Brand & Trademark Protection

Take the impersonation down before the campaign launches.

FOR BRAND, FRAUD, AND TRUST & SAFETY TEAMS AT CONSUMER-FACING ENTERPRISES

01 THE PROBLEM

Established brands are infrastructure for attackers: a recognized name is what makes a phishing page work, a fake support line convincing, a counterfeit portal profitable. The campaigns are built on domains, registered, parked, and weaponized on a predictable cadence, usually discovered only after customers are harmed.

02 THE APPROACH

Mythic watches that cadence. Its domain and infrastructure intelligence identifies brand-abusing registrations as they appear, connects them to the actor infrastructure behind them, and distinguishes parked opportunism from campaigns being armed for launch.

03 IN PRACTICE

Brand and fraud teams receive takedown-oriented intelligence: the hosting, registrar, and infrastructure context needed to move quickly, with actor attribution that turns a single takedown into visibility over the campaign behind it. The abuse ends before customers are harmed and before it reaches the brand's reputation.

FRAMEWORKS ATT&CK TA0042 T1583 · NIST CSF 2.0 DE.CM

WHAT YOU GET

- Early detection of look-alike and cybersquatting domains as they are registered
- Real-time brand and trademark search across newly observed adversary infrastructure
- Takedown-oriented intelligence: hosting, registrar, and infrastructure context

EVERY CONFIRMED BREACH CARRIES

01 Date and time of breach
02 Victim and destination IPs
03 Port and protocol
04 Data exfiltrated by the implant
05 Machine, user, OS, file paths
06 The implant responsible

> Nothing to install, no hardware, no access to any environment required. Mythic observes from the adversary's side of the exchange.

ABOUT VIGILOCITY

Vigilocity builds technology for identifying and eliminating threat actor infrastructure, drawing on decades of counterintelligence operations inside adversary networks.

THE METHOD

Reverse Attack Surface Analysis works from the attacker inward: tracking adversary infrastructure as it is built, then observing the victim networks that begin talking to it.

WHO RELIES ON MYTHIC

Global financial institutions, Fortune 100 brands, Big Four advisory firms, and national governments. Our clients do not appear on this page. That is part of the service.

