

Threat Infrastructure Disruption

Act while the attacker is still setting up.

FOR SECURITY OPERATIONS, THREAT INTELLIGENCE, AND INCIDENT RESPONSE TEAMS

01 THE PROBLEM

Ransomware and phishing campaigns do not begin at detonation. They begin days or weeks earlier, when the adversary registers domains, stands up command-and-control servers, and stages delivery infrastructure. Defenders watching from inside the perimeter see none of it until the first click.

02 THE APPROACH

Mythic's Reverse Attack Surface Analysis works from the adversary's infrastructure inward: identifying emerging campaigns as their infrastructure is established, attributing it to actors and tooling, and predicting likely targets from the actor's observed habits.

03 IN PRACTICE

Defenders get the window between setup and launch: time to block the infrastructure, pursue takedowns, and tune defenses to the specific actor and tooling headed their way, instead of the usual race that starts after the campaign is live.

FRAMEWORKS ATT&CK TA0042 · TA0011 · NIST CSF 2.0 DE.CM

WHAT YOU GET

- Identification of malicious domains and C2 infrastructure at establishment, not post-incident
- Blocking and takedown intelligence that shrinks the attacker's window
- Campaign context: which actor, which tooling, which targets

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 VIGILOCTY

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.