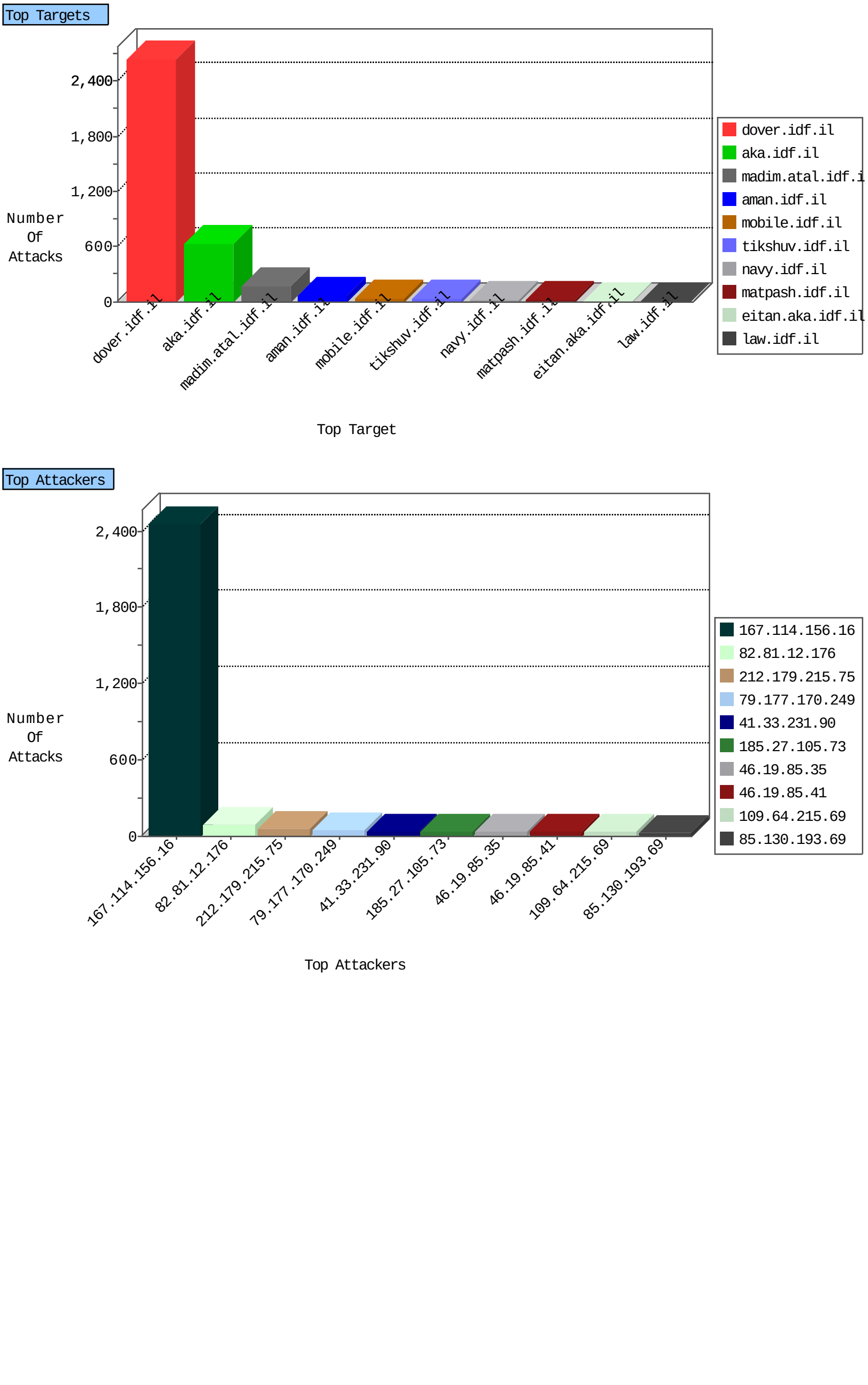
01-24-2016-19:04:00 to 01-24-2016-20:04:00

IDF Under Attack Daily Report



01-24-2016-19:04:00 to 01-24-2016-20:04:00

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	3121
82.81.12.176	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	96
79.182.196.41	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	6
109.67.125.101	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	6
197.114.30.13	Algeria	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
79.183.227.154	Israel	147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	3
115.230.124.164	China	147.237.77.216	dover.idf.il	block-sp-traf1	drop	1
210.233.165.203	Japan	147.237.76.31	nakchal.idf.il	Block_Udp_All_Nets	drop	1
141.212.122.174	United States	147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	1
66.102.9.118	United States	147.237.72.166	aka.idf.il	HTTP-Misc-BadBlue-Dir-Trave-2	dest-reset	1
89.248.174.4	Netherlands	147.237.76.177	ncore.idf.il	Block_Ntp_All_Net	drop	1

01-24-2016-19:04:00 to 01-24-2016-20:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
45.63.70.210		147.237.77.74	law.idf.il	C008: HTTP: Xenu UserAgent	Block	1
188.165.15.21	France	147.237.76.31	nakchal.idf.il	C228: HTTP: AhrefBot crawler	Block	1
188.165.15.121	France	147.237.76.86	navy.idf.il	C228: HTTP: AhrefBot crawler	Block	1

