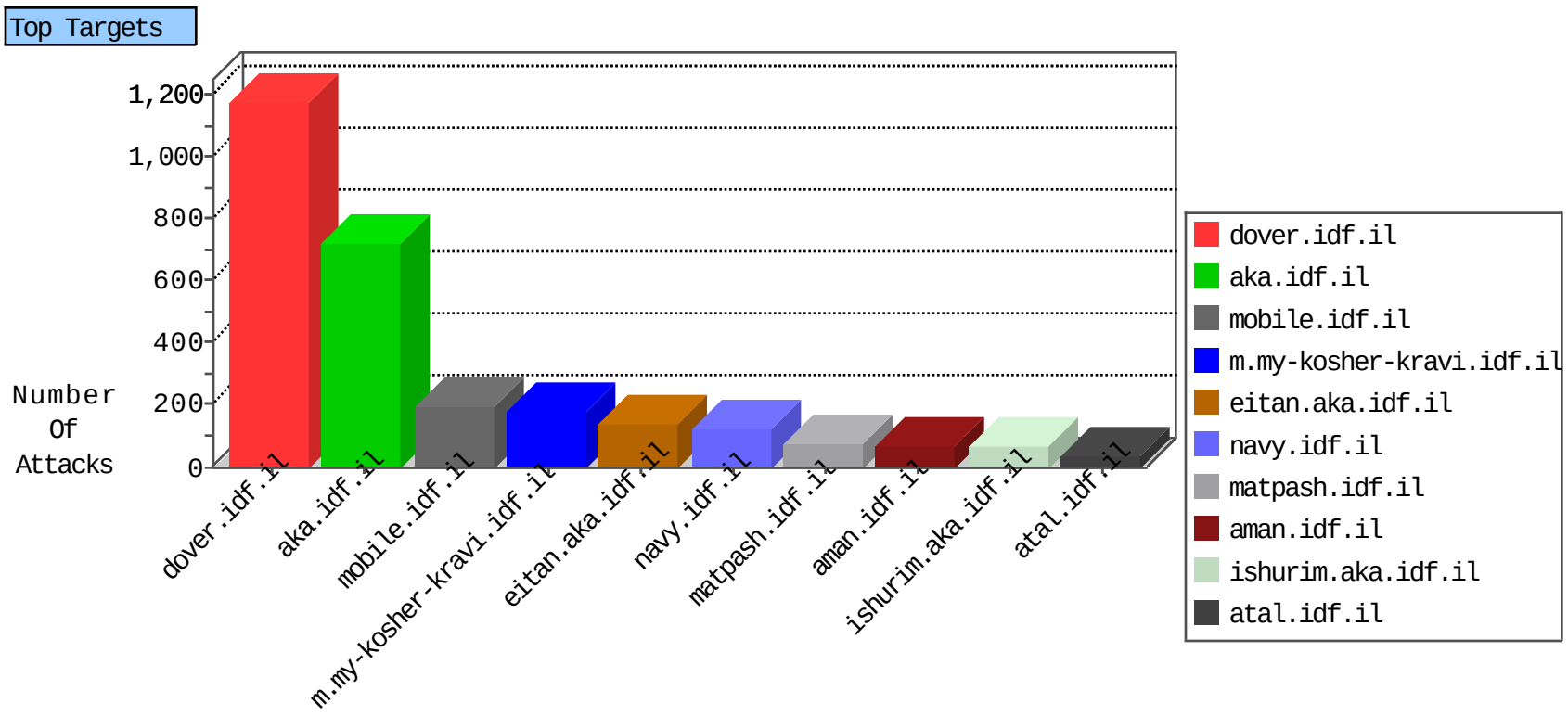
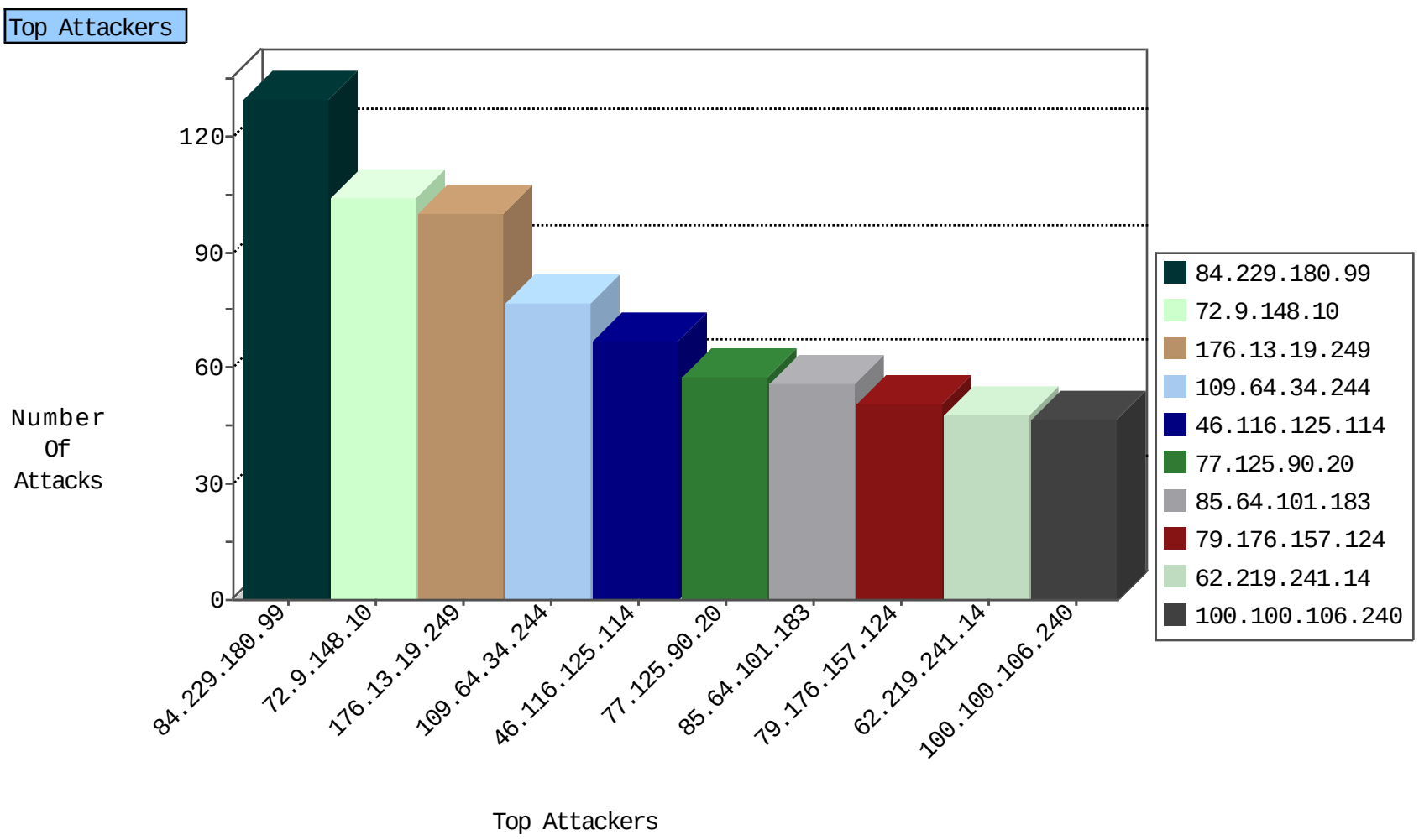
10-20-2015-21:04:01 to 10-20-2015-22:04:01

