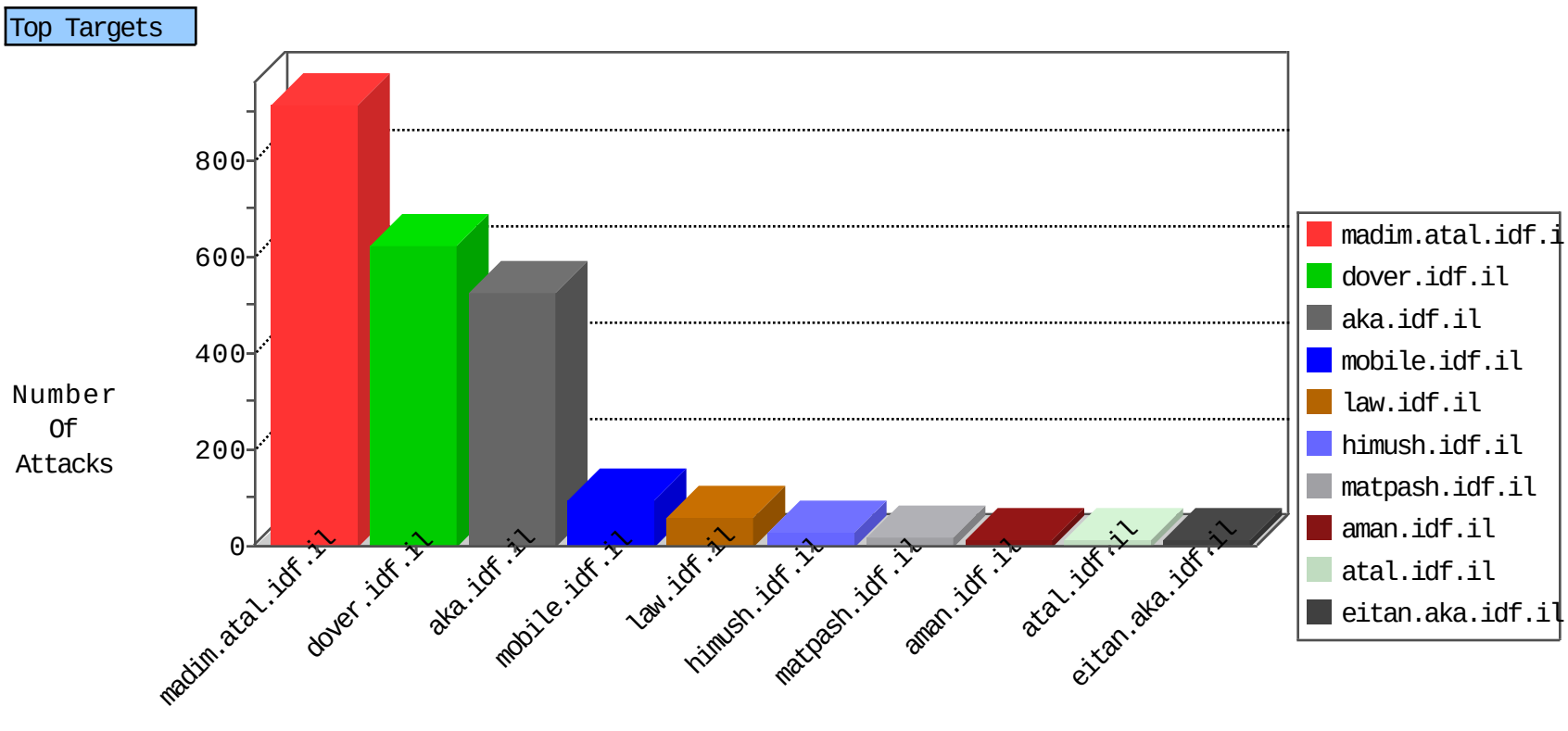
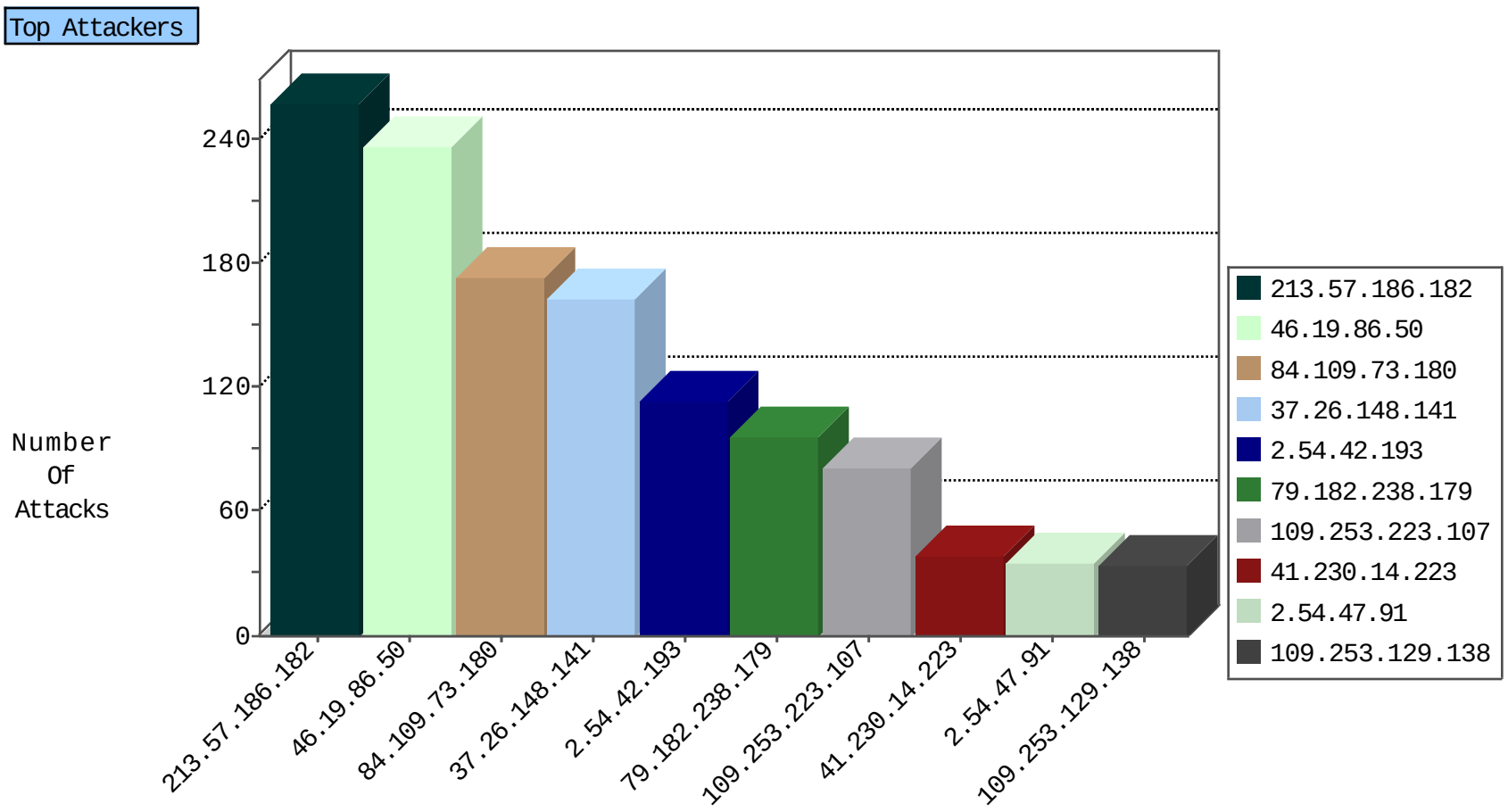
01-31-2016-23:04:01 to 02-01-2016-00:04:01

