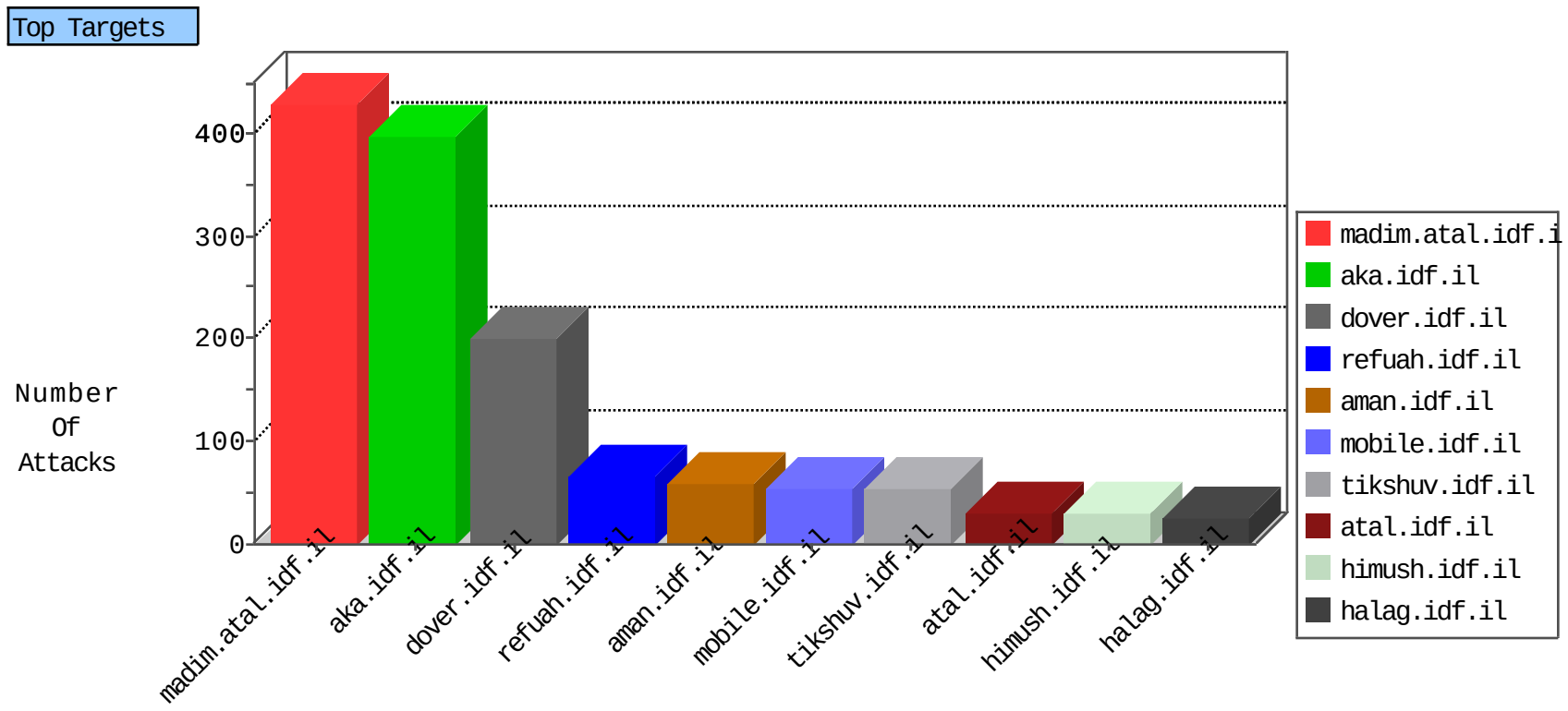
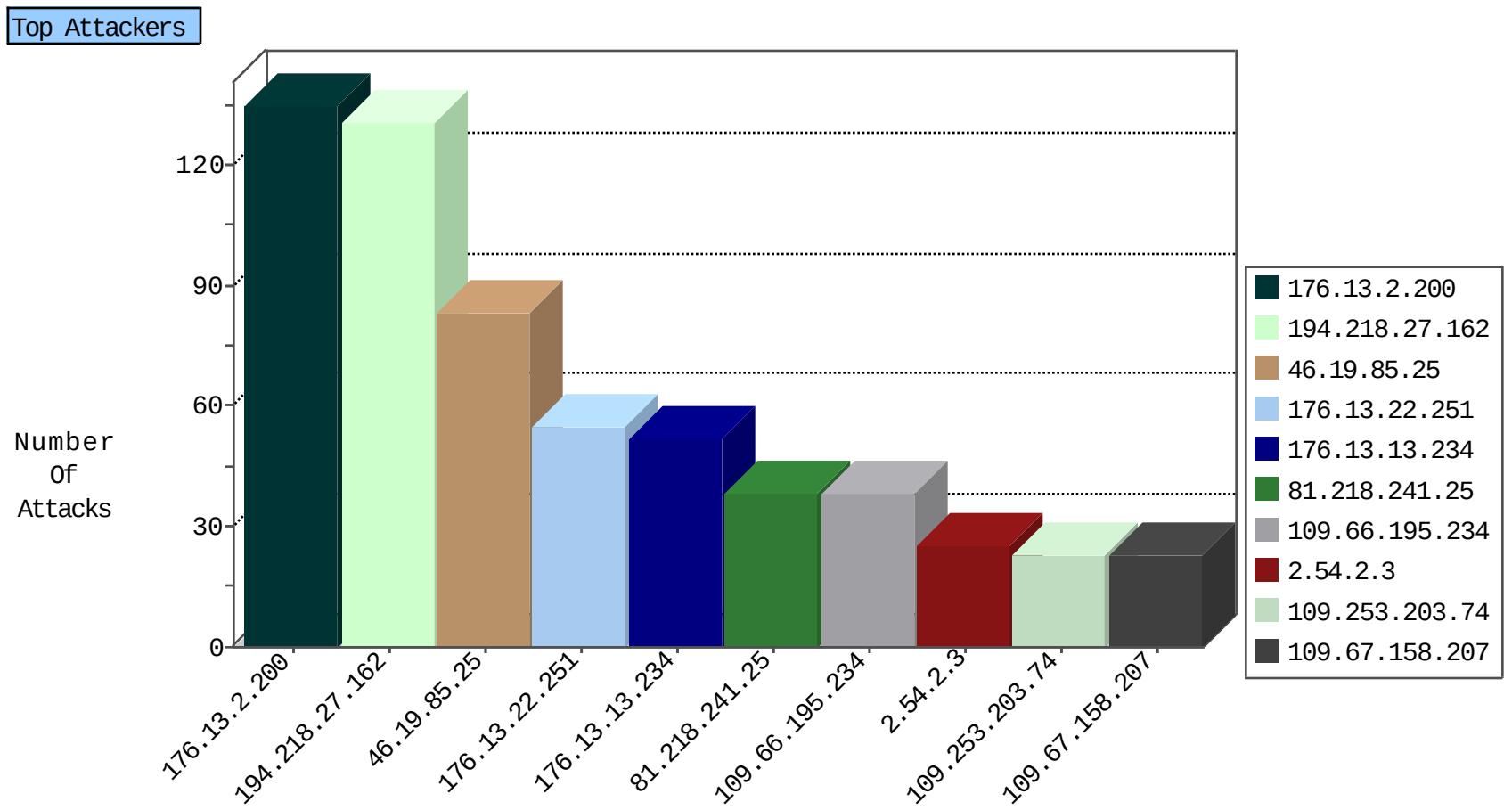
03-02-2016-13:04:01 to 03-02-2016-14:04:01

