

RADinsight Threat Intelligence

Telecom Business Security Services

To safeguard their normal business operation, enterprises need to protect their resources from malicious traffic, minimize attack surfaces, and secure access to corporate resources. In many cases, this complex task is too challenging to handle internally. Hence, many organizations prefer to outsource managed solutions from communications service providers (CSPs). According to analyst firm Analysis Mason, 61% of small businesses and 79% of medium businesses prefer to purchase cyber security services along with network and internet services, as opposed to them being standalone or part of an IT service. This is a perfect opportunity for CSPs to expand their offering with managed cyber security services.

RADinsight TI (Threat Intelligence) allows CSPs to augment their security service offering with network-embedded security architecture that is implemented at customer and network edges. This enables CSPs to deliver secure access and malicious traffic prevention to their business customers.

DDoS in Telecom

Distributed Denial-of-Service (DDoS) attacks are one of the key risks that disrupt normal operation. These attacks have increased dramatically recent times. According to RADware's 2024 Threat Report, DDoS attacks per customer grew by 94% in 2023 compared to 2022. The average DDoS attack volume per customer also increased by 48% in the same year. Additionally, the sophistication of these attacks has risen, causing significant disruptions to both CSPs and enterprises.



DDoS mitigation services by over-the-top (OTT) providers are currently dominating the market. They are either being sold directly to enterprises or resold by CSPs. However, to remain competitive, CSPs should be able to offer enterprise customers affordable DDoS protection solutions that are based on their own network's intelligence. This would allow them to address different sets of functional and commercial requirements, while monetizing their network and keeping its performance and integrity.

DDoS Defense Strategies

The most popular method to thwart a DDoS attack is by "scrubbing" suspicious traffic, meaning rerouting suspicious traffic to dedicated scrubbing centers where it's analyzed. Legitimate traffic is then routed back to its destination, while confirmed malicious traffic is blocked. Here are various types of scrubbing, and their use depends on the perceived risk and available budget:

Reactive scrubbing is mainly used by customers with a low perceived risk. It is activated on customer request when that customer experiences a DDoS attack. As result, traffic coming from the internet to the customer is rerouted to the scrubbing center using BGP (Border Gateway Protocol), typically within 15 min of alert. The scrubbing center filters out malicious traffic and passes on clean traffic towards the protected destination. This method consumes the least amount of scrubbing resources and is therefore the least expensive one. However, it leaves the enterprise exposed to the attack until the scrubbing process is activated, which takes valuable time during which the enterprise can be compromised.



Figure 1. Reactive Scrubbing

Proactive scrubbing is used for businesses with a higher perceived risk, who are experiencing more frequent DDoS attacks. In this method, inbound traffic is constantly monitored by the service provider via an additional detection module. Upon detecting an attack (typically within 2 minutes), the infected traffic is rerouted to the scrubbing center using BGP. The traffic remains active for a period defined by the service provider pricing policy, which could range from four hours to unlimited. The detection is based on NetFlow analysis, and its cost depends on the NetFlow sampling rate. Due to cost considerations and the nature of aggregated traffic, the detection module is normally tuned to a relatively high-resolution threshold, making it suitable for volumetric attacks and large enterprise traffic. However, the majority of DDoS attacks are short and peak below 1Gbps, so they might be detected too late or be completely missed by scrubbing center detection modules. These low volume attacks can take down an SMB (small to medium business) firewall in a second, enabling a cybercriminal to infiltrate and map a company's network, and possibly install malware to cause significant damage.

Low volume DDoS attacks don't require extensive resources to launch – they can be carried out from a single machine so that virtually anyone can launch it. That is also the reason why these attacks are very popular among DDoS-for-hire services targeting SMBs.



Figure 2. Proactive Scrubbing

Always-on scrubbing is the most effective, but also the most expensive type of scrubbing. It implies permanent rerouting of traffic to the scrubbing center. This method is used for customers with "clean pipe" requirements or when the scrubbing detection sampling rate is too low for a timely attack detection on SMBs with relatively low bandwidth.



Figure 3. Always-on Scrubbing

In addition to scrubbing techniques, there are also In-line appliances that operate directly in the path of the network traffic to inspect and filter it in real-time. These can be used as an alternative to scrubbing centers. Although they provide fast mitigation of DDoS attacks, they require a substantial hardware footprint to accommodate inspection of the entire traffic. They are also quite expensive, become ineffective when saturated and create additional weak points in the network.



Figure 4. In-line Appliance

RADinsight Threat Intelligence

RADinsight TI (Threat Intelligence) is a disaggregated, software-based DDoS protection solution that is distributed across customer and network edges. It operates on top of existing network hardware to provide proactive DDoS protection over Ethernet access and managed routers. It addresses the needs of enterprises of all sizes, providing CSPs with a competitive solution for their business customers.



