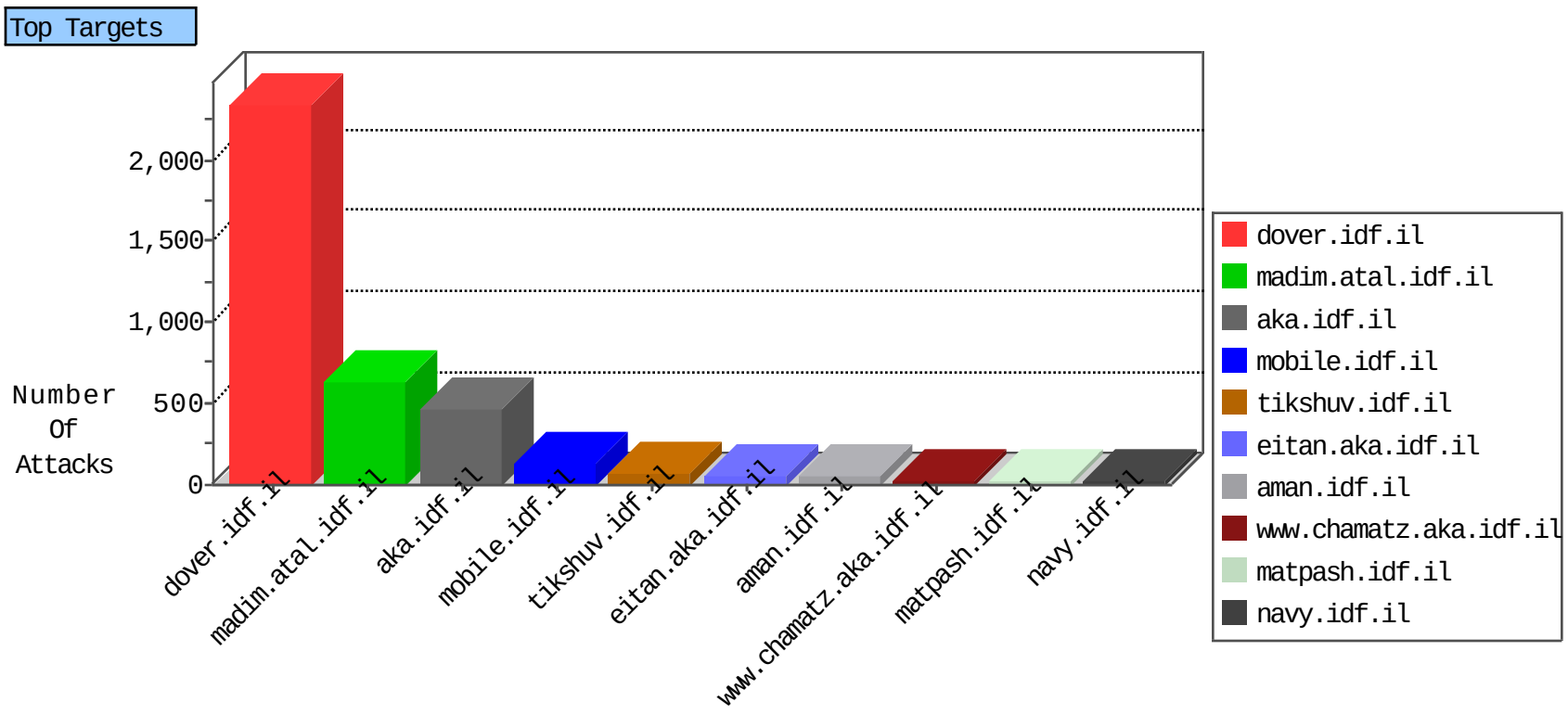
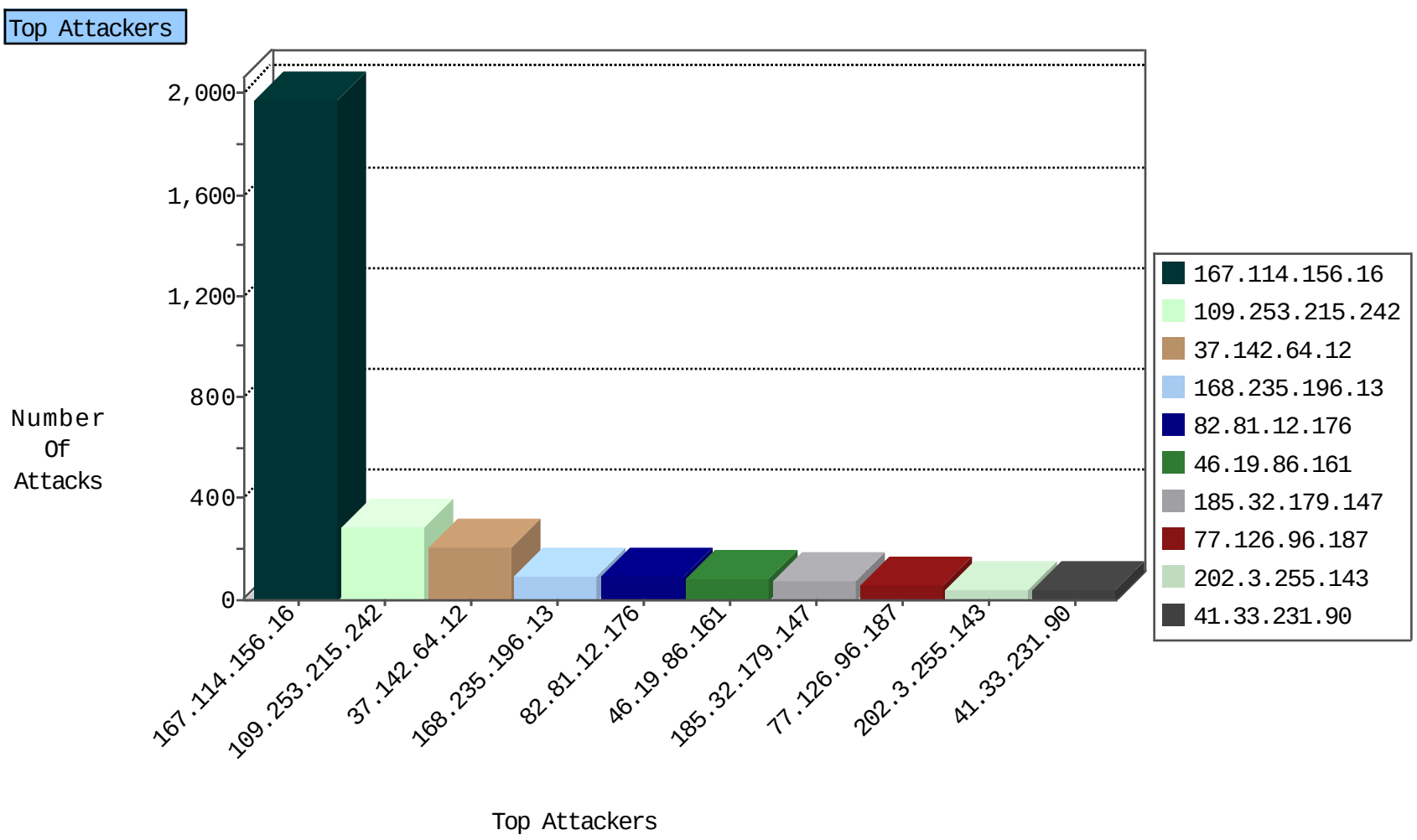
01-19-2016-18:04:00 to 01-19-2016-19:04:00

