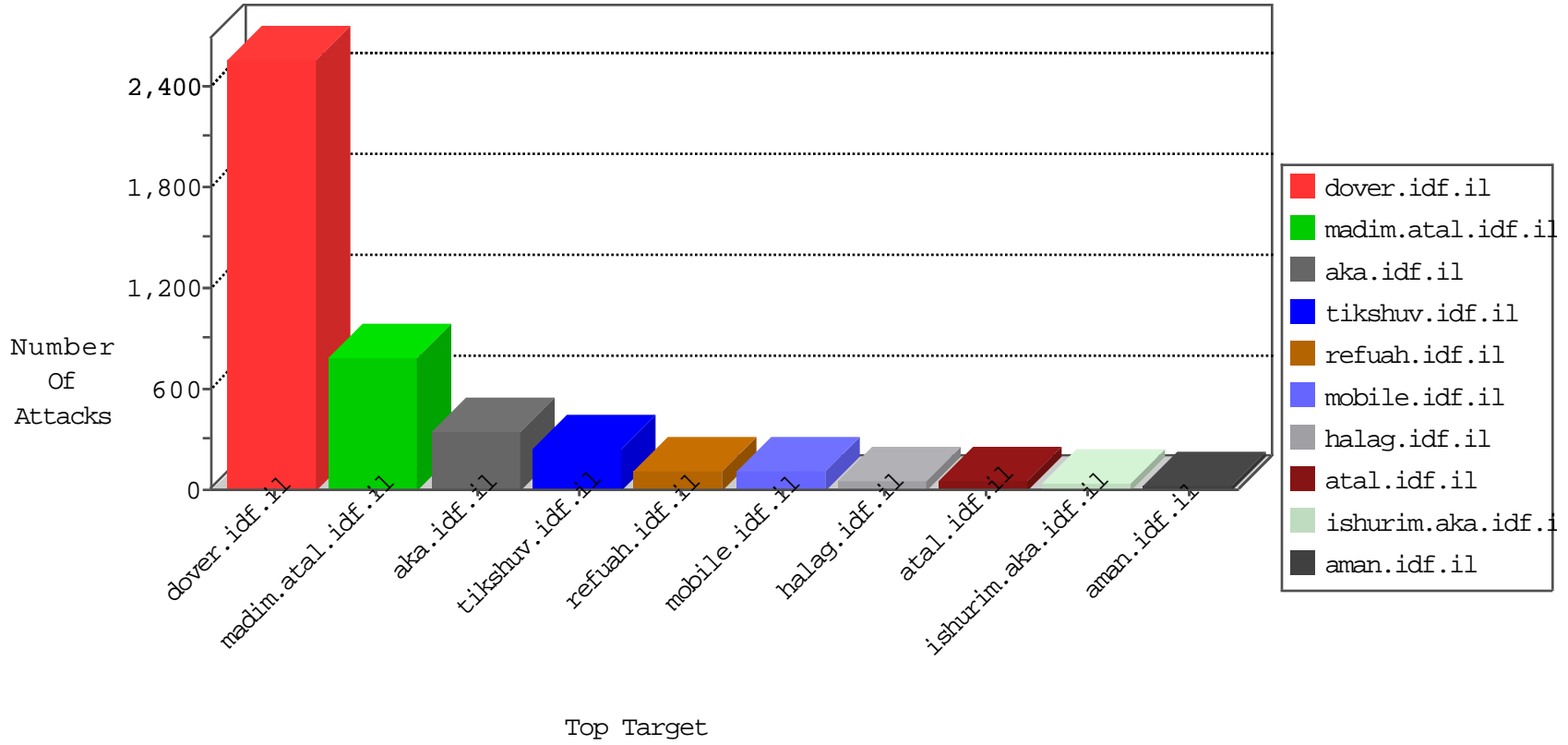


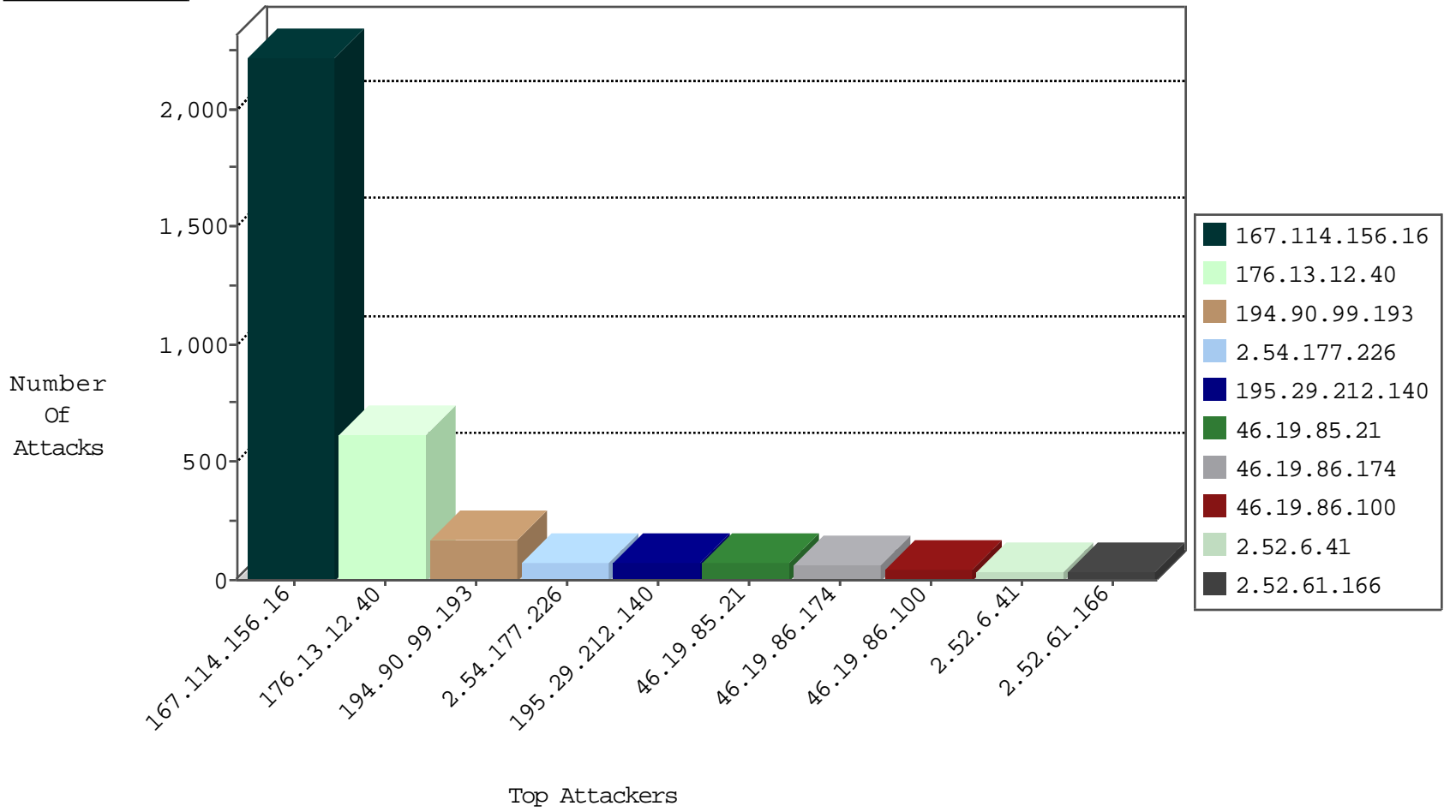
IDF Under Attack Daily Report



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	3173
79.177.11.229	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	6
79.180.30.243	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	6
107.150.60.242	United States	147.237.76.147	chinuch.aka.idf.il	block-sp-trafl	drop	1
58.97.111.10	Thailand	147.237.72.166	aka.idf.il	Invalid TCP Flags	drop	1
79.177.11.229	Israel	147.237.76.42	refuah.idf.il	Block_Udp_All_Nets	drop	1
107.150.60.244	United States	147.237.76.39	mobile.meitav.idf.il	block-sp-trafl	drop	1
63.141.227.98	United States	147.237.76.147	chinuch.aka.idf.il	Block_Ntp_All_Net	drop	1
66.240.219.146	United States	147.237.76.42	refuah.idf.il	Block_Udp_All_Nets	drop	1
58.97.111.9	Thailand	147.237.72.166	aka.idf.il	Invalid TCP Flags	drop	1
77.247.178.132	Netherlands	147.237.76.147	chinuch.aka.idf.il	Block_Udp_All_Nets	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
194.114.146.227	Israel	147.237.72.166	aka.idf.il	C1000169: Block - dns poisoning (Clalit)	Permit	2
182.160.107.83	Bangladesh	147.237.77.216	dover.idf.il	16798: HTTP: GNU Bash HTTP Header Remote Code Execution Vulnerability	Block	2
185.130.5.235		147.237.0.15	kosher-kravi.idf.il	20085: HTTP: Muieblackcat Security Scanner Initial Request	Block	1
185.130.5.235		147.237.0.19	madim.atal.idf.il	20085: HTTP: Muieblackcat Security Scanner Initial Request	Block	1
185.130.5.235		147.237.72.167	ishurim.aka.idf.il	20085: HTTP: Muieblackcat Security Scanner Initial Request	Block	1
172.245.24.138	United States	147.237.77.216	dover.idf.il	C1000106: HTTP: majestic bot	Block	1
185.130.5.235		147.237.76.30	himush.idf.il	20085: HTTP: Muieblackcat Security Scanner Initial Request	Block	1

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	1
185.130.5.235	147.237.72.167		ishurim.aka.idf.il	ET WEB_SERVER Muieblackcat scanner	1
185.130.5.216	147.237.76.38		e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
185.32.179.101	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
113.171.23.126	147.237.76.44	Vietnam	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
109.253.156.111	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.19.86.249	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
185.130.5.235	147.237.76.30		himush.idf.il	ET WEB_SERVER Muieblackcat scanner	1
185.130.5.231	147.237.76.177		noore.idf.il	ET SCAN Potential SSH Scan	1
185.130.5.216	147.237.72.166		aka.idf.il	ET SCAN Potential SSH Scan	1
185.12.24.202	147.237.77.216	Iraq	dover.idf.il	OS-WINDOWS Microsoft Forefront UAG javascript handler in URI XSS attempt	1
112.198.75.112	147.237.72.166	Philippines	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
79.177.63.118	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
195.29.212.140	Croatia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	73
46.19.86.174	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	63
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	34
217.132.7.202	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	28
46.19.85.21	Israel	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	24
213.8.41.250	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	21
212.179.21.194	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	20
80.246.130.89	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	19
79.177.63.118	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	18
85.64.204.140	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	15
