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

Java exploits dropped **34%**

Exploit kit activity fell **88%**

Preferred attack vectors:
- PDF
- Adobe Flash
- Microsoft Internet Explorer
- Microsoft Silverlight

Malvertising **250%**
Add-ons spike in October

Users
Complicit Enablers

2X
The likelihood that users in highly targeted industries succumb to Clickfraud and Adware

Unpatched browsers are a dominating concern

Percentage of users running latest versions:

Microsoft Internet Explorer	Google Chrome
10%	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

Download the 2015 Annual Security Report
www.cisco.com/go/asr2015

cisco