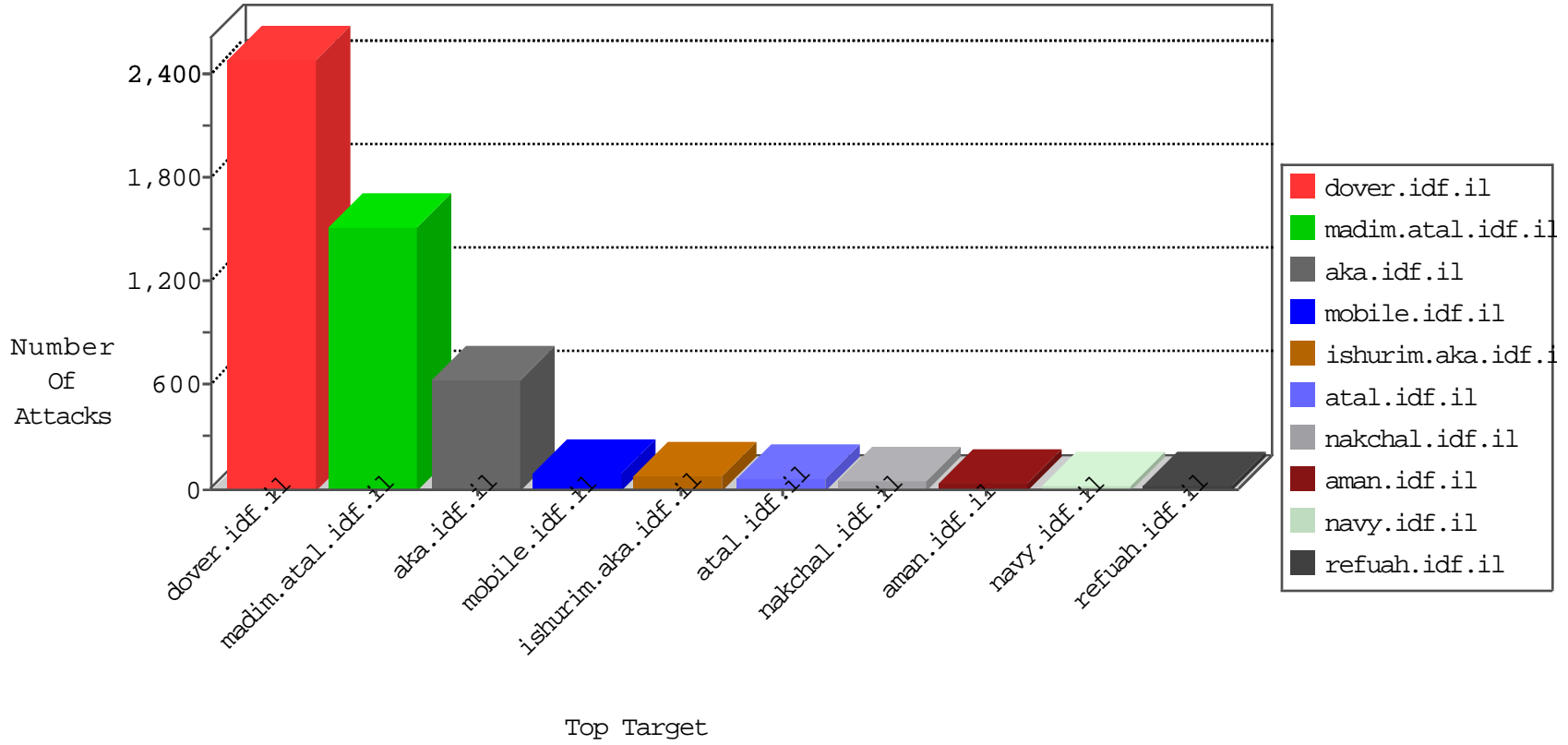


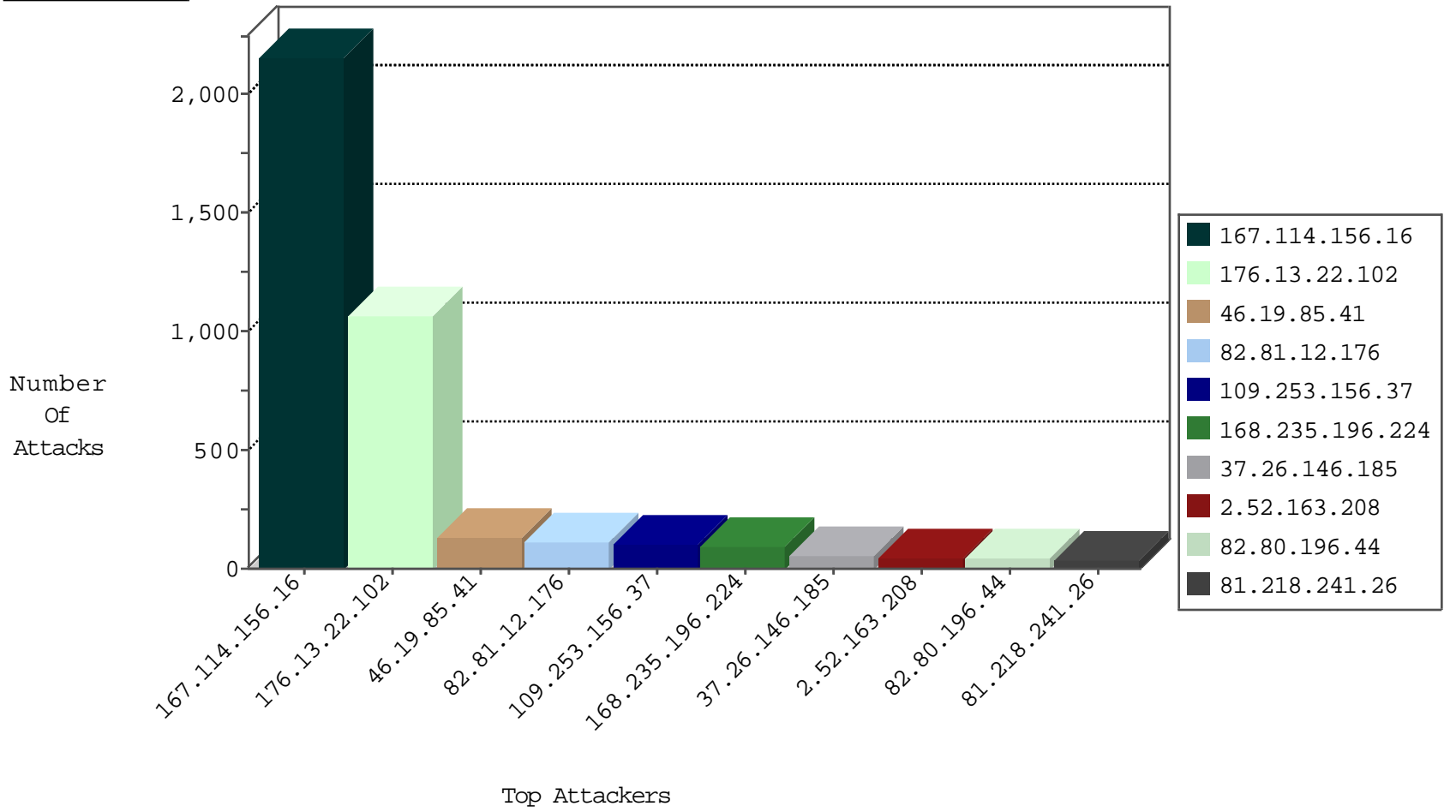
IDF Under Attack Daily Report



Top Targets



Top Attackers



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	3017
82.81.12.176	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	112
81.218.241.26	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	104
212.179.54.237	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
168.235.196.224	United States	147.237.77.216	dover.idf.il	F_Dover_Under_Attack_Con_Http	drop	2
38.229.1.13	United States	147.237.76.39	mobile.meitav.idf.il	Block_Ntp_All_Net	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
212.179.225.88	Israel	147.237.72.166	aka.idf.il	C008: HTTP: Xenu UserAgent	Block	1

