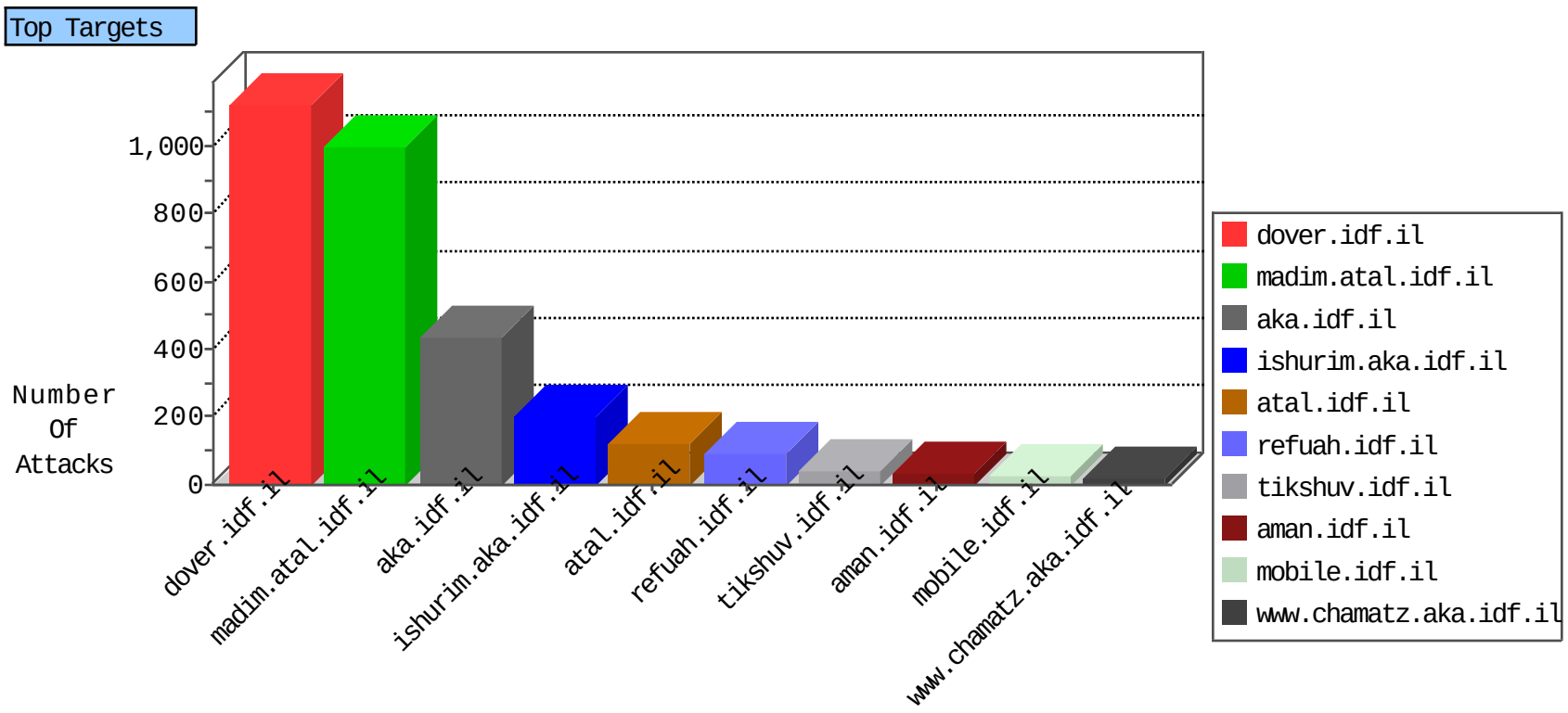
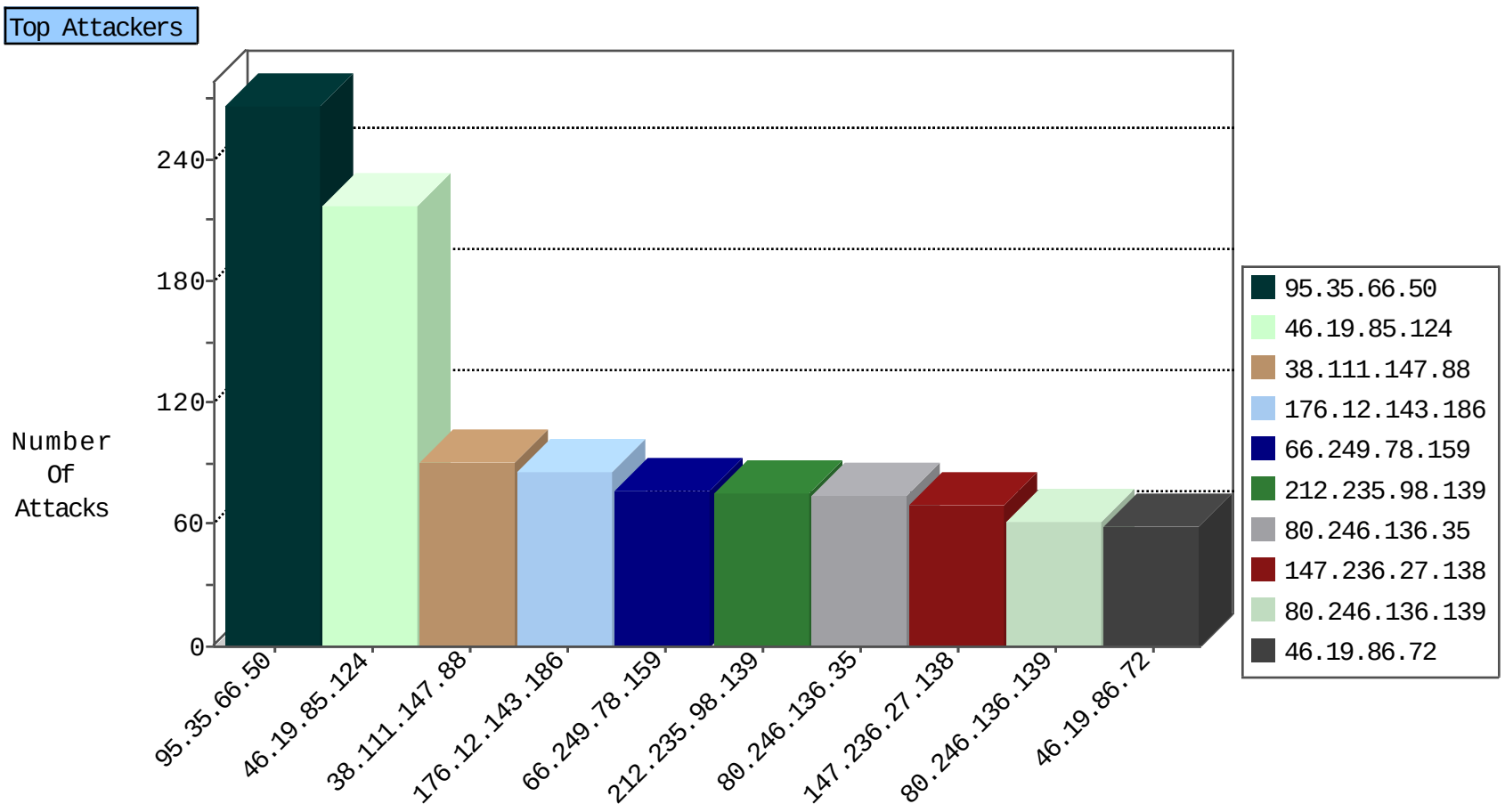
11-22-2015-10:04:06 to 11-22-2015-11:04:06

