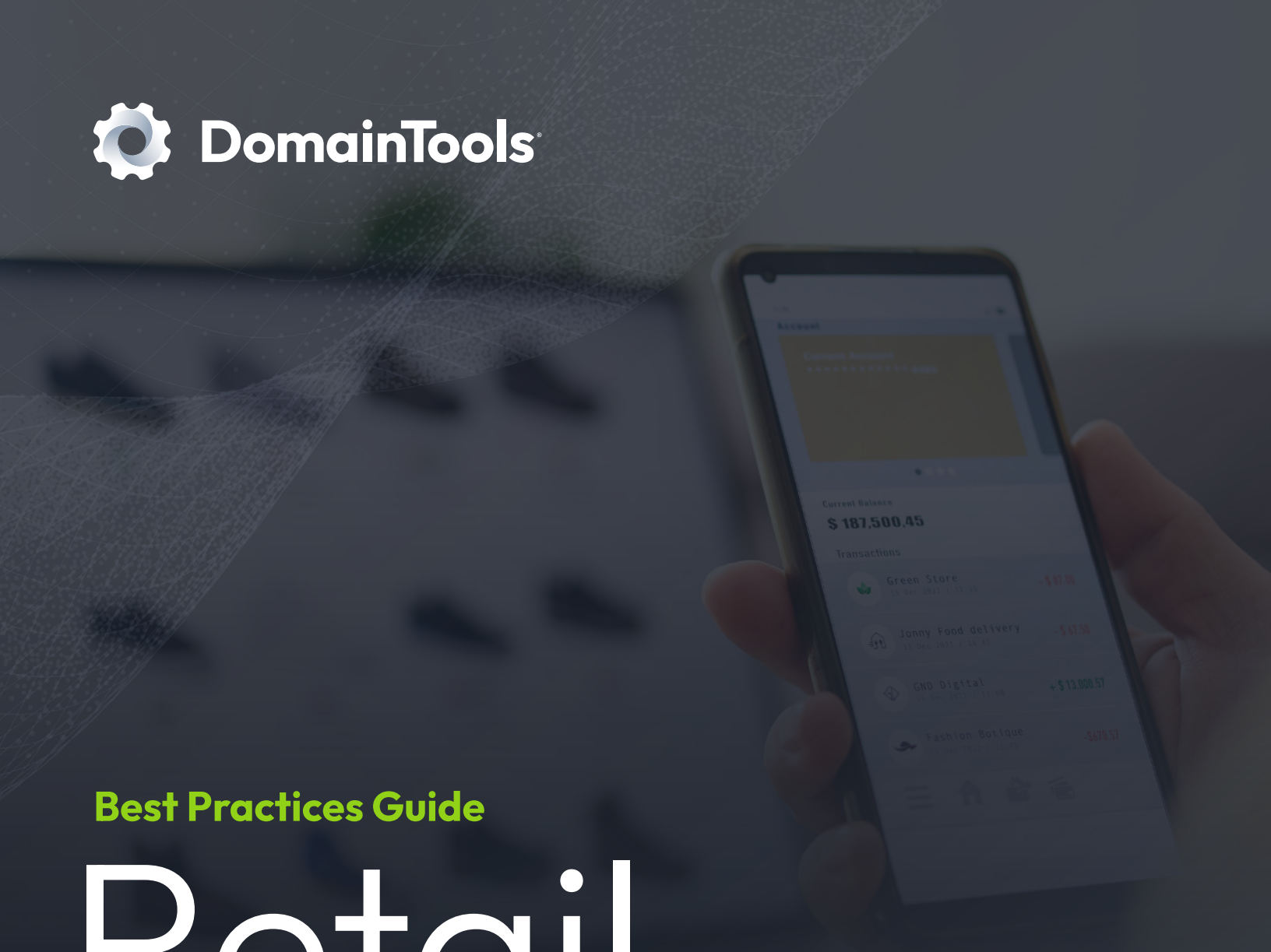
DomainTools



Best Practices Guide

Retail

domaintools.com

Introduction

Welcome to this Best Practices Guide from DomainTools. This reference offers insights into the cyber threats facing the retail sector, what the landscape looks like for defenders, and how security teams are making effective use of adversary infrastructure analysis to gain an edge.

The Guide consists of four sections:

- The current threat landscape
- Successes and limitations of common defensive strategies
- The value of DNS and DNS-adjacent data in adversary analysis, and why DomainTools is a leader in this space
- How security teams are solving important security problems with DomainTools

At the end, we offer links to various resources to help you learn more about DomainTools offerings.

The Retail Cyber Threat Landscape

It is a truism almost to the point of cliché that the threat landscape is evolving, and going into the mid-2020s, this is as true as ever. Certain trends, however, suggest that this evolution may be quickening relative to earlier years. In particular, the introduction and widespread adoption of large language models such as ChatGPT and its peers seem to be accelerating the pace of change, with these tools offering phishers more convincing lures, Business Email Compromise (BEC) actors the possibility of deepfake voice impersonations of trusted colleagues, and malware authors new ways to craft variants that can bypass many detection technologies. **The retail sector is in no way immune to these threats; they manifest year-round but seem to bloom during each year's busy holiday shopping season.** Magecart and its ilk continue to incur losses, and fraudulent sites, often hosted on look-alike domains, draw unsuspecting shoppers away from the companies they are imitating.

