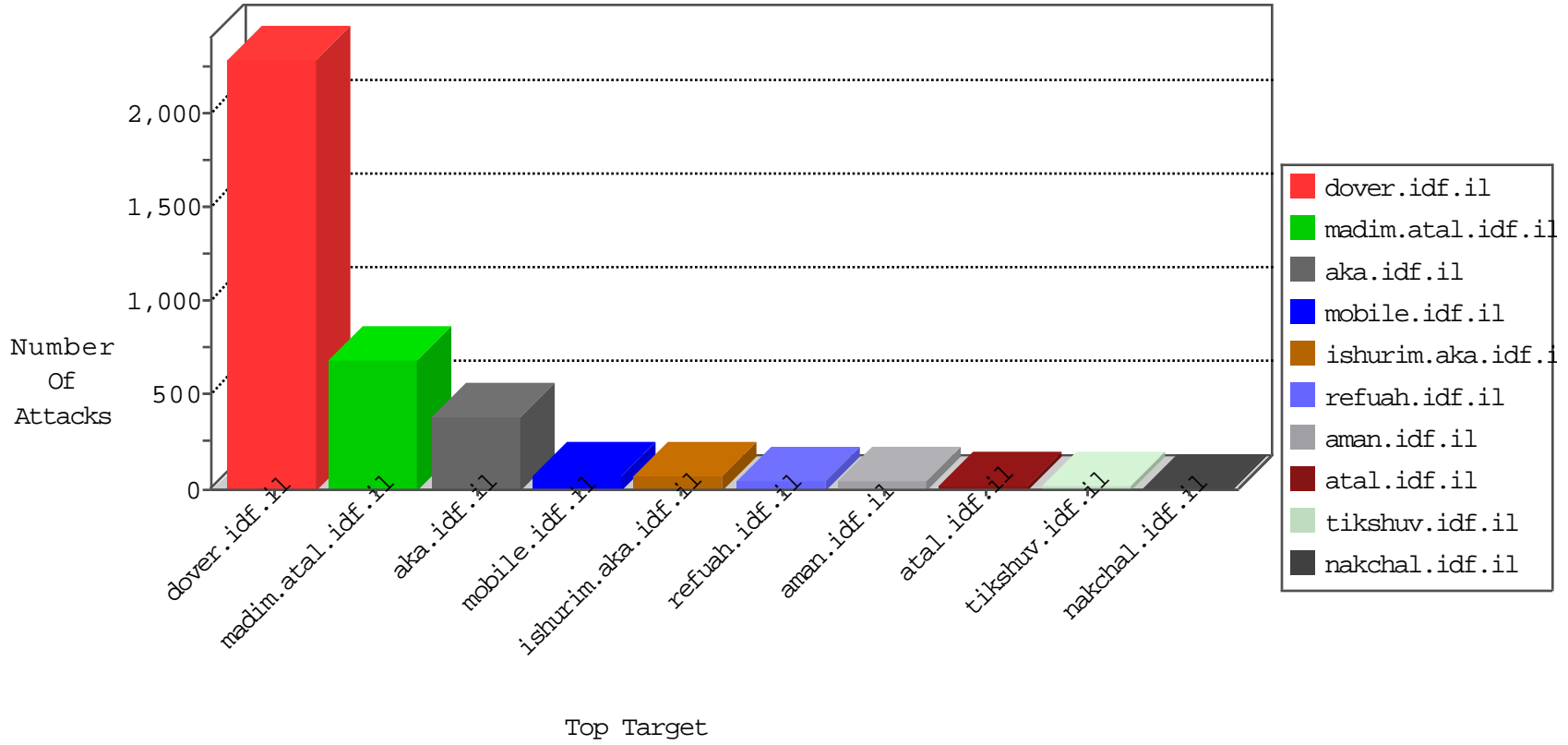


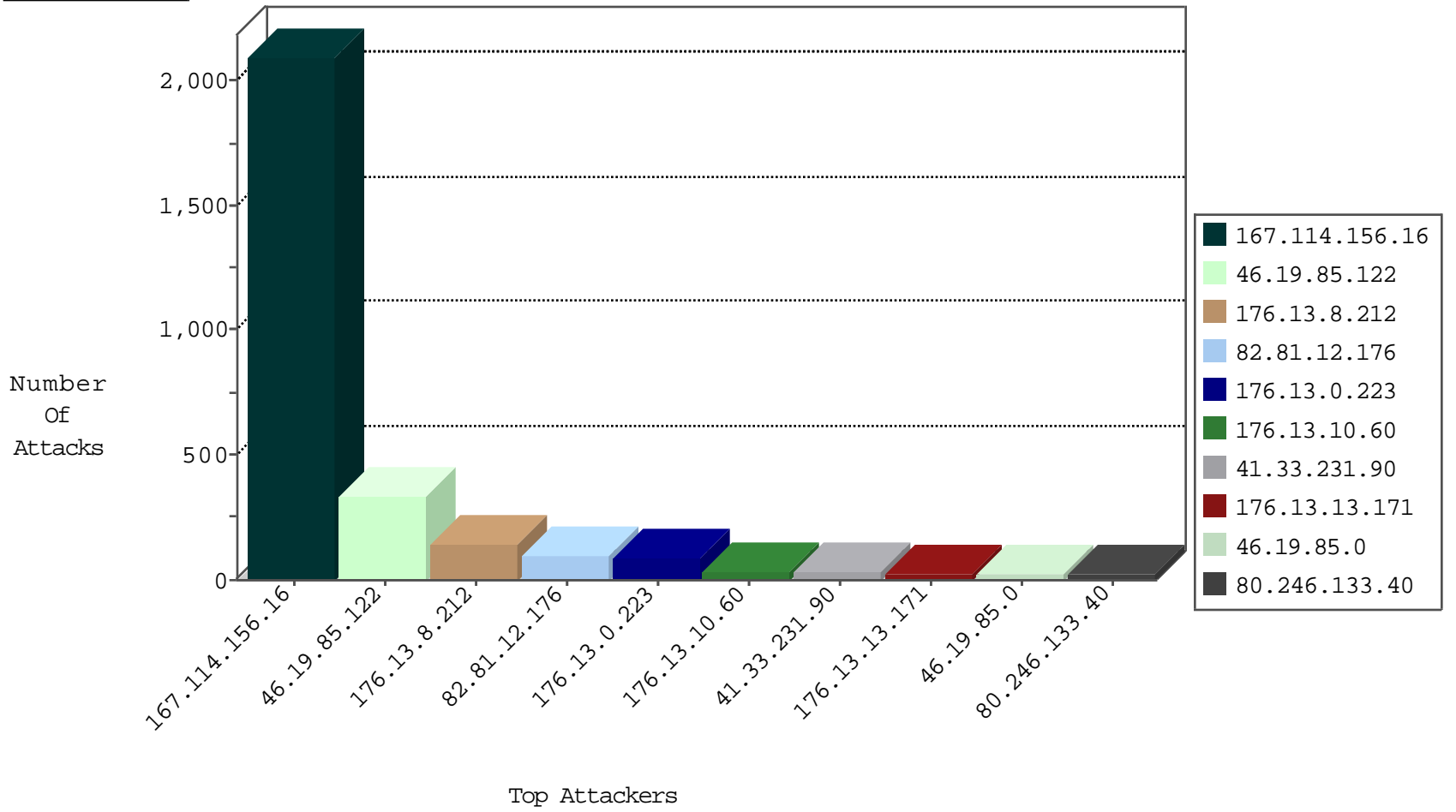
IDF Under Attack Daily Report



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	3061
82.81.12.176	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	92
130.75.174.172	Germany	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	6
212.179.54.237	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
71.6.165.200	United States	147.237.76.201	e.atal.idf.il	Block_Udp_All_Nets	drop	1
183.60.48.25	China	147.237.76.197	e.himush.idf.il	JLM_Under_Attack_Con_Tcp	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
182.96.195.239	China	147.237.77.216	dover.idf.il	9221: HTTP: PUT Method Execution over HTTP/WebDAV	Block	1
84.95.200.200	Israel	147.237.77.216	dover.idf.il	C008: HTTP: Xenu UserAgent	Block	1
172.245.218.130	United States	147.237.76.86	navy.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
66.249.78.89	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	2
194.114.146.227	147.237.77.216	Israel	dover.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
192.117.188.130	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
85.65.96.214	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.178.197.94	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.45.137.67	147.237.77.226	Turkey	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 1024	1
37.34.90.94	147.237.77.216	Palestinian Territory, Occupied	dover.idf.il	portscan: TCP Distributed Portscan	1
2.52.131.22	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
193.105.134.220	147.237.77.226	Sweden	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 1024	1
109.67.48.55	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
84.117.113.152	147.237.0.33	Romania	idf.il	ET SCAN NMAP -sS window 1024	1
46.19.86.85	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
5.29.156.15	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
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	27
80.246.133.40	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	21
46.19.85.159	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	19
46.19.85.0	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	18
85.130.246.101	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
217.132.112.87	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	11
37.26.148.165	Israel	147.237.72.166	aka.idf.il	drop	SAM rule	drop	10
94.230.86.251	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
212.179.218.166	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
185.32.179.163	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
193.43.245.250	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
109.65.59.94	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.0	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
141.8.132.112	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.8	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
176.13.17.84	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
