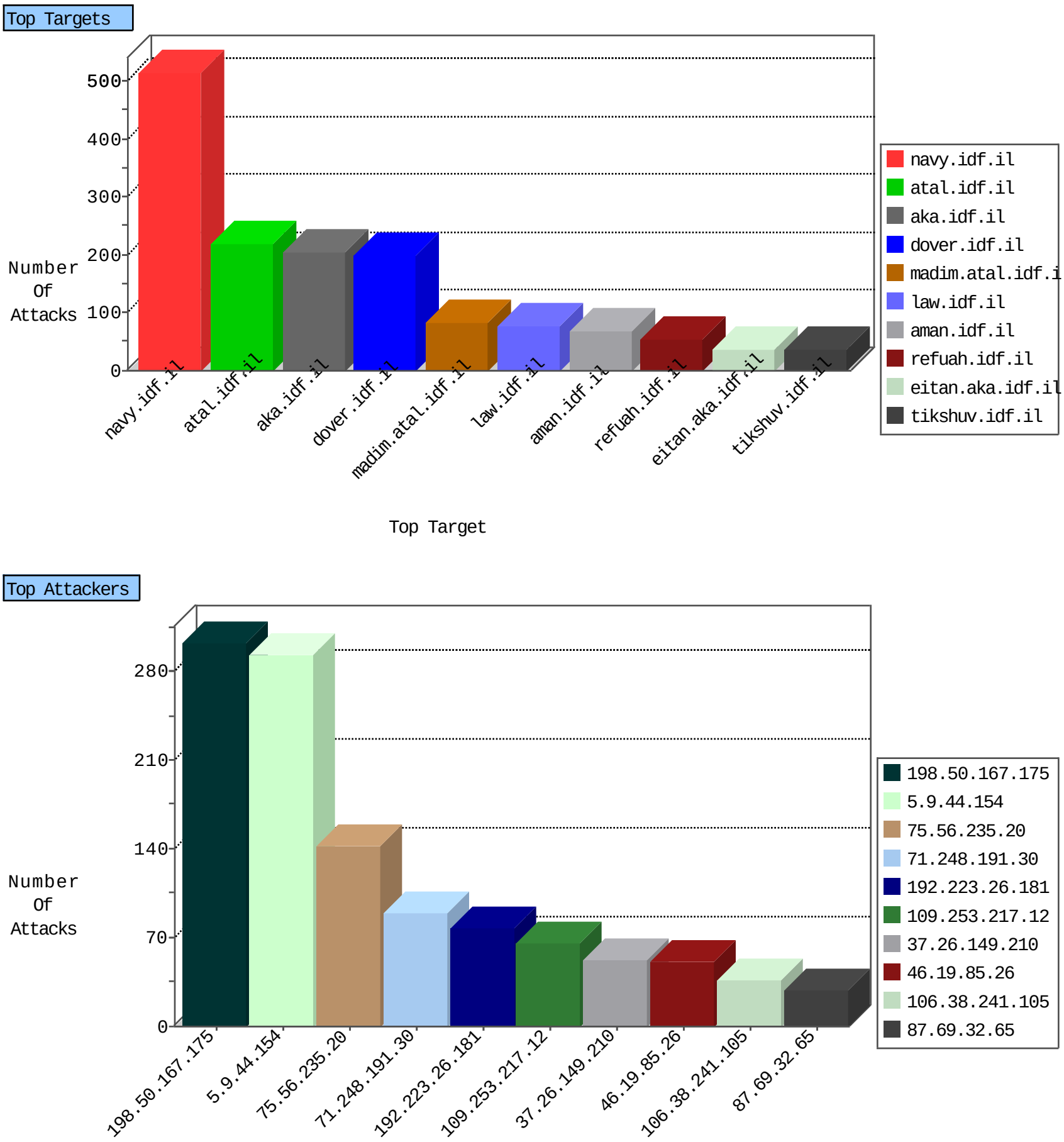
09-11-2016-22:04:08 to 09-11-2016-23:04:08

