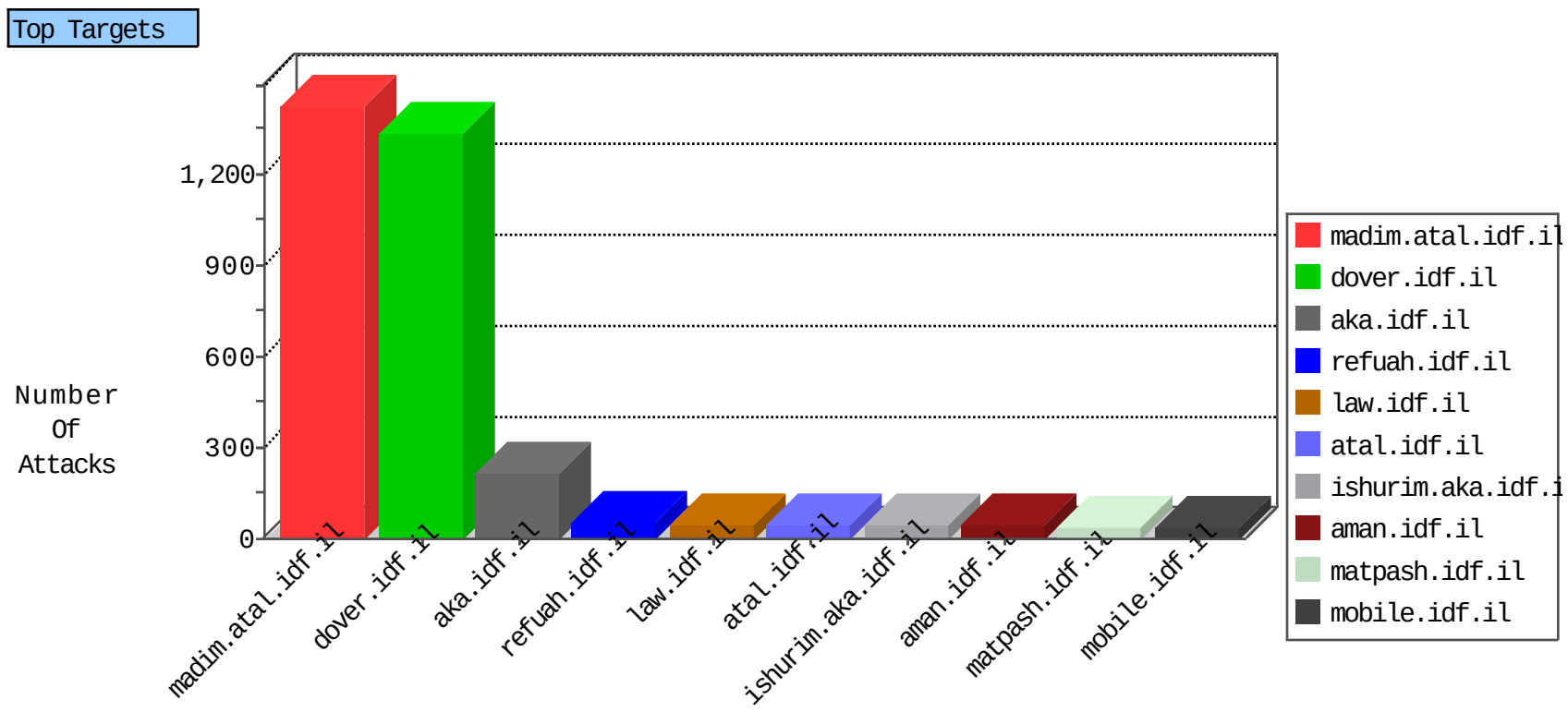
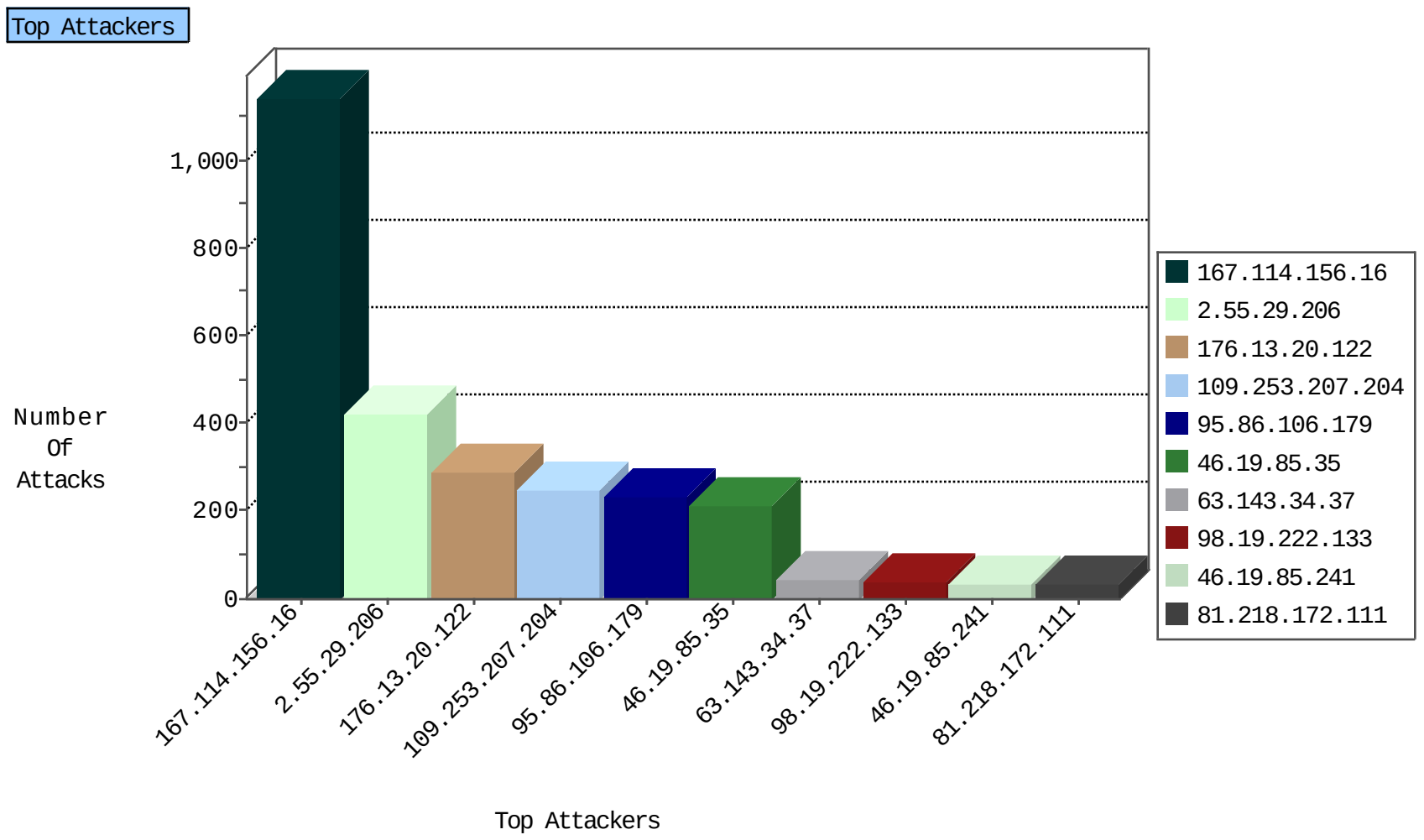
04-14-2016-16:04:03 to 04-14-2016-17:04:03

