SOLUTION BRIEF

Domain Hijacking Recovery & Forensic Investigation

Specialized expertise to rapidly restore control and ensure successful outcomes in the face of domain-related attacks.

Domain hijacking incidents demand the most urgent level of response to limit damage to the brand and the business. Yet, these incidents often expose a coverage gap in most cyber insurance policies and are frequently under addressed by digital forensics and incident response (DFIR) providers.

IDX Domain Recovery Solutions

IDX delivers an end-to-end solution that combines rapid domain takedown, forensic investigation, and domain recovery. By removing threat actors' control, conducting a comprehensive forensic investigation, and working with registrars and hosting providers to restore domain ownership, IDX provides a structured process that minimizes business disruption and supports effective incident resolution.

WHAT IS DOMAIN HIJACKING?

Domain hijacking happens when an attacker gains control of an organization's internet domain, enabling them to manipulate or misuse domain services like websites and emails, most often to perpetrate further attacks for financial gain.

WHY IS DOMAIN HIJACKING ON THE RISE?

The growing complexity of companies' web and cloud infrastructure is leading to more prevalent security gaps. Moreover, as companies more successfully defend against ransomware, threat actors are looking for new tactics — and these gap-riddled domains become attractive targets.

Domain hijacking demands an urgent response

Time is critical when responding to a domain hijacking incident. When guiding clients through these challenges, it's crucial to understand the immediate and severe impacts:

SERVICE DISRUPTION

Domain hijacking can abruptly cut off access to essential services like websites and email, halting business operations.

CUSTOMER LOYALTY AND REPUTATION DAMAGE

Service interruptions can erode customer trust, exposing web visitors to phishing attacks or malicious content, and leading to lasting reputational harm.

FINANCIAL LOSSES

The financial toll includes operational downtime, fraudulent activities, and the substantial costs of recovery, which can be slow and resource intensive.

DATA BREACH RISKS AND LEGAL & COMPLIANCE ISSUES

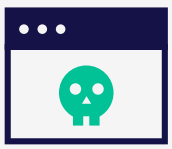
Attackers gaining control of a domain can access sensitive data, leading to potential legal challenges and regulatory penalties.

THE PROBLEM

Conventional DFIR doesn't cover domain hijacking

Domain hijacking presents one of the most dangerous attack types due to the immediacy and magnitude of negative impacts. What makes this worse is that the usual vendors and tools organizations rely on often aren't equipped to effectively address these incidents. Handling a domain hijacking incident requires specialized expertise that goes beyond what most conventional DFIR providers offer.

Conventional DFIR Lacks:



NICHE TECHNICAL EXPERTISE

Conventional DFIR focuses on system-level intrusions, malware analysis, and network forensics. But domain hijacking incidents require specialized knowledge of DNS configurations, domain registrars, and internet infrastructure.

LEGAL & OWNERSHIP COMPLEXITIES

Domain hijacking often involves legal and ownership challenges, especially with domains registered in different jurisdictions. DFIR teams typically lack the legal expertise or authority to resolve these issues.

SPECIALIZED RESPONSE PROTOCOLS & TECHNOLOGY

Unlike other breaches, responding to domain hijacking demands specialized protocols and technology to execute immediate takedown, along with expert coordination with domain registrars, hosting providers, and other legal entities.

THE SOLUTION

IDX Domain Hijacking Recovery & Forensic Investigation

IDX provides the only connected solution for Domain Hijacking Recovery & Forensic Investigation — a comprehensive and proven approach to swiftly and effectively restore domain control to organizations.

IMMEDIATE DOMAIN TAKEDOWN

Rapid response to remove the domain from the control of threat actors, mitigating immediate damage and preventing further malicious activities.

EFFECTIVE COORDINATION TO RESTORE DOMAIN CONTROL

IDX works closely with domain registrars and hosting providers to restore rightful control of the domain back to the organization.

COMPREHENSIVE FORENSIC INVESTIGATION

In-depth forensic analysis collects and compiles evidence of the malicious takeover, building an irrefutable case for legal and restorative actions.

FOR INSURERS

IDX Takedown Services

In addition to Domain Hijacking Recovery & Forensic Investigation, IDX offers ad-hoc takedown services, developed for insurers, outside counsel, and policyholders to easily request a takedown before, during or after a cyber claim.

SINGLE TARGET TAKEDOWN

IDX targets the takedown of a single entity, such as a web domain, email, or social media account. Service includes engaging directly with the registrar to compel action on our complaint. The process can be swift, often taking as little as 48 hours, but in some cases, it may extend up to six weeks, depending on various factors.

DOUBLE TARGET TAKEDOWN

Same as a single target takedown, but commonly used to target both web and email domains, which is particularly useful in cases where a threat actor may be using the domain to phish.