Figure 5. RADinsight TI: Access Embedded Security

RADinsight TI solution:

- Allows bundling with Ethernet Access or managed CPE as an add-on
- Allows CSPs to offer attractive security services to new customers, enabling them to eliminate the cost barrier
- SaaS model helps controlling investments
- Provides a better service with distributed detection for all attack volumes
- Scales with access bandwidth
- Improves network utilization/lowers network cost by eliminating the need to traffic rerouting
- Multi-vendor support

Solution Brief

Victim3		~ Er	Partially Miligated	Mode User Confirmation			Group			1.64G 38	n 11.62K
Time Filter: Last 5 minutes	8									Stop Auto Mitigati	ion + Manual Mi
Total Inbound Trat	fic	_					Jun 2024 06 47:00 F Istal 1.5 Halcous 836. halcor Hadrect Nadeect 1.2	1M 965 XI BIP5) 4M 0 95	al licious	ter Contribution	List Ring BPS a dpro-emulat dpro-emulat a dpro-emulat b dpro-emulat
1G 0 10:42	10:42:30 10	Protecting Edge Colleman System Protection Cright / Version Victim3	m må / Protected Object DasAde	Sard Mana	Particly Milgared	Block User Confirmation		Group #A2		,	1930 298 19K
ID IP Range 2_143 12.53.1	Detection Severity	55 45 35							footMatics	- 1	
10 IP Range 2_143 12.53.1.	Detection Severity	Attacked Pp # D	1940-30 ESM election & Miligation	19430	19-45 Policer	19.05.50 18.04 Display Activ	1996.20 Diseases All	18-07 19-07-00 Praffic - 12,53,159,3	Ind Malco Mal		
ю Р Янере 2_143 12.531. Тор 10 Аррісаю	Detection Severity <u>1133</u> SECON	Attacked Pp # D	198330 1654 election & Milgarion Milgados Seevity	1984-30 Traffic Filters 2 Ion jon So	1945 Policer at the Ex	19.55.30 19.04 Display Active C	et sec.30 Director Alt 10 40	18-07 18-07-09 traffic + 12,53,159.3	Ind Micro Micro Micro Micro Micro Micro 78:60		
10 Ф Янара 2_143 12.53.1. Тор 10 <u>Аррісан</u> наже ©	Detection Severity <u>1133</u> SECON Ons Talkers Destinat Protect/Put	40 40 40 40 40 40 40 40 40 40 40 40 40 4	1923.01 1956 electon & Mitgation Mitgation Security 2.1.01 Wittener	1994-30 Traffic Filters ® Net (per Sta 507-204 148.87X 06	19-05 Policer at time Ete 5 Jun;14:20:52	19.95/20 U.96 Display Active (1 Tase	1940.30 Proper All Food IF 10 40 30	11.07 10.07.00 Paraffe - 12,53,159.3	 Find Minito Print Print Minito Print <li< td=""><td></td><td></td></li<>		
10 Ф Янере 2_143 12.53.1. ТОР 10 Аррісал Name © ТСР 100	Detection Severity 1.143 MICRAN ons Talkers Destinat ProtectPert TCP:1900	40 40 40 40 40 40 40 40 40 40 40 40 40 4	1983/8 1864 etector & Mögston Register Leony 2.13 Witten	1994.20 Traffic Filters & bes pes So 907.204 148.87K 06	12-05 Policer at time Exe 6 Jun(14-20-32	1100.2 108 Data Arter (The	1996.20 Dropey At Total IF 10 50 50 50 50 50	1807 1803.30 traffic - 12.53.159.3	 Find Minor Price Minor Minor Price Price Price Price Price Price 		
10 Ф Якере 2_143 1253.1 Тор 10 <u>Аррісалі</u> жане 0 тор:100 sunpc	Detection Severity - 1.143 INCOM Ons Talkers Destinat Protect Part TCP/1900 TCP/111	10 60 60 60 60 60 60 60 60 60 60 60 60 60	theological and the second sec	1996.20 Tradic Filers ¥ Nes (per So 507.204 148.87K 05	toos Policer at they Exe 5. Jung 14 20 32	110.2 100 Duay Acri (120	19.66.28 Diructory All F 10 10 10 10 10 10 10 10 10 10 10 10 10	1047 1045.05 traffic - 12,53,159,3	 Indi Mato 		
р Ф Якера 2_143 12531 Тор 10 Аррісал кане 0 тор: 1900 sumpc sumpc	Otheration Severity - 1.13 Microsov Talkars Destanda Presection TCP 190 TCP 190	Atached Py © D	etection * Mitigation Register Eventy 2.132 Without	HARDA Tradic Filers ¥ Nes (per Se Se7 200 HB 87K 05	to as Policer at the Ew Exactly 2012	1140.3 1140 Duay Ann C 1 Ine	10 00.00 10 0000 A 10 40 20 20 20 20 20 20 20 20 20 2	9.67 9.63.59 9 traffic - 12.53.150.3	Ind Mac M		
	Detection Severity - 1.13 BECOM ON Talvers Destinant PetercePeter TCP 110 TCP 112 TCP 122 TCP 151	Anades Ps () Anades Ps () Table 1 () T	etection * Mogason magain teamy 2.13 minor	1994.20 Tradic Filters F Met (pet Sta 907.201 148.87C 00	Notes Policer at the first 6. Jun(54.2032	1100.3 10M Doury Active C Doury Active C	19 56.0 10 Monty All 10 10 10 10 10 10 10 10 10 10	9.07 9.03.0 9 traffic - 12.53,150.3 0 0 9.0	Indi Nacio Na		
0 P Range 2,143 12.33.1 Name 0 TCP 100 Sump Into Sump Into Sump Into	Delotion Severity 1.53 WEDRA Delotion Tables Destinat Protect/Prot TCP 1900 TCP 191 TCP 192 TCP 193	50 50 50 50 50 50 50 50 50 50 50 50 50 5	1933. USA etection * Miligation Miligation Learning 2.132 William 2.143 William	NACH Tradic Pilers # No jan for 107304 Vellow for 109304 Vellow for	Notes Policer at the Exe 5. Juny 14 20 52	1000-20 0000 Damas Anton () Tam	Table St Prover att Table St St St St St St St St St St St St St S	11.07 11.0.1.50 Traffic - 12.53.150.3 0 10.0 10.0 10.0 10.0	 In our In our		
0 Рануе 2,143 12.03.1 ТСР 10 <u>Аррисан</u> ТСР 1100 5/17/17/17/17/17/17/17/17/17/17/17/17/17/	Destina Sentra 1.53 Elitera Pastear Part Pastear Part TCP 160 TCP 151 TCP 152 TCP 151	10 0 0 0 0 0 0 0 0 0 0 0 0 0	etato Van etato F Magaton ELO Meser ELO Meser Mesere 19111	19923 Traffic Filters # Net Table 1000 00 1007 200 148 800 00 2000 1 7 200	Bells Policer at the Exe Exertit 2002	NASS NA Dama hav () Tax	100.5 100.5 100.0 10 10 10 10 10 10 10 10 10 1	907 00730 traffic + 12,53,190,3 0 00 1994 1994 1994 1994 1994	Ind I		
0 Рание 2,143 2,231 New 0 О ТСР 100 Аррисан 5007 100 5007 100 50000000000000000000000000000000000	Descton Soundy 1.53 BODING Tables Destruct Personal TCP 160 TCP 161 TCP 161 TCP 161	10 10 10 10 10 10 10 10 10 10	UBLIC DAR electron F Magneton memor Lectron F 2.2.0 without Manufacture Top H2H Top H1 Top H1 Top H1 Top H1	104628 8 Traffic Filters # 1057304 V48 DNC 00 1057304 V48 DNC 00 1057304 1720K 105804 1720K	Bells Policer at the Exe Exertic 2002	100.3 100 Damp Acres (100 Alerts 9 (1710)004227,34,96,74 (1710)004227,94,96,76	100.07 100 00 00 00 00 00 00 00 00 00 00 00 00	10.0° 000.00 19.06 - 12.53.150.3 00 0.0 10 10 10 10 10 10 10 10 10 10 10 10 10	- 64 - 64 - 64 - 64 - 64 - 64 - 64 - 64	ана са	

