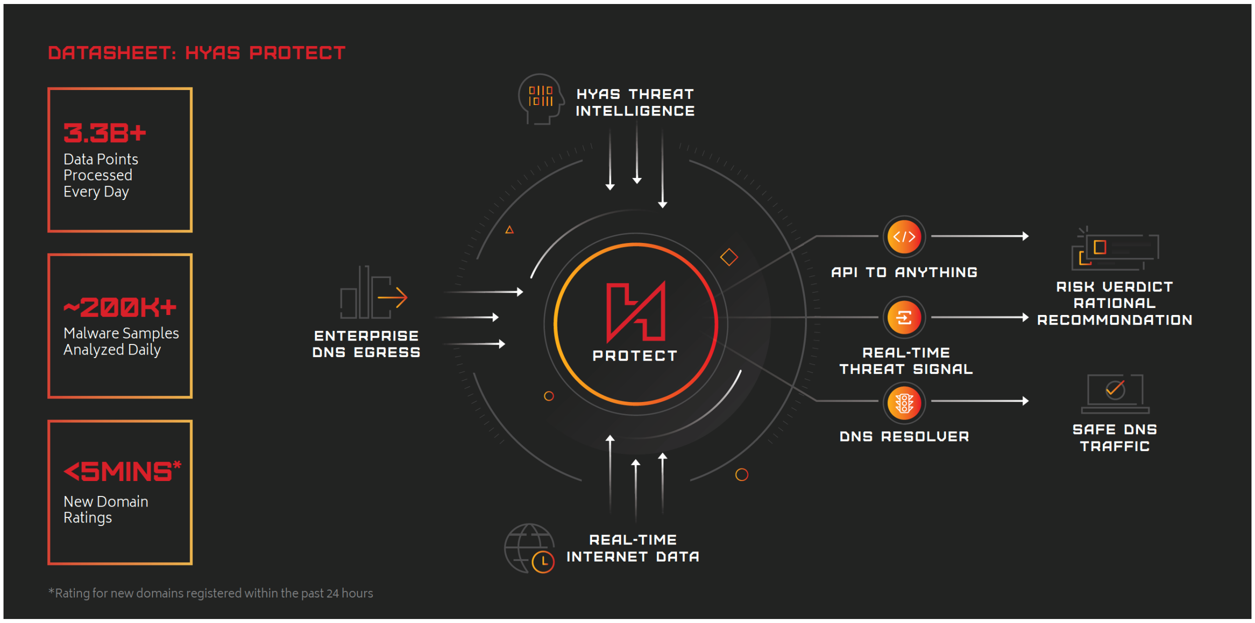

Figure 1 – (HYAS Protect)

HYAS Protect Deployment Options

DNS Resolver - HYAS Protect operates as your DNS resolver to block bad domains, IPs, and nameservers with superior security, reliability, and performance; deploy in minutes across your entire infrastructure; built-in support for Domain Generation Algorithm (DGA) detection, DNSSEC, DNS over HTTPS and DNS over TLS.

Real-Time Threat Signal - Verdicts and analysis of your DNS traffic augment existing security systems via API integration into your SIEM, SOAR, Firewall, or other component in your security stack.

Investigation and Static Analysis - Enable security operations center (SOC) teams investigating incidents to evaluate suspect domains or perform a static analysis of DNS egress traffic.

What Does Protective DNS Provide?

Proactive Security - Identify and prevent attacks before they happen, independent of protocol, for devices inside and outside your network. Flexible deployment supports WFH/hybrid work models and protects IoT devices.

Augment Existing Investments - Integrate via APIs with existing SIEM, SOAR, firewalls and other systems with reputation, rationale, and related data from HYAS Protect.

Dissect DNS to Augment Existing Investments – Understand your DNS traffic, sort and filter for high-risk behavior, and feed that knowledge via APIs into existing SIEM, SOAR, firewalls and other systems with risk, rationale, and related data.

Threat Visibility - HYAS Protect provides a high-fidelity threat signal to reduce alert fatigue and improve your network intelligence. Detect and block low-and-slow attacks, supply chain attacks, and other intrusions that are hiding in your network.

Avoid Ransomware, Phishing and Supply Chain Compromise - Stop attacks before they get started by blocking malicious domains and ensuring that users don’t accidentally communicate with adversary infrastructure

Conclusion

The goal of any comprehensive cybersecurity program is to draw down risk. Protective DNS provides an essential layer of security and is a foundational solution that can integrate seamlessly with existing solutions to provide increased network visibility, intrusion detection, preemptive blocking, and actionable alerts. The net result is enhanced functionality of already implemented solutions and increased security team efficiency.

We invite you to please reach out for a demo of HYAS Protect and see first-hand how Protect can be utilized to make our nation's electric grid stronger and more resilient.

Thank you and please reach out Rob Kleinberg for further information.

Point of Contact: Rob Kleinberg
Email: rob.kleinberg@hyas.com
Phone: (720) 450-6544
Address:
HYAS Infosec
500 - 3 Fan Tan Alley
Victoria, BC V8W 3G9 Canada