



Cisco 2017
Midyear Cybersecurity Report

Table of Contents

Executive Summary	03
Major Findings	05
Introduction	07
Attacker Behavior	09
Exploit kits: Down, but not likely out.....	09
How defender behavior can shift attackers' focus.....	11
Web attack methods provide evidence of a mature Internet	12
Web block activity around the globe	13
Spyware really is as bad as it sounds.....	14
Decline in exploit kit activity likely influencing global spam trends	18
Malicious email: A closer look at malware authors' file type strategies.....	19
Worried about ransomware? Business email compromise may be a bigger threat	22
Malware evolution: A 6-month perspective.....	23
Threat intelligence from Talos: On the trail of attacks and vulnerabilities	24
Time to detection: The tug-of-war between attackers and defenders tightens.....	26
Time-to-evolve trends: Nemucod, Ramnit, Kryptik, and Fareit.....	28
The expanding life spans—and overlap—of DGA domains.....	33
Analyzing infrastructure broadens knowledge of attacker tools.....	34
Supply chain attacks: One compromised vector can affect many organizations.....	36
The IoT is only just emerging but the IoT botnets are already here	39
Extortion in cyberspace: Ransom denial of service (RDoS)	41
The changing economics of malicious hacking	42
Ransomed medical devices: It's happening	42
Vulnerabilities	46
Geopolitical update: WannaCry attack underscores risk of hoarding knowledge about exploitable vulnerabilities.....	46

Vulnerabilities update: Rise in attacks following key disclosures	47
Don't let DevOps technologies leave the business exposed.....	50
Organizations not moving fast enough to patch known Memcached server vulnerabilities.....	54
Malicious hackers head to the cloud to shorten the path to top targets	56
Unmanaged infrastructure and endpoints leave organizations at risk.....	59

Security Challenges and Opportunities for Defenders

61

Security Capabilities Benchmark Study: Focus on verticals.....	61
Company size affects approach to security.....	62
Using services to bridge knowledge and talent gaps	63
Outsourcing Service and Threat Alert Data by Country.....	64
IoT security risks: Preparing for the future—and the now	65
Security Capabilities Benchmark Study: Focus on select verticals.....	66
Service providers	66
Public sector	68
Retail	70
Manufacturing	72
Utilities	74
Healthcare.....	76
Transportation	78
Finance	80

Conclusion

83

Security leaders: It's time to claim a seat at the top table.....	84
--	----

About Cisco

86

Cisco 2017 Midyear Cybersecurity Report contributors.....	86
Cisco 2017 Midyear Cybersecurity Report technology partners	88