Aktualne trendy w atakach DDoS – perspektywa izraelska

Andrzej Sienkiewicz Sales Engineer @ Radware CSO Council, 23.11.23 °: radware

Web DDoS Tsunami – the new weapon in cyberwafare

The flows are encrypted	Invisible to anti-DDoS appliances
Each flow looks like legitimate traffic	Go right through WAF protections
Utilize ultra-high RPS rate	Overwhelming web servers, backend databases, etc.
Generated from large Botnets	Rate limiting is ineffective
Use multiple evasion techniques	e.g., Randomization (of HTTP Method, Headers, Cookies, referrer, UA and more), IP (XFF) Spoofing, open headless browser to harvest application cookies, anonymous proxies,

It all started with the Russians...

- The Russian DDoS attack campaign started as soon as the war begun
- The attacks disrupted critical resources of the Ukrainian Government
- Radware was urgently called to protect Ukraine
- The attack campaign peaked at only 400Gbps, but employed relatively sophisticated attack vectors, including application layer DDoS attacks



On Wednesday, before Putin declared war and the bombing began, distributed denial-of-service (DDoS) attacks pummeled the websites of Ukraine's Defense Ministry and one of its major commercial banks, PrivatBank. Such attacks flood the victim's servers with connection requests, causing them to seize up as they would if millions of genuine people tried to log on at once.

Now they are **Everywhere**!

HTTP/s Flood attack campaigns in the last months on assets in:

- The US
- Canada
- Germany
- Poland
- The UK
- India
- Israel

...

- Australia
- Scandinavia



DDo

Attack on SAS: Application-layer DDoS Campaign (HTTP/s Floods)

Anonymous Sudan Forwarded from Anonymous Sudan



Infrastructure: The Danish education sector was brought down by the burning of the Quran

https://www.ku.dk/ | Københavns Universitet https://check-host.net/check-report/ec3b718k18e

https://www.dtu.dk/ | Danmarks Tekniske Universitet https://check-host.net/check-report/ec3b761k49f

https://ruc.dk/ | Roskilde Universitet https://check-host.net/check-report/ec3b5d7k34b

https://www.en.aau.dk/ | Aalborg Universitet (AAU) https://check-host.net/check-report/ec3b66akcc3

https://www.sdu.dk/ | Syddansk Universitet https://check-host.net/check-report/ec3b70ckf11

https://en.itu.dk/ | IT-Universitetet i København https://check-host.net/check-report/ec3b66dk381



#AnonymousSudan

si radware 5

HTTP/s Flood Attack Tools Available in the Wild

CC

- HTTP method can be random GET\POST\HEAD...
- Randomized HTTP headers values : accept*, referer, UA... from pre-defined list
- Custom static cookie
- Single random query args
- Hundreds-thousands of distinct requests
- Very few attack vectors
- Support HTTPs, HTTP Pipeline
- Use open Proxy SOCK4,5

11111	11111	///////////////////////////////////////
CCCCC/	CCCCC/	CC-attack /
CC/	cc/	/
CC/	CC/	Layer 7 1/
cc/////	cc/////	ddos tool /
CCCCC/	CCCCC/	11/

Saphyra

- HTTP method can be random GET\POST\HEAD...
- Random HTTP headers values - accept*, UA ...
- Randomized cookies (0,1-5)
- Query args are random (1-5)
- Random referer appearance and values
- Millions of distinct requests
- Very few attack vectors
- Support HTTPs, HTTP Pipeline

MHDDoS

- Randomization... (method, headers, UA, Cookies, empty requests)
- Hundreds-thousand of distinct requests
- Large number of attack vectors
- Approaches to bypass existing mitigation techniques, e.g. impersonate Google Analytics
- IP (X-FF) spoofing
- Support HTTPs, HTTP Pipeline
- Use open Proxy SOCK4,5

MHDDoS

Blood

- Large number of attack vectors
- Randomization... (method, headers, UA, Cookies, empty requests)
- Hundreds-thousand of distinct requests
- Approaches to bypass existing mitigation techniques, e.g. open headless browser to harvest application cookies, controlled cipher suite
- Support HTTPs, HTTP Pipeline
- Use open Proxy SOCK4,5





... and it continues with Hamas



- October-November 2023 Operation "Iron Swords" – DDoS Attacks
- More than 500 DDoS attacks targeting various sectors have been mitigated in the last 30 days
- The volume of attacks has reached up to 1,300,000 requests per second
- The targeted sectors include media, government services, critical infrastructure, and the financial services industry

