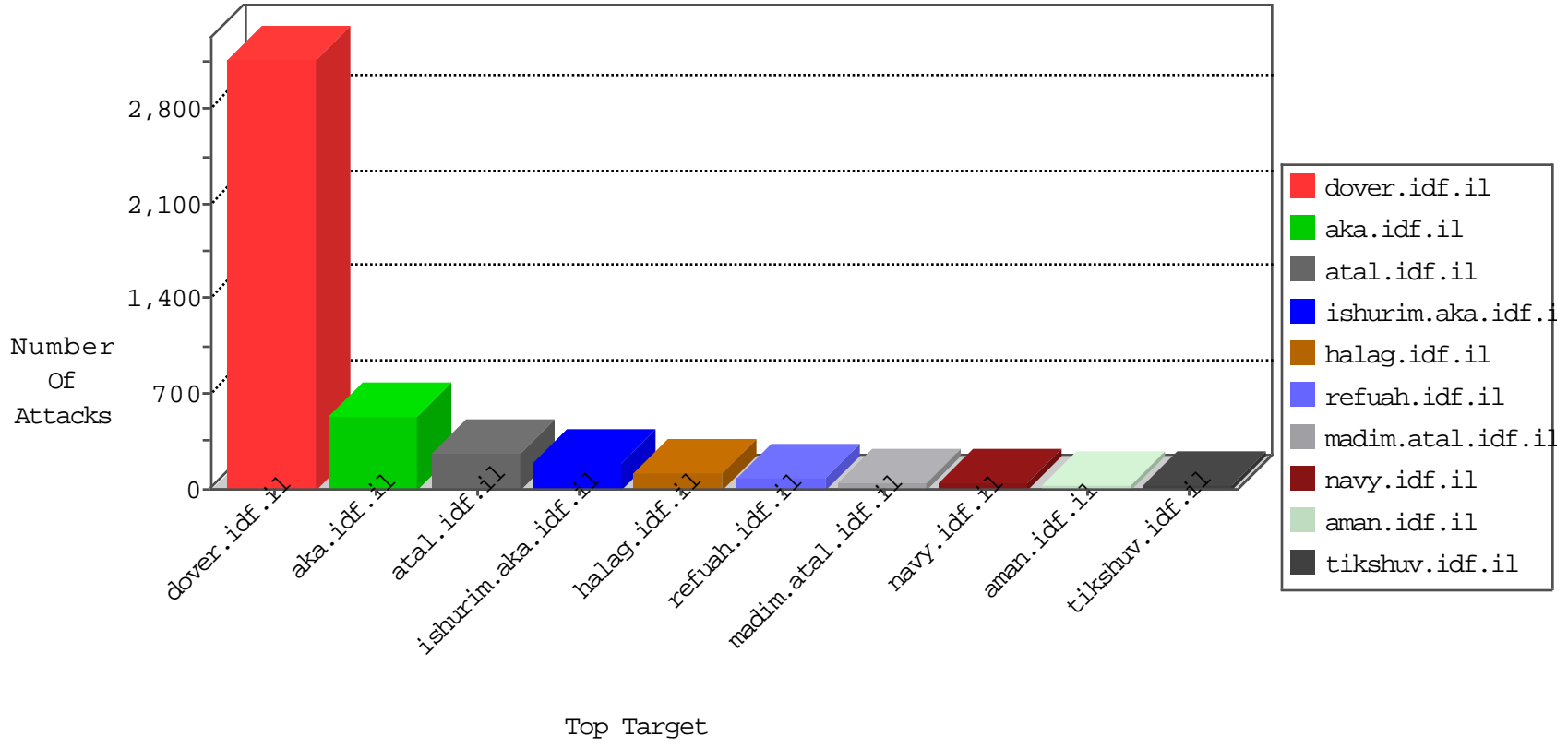


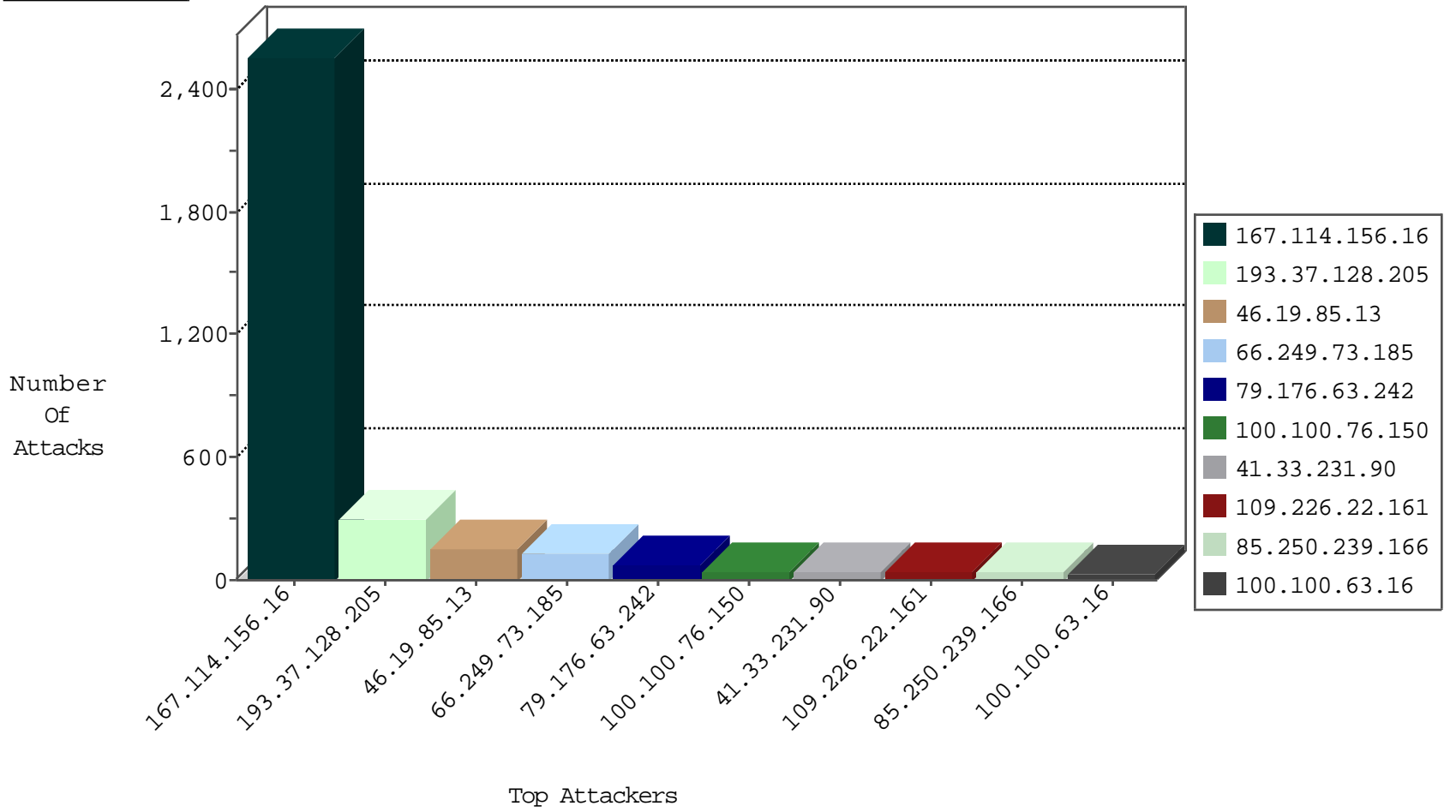
IDF Under Attack Daily Report



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	3366
66.249.78.82	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	131
81.218.5.130	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	12
91.208.129.129	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
79.178.110.130	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
149.78.2.63	Israel	147.237.76.200	eitan.aka.idf.il	Block_Udp_All_Nets	drop	3
94.102.50.45	Netherlands	147.237.76.34	yohalan.idf.il	Block_Ntp_All_Net	drop	1
109.106.142.55	Russian Federation	147.237.76.38	e.e.meitav.idf.i	Block_Udp_All_Nets	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
123.126.113.80	China	147.237.72.166	aka.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1
183.98.103.2	Korea, Republic of	147.237.77.74	law.idf.il	9221: HTTP: PUT Method Execution over HTTP/WebDAV	Block	1
188.165.15.223	France	147.237.76.30	himush.idf.il	C228: HTTP: AhrefBot crawler	Block	1

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
66.249.75.44	147.237.77.233	United States	atal.idf.il	ET SCAN NMAP -sA (2)	3
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	3
66.249.66.43	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
5.29.35.70	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.182.5.49	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
65.255.43.24	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sS window 2048	1
212.150.5.74	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.121.67.138	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
193.105.134.220	147.237.8.14	Sweden	e.orchot.idf.il	ET SCAN NMAP -sS window 1024	1
46.117.154.27	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
120.7.108.127	147.237.0.35	China	akaws.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
37.26.149.168	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
91.135.102.176	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
31.6.71.154	147.237.72.167	Poland	ishurim.aka.idf.il	ET SCAN NMAP -sS window 1024	1
79.183.230.55	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.178.200.92	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
66.249.66.78	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	1
65.255.43.24	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sS window 4096	1
65.255.43.24	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -f -sS	1
46.120.31.35	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
151.11.201.3	147.237.76.198	Italy	e.yohalan.idf.il	ET SCAN NMAP -sS window 4096	1
46.107.48.163	147.237.77.216	Hungary	dover.idf.il	portscan: TCP Distributed Portscan	1
93.173.234.248	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
31.154.92.199	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
80.246.138.133	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
193.37.128.205	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	248
46.19.85.13	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	149
66.249.73.185	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	130
79.176.63.242	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	69
193.37.128.205	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	50
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
109.226.22.161	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
100.100.76.150		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	28
100.100.63.16		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
