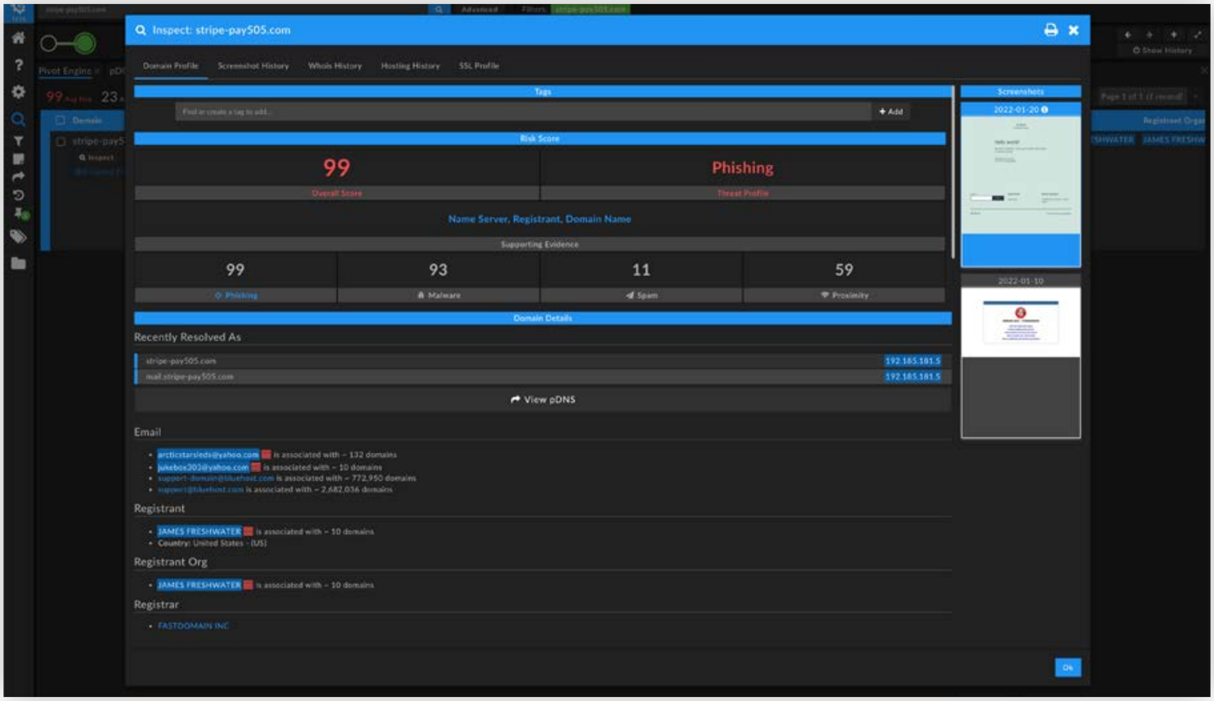
DOMAINTOOLS®

DomainTools Iris Investigate

Map Connected Infrastructure to Get Ahead of Threats

There are more than 300 million domain names, over 4 billion IP addresses and many more nameservers, hostnames and email addresses within the infrastructure of DNS. Criminals make use of all of these resources to attack their targets, moving often and hiding in plain sight behind Whois privacy and shared hosting environments. DomainTools Iris Investigate helps incident responders, threat hunters, and other SOC professionals understand the risk of Internet domain names and the infrastructure that supports them. Iris Investigate combines enterprise-grade domain intelligence and predictive risk scoring with industry leading passive DNS data to guide threat investigations and uncover connected infrastructure. Iris Investigate helps teams characterize and map evolving attack campaigns.



Inspect: stripe-pay505.com

Risk Score

99 Overall Score

Phishing Threat Profile

Name Server, Registrant, Domain Name

Supporting Evidence

99	93	11	59
Phishing	Malware	Spam	Proximity

Domain Details

Recently Resolved As

stripe-pay505.com	192.185.181.5
mail.stripe-pay505.com	192.185.181.5

View pDNS

Email

- arcticstarsleds@yahoo.com is associated with ~ 132 domains
- jukebox303@yahoo.com is associated with ~ 10 domains
- support-domain@bluehost.com is associated with ~ 772,950 domains
- support@bluehost.com is associated with ~ 2,682,036 domains

Registrant

- JAMES FRESHWATER is associated with ~ 10 domains
- Country: United States - (US)

Registrant Org

- JAMES FRESHWATER is associated with ~ 10 domains

Registrar

- FASTDOMAIN INC

Benefits

- **Better Data Gives You Better Answers**: Put the world's largest database of domain profile information and industry-leading Passive DNS data from Farsight Security to work for you and avoid the blind spots that come with inferior data sources.
- **Designed By Investigators, For Investigators**: DomainTools works with some of the best security analysts and threat hunters in the world. With features like Guided Pivots, you are able to quickly pinpoint the most valuable investigative path.
- **Changes the Economics of Adversary Analysis**: The expense of hiring external expertise or assigning internal resources to adversary analysis has always been prohibitive. DomainTools Iris Investigate changes the equation, enabling high-confidence adversary profiling and attribution at costs far below traditional means.
- **Provides Visibility Beyond the Firewall**: Simply identifying malicious domains and IP addresses doesn't protect organizations against the extended networks operated by threat actors. DomainTools Iris Investigate gives organizations the ability to create forensic maps of criminal activity to triage threat indicators, assess risk, and prevent future attacks.
- **APIs**: The Iris Investigate API offers similar outcomes and brings a critical subset of Iris Investigate capabilities to third-party products and custom integrations, enabling rapid in-context profiling of domain-based threats and effective pivots that help build comprehensive lists of malicious infrastructure.

"With DomainTools, we're able to identify malicious activities sooner and respond to them before business or operational risk occurs and prevent the impact connected with a security incident." — DomainTools Customer, IDC Study

DOMAINTOOLS®

Test the power of the world's Largest DNS Forensics Database Today.

WWW.DOMAINTOOLS.COM