- Anonymized list of selected customers in Israel:
 - Major mass media group
 - Major news outlet
 - Bank A: one of the largest banks
 - Bank B: one of the largest banks
 - Bank C: one of the largest banks
 - Public services company
 - State-owned transport service
 - Government services
 - State-owned critical infrastructure service
 - Major transport authority

TIME

H acking groups, including some tied to Russia, are attacking Israeli government and media websites, allying themselves with the Palestinian military group Hamas that launched a series of deadly strikes on the country over the weekend.

Source: Radware Attack Detection and Mitigation Data



State-owned public service: HTTPS Flood > 650K RPS

	Mitigation		
750k 9/10/2023 04:29:00 • Inbound: 631,509 RPS • Blocket: 533,700 RPS	Total Requests Received Dropped 34,138,222 20,801,953	Average Values Requests per Second 59,891 RPS	Maximum Values Requests per Second 631,509 RPS
250k 0 0 0 0 0 0 0 0 0 0 0 0 0	Latest Real Time Signature HTTP Method = GET AND Number of Query Arguments = 0, 1 AND Number of Cookies = 0, 1, 18, 19, 20, 21, 7 AND Number of Standard Headers = 4, 5, 6, 7 AND		
Voltation for the second seco	Header 'content*' does not exist AND Header 'origin' does not exist AND Header 'te' does not exist		

Government service: Network Flood > 135Gbps



Source: Radware Attack Detection and Mitigation Data

Most common attack vectors observed:

- HTTPS Flood
- Network Flood IPv4 UDP
- Network Flood IPv4 UDP-FRAG
- Network Flood IPv4 ICMP
- SYN Flood HTTP
- ICMP-BlackNurse-Attack
- BO-Apache-HTTPD-log-Cookie
- DDOS-APPLE-ARMS-AMP
- DDOS-Mirai-GENUDP-flood
- DDoS-UDP-MEMCACHED-AMP
- DOSS-chargen-reflected
- DOSS-DNS-Ref-L4-Above-3000
- DOSS-UDP-flood-80-Req
- DOSS-UDP-flood-80-Res
- DOSS-UDP-no-data
- TCP Anomalies
- TCP-FIN-ACK Flood
- DOSS-APPLE-ARMS-AMP
- DOSS-Mirai-GENUDP-flood
- DOSS-SSL-ClearText
- DNS Amplification
- DNS Random Sub-Domain

Observed attack size ranges:

- 1.2Gbps 135Gbps
- 9K RPS 1.5M RPS
- 4K QPS 16K QPS

Observed range of single attack duration times:

2 min – 1443 min



Gov't Sector – Israel Full mitigation and no impact



Banking Sector – Israel Full mitigation and no impact

Analytics Application Analytics N	twork Analytics Bot Manager Analy	rtics					
	Select Assets	Q Select Sites	Q 11	ne Zone: Local 🗸 Units: BPS 🗸	Aggregation Type: Max 🛩 🛛	Origin: Cloud In 🌱 Time Range: Not Selec	ted V 🕐 Last 1 Month
Sites Traffic			Export	Assets Traffic			Query Type: Assets 👻 👔
150,000 Mbps			St Reset Zoom	150,000 Mbps			3 Reset
125,000 Mbps			1	125,000 Mbps			
100,000 Mbps				100.000 Mbps			
75 000 Miles				75 010 Mines			
concorrentity				r a ann mugra			
50,000 Mbps				50,000 Mbps			
25,000 Mbps				25,000 Mbps			
				The American			-
Top Source Countries			Export	Top Services			C I
🚥 Canada 🛛 🚥 Russia							81535.
- Indonesia - Ukraine		and the second sec		UDP/443			70730.1
Colombia United States	/			HTTPS		_	50338.
- Thailand - Argentina				UDP/80	-		24427.3
- Philippines - Poland				HTTP			8444.8-
🛑 Vietnam 🛑 South Africa				UDP/53			7689.7
 Netherlands India 				TCP/31464			0910.00
							558.41

Attack Type:

• DDOS

Date/time:

- October 10th 2023
- 9:32 PM Local time

Additional Comments

• Major Spike in Level 4 traffic

 $\mathbf{\bullet}$

64

Banking Sector – Israel

Full mitigation and no impact



Attack Type:

