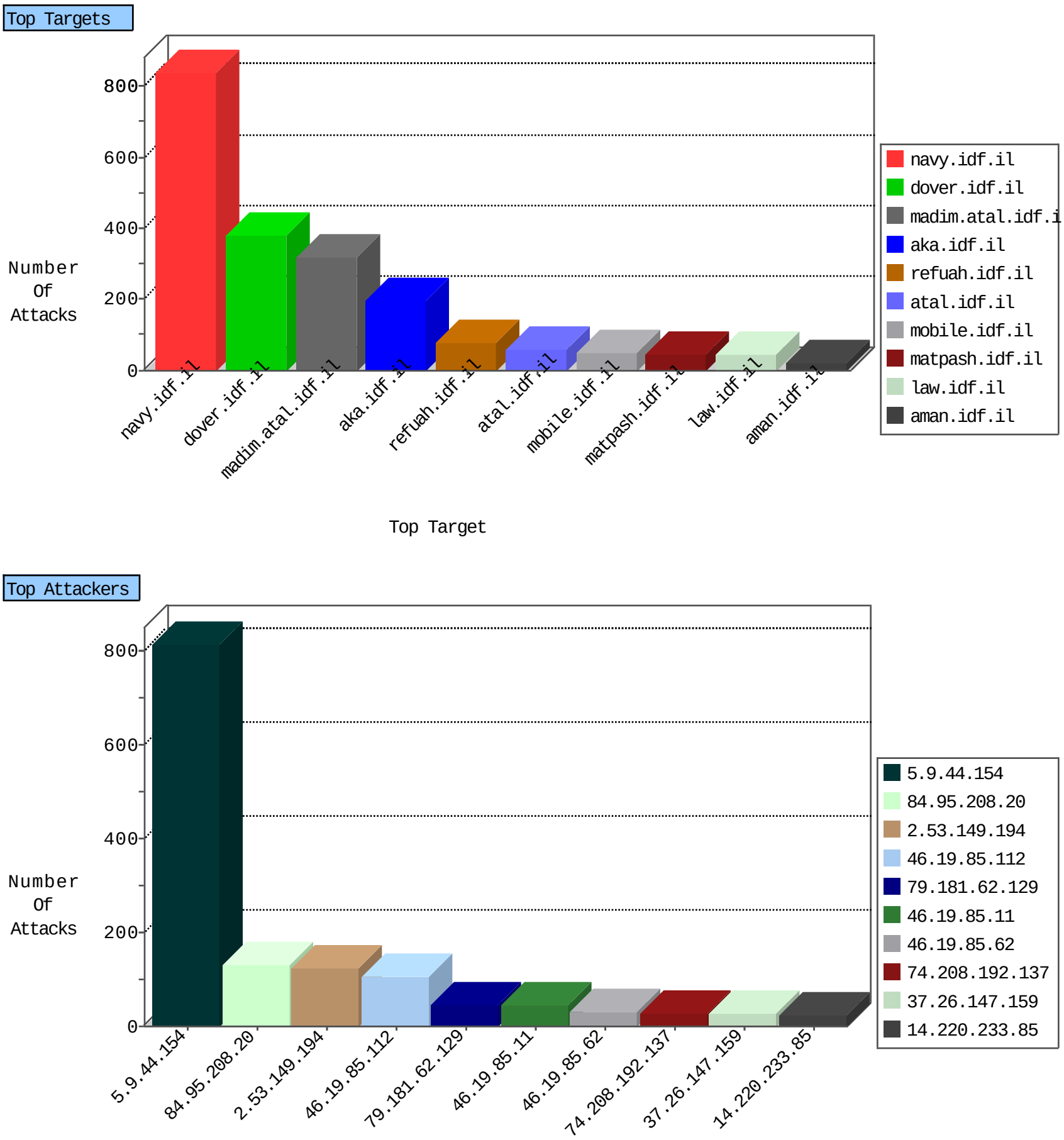
09-22-2016-12:04:03 to 09-22-2016-13:04:03

