

# 2015 Cybersecurity: Attack Resiliency Challenges Industry Collaboration



**Attackers** are commandeering legitimate infrastructure and reaping millions in profit.



**Defenders** are struggling to detect and combat threats, and confidence is falling.

## Attackers Evade and Reconstitute

Attackers are building resiliency into their operations. If detected, attackers quickly reconfigure and can reconstitute on new systems with new IPs in minutes

### Angler

This attack often goes undetected by commandeering high reputation resources

**15K** unique sites redirect traffic via malvertising

**Proxy Servers**  
Multiple servers without malware, but with commingled resources on legitimate hosting providers, funnel users toward exploit servers

**Exploit Servers**  
60% of payloads are ransomware. Delivery is global and through multiple providers

**Status Servers**  
If operating status is compromised, or tampering is detected, the attackers are alerted

**Small IP Infrastructure**  
Attackers can roll through IPs on 8-12 active systems per day

**\$60M** /year estimated profit from just two identified campaigns alone

## SSHPsycho

The global, collaborative, brute-force attack

**DDoS**  
10,000 X Machines leveraged

**Botnet Set Up**  
1. China-based brute-force password attacks to create botnet  
2. 24 hours later, US-based login with harvested passwords, to download DDoS root-kit on compromised devices

**Massive Impact**  
35% of all SSH traffic across the Internet was comprised by SSHPsycho

**Commingled and Compromised**  
221% increase in compromised WordPress sites

## Defenders Lack Collaboration

Defender confidence in their ability to detect, defend, and recover from cyber attacks is falling, while regulators and investors are seeking more visibility into organization's cyber risk strategy.

### Falling Confidence

Confidence in having the latest technology down to 59%  
NOT having the latest technology increased to 37%

### Before

54% confidence in ability to verify an attack occurred

### During

54% confidence in ability to defend against attacks

### After

45% confidence in ability to scope and contain an attack

## Compromised and Fractured

92% of Cisco devices surveyed across the Internet were running known vulnerabilities, with an average of 26 each

31% of Cisco devices surveyed were EOS

5% of Cisco devices were EOL

56% review security policies on a regular basis

## Constraints

Organizations exhibit low degree of collaboration: During security incidents, only

- 21% notify business partners
- 18% notify external authorities
- 15% insurance companies

- Barriers to adopting advanced security technology
- 39% Budget
  - 32% Compatibility issues
  - 25% Certification requirements



Download the Cisco 2016 Annual Security Report  
[www.cisco.com/go/asr2016](http://www.cisco.com/go/asr2016)