DDOS

•

Traffic Bandwidth

Additional Comments

- Cloud Clean (green) stays level •
 - **Blocking and removal** lacksquare
- No impact on servers •

6%

News Organization Sector – Israel

Full mitigation and no impact

Assets	Applicat	tion Protectio	n Infra	ew Settin	ection	Health Checks	s Web [DDoS Protecti	20										
As:	set • Networ	rk			90														
I rattic									Time Z	lone: UTC 🗸	Units: Bits/s	s 🗸	Vectors: Clou	d 🗸	Visualization	n: Normal 🗸	0	ast month	۵
200 00ps																			Reset
150 Gbps																			
100 Gbps																			
50 Gbps																			
									\backslash										
0	22:00	7. Oct	02:00) 04:0	0	06:00	08:00	10:00	12:0	00 14:	00 10	5:00	18:00	20:00	22	2:00	8. Oct	02:00	0.
0	22:00 Cloud Incomi	7. Oct ing — Cl o	02:00 ud Clean 🗧	04:0	0 g — (06:00 CPE Clean 🗨	08:00 network fla	10:00 ood IPv4 TCP-SY	12:0 N netwo	00 14: ork flood IPv4 UDI	00 10 • — DOSS-t	5:00 cp-frag-oddne	18:00 255 <mark>—</mark> ne	20:00 twork flood I	22 Pv4 UDP-FRA	2:00 3 — netwo	8. Oct prk flood IPv4	02:00 I TCP-FRAG	0 • Secu
0 Events	22:00 Cloud Incomi Security	7. Oct ing — Clo Operati	02:00 ud Clean • onal	04:01	0 g — (06:00 CPE Clean 🗲	08:00 network fla	10:00 lood IPv4 TCP-SY	12:0 N netwo	00 14: ork flood IPv4 UDI	00 10 • — DOSS-t	5:00 cp-frag-oddne	18:00 255 <u>–</u> ne	20:00 twork flood l	2: IPv4 UDP-FRA(2:00 3 <u>—</u> netwo	8. Oct ark flood IPv4	02:00 I TCP-FRAG	0 • Secur
o Events	22:00 Cloud Incomi Security	7. Oct ing – Clo Operati	02:00 ud Clean d	04:01	0 g 🛑 (06:00 CPE Clean	08:00 network flo	10:00 ood IPv4 TCP-SY	12:0 N netwo	00 14: ork flood IPv4 UDI	00 1(• DOSS-t	5:00 cp-frag-oddne	18:00 255 👄 ne	20:00 twork flood l	2: IPv4 UDP-FRA(2:00 3 🕳 netwo	8. Oct ork flood IPv4	02:00 I TCP-FRAG	0 • Secu
0 Events	22:00 Cloud Incomi Security Start Date	7. Oct ing Clo Operati	02:00 ud Clean d	CPE Incoming	g 🕳 g	06:00 CPE Clean –	08:00 • network flo	10:00 ood IPv4 TCP-S1 Categ	12:0 N netwo	00 14: ork flood IPv4 UDI Source	00 1 (P DOSS-t Asset Nam	5:00 cp-frag-oddne e	18:00 ess ne	20:00 twork flood l Address	2: IPv4 UDP-FRA(Des	2:00 3 — netwo tination IP Addr	8. Oct ork flood IPv4	02:00 I TCP-FRAG Gro	0 • Secut
0 Events	22:00 Cloud Incomi Security Start Date October 1	7. Oct ing Clo Operati e 0 10, 2023, 13:22	02:00 ud Clean •	CPE Incoming Severity High	g 🌒 g	06:00 CPE Clean • :k Name occation Permane	08:00 network fic	10:00 ood IPv4 TCP-SV Categ GeoFi	12:0 N netwo	00 14: ork flood IPv4 UDI Source Cloud	00 10 DOSS-t Asset Nam	s:00 cp-frag-oddne e	18:00 ess ne Source IP / Multiple	20:00 twork flood l Address	22 Pv4 UDP-FRA(Des Mul	200 3 — netwo tination IP Addr tiple	8. Oct ork flood IPv4 ress	02:00 I TCP-FRAG Gro Secu	0 • Secur up rrity
e Events	22:00 Cloud Incomi Security Start Date October 1 October 1	7. Oct ing Cla Operati e C 10, 2023, 13:22 10, 2023, 6:51	02:00 ud Clean d	CPE Incoming Severity High	0 g - 0 Attac Geolo netwo	06:00 CPE Clean k Name socation Permane socation Permane	08:00 network flo ent DP-FRAG	10:00 ood IPv4 TCP-SV Categ GeoFi Behav	12.0 N network ory red tioral DoS	00 14: ork flood IPv4 UDI Source Cloud Cloud	00 1(e	18:00 255 — ne Source IP / Multiple	20:00 twork flood l Address	22 IPv4 UDP-FRAG Des Mul	2:00 3 🌧 netwo tination IP Addr tiple	8. Oct ork flood IPv4	02:00 ITCP-FRAG Gro Secu	0 • Secur up rrity
