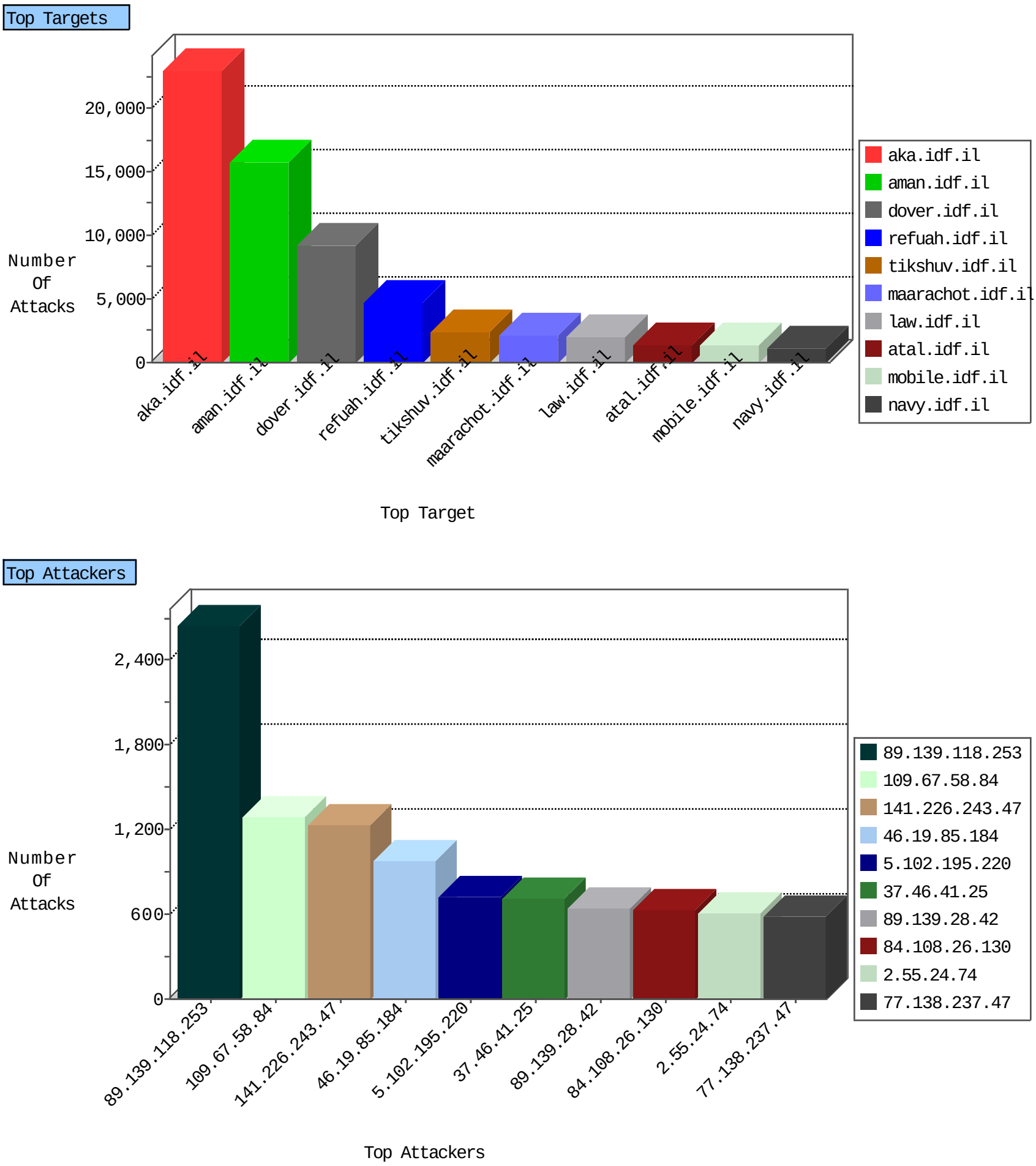
09-10-2016-21:04:05 to 09-10-2016-22:04:05

IDF Under Attack
Daily Report



09-10-2016-21:04:05 to 09-10-2016-22:04:05

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
41.96.217.128	Algeria	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	77642
115.230.125.146	China	147.237.0.16	my-kosher-kravi.idf.il	JLM_Purple_Con_Limit_Tcp	drop	1
115.230.125.146	China	147.237.0.17	m.my-kosher-kravi.idf.il	JLM_Purple_Con_Limit_Http	drop	1
115.230.125.146	China	147.237.0.200	m4u.idf.il	JLM_Purple_Con_Limit_Http	drop	1

