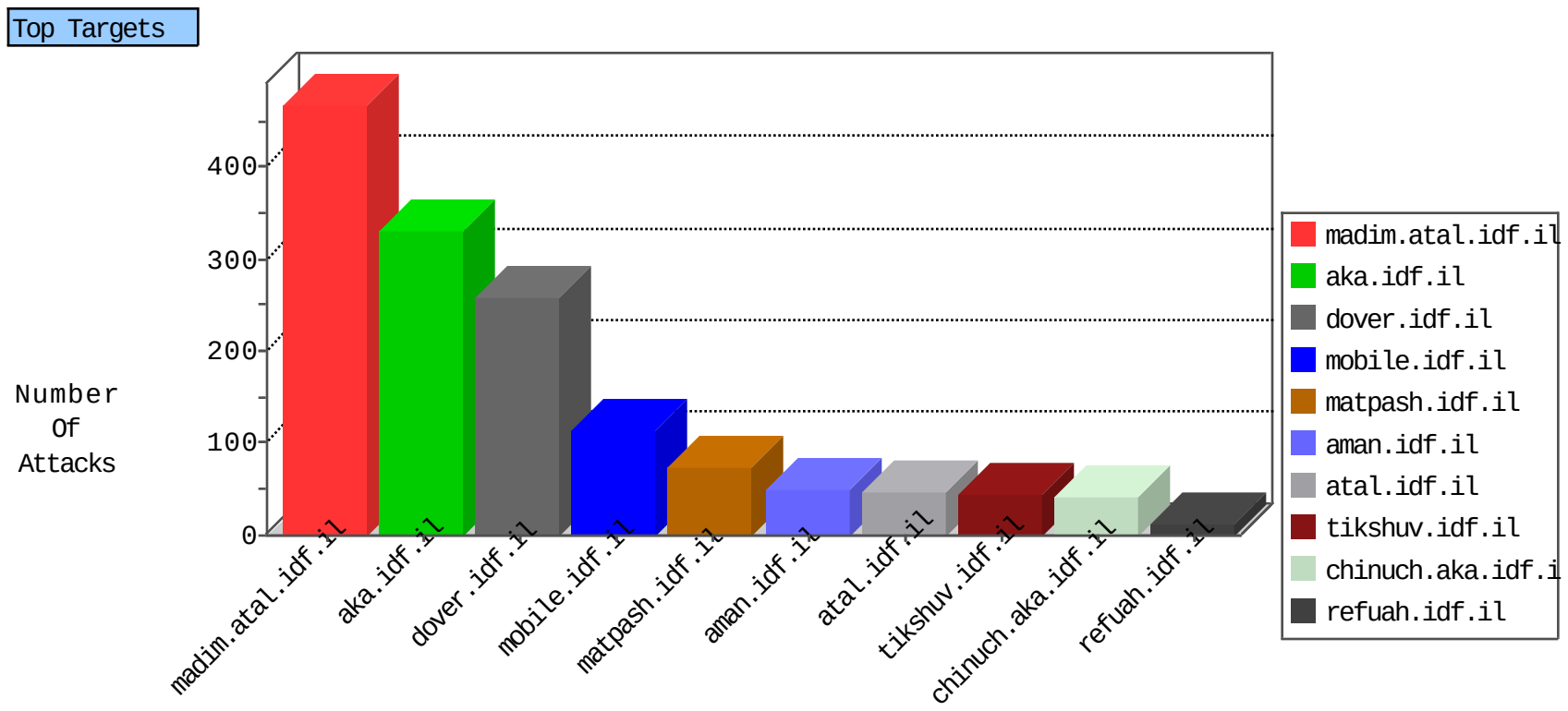
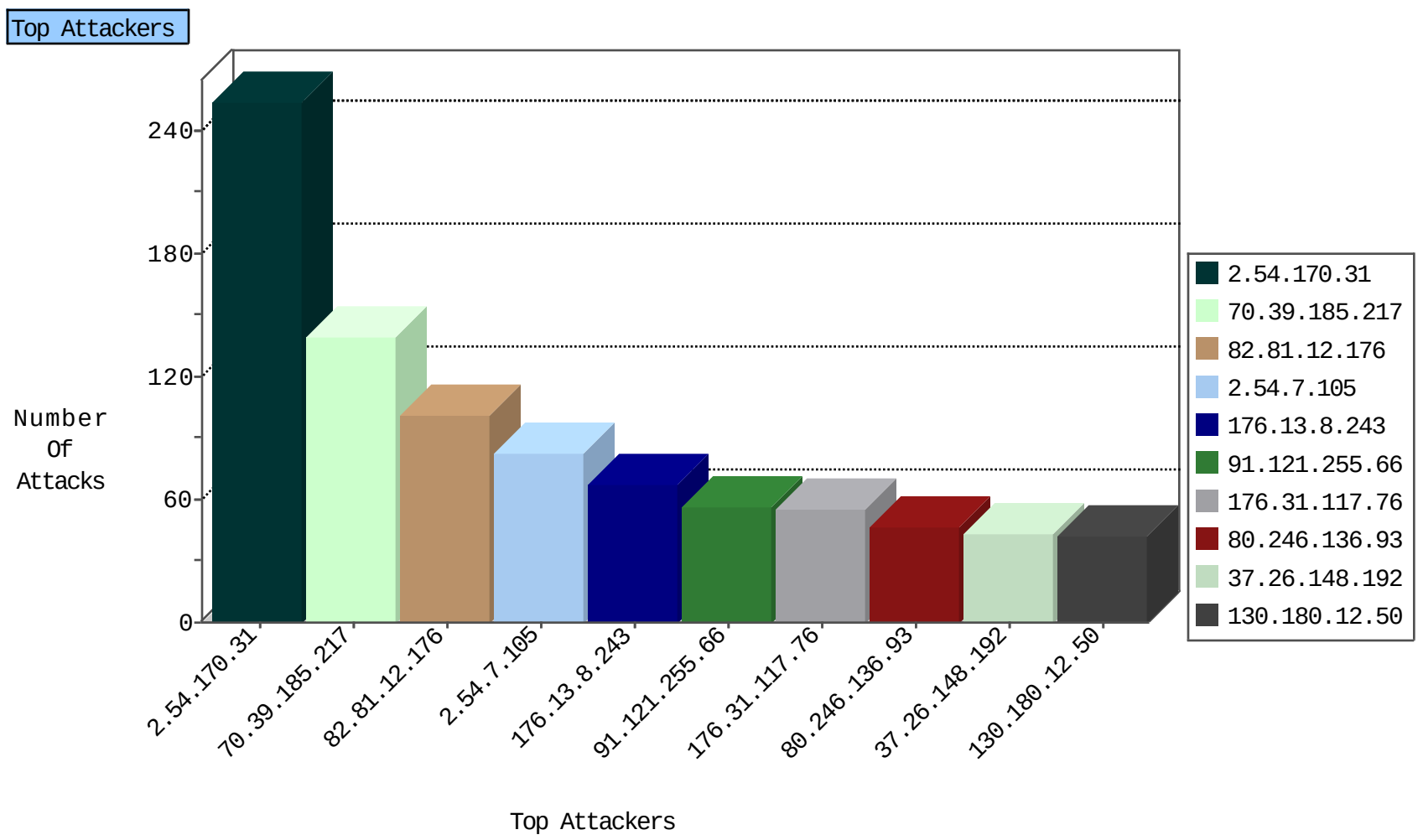
01-29-2016-09:04:05 to 01-29-2016-10:04:05

