A Brief Guide to IT Hygiene

Aitē PARTNER. ADVISOR. CATALYST.

IMPACT BRIEF

APRIL 2020

Joseph Krull, CISSP, IAM, CISA, CRISC, CIPP
+1.210.421.8233

Ahead of the Curve: Accelerate Cyber Response With DNS Insights

The Domain Name Service (DNS) functions like a giant phone directory to power the internet. Humans have a hard time remembering multiple strings of random numbers but can more easily remember proper names and words. For example, it would be quite challenging to remember the internet protocol (IP) addresses 64.233.160.0 and 69.63.176.13, but it is much easier to remember www.google.com and www.facebook.com. DNS works diligently in the background to convert those names into IP addresses and facilitates routing of requests to the proper destination on the internet. For most internet users, the power and technology behind DNS are simply unknown; however, for savvy cybersecurity professionals, DNS data can be an important tool used for both active cyber defense and investigative/forensics purposes.

DNS-derived data can reveal a broad range of attacker activities, including registration of new domains to support attacks and creation of command and control (C2) servers for malware, phishing, and ransomware. Also, because DNS data can flow freely into and out of networks, attackers actively use DNS data streams to exfiltrate stolen data and avoid detection.

Until now, using DNS data for cyber defense was limited by three key factors: timeliness of data, the need to analyze extremely large data sets, and the requirement for expert analysis by traditionally overworked cyber analysts. This Impact Brief describes how DNS can be used as part of a comprehensive cyber defense program, recent developments related to accelerating the availability and analysis of DNS data feeds, and an example of how one organization uses DNS data to rapidly detect and block attacker activities.

Do you have a comprehensive cyber defense program?

Until now, using passive DNS data for cyber defense was limited by three key factors: timeliness of data, the need to analyze extremely large datasets, and the requirement for expert analysis by traditionally overworked cyber analysts. This Impact Brief provides information on how passive DNS insights can be used as part of a comprehensive cyber defense program, recent developments related to accelerating the availability and analysis of DNS data feeds, and an example of how one organization is using UltraThreat Feeds to rapidly detect and block attacker activities.