IDF Under Attack Daily Report



09-22-2016-12:04:03 to 09-22-2016-13:04:03

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
84.95.45.163	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	6
2.53.58.61	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	6
66.249.93.83	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	6
50.87.144.145	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	5
82.145.211.222	Europe	147.237.76.31	nakchal.idf.il	Black List	drop	5
80.230.221.41	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
80.246.133.228	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
85.65.144.3	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
123.59.59.52	China	147.237.76.31	nakchal.idf.il	block-sp-traf1	forward	2
63.141.231.195	United States	147.237.76.147	chinuch.aka.idf.il	block-sp-traf1	forward	2
63.141.242.195	United States	147.237.76.39	mobile.meitav.idf.il	block-sp-traf1	forward	2
173.208.197.204	United States	147.237.76.200	eitan.aka.idf.il	block-sp-traf1	forward	2
69.30.226.221	United States	147.237.77.234	halag.idf.il	block-sp-traf1	forward	1
204.12.220.84	United States	147.237.0.17	m.my-kosher-kravi.idf.il	block-sp-traf1	forward	1
69.30.193.254	United States	147.237.77.233	atal.idf.il	block-sp-traf1	forward	1
142.54.174.83	United States	147.237.77.235	sviva.idf.il	block-sp-traf1	forward	1
63.141.231.195	United States	147.237.77.170	maarachot.idf.il	block-sp-traf1	forward	1
84.95.208.20	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1
69.30.226.220	United States	147.237.72.156	aman.idf.il	block-sp-traf1	forward	1
173.208.197.203	United States	147.237.72.167	ishurim.aka.idf.il	block-sp-traf1	forward	1
69.30.226.221	United States	147.237.72.166	aka.idf.il	block-sp-traf1	forward	1

09-22-2016-12:04:03 to 09-22-2016-13:04:03

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
74.208.192.137	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
162.210.196.100	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2
162.210.196.130	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2
199.58.86.206	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	2
51.255.36.85	France	147.237.77.74	law.idf.il	C1000074: HTTP: majestic bot	Permit	2
240.0.10.13		147.237.77.216	dover.idf.il	0055: IP: Source IP Address Spoofed (Reserved for Testing)	Block	1

09-22-2016-12:04:03 to 09-22-2016-13:04:03

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
74.208.192.137	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	22
66.249.93.67	147.237.77.233	Europe	atal.idf.il	ET SCAN NMAP -sA (2)	22
193.47.165.251	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	2
213.151.48.138	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
94.102.56.151	147.237.77.61	Netherlands	e.cogat.idf.il	ET SCAN Potential SSH Scan	1
195.70.44.28	147.237.0.17	Hungary	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
94.102.56.151	147.237.76.199	Netherlands	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
62.180.25.66	147.237.77.216	Germany	dover.idf.il	portscan: TCP Distributed Portscan	1
94.102.56.151	147.237.76.39	Netherlands	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1
46.19.86.101	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
183.60.48.25	147.237.0.35	China	akaws.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
94.102.56.151	147.237.72.14	Netherlands	dover.idf.il(old)	ET SCAN Potential SSH Scan	1
14.163.66.112	147.237.77.243	Vietnam	mobile.idf.il	ET SCAN NMAP -f -sS	1
183.60.48.25	147.237.0.17	China	m.my-kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
84.229.25.42	147.237.72.166	Israel	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
2.55.4.224	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
132.64.27.173	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
84.108.177.115	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
109.253.197.207	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.181.79.20	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
95.86.110.252	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
77.126.93.145	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
94.102.56.151	147.237.77.212	Netherlands	e.dover.idf.il	ET SCAN Potential SSH Scan	1
211.149.201.80	147.237.77.176	China	matpash.idf.il	ET SCAN NMAP -sS window 1024	1
68.194.83.205	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
94.102.56.151	147.237.76.201	Netherlands	e.atal.idf.il	ET SCAN Potential SSH Scan	1
64.137.168.128	147.237.76.44	Canada	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
193.124.58.72	147.237.72.166	Russian Federation	aka.idf.il	portscan: TCP Distributed Portscan	1
94.102.56.151	147.237.76.44	Netherlands	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
46.183.223.228	147.237.0.19	Latvia	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
183.60.48.25	147.237.76.147	China	chinuch.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
94.102.56.151	147.237.72.217	Netherlands	e.idf.il	ET SCAN Potential SSH Scan	1
14.163.66.112	147.237.77.243	Vietnam	mobile.idf.il	ET SCAN NMAP -sS window 2048	1
183.60.48.25	147.237.0.34	China	tikshuv.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
94.102.56.151	147.237.0.33	Netherlands	idf.il	ET SCAN NMAP -sS window 1024	1
2.55.177.74	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
183.60.48.25	147.237.0.15	China	kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
84.108.206.116	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
113.240.250.154	147.237.77.233	China	atal.idf.il	ET SCAN NMAP -sS window 1024	1
82.102.145.121	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
100.13.130.4	147.237.76.196	United States	e.sviva.idf.il	ET SCAN NMAP -sS window 1024	1
79.178.157.213	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
94.102.56.151	147.237.77.216	Netherlands	dover.idf.il	ET SCAN Potential SSH Scan	1

