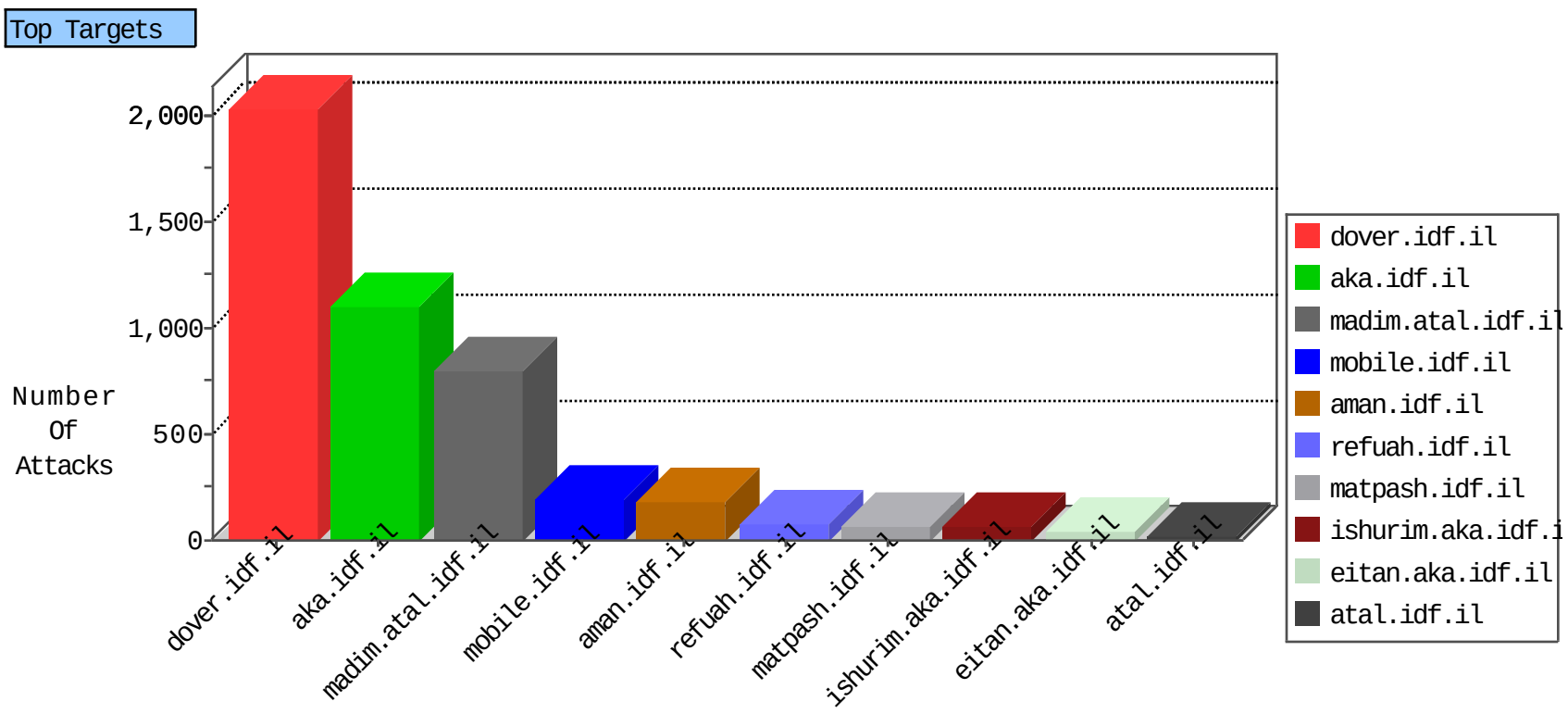
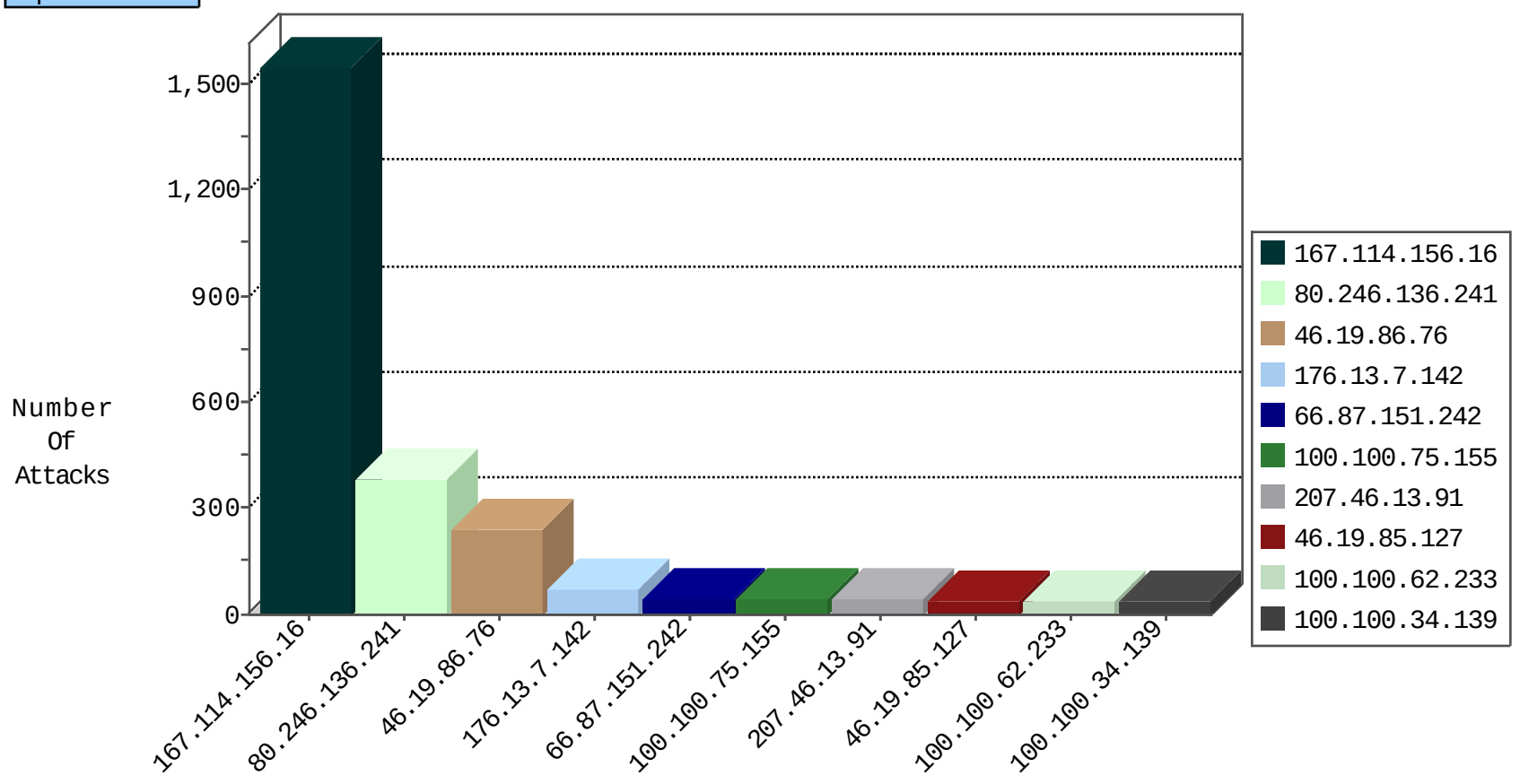
11-29-2015-17:04:01 to 11-29-2015-18:04:01

