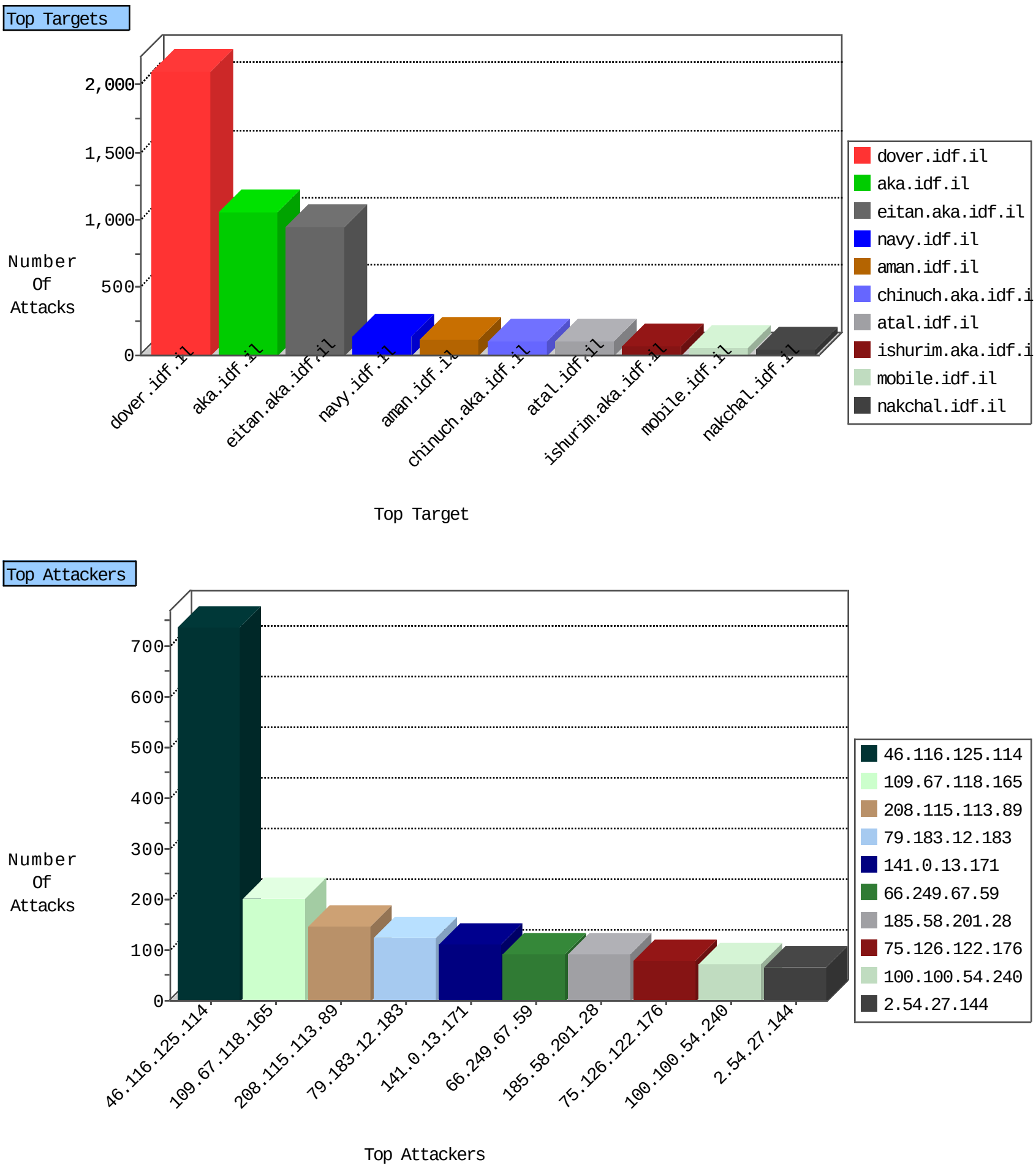
10-19-2015-18:04:00 to 10-19-2015-19:04:00