31.168.240.83	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.66.36.86	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.183.163.57	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.123	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
109.64.144.73	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
77.126.11.238	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.253.216.75	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
68.180.229.239	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
176.13.13.213	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
109.253.132.39	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
185.127.10.35		147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
46.19.86.180	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
176.13.13.213	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
82.80.140.27	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
37.26.149.227	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
199.244.88.182	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	5
46.19.85.3	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
2.52.2.18	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
192.254.209.21	United States	147.237.77.176	matpash.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	5
212.179.218.166	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
46.19.86.84	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
46.19.85.3	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
212.179.218.166	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	4
176.13.18.134	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
94.230.86.251	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
176.13.3.246	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
46.19.85.241	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	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
31.168.153.134	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.178.52.65	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.212	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
62.90.234.117	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
192.114.23.209	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.122	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	187
46.19.85.122	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	132
176.13.8.212	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	94
176.13.0.223	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	91
176.13.8.212	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	37
176.13.10.60	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	28
176.13.13.171	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	24
46.19.85.157	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	21
46.19.85.87	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	18
46.19.85.122	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (403)	Block	15
176.13.8.212	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (403) in Session from 176.13.8.212	Block	10
209.88.173.130	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/\$\$\$&?&?\$\$\$	Block	9
192.116.149.197	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/	Block	7
