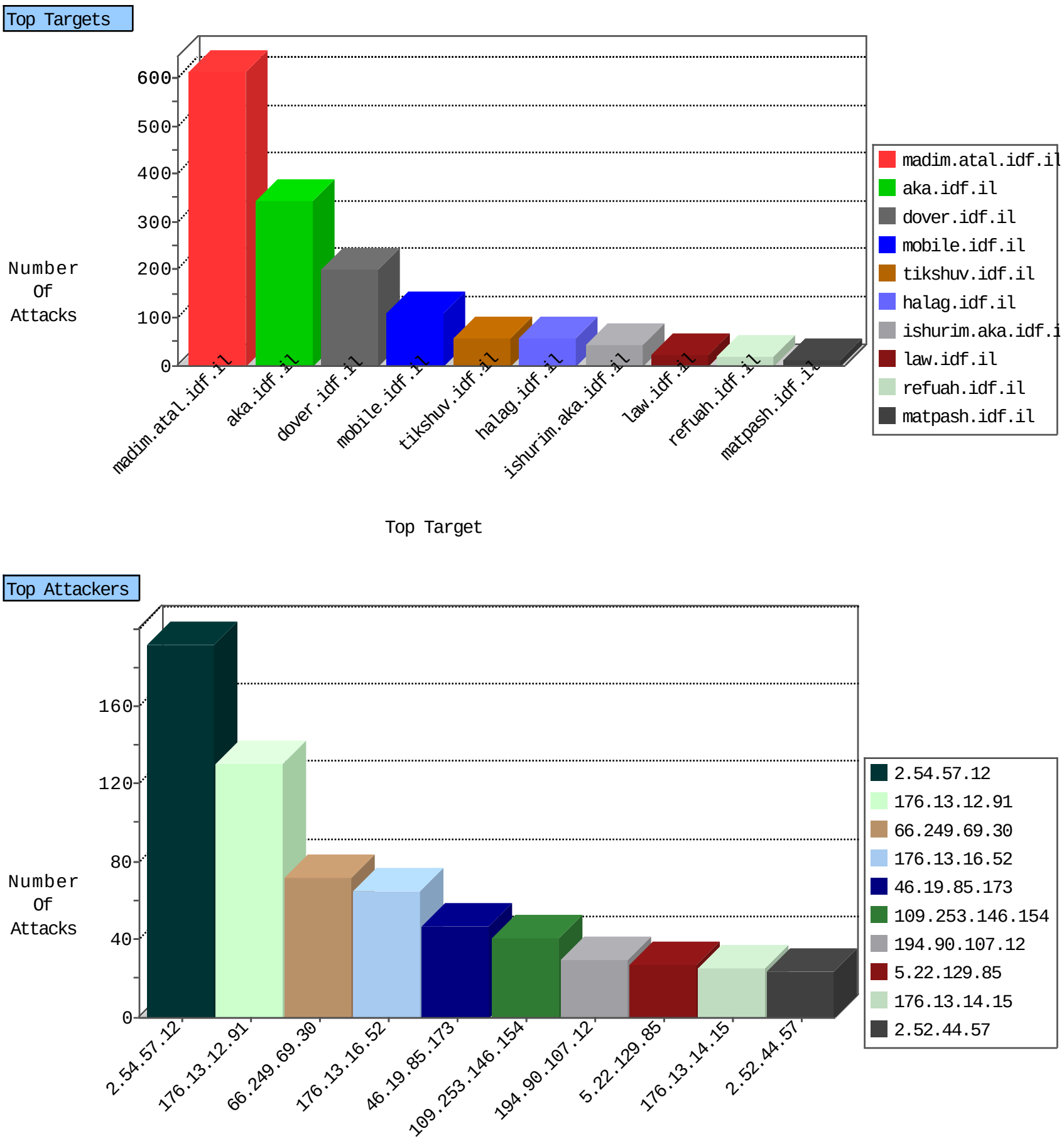
03-06-2016-11:04:09 to 03-06-2016-12:04:09