IDF Under Attack
Daily Report



10-19-2015-18:04:00 to 10-19-2015-19:04:00

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
212.25.84.200	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	433
81.218.241.25	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	136
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood full table	drop	26
66.249.81.206	United States	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	24
185.32.179.34	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-SSL-renegotiation-Cli	dest-reset	22
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	9
82.102.169.113	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	8
109.64.10.94	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	8
176.13.5.87	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	5
85.250.0.226	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
2.54.58.15	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
37.26.149.160	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	5
93.173.246.207	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	4
2.54.144.159	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
62.219.254.22	Israel	147.237.72.167	ishurim.aka.idf.il	Block_Udp_All_Nets	drop	3
79.181.148.211	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
46.19.86.77	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	3
212.179.21.194	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
14.125.197.160	China	147.237.0.200	m4u.idf.il	Frk_Under_Attack_Con_Tcp	drop	2
176.13.6.145	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
2.54.144.159	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
85.250.156.220	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
46.19.85.89	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	2
93.174.93.146	Netherlands	147.237.76.34	yohalan.idf.il	Invalid TCP Flags	drop	1
2.54.6.38	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
93.174.93.146	Netherlands	147.237.76.34	yohalan.idf.il	Invalid TCP Flags	drop	1
2.54.6.38	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
141.0.13.171	Norway	147.237.77.216	dover.idf.il	SYN Flood full table	drop	1
87.69.38.156	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
71.6.167.142	United States	147.237.76.196	e.sviva.idf.il	Block_Udp_All_Nets	drop	1
46.19.85.155	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	1
2.54.144.159	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
93.174.93.146	Netherlands	147.237.76.202	e.halag.idf.il	Invalid TCP Flags	drop	1
31.168.171.81	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	1
141.0.13.171	Norway	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
87.69.82.108	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	1
93.174.93.146	Netherlands	147.237.77.179	e.mazi.idf.il	Invalid TCP Flags	drop	1
85.250.0.226	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
66.249.67.53	United States	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
2.54.144.159	Israel	147.237.77.216	dover.idf.il	SYN Flood delete reset	drop	1
142.54.174.68	United States	147.237.77.234	halag.idf.il	block-sp-traf1	drop	1
46.19.86.77	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
10.0.0.10		147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
2.54.6.38	Israel	147.237.77.216	dover.idf.il	SYN Flood full table	drop	1

10-19-2015-18:04:00 to 10-19-2015-19:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
84.94.193.188	Israel	147.237.72.166	aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
95.86.67.134	Israel	147.237.77.226	www.chamatz.aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2

10-19-2015-18:04:00 to 10-19-2015-19:04:00

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
77.125.96.178	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	3
132.72.138.1	147.237.77.216	Israel	dover.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	2
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	2
192.118.30.102	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
54.152.31.52	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sS window 1024	1
190.124.35.115	147.237.0.200	Nicaragua	m4u.idf.il	ET SCAN NMAP -sS window 3072	1
46.117.70.76	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
188.68.224.151	147.237.72.14	Poland	dover.idf.il(old	ET SCAN NMAP -sS window 2048	1
37.142.101.119	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
176.13.8.105	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
5.230.152.138	147.237.8.45	Germany	e.eitan.idf.il	ET SCAN NMAP -sS window 4096	1
5.230.152.138	147.237.8.45	Germany	e.eitan.idf.il	ET SCAN NMAP -f -sS	1
84.228.192.210	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
80.246.130.200	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
210.61.150.154	147.237.76.42	Taiwan	refuah.idf.il	ET SCAN NMAP -sS window 2048	1
77.126.41.141	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	1
70.210.33.22	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
190.124.35.115	147.237.0.200	Nicaragua	m4u.idf.il	ET SCAN NMAP -sS window 4096	1
46.117.81.38	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
188.68.224.151	147.237.72.14	Poland	dover.idf.il(old	ET SCAN NMAP -sS window 4096	1
188.68.224.151	147.237.72.14	Poland	dover.idf.il(old	ET SCAN NMAP -f -sS	1
37.26.147.178	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
176.12.146.38	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
5.230.152.138	147.237.8.45	Germany	e.eitan.idf.il	ET SCAN NMAP -sS window 2048	1
95.86.116.228	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
84.109.176.196	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
218.108.132.58	147.237.77.235	China	sviva.idf.il	ET SCAN NMAP -sS window 1024	1
79.179.203.158	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
210.61.150.154	147.237.76.42	Taiwan	refuah.idf.il	ET SCAN NMAP -f -sS	1