09-10-2016-21:04:05 to 09-10-2016-22:04:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.4.116.197	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Permit	82
106.38.241.105	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	30
106.38.241.105	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	9
91.121.86.136	France	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	9
46.4.116.197	Germany	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Permit	4
46.4.116.197	Germany	147.237.77.74	law.idf.il	C1000074: HTTP: majestic bot	Permit	3
106.38.241.105	China	147.237.77.74	law.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	2
162.210.196.98	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

09-10-2016-21:04:05 to 09-10-2016-22:04:05

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
109.64.105.153	147.237.72.166	Israel	aka.idf.il	Xenu Link Sleuth User Agent	18
163.172.129.15	147.237.76.177	United Kingdom	ncore.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
163.172.129.15	147.237.0.200	United Kingdom	m4u.idf.il	ET SCAN NMAP -sS window 1024	1
109.60.153.178	147.237.76.197	Russian Federation	e.himush.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
89.163.224.101	147.237.77.170	Germany	maarachot.idf.il	ET SCAN Potential SSH Scan	1
89.163.224.101	147.237.8.27	Germany	e.madim.atal.idf.il	ET SCAN Potential SSH Scan	1
46.161.40.17	147.237.8.14	Russian Federation	e.orchot.idf.il	ET SCAN NMAP -sS window 1024	1
176.58.124.35	147.237.77.212	United Kingdom	e.dover.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
5.255.90.133	147.237.76.39	Netherlands	mobile.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
163.172.129.15	147.237.76.198	United Kingdom	e.yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
5.255.90.133	147.237.0.17	Netherlands	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
163.172.129.15	147.237.72.167	United Kingdom	ishurim.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
139.162.225.219	147.237.76.200	United States	eitan.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
109.60.153.178	147.237.76.201	Russian Federation	e.atal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
109.60.153.178	147.237.0.200	Russian Federation	m4u.idf.il	ET SCAN NMAP -sS window 1024	1
89.163.224.101	147.237.8.50	Germany	e.tikshuv.idf.il	ET SCAN Potential SSH Scan	1
66.249.93.154	147.237.77.170	Europe	maarachot.idf.il	ET SCAN NMAP -sA (2)	1
23.91.75.231	147.237.8.27	United States	e.madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
163.172.129.15	147.237.77.19	United Kingdom	law-forum.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
5.255.90.133	147.237.76.34	Netherlands	yohalan.idf.il	ET SCAN NMAP -sS window 1024	1

09-10-2016-21:04:05 to 09-10-2016-22:04:05

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
89.139.118.253	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	2651
109.67.58.84	Israel	147.237.72.156	aman.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	1297
141.226.243.47	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	1239
46.19.85.184	Israel	147.237.77.74	law.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	980
89.139.28.42	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	641
5.102.195.220	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	630
84.108.26.130	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	615
2.55.24.74	Israel	147.237.72.156	aman.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	608
77.138.237.47	France	147.237.72.156	aman.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	587
37.46.41.25	Israel	147.237.76.42	refuah.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	569
79.178.249.218	Israel	147.237.72.156	aman.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	507
188.120.154.84	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	428
80.179.8.175	Israel	147.237.72.156	aman.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	412
176.13.3.98	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	401
66.249.73.163	United States	147.237.77.170	maarachot.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	396
66.249.66.232	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	379
46.19.85.77	Israel	147.237.72.156	aman.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	370
80.246.138.1	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	368
46.19.86.238	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	346
77.139.12.24	France	147.237.77.170	maarachot.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	345
109.253.207.100	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	332
217.132.153.4	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	315
84.109.131.93	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	310
87.70.7.13	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	305
84.111.64.45	Israel	147.237.77.74	law.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	299
109.253.218.92	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	290
46.117.108.129	Israel	147.237.77.226	www.chamatz.aka.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	285
80.246.130.214	Israel	147.237.77.226	www.chamatz.aka.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	278
79.180.146.67	Israel	147.237.72.156	aman.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	277
89.237.75.96	France	147.237.72.156	aman.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	276
109.67.179.12	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	276
46.116.127.146	Israel	147.237.76.42	refuah.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	272
84.94.181.18	Israel	147.237.76.42	refuah.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	270
2.53.181.92	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	264
176.13.11.234	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	263
141.226.149.142	Israel	147.237.72.156	aman.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	259
79.181.101.28	Israel	147.237.72.156	aman.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	259

