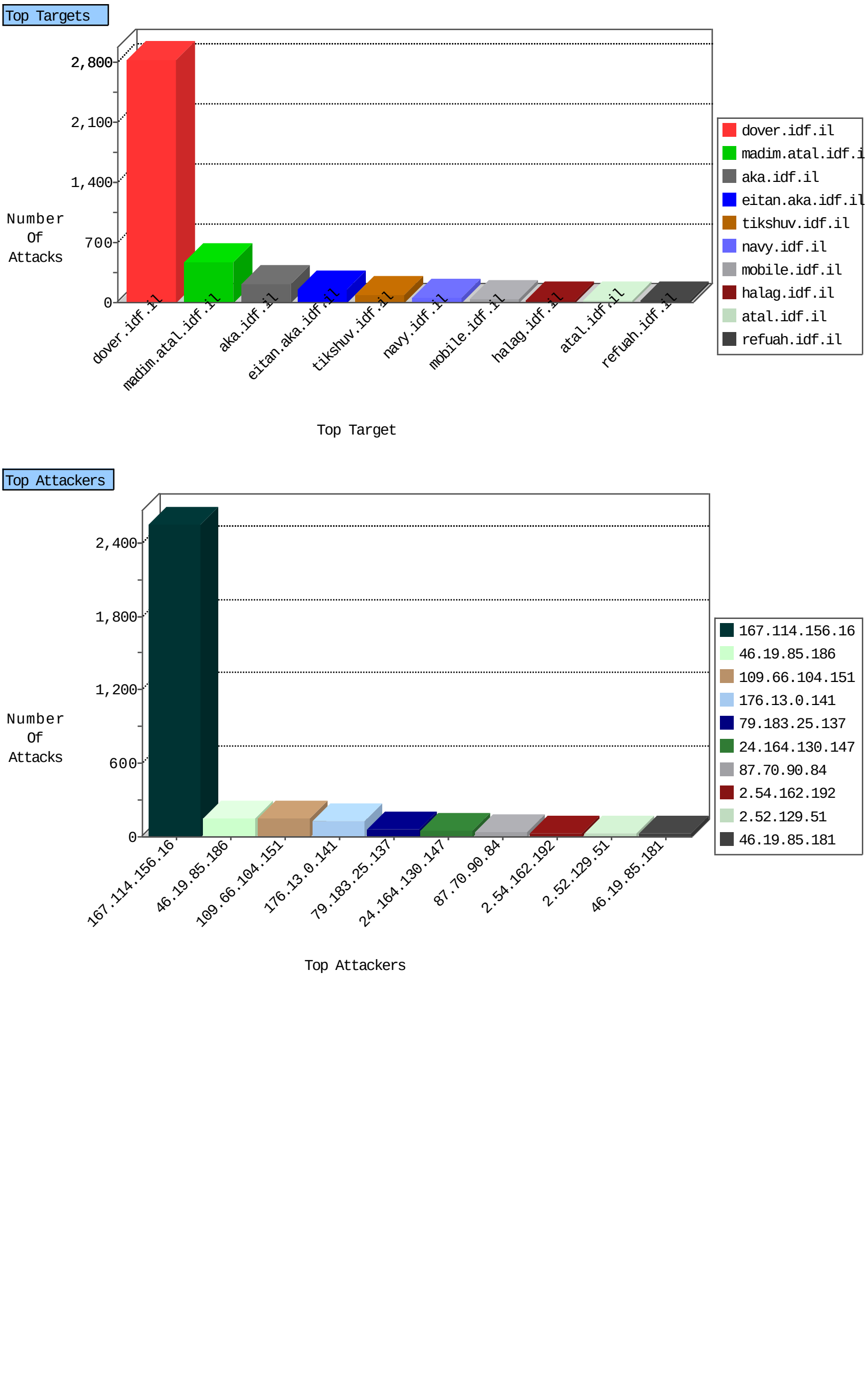
03-15-2016-21:04:09 to 03-15-2016-22:04:09

IDF Under Attack Daily Report



03-15-2016-21:04:09 to 03-15-2016-22:04:09

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	3343
81.218.65.210	Israel	147.237.0.34	tikshuv.idf.il	Block_Udp_All_Nets	drop	3
180.97.31.70	China	147.237.0.17	m.my-kosher-kravi.idf.il	Invalid L4 Header Length	drop	1
104.239.173.81		147.237.8.50	e.tikshuv.idf.il	Invalid L4 Header Length	drop	1

