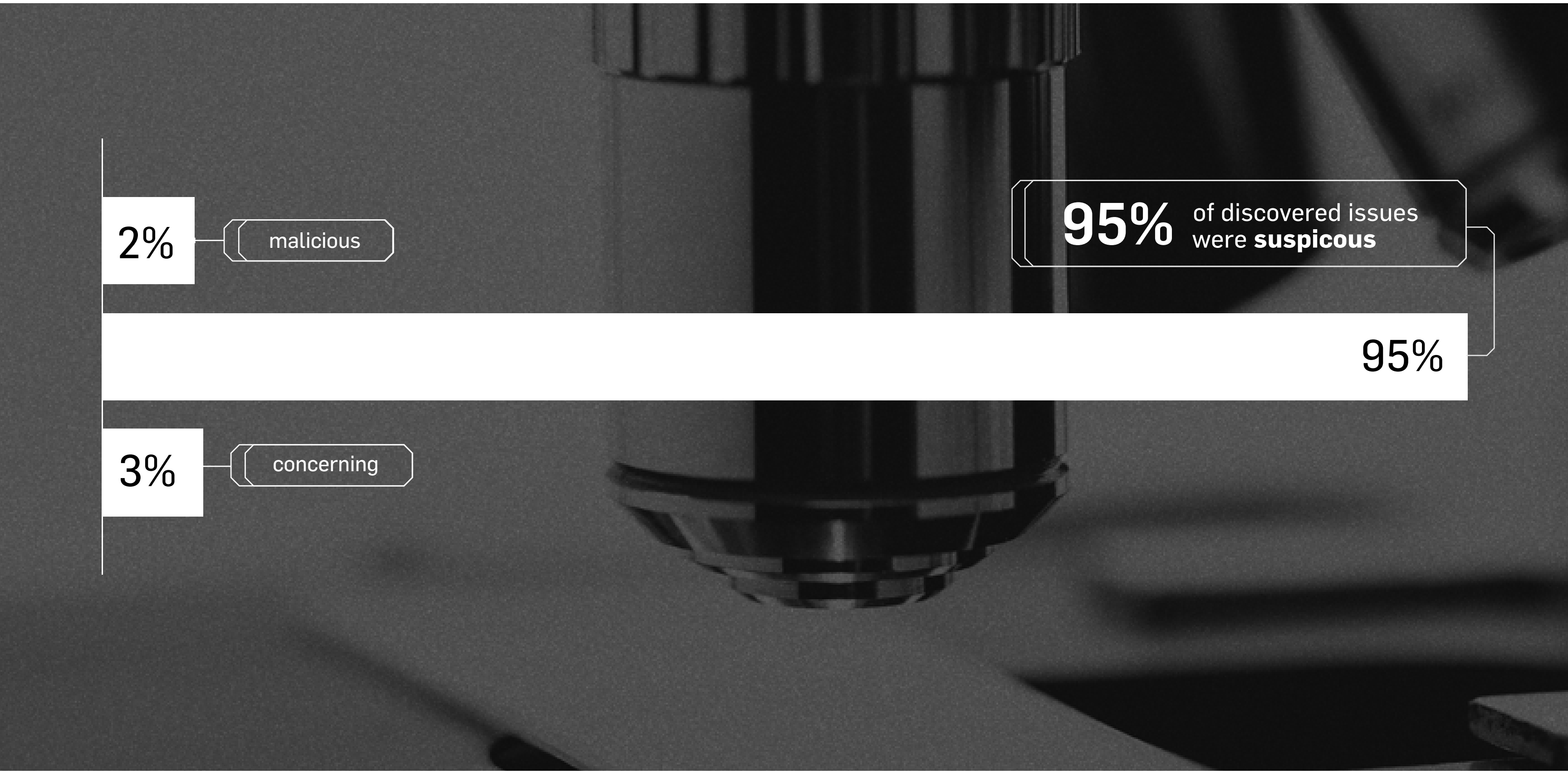
ECOMMERCE SECURITY TRENDS

Findings From Ecommerce Security Service by SecurityMetrics

SecurityMetrics Shopping Cart Inspect helps businesses detect if their Shopping Cart has been breached.

With the help of Shopping Cart Inspect, SecurityMetrics Forensic Analysts review businesses' rendered webpage code on their shopping cart URL to collect evidence of a skimming attack.



95% of discovered issues were **suspicous**

64%

of payment page reviews completed with Shopping Cart Inspect identified malicious, suspicious, and/or concerning issues on researched ecommerce sites.

On average, inspected websites had 0.73 issues discovered.