GLOBAL DISRUPTION NETWORK ADD-ON

Available as an add-on to IDX's single or double target takedown service, the Global Disruption Network (GDN) significantly reduces web traffic to harmful domains by submitting them to domain alerting networks. In cases where IDX is conducting a web takedown for phishing-related activities and the domain captures signup or login information, we submit it to Google Web Risk, which flags the domain as malicious and prevents it from being loaded without manual action across all Chrome-based browsers.

UNIFORM DOMAIN-NAME DISPUTE-RESOLUTION POLICY (UDRP)

This option is the only permanent solution for reclaiming a domain from a threat/bad actor and transferring ownership back to you. IDX manages the entire process, including preparing and submitting the 30+ page UDRP complaint, filing, and petitioning the World Intellectual Property Organization (WIPO) to appoint a one-member panel to oversee the dispute. We handle any rebuttals submitted by the threat/bad actor and assist with transferring the domain to your control following a successful decision. While this process can take 90-120 days, it guarantees permanent domain ownership. The total cost includes the $2,500 WIPO filing fee.

HOW IT WORKS

One partner for complete investigation, remediation and response

IDX eliminates the need to patch together multiple vendors, providing services that cover the full spectrum of needs around remediating domain hijacking incidents.

1

IDENTIFICATION

IDX quickly assesses the scope of the domain hijacking, identifying affected DNS, registrars, hosts, and any impacted systems or services (e.g., payment gateways, email, web apps). If cyber insurance is involved, IDX works under privilege with outside counsel and the claims adjuster to maximize coverage.

2

CONTAINMENT

Through the IDX platform, we directly connect to registrars and DNS hosts, blocking the threat actors' access and preventing their ability to make further changes to the DNS. Deep and dark web monitoring is deployed to watch for data leaks or coordinated attack chatter.

3

FORENSIC INVESTIGATION

IDX collects logs and digital artifacts to build a timeline and create a clear picture of the root point of compromise. The evidence is compiled and presented to registrars, hosts, and law enforcement in a way that invokes action and captures the full extent of the theft, ensuring the threat actor has no valid ownership claim.

4

LEGAL & REGULATORY COLLABORATION

IDX works with counsel to meet contractual, regulatory, and legal obligations, including identifying unauthorized access or data exfiltration. IDX then builds an impacted persons list through data analysis and review, ensuring the appropriate action can be taken to demonstrate compliance. This step includes a robust data mining analysis and manual document review.

5

REMEDIATION & RECOVERY

Lastly, IDX has the ability to take necessary actions, including UDRP filings when needed, to regain control of the hijacked domain and DNS associated with compromised systems. IDX can work with your IT team to restore access, implement multi-factor authentication, and provide long-term deep and dark web monitoring for ongoing threats.

Don't wait for the inevitable cyber attack.
Ask us about our Full-Service Response Capabilities!

855.HELP.IDX | response@idx.us

CASE STUDY

IDX helps large public utility rapidly reclaim domain

CUSTOMER: *Large public utilities operator*

4.5 hours
Time to coordinate domain takedown and prevent further damage.

35 days
vs. 17+ weeks
Time to restoring domain control with IDX, compared to averages.

$2.2M
Estimated savings in revenue through accelerated recovery of domain control.

SITUATION

After the CTO fell victim to an MFA bypass attack on the company's hosting account, the company lost control of web and email DNS. The threat actor quickly transferred the domain from the company's hosting account to a separate, new third-party account owned by the threat actor. The threat actor then began to extort via a ransom demand for the company to get back control of their domain and DNS.

IDX RESOLUTION

Immediate domain takedown

Working behind the scenes with both the registrar and web host, IDX helped to get the domain shut down from the threat actor's web and email hosting account within hours, preventing the threat actor from perpetrating further malicious actions.

Comprehensive forensic investigation

IDX conducted a comprehensive business email compromise (BEC) investigation to collect strategic artifacts and other indicators of compromise to demonstrate and support the path of the illegitimate domain hijacking by the threat actor.

Effective restoration of domain control

IDX filed a Uniform Domain-Name Dispute-Resolution Policy (UDRP) on behalf of the company, providing robust evidence from its forensic investigation to irrefutably show that the company's CTO did not authorize the domain transfer to win back rightful control of the domain and ensure the threat actor could not re-victimize the company.

IDX

IDX is a leading provider of identity protection and cyber response services for companies and individuals throughout the U.S. We combine consumer-centric software and concierge-style professional services in serving organizations across government, healthcare, commercial enterprises, financial institutions, and higher education.

Have questions? We'd like to help.

855-HELP-IDX
response@idx.us