IDF Under Attack Daily Report

Top Targets



Top Attackers



01-29-2016-09:04:05 to 01-29-2016-10:04:05

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
82.81.12.176	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	101
204.42.253.2	United States	147.237.76.148	gqcenter.aka.idf.il	Block_Ntp_All_Net	drop	2
70.39.185.217	Satellite Provider	147.237.77.216	dover.idf.il	F_Dover_Under_Attack_Con_Http	drop	2
217.146.91.36	United Kingdom	147.237.76.196	e.sviva.idf.il	Block_Udp_All_Nets	drop	1

01-29-2016-09:04:05 to 01-29-2016-10:04:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
86.62.73.199	Russian Federation	147.237.77.216	dover.idf.il	C008: HTTP: Xenu UserAgent	Block	1
71.170.23.126	United States	147.237.77.216	dover.idf.il	C008: HTTP: Xenu UserAgent	Block	1
86.62.73.199	Russian Federation	147.237.77.176	matpash.idf.il	C008: HTTP: Xenu UserAgent	Block	1

01-29-2016-09:04:05 to 01-29-2016-10:04:05

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
130.180.12.50	147.237.77.233	Germany	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	4
182.18.160.216	147.237.0.17	India	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	3
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	2
66.249.78.254	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
182.18.160.216	147.237.0.35	India	akaws.idf.il	ET SCAN Potential SSH Scan	2
94.76.11.255	147.237.72.14	Bahrain	dover.idf.il(old)	ET SCAN NMAP -sS window 1024	2
193.105.134.220	147.237.76.177	Sweden	ncore.idf.il	ET SCAN NMAP -sS window 1024	1
37.143.82.50	147.237.0.19	Netherlands	madim.atal.idf.il	ET SCAN NMAP -sS window 4096	1
183.60.109.43	147.237.76.198	China	e.yohalan.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
183.60.109.43	147.237.76.147	China	chinuch.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
183.60.109.43	147.237.0.34	China	tikshuv.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
223.4.174.30	147.237.76.202	China	e.halag.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
177.206.68.6	147.237.76.30	Brazil	himush.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
223.4.174.30	147.237.76.177	China	ncore.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
199.191.56.188	147.237.0.15	United States	kosher-kravi.idf.il	ET SCAN NMAP -sS window 4096	1
91.201.236.114	147.237.77.216	Ukraine	dover.idf.il	ET SCAN NMAP -sS window 1024	1
185.112.102.144	147.237.0.200		m4u.idf.il	ET SCAN Potential SSH Scan	1
37.143.82.50	147.237.0.19	Netherlands	madim.atal.idf.il	ET SCAN NMAP -sS window 3072	1
183.60.109.43	147.237.76.177	China	ncore.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
183.60.109.43	147.237.76.86	China	navy.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
182.18.160.216	147.237.0.15	India	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
223.4.174.30	147.237.76.200	China	eitan.aka.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
168.62.238.153	147.237.8.14	United States	e.orchot.idf.il	ET SCAN NMAP -sS window 1024	1
223.4.174.30	147.237.76.86	China	navy.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
198.20.69.74	147.237.76.39	United States	mobile.meitav.idf.il	ET DROP Dshield Block Listed Source	1
91.201.236.114	147.237.77.216	Ukraine	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1

