

DISRUPTING THE CYBERCRIME EXPLOITATION LIFE-CYCLE

Cyber-criminals use multiple attack vectors to compromise an organization.

iSheriff disrupts the malware exploitation life-cycle to provide unique threat protection and visibility, delivering more effective threat detection and remediation than traditional perimeter and host-based security models.



Find a site that's running vulnerable services



Hack that site to make it distribute malware (e.g. via drive-by download)



iSheriff Web Security scans sites for malicious content and vulnerabilities in real time



Send large volumes of phishing emails to unsuspecting users, tricking them to click on links pointing to the hacked site



iSheriff Email Security scans emails for phishing attacks and malicious links, which are automatically blocked



Install a key logger, or other malicious application, on the endpoint device



Malicious Web content is automatically blocked globally in the cloud across iSheriff's entire user base



Move laterally across the network to infect other devices



iSheriff Endpoint Security prevents malware (such as keyloggers) from installing or executing on endpoints and servers



Profit from credentials & other sensitive data stolen from hacked devices



iSheriff Web and Email data leak protection blocks exfiltration of sensitive information

iSheriff's cloud-based security is the simplest and most cost-effective way to protect data and devices from digital threats. Delivered as a continuously updated cloud service that is easy to deploy and manage from a single pane-of-glass console, iSheriff provides advanced multi-layered threat protection to keep your organization secure.