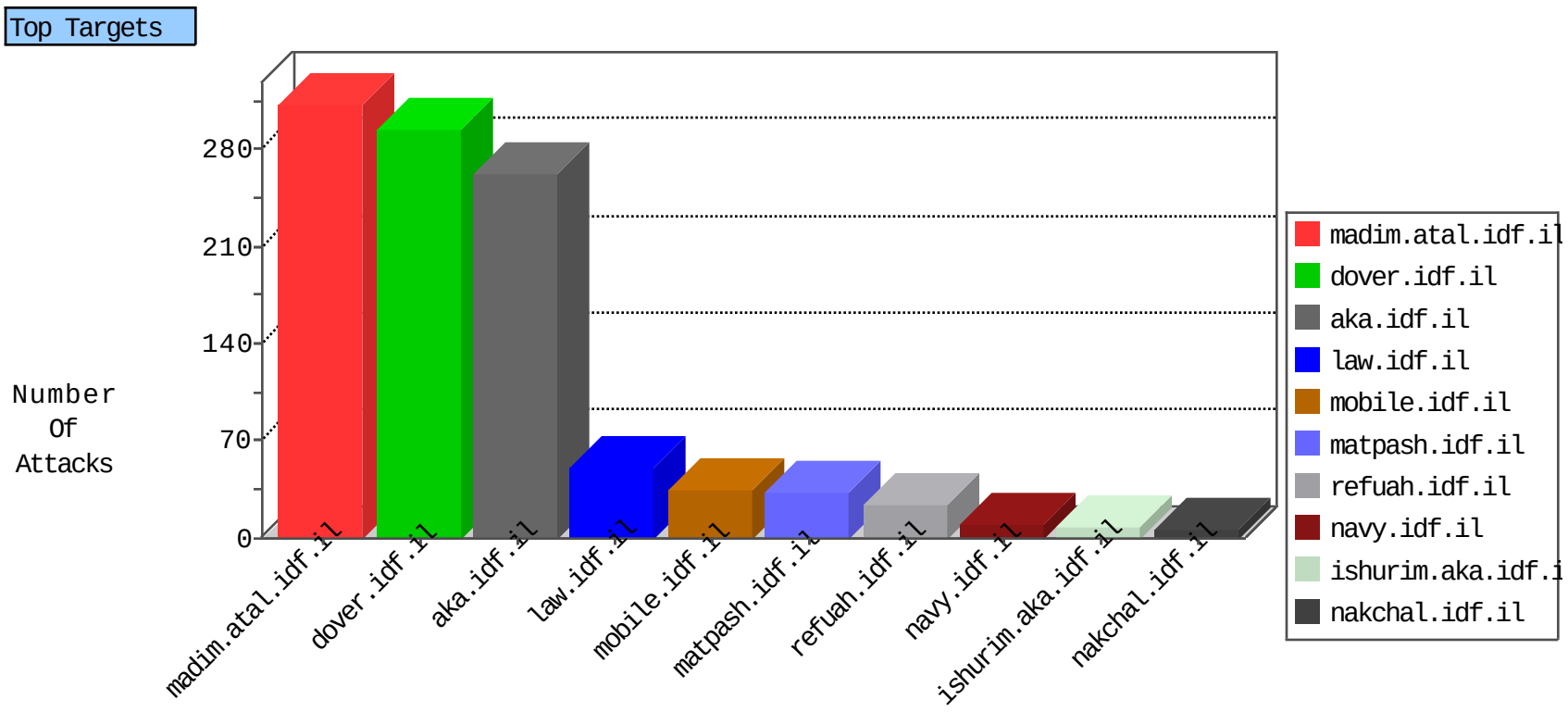
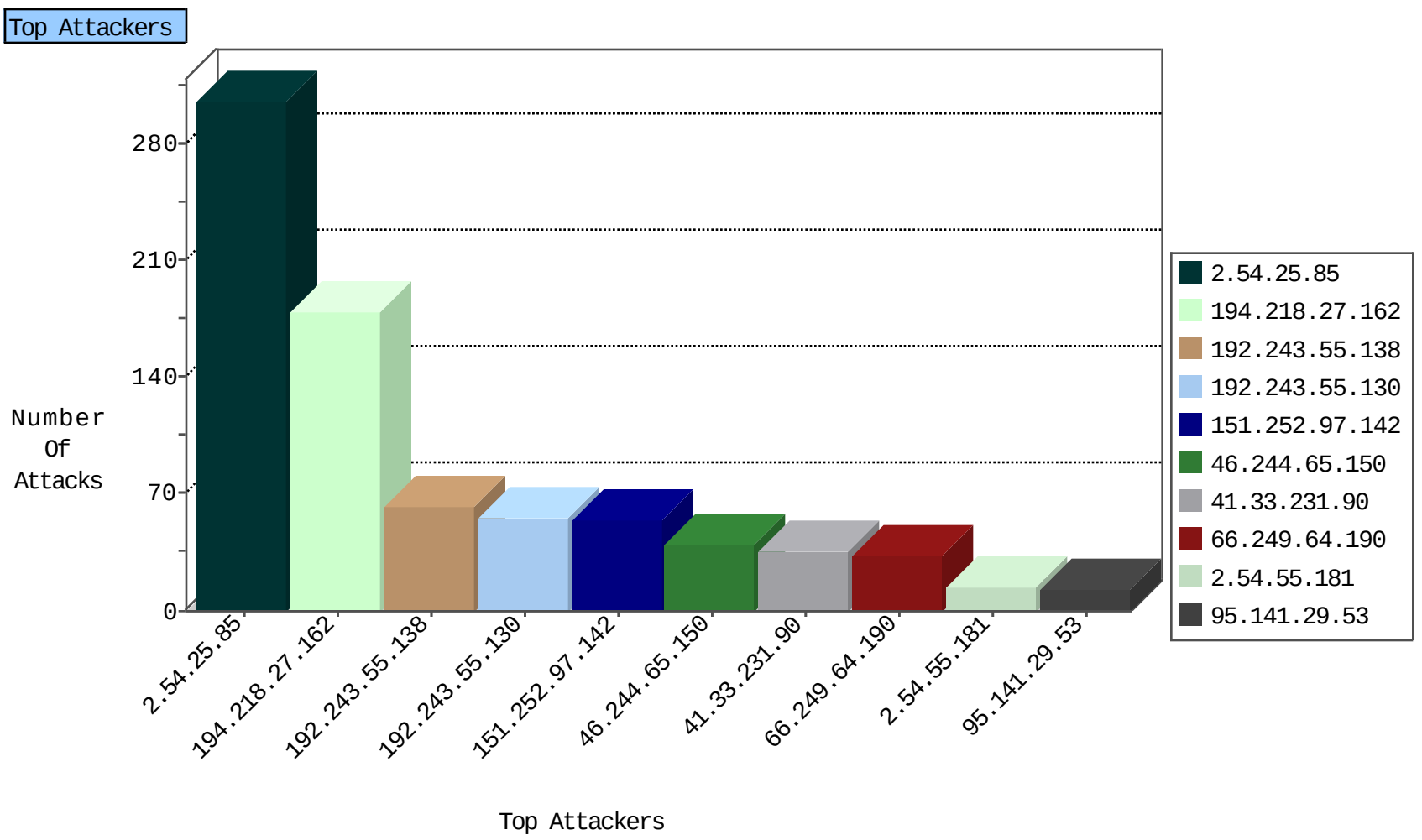
03-03-2016-00:04:09 to 03-03-2016-01:04:09

