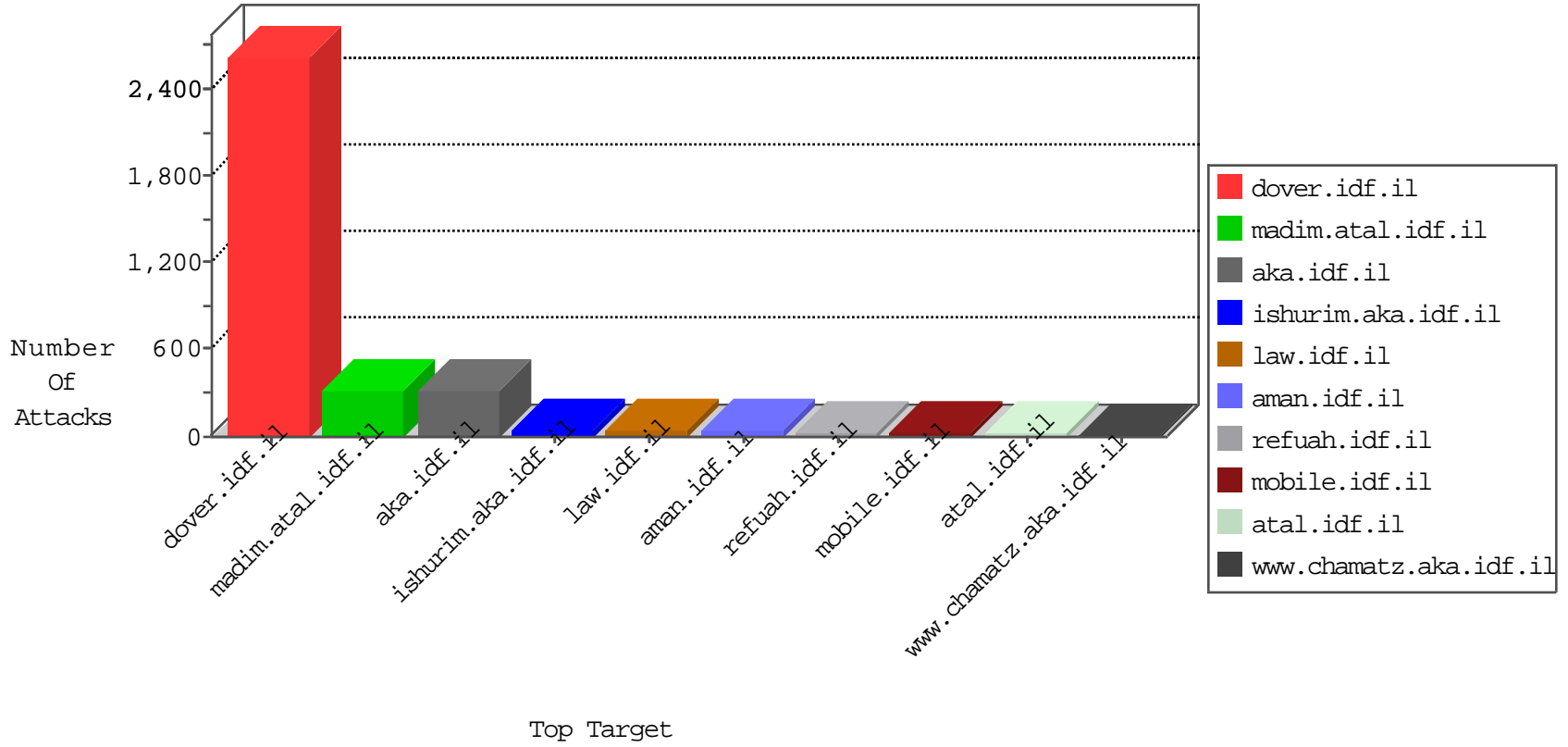


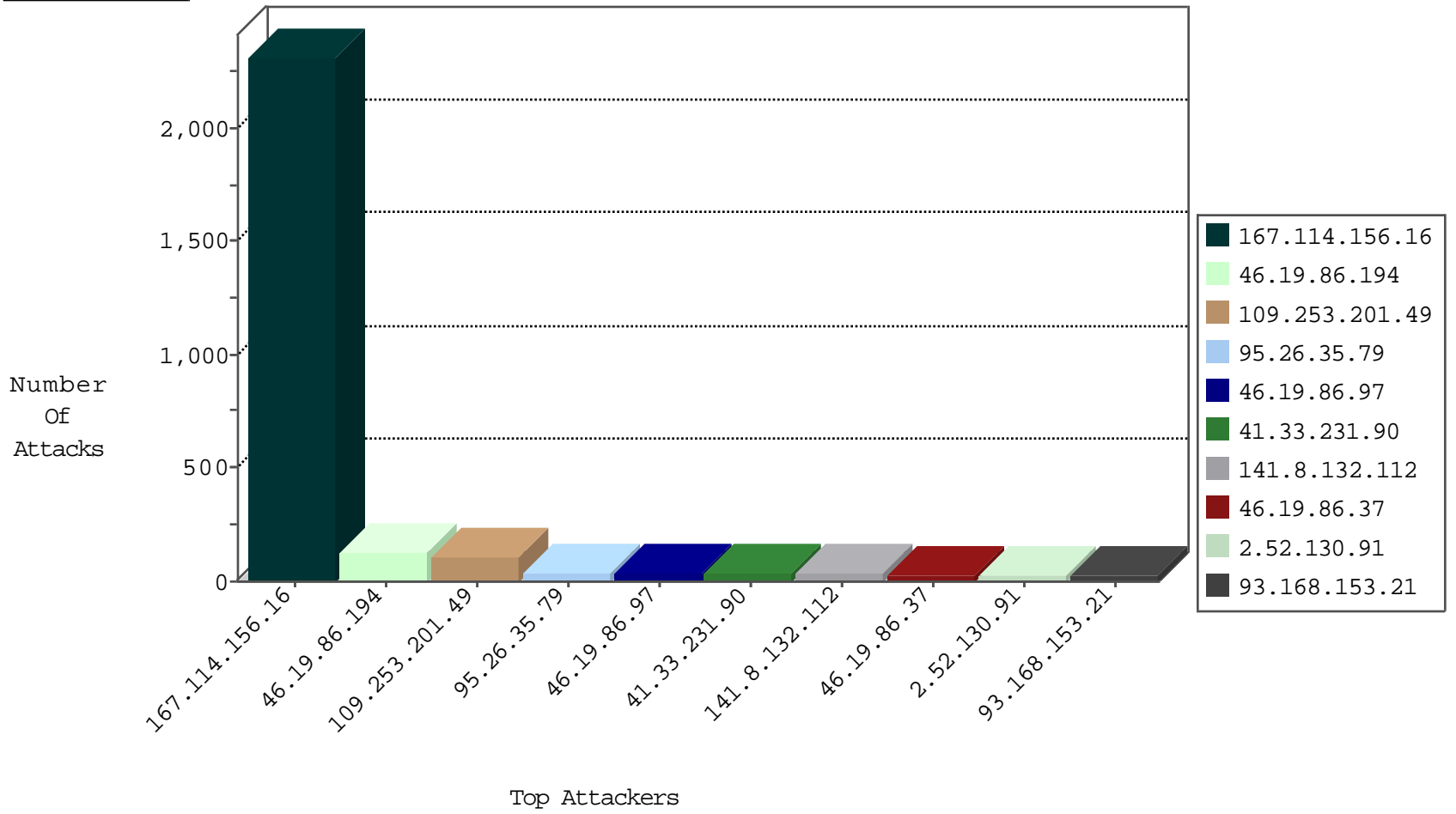
IDF Under Attack Daily Report



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	3067
24.114.75.4	Canada	147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	91
109.64.38.127	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	9
52.16.5.197	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
31.168.240.21	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
207.46.13.157	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	2
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	forward	2
142.54.160.214	United States	147.237.77.19	law-forum.idf.il	block-sp-traf1	drop	1
142.54.160.213	United States	147.237.0.15	kosher-kravi.idf.il	block-sp-traf1	forward	1
142.54.160.213	United States	147.237.72.166	aka.idf.il	block-sp-traf1	drop	1
95.100.174.66	Europe	147.237.76.202	e.halag.idf.il	Block_Udp_All_Nets	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
89.248.110.167	Spain	147.237.72.166	aka.idf.il	16798: HTTP: GNU Bash HTTP Header Remote Code Execution Vulnerability	Block	14
185.63.188.120	Russian Federation	147.237.77.216	dover.idf.il	16798: HTTP: GNU Bash HTTP Header Remote Code Execution Vulnerability	Block	1

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
2.54.36.64	147.237.72.166	Israel	aka.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	5
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	2
66.249.64.171	147.237.77.233	United States	atal.idf.il	ET SCAN NMAP -sA (2)	2
176.13.19.191	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
113.59.33.61	147.237.0.33	China	idf.il	ET SCAN NMAP -f -sS	1
46.19.85.64	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
2.54.23.227	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
220.231.195.122	147.237.0.15	China	kosher-kravi.idf.il	ET SCAN NMAP -sS window 3072	1
209.88.198.1	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
185.32.179.171	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
113.59.33.61	147.237.0.33	China	idf.il	ET SCAN NMAP -sS window 2048	1
220.231.195.122	147.237.0.15	China	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
199.203.68.10	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
193.169.70.108	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
95.26.35.79	Russian Federation	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	35
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
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	29
46.19.86.37	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	27
46.19.85.51	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	22
176.13.11.171	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	15
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
46.19.86.168	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
82.80.64.158	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	11
82.205.8.72	Palestinian Territory, Occupied	147.237.72.167	ishurim.aka.idf.il	drop	First packet isn't SYN	drop	10
141.8.184.5	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
2.54.150.162	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