132.3.57.82	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
85.64.157.231	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	24
66.249.82.88	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
80.246.130.148	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	21
5.144.62.222	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	20
132.3.57.80	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
85.250.239.166	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	16
100.100.97.64		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
85.250.239.166	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	16
66.249.78.37	United States	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
100.100.60.163		147.237.76.147	chinuch.aka.idf.il	drop	First packet isn't SYN	drop	12
204.12.251.37	United States	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	9
37.46.39.67	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
100.100.76.150		147.237.72.167	ishurim.aka.idf.il	drop	First packet isn't SYN	drop	9
84.229.53.137	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	9
212.179.246.90	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
79.181.149.40	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	9
46.19.85.136	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
212.235.98.139	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	9
46.19.85.136	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
109.226.17.214	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
2.54.129.62	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	8
132.3.57.78	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
46.19.85.109	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
216.185.39.146	United States	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	8
132.3.57.79	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
46.19.85.220	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
100.100.85.89		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	7
79.179.131.171	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
2.52.185.30	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
213.8.173.98	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.125	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
66.249.73.193	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.65.218.211	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.120.56.93	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
100.100.60.163		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
79.179.189.206	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.125	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
2.52.184.206	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
46.19.85.169	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.120.56.93	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.199	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	11
37.26.149.218	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
85.64.22.233	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ufr/reaction/	Block	5
91.207.88.231	Ukraine	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 91.207.88.231	Block	5
91.207.88.231	Ukraine	147.237.72.166	aka.idf.il	PHP Attempt	Block	5
93.173.39.183	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ufr/reaction/	Block	4
176.126.163.240	Ukraine	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	4
72.9.148.10	United States	147.237.77.216	doover.idf.il	Distributed Suspicious Response Code	Block	4