IDF Under Attack
Daily Report

Top Targets



Top Attackers



11-29-2015-17:04:01 to 11-29-2015-18:04:01

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.66.33	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	6464
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	3617
81.218.241.26	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	101
66.249.66.125	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	43
66.249.81.215	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	12
66.249.81.218	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	12
37.26.148.222	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	8
199.30.25.73	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	5
66.249.81.212	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
79.180.134.246	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
65.19.138.33	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
134.147.203.115	Germany	147.237.76.39	mobile.meitav.idf.il	Block_Ntp_All_Net	drop	2
52.16.5.197	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	2
46.166.188.68	Netherlands	147.237.76.38	e.e.meitav.idf.il	Block_Udp_All_Nets	drop	1
90.188.117.75	Russian Federation	147.237.76.197	e.himush.idf.il	Block_Udp_All_Nets	drop	1
67.79.13.53	United States	147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	1
115.230.124.164	China	147.237.77.216	dover.idf.il	block-sp-traf1	drop	1

11-29-2015-17:04:01 to 11-29-2015-18:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
77.127.144.47	Israel	147.237.77.170	maarachot.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
188.165.15.238	France	147.237.76.31	nakchal.idf.il	C228: HTTP: AhrefBot crawler	Block	1

11-29-2015-17:04:01 to 11-29-2015-18:04:01

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	2
185.120.126.34	147.237.77.216		dover.idf.il	portscan: TCP Distributed Portscan	2
167.114.156.16	147.237.77.216	Canada	dover.idf.il	portscan: TCP Distributed Portscan	1
82.80.196.44	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.179.99.45	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
62.219.191.152	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
31.6.71.154	147.237.0.33	Poland	idf.il	ET SCAN NMAP -sS window 1024	1
212.143.221.168	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
89.138.177.27	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
80.246.136.241	147.237.0.19	Israel	madim.atal.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	1
66.249.64.254	147.237.77.233	United States	atal.idf.il	ET SCAN NMAP -sA (2)	1
62.209.8.197	147.237.77.216	Bahrain	dover.idf.il	portscan: TCP Distributed Portscan	1
2.52.138.84	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

11-29-2015-17:04:01 to 11-29-2015-18:04:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
100.100.75.155		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	43
100.100.62.233		147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	39
100.100.34.139		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	38
46.19.86.78	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	37
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	32
79.182.222.209	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	27
207.46.13.91	United States	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	26
100.100.113.150		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	25
66.87.151.242	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	25
65.49.14.150	Anonymous Proxy	147.237.76.42	refuah.idf.il	drop		drop	24
213.57.134.121	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	23
100.100.116.240		147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	22
46.19.85.17	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
66.87.151.242	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	19
109.67.52.198	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
213.57.131.247	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	17
46.19.86.145	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
207.46.13.91	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
100.100.112.139		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	15
2.54.179.209	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
176.13.7.86	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	14
100.100.0.69		147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	14
100.100.28.123		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	14
213.57.133.125	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	14
37.26.147.165	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	14
176.13.5.222	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	14
46.43.77.226	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	12
2.54.55.36	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	12
37.26.146.221	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
100.100.28.123		147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	12
176.12.140.224	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
100.100.68.210		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	12
79.182.213.190	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
100.100.90.140		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	12
37.26.146.140	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
176.12.142.34	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
176.13.16.226	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	11
2.52.187.236	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	11
213.57.131.247	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	10
46.19.86.189	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
46.117.8.131	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	10
176.13.13.150	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
46.117.8.131	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
185.18.206.194	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
2.54.188.254	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
136.243.36.96	Germany	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
2.54.136.32	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.85.239	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
79.182.2.131	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	9

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
80.246.136.241	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	219
46.19.86.76	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	128
80.246.136.241	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	116
46.19.86.76	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	112
176.13.7.142	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	65
80.246.136.241	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (403)	Block	44
46.19.85.127	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	31
46.19.85.107	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	29
46.19.85.86	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	26
37.26.147.217	Israel	147.237.77.243	mobile.idf.il	Distributed Parameter Type Violation on mobile.idf.il/sachar/changepassword parameter CurrentPassword	Block	15
176.13.7.86	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	6
176.13.18.224	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	6
46.19.85.17	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	5
84.109.90.213	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ufi/reaction/	Block	4
2.54.179.209	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	4
37.142.242.250	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ufi/reaction/	Block	4
202.191.63.147	Australia	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	3
109.67.81.162	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
199.7.108.230	United States	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	3
185.3.146.241	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ufi/reaction/	Block	3
69.27.102.9	Canada	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	3
66.249.66.61	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
173.254.55.137	United States	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	3
176.13.13.150	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
91.207.158.161	Norway	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	3
82.80.142.40	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ufi/reaction/	Block	3
69.27.102.9	Canada	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	3
104.44.135.149	United States	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	3
193.28.176.217	United Kingdom	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	3
77.127.231.214	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Unknown SSL Session	None	3
104.44.135.149	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 104.44.135.149	Block	3
69.27.102.9	Canada	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 69.27.102.9	Block	3
185.11.164.12	Portugal	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	3
203.162.53.47	Vietnam	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	3
58.96.19.246	Australia	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	3
69.27.102.9	Canada	147.237.77.216	dover.idf.il	Distributed Admin Blocking	Block	2
193.28.176.217	United Kingdom	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/index.php	Block	2
5.28.189.168	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
173.254.55.137	United States	147.237.77.216	dover.idf.il	Distributed Admin Blocking	Block	2
46.116.131.217	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
136.243.36.96	Germany	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
208.184.112.75	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	2
91.207.158.161	Norway	147.237.77.176	matpash.idf.il	Distributed Admin Blocking	Block	2
37.26.146.221	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
2.54.136.32	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
79.180.10.221	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ufi/reaction/	Block	2
46.19.85.134	Israel	147.237.72.166	aka.idf.il	Distributed Parameter Read Only Violation www.aka.idf.il/main/sachar/registrationwizard/register.aspx parameter	None	2
77.126.151.156	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation Password in mobile.idf.il/sachar/login	Block	2
203.162.53.47	Vietnam	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/index.php	Block	2
37.142.68.16	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ufi/reaction/	Block	2