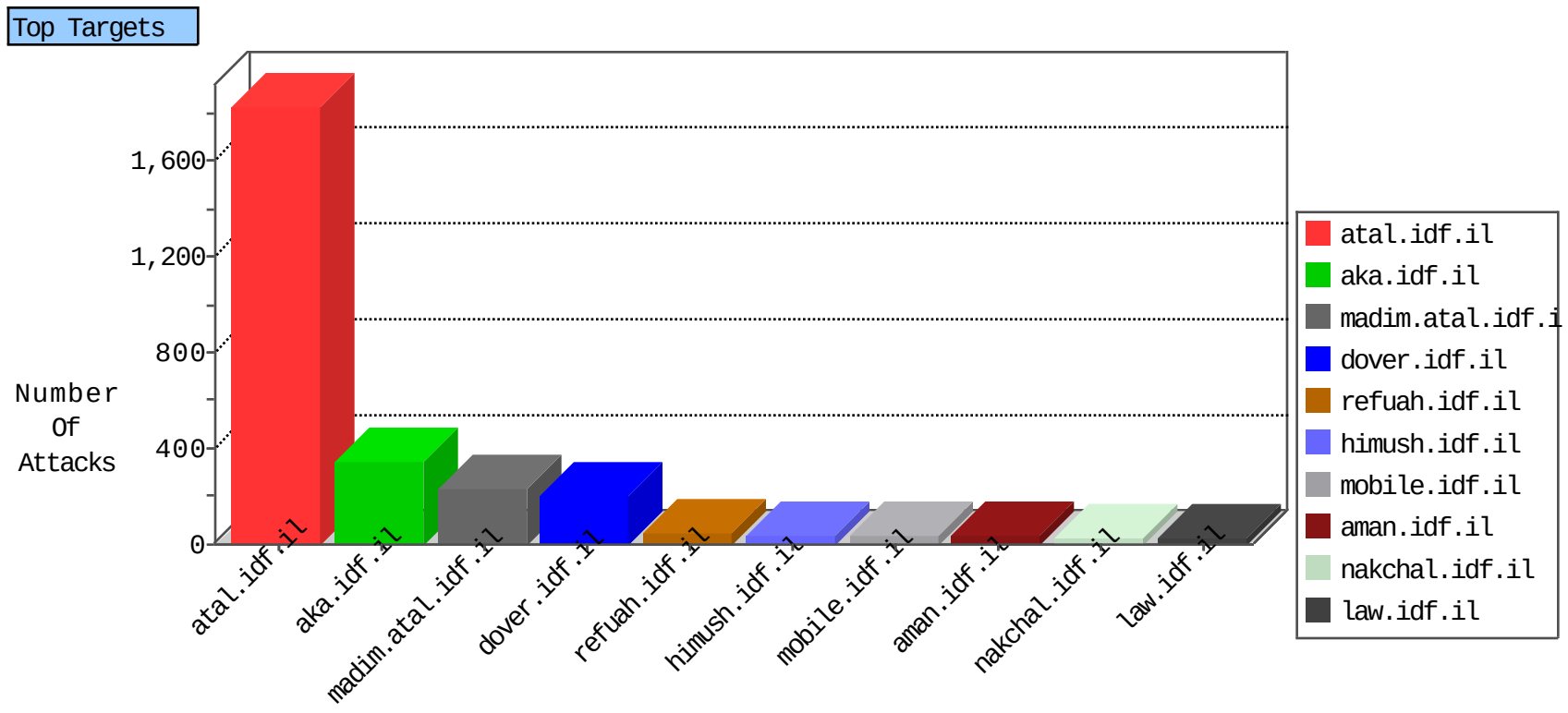
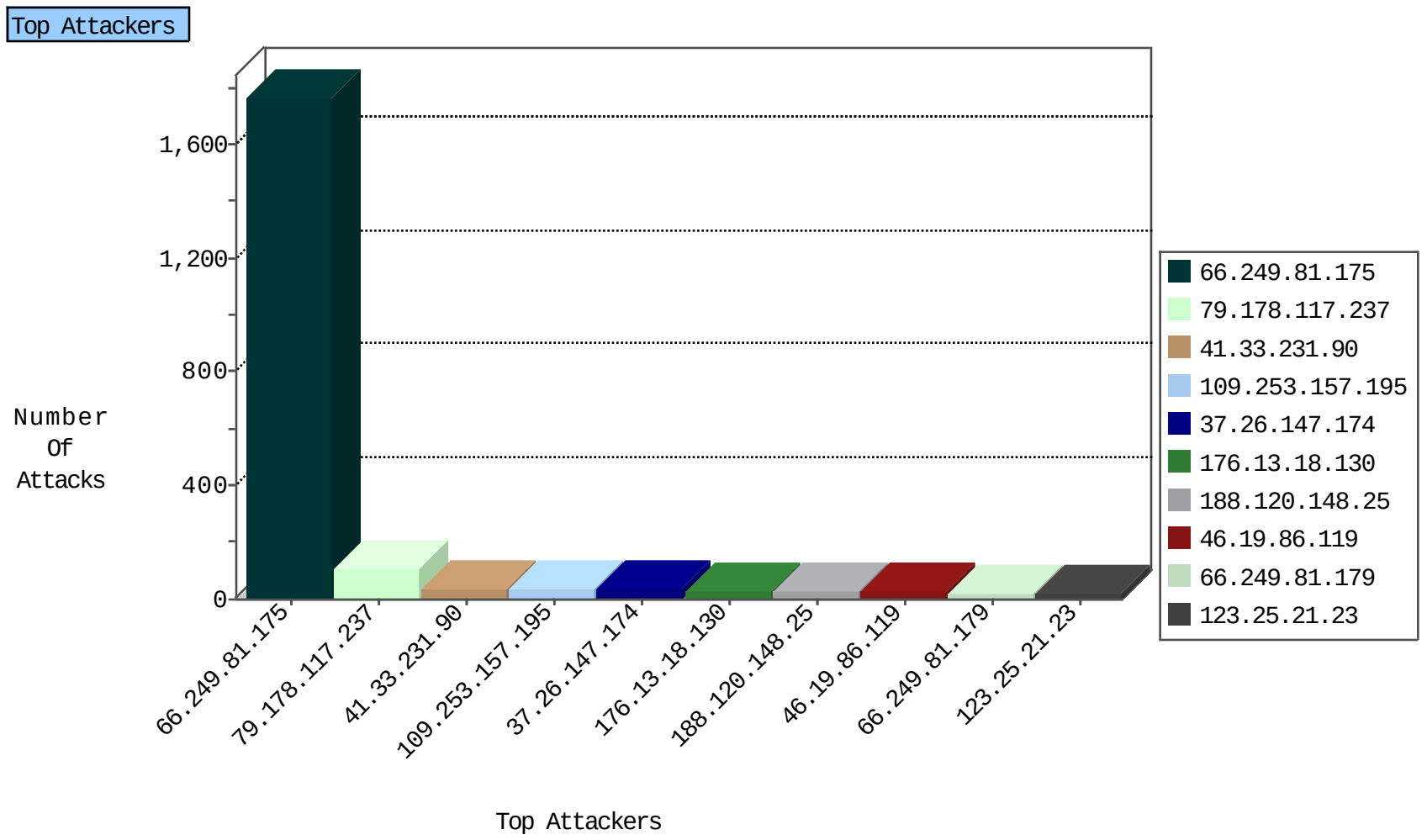
02-08-2016-19:04:03 to 02-08-2016-20:04:03