46.19.86.8	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	5
37.26.149.157	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	5
109.253.208.162	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
192.116.149.197	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/8/	Block	3
194.114.146.227	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/sip_storage/files/9/2479.jpg	Block	3
185.32.179.145	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
5.28.185.187	Israel	147.237.76.42	refuah.idf.il	Parameter Type Violation ctl00\$ContentPlaceholder1\$txtLastName in www.refua.atal.idf.il/1518-he/refuah.aspx	Block	3
2.54.167.173	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.85.2	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
2.54.4.28	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
37.26.147.231	Israel	147.237.76.147	chinuch.aka.idf.il	Distributed Unauthorized URL Access on www.chinuch.aka.idf.il/404.htm	Block	3
109.65.221.121	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/nekudot/index	Block	3
176.13.17.164	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
37.142.222.233	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 37.142.222.233	Block	2
85.64.137.76	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
176.13.18.203	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1071	Block	2
217.132.112.87	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	2
176.13.19.23	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
109.253.132.39	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
176.13.13.213	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
176.13.17.84	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
176.13.8.156	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
66.249.78.109	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/robots.txt	Block	1
178.255.215.87	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-19689-he/kkkkkkk=17a07365kkkkkkk_17a07365	Block	1
37.26.149.171	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
5.12.226.242	Romania	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
95.86.124.55	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.19.86.239	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
176.13.10.60	Israel	147.237.0.19	madim.atal.idf.il	Parameter Type Violation ctl00\$ContentPlaceholder1\$txtEntrance in madim.atal.idf.il/mobile/1088-he/meretz.aspx	Block	1
84.108.217.91	Israel	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	1
204.111.62.193	United States	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	1
169.229.3.91	United States	147.237.77.233	atal.idf.il	Malformed URL [[#15]][[#23]]'â€°xâ€°[[#25]]ÂŽÃ·	Block	1
46.19.85.3	Israel	147.237.77.216	dover.idf.il	Illegal HTTP Version	Block	1
169.229.3.91	United States	147.237.72.156	aman.idf.il	Multiple Abnormally Long Request from 169.229.3.91	Block	1
79.177.197.71	Israel	147.237.72.166	aka.idf.il	Unknown Parameter x in www.aka.idf.il/main/sachar/payslips.aspx	None	1
37.26.148.144	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1