IDF Under Attack
Daily Report





10-20-2015-21:04:01 to 10-20-2015-22:04:01

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood full table	drop	123
2.54.160.152	Israel	147.237.72.166	aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	90
5.156.41.242	Romania	147.237.77.216	dover.idf.il	Web-etc/passwd-Dir-Traversal	dest-reset	41
93.172.198.250	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	35
98.25.49.235	United States	147.237.77.216	dover.idf.il	SYN Flood full table	drop	25
87.69.62.140	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	18
67.64.129.33	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	14
62.219.241.14	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	10
87.68.18.249	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	10
79.177.3.48	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	10
46.19.86.208	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	8
2.54.152.185	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	7
85.250.19.124	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
79.176.193.48	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
79.180.59.54	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
79.176.111.117	Israel	147.237.72.156	aman.idf.il	Block_Udp_All_Nets	drop	6
123.176.5.96	Maldives	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
79.176.120.74	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
4.15.72.218	United States	147.237.77.216	dover.idf.il	SYN Flood full table	drop	6
79.182.208.135	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
95.86.78.127	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
2.54.181.211	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
176.13.9.58	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
46.120.161.112	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
176.13.12.144	Israel	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	5
79.180.132.34	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	5
87.69.17.251	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
84.196.179.39	Belgium	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
109.64.139.179	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
5.28.156.54	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
46.19.85.185	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
84.111.110.68	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
46.19.86.101	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
4.15.72.218	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
176.13.12.144	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	4
176.13.2.234	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	3
84.110.81.222	Israel	147.237.77.233	atal.idf.il	Block_Udp_All_Nets	drop	3
95.86.122.179	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
62.219.254.22	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
79.176.34.72	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
46.121.120.58	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
79.176.120.74	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
62.219.254.22	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
79.180.36.164	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	3
46.19.86.208	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
84.228.185.93	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
93.173.248.207	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
77.125.155.206	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
89.138.235.185	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2

10-20-2015-21:04:01 to 10-20-2015-22:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
84.228.176.159	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	3

10-20-2015-21:04:01 to 10-20-2015-22:04:01

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	7
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
59.46.193.114	147.237.0.200	China	m4u.idf.il	GPL SCAN nmap TCP	2
218.24.171.223	147.237.0.200	China	m4u.idf.il	GPL SCAN nmap TCP	2
79.143.180.44	147.237.77.226	Germany	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 1024	1
46.116.219.214	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
54.72.81.157	147.237.76.200	Ireland	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
5.39.222.253	147.237.76.30	Netherlands	himush.idf.il	ET SCAN NMAP -sS window 1024	1
54.72.81.157	147.237.76.198	Ireland	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
54.72.81.157	147.237.76.176	Ireland	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
54.72.81.157	147.237.76.86	Ireland	navy.idf.il	ET SCAN Potential SSH Scan	1
54.72.81.157	147.237.76.42	Ireland	refuah.idf.il	ET SCAN Potential SSH Scan	1
108.61.220.143	147.237.0.17	United States	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 4096	1
54.72.81.157	147.237.76.34	Ireland	yohalan.idf.il	ET SCAN Potential SSH Scan	1
79.143.180.44	147.237.77.227	Germany	e.hamaz.idf.il	ET SCAN NMAP -sS window 1024	1
54.72.81.157	147.237.76.30	Ireland	himush.idf.il	ET SCAN Potential SSH Scan	1
78.188.21.238	147.237.76.42	Turkey	refuah.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
43.229.53.89	147.237.0.35	Japan	akaws.idf.il	ET SCAN Potential SSH Scan	1
54.72.81.157	147.237.76.202	Ireland	e.halag.idf.il	ET SCAN Potential SSH Scan	1
5.39.222.253	147.237.76.38	Netherlands	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
54.72.81.157	147.237.76.199	Ireland	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
2.97.109.163	147.237.76.39	United Kingdom	mobile.meitav.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
54.72.81.157	147.237.76.196	Ireland	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
54.72.81.157	147.237.76.147	Ireland	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
196.221.146.214	147.237.8.27	Egypt	e.madim.atal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
54.72.81.157	147.237.76.44	Ireland	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
165.228.233.142	147.237.76.202	Australia	e.halag.idf.il	ET SCAN NMAP -sS window 4096	1
54.72.81.157	147.237.76.39	Ireland	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1
108.61.220.143	147.237.0.17	United States	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
54.72.81.157	147.237.76.31	Ireland	nakchal.idf.il	ET SCAN Potential SSH Scan	1