IDF Under Attack
Daily Report



Top Target



Top Attackers

11-22-2015-10:04:06 to 11-22-2015-11:04:06

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
192.118.30.102	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	245
80.179.18.228	Israel	147.237.72.167	ishurim.aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	154
82.166.219.240	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	14
212.143.3.44	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	9
10.0.0.4		147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	5
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	4
31.168.233.62	Israel	147.237.72.156	aman.idf.il	Block_Udp_All_Nets	drop	3
212.150.59.209	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	3
2.54.172.70	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	3
134.147.203.115	Germany	147.237.76.176	test.ncore.idf.il	Block_Ntp_All_Net	drop	2
192.114.23.208	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
79.177.220.10	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	2
115.231.222.40	China	147.237.0.15	kosher-kravi.idf.il	Frk_Under_Attack_Con_Http	drop	2
185.120.126.12		147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
109.253.93.174	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
2.54.37.86	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
115.231.222.40	China	147.237.0.15	kosher-kravi.idf.il	Frk_Purple_Con_Limit_Http	drop	1
185.3.144.120	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
195.69.239.21	Russian Federation	147.237.76.196	e.sviva.idf.il	Block_Udp_All_Nets	drop	1

11-22-2015-10:04:06 to 11-22-2015-11:04:06

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
147.236.31.111	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1