According to a 2023 report from Trustwave, the following threat types are among the most severe for retail:

- Email-Borne Malware
- Routine phishing and BEC
- Credential Access
- Consumer-Based Attacks
- Gift Card Fraud and Scams

These threats often rely on fraudulent domains that imitate the retail company names and brands, or that imitate other companies such as vendors, business process applications, or e-commerce platforms. Detecting, blocking, and reporting such domains can provide significant protection against these threats, often before the actor controlling the infrastructure has weaponized it. More broadly, no matter how sophisticated or unique the cyber threat, **something all of them have in common is that they rely on the use—or abuse—of Internet infrastructure that is observable, comparatively static, and often rich in contextual information** that defenders can, and do, use to considerable effect in aligning defenses with confirmed or suspected adversaries. This Guide will show you how.

Current State—What's Working and What's Not

Security technologies and practices have not stood still while the threats evolved—they have evolved right along with them. And security innovations have not always lagged threats, with seemingly daily advances that improve detection, defense, visibility, and remediation. Nevertheless, breaches and compromises roll on. A reasonable assessment of a security organization that is doing things "right" might be necessary but not sufficient: the steps today's defenders take are generally good and prudent ones, and in some cases, truly stellar work is being done and shared. Yet, the teams that have the strongest postures and best track records will be the first to admit that they are anything but invincible. So the goal is not perfection; it is to make reasonable, cost-effective advances that make measurable positive differences in outcomes.

Technology or approach	Gaps that remain
Reputation lists and observation-based threat intelligence feeds	Newly-registered domains are generally a blind spot to these technologies because reputation feeds are built on observed harm in the wild, or analysis of traffic already in the environment
Deep packet inspection, sandboxing, heuristics-based rules	Susceptible to novel techniques or malware
Forensic analysis of domains or IP addresses that touched the protected environment	Threat actors usually control more infrastructure than what is initially observed. If forensics do not account for this additional infrastructure, it may cause future harm.

Most large retailers deploy a good set of defenses, which typically include relatively late-model products in the realms of network defense, host defense, identity and access management, visibility and situational awareness tools, cyber threat intelligence, and orchestration and automation of some or all of these—and this is an incomplete list. But it's worth pointing out two truths about technology stacks that incorporate these tools:

1. Malicious activity is still proceeding and frequently succeeding
2. Almost every technology mentioned operates, at some level, within the framework of DNS

This second point is what we will explore next.

The Importance of Adversary Infrastructure Analysis

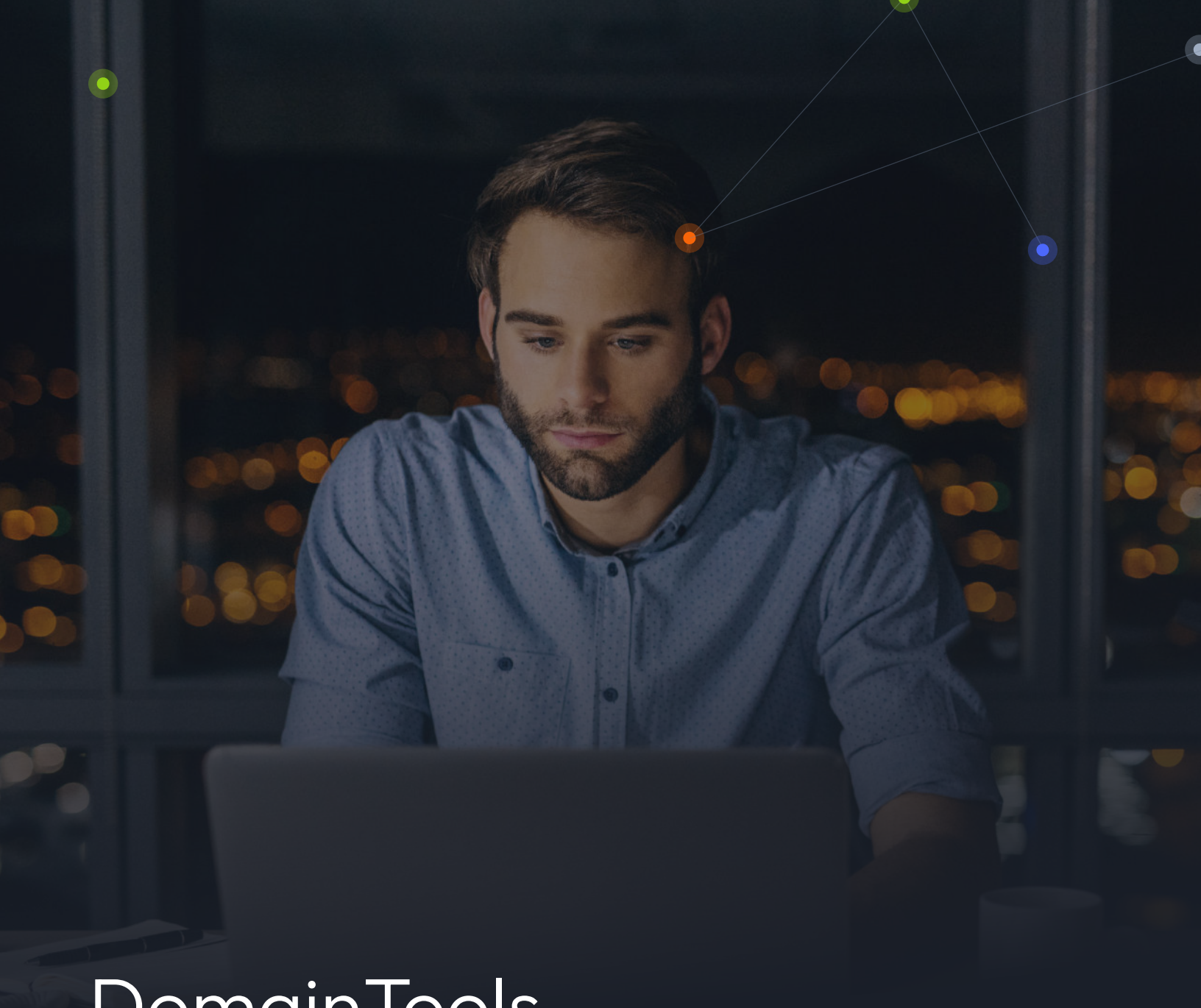
Because today's retail SOCs, fusion centers, intelligence teams, and any other entities entrusted with cyber defense are moving at such a rapid pace, with constrained staffing, it is fair to ask why resources should be expended on infrastructure analysis. After all, that time has an opportunity cost; each minute or hour spent on such analysis cannot be spent on other tasks.