01-24-2016-19:04:00 to 01-24-2016-20:04:00

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
46.19.85.227	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
185.130.5.200	147.237.77.233		atal.idf.il	ET SCAN Potential SSH Scan	1
37.142.64.45	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.64.49.46	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
5.29.178.132	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
85.250.43.127	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
2.52.5.247	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
217.132.55.95	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
85.64.8.199	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
185.130.5.240	147.237.77.227		e.hamaz.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
79.179.212.17	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
185.130.5.240	147.237.76.199		e.nakchal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
79.177.218.38	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
185.130.5.240	147.237.76.197		e.himush.idf.il	ET SCAN NMAP -sS window 1024	1
68.180.229.239	147.237.72.166	United States	aka.idf.il	portscan: TCP Distributed Portscan	1
185.130.5.240	147.237.8.28		e.mobile-ks.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
62.90.77.124	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
185.130.5.240	147.237.0.19		madim.atal.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
37.142.245.136	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
109.253.219.116	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
37.26.149.238	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
94.159.167.62	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
5.29.176.72	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
85.65.70.39	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
80.246.130.0	147.237.77.216	Israel	dover.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1
185.130.5.240	147.237.77.216		dover.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
79.178.22.100	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
185.130.5.240	147.237.76.197		e.himush.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
79.176.2.70	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
185.130.5.240	147.237.76.30		himush.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
66.249.78.89	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	1
185.130.5.240	147.237.0.34		tikshuv.idf.il	ET SCAN Potential VNC Scan 5900-5920	1

01-24-2016-19:04:00 to 01-24-2016-20:04:00

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
212.179.215.75	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	54
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
85.130.193.69	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
79.183.135.160	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
185.27.105.73	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	18
185.27.105.73	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	18
109.64.215.69	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	12
109.64.215.69	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	12
79.176.188.114	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	11
79.179.28.195	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
37.26.147.206	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
2.54.104.242	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	8
93.172.255.95	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
46.60.4.207	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	8
109.64.215.69	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	7
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
79.180.19.58	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.243	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
82.80.130.133	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
77.125.105.214	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.120.17.107	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
109.65.42.150	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.177.197.36	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.64.11.146	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
109.253.198.21	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
82.80.130.133	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
66.102.9.54	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	5
2.52.128.50	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	5
109.65.210.247	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
94.230.86.64	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
31.210.187.156	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
37.26.149.170	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
37.142.242.25	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	4
37.26.146.198	Israel	147.237.77.243	mobile.idf.il	Bad TCP sequence		alert	4
188.120.148.156	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
2.54.104.242	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
2.54.104.242	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
37.26.148.217	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
84.108.153.86	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
80.246.137.157	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
212.179.215.75	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
5.102.196.56	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
80.246.140.101	Israel	147.237.72.166	aka.idf.il	SYN Attack		reject	3
94.159.147.232	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
185.3.147.200	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
77.125.94.175	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
79.181.61.16	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.177.170.249	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	41
46.19.85.35	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	36
46.19.85.41	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	34
2.54.128.165	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	13
176.13.0.234	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	9
176.13.16.222	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	7
79.177.170.249	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	6
213.159.38.90	Lithuania	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	6
84.229.134.91	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 84.229.134.91	Block	6
213.159.38.90	Lithuania	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 213.159.38.90	Block	5
2.52.38.23	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	5
176.228.71.215	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	4
2.54.180.124	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	4
84.229.134.91	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/4/	Block	3
5.22.135.195	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
79.181.61.16	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
212.76.107.74	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 212.76.107.74	Block	2
2.54.62.21	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
93.172.255.95	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
146.185.234.48	Russian Federation	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 146.185.234.48	Block	2
185.120.126.34		147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
46.19.85.177	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
213.151.37.174	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/registrationwizard/step4.aspx	Block	2
103.194.170.165		147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	2
46.120.103.66	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
185.32.179.229	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
93.173.183.102	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Unknown SSL Session	None	1
46.19.85.234	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
157.55.39.64	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/robots.txt	Block	1
109.65.182.234	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.220.158.115	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to 147.237.0.34/sip_storage/files/4/size220x0/1744.jpg	Block	1
94.159.172.124	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
93.172.163.197	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.117.225.131	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 46.117.225.131	Block	1
130.193.50.31	Russian Federation	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
84.108.116.223	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Unknown SSL Session	None	1
107.178.194.79	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
68.180.228.175	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-9686-he/refuah.aspx	Block	1
213.8.204.83	Israel	147.237.77.74	law.idf.il	PHP Attempt	Block	1
46.120.104.34	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
185.120.125.52		147.237.72.166	aka.idf.il	Double URL Encoding - parameter: search in www.aka.idf.il/main/giyus/pniothandler1.asmx/search	Block	1
93.173.183.102	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Unknown SSL Session	None	1
46.19.86.49	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
157.55.39.114	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 157.55.39.114	Block	1
85.65.164.246	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
79.181.33.77	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
5.255.253.47	Russian Federation	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
109.186.148.163	Israel	147.237.77.216	dover.idf.il	Parameter Type Violation SearchText in www.idf.il/1065-he/dover.aspx	Block	1
94.249.70.250	Jordan	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-ar	Block	1
66.249.78.4	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1437-he/atal.aspx	Block	1