IDF Under Attack Daily Report

Top Targets



Top Attackers



04-14-2016-16:04:03 to 04-14-2016-17:04:03

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	1143
81.218.65.210	Israel	147.237.77.176	matpash.idf.il	Block_Udp_All_Nets	drop	9
79.178.23.64	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
101.201.147.32	China	147.237.72.167	ishurim.aka.idf.il	block-sp-traf1	forward	2
42.156.241.248	China	147.237.8.45	e.eitan.idf.il	Block_Udp_All_Nets	drop	1
71.6.158.166	United States	147.237.72.167	ishurim.aka.idf.il	Block_Ntp_All_Net	drop	1
31.168.13.78	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1

04-14-2016-16:04:03 to 04-14-2016-17:04:03

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
98.19.222.133	United States	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	12
176.13.18.172	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	10
83.143.81.94	Norway	147.237.76.31	nakchal.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	8
207.241.237.222	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
96.47.2.10	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
63.143.34.37	United States	147.237.76.86	navy.idf.il	3808: HTTP: SQL Injection Variable Declaration Evasion	Block	4
106.38.241.144	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	4
63.143.34.37	United States	147.237.77.216	dover.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
82.165.24.123	Germany	147.237.76.42	refuah.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
63.143.34.37	United States	147.237.77.216	dover.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	4
177.185.194.47	Brazil	147.237.77.176	matpash.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	4
70.89.127.78	United States	147.237.77.216	dover.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
177.185.194.138	Brazil	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
213.8.204.61	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
46.19.85.156	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
82.81.96.41	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
106.38.241.106	China	147.237.76.42	refuah.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
82.166.148.243	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
106.38.241.106	China	147.237.77.176	matpash.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
106.38.241.106	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
79.183.173.108	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1

04-14-2016-16:04:03 to 04-14-2016-17:04:03

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
98.19.222.133	147.237.77.233	United States	atal.idf.il	SQL Injection - Select From	25
83.143.81.94	147.237.76.31	Norway	nakchal.idf.il	SQL Injection - Select From	19
63.143.34.37	147.237.77.216	United States	dover.idf.il	SQL Injection - Select From	16
63.143.34.37	147.237.76.86	United States	navy.idf.il	SQL Injection - Select From	15
70.89.127.78	147.237.77.216	United States	dover.idf.il	SQL Injection - Select From	12
177.185.194.138	147.237.77.74	Brazil	law.idf.il	SQL Injection - Select From	10
82.165.24.123	147.237.76.42	Germany	refuah.idf.il	SQL Injection - Select From	10
177.185.194.47	147.237.77.176	Brazil	matpash.idf.il	SQL Injection - Select From	6
96.47.2.10	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	4
82.166.148.243	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
212.235.98.139	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
212.179.90.106	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
62.219.13.180	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
106.39.38.20	147.237.76.34	China	yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
46.121.43.206	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
91.202.171.11	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
88.204.187.90	147.237.0.15	Kazakstan	kosher-kravi.idf.i	ET SCAN NMAP -f -sS	1
212.179.133.50	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
66.249.78.158	147.237.72.166	United States	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	1
50.139.116.160	147.237.76.147	United States	chinuch.aka.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
37.26.148.129	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
94.159.147.170	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
88.204.187.90	147.237.0.15	Kazakstan	kosher-kravi.idf.i	ET SCAN NMAP -sS window 2048	1
84.109.24.98	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1

04-14-2016-16:04:03 to 04-14-2016-17:04:03

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
81.218.172.111	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	32
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
2.53.141.175	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
79.182.142.234	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
2.55.41.96	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
2.55.129.26	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
31.168.198.94	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
79.183.196.24	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
2.53.149.99	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.177.184.14	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	6
46.19.85.241	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
185.120.126.35	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.241	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
149.78.19.115	United States	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
132.64.54.146	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
70.209.140.237	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
79.177.184.14	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
79.177.184.14	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
37.46.41.61	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.85.241	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
79.177.10.57	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
66.249.93.243	Europe	147.237.77.176	matpash.idf.il	drop		drop	4
177.185.192.50	Brazil	147.237.77.74	law.idf.il	drop	SAM rule	drop	4
79.177.10.57	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
109.186.184.18	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
149.50.102.76	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	4
65.202.145.2	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
177.185.194.45	Brazil	147.237.77.74	law.idf.il	drop	SAM rule	drop	4
212.179.21.194	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
65.202.145.2	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.85.241	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
202.124.109.87	New Zealand	147.237.77.74	law.idf.il	drop	SAM rule	drop	4
79.183.121.26	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.177.175.107	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
87.69.205.112	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
109.65.22.194	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
176.13.22.221	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
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
149.78.235.191	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
77.125.117.118	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
81.218.185.181	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
185.27.105.181	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.26.147.167	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.182.110.1	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.139	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
176.13.0.208	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.77	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