The Importance of Adversary Infrastructure Analysis

While there is no individual "right" answer, our work with practitioners around the world has led us to certain well-tested axioms:

- **Everything that happens on the Internet uses domains and/or IP addresses.** Malware families come and go and network- or protocol-based attacks have their moments in the sun; but amid all of these cycles and evolutions, the fundamental infrastructure on which the vast majority of them rely remains relatively familiar: domains and IPs.
- **There are almost always clues available.** Staying all the way in the shadows of the Internet is challenging, time-consuming, and often works against the scale and speed that bad actors depend on to make crime pay.
- **You can tell a lot about a domain by the company it keeps.** Malicious domains tend not to be "lone wolves." Any malicious campaign designed to have a significant impact will almost universally rely on multiple objects (domains, IPs, certificates, etc).
- **Adversaries make mistakes.** If attackers want to ensure that they can't be identified or blocked, they have to avoid leaking identifying or connecting information. That is not particularly hard when the actor is running a single domain, but when they scale that to dozens, hundreds, or thousands, the odds of a leak become much greater.

Top-performing security teams around the world operate on these axioms daily.



DomainTools

DomainTools provides comprehensive Internet intelligence to security practitioners and advanced security teams. The solutions help teams identify external risks, investigate threats, and proactively protect organizations in a constantly evolving threat landscape. DomainTools constantly monitors the Internet and brings together the most comprehensive and trusted domain, website, and DNS data to deliver context and machine learning-driven risk analytics in near-real time, providing critical tools and services for the following use cases:

Phishing, BEC, and e-Commerce Fraud Prevention

Know if and when malicious domains and infrastructure are spoofing your assets before they can cause damage.

Threat Intelligence

Detect relevant indicators earlier in their lifecycle to identify and disrupt incipient attacks.

Forensics and Incident Response

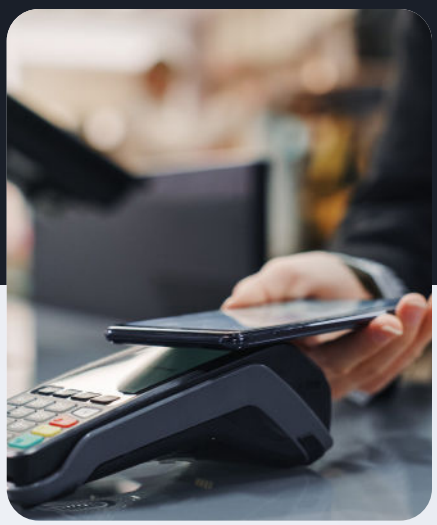
Respond to and triage potential incidents with confidence and speed.

Threat Hunting

Discover indicators of compromise (IOCs) and malicious infrastructure that may be targeting your network.

Enrichment

Enrich homegrown or third-party security applications with effective Internet intelligence.



