



Best Practices Guide

# Technology

[domaintools.com](https://domaintools.com)







SIGNAL STRENGTH

135.09

# Introduction

Welcome to this Best Practices Guide from DomainTools. This reference offers insights into the cyber threats facing the tech 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 Technology 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 (LLMs) 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 tech sector is in no way immune to these threats and is often the first place threat actors look to carry out an attack.** Cyberdefense is often the last thought in a corporate culture designed to encourage fast, intense innovation and collaboration. As a result, technology organizations typically have a large attack surface to protect that often provides a path to other sectors.

These threats often rely on fraudulent domains that imitate the company's 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.



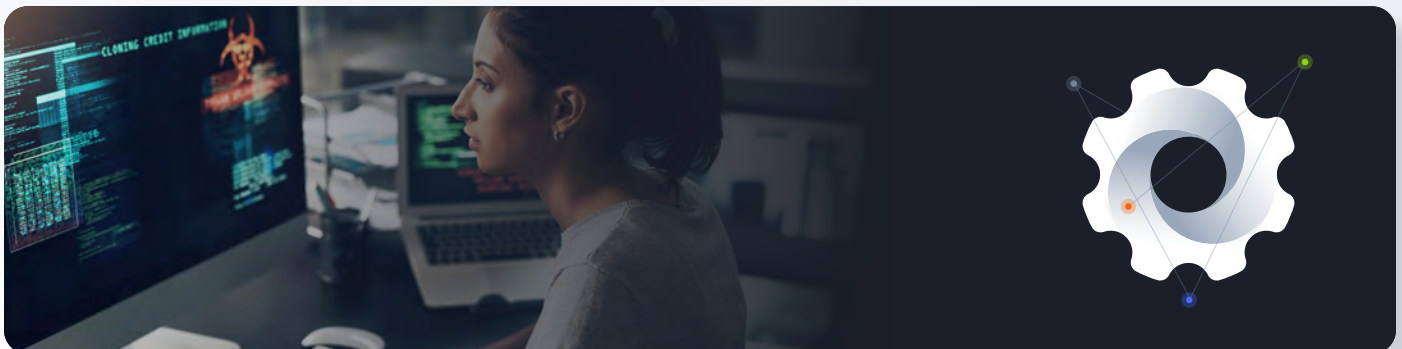
## Current State—What’s Working and What’s Not

🛡️ 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

Some tech organizations 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 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.



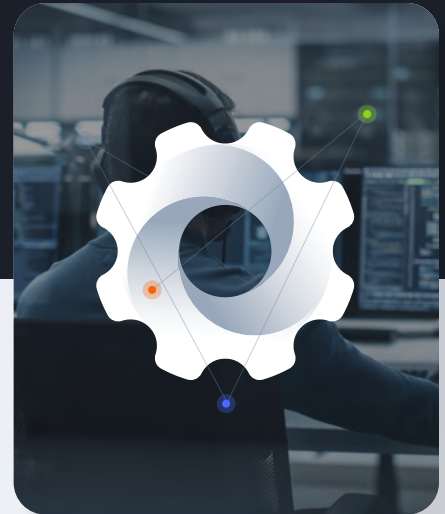
### Threat Hunting

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; [Iris Enrich](#) is a robust API that includes Whois, DNS, SSL certificate, and other metadata, as well as 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.

## Common Use Cases and Where DomainTools Fits In

### New Domain Discovery:

- 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 [National Council of ISACs](#) or law enforcement

