DATASHEET

RESEARCH AND INVESTIGATE THREATS

LEAVE YOUR FOE WITH NOWHERE TO HIDE

RISKIQ®

INVESTIGATE AND RESPOND QUICKLY TO NEW SECURITY THREATS AND ATTACKS

PassiveTotal provides access to the most comprehensive, internet-wide data sets available to protect organizations from modern cybersecurity threats. The platform maps and exposes threat infrastructure and provides unparalleled external context and intelligence to internal events and incidents.

PREDICT THREATS FORMING ON THE INTERNET

- Leverage multiple data sets and intelligent analytics 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 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, email, SSL certificates, host pairs, web trackers, WHOIS, and RiskIQ comprehensive web crawling
- Quickly pivot between data sets in a single platform, allowing for connections to be made between disparate or seemingly unrelated information

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 elements that may be targeting your brand for hijacking, infringement, or phishing

PASSIVETOTAL DATA SETS

- Passive DNS
- WHOIS
- SSL Certificates
- Web and Social Trackers
- Host Pairs

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

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

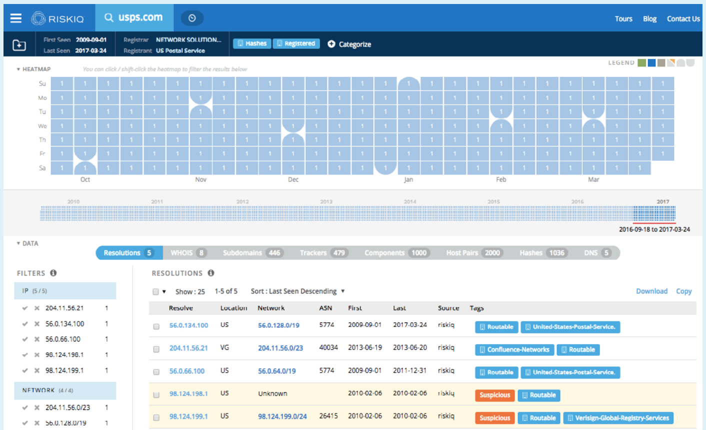
Enable collaboration between security analysts and incident response teams to enrich investigations and reduce time to response with TeamStream and project capabilities

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

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. PassiveTotal collects all the necessary data into a single platform, so analysts can spend their time focusing on threats, not data collection and processing.



First Seen 2009-09-01
Last Seen 2017-03-24
Registrar NETWORK SOLUTION...
Registrant US Postal Service

FILTERS

IP (5 / 5)

204.11.56.21	1
56.0.134.100	1
56.0.66.100	1
98.124.198.1	1
98.124.199.1	1

NETWORK (4 / 4)

204.11.56.0/23	1
56.0.128.0/19	1

RESOLUTIONS

Show : 25 1-5 of 5 Sort : Last Seen Descending

Resolve	Location	Network	ASN	First	Last	Source	Tags
56.0.134.100	US	56.0.128.0/19	5774	2009-09-01	2017-03-24	riskiq	Routable United-States-Postal-Service.
204.11.56.21	VG	204.11.56.0/23	40034	2013-06-19	2013-06-20	riskiq	Confluence-Networks Routable
56.0.66.100	US	56.0.64.0/19	5774	2009-09-01	2011-12-31	riskiq	Routable United-States-Postal-Service.
98.124.198.1	US	Unknown		2010-02-06	2010-02-06	riskiq	Suspicious Routable
98.124.199.1	US	98.124.199.0/24	26415	2010-02-06	2010-02-06	riskiq	Suspicious Routable Verisign-Global-Registry-Services

PASSIVE DNS

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.

How to use it

- Indicator of Compromise (IOC) correlation
- Historical resolution lookups
- Time-based analysis

WHOIS

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.

How to use it:

- Identify additional domains registered using similar information
- Determine the maliciousness of a given domain or IP address based on ownership records
- SIEM event enrichment

PASSIVETOTAL MONITORS

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.

How to use them:

- Get real-time alerts when a domain or IP address of interest is changed
- Receive notifications when new domains pop up in the wild
- Understand related infrastructure by setting monitors on keywords and PassiveTotal tags

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 billions 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
- **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
- **Open source intelligence** (**OSINT**) available in the broader security community and media can surface additional information about particular threats and link attacks to known groups and actors

PASSIVETOTAL PROJECTS

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.

How to use them:

- Group threat infrastructure into projects
- Share projects between teams in your organization
- Real-time notifications can be set to alert on changes