IDF Under Attack Daily Report

Top Targets



Top Attackers



03-02-2016-13:04:01 to 03-02-2016-14:04:01

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
81.218.241.25	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	232
0.0.0.0		147.237.77.216	dover.idf.il	SYN Flood out of context	drop	36
212.179.132.204	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	5
79.177.105.174	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	5
212.143.165.117	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
81.218.251.251	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
222.74.217.16	China	147.237.77.121	e.navy.idf.il	Invalid TCP Flags	drop	2
178.214.90.31	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	TCP handshake violation, first packet not syn	drop	1
68.235.61.11	United States	147.237.76.177	ncore.idf.il	Block_Udp_All_Nets	drop	1
123.97.243.233	China	147.237.77.243	mobile.idf.il	Block_Udp_All_Nets	drop	1
184.105.247.235	United States	147.237.8.46	e.chinuch.idf.i	Block_Udp_All_Nets	drop	1
164.132.54.194	Italy	147.237.72.156	aman.idf.il	Block_Ntp_All_Net	drop	1
192.99.63.194	Canada	147.237.72.166	aka.idf.il	Block_Ntp_All_Net	drop	1
164.132.54.194	Italy	147.237.76.31	nakchal.idf.il	Block_Ntp_All_Net	drop	1

03-02-2016-13:04:01 to 03-02-2016-14:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
147.235.185.74	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	10
185.24.207.49	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
172.19.203.101		147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	5
157.55.39.210	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
207.46.13.96	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
62.210.148.246	France	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
212.235.67.205	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
79.176.80.248	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
79.179.128.52	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
199.58.86.206	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
62.210.148.246	France	147.237.76.86	navy.idf.il	C1000074: HTTP: majestic bot	Block	2
123.126.113.80	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1