09-22-2016-12:04:03 to 09-22-2016-13:04:03

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
5.9.44.154	Germany	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	816
141.0.12.34	Norway	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	20
176.13.231.133	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
213.6.50.121	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	16
46.19.85.11	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	15
198.71.233.23	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	15
62.0.197.69	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	13
80.246.138.76	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
2.53.171.243	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.85.62	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
62.0.203.129	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
46.19.86.205	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
46.19.85.92	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	10
46.19.85.194	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
46.19.86.240	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
62.90.164.185	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	8
46.19.85.194	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	alert	8
82.80.198.164	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	8
46.19.86.240	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	8
46.19.85.62	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
37.26.147.159	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	7
46.19.85.11	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
46.19.86.205	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
37.26.147.159	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
37.26.147.159	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
46.31.97.24	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	7
37.26.147.159	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	7
81.218.51.218	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.11	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.62	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
2.54.194.104	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
89.237.88.43	France	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
46.19.85.11	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.62	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.47	Israel	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
62.153.155.170	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
46.19.85.47	Israel	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
2.53.147.83	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
46.19.85.11	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.59	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
77.139.93.244	France	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
46.19.85.242	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
109.253.140.244	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
46.19.85.242	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
62.0.197.69	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	4
80.246.133.67	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
46.19.86.167	Israel	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
80.179.40.62	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
5.102.253.28	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.86.167	Israel	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4

09-22-2016-12:04:03 to 09-22-2016-13:04:03

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.53.149.194	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	122
46.19.85.112	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	105
84.95.208.20	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	47
79.181.62.129	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	45
84.95.208.20	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	32
14.220.233.85	China	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 14.220.233.85	Block	17
84.95.208.20	Israel	147.237.77.226	www.chamatz.aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	8
84.95.208.20	Israel	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	8
14.220.233.85	China	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	6
84.95.208.20	Israel	147.237.77.226	www.chamatz.aka.idf.il	PHP Attempt	Block	6
2.53.8.215	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
176.13.236.129	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
183.152.168.95	China	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 183.152.168.95	Block	4
84.95.208.20	Israel	147.237.72.166	aka.idf.il	PHP Attempt	Block	4
217.132.159.192	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/guyus	Block	4
2.53.138.237	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
84.95.208.20	Israel	147.237.76.200	eitan.aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	4
109.253.136.96	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
77.138.211.0	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar	Block	3
109.253.194.234	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.0.58	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
84.95.208.20	Israel	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	3
82.230.131.4	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/home/default.aspx	Block	3
109.253.203.40	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
84.95.208.20	Israel	147.237.77.233	atal.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	3
176.13.231.133	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
109.253.134.195	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
185.27.106.99	Israel	147.237.0.19	madim.atal.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtCaptcha in madim.atal.idf.il/login.aspx	Block	3
46.121.98.11	Israel	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	2
84.95.208.20	Israel	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	2
79.178.32.175	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/giyus/general	Block	2
2.24.85.248	United Kingdom	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/kapatz/	Block	2
2.53.171.243	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
84.95.208.20	Israel	147.237.77.233	atal.idf.il	PHP Attempt	Block	2
80.246.137.134	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
84.95.208.20	Israel	147.237.77.234	halag.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	2
80.246.139.80	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
169.229.3.91	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Illegal Byte Code Character in Method Ôˆ8\+wÇ£[[#17]]q¸ ¨h>	Block	1
217.194.207.24	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
194.90.252.194	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/templates/faq/faq.aspx	Block	1
46.4.74.42	Germany	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/brothers/skira/default.asp	Block	1
169.229.3.91	United States	147.237.77.233	atal.idf.il	NULL Character in Method ¦Þ>ßY!ÁL½}@Ýaê[[#25]][[#22]]¤:	Block	1
84.95.208.20	Israel	147.237.0.34	tikshuv.idf.il	Distributed PHP Attempt	Block	1
157.55.39.226	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/...	Block	1
46.19.85.26	Israel	147.237.77.216	dover.idf.il	Distributed Malformed URL	Block	1
213.8.204.18	Israel	147.237.76.42	refuah.idf.il	Distributed PHP Attempt	Block	1
84.95.208.20	Israel	147.237.77.234	halag.idf.il	PHP Attempt	Block	1
180.76.15.9	China	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1638-he/refuah.aspx	Block	1
82.145.219.135	Europe	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/rabanut/general.aspx	Block	1
169.229.3.91	United States	147.237.0.17	m.my-kosher-kravi.idf.il	NULL Character in Header Name at	Block	1

09-22-2016-12:04:03 to 09-22-2016-13:04:03