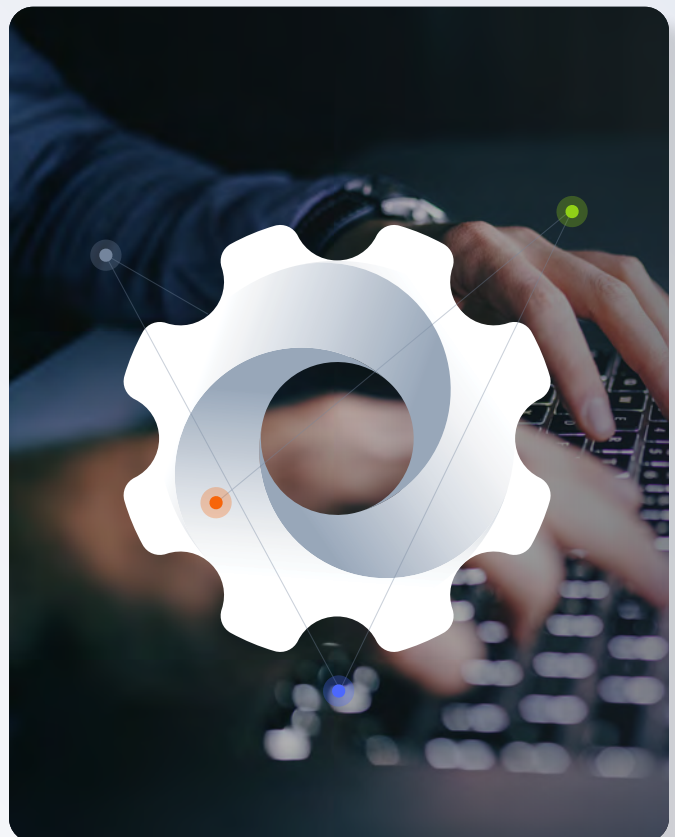
### Threat Hunting:

- 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



## Common Use Cases and Where DomainTools Fits In

### Predictive Scoring for Prioritized Response:

- Leverage our daily **Predictive Risk Scoring Feeds** and gain a risk-based view of newly registered or updated hosts, IPs and domains.
- Build accurate predictive domain risk scoring into your new and existing workflows
- Respond faster to domains before they are weaponized
- Use the DomainTools **Hosting IP Risk Feed and Hotlist** to enhance detection and blocking of risky infrastructure
- Observe the domain's proximity score to see how connected it is to other known-bad domains
- Observe the domain's threat profile to see how closely it resembles other known-bad domains
- Use the **Domain Risk Feed and Hotlist** for daily updates on high-risk domains that are associated with Passive DNS activity
- Use **Iris Detect** to monitor names and brands of vendors for potential imitations, e.g. Microsoft365, Salesforce, etc;
- When prioritized 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)

### API Throughput:

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. Iris Enrich API uses an independent service level to define access levels, query caps and rate limits. It does not pull from the same queries as the Iris Investigate UI and can therefore be used at much greater scale and throughput. 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.



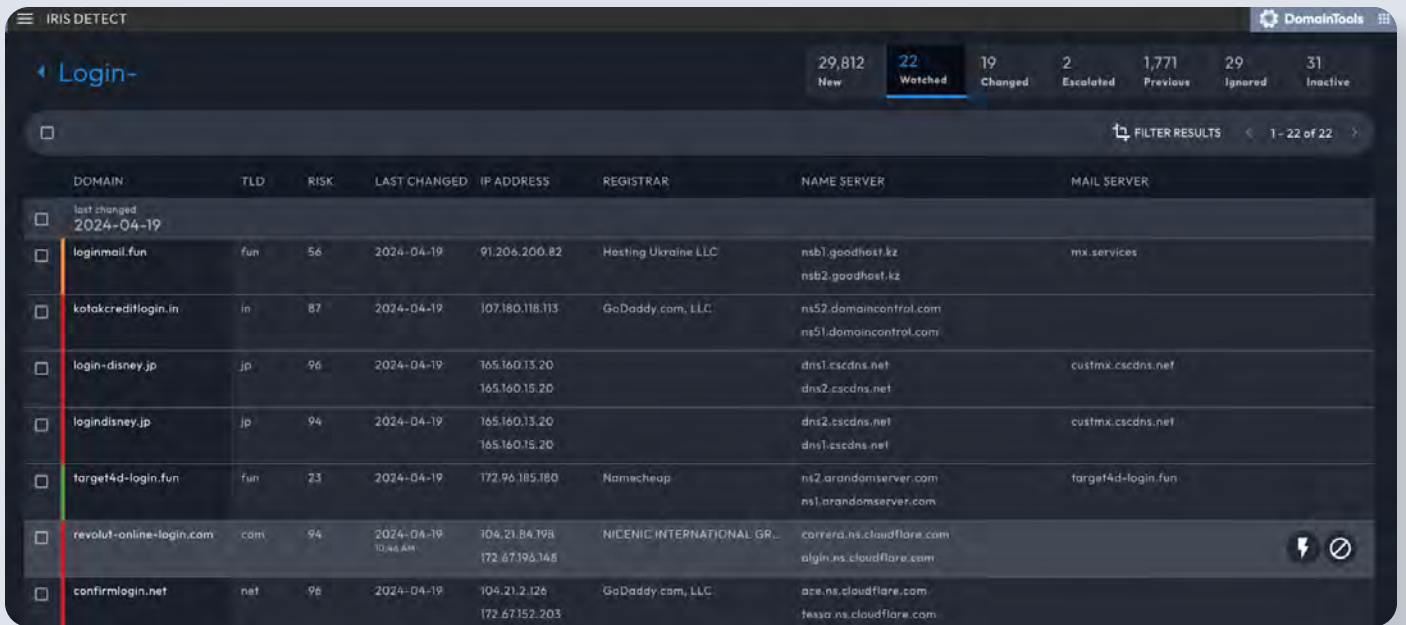
# Real-World Example: Login Spoof Campaign