The DomainTools **Iris Internet Intelligence Platform** is made up of three components. Iris Detect provides a near real-time internet infrastructure detection, monitoring, and enforcement platform and API, ideally suited to quickly finding domains spoofing brand and company names; Iris Enrich is a robust API that includes Whois, DNS, SSL certificate, and risk scoring elements to enrich indicators at scale; and Iris Investigate provides a platform and API that supplies and maps domain intelligence, risk scoring, and industry- leading passive DNS data.

Farsight Newly Observed Domains is a feed regularly used (sometimes in parallel with Iris Detect) to spot the emergence of domains spoofing a brand, company, or other keyword.

DomainTools also provides Threat Intelligence Feeds that can be integrated into threat intelligence platforms and other tools to provide predictive domain risk scoring, hotlists, newly discovered hostnames and domains, and more.

Farsight DNSDB is a comprehensive passive DNS near real-time and historical database of global internet infrastructure data, that can be accessed and queried by DomainTools customers and integrated into tools through an API to help reduce risk.

Common Use Cases and Where DomainTools Fits In

Each of the following is a summarized sequence giving an example of how security teams use certain DomainTools products in common workflows. The exact use case will have slight variations for every organization.

Detecting Infringement and Spoofing:

- ✓ Configure Iris Detect to monitor key brand and company names or trademarks
  - Consider also using Farsight Newly Observed Domains for an additional layer of detection
- ✓ Review matching domains; designate the most threatening for enforcement action
- ✓ Add middle-tier risk domains to Watchlist to monitor for future weaponization
- ✓ Export high-risk domain names to Iris Investigate to gain insights on the larger campaigns connected to the domains
- ✓ Working with detection engineering and security controls teams, build detection and blocking rules for the extended threat campaigns uncovered in Iris Investigate
- ✓ Share high-confidence threat infrastructure with trust groups such as RH-ISAC or law enforcement

Threat Hunting:

- Ingest domain indicators from trust group, threat actor report, or other source
- Run a query on the domains in **Iris Investigate**; pivot and expand to uncover additional connected infrastructure; save query for expanded set as an Iris Investigate hash (saved query)
- Retro-hunt for presence of any of the expanded indicator set in earlier logs or alerts
- Set SIEM or security control alerts for traffic involving any of the expanded indicator set
- Re-run Iris Investigate hash (a form of stored query) daily to pick up new indicators matching the established pattern
- Identify and investigate hits on any of the indicators; hand off to analyst or IR teams as appropriate

Incident Response:

- When an alert fires, with a high enough severity that the team decides to investigate:
- Identify any external domains or IP addresses associated with the alert
- Search on the domain(s) or IP(s) in Iris Investigate; pivot and expand to uncover additional indicators; save query for expanded set as an Iris Investigate hash. Some teams will also pivot in DNSDB for additional connections
- Retro-hunt for presence of any of the extended indicator set in earlier logs or alerts
- Any traffic flows to any of the extended indicator set are now immediately suspicious
- The full scope of traffic to any of the extended indicator set may be considered part of the incident
- Set SIEM or security control alerts for traffic involving any of the extended indicator set

Security Analysis:

- Ingest IOCs from trust group, threat actor report, or other source
- Search on IOCs in Iris Investigate; pivot and expand to uncover additional indicators; save query for expanded set as an Iris Investigate hash
- Analyze extended infrastructure (in other tools such as Censys, Shodan, etc) for clues about additional TTPs that may be telegraphed by it
- Re-run Iris Investigate hash daily to pick up new indicators matching the established pattern; detect and investigate hits on any of the indicators
- Use Iris Detect to monitor names and brands of vendors for potential imitations, e.g. Microsoft365, Salesforce, etc;
- When spoof domains are discovered, work with Detection Engineering to set up monitoring of any outbound connections to the spoof domains (Or, set up blocking rules ahead of time for the spoof domains)