events	22:00 Cloud Incomi Security Start Date October 1 October 1	7. Oct ing Clo Operati e 2 10, 2023, 13:22	02:00 ud Clean • onal	CPE Incoming Severity High High	0 g d Attac Geole	06:00 CPE Clean	08:00 network flo ent DP-FRAG Attac	10:00 ood IPv4 TCP-S1 Categ GeoFi Behav ock ID	12:0 N network	00 14: ork flood IPv4 UDI Source Cloud Cloud Sour	Asset Nam	s:00 cp-frag-oddne e	18:00 ess — ne Source IP / Multiple	20:00 twork flood l Address Real Time 1	22 Pv4 UDP-FRA(Des Mul Signature	2:00 3 — netwo tination IP Addr tiple	8. Oct brik flood IPv4 ress	02:00 I TCP-FRAG Gro Secu	0- Secur up rrity
Events	22:00 Cloud Incomi Security Start Date October 1 October 1	7. Oct ing Clo Operati 10, 2023, 13:22 10, 2023, 6:51 10/10/2023	02-00 ud Clean onal	CPE Incoming CPE Incoming Severity High High Attack Sizes Attack Peak BV	0 g — 0 Attac Geolo netwo	06:00 CPE Clean k Name ocation Permane ork flood IPv4 UE	08:00 network flo ent DP-FRAG Attac Radw	10:00 cood IPv4 TCP-S1 Categ GeoFr Behav ck ID vare ID: 90	12:1 N network	00 14: ork flood IPv4 UDI Source Cloud Cloud Sour Proto	Asset Nam	s:00 cp-frag-oddne e UDP	18:00 ess — ne Source IP / Multiple	20:00 twork flood I Address	22 IPv4 UDP-FRAC Des Mul Signature	2:00 3 — netwo tination IP Addr tiple	8. Oct Dark flood IPv4	02:00 ITCP-FRAG Gro Secu	0- Secur up urity
0 Events	22:00 Cloud Incomi Security Start Date October 1 October 1 October 1 Time: Time: Time: Cix Name:	7. Oct ing Clo Operati 0. 2023, 13-22 10. 2023, 6:51 10/10/2023 network flor	02:00 ud Clean • onal • 06:51 07:09 d IPv4	CPE Incoming CPE Incoming Severity High High Attack Sizes Attack Peak BV Attack Peak Pea	0 g Attac Geolc netwo N: 7 2S: 1 1 2S: 1	06:00 CPE Clean k Name ocation Permane ork flood IPv4 UE 71.4 Mbps 11018 pps 28101509 kb	08:00 network fic ent DP-FRAG Attac Polici	10:00 cood IPv4 TCP-S1 Categ GeoFi Behav vare ID: 90 ck ID: 285 vare: 0 200	12:0 N netwo ory red ioral DoS 05278-1686830 UNT 192 115	00 14: ork flood IPv4 UDI Source Cloud Cloud Cloud Sour Proto Sour : 80 Sour	Asset Nam	5:00 cp-frag-oddne e UDP 115.164.50	18:00 ess ne Source IP / Multiple	20:00 twork flood I Address Real Time S	22 IPv4 UDP-FRAG Des Mult Signature ent Offset:	2:00 3 — netwo tination IP Addr tiple	8. Oct Drk flood IPv4	02:00 ITCP-FRAG Gro Secu	0- Secur up rity
0 Events	22:00 Cloud Incomi Security Start Data October 1 October 1 October 1 Time: ck Name:	7. Oct ing Clo Operati 0, 2023, 13:22 10, 2023, 6:51 10/10/2023 network floc UDP-FRAG	02:00 onal 06:51 07:09 d IPv4	CPE Incoming CPE Incoming Severity High High Attack Sizes Attack Peak BW Attack Peak BW Attack Total Vo Attack Total Vo	9 • • • • • • • • • • • • • • • • • • •	06:00 CPE Clean sk Name ocation Permane ork flood IPv4 UE 71.4 Mbps 11018 pps 28101 509 kb 4443440	08:00 network flo ent DP-FRAG Attac Radw Attac Policio Source	10:00 cod IPv4 TCP-SN Categ GeoFi Behav ork ID vark ID: 286 yl Name: 500 ce: Clo	12.0 N network netw	00 14: ork flood IPv4 UDI Source Cloud Cloud Cloud Cloud Sour Proto Sourc as0 Sour Targe	Asset Nam	e UDP 115.164.50 Multiple	18:00 sss ne Source IP / Multiple	20:00 twork flood I Address Real Time S OR Fragme 185 OR	22 IPv4 UDP-FRAG	2:00 3 — netwo tination IP Addr tiple	8. Oct ork flood IPv4	02:00 ITCP-FRAG Gro Secu	0- Secur up rity