Registering spoofs of legitimate domains is often one of an adversary's first moves in mounting a Business Email Compromise campaign, 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 tech organizations.

Tech organizations are not a monolith and one may deal with use cases and industries completely different from the other. One unifying aspect is a heavy presence of online infrastructure and vendors within one's supply chain. One of the most common DNS related tactics techniques and procedures (TTPs) carried out by the [Scattered Spider cybercriminal group](#) is to generate domains showing patterns such as `victimname-ss0[.]com`, `[victimname]-servicedesk[.]com`, and `victimname-okta[.]com` to identify usernames, passwords, and other personal data.

## Real-World Example: Login Spoof Campaign

Monitoring the string “login-” for spoofs with Iris Detect turned up the following domains (among many others):



DOMAIN	TLD	RISK	LAST CHANGED	IP ADDRESS	REGISTRAR	NAME SERVER	MAIL SERVER
last changed 2024-04-19							
loginmail.fun	fun	56	2024-04-19	91.206.200.82	Hosting Ukraine LLC	nsb1.goodhost.kz nsb2.goodhost.kz	mx.services
katakreditlogin.in	in	87	2024-04-19	107.180.118.113	GoDaddy.com, LLC	ns52.domaincontrol.com ns51.domaincontrol.com	
login-disney.jp	jp	96	2024-04-19	165.160.13.20 165.160.15.20		dns1.cscdns.net dns2.cscdns.net	custmx.cscdns.net
logindisney.jp	jp	94	2024-04-19	165.160.13.20 165.160.15.20		dns2.cscdns.net dns1.cscdns.net	custmx.cscdns.net
target4d-login.fun	fun	23	2024-04-19	172.96.185.180	Namecheap	ns2.arandomserver.com ns1.arandomserver.com	target4d-login.fun
revolut-online-login.com	com	94	2024-04-19 10:44 AM	104.21.84.198 172.67.196.148	NICNIC INTERNATIONAL GR...	carrera.ns.cloudflare.com algin.ns.cloudflare.com	
confirmlogin.net	net	98	2024-04-19	104.21.2.126 172.67.152.203	GoDaddy.com, LLC	ace.ns.cloudflare.com tessa.ns.cloudflare.com	

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. We export these domains to **Iris Investigate** which shows us more data surrounding each domain of interest.

## Real-World Example: Login Spoof Campaign

The screenshot shows the IRIS Investigate Pivot Engine interface. The search criteria are 'domain names, IP addresses, name server, email address'. The results table is as follows:

DOMAIN	TAGS	FIRST SEEN	RISK SCORE	EMAIL	EMAIL DOMAIN	CONTACT INFORMATION
confirmlogin.net	1 GUIDED PIVOT	2024-04-19 9:51 AM 7 hours ago	96	select contact domain holder link at https://www.godaddy.com/whois/result... dns@cloudflare.com select contact domain holder link at https://www.godaddy.com/whois/result... select contact domain holder link at https://www.godaddy.com/whois/result... abuse@godaddy.com	cloudflare.com godaddy.com	NAME Registration Private
confirmlogin.online		2024-04-19 5:44 AM 12 hours ago	92	please query the rdds service of the registrar of record identified in this outp... Please query the RDDS service of the Registrar of Record Identified in this o... dns@cloudflare.com please query the rdds service of the registrar of record identified in this outp... please query the rdds service of the registrar of record identified in this outp... abuse@namesilo.com	namesilo.com cloudflare.com	NAME ORGA Privacy
cumbartanduk-login.com		2024-04-19 6:51 AM 11 hours ago	100	dns@cloudflare.com abuse@nicenic.net	cloudflare.com nicenic.net	

Many of these domains have been created just hours before this investigation and our Domain Risk Score has already classified them as high-risk. One domain, created just 11 hours ago, has already been observed to be used behind a phishing campaign; giving it a risk score of 100. A tech organization can be overwhelmed by seeing new domains spoofing common login strings produced every other hour. Full visibility to address these domains all at once and discover newly created domains right away is especially important in a fast-paced tech organization with a wide attack surface. Luckily, some information has already been left behind by the first domain created 7 hours ago.

