

SERVICE PROVIDER

6 KEY FINDINGS

From the 15th Annual Worldwide Infrastructure Security Report (WISR)

While DDoS attacks evolve in size, volume, frequency, and complexity each year, attackers never stray from one bedrock principle: If it's important to network operators and enterprises, it's important to them.

1

Multi-vector attacks are up; DDoS attacks are a top concern of service providers

In 2019, 58% of service providers reported multi-vector attacks. And 65% say DDoS attacks are a top concern for 2020.

58% Reported multi-vector attacks



65% Say DDoS attacks are top concern for 2020

2

Publicly exposed service infrastructure is #2 concern for service providers

Attacks on publicly exposed service infrastructure such as cloud services increased dramatically. 51% of service providers reported such attacks in 2019 compared with only 38% in 2018. 55% call it a top concern for 2020.

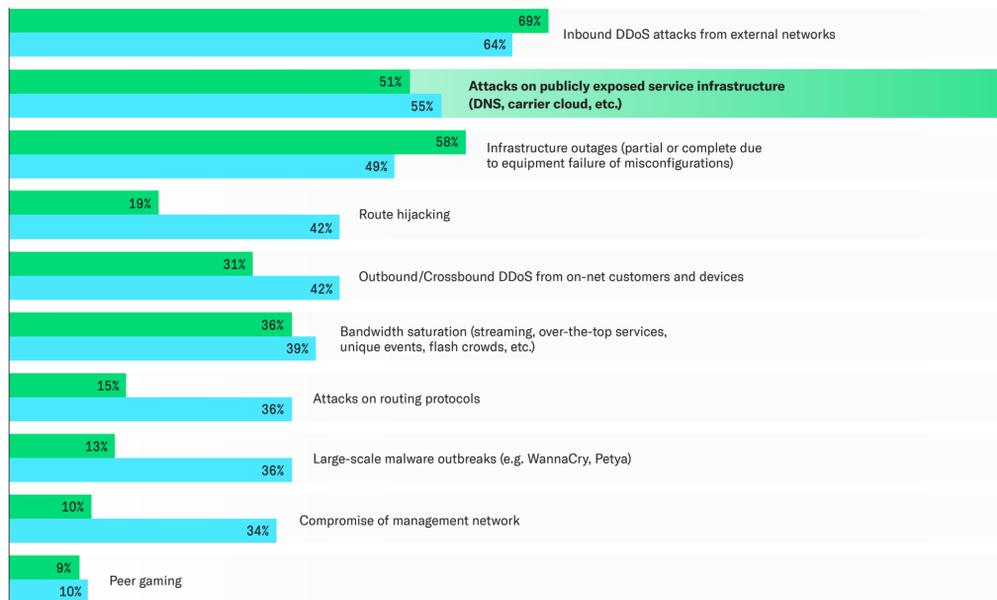


Figure 1: Service Provider Threats vs. Concerns

3

Hot service provider attack targets



Carpet Bombers Sideswipe Satellite Telecoms

Satellite telecommunications saw significant increase in attacks, with 295 percent increase in attack frequency, likely due to scenarios such as the high-impact carpet-bombing attacks that targeted financial organizations in Asia Minor and Europe in 2H 2019. By sharing large netblocks with organizations that didn't have their own IP space, the satellite telecommunications providers experienced significant collateral damage from these attacks.

▲295% Increase in attack frequency



Focus Point: Mobile Networks

Adversaries turned up the attack volume on the wireless telecommunications sector, with a 64% increase in attack frequency and a 33% increase in max attack size. Gaming continues to be a large motivation for attacks, and mobile networks are increasingly popular access points, since users in many Asian countries rely on their phone service for wireless hotspots. Attackers naturally follow their targets, leading to the upward attack growth in the sector. Attacks in the wired telecommunications sector, meanwhile, grew at a comparatively modest 3%.

▲64% Increase in attack frequency

4

Telecommunications is hackers' choice

Telecommunications is number 1, 2, and 4 — out of 4 — on the top sub-vertical sectors with a combined **1,991,927 attack frequency**.

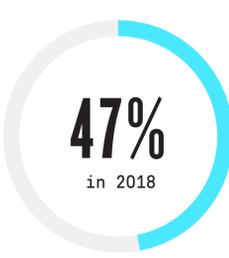
Rank	Vertical	Attack Frequency	Max Attack	Classification
1	Wired Telecommunications Carriers	1,073,851	421.5 Gbps	Information
2	Telecommunications	575,749	348.9 Gbps	Information
3	Data Processing, Hosting + Related Services	467,475	243.4 Gbps	Information
4	Wireless Telecommunications Carriers	342,327	492.5 Gbps	Information

Figure 2: Top Four Sub-Vertical Sectors

5

Interest grows in managed security services from 47% to 60% from 2018 to 2019

The challenging hiring market has caused more enterprises to turn to service providers for security support, as more than half of service providers reported growing interest in DDoS managed services from customers. Cloud/hosting providers were the top vertical expressing interest, up from 5th place last year. As we predicted, this has led to an explosion in managed security service offerings.



6

Service providers need third-party assistance with their SOC's

Service providers are turning to third parties when it comes to Security Operation Center (SOC) capabilities. The people problem is so acute that even at companies where the network is the business, 42% either have no SOC at all, outsource completely, or use the hybrid model.

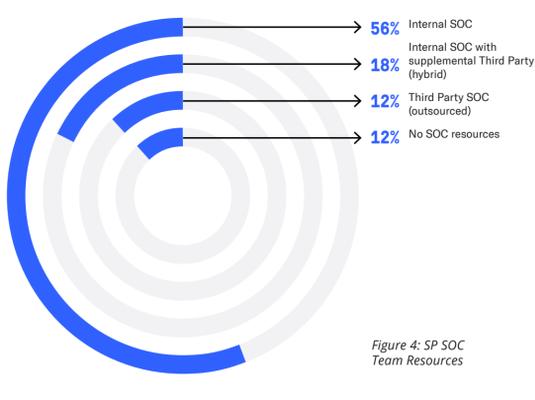


Figure 4: SP SOC Team Resources

THE TAKEAWAY

The overall threat landscape only knows one direction: up.

Nation-state groups proliferate globally while cybercriminals seem one step ahead of the game, targeting not only enterprises and service providers, but also their customers. Key digital transformation technology like cloud services and mobile networks and devices have become prime targets, while botmasters eagerly take advantage of the ongoing deluge of vulnerable IoT devices. These adversaries are smart and motivated, and we can count on them discovering and weaponizing new attack vectors or adding new variations to existing ones.

[READ THE FULL REPORT](#)

[GET MORE DDoS INFO FOR CSPs](#)