IDF Under Attack Daily Report





01-19-2016-18:04:00 to 01-19-2016-19:04:00

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	DOS-Tool-SwitchbladG	dest-reset	3225
82.81.12.176	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	95
81.218.241.26	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	94
46.19.85.137	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	71
79.178.6.161	Israel	147.237.72.156	aman.idf.il	Block_Udp_All_Nets	drop	6
79.177.211.180	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	6
168.235.196.13	United States	147.237.77.216	dover.idf.il	F_Dover_Under_Attack_Con_Http	drop	4
109.66.160.66	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
52.16.5.197	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
27.109.230.164	Macau	147.237.76.201	e.atal.idf.il	Block_Udp_All_Nets	drop	1
71.6.167.142	United States	147.237.76.38	e.e.meitav.idf.il	Block_Udp_All_Nets	drop	1
27.109.230.164	Macau	147.237.76.202	e.halag.idf.il	Block_Udp_All_Nets	drop	1
200.35.95.235	Venezuela	147.237.76.176	test.ncore.idf.il	L4 Source or Dest Port Zero	drop	1

01-19-2016-18:04:00 to 01-19-2016-19:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
217.132.47.52	Israel	147.237.0.34	tikshuv.idf.il	C212: HTTP: prefix 1.01 in the URL	Block	14
79.176.57.138	Israel	147.237.0.34	tikshuv.idf.il	C212: HTTP: prefix 1.01 in the URL	Block	8
176.13.13.35	Israel	147.237.0.34	tikshuv.idf.il	C212: HTTP: prefix 1.01 in the URL	Block	6
79.180.21.188	Israel	147.237.0.34	tikshuv.idf.il	C212: HTTP: prefix 1.01 in the URL	Block	5
109.253.201.42	Israel	147.237.0.34	tikshuv.idf.il	C212: HTTP: prefix 1.01 in the URL	Block	4
87.69.92.102	Israel	147.237.0.34	tikshuv.idf.il	C212: HTTP: prefix 1.01 in the URL	Block	3
195.110.40.7	Israel	147.237.0.34	tikshuv.idf.il	C212: HTTP: prefix 1.01 in the URL	Block	2
85.65.62.97	Israel	147.237.0.34	tikshuv.idf.il	C212: HTTP: prefix 1.01 in the URL	Block	2
77.126.165.40	Israel	147.237.0.34	tikshuv.idf.il	C212: HTTP: prefix 1.01 in the URL	Block	2
106.38.241.106	China	147.237.76.42	refuah.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1
106.38.241.106	China	147.237.77.216	dover.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1
207.46.13.48	United States	147.237.0.34	tikshuv.idf.il	C212: HTTP: prefix 1.01 in the URL	Block	1
62.210.226.9	France	147.237.72.166	aka.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	1
211.23.251.92	Taiwan	147.237.77.233	atal.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	1
106.38.241.106	China	147.237.72.166	aka.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1
192.168.1.6		147.237.0.34	tikshuv.idf.il	C212: HTTP: prefix 1.01 in the URL	Block	1