10-20-2015-21:04:01 to 10-20-2015-22:04:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
77.125.90.20	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	58
100.100.106.240		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	47
79.176.218.101	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	42
92.241.35.218	Jordan	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	39
100.100.82.105		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	38
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
62.219.241.14	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	30
85.64.101.183	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	28
109.65.16.55	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	27
2.54.186.127	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	25
46.19.85.164	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	22
79.176.206.131	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
54.224.21.23	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
37.142.115.206	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	21
170.235.205.42	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
66.249.67.65	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	20
46.19.85.44	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	17
5.22.129.154	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
4.15.72.218	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
185.32.179.221	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
100.100.0.213		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	16
185.29.96.100	Italy	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	16
37.142.156.250	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	16
109.160.134.147	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
79.180.36.164	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
100.100.35.122		147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	12
79.180.132.34	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
79.176.157.124	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
149.78.30.249	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	11
79.182.208.135	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
46.19.86.93	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
207.191.13.254	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
131.253.25.250	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
212.199.121.158	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
109.65.147.223	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.116.109.10	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
93.172.198.250	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
87.68.18.249	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
79.180.100.137	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
66.249.67.53	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
37.142.125.247	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	8
109.66.172.76	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	8
149.78.164.206	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
185.29.96.100	Italy	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
100.100.51.186		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	7
100.100.88.182		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	7
46.116.172.163	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	7

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
72.9.148.10	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/994-8613-he/navy.aspx.aspx	Block	104
176.13.19.249	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	100
84.229.180.99	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1362	Block	78
109.64.34.244	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	77
46.116.125.114	Israel	147.237.76.200	eitan.aka.idf.il	Too Many of the Same Response Code (404) in Session from 46.116.125.114	Block	65
84.229.180.99	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 84.229.180.99	Block	52
79.176.157.124	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	39
213.57.173.169	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	39
85.64.101.183	Israel	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to www.eitan.aka.idf.il/shared/ajax/lightboxmediagallery.aspx	Block	26
2.54.189.93	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	13
176.13.8.227	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	13
85.65.170.93	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	13
79.183.56.37	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	13
199.16.156.125	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/4/size220x0/17374.jpg	Block	13
46.116.172.163	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/sip_storage/files/8/1668.doc	Block	13
157.55.39.66	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to 147.237.76.86/robots.txt	Block	13
84.228.73.119	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1135-he/atal.aspx	Block	13
5.28.186.144	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/6/4616.jpg	Block	13
87.68.30.65	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/https:/www.aka.idf.il/	Block	13
79.183.226.249	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/himush/site/he/himush.asp	Block	13
207.46.13.187	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	13
66.249.64.161	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/templates/shared/usercontrols/headerupper/	Block	13
157.55.39.211	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/console/core/doc_mgr/general.aspx	Block	13
79.177.202.158	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	13
17.138.54.139	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/apple-app-site-association	Block	13
176.13.20.69	Israel	147.237.0.19	madim.atal.idf.il	Cookie Tampering on cookie Login: Expected ********** ********** ********** *******, Observed ********** ********** ********** *	None	13
87.69.198.63	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/https:/www.aka.idf.il/	Block	13
80.246.139.145	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	13
207.46.13.187	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/console/core/doc_mgr/null	Block	13
66.249.67.59	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.67.59	Block	13
157.55.39.212	United States	147.237.72.166	aka.idf.il	Unknown Parameter 4f9c0c80 in www.aka.idf.il/main/home/default.aspx	None	13
79.179.55.208	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	13
17.138.60.205	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/apple-app-site-association	Block	13
180.97.106.162	China	147.237.76.30	himush.idf.il	Unauthorized URL Access to 147.237.76.30/	Block	13
80.246.140.94	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/sachar/index	Block	13
67.19.79.218	United States	147.237.72.167	ishurim.aka.idf.il	Unauthorized URL Access to /robots.txt	Block	13
2.54.61.165	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	13
173.252.88.87	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to 147.237.0.34/sip_storage/files/4/size220x0/1744.jpg	Block	13
79.179.173.148	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/https:/www.aka.idf.il/	Block	13
199.16.156.125	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 199.16.156.125	Block	13
149.88.76.76	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/https:/www.aka.idf.il/	Block	13
84.110.81.222	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1135-he/atal.aspx	Block	13