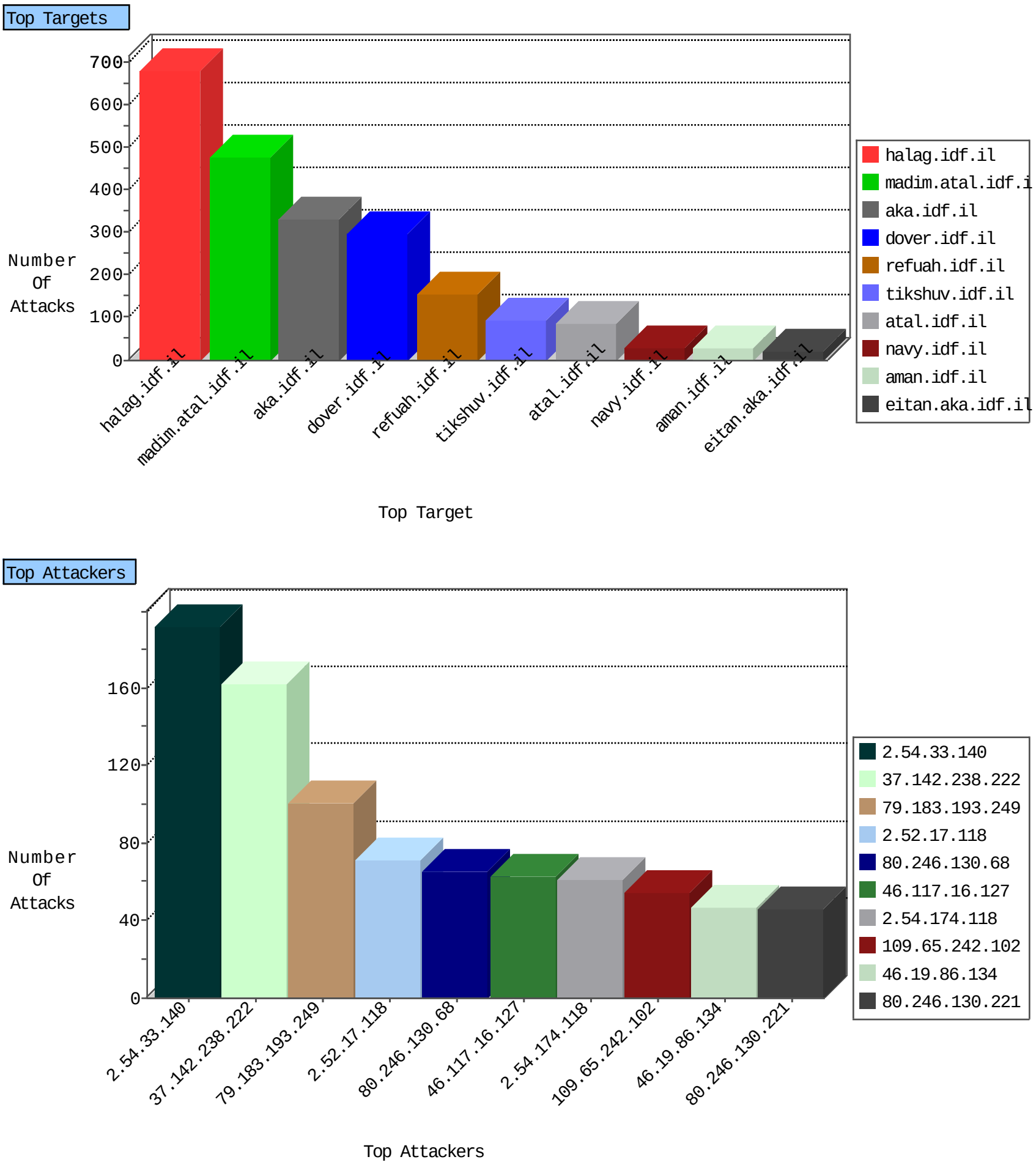
02-25-2016-18:04:04 to 02-25-2016-19:04:04

IDF Under Attack Daily Report



02-25-2016-18:04:04 to 02-25-2016-19:04:04

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	2
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	2
198.23.190.39	United States	147.237.72.14	dover.idf.il(old)	Block_Ntp_All_Net	drop	1
185.130.5.224		147.237.0.33	idf.il	Block_Udp_All_Nets	drop	1
36.103.106.145	China	147.237.76.177	ncore.idf.il	Block_Udp_All_Nets	drop	1
185.130.5.224		147.237.8.14	e.orchot.idf.il	Block_Udp_All_Nets	drop	1
36.103.106.145	China	147.237.76.202	e.halag.idf.il	Block_Udp_All_Nets	drop	1
185.130.5.224		147.237.77.176	matpash.idf.il	Block_Udp_All_Nets	drop	1

02-25-2016-18:04:04 to 02-25-2016-19:04:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
80.246.130.166	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	12
85.250.204.18	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	12
149.88.188.253	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	10
213.57.163.60	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
149.88.163.192	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
132.76.61.51	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
149.88.195.75	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
109.66.211.232	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
79.183.193.249	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
199.58.86.209	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
37.26.147.148	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
212.76.125.11	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
46.19.86.193	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
77.126.15.221	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
109.66.3.114	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
199.58.86.209	United States	147.237.77.74	law.idf.il	C1000074: HTTP: majestic bot	Block	1