IDF Under Attack Daily Report

Top Targets



Top Attackers



03-03-2016-00:04:09 to 03-03-2016-01:04:09

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.244.65.150	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	DOS-LOIC-TCP-80-dun	dest-reset	25
46.244.65.150	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	14
79.177.116.56	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	6
81.218.65.210	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	6
192.81.214.156	United States	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	5
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
192.171.18.125		147.237.77.205	prisha.idf.il	Block_Ntp_All_Net	drop	1
185.130.5.246		147.237.72.166	aka.idf.il	Block_Ntp_All_Net	drop	1
42.112.10.80	Vietnam	147.237.72.167	ishurim.aka.idf.il	Invalid TCP Flags	drop	1
42.112.10.73	Vietnam	147.237.72.167	ishurim.aka.idf.il	Invalid TCP Flags	drop	1
185.130.5.246		147.237.76.200	eitan.aka.idf.il	Block_Ntp_All_Net	drop	1
42.112.10.65	Vietnam	147.237.72.167	ishurim.aka.idf.il	Invalid TCP Flags	drop	1
192.171.18.125		147.237.76.196	e.sviva.idf.il	Block_Ntp_All_Net	drop	1
42.112.10.74	Vietnam	147.237.72.167	ishurim.aka.idf.il	Invalid TCP Flags	drop	1
185.130.5.246		147.237.76.201	e.atal.idf.il	Block_Ntp_All_Net	drop	1
42.112.10.66	Vietnam	147.237.72.167	ishurim.aka.idf.il	Invalid TCP Flags	drop	1
192.171.18.125		147.237.76.198	e.yohalan.idf.il	Block_Ntp_All_Net	drop	1
185.130.5.246		147.237.8.27	e.madim.atal.idf.il	Block_Ntp_All_Net	drop	1
42.112.10.75	Vietnam	147.237.72.167	ishurim.aka.idf.il	Invalid TCP Flags	drop	1
185.130.5.246		147.237.77.216	dover.idf.il	Block_Ntp_All_Net	drop	1
42.112.10.70	Vietnam	147.237.72.167	ishurim.aka.idf.il	Invalid TCP Flags	drop	1

03-03-2016-00:04:09 to 03-03-2016-01:04:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
61.135.189.119	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	4
31.154.163.198	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
144.76.30.236	Germany	147.237.76.31	nakchal.idf.il	C1000074: HTTP: majestic bot	Block	2
144.76.30.236	Germany	147.237.77.74	law.idf.il	C1000074: HTTP: majestic bot	Block	2
94.159.149.181	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
144.76.30.236	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
106.38.241.106	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
123.126.113.80	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1

03-03-2016-00:04:09 to 03-03-2016-01:04:09

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
61.153.237.122	147.237.76.148	China	gqcenter.aka.idf.il	GPL SCAN nmap TCP	2
60.12.88.242	147.237.76.148	China	gqcenter.aka.idf.il	GPL SCAN nmap TCP	2
61.240.144.66	147.237.77.227	China	e.hamaz.idf.il	ET SCAN NMAP -sS window 1024	1
27.221.10.43	147.237.76.199	China	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
201.172.109.61	147.237.8.14	Mexico	e.orchot.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
175.139.165.68	147.237.76.30	Malaysia	himush.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
137.226.113.7	147.237.76.42	Germany	refuah.idf.il	ET SCAN Suspicious User-Agent Containing Web Scan/er, Likely Web Scanner	1
81.27.85.28	147.237.76.42	United Kingdom	refuah.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.66	147.237.76.31	China	nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
218.246.0.97	147.237.0.17	China	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
201.42.42.106	147.237.76.34	Brazil	yohalan.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
175.139.165.68	147.237.0.34	Malaysia	tikshuv.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
137.226.113.7	147.237.76.31	Germany	nakchal.idf.il	ET SCAN Suspicious User-Agent Containing Web Scan/er, Likely Web Scanner	1