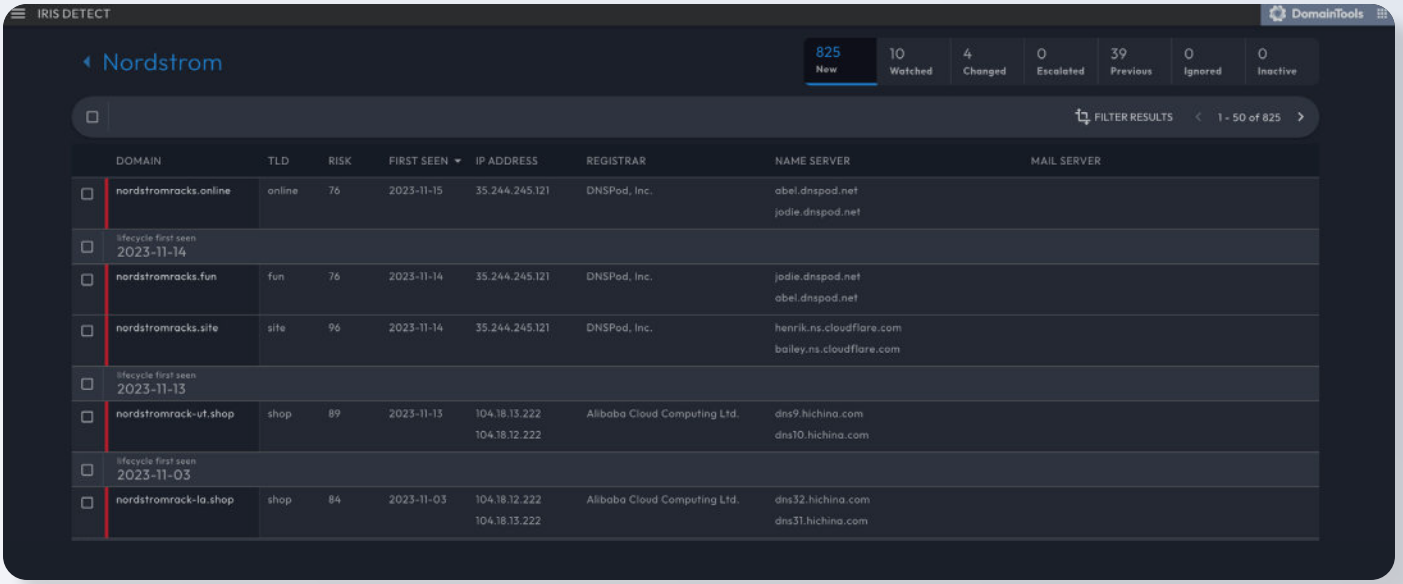
Additionally, many SOC personnel use the Iris Enrich API to decorate domains appearing in popular SIEM or SOAR platforms such as Splunk, Microsoft Sentinel, Cortex XSOAR, and others. Such enrichment allows analysts to quickly assess connections made to any domains identified as high-risk (according to the DomainTools Risk Score), newly created, or both. Armed with this information, analysts can then make informed decisions about which domains might merit further investigation.

Real-World Example: Retail Spoof Campaign

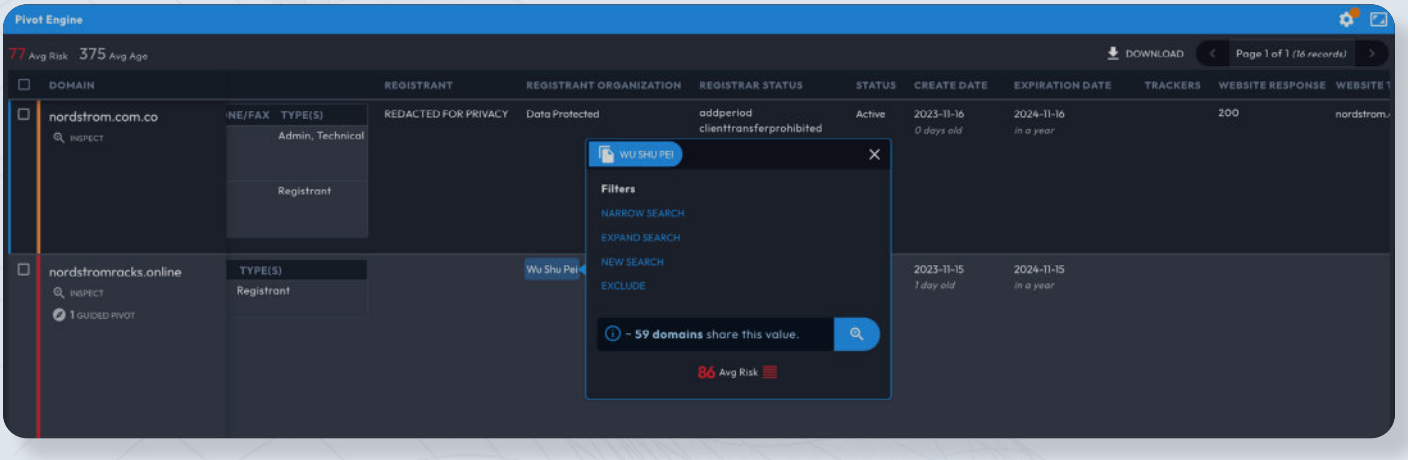
Registering spoofs of legitimate domains is often one of an adversary's first moves in creating a fraud or counterfeiting campaign, mounting a phishing or watering hole attack, or creating later-stage servers for command and control (C2) or data exfiltration; in any of these activities, the domain names are intended to deceive end-users or security personnel. A recent (as of this writing) cluster of activity involved a number of domains that spoofed notable retailers.