11-22-2015-10:04:06 to 11-22-2015-11:04:06

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
212.179.21.194	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	2
80.246.137.63	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
77.127.182.249	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
222.127.194.190	147.237.76.201	Philippines	e.atal.idf.il	ET SCAN NMAP -sS window 1024	1
65.55.215.49	147.237.72.166	United States	aka.idf.il	portscan: TCP Distributed Portscan	1
216.250.117.57	147.237.76.148	United States	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
46.19.86.24	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
216.250.117.57	147.237.0.19	United States	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
176.12.144.163	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
109.66.80.183	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
81.218.135.161	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.180.16.110	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
66.249.64.60	147.237.72.166	United States	aka.idf.il	portscan: TCP Distributed Portscan	1
216.250.117.57	147.237.76.200	United States	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
46.228.207.18	147.237.77.74	Germany	law.idf.il	ET SCAN NMAP -sS window 1024	1
216.250.117.57	147.237.0.200	United States	m4u.idf.il	ET SCAN Potential SSH Scan	1
185.32.179.141	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
149.78.141.232	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
85.64.93.26	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

11-22-2015-10:04:06 to 11-22-2015-11:04:06

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
38.111.147.88	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	91
212.235.98.139	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	76
66.249.78.159	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	74
147.236.27.138	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	69
208.115.111.73	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	44
46.19.86.72	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	43
208.69.40.101	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	42
46.19.85.218	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	36
107.182.131.117	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	31
72.9.148.10	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	28
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	28
50.65.198.88	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	26
212.179.21.194	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	23
89.234.157.254	France	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
54.224.21.23	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	21
212.235.103.211	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	17
46.19.85.67	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	17
2.52.26.139	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	16
46.19.86.72	Israel	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	16
100.100.32.209		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	15
109.186.97.98	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	13
46.19.85.251	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	13
46.19.85.178	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	13
54.244.22.103	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
100.100.8.74		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	12
79.183.36.112	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
31.186.228.32	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
31.186.228.58	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
82.166.219.240	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
2.52.22.71	Israel	147.237.77.226	www.chamatz.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	11
31.186.228.95	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
192.114.105.254	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
31.186.228.60	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
185.120.126.12		147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	10
68.180.228.112	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
100.100.28.63		147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	10
31.186.228.94	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
31.186.228.59	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
31.186.228.31	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
2.52.26.139	Israel	147.237.76.42	refuah.idf.il	SYN Attack		reject	9
100.100.28.63		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
31.168.85.251	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
2.52.26.139	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
185.120.126.12		147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	alert	8
2.52.26.139	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid sequence number	monitor	8
176.12.140.165	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
31.186.228.96	United Kingdom	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
31.186.228.57	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
46.19.85.217	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8

11-22-2015-10:04:06 to 11-22-2015-11:04:06

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
95.35.66.50	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	140
95.35.66.50	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	115
46.19.85.124	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	107
46.19.85.124	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	99
176.12.143.186	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	80
80.246.136.35	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	68
80.246.136.139	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	61
176.12.147.96	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	54
176.12.149.226	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	42
2.54.138.151	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	37
176.13.0.179	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	36
2.54.7.41	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	29
176.12.151.42	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	19
46.19.85.124	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (403)	Block	9
37.26.147.149	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	8
185.32.179.166	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	8
37.142.225.37	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	6
2.54.1.112	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
81.218.241.25	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/$$$&?&?$$$	Block	6
80.246.136.35	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	6
176.13.10.13	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
80.246.136.254	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
194.90.229.225	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 194.90.229.225	Block	4
176.13.21.36	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	4
46.19.85.29	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
149.78.73.137	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/undefined	Block	4
176.13.4.126	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
46.19.86.51	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.14.163	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1071	Block	3
176.12.138.9	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.54.44.95	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.8.131	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.12.147.150	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
193.16.147.2	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/4/	Block	3
176.13.0.188	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
37.26.149.218	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
91.200.12.95	Ukraine	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	2
46.19.85.173	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	2
2.54.181.98	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
80.246.139.215	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
91.200.12.139	Ukraine	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	2
176.12.143.186	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	2
31.210.186.165	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.19.86.254	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
138.134.192.10	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/milnet	Block	1
2.54.141.218	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
84.108.130.62	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
188.120.153.23	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
109.64.165.189	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl49.y in www.aka.idf.il/main/sachar/viewpniot.aspx	None	1
217.194.202.17	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1

11-22-2015-10:04:06 to 11-22-2015-11:04:06