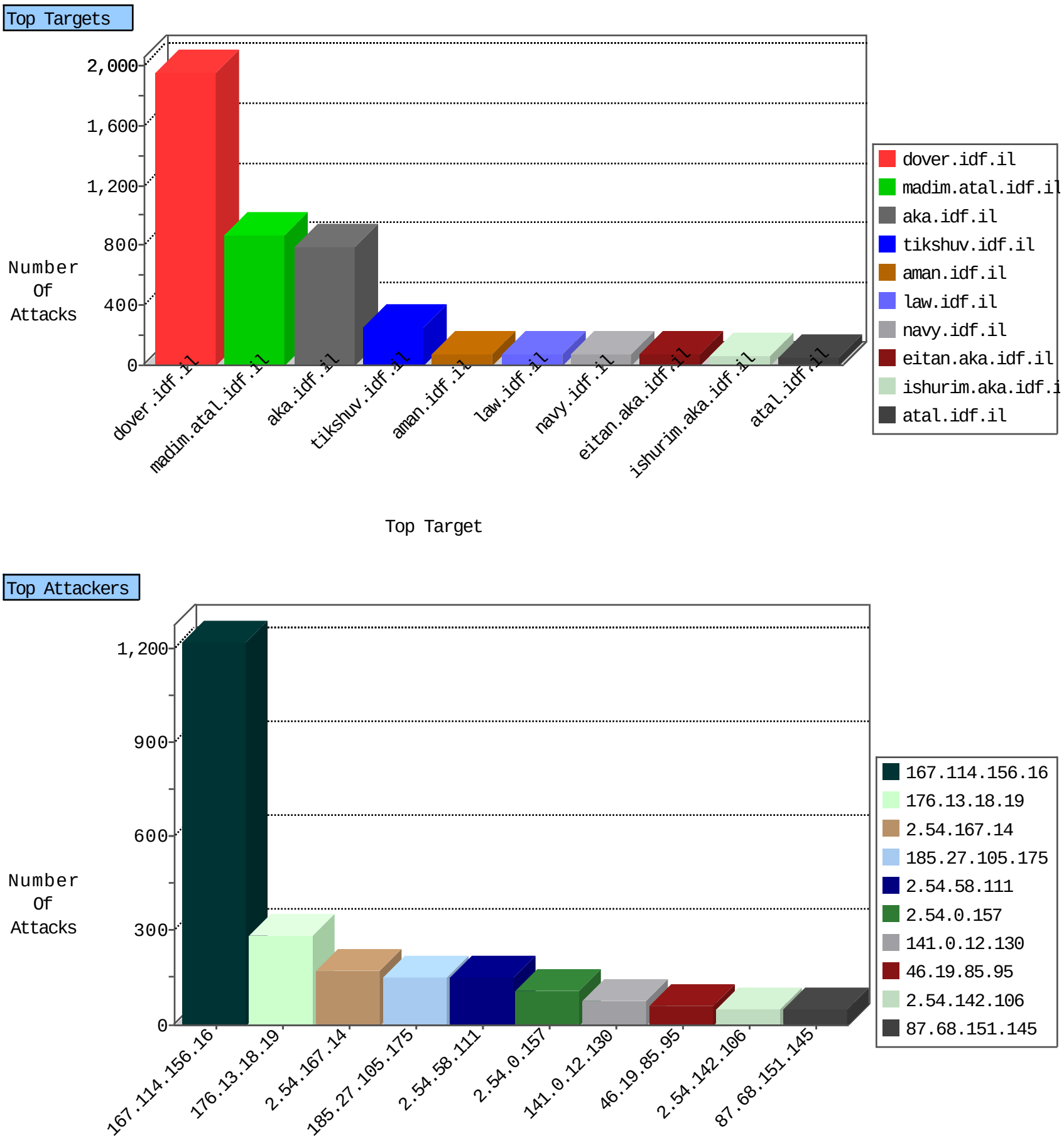
01-07-2016-12:04:06 to 01-07-2016-13:04:06

IDF Under Attack
Daily Report



01-07-2016-12:04:06 to 01-07-2016-13:04:06

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	3055
66.249.73.198	Israel	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	238
81.218.241.25	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	93
109.160.164.179	Israel	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	76
115.239.228.10	China	147.237.76.39	mobile.meitav.idf.il	JLM_Purple_Con_Limit_Http	drop	3
115.239.228.10	China	147.237.76.39	mobile.meitav.idf.il	JLM_Under_Attack_Con_Http	drop	2
77.247.178.132	Netherlands	147.237.76.196	e.sviva.idf.il	Block_Ntp_All_Net	drop	1
77.247.178.132	Netherlands	147.237.76.200	eitan.aka.idf.il	Block_Ntp_All_Net	drop	1

01-07-2016-12:04:06 to 01-07-2016-13:04:06

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.240.213.93	United States	147.237.76.177	ncore.idf.il	13891: TLS: OpenSSL Encrypted/Unencrypted Heartbeat Packet	Permit	2