Real-World Example: Retail Spoof Campaign

Monitoring the string “nordstrom” for spoofs with **Iris Detect** in the days approaching a Black Friday/Cyber Monday weekend turned up the following domains (among many others):

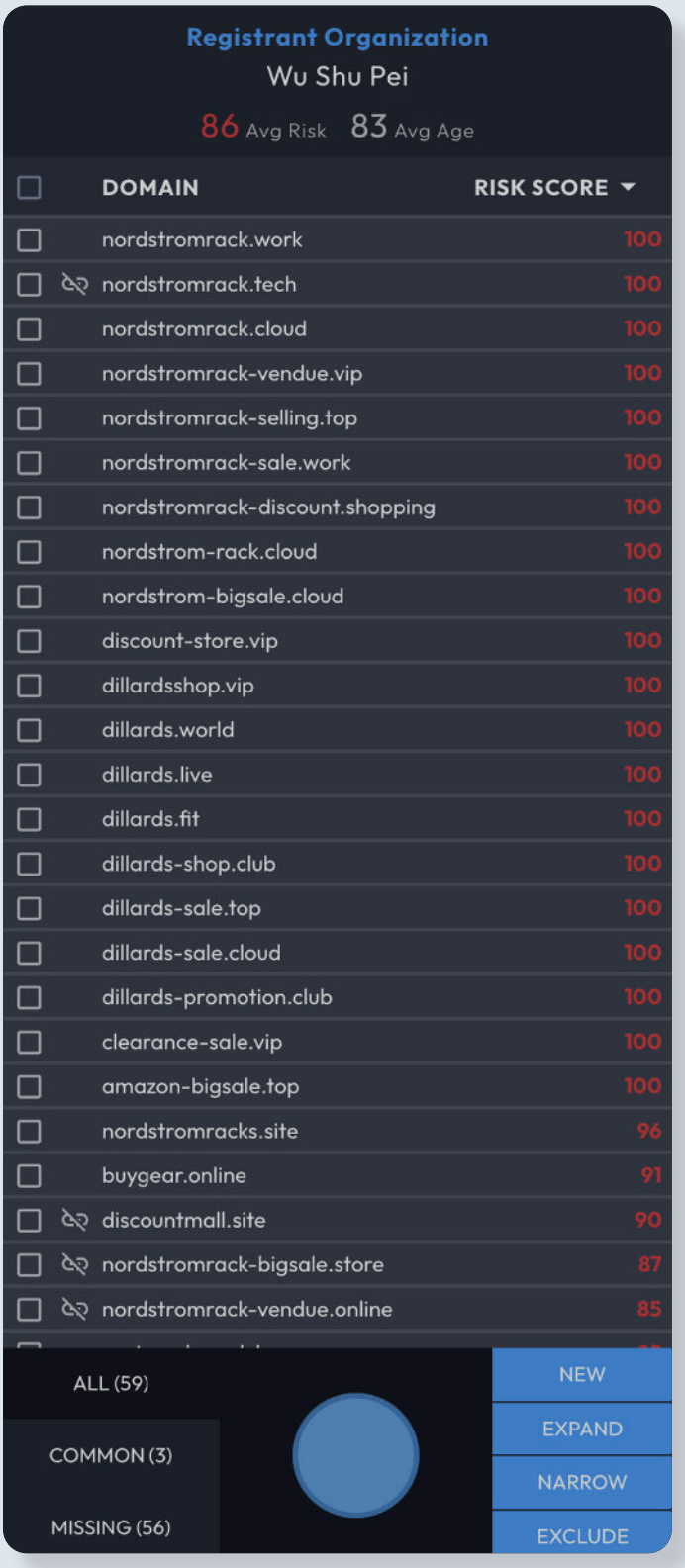


Since we know that domains are rarely “lone wolves,” we can carry out a further investigation to examine what other domains might be closely connected to these. Iris Investigate shows us that around 59 domains all shared the same Registrant Organization and that the average Risk Score of those domains was very high, at 86:



