DomainTools

Whitepaper

Zero Trust and DomainTools

Introduction

Increasingly, security and risk management personnel are implementing various initiatives centered on the concept of Zero Trust, whether because of regulatory guidelines, CISO guidance, or both. Internet intelligence from DomainTools can play an important role in such initiatives, because connections from the protected environment to unknown (and therefore untrusted) infrastructure represent a genuine and pervasive risk. DomainTools offers a variety of tools and data that help security teams:

- Identify and/or block connections to newly-created domains
- Build context around adversary-controlled infrastructure
- Identify clusters of malicious activity based infrastructure patterns
- Monitor emerging attack campaigns as the adversary develops them

Rather than implicitly trusting domains unless or until there is a reason to block them, it is becoming increasingly popular to automatically block all domains younger than a certain threshold. This is effective because many web proxies, SMTP proxies, and other controls have no way to categorize domains when they are first registered; such controls often rely on reputation scoring or analysis of served content. When a domain is initially registered, some time may pass before it is provisioned and thus able to be assessed by traffic or application analysis tools.

DomainTools data, as enrichment in SIEM, SOAR, or TIP, or proprietary tools, can enable newly-created domain alerting or blocking. Similarly, DomainTools Risk Scores provide a means of identifying domains that may not be on a typical observation-based denylist as yet, but which may represent a threat and thus should not be trusted. DomainTools is already trusted by US Federal/Government agencies, as well as many private sector enterprises, to help meet Zero Trust architecture needs around threat intelligence.

The foundational objective of Zero Trust is to prevent trouble before it occurs. However, full prevention of incursions or dangerous connections is not achievable in real-world environments. When trusted assets have connected to malicious infrastructure, DomainTools enrichment and investigative tools can be applied by IR or forensic teams. In such scenarios, DomainTools data may provide insights that cause the IR team to “retroactively revoke trust” of a given domain—that is, a domain that was not flagged or blocked previously but which, thanks to DomainTools data, is now seen to be dangerous.

Several principles of Zero Trust are directly addressed by DomainTools products and data in the following specific ways:

Do not trust unknown resources

- Use Iris Enrich, or Farsight Newly Observed Domains or Newly Observed Hostnames to flag newly observed domains.
- Use Domain Risk Score to flag high-risk domains.
- Use Iris Detect or Newly Observed Domains or Newly Observed Hostnames to identify domains that spoof particular keywords such as the organization's name, or its close associates or vendors.
- In any of the above scenarios, domains flagged by DomainTools can then be incorporated into custom denylists or other security controls. SOAR or proprietary scripting can automate these processes.

Monitor the environment in real time

- Use machine-scale Iris Enrich and/or Farsight DNSDB enrichment to identify young and/or high-risk domains (or domains meeting more customized criteria such as hosting geography, registrar, ASN, etc)

Apply Least Privilege principles to user access of Internet-based resources

- For security controls with a spectrum of dispositions available, DomainTools enrichment and/or risk scores may be referenced to calibrate the level of control.
  - For example, in an email filter, deny any connections from domains younger than a given value, or with risk scores above a given threshold; allow connections but disable attachments and links for domains with ages or risk scores within a designated band of age/score values, etc.
  - In a web filter, deny connections to domains younger than a given value or with high risk scores; place an interstitial warning for domains in a slightly lower risk/age band, etc.

Zero Trust is a far-reaching concept that pervades almost every area within the security practice, as well as information and operational technology in general. But for those components of Zero Trust that involve connections between the trusted environment and unverified Internet infrastructure, DomainTools Internet intelligence, delivered in a variety of products and integrations, can make a significant contribution to the fulfillment of the Zero Trust objective.

About DomainTools

DomainTools is the global leader for Internet intelligence and the first place security practitioners go when they need to know. The world's most advanced security teams use our solutions to identify external risks, investigate threats, and proactively protect their organizations in a constantly evolving threat landscape.

DomainTools