03-03-2016-00:04:09 to 03-03-2016-01:04:09

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
194.218.27.162	Sweden	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	120
194.218.27.162	Sweden	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	60
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
151.252.97.142	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	17
151.252.97.142	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	16
66.249.64.190	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	16
151.252.97.142	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	13
95.141.29.53	Luxembourg	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	12
192.243.55.138	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	10
92.236.75.7	United Kingdom	147.237.77.216	dover.idf.il	drop	SAM rule	drop	9
192.243.55.138	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
192.243.55.138	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	9
192.243.55.130	Dominica	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
151.252.97.142	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	8
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
77.126.151.206	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
192.243.55.138	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
37.26.147.146	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
80.246.136.181	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
87.68.251.80	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
192.243.55.130	Dominica	147.237.77.176	matpash.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
192.243.55.130	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
82.81.81.218	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.55.181	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
192.243.55.138	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
192.243.55.130	Dominica	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
192.243.55.138	Dominica	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
192.243.55.130	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.85.228	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
192.243.55.130	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
188.161.52.153	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
192.243.55.130	Dominica	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
46.19.85.149	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
192.243.55.138	Dominica	147.237.77.176	matpash.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
5.22.131.29	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
2.54.55.181	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
192.243.55.130	Dominica	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	4
192.243.55.130	Dominica	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
141.8.132.112	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
188.120.148.199	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
37.26.147.146	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	alert	3
79.183.18.32	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
84.228.193.66	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.176.103.99	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
77.127.14.137	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.55.181	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
46.19.86.204	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.66.182.243	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
192.243.55.138	Dominica	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
79.179.208.103	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3

03-03-2016-00:04:09 to 03-03-2016-01:04:09

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.54.25.85	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	306
66.249.64.190	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.64.190	Block	14
66.249.66.76	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
46.19.85.124	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.19.56	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
66.249.66.75	United States	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 66.249.66.75	Block	2
37.26.148.198	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	2
66.249.66.72	United States	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 66.249.66.72	Block	2
66.249.64.190	United States	147.237.72.166	aka.idf.il	PHP Attempt	Block	1
192.243.55.130	Dominica	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/templates/getfile/getfile.aspx?filename=xgf5b3nolwrvy3ncdghpa2fcbwvzahvsyxzcbwvryxjrzwlux3jpc2h1bvwxlnbkzg==&infocenteritem=true	Block	1
82.81.55.161	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
213.8.204.49	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/mas.aspx	None	1
109.66.202.238	Israel	147.237.77.243	mobile.idf.il	Untraceable SSL Sessions: Open Mode	None	1
71.43.100.242	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/).html(	Block	1
66.249.64.190	United States	147.237.72.166	aka.idf.il	Unknown Parameter cat.. in www.aka.idf.il/main/drushim/misrot.aspx	None	1
194.72.238.241	United Kingdom	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/xyzzy	Block	1
82.81.81.218	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
66.249.66.75	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/giyus/forum/asp/showforum.asp	Block	1
37.60.47.124	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/faq.aspx	Block	1
137.226.113.7	Germany	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/	Block	1
77.126.151.206	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	1
66.249.64.190	United States	147.237.72.166	aka.idf.il	Unknown Parameter d.. in www.aka.idf.il/giyus/general/	None	1
199.30.24.112	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
5.102.232.209	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/markiveysachar.aspx	None	1
95.141.29.53	Luxembourg	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
79.179.161.71	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files	Block	1
66.249.64.234	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/926-he/atal.aspx	Block	1
207.46.13.51	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/news/news.aspx	Block	1
37.26.147.146	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
107.150.42.36	United States	147.237.76.39	mobile.meitav.idf.il	Unauthorized URL Access to www.yun.ph/	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1381-he/dover.aspx	Block	1
188.43.123.70	Russian Federation	147.237.77.216	dover.idf.il	Parameter Type Violation SearchText in www.idf.il/1065-en/dover.aspx	Block	1
80.246.136.181	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
37.26.147.242	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/shared/clientscripts/jquery/jquery-1.4.2.min.js	Block	1
207.46.13.74	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/dynamic_map/dynamic_map.aspx	Block	1
108.30.58.92	United States	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	1
68.180.230.29	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/901-he/cogat.aspx	Block	1

03-03-2016-00:04:09 to 03-03-2016-01:04:09