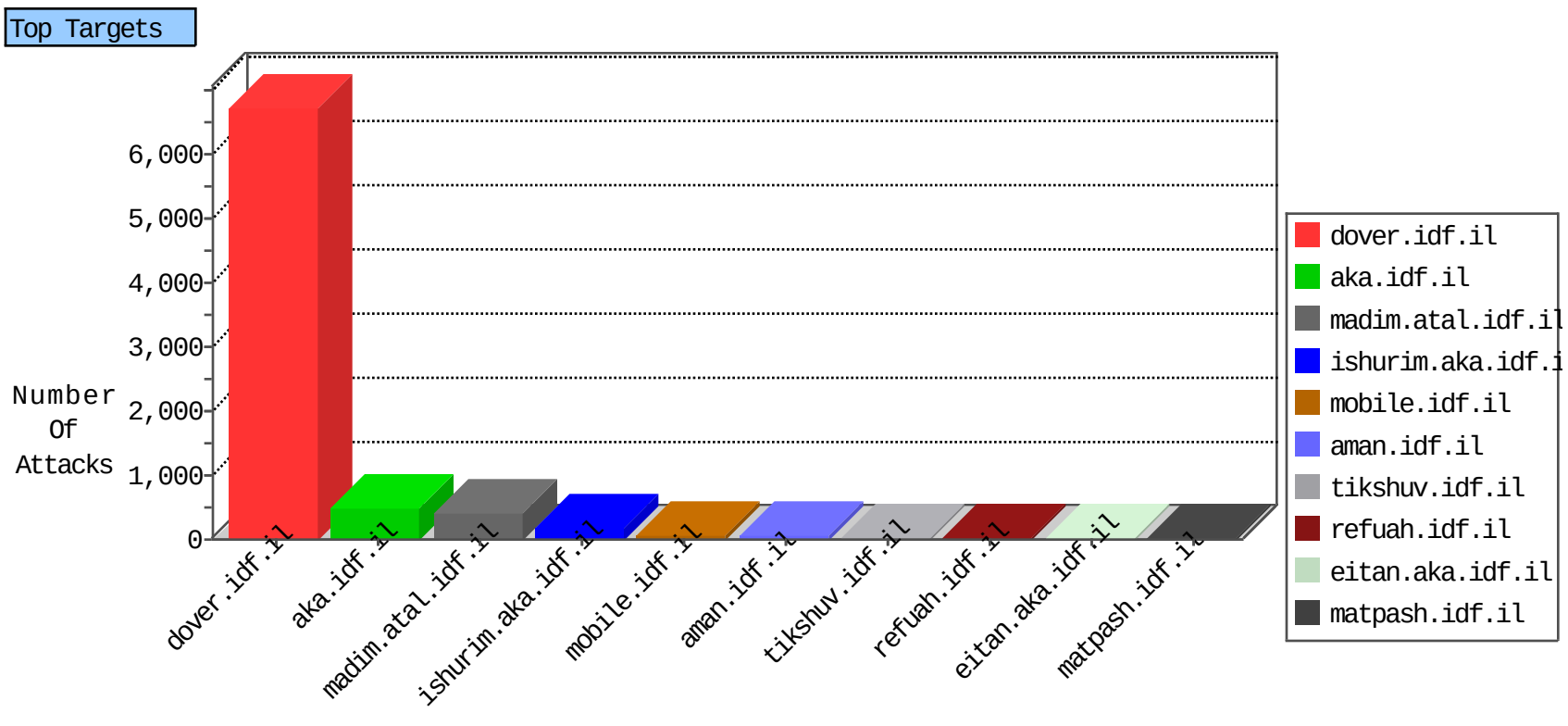
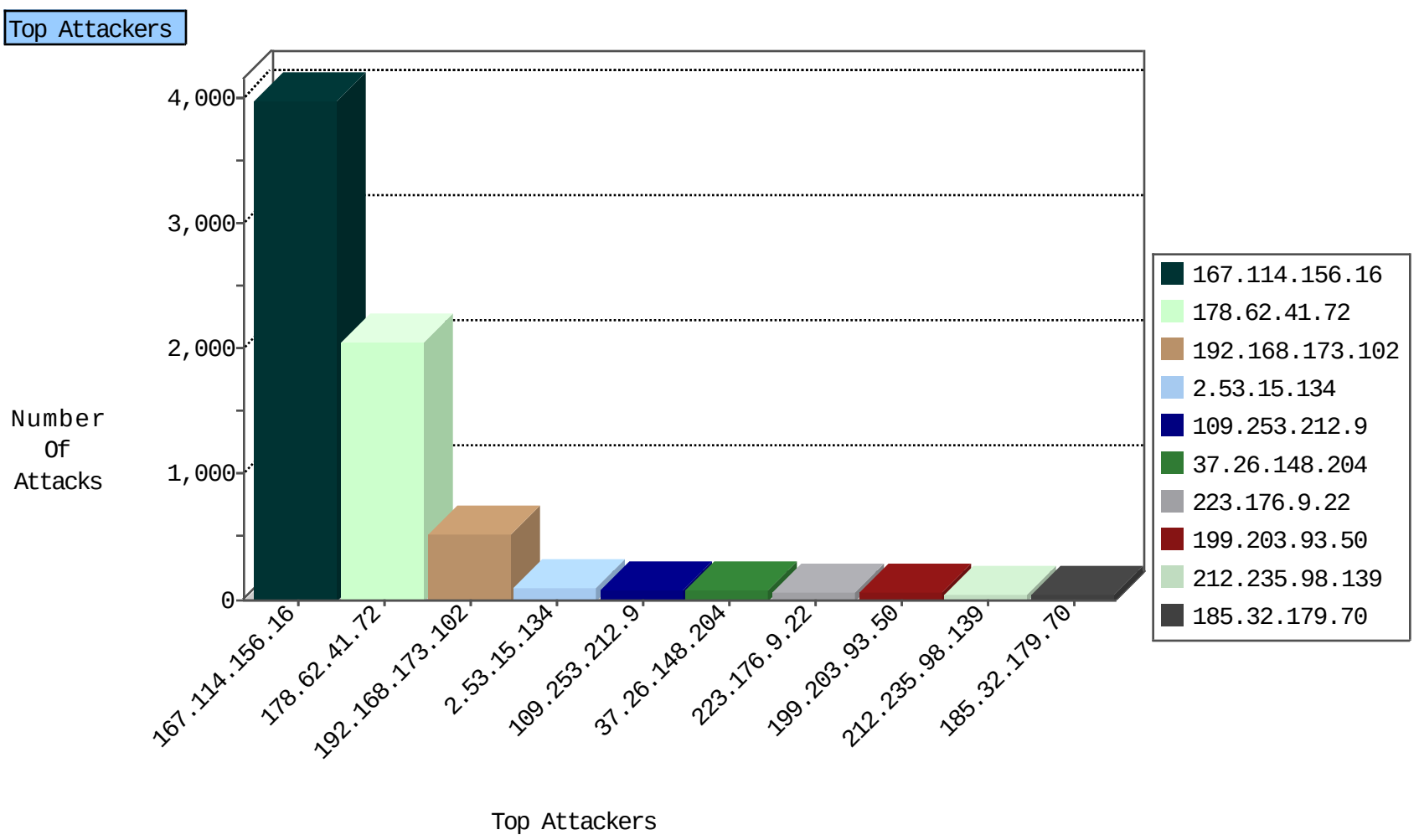
04-10-2016-13:04:08 to 04-10-2016-14:04:08