IDF Under Attack
Daily Report

Top Targets



Top Attackers



01-31-2016-23:04:01 to 02-01-2016-00:04:01

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
37.26.148.141	Israel	147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	1645
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	49
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	20
212.179.21.194	Israel	147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	16
176.13.23.167	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	5
213.57.160.177	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	5
85.64.134.38	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
115.239.228.10	China	147.237.76.202	e.halag.idf.il	JLM_Under_Attack_Con_Http	drop	2
142.54.160.212	United States	147.237.0.17	m.my-kosher-kravi.idf.il	block-sp-traf1	forward	1
192.99.39.151	Canada	147.237.76.44	e.refuah.idf.il	Block_Udp_All_Nets	drop	1
184.26.161.65	United States	147.237.76.38	e.e.meitav.idf.il	Block_Udp_All_Nets	drop	1
52.53.222.9	United States	147.237.76.197	e.himush.idf.il	Block_Ntp_All_Net	drop	1
142.54.160.211	United States	147.237.72.156	aman.idf.il	block-sp-traf1	drop	1
185.130.5.224		147.237.76.34	yohalan.idf.il	Block_Udp_All_Nets	drop	1
74.91.28.61	United States	147.237.77.216	dover.idf.il	block-sp-traf1	drop	1

01-31-2016-23:04:01 to 02-01-2016-00:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
123.126.113.80	China	147.237.72.166	aka.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1
144.76.12.75	Germany	147.237.72.166	aka.idf.il	C106: HTTP: majestic bot	Block	1
151.80.31.134	Italy	147.237.76.31	nakchal.idf.i	C228: HTTP: AhrefBot crawler	Block	1
89.216.115.8		147.237.77.216	dover.idf.il	17272: HTTP: Suspicious User-Agent (WindowsNT) With No Separating Space	Block	1

01-31-2016-23:04:01 to 02-01-2016-00:04:01

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	4
212.116.170.92	147.237.77.216	Israel	dover.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	3
61.240.144.64	147.237.77.212	China	e.dover.idf.il	ET SCAN NMAP -sS window 1024	1
218.246.0.97	147.237.76.177	China	ncore.idf.il	ET SCAN NMAP -sS window 1024	1
59.45.79.117	147.237.0.15	China	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.77.243	China	mobile.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.77.234	China	halag.idf.il	ET SCAN Potential SSH Scan	1
189.69.159.161	147.237.8.27	Brazil	e.madim.atal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
59.45.79.117	147.237.77.179	China	e.mazi.idf.il	ET SCAN Potential SSH Scan	1
115.29.224.200	147.237.0.34	China	tikshuv.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
59.45.79.117	147.237.77.74	China	law.idf.il	ET SCAN Potential SSH Scan	1
95.86.96.216	147.237.72.166	Israel	aka.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1
59.45.79.117	147.237.76.201	China	e.atal.idf.il	ET SCAN Potential SSH Scan	1
93.173.153.16	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
59.45.79.117	147.237.76.197	China	e.himush.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.66	147.237.76.201	China	e.atal.idf.il	ET SCAN NMAP -sS window 1024	1
59.45.79.117	147.237.76.176	China	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.65	147.237.76.39	China	mobile.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
59.45.79.117	147.237.76.42	China	refuah.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.64	147.237.77.205	China	prisha.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
212.199.57.198	147.237.77.216	Israel	dover.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1
46.151.53.217	147.237.72.156	Ukraine	aman.idf.il	ET SCAN NMAP -sS window 1024	1
59.45.79.117	147.237.77.235	China	sviva.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.77.227	China	e.hamaz.idf.il	ET SCAN Potential SSH Scan	1
115.29.224.200	147.237.0.200	China	m4u.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
59.45.79.117	147.237.77.121	China	e.navy.idf.il	ET SCAN Potential SSH Scan	1
115.29.224.200	147.237.0.17	China	m.my-kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
59.45.79.117	147.237.77.61	China	e.cogat.idf.il	ET SCAN Potential SSH Scan	1
95.86.96.177	147.237.77.216	Israel	dover.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	1
59.45.79.117	147.237.76.198	China	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.67	147.237.77.179	China	e.mazi.idf.il	ET SCAN NMAP -sS window 1024	1
59.45.79.117	147.237.76.177	China	ncore.idf.il	ET SCAN Potential SSH Scan	1
61.240.144.66	147.237.72.166	China	aka.idf.il	ET SCAN NMAP -sS window 1024	1
59.45.79.117	147.237.76.44	China	e.refuah.idf.il	ET SCAN Potential SSH Scan	1