01-19-2016-18:04:00 to 01-19-2016-19:04:00

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	3
62.210.226.9	147.237.72.166	France	aka.idf.il	SQL Injection - Select From	2

01-19-2016-18:04:00 to 01-19-2016-19:04:00

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
168.235.196.13	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	93
77.126.96.187	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	57
202.3.255.143	French Polynesia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	37
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
149.88.179.43	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	28
79.178.34.210	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
46.19.86.165	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
2.54.58.53	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.86.59	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
84.94.158.116	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.43.109.21	Palestinian Territory Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	11
109.253.215.242	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
79.180.153.220	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
79.180.155.177	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.86.161	Israel	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
46.19.85.77	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
93.172.26.188	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
46.19.86.161	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
31.210.188.48	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.85.170	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
46.19.86.161	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
41.46.111.82	Egypt	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
79.176.12.62	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.182.192.173	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.178.6.221	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
79.178.6.221	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
79.178.14.28	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
81.218.241.26	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
109.65.162.23	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.183.169.198	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.143.221.67	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	6
37.142.238.222	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
82.80.193.236	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
84.228.203.172	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.65.168.105	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.116.224.104	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.86.171	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
79.177.151.52	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
31.210.188.48	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
80.246.136.53	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
46.19.85.77	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
109.73.15.150	Russian Federation	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
185.56.88.90	United Arab Emirates	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4

01-19-2016-18:04:00 to 01-19-2016-19:04:00

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
100.127.42.244		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
109.253.220.128	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
46.19.85.224	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
185.3.147.235	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
2.52.137.37	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4

01-19-2016-18:04:00 to 01-19-2016-19:04:00

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.253.215.242	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	107
37.142.64.12	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	104
37.142.64.12	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	104
109.253.215.242	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	97
185.32.179.147	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	74
46.19.86.161	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	55
109.253.215.242	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (403) in Session from 109.253.215.242	Block	53
149.88.179.43	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	8
79.179.211.16	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/6/	Block	6
176.13.11.221	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.253.215.242	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
89.139.229.1	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/sip_storage/files/6/	Block	3
46.19.86.59	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
109.253.132.224	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.86.211	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
109.253.146.77	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
109.65.168.105	Israel	147.237.77.233	atal.idf.il	Parameter Type Violation search in www.atal.idf.il/1440-he/atal.aspx	Block	2
46.19.86.164	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.19.86.109	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
176.13.2.75	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
176.13.22.10	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.19.86.165	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
46.117.128.94	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
192.115.177.202	Israel	147.237.77.216	dover.idf.il	Parameter Type Violation SearchText in www.idf.il/1065-he/dover.aspx	Block	1
95.86.89.1	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-20712-he/idfgdover.aspx&sa=u&ved=0ahukewih0zgkqlbkahwrvymkhxmrdjmqfggwmaq&usg=afqjcnfoxg1ivm6px3_nhshy9kkqe24-8w	Block	1
84.108.248.170	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.19.86.139	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
79.179.183.54	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
37.142.64.62	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
5.175.0.137	Germany	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/shared/usercontrols/headerupper/	Block	1
109.65.54.52	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.220.158.106	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
207.232.46.209	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	1
176.228.52.184	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$cb14243682 in aka.idf.il/main/sachar/payslips.aspx	None	1
89.139.143.199	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.19.85.122	Israel	147.237.76.42	refuah.idf.il	Unknown HTTP Request Method nId=mnhvan45x3far4vxfnb0rx55; in URL __atuvc=3	Block	1
80.246.139.30	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
77.125.242.175	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/sip_storage/files/9/2479.jpg	Block	1
217.132.146.69	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
37.26.148.224	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.117.130.252	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
192.115.177.202	Israel	147.237.77.216	dover.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$ucNewsFlashControl$txtSearch in www.idf.il/1153-he/dover.aspx	Block	1
95.86.103.136	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
84.109.69.188	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.19.86.153	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/nekudot/index	Block	1
176.13.13.42	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
37.142.238.222	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
17.142.156.109	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	1
109.65.162.23	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
66.249.69.26	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1

01-19-2016-18:04:00 to 01-19-2016-19:04:00