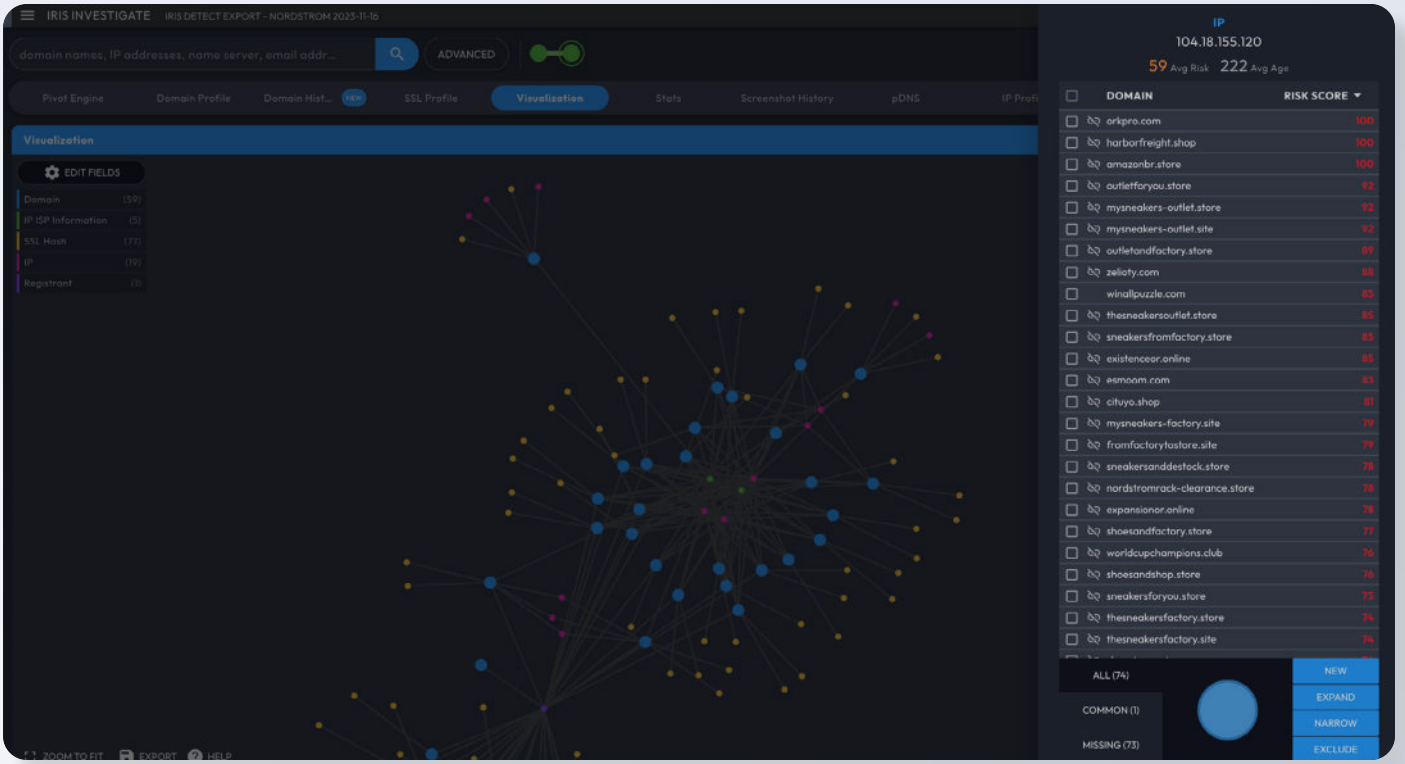
We can then examine the domain names that share this registrant organization string, and this shows very specific retail targeting.

Real-World Example: Retail Spoof Campaign



As we can see, not only has this actor registered many domains spoofing the Nordstrom retail chain, but also others such as Dillard's, Bed Bath and Beyond, and more (not all visible in the screenshot). We can see that the registrant demonstrates a clear pattern of activity, repeatedly registering new domains with this registrant organization name in the Whois records, so we tag these domains with "Retail Impersonation."

We can also use the Visualization panel in Iris Investigate to quickly see patterns or clustering within the set of domains. One of the IP addresses shown in the visualization has an additional set of some 73 additional domains, all showing the same pattern of impersonation of retail brands. We can bring these into our set, too. In just a few steps, we have uncovered a substantial malicious campaign targeting a variety of well-known retail brands.



We now have some options available to act on the information we have just developed. We can:

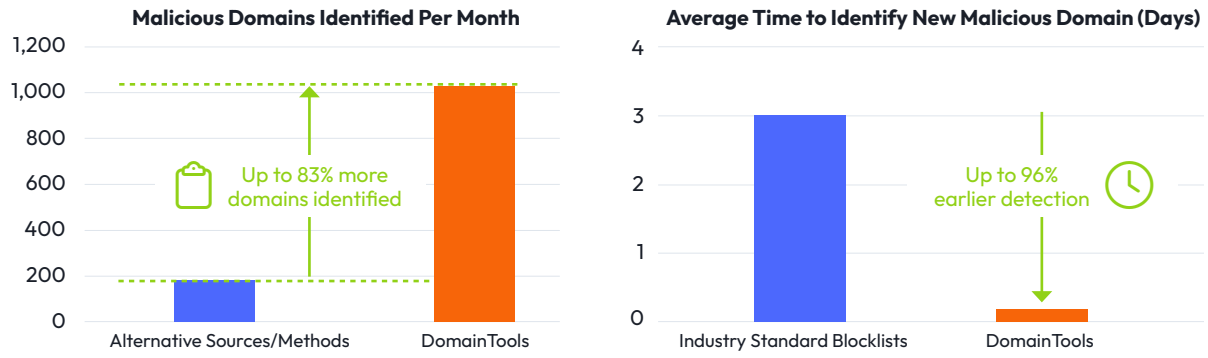
- Use the Iris **Investigate API** to create a recurring query for any new domain registrations matching this registrant and/or this IP address, since this actor appears to adhere to this pattern
- Share the domains and/or IP addresses with a trust group such as RH-ISAC and/or law enforcement
- Create alerts for any traffic from our protected environment to any of the domains
- Create blocking rules for the domains and/or the IP addresses associated with them

The domains tied to the original two spoofs of Nordstrom would not have been possible without connected-domain data, and the additional context provided by Domain Risk Scoring helps increase our confidence that the domains in question are malicious.

Organizational Benefits

Because of the benefits of techniques such as the one illustrated above, DomainTools customers consistently report significant organizational wins in the form of cost savings, improved detection rates, analytical efficacy, and more. According to Enterprise Strategy Group, DomainTools customers **identified as many as 83% more malicious domains** with DomainTools than with alternatives, and **detected malicious domains up to 96% earlier** than with industry-standard blocklist sources.