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
66.249.64.181	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	2
84.95.2.150	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
66.249.78.165	147.237.72.166	United States	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
62.0.109.182	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
206.253.224.14	147.237.72.166	United States	aka.idf.il	portscan: TCP Distributed Portscan	1
193.201.227.70	147.237.76.39	Ukraine	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1
191.240.136.5	147.237.77.234	Brazil	halag.idf.il	ET SCAN NMAP -sS window 1024	1
132.74.216.184	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
90.188.10.98	147.237.8.46	Russian Federation	e.chimuch.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
79.181.202.87	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
218.246.0.97	147.237.76.202	China	e.halag.idf.il	ET SCAN NMAP -sS window 1024	1
193.201.227.70	147.237.76.148	Ukraine	ggcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
193.201.227.70	147.237.0.33	Ukraine	idf.il	ET SCAN Potential SSH Scan	1
147.236.34.81	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.253.139.84	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
168.235.196.224	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	90
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
141.8.132.112	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	33
49.151.63.18	Philippines	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	32
46.19.85.27	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	25
192.116.218.93	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	25
2.54.15.41	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
2.54.61.210	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	16
81.218.241.26	Israel	147.237.72.167	ishurim.aka.idf.i	drop	First packet isn't SYN	drop	13
176.13.16.89	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
80.179.23.231	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
81.218.241.26	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	12
85.130.128.146	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
40.77.167.27	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
176.13.17.118	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
82.80.196.44	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence		monitor	10
109.253.204.239	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.86.96	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
80.246.130.32	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
79.182.104.94	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	9
2.52.164.70	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
62.90.202.57	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
217.132.14.214	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	alert	8
109.253.145.92	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	8
95.199.8.43	Sweden	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
217.132.14.214	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	8
46.19.85.137	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
109.253.145.92	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	8
37.26.146.185	Israel	147.237.0.19	madim.atal.idf.il	Bad TCP sequence		monitor	7
192.117.138.210	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	7
46.19.85.101	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
2.54.142.198	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
2.54.18.157	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
109.64.137.251	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
192.116.218.93	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.86.92	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
80.246.130.32	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
81.218.161.149	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.180.51	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
109.64.137.251	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.86.18	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
59.46.215.131	China	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
46.19.85.44	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
82.80.196.44	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.19	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
37.26.148.189	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
82.80.196.44	Israel	147.237.72.167	ishurim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
46.19.85.19	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
192.116.239.196	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
192.116.148.105	Israel	147.237.72.166	aka.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
176.13.22.102	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	588
176.13.22.102	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	328
176.13.22.102	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (403) in Session from 176.13.22.102	Block	142
109.253.156.37	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	87
46.19.85.41	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	83
46.19.85.41	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	41
37.26.146.185	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	40
2.52.163.208	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	40
2.54.143.187	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	29
109.253.201.101	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	29
176.13.19.86	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	24
176.13.15.45	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	17
46.19.85.212	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	13
109.253.156.37	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	10
109.253.128.86	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
192.116.148.105	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 192.116.148.105	Block	5
2.54.15.41	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	5
176.228.192.21	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 176.228.192.21	Block	4
176.13.16.89	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	4
176.13.17.118	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	4
46.19.86.247	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.54.15.41	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.253.204.239	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
81.218.101.3	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/sip_storage/files/4/	Block	3
46.19.86.96	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
204.111.62.193	United States	147.237.77.74	law.idf.il	PHP Attempt	Block	3
109.253.159.35	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
204.111.62.193	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/xmlrpc.php	Block	3
192.116.148.105	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/7/	Block	3
193.33.2.113	Spain	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	2
107.178.194.87	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	2
89.138.68.250	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
69.171.231.225	United States	147.237.72.166	aka.idf.il	Multiple Post Request - Missing Content Type: 'none'	Block	2
109.253.223.70	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1152	Block	2
69.171.231.226	United States	147.237.72.166	aka.idf.il	Post Request - Missing Content Type	Block	2
79.182.214.203	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/undefined	Block	2
176.13.11.220	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
176.13.18.252	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
2.54.20.49	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
2.54.20.228	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
85.64.109.198	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/sachar/default.aspx	Block	1
216.218.206.66	United States	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.16/	Block	1
207.46.13.130	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/	Block	1
46.19.85.248	Israel	147.237.77.216	dover.idf.il	Illegal HTTP Version	Block	1
163.53.151.57	Bangladesh	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	1
81.218.101.3	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 81.218.101.3	Block	1
68.180.230.224	United States	147.237.76.31	nakchal.idf.il	Parameter Type Violation pageNum in www.nakchal.idf.il/1073-he/nakchal.aspx	Block	1
46.19.85.25	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/nekudot/index	Block	1
2.54.175.201	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	1
66.249.78.11	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1351-he/atal.aspx	Block	1