10-19-2015-18:04:00 to 10-19-2015-19:04:00

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
109.67.118.165	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	201
208.115.113.89	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	146
79.183.12.183	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	124
141.0.13.171	Norway	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	111
100.100.54.240		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	73
96.47.226.20	Anonymous Proxy	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	59
185.58.201.28	Lebanon	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	48
41.89.10.241	Kenya	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	47
37.142.180.3	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	40
66.249.67.59	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	38
37.142.204.179	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	37
66.102.7.233	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
79.18.240.254	Italy	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	35
46.19.85.129	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	33
37.140.188.112	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
100.100.12.160		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	29
37.142.250.172	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	27
176.106.226.145	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	27
100.100.84.11		147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	26
119.76.68.250	Thailand	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
37.142.237.154	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	24
84.95.86.182	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	23
76.108.60.229	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
81.218.144.226	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	21
199.203.151.170	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
2.54.163.208	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	19
46.120.104.94	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
91.79.154.23	Russian Federation	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	17
66.249.67.53	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	16
156.3.109.1	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
85.250.11.44	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
213.57.140.161	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	15
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
109.66.21.47	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
185.13.195.184	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
66.249.67.65	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	14
185.58.201.28	Lebanon	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	monitor	14
64.233.173.161	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	14
85.65.177.195	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
188.120.148.183	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	13
37.142.197.138	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	13
2.100.191.44	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	13
100.100.17.183		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	13
100.100.87.247		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
100.100.119.140		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	12
79.183.186.48	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
213.244.65.138	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
80.246.133.245	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	12
84.94.223.15	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12

10-19-2015-18:04:00 to 10-19-2015-19:04:00

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
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	728
75.126.122.176	United States	147.237.76.86	navy.idf.il	Distributed Unauthorized URL Access on www.navy.idf.il/994-8613-he/navy.aspx.aspx	Block	78
2.54.27.144	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	65
66.249.93.200	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/arr	Block	52
72.9.148.10	United States	147.237.76.86	navy.idf.il	Distributed Unauthorized URL Access on www.navy.idf.il/994-8613-he/navy.aspx.aspx	Block	52
66.249.67.59	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.67.59	Block	39
54.244.22.103	United States	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	39
46.19.85.62	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	39
66.249.67.53	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atal1/izkor/view_imgtop.asp	Block	26
217.194.198.145	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	26
37.26.148.165	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/himush/site/he/himush.asp	Block	26
85.65.177.195	Israel	147.237.76.31	nakchal.idf.il	Parameter Type Violation search in www.nakhal.idf.il/1120-he/nakhal.aspx	Block	26
95.86.67.134	Israel	147.237.77.226	www.chamatz.aka.idf.il	Multiple Unauthorized URL Access from 95.86.67.134	Block	26
84.111.54.184	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	26
66.249.67.71	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/robots.txt	Block	13
176.13.16.186	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1134-he/atal.aspx	Block	13
89.138.72.65	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	13
46.19.86.28	Israel	147.237.0.16	my-kosher-kravi.idf.il	Distributed Unauthorized URL Access on www.my-kosher-kravi.idf.il/	Block	13
79.177.42.45	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on aka.idf.il/https:/aka.idf.il/	Block	13
212.25.102.57	Israel	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/	Block	13
66.249.81.141	Israel	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/1746-he/lifestyle.aspx	Block	13
109.65.56.65	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on aka.idf.il/https:/aka.idf.il/	Block	13
31.168.101.163	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1250-he/atal.aspx	Block	13
84.228.45.182	Israel	147.237.72.166	aka.idf.il	Unknown Parameter catld in www.aka.idf.il/main/giyus/general.aspx	None	13
66.249.67.242	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/robots.txt	Block	13
192.117.12.65	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1134-he/atal.aspx	Block	13
89.139.44.79	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	13
84.94.89.205	Israel	147.237.76.147	chinuch.aka.idf.il	PHP Attempt	Block	13
66.249.81.206	Israel	147.237.72.166	aka.idf.il	Distributed URL is Above Root Directory	Block	13
66.249.67.59	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/robots.txt	Block	13
109.65.56.65	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/https:/www.aka.idf.il/	Block	13
193.201.224.32	Ukraine	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	13
66.249.69.43	Israel	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	13
46.121.62.37	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	13
5.22.129.133	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/www.tikshuv.idf.il	Block	13
84.94.89.205	Israel	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/xmlrpc.php	Block	13
66.249.93.196	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/arr	Block	13
149.78.22.37	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	13
85.65.177.195	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakhal.idf.il/images/shared/err_page.png	Block	13
37.142.64.50	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/markiveysachar.aspx	None	13
77.237.154.221	Czech Republic	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to /	Block	13
207.46.13.101	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/	Block	13
66.249.69.51	Israel	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	13
95.86.67.134	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/sip_storage/files/8/	Block	13
5.29.224.158	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on aka.idf.il/https:/aka.idf.il/	Block	13
66.249.93.196	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/arr	Block	13
66.249.67.65	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.67.65	Block	13
149.78.80.3	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	13
87.68.147.219	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/text.css	Block	13
79.176.121.254	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	13

10-19-2015-18:04:00 to 10-19-2015-19:04:00