93.168.153.21	Romania	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	8
46.19.86.160	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
93.168.153.21	Romania	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	8
2.52.130.91	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
62.209.28.112	Bahrain	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
109.253.136.120	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.36.64	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
5.22.130.224	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.79	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.86.194	Israel	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
79.183.228.29	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
93.158.152.31	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
31.168.89.106	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	6
93.168.153.21	Romania	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
141.8.184.25	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
40.77.167.20	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.67.170.243	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.50	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
2.52.130.91	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	5
188.178.248.115	Denmark	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
46.19.85.177	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	5
2.52.130.91	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
2.52.130.91	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.86.147	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
2.54.129.2	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
176.13.21.135	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
2.52.130.91	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
64.246.178.34	United States	147.237.76.86	navy.idf.il	Header Rejection	header rejection pattern found in request	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
46.19.86.103	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
5.22.130.224	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
109.65.129.23	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.52.3.55	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
46.19.85.177	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
132.64.73.149	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.151.198	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.253.201.49	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	109
46.19.86.194	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	77
46.19.86.194	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 46.19.86.194	Block	40
46.19.86.97	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	35
109.253.130.172	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	8
109.253.158.105	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	7
46.19.85.0	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
87.68.146.126	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.1.1	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.253.159.55	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.253.135.39	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.2.235	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