03-15-2016-21:04:09 to 03-15-2016-22:04:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
93.173.3.163	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	18
46.117.14.49	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
23.91.70.44	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
63.143.34.37	United States	147.237.77.216	dover.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
23.91.70.121	United States	147.237.77.233	atal.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	4
74.63.228.226	United States	147.237.76.86	navy.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
106.38.241.149	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	4
79.177.111.80	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
46.19.85.15	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
216.201.148.210	United States	147.237.77.216	dover.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
195.154.200.93	France	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	3
195.154.185.20	France	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Block	2
195.154.185.20	France	147.237.77.176	matpash.idf.il	C1000074: HTTP: majestic bot	Block	2
195.154.185.20	France	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
177.185.192.77	Brazil	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	2
85.65.0.194	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
41.225.41.64	Tunisia	147.237.77.216	dover.idf.il	18160: HTTP: Critroni Likely Malicious Tor Proxy Cookie	Block	1

03-15-2016-21:04:09 to 03-15-2016-22:04:09

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
63.143.34.37	147.237.77.216	United States	dover.idf.il	SQL Injection - Select From	12
74.63.228.226	147.237.76.86	United States	navy.idf.il	SQL Injection - Select From	12
23.91.70.121	147.237.77.233	United States	atal.idf.il	SQL Injection - Select From	6
177.185.192.77	147.237.77.74	Brazil	law.idf.il	SQL Injection - Select From	6
216.201.148.210	147.237.77.216	United States	dover.idf.il	SQL Injection - Select From	6
23.91.70.44	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	6
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
112.196.49.101	147.237.76.42	India	refuah.idf.il	ET SCAN NMAP -f -sS	1
94.102.48.194	147.237.76.199	Netherlands	e.nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
94.102.48.194	147.237.0.15	Netherlands	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
80.82.79.104	147.237.77.233	Netherlands	atal.idf.il	ET SCAN NMAP -sS window 1024	1
74.218.80.126	147.237.0.34	United States	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
112.196.49.101	147.237.76.42	India	refuah.idf.il	ET SCAN NMAP -sS window 1024	1
94.102.48.194	147.237.77.19	Netherlands	law-forum.idf.il	ET SCAN NMAP -sS window 1024	1
94.102.48.194	147.237.0.17	Netherlands	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
87.71.51.117	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1
79.182.32.19	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
37.139.27.231	147.237.76.148	Netherlands	gqcenter.aka.idf.il	ET SCAN NMAP -sS window 1024	1
185.92.72.82	147.237.77.235		sviva.idf.il	ET SCAN Potential SSH Scan	1
112.196.49.101	147.237.76.42	India	refuah.idf.il	ET SCAN NMAP -sS window 2048	1

03-15-2016-21:04:09 to 03-15-2016-22:04:09

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
79.183.25.137	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	57
24.164.130.147	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	54
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	22
46.19.85.181	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
212.76.110.148	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	16
192.116.172.24	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	15
2.54.19.200	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	13
2.54.133.72	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
2.54.42.69	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
37.26.148.151	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	11
85.64.211.214	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
2.54.162.192	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
192.116.172.24	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	alert	9
95.86.100.31	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
2.54.142.116	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
93.173.31.122	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
77.126.148.66	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	8
37.26.149.129	Israel	147.237.8.45	e.eitan.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
46.19.85.15	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
46.19.85.76	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
109.67.134.8	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.162.192	Israel	147.237.77.216	dover.idf.il	SYN Attack		reject	6
79.177.139.207	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
46.19.85.236	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.52.129.51	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
84.109.70.137	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
94.230.86.204	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.15	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
2.52.129.51	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
2.52.129.51	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
2.52.129.51	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
2.52.129.51	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	5
80.246.139.152	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
164.138.122.104	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
46.19.85.192	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack		reject	4
87.71.105.210	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
46.19.85.181	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
37.46.39.5	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
178.63.105.85	Germany	147.237.8.46	e.chinuch.idf.il	drop	SAM rule	drop	4
37.26.148.232	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.6.135	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.179.178.81	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.22.135.116	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
46.19.86.160	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.102.242.224	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
109.253.144.180	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.46.41.129	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
109.65.179.35	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