IDF Under Attack
Daily Report

Top Targets



Top Attackers



02-08-2016-19:04:03 to 02-08-2016-20:04:03

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	2
128.194.131.235	United States	147.237.72.166	aka.idf.il	block-sp-traf1	drop	2
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	2
79.103.166.153	Greece	147.237.77.227	e.hamaz.idf.il	Frk_Under_Attack_Con_Tcp	drop	1
142.54.160.212	United States	147.237.72.166	aka.idf.il	block-sp-traf1	drop	1

02-08-2016-19:04:03 to 02-08-2016-20:04:03

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

02-08-2016-19:04:03 to 02-08-2016-20:04:03

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
66.249.81.175	147.237.77.233	United States	atal.idf.il	ET SCAN NMAP -sA (2)	1753
80.246.133.177	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	8
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
66.249.81.179	147.237.77.233	United States	atal.idf.il	ET SCAN NMAP -sA (2)	2
85.65.124.77	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.121.203.117	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
123.25.21.23	147.237.76.44	Vietnam	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
213.57.41.99	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
84.94.80.32	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.116.127.86	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
123.25.21.23	147.237.76.34	Vietnam	yohalan.idf.il	ET SCAN Potential SSH Scan	1
82.81.129.158	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.97.11.102	147.237.76.86	Romania	navy.idf.il	ET SCAN Potential SSH Scan	1
123.25.21.23	147.237.8.46	Vietnam	e.chinuch.idf.il	ET SCAN Potential SSH Scan	1
178.39.218.11	147.237.77.216	Switzerland	dover.idf.il	portscan: TCP Distributed Portscan	1
123.25.21.23	147.237.8.28	Vietnam	e.mobile-ks.idf.il	ET SCAN Potential SSH Scan	1
79.180.230.151	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
123.25.21.23	147.237.77.233	Vietnam	atal.idf.il	ET SCAN Potential SSH Scan	1
123.25.21.23	147.237.0.35	Vietnam	akaws.idf.il	ET SCAN Potential SSH Scan	1
123.25.21.23	147.237.77.178	Vietnam	e.matpash.idf.il	ET SCAN Potential SSH Scan	1
123.25.21.23	147.237.0.16	Vietnam	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
123.25.21.23	147.237.76.199	Vietnam	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
62.83.80.168	147.237.77.216	Spain	dover.idf.il	portscan: TCP Distributed Portscan	1
94.102.51.30	147.237.77.212	Netherlands	e.dover.idf.il	ET SCAN NMAP -sS window 1024	1
123.25.21.23	147.237.76.196	Vietnam	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
46.166.129.183	147.237.77.74	Netherlands	law.idf.il	ET SCAN NMAP -sS window 2048	1
93.158.152.31	147.237.72.166	Russian Federation	aka.idf.il	portscan: TCP Distributed Portscan	1
46.166.129.183	147.237.77.74	Netherlands	law.idf.il	ET SCAN NMAP -f -sS	1
123.25.21.23	147.237.76.86	Vietnam	navy.idf.il	ET SCAN Potential SSH Scan	1
213.57.230.133	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
84.228.194.207	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.117.128.186	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
123.25.21.23	147.237.76.38	Vietnam	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
82.117.208.243	147.237.76.196		e.sviva.idf.il	ET SCAN NMAP -sS window 1024	1
212.47.237.95	147.237.77.212	France	e.dover.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
46.97.11.102	147.237.77.216	Romania	dover.idf.il	ET SCAN Potential SSH Scan	1
123.25.21.23	147.237.8.50	Vietnam	e.tikshuv.idf.il	ET SCAN Potential SSH Scan	1
81.169.251.74	147.237.77.179	Germany	e.mazi.idf.il	ET SCAN NMAP -sS window 1024	1
193.104.41.141	147.237.76.198	Moldova, Republic of	e.yohalan.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
46.97.11.102	147.237.76.31	Romania	nakchal.idf.il	ET SCAN Potential SSH Scan	1
123.25.21.23	147.237.8.45	Vietnam	e.eitan.idf.il	ET SCAN Potential SSH Scan	1
80.82.79.104	147.237.0.200	Netherlands	m4u.idf.il	ET SCAN NMAP -sS window 1024	1
123.25.21.23	147.237.77.235	Vietnam	sviva.idf.il	ET SCAN Potential SSH Scan	1
123.25.21.23	147.237.8.27	Vietnam	e.madim.atal.idf.il	ET SCAN Potential SSH Scan	1
79.178.27.20	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
123.25.21.23	147.237.77.226	Vietnam	www.chamatz.aka.idf.il	ET SCAN Potential SSH Scan	1
123.25.21.23	147.237.0.33	Vietnam	idf.il	ET SCAN Potential SSH Scan	1
123.25.21.23	147.237.77.176	Vietnam	matpash.idf.il	ET SCAN Potential SSH Scan	1
109.253.197.160	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
123.25.21.23	147.237.76.197	Vietnam	e.himush.idf.il	ET SCAN Potential SSH Scan	1