2.52.6.41	Israel	147.237.77.234	halag.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	13
77.126.10.73	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	13
85.64.204.140	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
192.116.232.69	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	11
2.52.61.166	Israel	147.237.77.216	dover.idf.il	SYN Attack		reject	11
46.19.85.21	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
2.52.61.166	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	7
80.246.133.177	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
2.52.61.166	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
46.19.85.88	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
2.52.61.166	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
79.183.2.225	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
185.3.144.42	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.108	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
132.64.73.149	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.52.147.236	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.108	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
2.54.138.251	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.51	Israel	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
192.118.27.253	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
2.52.6.41	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
2.54.159.178	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
2.52.6.41	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	Invalid sequence number	monitor	5
46.19.85.149	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
46.19.85.88	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
37.26.146.172	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
2.52.6.41	Israel	147.237.77.234	halag.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
46.19.86.223	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
2.52.6.41	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
5.102.254.113	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
2.54.15.169	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
46.19.85.88	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.85.149	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	4
46.19.85.108	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.85.166	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
199.203.215.1	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.86.87	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
46.19.86.223	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
46.19.85.137	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	4

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.12.40	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	259
176.13.12.40	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	204
194.90.99.193	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	166
176.13.12.40	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 176.13.12.40	Block	133
2.54.177.226	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	64
46.19.86.100	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	42
46.19.85.21	Israel	147.237.0.34	tikshuv.idf.il	Too Many of the Same Response Code (404) in Session from 46.19.85.21	Block	37
109.253.211.188	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	30
176.13.12.40	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (403) in Session from 176.13.12.40	Block	18