Figure 6. RADinsight TI GUI. SP and customer view

Technology and Architecture

RADinsight TI includes the **RADinsight TI Collectors**, which are located in regional data centers to collect telemetry from Ethernet access devices/managed routers. These collectors employ advanced AI algorithms to detect and classify orchestrated DDoS attacks through the **RADinsight Detectors**.

The RADinsight Detectors utilize the hardware of peering routers to mitigate attacks once detected at the customer edge. The mitigation policies are set by RADinsight TI Controller, which also exposes APIs towards the security management platforms used by the service provider. Fully containerized, the RADinsight TI Controller can be deployed on public clouds or at customer premises.

Significant TCO Reduction

RADinsight provides dramatic reduction of cost for hardware and the associated power, rack space, cooling, and similar requirements.

The growth in volume of both network traffic and DDoS attacks strains scrubbing capacity, especially as networks become more distributed with more peering points, resulting in network starvation as traffic needs to backhaul towards existing scrubbing centers at the expense of available bandwidth. RADinsight TI saves network resources needed for backhauling malicious traffic for scrubbing.

RADinsight TI requires much less ongoing engineering and network adjustments, maintaining CSP network architecture as is.

RADinsight TI applies a SaaS model and disaggregated architecture for gradual and controlled deployment and investments.

To learn more about RADinsight Threat Intelligence, contact us at market@rad.com.