02-08-2016-19:04:03 to 02-08-2016-20:04:03

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
109.253.157.195	Israel	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	alert	22
188.120.148.25	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	21
66.249.81.179	United States	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	19
109.67.154.8	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
66.249.81.175	United States	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	14
77.125.110.157	Israel	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	14
109.253.157.195	Israel	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	monitor	14
66.249.81.183	United States	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	14
109.253.216.82	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
91.206.181.242	Poland	147.237.77.216	dover.idf.il	drop	SAM rule	drop	12
2.52.49.124	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
176.228.217.52	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	9
37.26.147.155	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
5.29.196.61	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	8
46.19.86.61	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	8
188.161.1.64	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
66.249.66.93	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
80.246.133.177	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
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
66.249.66.95	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.100	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
98.124.11.59	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
79.177.30.172	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
66.249.81.174	United States	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.86	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
98.124.11.59	Canada	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
46.19.86.227	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
79.177.54.220	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
188.120.148.25	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
2.52.51.49	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
176.13.18.187	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.134	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
109.65.212.184	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
46.19.85.44	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	5
46.19.85.134	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
85.65.151.224	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
176.13.7.245	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
149.88.127.27	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
130.203.136.75	United States	147.237.72.166	aka.idf.il	drop	SAM rule	drop	4
31.210.186.49	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
213.140.59.136	Algeria	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
81.218.44.19	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
149.88.127.27	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
84.109.137.80	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.183.1.133	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
185.27.105.184	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

02-08-2016-19:04:03 to 02-08-2016-20:04:03

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.178.117.237	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	66
79.178.117.237	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 79.178.117.237	Block	40
37.26.147.174	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	34
176.13.18.130	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	29
46.19.86.119	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	28
80.246.136.213	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	15
84.228.182.148	Israel	147.237.0.34	tikshuv.idf.il	Too Many of the Same Response Code (404) in Session from 84.228.182.148	Block	9
109.253.221.212	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
128.194.131.148	United States	147.237.72.166	aka.idf.il	Multiple NULL Character in Method from 128.194.131.148	Block	4
79.177.148.153	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.52.49.124	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
46.19.85.86	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
86.171.45.11	United Kingdom	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	2
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.233	Block	2
2.54.53.81	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
176.13.0.125	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
5.28.135.102	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
79.182.206.190	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/undefined	Block	1
185.25.151.159	Poland	147.237.77.19	law-forum.idf.il	Unauthorized URL Access to testp5.mielno.lubin.pl/testproxy.php	Block	1
128.194.131.235	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/robots.txt	Block	1
66.249.78.18	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1396-he/atal.aspx	Block	1
109.65.53.86	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/https:/www.idf.il/	Block	1
2.54.63.93	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	1
198.20.69.74	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/	Block	1
81.200.91.15	Russian Federation	147.237.77.216	dover.idf.il	Parameter Type Violation lang in www.idf.il/1395-en/dover.aspx	Block	1
176.13.2.105	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
54.67.38.74	United States	147.237.0.19	madim.atal.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
109.160.167.18	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$btnAtudaPrint in www.aka.idf.il/main/giyus/atuda/asmachta.aspx	None	1
5.62.131.135	Russian Federation	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/arr/	Block	1
80.246.133.177	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1134-he/atal.aspx	Block	1
185.25.151.159	Poland	147.237.77.216	dover.idf.il	Unauthorized URL Access to testp4.pospr.waw.pl/testproxy.php	Block	1
128.232.110.28	United Kingdom	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/	Block	1
68.180.230.244	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	1
109.65.128.243	Israel	147.237.77.226	www.chamatz.aka.idf.il	Multiple Unauthorized URL Access from 109.65.128.243	Block	1
2.54.132.41	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/favicon.ico	Block	1
199.16.156.124	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/8/size220x0/16838.jpg	Block	1
83.130.99.240	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl38$ctl01$ctl03$cblQuestion$3 in www.aka.idf.il/main/giyus/questionnaire.aspx	None	1
176.13.8.57	Israel	147.237.77.216	dover.idf.il	Multiple Fullwidth/Halfwidth Unicode Encoding on URL/Parameter(+) from 176.13.8.57	Block	1
109.253.203.121	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-ar	Block	1
87.68.159.39	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$employmentStatus in www.aka.idf.il/main/sachar/payslips.aspx	None	1
185.25.151.159	Poland	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to testp5.mielno.lubin.pl/testproxy.php	Block	1
141.0.12.242	Norway	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/ar/uplouded	Block	1
77.66.60.75	Denmark	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/robots.txt	Block	1
46.19.86.162	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/favicon.ico	Block	1
109.65.128.243	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/sip_storage/files/8/	Block	1
2.54.179.67	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
83.166.235.5	Russian Federation	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
66.249.66.26	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1400-he/atal.aspx	Block	1
93.172.138.130	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
41.82.114.152	Senegal	147.237.77.216	dover.idf.il	E-mail collector robots 14	Block	1

02-08-2016-19:04:03 to 02-08-2016-20:04:03