

# Attackers Exploit Defensive Gaps

Adversaries are committed to continually refining or developing new techniques that evade detection and hide malicious activity. Security teams must adapt their approach to protecting the organization and users from increasingly sophisticated campaigns.

## Attackers Shifting Attack Methods

**250% SPAM**

Malicious spam activity back on the rise



Downloader

**6X**

more prevalent than other types of malware

Preferred attack vectors:



Adobe Flash



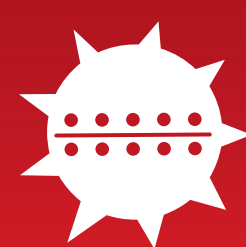
Microsoft Internet Explorer

Microsoft Silverlight

Java

exploits dropped

**34%**



Exploit kit activity fell

**88%**

**250%**

Malvertising Add-ons spike 250% in October



## Users Complicit Enablers

**2X**

Users in highly targeted industries twice as likely to succumb to Clickfraud and Adware



Unpatched browsers are a dominating concern

Percentage of users running latest versions:

Microsoft Internet Explorer **10%** Google Chrome **64%**

Malicious add-ons unwittingly loaded from untrustworthy sources



## Defenders Ineffective Defenses

Before an Attack



Only **40%**

of CISOs report using patching and configuration as a defense, while the others leave holes for the attackers to exploit

**56%**

of all OpenSSL versions are older than 50 months, potentially exposing crypto keys and passwords



During an Attack

**59%**

of SecOps report firewall logs are the most common tool to analyze compromised systems, offering limited data and no context

Only **43%**

of SecOps report leveraging Identity Administration and Provisioning, which means over 50% of organizations lack context to user identity and activity



After an Attack



No leading method to eliminate causes of security incidents were identified:

For example, only **55%**

of SecOps quarantine or remove malicious applications as a method

Once inside, attackers create a persistent, unchecked state of infection in stealth.

Based on 2014 data