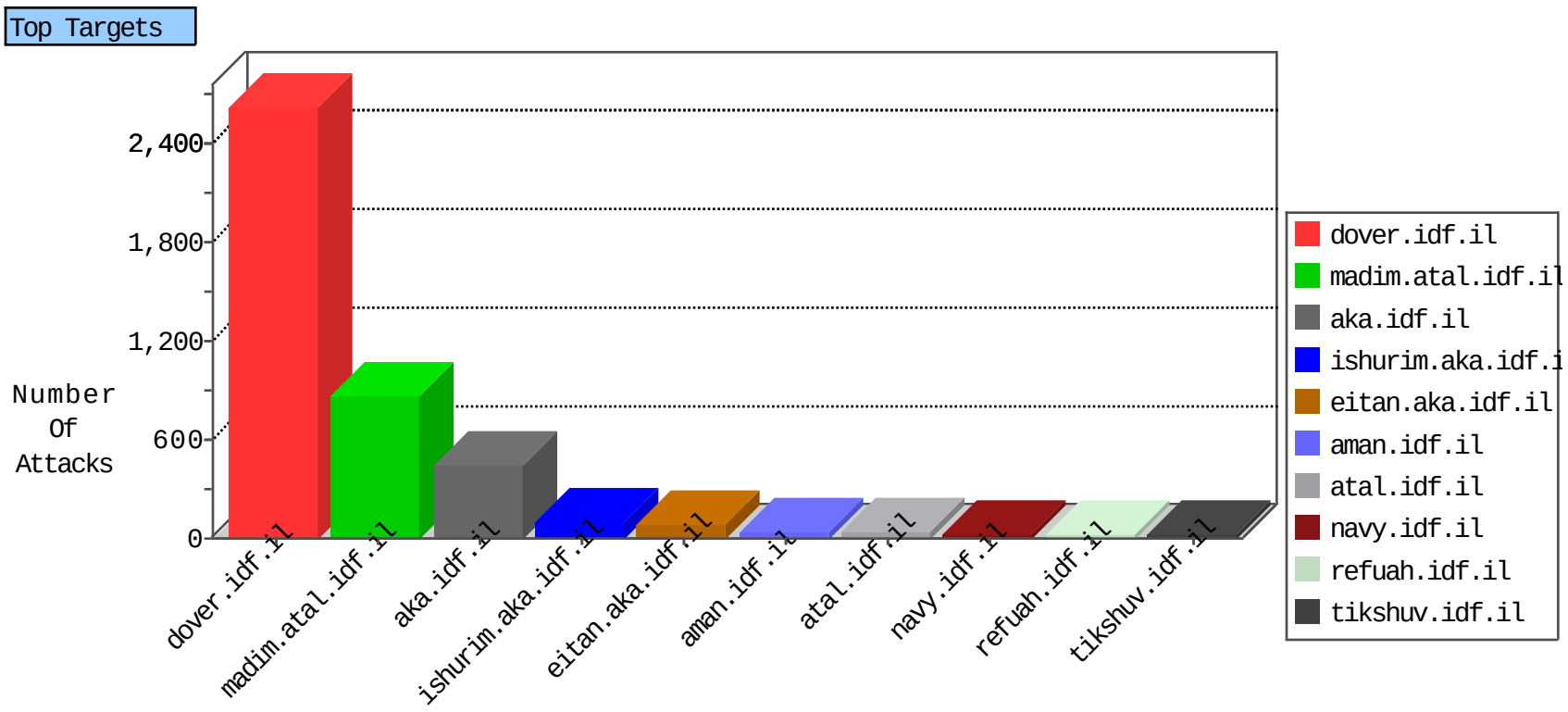
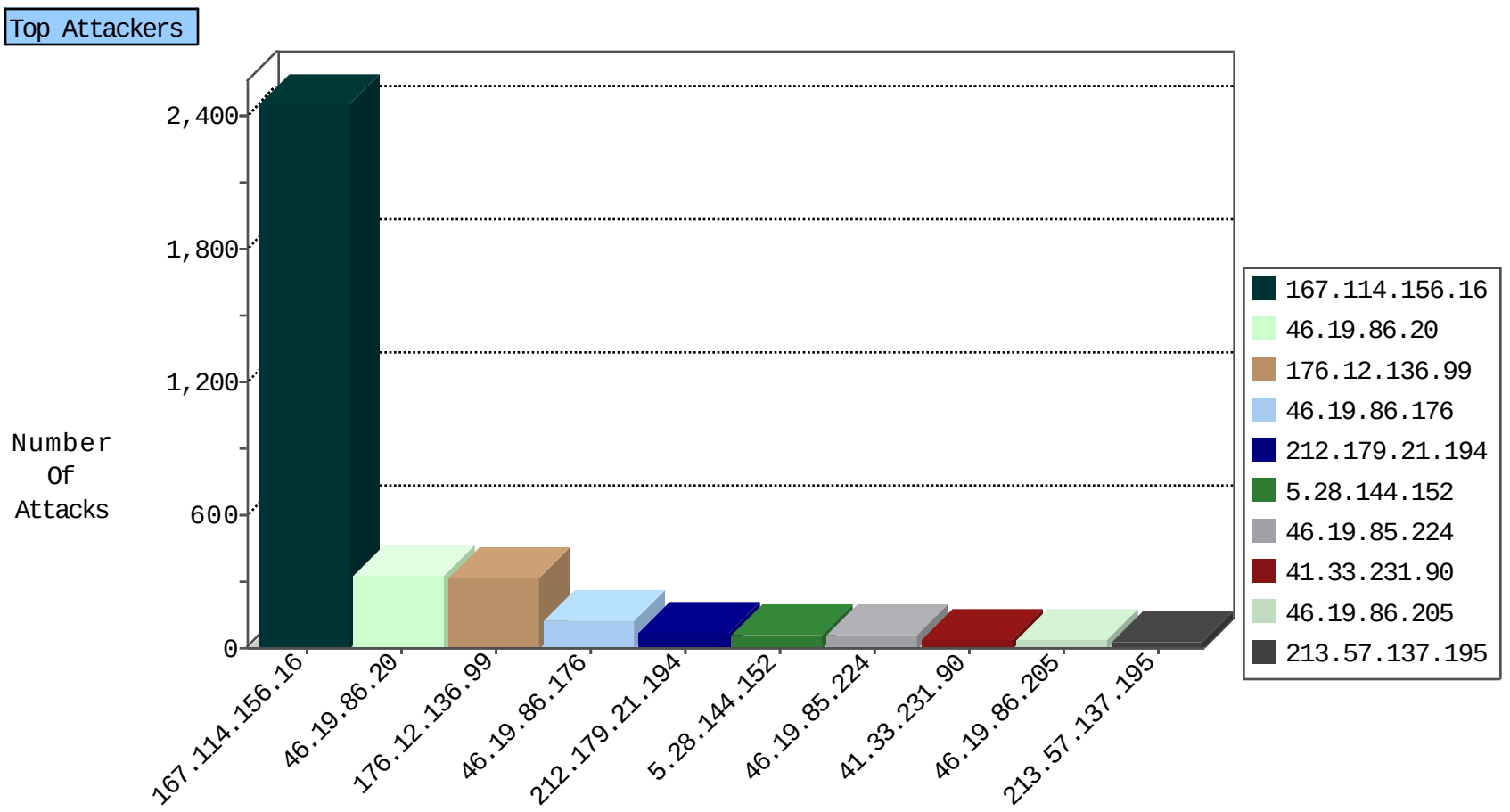
12-06-2015-16:04:00 to 12-06-2015-17:04:00