The screenshot shows the IRIS Investigate Pivot Engine interface with a pivot search on the website title 'Connect Wallet' for the domain 'confirmlogin.net'. The results table is as follows:

DOMAIN	TRACKERS	WEBSITE RESPONSE	WEBSITE TITLE	SERVER TYPE	REDIRECT	REDIRECT DOMAIN	MX INFORMATION
confirmlogin.net	CC US US	200	Connect Wallet	cloudflare			
confirmlogin.online	CC US US						

A modal window titled 'CONNECT WALLET' is open, showing search filters and results:

- Filters: NARROW SEARCH, EXPAND SEARCH, NEW SEARCH, EXCLUDE
- Results: - 46 domains share this value. (80 Avg Risk)

By pivoting on website title, we can examine the domain names that share this string, and this shows 46 domains with an average risk score of 80, centered on a specific target of personally identifiable information (PII).

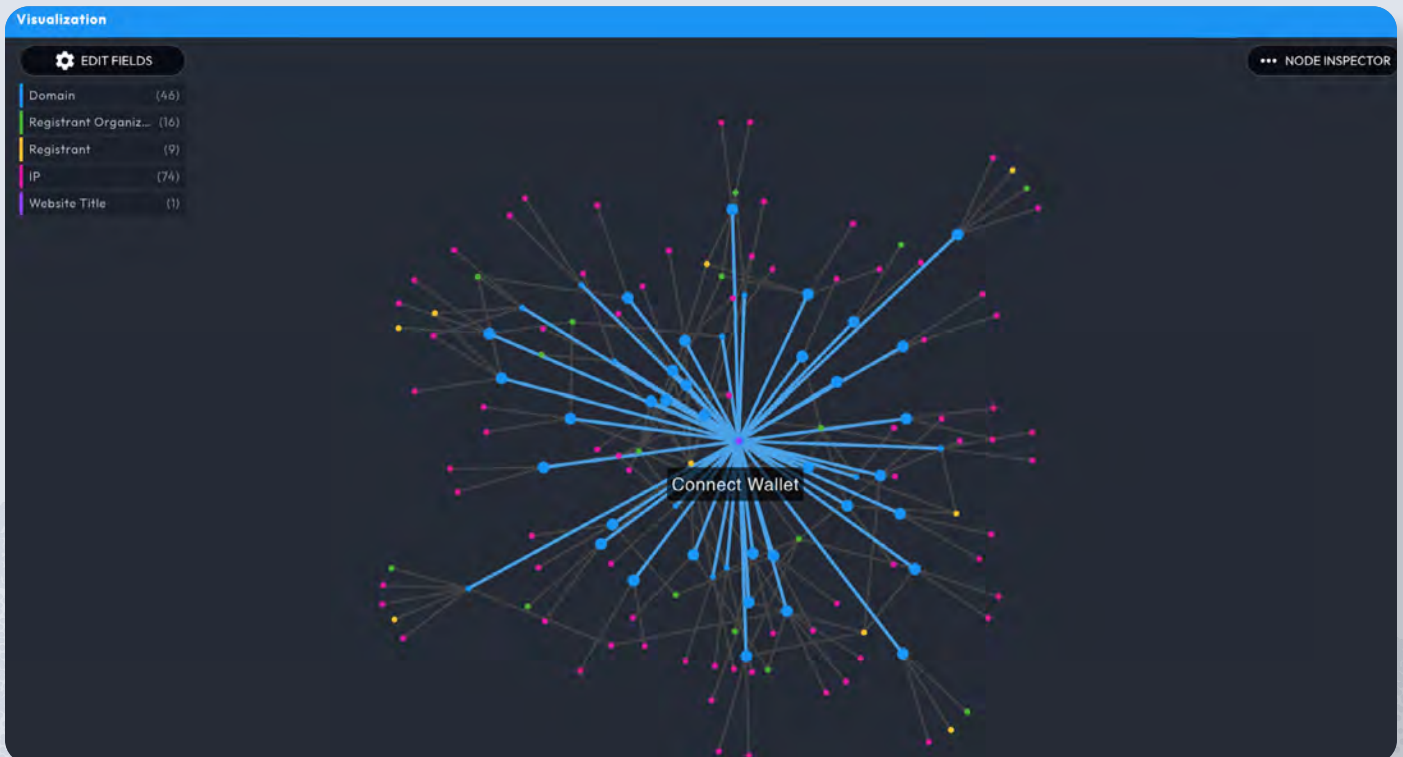
## Real-World Example: Login Spoof Campaign