03-15-2016-21:04:09 to 03-15-2016-22:04:09

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.186	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	151
109.66.104.151	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	148
176.13.0.141	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	126
213.57.75.41	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	16
2.54.147.114	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
66.249.81.212	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	5
213.251.182.103	France	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/0/size220x0/3410.jpg.src	Block	3
2.54.156.55	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
87.70.90.84	Israel	147.237.77.216	dover.idf.il	Multiple Untraceable SSL Sessions from 87.70.90.84 (Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE))	None	3
2.54.142.116	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
79.182.190.200	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
37.190.42.98	Russian Federation	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 37.190.42.98	Block	3
109.65.18.231	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
2.52.20.154	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
87.70.90.84	Israel	147.237.77.216	dover.idf.il	Multiple Abnormally Long Header Line from 87.70.90.84	Block	2
87.70.90.84	Israel	147.237.77.216	dover.idf.il	Multiple Illegal HTTP Version from 87.70.90.84	Block	2
87.70.90.84	Israel	147.237.77.216	dover.idf.il	Multiple Unknown HTTP Request Method from 87.70.90.84	Block	2
87.70.90.84	Israel	147.237.77.216	dover.idf.il	Multiple Illegal Byte Code Character in Header Name from 87.70.90.84	Block	2
81.28.197.146	France	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
87.70.90.84	Israel	147.237.77.216	dover.idf.il	Multiple Malformed URL from 87.70.90.84	Block	2
46.19.86.112	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
87.70.90.84	Israel	147.237.77.216	dover.idf.il	Multiple Illegal Byte Code Character in Method from 87.70.90.84	Block	2
87.70.90.84	Israel	147.237.77.216	dover.idf.il	Multiple NULL Character in Header Name from 87.70.90.84	Block	2
149.78.74.231	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
87.70.90.84	Israel	147.237.77.216	dover.idf.il	Multiple Illegal Byte Code Character in URL from 87.70.90.84	Block	2
46.19.85.189	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
84.109.70.137	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
37.26.146.214	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
87.70.90.84	Israel	147.237.77.216	dover.idf.il	Multiple NULL Character in Method from 87.70.90.84	Block	1
78.165.169.14	Turkey	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	1
66.249.69.48	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1153-20704-he/dover.aspx	Block	1
199.30.24.242	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/scripts.asmx/getjs	Block	1
37.190.42.98	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-en/dover.aspx'	Block	1
157.55.39.57	United States	147.237.72.166	aka.idf.il	Unknown Parameter catid in aka.idf.il/main/drushim/info.aspx	None	1
87.70.90.84	Israel	147.237.77.216	dover.idf.il	Illegal Byte Code Character in Header Name fJ.àÅûjŽJ}Òµ‘§Uøåyç¢«¼Ù[[#6]]WxJé¹Ì]ø"†ÛqM.ÃU!I±ßRîï;ü[[#8]]°ˆV† pçµ[[#21]]÷õ[[#20]]•?a…2qo¤6[[#23]]-Êz”Û#012^&`¶l†§ó"ÊÄ‹Gté©’‘¢	Block	1
80.246.130.90	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
5.28.191.224	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	1
87.70.90.84	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
66.249.81.215	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
2.53.9.106	Israel	147.237.77.226	www.chamatz.aka.idf.il	PHP Attempt	Block	1
87.70.90.84	Israel	147.237.77.216	dover.idf.il	Illegal Byte Code Character in URL [[#24]]_•™Ða[[#28]][[ъ#15ı*″]]…][[#12]](·ßc!¨¬[[#23]]\t[[ъ#6λ]]t9!¯ע„•¸†ÐdЋu:¸n¯ž[[#3]]Û·n…[[#26]]†¬0[[#1]][[#1]],Š’œ[[#16]]<\' [[#21]]4gnj'[[#27]]0[[ъ#24~e¦¨•*h]]	Block	1
46.19.85.236	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	1
157.55.39.193	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-14886-en/dover.aspx	Block	1
84.229.134.46	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
37.26.148.133	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
78.165.169.14	Turkey	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/xmlrpc.php	Block	1

03-15-2016-21:04:09 to 03-15-2016-22:04:09