193.43.245.250	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 193.43.245.250	Block	2
82.80.33.138	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
109.253.136.120	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/sachar/index	Block	2
2.54.164.141	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
2.54.37.139	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
37.26.148.215	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
176.13.18.62	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/nekudot/index	Block	2
84.108.184.59	Israel	147.237.76.30	himush.idf.il	Unauthorized URL Access to www.chimush.atal.idf.il/xmlrpc.php	Block	1
185.32.179.128	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
31.168.199.226	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
176.13.9.157	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1136-he/atal.aspx	Block	1
81.218.116.129	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
2.54.23.176	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
109.253.219.144	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.64.239	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1250-he/atal.aspx	Block	1
107.178.194.83	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
37.26.148.233	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
176.13.21.135	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
80.246.136.23	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
2.54.154.155	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
157.55.39.125	United States	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/	Block	1
2.52.5.81	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.120.6.156	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/giyus/pniotfindanswer.aspx	None	1
204.13.201.138	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
46.19.85.255	Israel	147.237.72.166	aka.idf.il	Multiple Fullwidth/Halfwidth Unicode Encoding on URL/Parameter(+) from 46.19.85.255	Block	1
185.32.179.244	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Unknown SSL Session	None	1
37.26.146.188	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/www.tikshuv.idf.il	Block	1
176.13.11.171	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/layout.css	Block	1
81.218.140.160	Israel	147.237.77.233	atal.idf.il	PHP Attempt	Block	1
2.54.24.192	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/giyus/controls/atuda/Å	Block	1
110.5.76.82	India	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
66.249.79.75	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	1
46.116.243.93	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/controls/atuda/Å	Block	1
193.43.245.250	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/aisurim	Block	1
107.178.194.87	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
82.80.196.44	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
40.77.167.20	United States	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
180.190.66.180	Philippines	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1