Attack Type:

• WebDDOS

Date/time:

- October 10th 2023
- 6:51AM Local time

Additional Comments

• 150Gbit/s

Service Sector – Israel

Full mitigation and no impact



Attack Type:

WebDDOS •

Date/time:

(10 per page → |< < (1 → →|

- October 8th 2023
- 8:27 PM Local time

Additional Comments

- There were two back-to-back • attacks.
- Both attacks mitigate with some • leakage since no baseline
- Attack mode WebDDOS

Transport Sector – Israel

Full mitigation and no impact

Security Events	Application Protection	Infrastructure Protection											
WAF DDoS	Bot We	b DDoS Protection											
Search	Q Ŧ										Quick Rang	ge: Last 1 Month 🖂	0
Diversion	Action	Attack ID	Time 🗘		Application Name		Host	Account Name	Source	Attack Vector	Severity	Status	
•	Blocked	c9b387f3-e06b-4770-8	08 Oct 2023 22:51:10						Multiple	HTTPS Attack	Critical	Terminated	
•	Blocked	c9b387f3-e06b-4770-8	30 Sep 2023 21:08:30						Multiple	HTTPS Attack	Critical	Terminated	
Summary		Detection						Mitigation					
Attack ID: Application:	c9b387f3-e06b-4770-8 new web site for workers	Requests Rate Attack Threshold Attack Threshold Attack Start Value 166 RPS 3,519 RPS	400k					Total Requests Received 16,996,933	Dropped 16,059,933	Average Values Requests per Second 9,939 RPS	Maximum V Requests pe 286,962 R	/alues r Second RPS	
Account: Security Module:	Web DDoS Protection		<u>∛</u> 200k					Latest Real Tim	e Signature				
Attack Vector:	HTTPS Attack		0					Number of Path El	ements = 0 AND				
Start Time:	30 Sep 2023 21:08:30 PM		_	21:10:00	21:20:00	21:30:00	shold	Number of Query A	Arguments = 0 AND				
End Time:	30 Sep 2023 21:36:50 PM			- inconto	- clean	- Alleys Inf	earrord	Number of Standar	rd Headers = 2 AND				
Protection Duration:	28 minutes 20 second							Number of Non-Sta	andard Headers = 0 AND				
Protection Status:	Terminated	Application Behavior () Attack Threshold Attack Start Value	• ¹⁰		٨	Δ		Header 'accept*' di	pes not exist AND				
Source:	Multiple	5 6.2	a 5 5		A		~	Header 'connection Header 'origin' doe	n aoes not exist AND s not exist AND				
Action:	Blocked		- La Carteria	7 -				Header 'referer' do	es not exist AND				
			< _ b					Header ison X door	not exist AND				

Attack Type:

WebDDOS

Date/time:

- September 30th 2023
- 9:08 PM Local time

Additional Comments

- WebDDOS pkgs were previous, but need RPS and WebDDOS to trigger
- 300,000 RPS
- Almost no leakage
- No Impact on customer

How Radware is protecting Israel?



Behavioral L7 baselining



Behavioral L7 baselining



 $K < 1 \rightarrow H$ 8

10 per page

۵

(A)

Behavioral TLS Fingerprinting



•

Q



Thank You!