176.13.5.73	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
85.250.149.89	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ufr/reaction/	Block	4
46.19.85.33	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.85.218	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.126.163.240	Ukraine	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 176.126.163.240	Block	3
37.26.148.154	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
212.25.82.89	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/ufr/reaction/	Block	3
84.108.240.87	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
149.78.9.10	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
79.178.212.93	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 79.178.212.93	Block	3
46.19.86.154	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
66.249.66.40	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
46.19.86.173	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
5.29.124.105	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ufr/reaction/	Block	2
109.66.128.206	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 109.66.128.206	Block	2
185.32.179.98	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.19.86.34	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
212.76.99.34	Israel	147.237.72.166	aka.idf.il	Suspicious Response Code_Custom_Temporary	Block	2
176.228.162.179	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
85.250.239.166	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
2.52.185.36	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//resources/images/innerpage/goback.gif	Block	1
79.179.120.232	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
193.37.128.205	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/style/shared/reset.css	Block	1
96.255.136.28	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
89.77.37.207	Poland	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/xmlrpc.php	Block	1
77.127.25.49	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
176.106.227.81	Israel	147.237.72.166	aka.idf.il	Unknown Parameter docId in www.aka.idf.il/main/giyus/main/giyus/resources/images/master/favicon.gif	None	1
5.175.13.138	Germany	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Unknown SSL Session	None	1
84.228.10.86	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/https://www.aka.idf.il/	Block	1
212.179.10.43	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/gius	Block	1
66.249.69.41	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/	Block	1
149.88.186.94	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
62.90.143.192	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	1
109.65.20.226	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
2.54.132.42	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
79.183.227.125	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/files/5/110425.pdf	Block	1
204.13.200.200	United States	147.237.77.216	doover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/doover.aspx.	Block	1
180.76.15.16	China	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/templates/shared/usercontrols/headerupper/	Block	1
2.52.26.55	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
79.178.212.93	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/	Block	1
68.180.228.112	United States	147.237.77.216	doover.idf.il	Distributed Suspicious Response Code	Block	1
167.114.156.198	Canada	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1