IDF Under Attack
Daily Report



09-11-2016-22:04:08 to 09-11-2016-23:04:08

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
128.223.8.114	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	3
79.178.235.26	Israel	147.237.76.42	refuah.idf.il	Black List	drop	3
109.67.16.148	Israel	147.237.77.216	dover.idf.il	Black List	drop	3
194.254.215.12	France	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	3
147.83.29.234	Spain	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
129.93.229.139	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
130.206.158.138	Spain	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
193.1.13.14	Ireland	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
129.97.74.12	Canada	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
139.78.141.243	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	2
128.223.8.112	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
200.19.159.35	Brazil	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
128.10.18.52	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
198.82.160.221	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
208.94.63.194	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
128.42.142.45	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
198.82.160.238	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
131.179.150.72	United States	147.237.72.156	aman.idf.il	network flood IPv4 ICMP	drop	1
129.10.120.193	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
216.48.80.12	Canada	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
130.194.252.8	Australia	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
128.208.4.197	United States	147.237.72.167	ishurim.aka.idf.il	network flood IPv4 ICMP	drop	1
200.19.159.34	Brazil	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
129.22.150.78	United States	147.237.72.217	e.idf.il	network flood IPv4 ICMP	drop	1
128.8.126.111	United States	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
195.113.161.83	Czech Republic	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1
130.195.4.69	New Zealand	147.237.72.166	aka.idf.il	network flood IPv4 ICMP	drop	1

09-11-2016-22:04:08 to 09-11-2016-23:04:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
138.201.125.143	Germany	147.237.76.200	eitan.aka.idf.il	C1000074: HTTP: majestic bot	Permit	21
106.38.241.105	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	21
106.38.241.105	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	13
75.56.235.20	United States	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	12
75.56.235.20	United States	147.237.77.233	atal.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	12
75.56.235.20	United States	147.237.77.233	atal.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	11
184.172.106.100	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
41.185.12.173	South Africa	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
77.67.47.7	France	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
166.62.42.29	United States	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	6
41.185.30.48	South Africa	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	5
138.201.125.143	Germany	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	3
106.38.241.105	China	147.237.77.170	maarachot.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	1
41.185.30.48	South Africa	147.237.77.233	atal.idf.il	9785: HTTP: SQL Injection (Referer Header)	Block	1

09-11-2016-22:04:08 to 09-11-2016-23:04:08

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
75.56.235.20	147.237.77.233	United States	atal.idf.il	SQL Injection - Select From	108
41.185.12.173	147.237.77.233	South Africa	atal.idf.il	SQL Injection - Select From	18
184.172.106.100	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	18
41.185.30.48	147.237.77.233	South Africa	atal.idf.il	SQL Injection - Select From	8
77.67.47.7	147.237.77.74	France	law.idf.il	SQL Injection - Select From	8
166.62.42.29	147.237.77.233	United States	atal.idf.il	SQL Injection - Select From	8
50.84.213.146	147.237.72.14	United States	dover.idf.il(old)	ET SCAN NMAP -sS window 2048	1
111.94.251.49	147.237.77.235	Indonesia	sviva.idf.il	ET SCAN NMAP -sS window 1024	1
50.84.213.146	147.237.72.14	United States	dover.idf.il(old)	ET SCAN NMAP -f -sS	1
106.38.241.105	147.237.72.166	China	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
46.172.71.251	147.237.76.44	Ukraine	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	1
93.174.95.106	147.237.76.198	Netherlands	e.yohalan.idf.il	ET SCAN NMAP -sS window 4096	1
91.201.236.158	147.237.0.200	Ukraine	m4u.idf.il	ET SCAN NMAP -sS window 1024	1
61.240.144.65	147.237.77.243	China	mobile.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
61.240.144.65	147.237.76.39	China	mobile.meitav.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
58.218.200.137	147.237.0.16	China	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
111.94.251.49	147.237.77.235	Indonesia	sviva.idf.il	ET SCAN NMAP -sS window 4096	1
50.84.213.146	147.237.72.14	United States	dover.idf.il(old)	ET SCAN NMAP -sS window 1024	1
109.253.158.185	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1
46.227.67.158	147.237.76.44	Sweden	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	1
94.102.48.195	147.237.77.205	Netherlands	prisha.idf.il	ET SCAN NMAP -sS window 1024	1
91.201.236.158	147.237.0.200	Ukraine	m4u.idf.il	ET SCAN NMAP -sS window 3072	1
66.249.93.13	147.237.77.226	Europe	www.chamatz.aka.idf.il	ET SCAN NMAP -sA (2)	1
61.240.144.65	147.237.77.216	China	dover.idf.il	ET SCAN Potential VNC Scan 5800-5820	1
61.240.144.65	147.237.72.14	China	dover.idf.il(old)	ET SCAN Potential VNC Scan 5800-5820	1