The screenshot displays the Iris Investigate interface. At the top, it shows "Website Title: Connect Wallet" and "Avg Risk: 80 Avg Age: 205". Below this is a table of domains with their respective risk scores. A modal window is open for tagging, showing "46 domains selected" and a "TAG" button.

DOMAIN	RISK SCORE
assetrectification.dev	100
authwallet.org	100
claim-starknet.network	100
confirmauth.com	100
confirmauth.net	100
connectwallet1.com	100
correctdatabase.online	100
greenycoin.xyz	100
launcher-starknet.network	100
symbcoin-auth.com	100
token-entangle.com	100
vavithers.io	100
x030f5f0abba08.com	100
zeiron.org	100
authlogin.net	98
loginauth.org	97
trushtsync.com	97
confirmlogin.net	96
loginconnect.net	96
authconnect.net	95
connectauth.net	95
erc404-pandora.com	95
auth.com	93
pactconnect.top	91
funds.online	90

As we can see, not only has this actor registered many domains with suspicious names like “confirmlogin” “authwallet” and “loginconnect” (not all visible in the screenshot). We can see that the registrant demonstrates a clear pattern of activity, repeatedly registering new domains with the website title “Connect Wallet” name in the Whois records, so we tag these domains with “Login Suspicious.”

We can also use the Visualization panel in Iris Investigate to quickly see patterns or clustering within the set of domains. In just a few steps, we have uncovered a substantial malicious campaign that could be used to target any tech organization, its employees, or its clients.





## Real-World Example: Login Spoof Campaign

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 an 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 spoofs of a website login 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.**





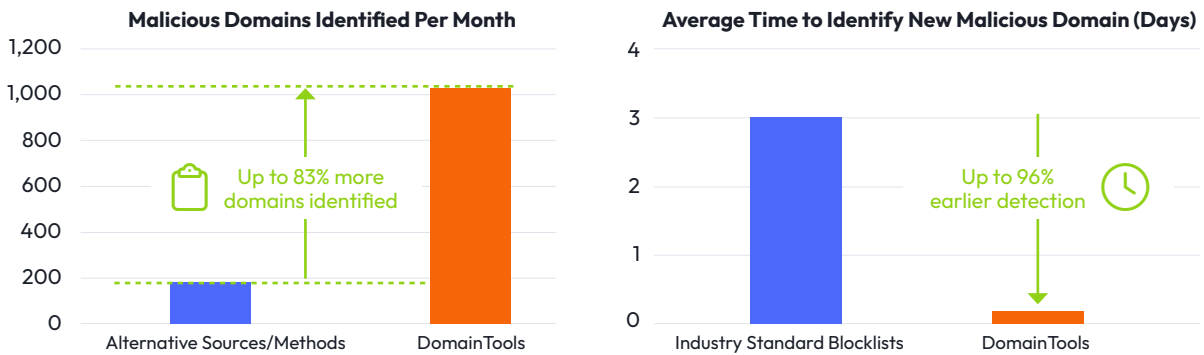
# Organizational Benefits

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 blacklist sources.



## Organizational Benefits

**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 blacklist. 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 tech 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 organizations everywhere.

## Recommended Resources:

- [Schedule a personalized demo of DomainTools products](#)
- [Unraveling Network Infrastructure Linked to the SolarWinds Hack](#)
- [CovidLock: Mobile Coronavirus Tracking App Coughs Up Ransomware](#)
- [A Brief Comparison of Reverse Image Searching Platforms](#)