Figure 3. Blended Customer-reported Metrics for DomainTools versus Alternative Methods and Industry-standard Blocklists

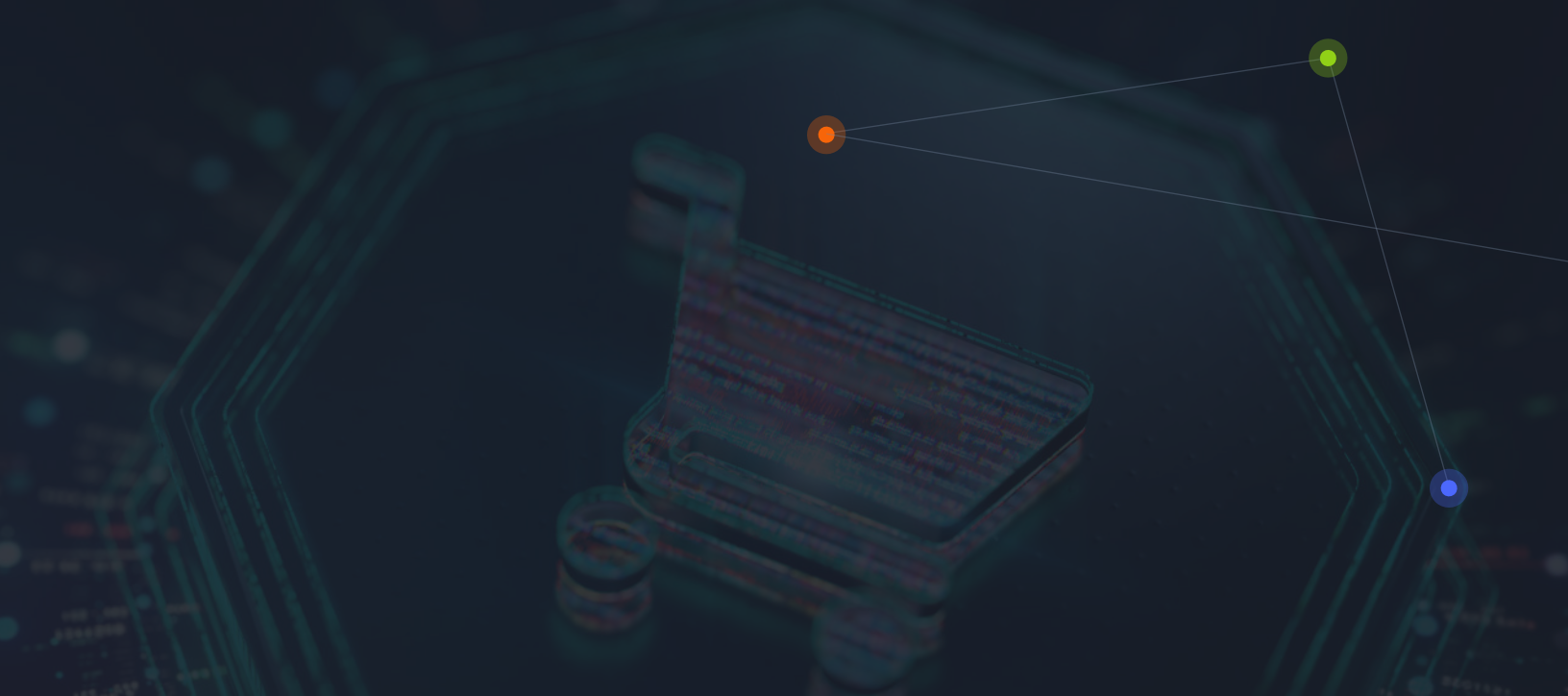


Source: Enterprise Strategy Group, a division of TechTarget, Inc.

DomainTools customers also report that their teams were more efficient, with some reporting savings of between 1.5 and 2 hours per day per employee.

"DomainTools gives us the earliest and most updated feed of newly created and updated domain and DNS infrastructure—so the second someone creates a domain, within five minutes, we know about it."

"Out of 1,000 domains determined to be malicious by Iris Detect, 68% did not appear in any other industry-standard blocklist. Of those that were detected elsewhere, Iris Detect and Investigate detected three days earlier on average, with most being detected within a three- hour period."



Conclusion and Additional Resources

The great majority of cyber threats to the retail sector use DNS and leave traces there which can be exploited for forensic and predictive purposes. DomainTools has amassed the world's largest datasets around Internet infrastructure, and for many years has leveraged the data to produce detection, enrichment, and investigative tools deeply informed by close work with practitioners in many of the world's most sophisticated security organizations. We believe that the data, tools, and methods described here have the potential to make a meaningful contribution to the protection of retail organizations everywhere.

Recommended Resources:

- Schedule a personalized demo of DomainTools products
- Formulating a Robust Pivoting Methodology
- Valuable Datasets to Analyze Network Infrastructure
- Using Infrastructure Analysis to Get Ahead of Attacks in Cyber Defense