RISKIQ®

RiskIQ PassiveTotal®

Investigate and Uncover Digital Threats

Investigate and Respond Quickly to Digital Threats and Attacks

RiskIQ unifies internet data sets into a single RiskIQ PassiveTotal® threat analysis platform, empowering security teams to accelerate investigations and eliminate threats. The platform maps and exposes threat infrastructure and provides unparalleled context and intelligence to events and incidents.

Predict Threats Forming on the Internet

- Quickly search using an Indicator of Compromise (IOC) across multiple data sets to connect disparate elements of threat infrastructure
- Stay one step ahead of attackers by setting monitors on suspicious infrastructure to be alerted to changes that could indicate weaponization or impending attack
- Create PassiveTotal projects that organize related threat infrastructure so you can collaborate on analysis and receive alerts on changes to any of that project's components

Investigate Infrastructure Used in Attacks

- Automatically aggregate and correlate data about a security event that would otherwise take an analyst days or hours of manual analysis
- Unify data from passive DNS, WHOIS, SSL certificates, host pairs, web trackers, email addresses, and RiskIQ virtual user web crawling
- Quickly pivot between data sets in a single platform, allowing for connections to be made between disparate or seemingly unrelated information

Search across all PassiveTotal Data Sets with one click:

- Passive DNS
- WHOIS
- SSL Certificates
- Web and Social Trackers
- Host Pairs
- Cookies
- DNS Records & Types

Key Benefits

- Reduce the time to response during security incidents
- Quickly triage alerts to prioritize threats
- Uncover unknown threats to the business
- Monitor the internet for malicious activity targeting you
- Collaborate among other analysts in your organization and across the RiskIQ Community

Advantages

Unrivaled Intelligence

Tap into the deepest, broadest data sets available for threat investigation and harness the power of RiskIQ's award-winning research, data science, and automation.

Force Multiplier

Give junior analysts access to a platform that allows them to operate more effectively by automatically correlating data across multiple data sets.

Work Smarter

Enable collaboration between security analysts and incident response teams to enrich investigations and reduce time to response with TeamStream® context and project capabilities.

Context Matters

Enrich investigations and quickly pivot between multiple data sets in a single platform, allowing connections to be made between disparate information and data sources.

Defend Your Organization From Attackers

- Uncover hidden facets of your attacker's infrastructure and enrich investigations so security teams understand adversaries and their techniques
- Proactively block malicious infrastructure that is related to known malicious organizations and actors before it's used against your organization
- Set monitors on branded terms to be alerted when elements are found that may be targeting your brand for hijacking, infringement, or phishing

Threat Infrastructure Analysis

Threat Infrastructure Analysis is a research process that brings context to incidents and attack campaigns by identifying and linking related entities through multiple data sets, including active and passive DNS, WHOIS, SSL certificates and other page content attributes. RiskIQ consolidates all the necessary data into a single platform, so analysts can spend their time focusing on threats, not data collection and processing.