01-07-2016-12:04:06 to 01-07-2016-13:04:06

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
109.253.144.172	147.237.77.216	Israel	dover.idf.il	GPL SCAN myscan	2
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	2
109.253.144.172	147.237.77.216	Israel	dover.idf.il	INDICATOR-SCAN myscan	2
59.45.79.117	147.237.76.199	China	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
177.101.78.179	147.237.0.35	Brazil	akaws.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
59.45.79.117	147.237.76.30	China	himush.idf.il	ET SCAN Potential SSH Scan	1
152.62.109.202	147.237.77.216	Europe	dover.idf.il	portscan: TCP Distributed Portscan	1
40.115.58.160	147.237.8.28	United States	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 1024	1
2.52.179.83	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
93.172.128.198	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
82.81.20.250	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
213.57.226.144	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
80.246.136.64	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
212.143.225.47	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
59.45.79.117	147.237.77.233	China	atal.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.77.178	China	e.matpash.idf.il	ET SCAN Potential SSH Scan	1
185.127.10.1	147.237.77.216		dover.idf.il	portscan: TCP Distributed Portscan	1
59.45.79.117	147.237.76.198	China	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
176.13.11.90	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
59.45.79.117	147.237.0.16	China	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
37.26.146.182	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.64.17.69	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
84.109.137.130	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
217.194.197.94	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
80.246.136.149	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
212.199.69.213	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.183.140.75	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
209.126.116.147	147.237.77.179	United States	e.mazi.idf.il	ET SCAN NMAP -sS window 1024	1
59.45.79.117	147.237.77.227	China	e.hamaz.idf.il	ET SCAN Potential SSH Scan	1
193.105.134.220	147.237.8.28	Sweden	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 1024	1

01-07-2016-12:04:06 to 01-07-2016-13:04:06

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
87.68.151.145	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	51
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
141.0.12.130	Norway	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	28
217.132.102.104	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	27
147.236.31.113	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	25
217.132.61.126	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
37.26.146.163	Israel	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	22
66.102.9.119	United States	147.237.77.234	halag.idf.il	drop	First packet isn't SYN	drop	22
77.125.115.139	Israel	147.237.72.167	ishurim.aka.idf.i	drop	First packet isn't SYN	drop	21
141.0.12.130	Norway	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	17
207.241.229.192	United States	147.237.72.166	aka.idf.il	drop	SAM rule	drop	17
66.249.93.99	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	16
46.19.86.225	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	15
31.168.11.194	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	14
46.19.86.158	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	14
80.179.114.11	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	14
66.249.93.107	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
66.102.9.5	United States	147.237.77.234	halag.idf.il	drop	First packet isn't SYN	drop	12
109.253.194.106	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
2.54.60.0	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
2.52.137.196	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
141.0.12.130	Norway	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
141.0.12.130	Norway	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	11
149.78.14.104	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
2.54.142.106	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	11
109.66.61.44	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
66.249.93.103	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
2.54.142.106	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	10
46.19.86.9	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
80.179.114.11	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	10
2.54.142.106	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	10
141.0.12.130	Norway	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	10
109.253.216.229	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	10
2.54.142.106	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
46.19.86.225	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
149.78.14.104	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	9
79.181.193.242	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
199.203.215.1	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
194.177.16.3	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
2.54.142.106	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	9
149.78.230.46	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.86.157	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	9
212.179.126.3	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
31.168.138.173	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
84.108.214.47	Israel	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
212.179.126.3	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	8
81.218.241.25	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	8
46.19.85.65	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
109.253.137.246	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.85.233	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
185.27.105.175	Israel	147.237.0.34	tikshuv.idf.il	Too Many of the Same Response Code (404) in Session from 185.27.105.175	Block	153
176.13.18.19	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	143
176.13.18.19	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	142
2.54.58.111	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	133
2.54.167.14	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	127
2.54.0.157	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	93
46.19.85.95	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	55
2.54.167.14	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	46
109.253.214.228	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	37
2.54.0.157	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	18
2.54.58.111	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 2.54.58.111	Block	17
46.210.137.25	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	15
80.246.136.72	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	12
2.54.54.57	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	9
46.19.86.15	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	9
213.57.189.144	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	8
185.32.179.96	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
46.19.85.95	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	5
79.177.145.9	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1152	Block	4
78.47.17.5	Germany	147.237.77.170	maarachot.idf.il	Distributed PHP Attempt	Block	3
46.19.85.79	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
109.253.146.192	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
79.177.145.9	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
176.13.18.179	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
46.120.212.117	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/6/	Block	3
204.13.200.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	3
109.66.61.44	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
2.54.47.2	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
40.77.167.17	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
78.47.17.5	Germany	147.237.77.170	maarachot.idf.il	Distributed Unauthorized URL Access on maarachot.idf.il/xmlrpc.php	Block	2
79.183.146.140	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
50.87.43.17	United States	147.237.77.170	maarachot.idf.il	Distributed PHP Attempt	Block	2
2.54.11.169	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/undefined	Block	2
176.13.20.204	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/sachar/index	Block	2
46.19.86.13	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to www.logistics.atal.idf.il/size100x0/sip_storage	Block	2
176.13.6.63	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
50.87.43.17	United States	147.237.77.170	maarachot.idf.il	Distributed Unauthorized URL Access on maarachot.idf.il/xmlrpc.php	Block	2
109.253.205.21	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
176.13.18.22	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
204.13.200.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	2
176.13.10.164	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/sachar/index	Block	2
107.178.194.79	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	2
78.46.5.136	Germany	147.237.77.170	maarachot.idf.il	Distributed PHP Attempt	Block	2
78.46.7.81	Germany	147.237.77.170	maarachot.idf.il	Distributed PHP Attempt	Block	2
50.62.161.217	United States	147.237.72.166	aka.idf.il	PHP Attempt	Block	1
109.253.146.67	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
2.54.184.41	Israel	147.237.77.216	dover.idf.il	Multiple Untraceable SSL Sessions from 2.54.184.41 (Open Mode)	None	1
185.27.105.175	Israel	147.237.0.34	tikshuv.idf.il	Too Many 404: Response Code per Session	Block	1
2.54.142.106	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
176.13.14.101	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1