IDF Under Attack Daily Report

Top Targets



Top Attackers



04-10-2016-13:04:08 to 04-10-2016-14:04:08

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	Block_Ip_Web_In	drop	3961
84.228.234.180	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	201
178.62.41.72	United Kingdom	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	12
81.218.65.210	Israel	147.237.77.176	matpash.idf.il	Block_Udp_All_Nets	drop	6
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	5
109.64.204.115	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
89.138.179.43	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	3
74.91.23.107	United States	147.237.72.156	aman.idf.il	block-sp-traf1	forward	2
69.197.185.22	United States	147.237.72.167	ishurim.aka.idf.il	block-sp-traf1	forward	2
212.235.98.139	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
74.91.17.179	United States	147.237.76.86	navy.idf.il	block-sp-traf1	forward	2
69.30.198.146	United States	147.237.77.19	law-forum.idf.il	block-sp-traf1	forward	2
107.150.32.58	United States	147.237.0.34	tikshuv.idf.il	block-sp-traf1	forward	2
74.91.20.194	United States	147.237.77.226	www.chamatz.aka.idf.il	block-sp-traf1	forward	2
173.208.197.251	United States	147.237.77.235	sviva.idf.il	block-sp-traf1	forward	2
69.30.226.219	United States	147.237.77.19	law-forum.idf.il	block-sp-traf1	forward	2
202.88.1.10	Hong Kong	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1
62.138.3.98	Germany	147.237.76.147	chinuch.aka.idf.il	Block_Ntp_All_Net	drop	1
185.94.111.1	Russian Federation	147.237.8.46	e.chinuch.idf.il	Block_Udp_All_Nets	drop	1
82.145.219.175	Europe	147.237.76.42	refuah.idf.il	Block_Ip_Web_In	drop	1
202.88.1.3	Hong Kong	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
82.145.219.175	Europe	147.237.77.233	atal.idf.il	Block_Ip_Web_In	drop	1

04-10-2016-13:04:08 to 04-10-2016-14:04:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
149.78.240.19	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	16
46.117.101.255	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
87.71.1.31	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
199.30.16.163	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
106.38.241.106	China	147.237.77.176	matpash.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
61.135.189.122	China	147.237.76.31	nakchal.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
157.55.39.162	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1

04-10-2016-13:04:08 to 04-10-2016-14:04:08

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
5.29.53.49	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	2
109.253.216.242	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.253.194.181	147.237.77.216	Israel	dover.idf.il	GPL SCAN myscan	1
84.94.38.200	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
77.127.165.80	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
212.235.98.139	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
66.249.93.82	147.237.77.233	Europe	atal.idf.il	ET SCAN NMAP -sA (2)	1
31.154.163.23	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
192.52.243.134	147.237.0.34	United States	tikshuv.idf.il	ET SCAN NMAP -sS window 4096	1
176.13.9.123	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
109.253.218.108	147.237.77.243	Israel	mobile.idf.il	GPL SCAN myscan	1
109.253.194.181	147.237.77.216	Israel	dover.idf.il	INDICATOR-SCAN myscan	1
93.173.40.39	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.182.167.208	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
76.181.249.213	147.237.77.233	United States	atal.idf.il	ET SCAN NMAP -sS window 3072	1
195.216.176.244	147.237.76.147	Latvia	chinuch.aka.idf.il	ET SCAN NMAP -sS window 1024	1
46.121.192.82	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
192.52.243.134	147.237.72.156	United States	aman.idf.il	ET SCAN NMAP -sS window 1024	1
190.61.250.160	147.237.77.216	Colombia	dover.idf.il	Tehila - Perl LWP with fake user agent	1
109.253.218.108	147.237.77.243	Israel	mobile.idf.il	INDICATOR-SCAN myscan	1