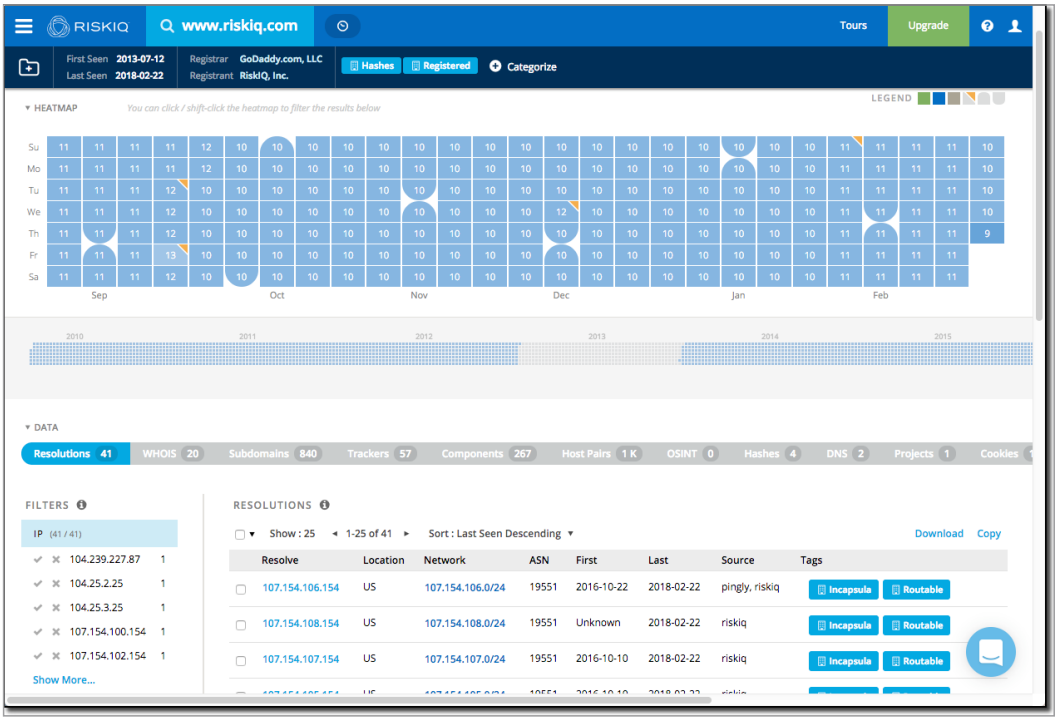

Fig 1: PassiveTotal search for www.riskiq.com, showing historical resolution of the domain and pivotable data set tabs.

Passive DNS	How to use it:
Passive DNS (PDNS) data provides analysts insight into how a particular domain name or IP address changes over time and enables them to identify other related domains and IP addresses. When researching a suspicious or malicious event, PDNS data can provide a timeline and context to an attack and surface additional malicious domains and IPs.	• Indicator of Compromise (IOC) correlation • Historical resolution lookups • Time-based analysis

WHOIS	How to use it:
Using current and historical WHOIS registration information, analysts can unmask an attacker's identity and infrastructure and link suspicious domains to others registered using similar information.	• Identify additional domains registered using similar information • Determine the maliciousness of a given domain or IP address based on ownership records • SIEM event enrichment

Contextual Analytics

There are other elements and web assets that are used in rendering websites that direct investigators to those responsible for an attack. Only PassiveTotal aggregates and correlates this data from the millions of pages that RiskIQ crawls every day, providing unmatched intelligence and insight.

This information includes:

- **SSL certificates** and their history can indicate discrepancies in timelines and similarities to other SSL certificates and internet infrastructure
- **Components** that are used to build websites, such as the server operating system, frameworks, CMS, and more
- **Host pairs** allow analysts to see dependencies between various components of websites, including referenced images, content sources, and client or server-side code to understand the relationships between hosts
- **Web trackers** for social and site analytics are often reused across multiple sites and can correlate back to a single entity
- **Projects** available in the broader security community and media can surface additional information about particular threats and link attacks to known groups and actors
- **Cookies** that are left on computers that visit a website are recorded when a RiskIQ virtual user visits a URL. RiskIQ correlates cookie source name and data with infrastructure hosting the cookies to allow analysts to pivot and find other sites with related cookies.
- **DNS Records** for domains that include mail exchange, TXT records, start of authority, and nameserver records.

PassiveTotal Monitors	How to use it:
Internet infrastructure changes all the time. Some changes are business as usual, but others can indicate a compromise or impending attack. Using PassiveTotal monitors, analysts can be notified when monitored infrastructure changes so it can be proactively investigated. This allows potential threats to be blocked before a malicious campaign is executed.	• Get real-time alerts based on our internet data sets including passive DNS, WHOIS, SSL certificates and OSINT • Receive notifications when new domains pop up in the wild • Understand related infrastructure by setting monitors on keywords and PassiveTotal tags

PassiveTotal Projects	How to use it:
Working together with other teams is difficult when investigations and cases change hands for further investigation or enforcement. Using PassiveTotal projects, teams can quickly consolidate and hand-off the items discovered in an investigation. Monitors can also be set on projects, proactively notifying teams that they may need to re-examine a threat.	• Group threat infrastructure into projects • Share projects between teams in your organization • Real-time notifications can be set to alert on changes

RISKIQ®

RiskIQ, Inc.
22 Battery Street, 10th Floor
San Francisco, CA. 94111

sales@riskiq.net
1 888.415.4447

Learn more at riskiq.com