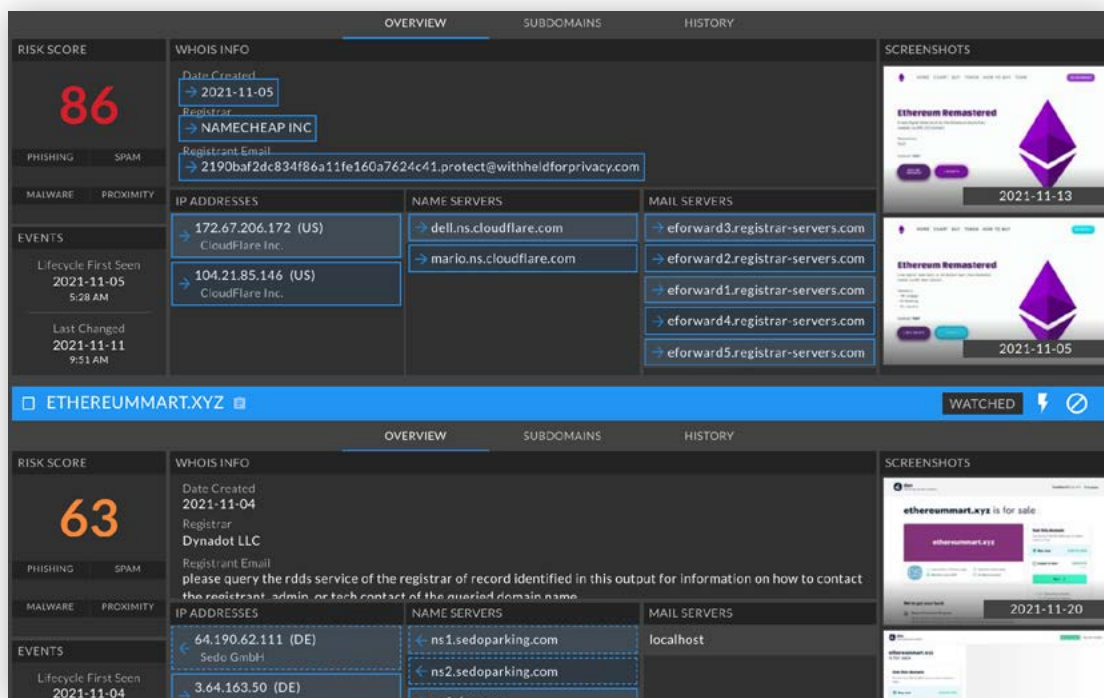




# DomainTools Iris Detect

## Discover and monitor lookalike domains with unmatched speed and coverage

**Threat actors move fast; you have to move faster.** Malicious domains spoofing legitimate brands, sites, and products cost companies billions of dollars annually in phishing and ransomware losses, sales of counterfeit products, and reputational harm. Meanwhile, **many thousands of new spoof domains flood the Internet every day.** Organizations have a pressing need to stay ahead of these actors and campaigns, but the available options have previously been unequal to the task. **DomainTools Iris Detect changes the game.**



The screenshot displays the DomainTools Iris Detect interface, showing two domain analysis results. The top result is for the domain **ETHEREUMMART.XYZ**, which has a risk score of 86. The bottom result is for the domain **ETHEREUMMART.XYZ**, which has a risk score of 63. Both results show WHOIS information, IP addresses, name servers, mail servers, and screenshots of the domain's content.

Domain	Risk Score	WHOIS Info	IP Addresses	Name Servers	Mail Servers	Screenshots
ETHEREUMMART.XYZ	86	<p>Date Created: 2021-11-05</p> <p>Registrar: NAMECHEAP INC</p> <p>Registrant Email: 2190baf2dc834f86a11fe160a7624c41.protect@withheldforprivacy.com</p>	<p>172.67.206.172 (US) CloudFlare Inc.</p> <p>104.21.85.146 (US) CloudFlare Inc.</p>	<p>dell.ns.cloudflare.com</p> <p>mario.ns.cloudflare.com</p>	<p>eforward3.registrar-servers.com</p> <p>eforward2.registrar-servers.com</p> <p>eforward1.registrar-servers.com</p> <p>eforward4.registrar-servers.com</p> <p>eforward5.registrar-servers.com</p>	<p>Ethereum Remastered (2021-11-13)</p> <p>Ethereum Remastered (2021-11-05)</p>
ETHEREUMMART.XYZ	63	<p>Date Created: 2021-11-04</p> <p>Registrar: Dynadot LLC</p> <p>Registrant Email: please query the rdds service of the registrar of record identified in this output for information on how to contact the registrant, admin, or tech contact of the queried domain name.</p>	<p>64.190.62.111 (DE) Sedo GmbH</p> <p>3.64.163.50 (DE) A100-DMV GmbH</p>	<p>ns1.sedoparking.com</p> <p>ns2.sedoparking.com</p> <p>ns1.dan.com</p>	<p>localhost</p>	<p>ethereummart.xyz is for sale: (2021-11-20)</p>

**“With the threat malicious domains pose and the methods threat actors use that make traditional tracking inefficient, DomainTools Iris Detect leads the way with impressively fast detection paired with features that separate precious signal from what would seem like noise using other vendor solutions”—Sasha Angus, Co-Founder, Scylla Intelligence**

## Discover, Watch, Act

Iris Detect is an Internet infrastructure detection, monitoring, and enforcement tool built on the industry's fastest and broadest domain discovery engine, as well as the world's largest databases of domain and IP address OSINT metadata. Capturing new domains within minutes of registration, and delivering key profile and risk data about them, Detect gives brand managers, digital risk and fraud prevention teams, and network defenders, a new level of capability for protecting their organizations against emerging cybercrime campaigns before these campaigns can inflict harm. By simply entering a keyword, such as a brand or product name, you set in motion a suite of technologies behind the scenes to alert you to dangerous new infrastructure. The discovery process also accounts for the latest tricks cybercriminals use to create look-alike domains, including homoglyphs, character substitutions, typos, and many others.

- **Discover:** with the ability to detect new registrations within minutes, Iris Detect employs the most sophisticated and extensive new-domain discovery capabilities in the industry, in all Top Level Domains. Initially-discovered domains are enriched with preliminary Whois, DNS, and Risk Score data, as well as screenshots. Detect sends notifications of newly-discovered domains matching the monitored keywords via API and email.
- **Watch:** domains of interest may be placed on a Watchlist, which provides alerts on changes to these domains as they move through their lifecycle. This gives the user an important method of tracking evolving threat campaigns, and identifying which domains are most likely to do harm. Such domains are candidates for escalation.
- **Act:** for domains showing intent to cause harm, two escalation actions are available. Report sends domains to Google Phishing Protection, which can block them in Chrome, Firefox, and Safari, among other browsers. Block flags domains in Iris Detect API responses for scripted enforcement actions in your security controls.

With a rich UI as well as a fully-supported API, Iris Detect suits a variety of analyst-driven and automated workflows to protect your users, customers, business partners, and Internet consumers around the world. Contact DomainTools to find out how our customers are reducing the likelihood of a major security event by as much as 82%, and realizing analyst team productivity gains of up to 51%.



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

[WWW.DOMAINTOOLS.COM](http://WWW.DOMAINTOOLS.COM)

© Copyright DomainTools, 2022