09-10-2016-21:04:05 to 09-10-2016-22:04:05

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
109.64.15.176	Israel	147.237.76.42	refuah.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	257
79.178.212.208	Israel	147.237.72.156	aman.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	257
46.19.86.161	Israel	147.237.77.170	maarachot.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	256
176.13.12.29	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	247
46.116.8.73	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	245
87.70.40.122	Israel	147.237.72.156	aman.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	239
79.181.247.148	Israel	147.237.72.156	aman.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	235
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	233
79.183.56.238	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	230
84.111.24.229	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	230
109.67.232.78	Israel	147.237.72.156	aman.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	229
80.246.139.59	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	228
2.53.157.56	Israel	147.237.77.233	atal.idf.il	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	221

09-10-2016-21:04:05 to 09-10-2016-22:04:05

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
213.57.49.167	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	126
93.172.216.75	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	109
46.19.85.122	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	11
109.64.105.153	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 109.64.105.153	Block	7
109.66.13.246	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
109.253.150.236	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
79.180.14.219	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.53.139.238	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
85.64.84.91	Israel	147.237.72.166	aka.idf.il	Distributed Unknown HTTP Request Method	Block	3
109.64.105.153	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 109.64.105.153	Block	3
89.237.75.96	France	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/favicon.ico	Block	2
79.178.110.137	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
77.138.117.135	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/kapatz/contactus.aspx	Block	1
104.131.210.43	United States	147.237.77.226	www.chamatz.aka.idf.il	NULL Character in URL ıžbf»Ý‹‘ßzža[[ɪƉ#0[[]]#5[["+ɲ]]#16–2°`tf‰n.]]¸]]#19[[¸,0¸¸+¸/¸]]#28[[]]#0[[]]#0[[ɤ	Block	1
104.131.210.43	United States	147.237.77.226	www.chamatz.aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
37.26.146.240	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	1
80.246.140.81	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	1
141.226.217.78	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
77.139.21.208	France	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/favicon.ico	Block	1
104.131.210.43	United States	147.237.77.226	www.chamatz.aka.idf.il	Multiple Illegal Byte Code Character in Method from 104.131.210.43	Block	1
46.19.85.102	Israel	147.237.76.86	navy.idf.il	Unknown HTTP Request Method 2C1471464840%2C%22https%3A%2F%2Fwww.google.co.il%2F%22%5D in URL	Block	1
212.129.62.79	France	147.237.0.17	m.my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.17/	Block	1
87.71.44.37	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1135-he/atal.aspx	Block	1
79.179.9.38	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	1
77.138.222.228	France	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 77.138.222.228	Block	1
104.131.210.43	United States	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to 147.237.77.226/changelog.txt	Block	1
104.131.210.43	United States	147.237.77.226	www.chamatz.aka.idf.il	Illegal Byte Code Character in Header Name	Block	1
40.77.167.81	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
84.108.14.8	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_KEY_EXCHANGE)	None	1
159.203.95.196	United States	147.237.76.30	himush.idf.il	Unauthorized Method HEAD for www.tech.atal.idf.il/	None	1
109.64.105.153	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/kamlar/	Block	1
77.139.100.68	France	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
104.131.210.43	United States	147.237.77.226	www.chamatz.aka.idf.il	Multiple Malformed URL from 104.131.210.43	Block	1
212.129.62.79	France	147.237.0.34	tikshuv.idf.il	Unauthorized Method HEAD for 147.237.0.34/	Block	1
109.253.202.38	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
77.138.222.228	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/smalim/smalim.aspx	Block	1
104.131.210.43	United States	147.237.77.226	www.chamatz.aka.idf.il	Unknown HTTP Request Method [[#22]][[#3]][[#1]][[#0]]•[[#1]][[#0]][[#0]]{[[#3]][[#3]]‹ in URL ıžbf»Ý‹‘ßzža[[ɪƉ#0[[]]#5[["+ɲ]]#16–2°`tf‰n.]]ɤ[[0#]][[0#]][[82#]]./¸+¸¸0,¸[[91#]]	Block	1
104.131.210.43	United States	147.237.77.226	www.chamatz.aka.idf.il	Illegal HTTP Version À[[#20]]À	Block	1
45.56.102.108	United States	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/eitan/pratim/pirteyerua/	Block	1
85.64.1.207	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/960.css	Block	1
176.13.3.98	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
109.64.105.153	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/hinuch	Block	1
78.11.48.201	Poland	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.102.9.24	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for aka.idf.il/main/home/default.aspx	Block	1
104.131.210.43	United States	147.237.77.226	www.chamatz.aka.idf.il	Multiple NULL Character in Method from 104.131.210.43	Block	1
213.8.204.53	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/general.aspx	Block	1
91.193.71.5	Ukraine	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/home/default.aspx	Block	1
79.181.27.69	Israel	147.237.72.167	ishurim.aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
109.253.211.94	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
77.138.237.47	France	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	1

09-10-2016-21:04:05 to 09-10-2016-22:04:05