03-02-2016-13:04:01 to 03-02-2016-14:04:01

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
89.139.247.250	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	2
179.43.141.209	147.237.76.42	Switzerland	refuah.idf.il	ET SCAN Potential SSH Scan	1
5.29.14.206	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
174.37.194.144	147.237.76.199	United States	e.nakchal.idf.il	ET SCAN NMAP -sS window 4096	1
2.54.180.37	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
174.37.194.144	147.237.76.196	United States	e.sviva.idf.il	ET SCAN NMAP -sA (2)	1
149.88.165.38	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
93.173.243.87	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
84.111.101.201	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
217.21.8.80	147.237.77.216	Palestinian Territory, Occupied	dover.idf.il	portscan: TCP Distributed Portscan	1
81.218.201.196	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	1
62.90.234.193	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
182.72.109.162	147.237.0.17	India	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
31.154.29.94	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
174.37.194.144	147.237.77.205	United States	prisha.idf.il	ET SCAN NMAP -sA (2)	1
5.22.135.108	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
174.37.194.144	147.237.76.196	United States	e.sviva.idf.il	ET SCAN NMAP -sS window 3072	1
2.54.32.181	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
149.88.175.22	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
95.35.157.105	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
217.132.30.219	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
82.80.160.196	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
212.143.66.70	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
77.127.137.253	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
186.116.218.227	147.237.76.44	Colombia	e.refuah.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
37.46.43.78	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1

03-02-2016-13:04:01 to 03-02-2016-14:04:01

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	88
194.218.27.162	Sweden	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	43
109.66.195.234	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	37
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	20
79.178.0.110	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	20
81.218.241.25	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	15
79.179.169.218	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
93.173.36.251	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	14
109.253.203.74	Israel	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	alert	12
109.253.203.74	Israel	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
176.13.8.78	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	10
46.19.86.188	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
2.52.37.57	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
31.13.161.237	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
199.203.84.144	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
46.19.85.88	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
37.26.147.197	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
84.95.193.101	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.99	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
141.8.132.112	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.183.169.121	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.177.60.253	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
31.13.161.237	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.99	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.151	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
2.54.129.191	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
192.115.83.5	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
46.19.85.151	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
46.19.85.242	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
46.19.85.41	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
46.19.85.41	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
195.34.139.6	Austria	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	4
37.46.41.242	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
176.13.8.78	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	4
62.219.224.149	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.253.192.102	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
185.3.144.23	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.178.53.170	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.46.39.21	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
77.125.123.221	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.26.147.173	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.99	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
79.181.218.200	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.52.131.121	Israel	147.237.0.19	madim.atal.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
79.177.58.169	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.26.147.241	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.162	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
84.94.100.192	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.58.135	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.178.191.12	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

03-02-2016-13:04:01 to 03-02-2016-14:04:01

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.2.200	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	135
46.19.85.25	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	83
176.13.22.251	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	55
176.13.13.234	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	52
2.54.2.3	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	25
109.67.158.207	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation Password in mobile.idf.il/sachar/login	Block	22
185.32.179.165	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	17
2.52.131.154	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	15
2.52.131.121	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	7
2.54.11.197	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
176.13.22.246	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	6
46.19.86.48	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
212.143.254.66	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 212.143.254.66	Block	5
66.249.66.25	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.66.25	Block	5
109.253.145.217	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
80.246.130.69	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
185.32.179.54	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
80.246.136.235	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.6.255	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
80.246.130.6	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
2.54.57.19	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.228.65.186	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/authentication/index	Block	3
2.52.2.99	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.54.15.138	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 2.54.15.138	Block	2
2.54.52.141	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
80.246.130.7	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
104.132.8.92	Ireland	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/main/giyus/authenticationservice.asmx/getauthuser	Block	2
46.118.230.187	Ukraine	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/mazi/	Block	1
173.252.80.118	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
93.173.60.46	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/sip_storage/files/0/size338x0/1620.jpg	Block	1
37.26.148.137	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
169.229.3.91	United States	147.237.72.156	aman.idf.il	Distributed Unknown HTTP Request Method	Block	1
68.180.230.29	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/1043-ar/cogat.aspx	Block	1
185.82.203.241		147.237.76.42	refuah.idf.il	Parameter Type Violation SortDir in www.refua.atal.idf.il/1387-he/refuah.aspx	Block	1
2.54.8.67	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
149.78.214.222	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
107.150.42.35	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.yun.ph/	Block	1
66.249.64.190	United States	147.237.72.166	aka.idf.il	Unknown Parameter KEY in www.aka.idf.il/valtam/asp/default.asp	None	1
176.13.9.45	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/nekudot/index	Block	1
169.229.3.91	United States	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in Method	Block	1
82.80.196.44	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
5.102.193.1	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$btnSubmit.x in www.aka.idf.il/main/sachar/payslips.aspx	None	1
169.229.3.91	United States	147.237.0.34	tikshuv.idf.il	Illegal Byte Code Character in Header Name	Block	1
79.179.186.169	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/https:/www.idf.il/	Block	1
185.89.217.233		147.237.76.31	nakchal.idf.il	URL is Above Root Directory www.nakhal.idf.il/../images/shared/home.png	Block	1
66.249.66.182	United States	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/style/1.he/grid.css	Block	1
134.191.232.70	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/favicon.ico	Block	1
52.30.171.229	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to /	Block	1
94.199.151.22	United Kingdom	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/templates/templatecontrols/generic/	Block	1
212.143.254.66	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/resources/styles/	Block	1

03-02-2016-13:04:01 to 03-02-2016-14:04:01