IDF Under Attack Daily Report





12-06-2015-16:04:00 to 12-06-2015-17:04:00

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	3374
80.179.18.228	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	65
134.147.203.115	Germany	147.237.76.39	mobile.meitav.idf.il	Block_Udp_All_Nets	drop	4
134.147.203.115	Germany	147.237.76.39	mobile.meitav.idf.il	Block_Ntp_All_Net	drop	2
27.154.179.211	China	147.237.76.30	himush.idf.il	Block_Udp_All_Nets	drop	1
167.88.7.246	United States	147.237.77.170	maarachot.idf.il	block-sp-traf1	drop	1
66.240.192.138	United States	147.237.76.177	ncore.idf.il	Block_Ntp_All_Net	drop	1
167.88.7.226	United States	147.237.77.176	matpash.idf.il	block-sp-traf1	drop	1
27.154.179.211	China	147.237.76.31	nakchal.idf.il	Block_Udp_All_Nets	drop	1
167.88.7.239	United States	147.237.76.30	himush.idf.il	block-sp-traf1	drop	1
27.154.179.211	China	147.237.76.176	test.ncore.idf.il	Block_Udp_All_Nets	drop	1
178.35.219.37	Russian Federation	147.237.76.201	e.atal.idf.il	Block_Udp_All_Nets	drop	1
167.88.7.242	United States	147.237.77.234	halag.idf.il	block-sp-traf1	drop	1
37.114.61.24	Germany	147.237.76.148	ggcenter.aka.idf.il	Block_Udp_All_Nets	drop	1

12-06-2015-16:04:00 to 12-06-2015-17:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