Those issues include the following classifications:

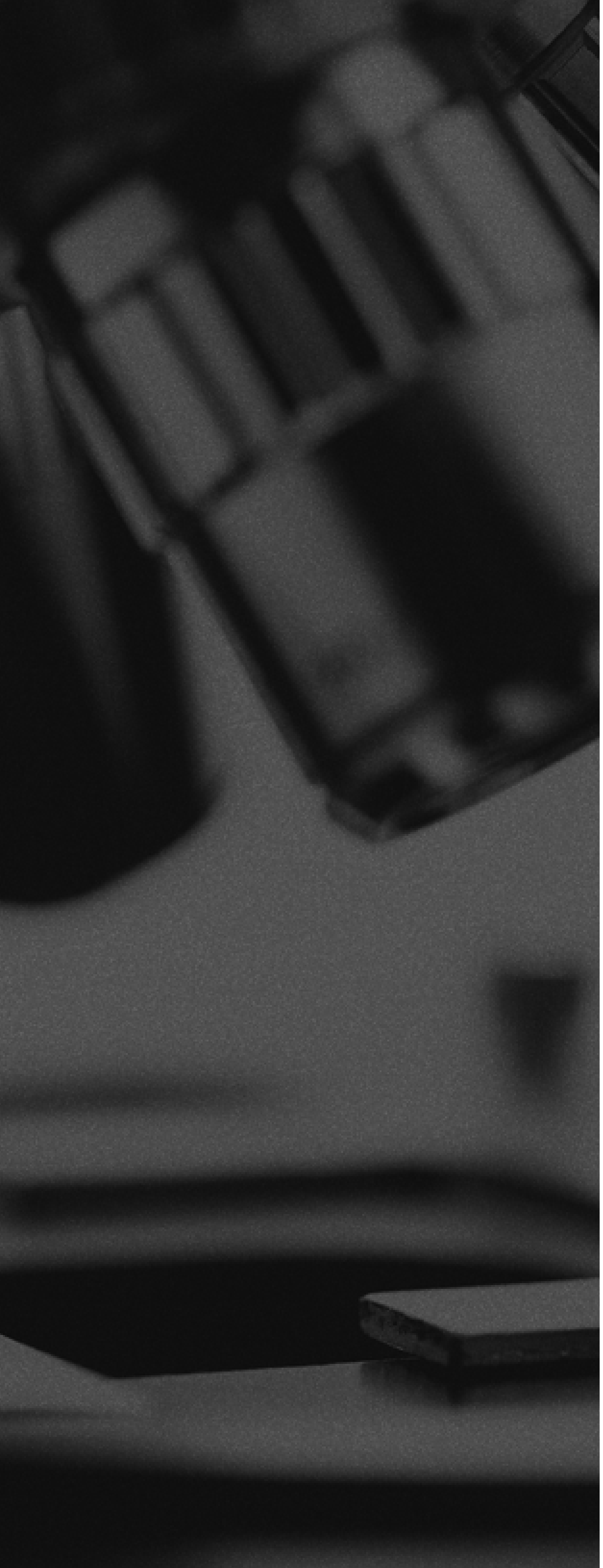
- **Malicious:** Evidence of card data being stolen. (*Highest threat level*)
- **Suspicious:** Identified issues increase the probability of a potential exploit. (*Medium threat level*)
- **Concerning:** Unlikely method of being breached, but identified issues could lead to a potential exploit. (*Low threat level*)

TOP 5 MALICIOUS ISSUES FOUND

1. **Malicious Javascript**
   Javascript appears to be acting in a malicious manner, such as harvesting credit cards or other sensitive data.
2. **Malicious Double Checkout**
   Double post of credit card data returning to alternate checkout page on merchant's server.
3. **Malicious Post**
   A script is running with a post of data to a known bad site.
4. **Form Jacking**
   Authorized payment webform is being replaced by a counterfeit.
5. **Directory Browsing Enabled**
   Directory Browsing is enabled on the web pages analyzed.

TOP 5 SUSPICIOUS ISSUES FOUND

1. **Javascript issue**
   Out-of-date JavaScripts can lead to vulnerabilities available for future malicious attacks.
2. **Out-of-date CMS - Suspicious**
   Out-of-date web components. Unpatched or un-updated software is a leading cause of sites losing sensitive data.
3. **Configuration Issue**
   Missing required web server security headers.
4. **Ads/Business Intelligence**
   Advertising/Analytics content is being pulled into the pages being reviewed in the checkout environment. This can be a source of intermittent card/data loss due to drive-by malvertising.
5. **Suspicious double checkout**
   Double post of credit card data returning merchant's checkout page on the server. This practice could impact security of the site and should be reviewed for business need.



TOP 5 CONCERNING ISSUES FOUND

1. **Configuration Vulnerability**
   A configuration item with a website or web server is not following best security practices.
2. **Checkout Configuration Issue**
   The implementation of certain aspects of the checkout process may not follow best security practices and could leave merchants vulnerable to certain types of attacks.
3. **Mixed HTTP/HTTPS**
   Content called via HTTP in an HTTPS environment, breaking strict SSL/TLS protocol. In severe cases, this can be exploited by bad actors to view privileged content.
4. **HTTP Header Issue**
   Improperly configured HTTP headers can provide attackers with specific information about your web server setup, such as vulnerable software versions.
5. **SPAM Watch**
   A domain has been flagged by the SPAM community, which could be using the email server to transmit malicious communications by bad actors.