17.138.57.83	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 17.138.57.83	Block	14
109.253.208.199	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1362	Block	14
2.54.177.226	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	10
80.246.139.242	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
212.179.180.30	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/sip_storage/files/6/size338x0/1796.jpg	Block	5
79.182.118.177	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 79.182.118.177	Block	5
62.219.99.130	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
176.13.3.148	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
81.218.241.25	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 81.218.241.25	Block	3
199.203.84.98	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 199.203.84.98	Block	3
112.198.75.112	Philippines	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in Method from 112.198.75.112	Block	2
109.253.199.156	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
109.253.138.204	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
112.198.75.112	Philippines	147.237.72.166	aka.idf.il	Multiple Malformed URL from 112.198.75.112	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
81.218.56.171	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 81.218.56.171	Block	2
109.253.146.26	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/nekudot/index	Block	2
79.182.118.177	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/sip_storage/files/8/	Block	2
112.198.75.112	Philippines	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in Header Name from 112.198.75.112	Block	2
112.198.75.112	Philippines	147.237.72.166	aka.idf.il	Multiple Unknown HTTP Request Method from 112.198.75.112	Block	2
109.253.128.7	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
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	2
193.106.206.10	Israel	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 193.106.206.10	Block	2
109.253.192.237	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/nekudot/index	Block	2
87.69.67.209	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/	Block	1
199.203.84.98	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/ gius	Block	1
112.198.75.112	Philippines	147.237.72.166	aka.idf.il	Malformed HTTP Header Line 1	Block	1
80.246.139.240	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
176.106.44.186	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Multiple Fullwidth/Halfwidth Unicode Encoding on URL/Parameter(+) from 176.106.44.186	Block	1
37.26.146.172	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	1
2.54.15.169	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
109.253.138.156	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
79.182.239.115	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/	Block	1
171.100.101.98	Thailand	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
107.178.194.79	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
68.180.229.239	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/iturim/asp/displayallsoliders.asp	Block	1
46.19.85.21	Israel	147.237.0.34	tikshuv.idf.il	Too Many 404: Response Code per Session	Block	1
112.198.75.112	Philippines	147.237.72.166	aka.idf.il	Illegal Byte Code Character in Header Value	Block	1
84.109.113.214	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
193.106.206.10	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/sip_storage/files/0/size338x0/1640.jpg	Block	1
80.246.136.142	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1