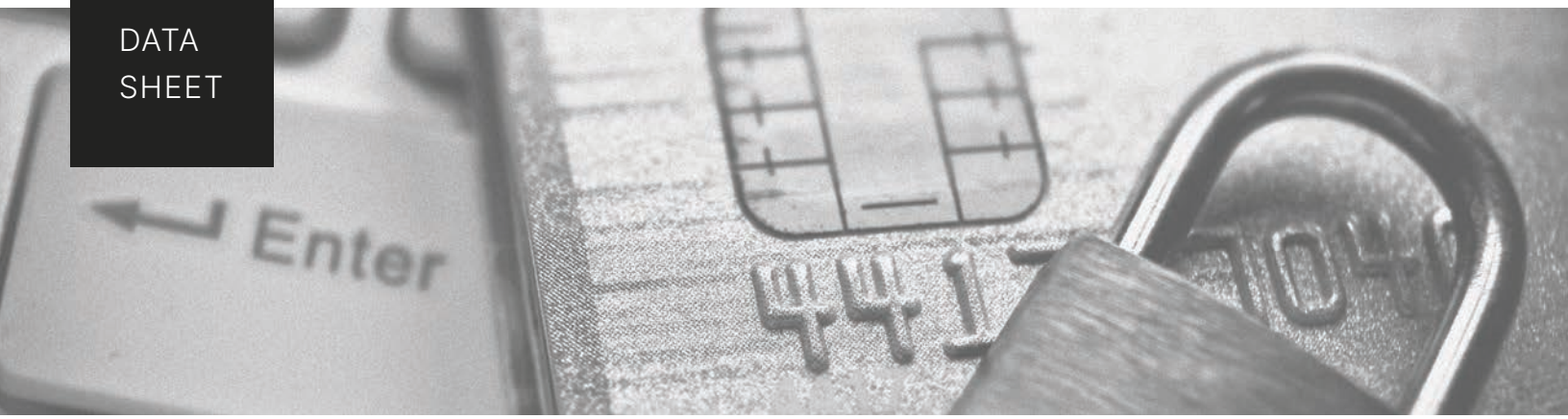
Recorded Future®

DATA SHEET



Magecart Overwatch

Identify compromised e-commerce domains

Card Not Present (CNP) fraud largely comes from Magecart digital skimming attacks, which involve hackers injecting malicious code into target websites to steal payment card data from unsuspecting shoppers. This data is then exfiltrated to the hacker's own infrastructure and sold on the dark web. As card fraud continues to shift online, strong Magecart-monitoring capabilities are essential to any institution's efforts to stay one step ahead of fraudsters.

Recorded Future Payment Fraud Intelligence developed Magecart Overwatch to map criminal activity across e-commerce sites. Through proactive domain scanning and detailed technical and card data analysis, Magecart Overwatch provides near real-time visibility into newly breached e-commerce domains, globally, enabling financial institutions to take immediate action for fraud mitigation.

Capabilities

Magecart Overwatch provides immediate insight into infected e-commerce sites, including:

- Matching criminal indicators of compromise (IOCs) to active infections
- Tracking a breached domain's full exposure window
- Covering the attacker's infrastructure, including attacker domains, malicious code, and exfiltration domains
- Uploading all data points to a custom dashboard to identify parallel links between infections
- Providing custom merchant monitoring, which delivers daily alerts on newly identified infections configured to client preferences

KEY BENEFITS

- Receive comprehensive, immediate, and actionable intelligence on compromised domains
- Access premium research on Magecart skimmers, Magecart digital skimming attacks, and identified skimmer domains
- Supplemental reporting analyzes new cybercriminal campaigns and tactics, techniques, and procedures (TTPs)

The Finished Intelligence Portal (available by subscription) enriches Magecart data with:

- Detailed analysis of notable Magecart digital skimming attacks
- In-depth enrichment of the targeted sites, including Merchant Name, Merchant ID, global ranking, and much more
- Analysis on the links between magecart campaigns and the criminal dark web shops where the stolen data is later trafficked
- Relationships to broader campaigns, including other targeted sites and their information, and new methodologies

The Recorded Future Edge

Magecart Overwatch's monitoring capabilities provide comprehensive, immediate, and actionable intelligence on compromised domains across the globe. We provide the full window of exposure from the time the infection was identified through when it was remediated. This premium analytical tool exposes Magecart skimmers, Magecart digital skimming attacks, and identified skimmer domains to enable proactive fraud mitigation strategies. In addition to our Finished Intelligence Portal, we offer Magecart reporting specific to your organization as an additional service.