01-29-2016-09:04:05 to 01-29-2016-10:04:05

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
70.39.185.217	Satellite Provid	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	70
70.39.185.217	Satellite Provid	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	67
176.31.117.76	France	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	55
37.26.148.192	Israel	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	43
130.180.12.50	Germany	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	36
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
2.54.7.105	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	31
91.121.255.66	France	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	25
109.253.199.6	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
91.121.255.66	France	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	21
2.54.7.105	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	13
2.54.7.105	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	13
2.54.7.105	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	13
2.54.7.105	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	12
84.94.22.166	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
109.253.145.212	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.86.82	Israel	147.237.76.147	chinuch.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
213.57.63.143	Israel	147.237.77.243	mobile.idf.il	drop	First packet isn't SYN	drop	8
62.219.146.214	Israel	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
91.121.255.66	France	147.237.76.147	chinuch.aka.idf.il	SYN Attack		reject	7
46.19.86.145	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.150	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
37.26.148.247	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
141.8.183.16	Russian Federation	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	6
5.28.158.181	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
80.246.130.56	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
46.19.85.151	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.151	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
79.182.48.54	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
84.228.79.91	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.26.146.210	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.245	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
2.52.168.83	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
77.126.30.193	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.150	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
5.102.254.148	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
79.177.183.156	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
81.218.156.204	Israel	147.237.77.226	www.chamatz.aka.idf.il	drop	First packet isn't SYN	drop	4
46.120.92.244	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
31.210.186.135	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
212.199.57.200	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	3
2.54.24.217	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
77.126.100.125	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
94.230.86.153	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
176.13.13.216	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.178.113.53	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
91.121.255.66	France	147.237.72.156	aman.idf.il	SYN Attack		reject	3

01-29-2016-09:04:05 to 01-29-2016-10:04:05

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.54.170.31	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	147
2.54.170.31	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	107
176.13.8.243	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	67
80.246.136.93	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	33
85.65.71.95	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	21
2.54.159.27	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	19
80.246.137.252	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	18
164.138.113.229	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	14
80.246.136.93	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	13
149.88.197.175	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation Password in mobile.idf.il/sachar/login	Block	7
79.181.221.2	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
176.13.3.144	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 176.13.3.144	Block	5
109.253.199.6	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	5
84.108.66.146	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	4
109.253.138.255	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
5.29.159.185	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
84.94.22.166	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
109.67.51.58	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
176.13.9.116	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
46.19.85.175	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
5.29.46.63	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
80.246.137.229	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
77.126.30.193	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
84.108.235.32	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 84.108.235.32	Block	2
176.13.3.144	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1465	Block	2
46.19.86.45	Israel	147.237.77.243	mobile.idf.il	Distributed Parameter Type Violation on mobile.idf.il/sachar/login parameter Password	Block	2
213.151.44.152	Israel	147.237.76.42	refuah.idf.il	Multiple Unauthorized URL Access from 213.151.44.152	Block	2
79.179.32.4	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
2.54.130.9	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
109.253.137.106	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.78.82	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/templates/shared/usercontrols/lobbyinfocenteritem/	Block	1
213.151.44.152	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/&sa=u&ved=0ahukewjy1lbhws7kahwhmhokht_lcbaqfggimaa&usg=afqjcnhsjqzgxohl-8ga1aemjbw8wkvaxw	Block	1
176.13.18.174	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/nekudot/index	Block	1
46.117.243.209	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
107.178.194.79	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
84.108.66.146	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/nekudot/index	Block	1
31.154.94.81	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/faq.aspx	Block	1
204.13.201.138	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.78.159	Block	1
46.19.86.44	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Unknown SSL Session	None	1
85.65.168.92	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
5.29.101.135	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/https:/www.aman.idf.il/	Block	1
193.90.12.89	Norway	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
79.176.10.225	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
155.254.203.127	Tajikistan	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/hebrew/main.asp	Block	1
107.178.194.87	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
66.249.64.48	Israel	147.237.77.170	maarachot.idf.il	Multiple Unauthorized URL Access from 66.249.64.48	Block	1
37.142.163.210	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
208.184.112.74	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
79.182.235.19	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1

01-29-2016-09:04:05 to 01-29-2016-10:04:05