IDF Under Attack Daily Report



03-06-2016-11:04:09 to 03-06-2016-12:04:09

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.86.53	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	7
2.54.190.110	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	7
81.218.65.210	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	6
82.145.217.125	Europe	147.237.72.166	aka.idf.il	Block_Ip_Web_In	drop	5
176.13.1.52	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
93.172.147.82	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
134.147.203.115	Germany	147.237.0.16	my-kosher-kravi.idf.il	Block_Ntp_All_Net	drop	2
91.199.69.254	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
71.6.165.200	United States	147.237.76.31	nakchal.idf.il	Block_Udp_All_Nets	drop	1
10.0.0.6		147.237.77.234	halag.idf.il	Invalid TCP Flags	drop	1
176.13.1.52	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
108.186.168.25	United States	147.237.77.227	e.hamaz.idf.il	Block_Ntp_All_Net	drop	1
23.94.69.234	United States	147.237.77.74	law.idf.il	Block_Ntp_All_Net	drop	1
184.105.139.85	United States	147.237.77.243	mobile.idf.il	Block_Udp_All_Nets	drop	1

03-06-2016-11:04:09 to 03-06-2016-12:04:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
81.218.251.252	Israel	147.237.0.34	tikshuv.idf.	C1000138: HTTP: prefix 1.01 in the URL	Block	12
109.65.83.95	Israel	147.237.0.34	tikshuv.idf.	C1000138: HTTP: prefix 1.01 in the URL	Block	9
31.168.232.154	Israel	147.237.0.34	tikshuv.idf.	C1000138: HTTP: prefix 1.01 in the URL	Block	8
109.65.79.180	Israel	147.237.0.34	tikshuv.idf.	C1000138: HTTP: prefix 1.01 in the URL	Block	8
81.218.151.130	Israel	147.237.0.34	tikshuv.idf.	C1000138: HTTP: prefix 1.01 in the URL	Block	8
95.86.120.47	Israel	147.237.0.34	tikshuv.idf.	C1000138: HTTP: prefix 1.01 in the URL	Block	6
132.66.62.239	Israel	147.237.0.34	tikshuv.idf.	C1000138: HTTP: prefix 1.01 in the URL	Block	2
177.17.188.131	Brazil	147.237.77.216	dover.idf.il	12348: HTTP: PHP-CGI Query String Parameter Command Injection Vulnerability	Block	1
66.102.9.107	United States	147.237.0.34	tikshuv.idf.	C1000138: HTTP: prefix 1.01 in the URL	Block	1
106.120.173.159	China	147.237.77.233	atal.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
66.102.9.127	United States	147.237.0.34	tikshuv.idf.	C1000138: HTTP: prefix 1.01 in the URL	Block	1

03-06-2016-11:04:09 to 03-06-2016-12:04:09

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
2.54.24.6	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.65.83.95	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
82.117.208.243	147.237.77.216		dover.idf.il	ET SCAN NMAP -sS window 1024	1
79.183.189.1	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
212.143.47.165	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
61.244.49.137	147.237.0.35	Hong Kong	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
61.163.231.229	147.237.77.226	China	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 1024	1
185.72.179.221	147.237.77.74		law.idf.il	ET SCAN NMAP -sS window 1024	1
37.26.148.130	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
179.32.124.91	147.237.0.15	Colombia	kosher-kravi.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
23.125.172.41	147.237.8.24	United States	e.lifestyle.idf.il	ET SCAN NMAP -sS window 4096	1
113.76.90.146	147.237.76.177	China	ncore.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
2.54.56.237	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
109.65.83.95	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
89.139.188.40	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
80.178.126.194	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
213.57.234.205	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.178.16.161	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
207.232.27.5	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
61.244.49.137	147.237.0.19	Hong Kong	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
192.198.151.45	147.237.72.167	Europe	ishurim.aka.idf.il	ET SCAN NMAP -sA (2)	1
37.26.148.212	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
185.32.179.143	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
31.168.16.116	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
134.191.232.70	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
23.125.172.41	147.237.8.24	United States	e.lifestyle.idf.il	ET SCAN NMAP -sS window 3072	1
109.253.159.200	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1