01-31-2016-23:04:01 to 02-01-2016-00:04:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
79.182.238.179	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	96
213.57.186.182	Israel	147.237.0.19	madim.atal.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	34
109.253.129.138	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	33
195.239.16.40	Russian Federation	147.237.77.74	law.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	26
195.239.16.53	Russian Federation	147.237.77.74	law.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	26
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	25
41.230.14.223	Tunisia	147.237.72.166	aka.idf.il	drop	SAM rule	drop	21
2.54.47.91	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	17
37.26.148.141	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	16
212.76.127.219	Israel	147.237.76.30	himush.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	15
41.230.14.223	Tunisia	147.237.77.216	dover.idf.il	drop	SAM rule	drop	14
93.172.190.110	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
109.66.99.116	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
109.253.143.39	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
212.76.127.10	Israel	147.237.76.30	himush.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	12
46.19.86.113	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	11
79.180.98.52	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
188.161.118.70	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
79.176.15.57	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
87.69.195.92	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
213.57.47.107	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
212.199.57.194	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
2.54.34.241	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
172.56.36.252	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
2.54.38.232	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
37.26.148.141	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	8
132.66.48.33	Israel	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
31.168.197.195	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
94.159.253.55	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop		drop	7
46.19.85.148	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.86.226	Israel	147.237.0.19	madim.atal.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
149.255.208.96	Iraq	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.148	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
109.66.229.242	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
104.200.151.74	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
213.57.160.177	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
212.143.40.201	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
31.154.254.74	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
109.65.160.67	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
79.181.191.109	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
85.64.57.74	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
2.54.47.91	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
79.178.170.153	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
2.54.47.91	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	5
109.253.134.130	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
84.95.251.118	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	5
109.253.143.170	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
213.57.160.177	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
109.253.143.170	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
213.57.186.182	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	165
84.109.73.180	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	133
46.19.86.50	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	128
46.19.86.50	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	105
109.253.223.107	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	67
2.54.42.193	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	67
213.57.186.182	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	59
2.54.42.193	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	47
84.109.73.180	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	37
109.253.223.107	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	14
176.13.0.83	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
109.67.60.175	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1071	Block	5
185.120.126.59		147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	5
2.52.185.63	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation NewPassword in mobile.idf.il/sachar/changepassword	Block	4
149.50.74.173	United States	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
84.229.82.186	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 84.229.82.186	Block	4
149.88.52.180	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
84.109.73.180	Israel	147.237.77.243	mobile.idf.il	Distributed Parameter Type Violation on mobile.idf.il/sachar/login parameter Password	Block	3
2.52.185.63	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation Password in mobile.idf.il/sachar/login	Block	3
46.19.85.26	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.253.201.216	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.54.149.89	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.253.143.39	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
93.172.190.110	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
109.66.99.116	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
191.232.136.61	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/home/main/home/default.aspx	Block	2
77.127.190.124	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
68.180.229.173	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
217.194.198.104	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in Method from 217.194.198.104	Block	2
176.13.4.21	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
79.177.172.196	Israel	147.237.0.19	madim.atal.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtCity in madim.atal.idf.il/1088-he/meretz.aspx	Block	2
37.26.147.220	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/main/sachar/registrationwizard/register.aspx	None	2
176.13.17.109	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
46.19.85.177	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
2.52.185.63	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
84.229.82.186	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1362	Block	2
46.19.86.100	Israel	147.237.77.74	law.idf.il	Parameter Type Violation Master$Header1$ucHeaderSearch$txtSearch in www.law.idf.il/205-he/patzar.aspx	Block	2
2.54.54.210	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
109.253.147.221	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
69.171.228.122	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
208.184.112.74	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
66.249.65.80	Israel	147.237.76.147	chinuch.aka.idf.i	Unauthorized URL Access to www.chinuch.aka.idf.il/894-he	Block	1
178.218.117.7	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/article/watch	Block	1
103.194.170.165		147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/main.asp	Block	1
217.194.198.104	Israel	147.237.72.166	aka.idf.il	Multiple NULL Character in Header Name from 217.194.198.104	Block	1
46.19.85.200	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
217.194.198.104	Israel	147.237.72.166	aka.idf.il	Illegal HTTP Version	Block	1
79.178.191.172	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
5.144.63.66	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
217.194.198.104	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1