09-11-2016-22:04:08 to 09-11-2016-23:04:08

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		monitor	172
5.9.44.154	Germany	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	98
71.248.191.30	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	86
192.223.26.181	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	77
198.50.167.175	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	20
5.9.44.154	Germany	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	19
141.0.12.215	Norway	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	18
198.50.167.175	Canada	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	16
46.19.85.70	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	16
198.50.167.175	Canada	147.237.0.17	m.my-kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	15
195.60.235.57	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	15
46.19.85.26	Israel	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	15
198.50.167.175	Canada	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	15
46.19.85.26	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	15
198.50.167.175	Canada	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	15
198.50.167.175	Canada	147.237.77.235	sviva.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	14
198.50.167.175	Canada	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	14
198.50.167.175	Canada	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	14
198.50.167.175	Canada	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	13
198.50.167.175	Canada	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	13
198.50.167.175	Canada	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	13
198.50.167.175	Canada	147.237.0.15	kosher-kravi.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	13
198.50.167.175	Canada	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	13
198.50.167.175	Canada	147.237.77.170	maarachot.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	12
198.50.167.175	Canada	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	12
198.50.167.175	Canada	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	12
87.69.32.65	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	12
198.50.167.175	Canada	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	12
198.50.167.175	Canada	147.237.76.39	mobile.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	11
198.50.167.175	Canada	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	11
198.50.167.175	Canada	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	10
198.50.167.175	Canada	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	10
198.50.167.175	Canada	147.237.77.234	halag.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	9
46.19.85.26	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	9
87.69.32.65	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	9
87.69.32.65	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	8
46.19.85.70	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	8
185.3.147.67	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
37.26.149.210	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
37.26.149.210	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	7
185.27.105.71	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.26.149.210	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
37.26.149.210	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	6
37.26.149.210	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
37.26.149.210	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	6
79.180.213.197	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.53.38.160	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
195.60.235.57	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	6
46.19.85.26	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.26	Israel	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	5

09-11-2016-22:04:08 to 09-11-2016-23:04:08

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.253.217.12	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	66
218.87.63.144	China	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 218.87.63.144	Block	17
79.179.134.143	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	8
218.87.63.144	China	147.237.77.216	dover.idf.il	PHP Attempt	Block	6
46.120.36.19	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	6
77.124.23.51	Israel	147.237.72.156	aman.idf.il	Distributed Illegal Byte Code Character in Parameter Value	Block	4
79.181.188.176	Israel	147.237.76.147	chinuch.aka.idf.i	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	3
5.102.195.37	Israel	147.237.72.156	aman.idf.il	Unauthorized HTTP Method	Block	2
77.138.71.214	France	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
5.29.26.18	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
109.253.198.175	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
77.138.251.92	France	147.237.77.216	dover.idf.il	Parameter Type Violation aspxerrorpath in www.idf.il/error.htm	Block	2
5.29.53.156	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
109.66.9.12	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
5.29.64.59	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
77.237.138.202	Czech Republic	147.237.77.170	maarachot.idf.il	Unauthorized Method HEAD for /	Block	1
77.124.21.71	Israel	147.237.72.156	aman.idf.il	Illegal Byte Code Character in Parameter Value at 101 for www.aman.idf.il/modiin/questionnaires.aspx	Block	1
84.229.37.158	Israel	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to madim.atal.idf.il/shared/ajax/updatemakatqauntity.aspx	Block	1
66.249.65.188	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1412-he/refuah.aspx	Block	1
46.116.111.93	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/undefined	Block	1
218.87.63.144	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/index.asp	Block	1
106.38.241.105	China	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
66.249.66.176	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/giyus/forum/asp/showforum.asp	Block	1
77.124.26.190	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
46.116.117.87	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
77.139.10.88	France	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/favicon.ico	Block	1
66.249.76.70	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/scripts.asmx/getjs	Block	1
157.55.39.34	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-13437-he/dover.aspx„'¯¬¿¬£'½¬¿¬¯¬'½¬¿¬¯¬'•'½	Block	1
79.181.239.67	Israel	147.237.72.167	ishurim.aka.idf.i	Unauthorized Request Content Type text/ping	Block	1
77.124.38.198	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1135-he/atal.aspx	Block	1
109.66.149.20	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
77.139.10.202	France	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	1
75.112.192.77	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
5.29.64.59	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/rabanut/contactus.aspx	Block	1
82.2.226.217	United Kingdom	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/home/default.aspx	Block	1
77.124.49.122	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/guyus	Block	1
66.102.8.213	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/sachar/viewpayslip.aspx	Block	1
109.66.149.20	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1

09-11-2016-22:04:08 to 09-11-2016-23:04:08