03-06-2016-11:04:09 to 03-06-2016-12:04:09

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
66.249.69.30	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	72
194.90.107.12	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	27
5.22.129.85	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	27
213.8.204.78	Israel	147.237.72.166	aka.idf.il	drop	SAM rule	drop	17
80.246.133.229	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	15
2.54.22.122	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	13
46.19.85.64	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
84.229.241.72	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
37.26.146.159	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
212.179.21.194	Israel	147.237.77.212	e.dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
79.176.150.43	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
80.246.136.74	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	8
80.246.136.74	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	8
46.19.85.64	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.202	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
192.114.23.209	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
2.52.44.57	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
80.179.199.52	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
192.114.23.209	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
46.19.86.153	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
195.160.242.40	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.202	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
176.13.5.42	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.245	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
106.38.241.106	China	147.237.77.216	dover.idf.il	drop	SAM rule	drop	5
2.52.44.57	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
192.114.91.249	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
2.52.44.57	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	5
79.181.104.130	Israel	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
2.54.27.229	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
84.108.127.204	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
2.52.44.57	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
194.90.178.37	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	4
46.19.85.2	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
2.52.44.57	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
46.19.85.68	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
192.114.91.249	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
46.253.85.55	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	4
100.127.178.101		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
79.176.193.222	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
87.68.50.120	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
149.78.236.128	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
80.246.136.42	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
178.255.215.87	France	147.237.76.147	chinuch.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
193.16.147.2	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.67.165.130	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
62.0.98.156	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.155.23	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
80.178.195.47	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

03-06-2016-11:04:09 to 03-06-2016-12:04:09

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.54.57.12	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	192
176.13.12.91	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	131
176.13.16.52	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	65
46.19.85.173	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	46
109.253.146.154	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	41
176.13.14.15	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	25
37.26.147.232	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	19
109.253.197.85	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	18
109.253.132.172	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	12
2.54.152.57	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	12
46.19.86.247	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	9
109.253.221.43	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	9
109.253.214.196	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	8
81.218.241.25	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 81.218.241.25	Block	6
37.239.154.27	Iraq	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/arr/	Block	5
39.50.146.155	Pakistan	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	4
176.13.8.118	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
37.26.146.159	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
80.246.139.191	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
79.177.1.208	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
192.116.232.69	Israel	147.237.77.74	law.idf.il	Multiple Unauthorized URL Access from 192.116.232.69	Block	3
213.151.35.216	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.253.142.255	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1071	Block	3
80.246.136.108	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
62.0.98.156	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/valtam	Block	2
80.246.130.93	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	2
39.50.146.155	Pakistan	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	2
37.26.148.168	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
66.249.64.233	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.233	Block	2
39.50.146.155	Pakistan	147.237.77.74	law.idf.il	Distributed Unauthorized URL Access on www.law.idf.il/xmlrpc.php	Block	2
82.166.247.94	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
208.115.113.89	United States	147.237.77.216	dover.idf.il	Parameter Type Violation SortDir in www.idf.il/1153-en/dover.aspx	Block	2
109.253.213.78	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
39.50.146.155	Pakistan	147.237.77.74	law.idf.il	Distributed Unauthorized URL Access on www.mag.idf.il/xmlrpc.php	Block	2
109.253.140.141	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
81.218.251.250	Israel	147.237.76.147	chinuch.aka.idf.i	Distributed Unauthorized URL Access on www.chinuch.aka.idf.il/404.htm	Block	2
194.90.217.145	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	1
37.26.146.191	Israel	147.237.77.243	mobile.idf.il	Multiple Untraceable SSL Sessions from 37.26.146.191 (Open Mode)	None	1
85.64.146.246	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/files/2/110372	Block	1
2.54.160.44	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/text.css	Block	1
82.166.141.45	Israel	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to www.tikshuv.idf.il/modules/	Block	1
46.19.85.207	Israel	147.237.77.216	dover.idf.il	Illegal HTTP Version Sep 2010 12:32:44 GMT	Block	1
109.66.13.110	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/xmlrpc.php	Block	1
91.199.69.254	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
207.241.237.227	United States	147.237.72.166	aka.idf.il	Unknown Parameter docid in aka.idf.il/iturim/asp/displayonesoldier.asp	None	1
192.115.67.2	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
84.108.233.96	Israel	147.237.77.74	law.idf.il	Distributed Unauthorized URL Access on www.law.idf.il/xmlrpc.php	Block	1
46.19.86.108	Israel	147.237.76.42	refuah.idf.il	Parameter Type Violation searchText in www.refua.atal.idf.il/1405-he/refuah.aspx	Block	1
46.19.85.173	Israel	147.237.0.19	madim.atal.idf.il	Cookie Tampering on cookie Login: Expected ********** ********** ********** ****, Observed ********** ********** **********	None	1
213.8.204.38	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/https:/www.idf.il/	Block	1

03-06-2016-11:04:09 to 03-06-2016-12:04:09