04-10-2016-13:04:08 to 04-10-2016-14:04:08

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
178.62.41.72	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1005
178.62.41.72	United Kingdom	147.237.77.216	dover.idf.il	drop		drop	413
192.168.173.102		147.237.77.216	dover.idf.il	Geo-location enforcement	Geo-location inbound enforcement	monitor	356
178.62.41.72	United Kingdom	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	322
178.62.41.72	United Kingdom	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	303
192.168.173.102		147.237.72.166	aka.idf.il	Geo-location enforcement	Geo-location inbound enforcement	monitor	175
223.176.9.22	India	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	60
212.235.98.139	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	49
149.88.62.22	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	44
199.203.93.50	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	alert	28
199.203.93.50	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	28
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	27
84.95.86.30	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
46.19.86.31	Israel	147.237.72.166	aka.idf.il	drop	SAM rule	drop	20
84.108.136.224	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	16
2.52.158.68	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	12
194.90.15.61	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
2.54.155.160	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
89.138.179.43	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
46.19.86.154	Israel	147.237.72.166	aka.idf.il	drop	SAM rule	drop	10
46.19.86.217	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
109.253.139.4	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
216.72.40.186	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
46.19.85.245	Israel	147.237.76.42	refuah.idf.il	drop	SAM rule	drop	8
84.95.86.30	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	7
207.46.13.21	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
5.102.254.111	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
31.168.199.185	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.166	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
46.19.85.32	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
2.53.31.251	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.65.136.168	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
52.29.223.39	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
176.13.13.226	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
109.65.172.110	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.52.161.167	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
79.177.69.130	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
156.109.18.122	Europe	147.237.72.167	ishurim.aka.idf.i	drop	First packet isn't SYN	drop	5
212.150.198.67	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.86.221	Israel	147.237.72.167	ishurim.aka.idf.i	drop	SAM rule	drop	5
176.13.6.36	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
84.228.234.180	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
80.246.139.194	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
80.246.139.194	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	5
192.114.23.18	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
5.108.141.32	Saudi Arabia	147.237.77.216	dover.idf.il	drop	SAM rule	drop	4
193.43.245.250	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
185.32.179.232	Israel	147.237.72.166	aka.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
2.53.15.134	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	91
109.253.212.9	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	88
37.26.148.204	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	79
185.32.179.70	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	45
46.19.86.133	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	40
2.53.39.59	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	23
5.189.190.212	Germany	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	20
149.78.166.226	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	18
5.29.123.133	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 5.29.123.133	Block	9
81.218.241.26	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 81.218.241.26	Block	5
5.189.190.212	Germany	147.237.77.170	maarachot.idf.il	Distributed Suspicious Response Code	Block	5
79.178.123.130	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
192.116.232.69	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 192.116.232.69	Block	3
109.253.139.4	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
95.35.70.155	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
176.13.9.182	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
190.61.250.160	Colombia	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 190.61.250.160	Block	2
2.55.41.166	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
212.235.62.200	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/hebrew/organization/nakhal	Block	2
79.182.5.92	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/nekudot/index	Block	1
2.53.1.90	Israel	147.237.77.243	mobile.idf.il	Untraceable SSL Sessions: Open Mode	None	1
69.30.198.146	United States	147.237.77.19	law-forum.idf.il	Unauthorized URL Access to www.app-softwares.com/	Block	1
104.131.84.88	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/shared/usercontrols/headerupper/	Block	1
38.111.147.84	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-he	Block	1
217.69.133.246	Russian Federation	147.237.72.166	aka.idf.il	Unknown Parameter docid in aka.idf.il/kamlar/klali/default.asp	None	1
212.34.12.92	Jordan	147.237.77.216	dover.idf.il	Abnormally Long Request method	Block	1
87.69.19.217	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/kapatz/undefined	Block	1
176.120.63.141	Ukraine	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/1044-he/ishurim.aspx	Block	1
79.110.207.94	Poland	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
62.0.100.86	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl73 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
132.76.61.52	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/mailbox.aspx	None	1
37.26.148.200	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
212.235.62.200	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized HTTP Method	Block	1
94.203.77.4	United Arab Emirates	147.237.77.176	matpash.idf.il	PHP Attempt	Block	1
79.182.190.136	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
190.61.250.160	Colombia	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-18014-en/dover.aspx/index.php/api/xmlrpc	Block	1
69.30.226.219	United States	147.237.77.19	law-forum.idf.il	Unauthorized URL Access to www.369bs.com/	Block	1
157.55.39.13	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
105.155.0.34	Morocco	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-he/index.aspx	Block	1
41.252.79.125	Libyan Arab Jamahiriya	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
212.34.12.92	Jordan	147.237.77.216	dover.idf.il	Malformed URL	Block	1
87.70.112.235	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/s	Block	1
178.62.41.72	United Kingdom	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
79.177.48.37	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/faq.aspx	Block	1
66.249.65.217	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
132.76.61.52	Israel	147.237.72.166	aka.idf.il	Unknown Parameter amp;t in www.aka.idf.il/main/sachar/scriptresource.axd	None	1
212.235.62.200	Israel	147.237.77.216	dover.idf.il	Unauthorized HTTP Method	Block	1
94.203.77.4	United Arab Emirates	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
81.218.149.87	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/main/	Block	1
192.116.232.69	Israel	147.237.76.42	refuah.idf.il	Multiple Unauthorized URL Access from 192.116.232.69	Block	1