SecureDNS℠

/ DOMAIN DEFENSE

Defense against domain-based threats—before they happen

Fighting modern cybercrime, earlier—better

An attack on your network is systematic—involving lots of phases in the kill chain. After the initial stage of reconnaissance, cyber attacks move into weaponization of the exploit before delivering the malicious attachment or redirected web link. By disrupting the attackers infrastructure, SecureDNS proactively blocks the initial exploit from ever evolving into a malicious attack.

Furthermore, most attacks with the objective of data exfiltration initiate command and control callback—a phase later executed in the kill chain. SecureDNS, leveraging advanced threat intelligence from ShadowNet™, identifies where those bad domains and bad IPs are staged—effectively preventing both infiltration and exfiltration at the DNS and IP layers.

Threat prediction. Real-time protection.

Technology has reached a high level of user prediction—real-time learning. Much like how Netflix* studies your watching habits to suggest similar shows, SecureDNS detects threats from internet activity and can deliver timely training to users.

Our veteran threat intelligence team at RA Labs analyzes the malicious data in real time to provide an always-on defense that complements an organization's existing security infrastructure. The information we process includes:

- / Where threats originated
- / Who is behind them
- / Command and control callback
- / Breadth of threats
- / Frequency of threats

Killing the kill chain

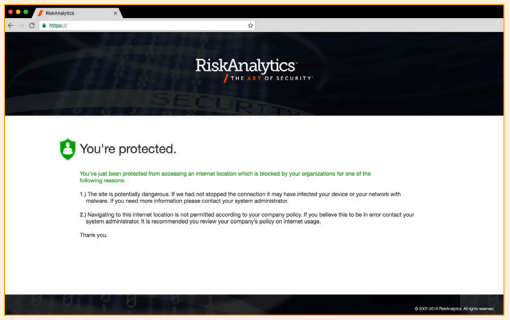
Combining human threat intelligence with mechanized mitigation, threats are blocked before malicious attacks like phishing, ransomware and botnets even take shape or come close to reaching your network perimeter. This preemptive kill chain approach prevents malicious communications before they begin—proactively redirecting users to a safe landing page or sending the bad traffic to a sinkhole. SecureDNS is the intelligent intervention you need to keep your organization a step ahead of new and emerging cyber threats.

*©2016 Netflix is a registered trademark of Netflix, Inc.

RA Force dashboard

Intuitive Dashboard lets you view total DNS and IP shuns, manage list subscriptions, monitor events customize preferences, and more.

A safe landing page



Users are redirected from malicious internet destinations to a safe landing page. Your administrator can see which workstation is redirected, providing insight to potential high-risk user behavior.

RiskAnalytics™
/ THE ART OF SECURITY™

SecureDNS℠

/ DOMAIN DEFENSE

Cyber kill chain*

1 Reconnaissance
Assessing and harvesting of victim email addresses and other PII

2 Weaponization
Combining exploit with remote backdoor access into deliverable payload

3 Delivery
Transferring of weapon to target via email, URL, USB, etc.
/ Many attacks rely on DNS for weapon delivery. SecureDNS protects users from known exploit kits, malware and phishing delivery sites.

4 Exploitation
Targeting a vulnerability to trigger code on victim's system

5 Installation
Using access on network to install malware

6 Command & Control (C2)
Offering "hands on keyboard" remote control of victim's system
/ Malware will try to establish a control channel upon installation, giving hackers control of infected systems. SecureDNS disrupts malware C&C communication, making it far less harmful to the victim's network. This behavior is then easily detected and tracked by RiskAnalytics.

7 Exfiltration
Collecting, encrypting and extracting of victim's information

*Based on Lockheed Martin's "Cyber Kill Chain".

Broad protection from many threats

SecureDNS offers a low-cost, high-value solution to drastically minimize your exposure and mitigate DNS tunneling attacks, malware infection, and a variety of other DNS-based risks, including:

- **/ Malware callback events**
  By blocking malware from communicating with command and control, SecureDNS prevents attacks from advancing to the next stage.
- **/ TypoSquatters**
  In the event user mis-type a website's URL. SecureDNS blocks typosquatters from malvertising, phishing scams and drive-by malware downloaders
- **/ FastFlux**
  Through a dynamic, intelligence-driven feed of malicious domains and their associated IPs, SecureDNS provides defense to combat mechanized adversaries, including botnets that use FastFlux to rapidly rotate IPs and domain names.
- **/ Data exfiltration**
  SecureDNS kills advanced persistent threats that use a malicious domain in the exfiltration of corporate or employee data.

Accurate, flexible geo-blocking

- **/ Block specific TLDs**
  With SecureDNS, you can easily block top-level domains (TLDs) like .cn (China) or .ru (Russia). Blocking TLDs provides more accurate geo-blocking with fewer false positives than attempting to block by country-based IPs.
- **/ TLD control**
  You can control sessions with foreign domains, but still allow connections to any distributed business infrastructure hosted there.

Contact us at
support@RiskAnalytics.com / 1.855.639.4427
for information.

RiskAnalytics™
/ THE ART OF SECURITY™