02-25-2016-18:04:04 to 02-25-2016-19:04:04

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
31.210.187.210	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
213.57.247.119	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
93.173.140.145	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
212.76.125.11	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1
87.70.22.84	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.180.59.213	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
183.60.48.25	147.237.0.19	China	madim.atal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
79.179.58.118	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
148.251.21.227	147.237.72.166	Germany	aka.idf.il	portscan: TCP Distributed Portscan	1
46.120.237.85	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
116.121.137.5	147.237.76.30	Korea, Republic of	himush.idf.il	ET SCAN NMAP -f -sS	1
46.19.85.103	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
112.196.49.101	147.237.77.178	India	e.matpash.idf.il	ET SCAN NMAP -sS window 1024	1
38.105.146.70	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sS window 2048	1
220.231.195.122	147.237.72.166	China	aka.idf.il	ET SCAN NMAP -sS window 4096	1
109.66.54.17	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
37.26.146.210	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
217.132.13.225	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
94.159.184.98	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
213.57.163.60	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
88.162.163.250	147.237.77.216	France	dover.idf.il	portscan: TCP Distributed Portscan	1
204.101.135.203	147.237.77.226	Canada	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 1024	1
80.179.96.90	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
185.120.125.56	147.237.77.216		dover.idf.il	portscan: TCP Distributed Portscan	1
79.180.22.214	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
180.97.106.37	147.237.8.24	China	e.lifestyle.idf.il	ET SCAN Potential SSH Scan	1
46.229.133.233	147.237.76.31	Russian Federation	nakchal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
116.121.137.5	147.237.76.30	Korea, Republic of	himush.idf.il	ET SCAN NMAP -sS window 2048	1
46.116.153.79	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
112.196.49.101	147.237.77.178	India	e.matpash.idf.il	ET SCAN NMAP -sS window 4096	1
38.105.146.70	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sS window 3072	1
109.67.172.171	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
38.105.146.70	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -f -sS	1
220.231.195.122	147.237.72.166	China	aka.idf.il	ET SCAN NMAP -sS window 3072	1
109.65.153.160	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

02-25-2016-18:04:04 to 02-25-2016-19:04:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
79.183.193.249	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	90
80.246.130.68	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	64
46.117.16.127	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	62
80.246.130.221	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	45
176.13.20.254	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	43
79.176.220.113	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	39
80.246.133.243	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	38
80.246.130.250	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	37
80.246.133.81	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	35
109.65.242.102	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	35
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	34
46.117.30.165	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	34
185.120.125.56		147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	31
176.13.15.74	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	29
176.228.84.22	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	29
46.117.67.124	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	28
77.125.142.5	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	27
80.246.133.157	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	23
212.76.127.10	Israel	147.237.77.233	atal.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	21
2.52.17.118	Israel	147.237.77.216	dover.idf.il	SYN Attack		reject	19
109.65.242.102	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	18
2.54.174.118	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	18
84.228.242.11	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	16
2.54.24.191	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	15
176.228.84.22	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	alert	15
109.67.172.171	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	15
2.54.174.118	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	13
84.228.136.81	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	13
2.54.174.118	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	13
46.19.85.120	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	13
2.54.174.118	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	13
2.52.17.118	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	12
2.52.17.118	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	12
2.52.17.118	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
2.52.17.118	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
37.46.41.198	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
109.253.146.159	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.46.41.190	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
79.183.193.249	Israel	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
185.120.126.34		147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
185.3.147.203	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.183.0.66	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.7.13	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
84.228.219.201	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.253.195.112	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
46.19.86.192	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
79.181.96.96	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
83.130.108.142	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.64.87.147	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6

02-25-2016-18:04:04 to 02-25-2016-19:04:04

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.54.33.140	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	192
37.142.238.222	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	160
46.19.86.134	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	47
37.26.147.220	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	36
80.250.149.60	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	19
109.64.87.147	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 109.64.87.147	Block	15
46.19.85.120	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 46.19.85.120	Block	7
208.115.113.88	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/giyus/forum/asp/showforum.asp	Block	7
2.54.141.4	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	7
109.64.87.147	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/1/	Block	5
113.85.27.73	China	147.237.77.216	dover.idf.il	PHP Attempt	Block	5
113.85.27.73	China	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 113.85.27.73	Block	3
185.32.179.8	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
37.26.147.166	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
113.85.27.73	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/plus/download.php	Block	2
209.232.147.220	United States	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	2
37.26.146.243	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/nekudot/index	Block	2
213.8.204.53	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1071	Block	2
46.121.102.109	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$btnAtudaBack in www.aka.idf.il/main/giyus/atuda/asmachta.aspx	None	1
203.133.171.71	Korea, Republic of	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/modiin/default.aspx	Block	1
176.13.20.254	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
84.109.88.107	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
80.246.130.250	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
109.65.242.102	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
77.125.142.5	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
2.54.160.206	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
2.52.44.179	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
93.160.60.22	Denmark	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1503-en/dover.aspx.	Block	1
46.117.16.127	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	1
185.82.200.91		147.237.0.19	madim.atal.idf.i	Unauthorized URL Access to 147.237.0.19/	Block	1
37.26.149.162	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
167.114.211.10	Canada	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/blog/wp-admin/	Block	1
81.218.53.114	Israel	147.237.72.156	aman.idf.il	Multiple Unauthorized URL Access from 81.218.53.114	Block	1
5.29.171.117	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/main/sachar/	Block	1
109.253.146.159	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
79.181.16.190	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
213.8.204.56	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/	Block	1
62.201.217.82	Iraq	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/arr/	Block	1
207.46.13.84	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
2.54.130.231	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
46.19.85.184	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
176.228.84.22	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
84.228.136.81	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
80.246.133.81	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
129.121.189.75	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/wp/wp-admin/	Block	1
2.54.187.96	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
109.67.172.171	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	1
77.125.152.234	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
2.54.13.152	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
94.136.40.75	United Kingdom	147.237.76.42	refuah.idf.il	Unauthorized URL Access to refua.atal.idf.il/wordpress/wp-admin/	Block	1

02-25-2016-18:04:04 to 02-25-2016-19:04:04