04-14-2016-16:04:03 to 04-14-2016-17:04:03

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
80.246.136.249	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
193.169.70.108	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

04-14-2016-16:04:03 to 04-14-2016-17:04:03

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.55.29.206	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	419
176.13.20.122	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	290
109.253.207.204	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	250
95.86.106.179	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	232
46.19.85.35	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	209
165.222.184.144	Switzerland	147.237.77.74	law.idf.il	Unauthorized HTTP Method	Block	4
2.53.20.252	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/nekudot/index	Block	3
176.13.11.224	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.85.241	Israel	147.237.76.42	refuah.idf.il	Distributed Malformed URL	Block	3
46.19.85.241	Israel	147.237.76.42	refuah.idf.il	Distributed Unknown HTTP Request Method	Block	3
212.179.21.194	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 212.179.21.194	Block	3
37.26.147.167	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
165.222.184.144	Switzerland	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 165.222.184.144	Block	3
46.120.75.247	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.53.47.109	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
176.13.1.249	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
2.53.141.175	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
46.19.85.241	Israel	147.237.76.42	refuah.idf.il	Multiple Illegal HTTP Version from 46.19.85.241	Block	2
46.19.85.241	Israel	147.237.76.42	refuah.idf.il	Distributed Abnormally Long Request	Block	2
37.26.147.211	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	1
207.46.13.132	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/	Block	1
66.249.93.243	Israel	147.237.77.176	matpash.idf.il	Multiple URL is Above Root Directory from 66.249.93.243	Block	1
169.229.3.91	United States	147.237.72.156	aman.idf.il	Malformed URL	Block	1
130.185.155.10	Sweden	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
212.179.21.194	Israel	147.237.77.216	dover.idf.il	Parameter Type Violation SearchText in www.idf.il/1065-he/dover.aspx	Block	1
178.140.85.40	Russian Federation	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.15/	Block	1
85.250.68.110	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/wp-login.php	Block	1
66.249.64.131	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/recruitlane.aspx	Block	1
169.229.3.91	United States	147.237.76.39	mobile.meitav.idf.il	Multiple Illegal Byte Code Character in Header Name from 169.229.3.91	Block	1
37.26.148.171	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
165.222.184.144	Switzerland	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/sip_storage/files/8/	Block	1
109.67.176.111	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
2.53.47.109	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
212.25.102.63	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/images/1.he/infocenteritem/	Block	1
79.183.121.26	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/mains/sachar	Block	1
176.13.12.84	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
169.229.3.91	United States	147.237.72.156	aman.idf.il	Unknown HTTP Request Method /[&6Ð¤ÙÉ¶Ll^ÕÕ¤[[#5]]åÙì»¶#W¥7L[[#18]][[#26]]¢#+î•ÎmíT$ýKÂ4Ê[[#27]]Ÿ.ãñË¬¥•Ïôöà5+ºN‹ in URL	Block	1
5.29.67.254	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
213.151.53.59	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1501-he/atal.aspx	Block	1
130.185.155.10	Sweden	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/wp-login.php	Block	1
178.255.215.87	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/sendtofriend/kkkkkkk=3b95da62kkkkkkk_3b95da62	Block	1
87.69.205.112	Israel	147.237.72.156	aman.idf.il	Multiple Untraceable SSL Sessions from 87.69.205.112 (Open Mode)	None	1
66.249.64.176	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to www.atal.idf.il/1133-he/אגף הטכנולוגיה והלוגיסטיקה.aspx	Block	1
169.229.3.91	United States	147.237.76.39	mobile.meitav.idf.il	Multiple Illegal Byte Code Character in Method from 169.229.3.91	Block	1
169.229.3.91	United States	147.237.72.156	aman.idf.il	Abnormally Long Request method	Block	1
176.13.16.228	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/sachar/tfasim.aspx'	Block	1
80.246.136.124	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
169.229.3.91	United States	147.237.76.39	mobile.meitav.idf.il	Distributed Malformed URL	Block	1
46.19.85.241	Israel	147.237.76.42	refuah.idf.il	Illegal HTTP Version	Block	1
17.142.156.109	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 17.142.156.109	Block	1

04-14-2016-16:04:03 to 04-14-2016-17:04:03