12-06-2015-16:04:00 to 12-06-2015-17:04:00

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	3
59.45.79.117	147.237.0.33	China	idf.il	ET SCAN Potential SSH Scan	1
93.172.64.195	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
40.115.58.160	147.237.77.227	United States	e.hamaz.idf.il	ET SCAN NMAP -sS window 1024	1
85.250.76.42	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
82.166.61.181	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.179.164.113	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
62.0.34.177	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
209.126.116.147	147.237.77.178	United States	e.matpash.idf.il	ET SCAN NMAP -sS window 1024	1
59.45.79.117	147.237.77.178	China	e.matpash.idf.il	ET SCAN Potential SSH Scan	1
201.235.215.254	147.237.0.19	Argentina	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
59.45.79.117	147.237.76.148	China	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
192.114.91.248	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
59.45.79.117	147.237.8.50	China	e.tikshuv.idf.il	ET SCAN Potential SSH Scan	1
159.122.238.133	147.237.8.24	Netherlands	e.lifestyle.idf.il	ET SCAN NMAP -sS window 3072	1
46.19.86.104	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
89.103.154.156	147.237.77.216	Czech Republic	dover.idf.il	portscan: TCP Distributed Portscan	1
85.64.147.194	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.183.208.103	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.177.110.113	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
212.179.226.169	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
59.45.79.117	147.237.77.227	China	e.hamaz.idf.il	ET SCAN Potential SSH Scan	1
209.126.116.147	147.237.76.202	United States	e.halag.idf.il	ET SCAN NMAP -sS window 1024	1
59.45.79.117	147.237.77.19	China	law-forum.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.76.86	China	navy.idf.il	ET SCAN Potential SSH Scan	1
187.188.120.123	147.237.77.233	Mexico	atal.idf.il	SERVER-APACHE Apache Tomcat Web Application Manager access	1

12-06-2015-16:04:00 to 12-06-2015-17:04:00

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
212.179.21.194	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	66
46.19.85.224	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	58
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
5.28.144.152	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	29
5.28.144.152	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	28
46.19.86.75	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	20
213.57.137.195	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	15
213.57.137.195	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	12
176.13.22.93	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	11
80.246.137.70	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.121.211.67	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
213.57.143.74	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	8
213.57.143.74	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	8
213.57.143.74	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	7
82.102.169.113	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
46.121.211.67	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
5.28.155.110	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
213.57.128.161	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
5.28.155.110	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
46.19.85.58	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
213.57.14.83	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
143.127.2.4	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
192.118.27.253	Israel	147.237.76.86	navy.idf.il	drop	First packet isn't SYN	drop	6
79.181.162.22	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
31.210.182.86	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.179.140.175	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.182.129.154	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.86.191	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
5.102.254.198	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.143	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
2.54.160.249	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
5.102.254.240	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
77.126.100.25	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
5.28.156.144	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
109.64.111.20	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
81.17.31.222	Switzerland	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
66.249.66.61	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
80.246.138.37	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
5.28.156.144	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
81.17.31.222	Switzerland	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
5.29.130.32	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
93.172.23.181	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
81.17.31.222	Switzerland	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
5.29.130.32	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
213.8.39.41	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
79.182.97.178	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
82.102.169.113	Israel	147.237.72.166	aka.idf.il	SYN Attack		reject	4
108.35.36.164	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
37.26.149.176	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
46.121.140.230	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.12.136.99	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	203
46.19.86.20	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	168
46.19.86.20	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	148
176.12.136.99	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	107
46.19.86.176	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	90
46.19.86.205	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	32
46.19.86.176	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	30
176.13.8.113	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	18
46.19.85.91	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	12
46.19.85.176	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	10
46.19.86.20	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (403)	Block	7
151.55.108.11	Italy	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 151.55.108.11	Block	6
84.111.184.168	Israel	147.237.76.147	chinuch.aka.idf.i	Distributed PHP Attempt	Block	4
84.111.184.168	Israel	147.237.76.147	chinuch.aka.idf.i	Unauthorized URL Access to www.chinuch.aka.idf.il/xmlrpc.php	Block	4
80.246.136.199	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
87.69.39.95	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 87.69.39.95	Block	3
176.12.136.99	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (403) in Session from 176.12.136.99	Block	3
213.8.204.30	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	3
109.186.4.98	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 109.186.4.98	Block	3
2.54.8.27	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.120.216.14	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.85.229	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
66.249.81.212	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
2.54.31.70	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.22.66	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
84.109.24.50	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
87.109.178.201	Saudi Arabia	147.237.77.216	dover.idf.il	PHP Attempt	Block	2
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	2
212.179.21.194	Israel	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to www.eitan.aka.idf.il/shared/ajax/lightboxmediagallery.aspx	Block	2
87.109.178.201	Saudi Arabia	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/xmlrpc.php	Block	2
79.182.97.178	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
91.143.80.201	Germany	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	2
77.126.215.173	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/international_training	Block	2
213.8.204.37	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 213.8.204.37	Block	2
2.54.176.74	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
79.183.185.157	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
185.32.179.28	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
2.54.37.57	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	2
82.166.197.58	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/7/	Block	2
79.179.20.100	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
176.13.22.93	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
46.19.85.175	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.66.31	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
176.12.136.99	Israel	147.237.0.19	madim.atal.idf.il	Too Many 403: Response Code per Session	Block	1
31.154.253.28	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/ ×˜×¤×¡×™×?	Block	1
85.65.221.31	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	1
2.52.157.134	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
84.109.24.50	Israel	147.237.0.19	madim.atal.idf.il	Double URL Encoding - parameter: ReturnUrl in madim.atal.idf.il/login.aspx	Block	1
208.184.112.74	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
46.19.86.253	Israel	147.237.76.42	refuah.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtLastName in www.refua.atal.idf.il/1518-he/refuah.aspx	Block	1