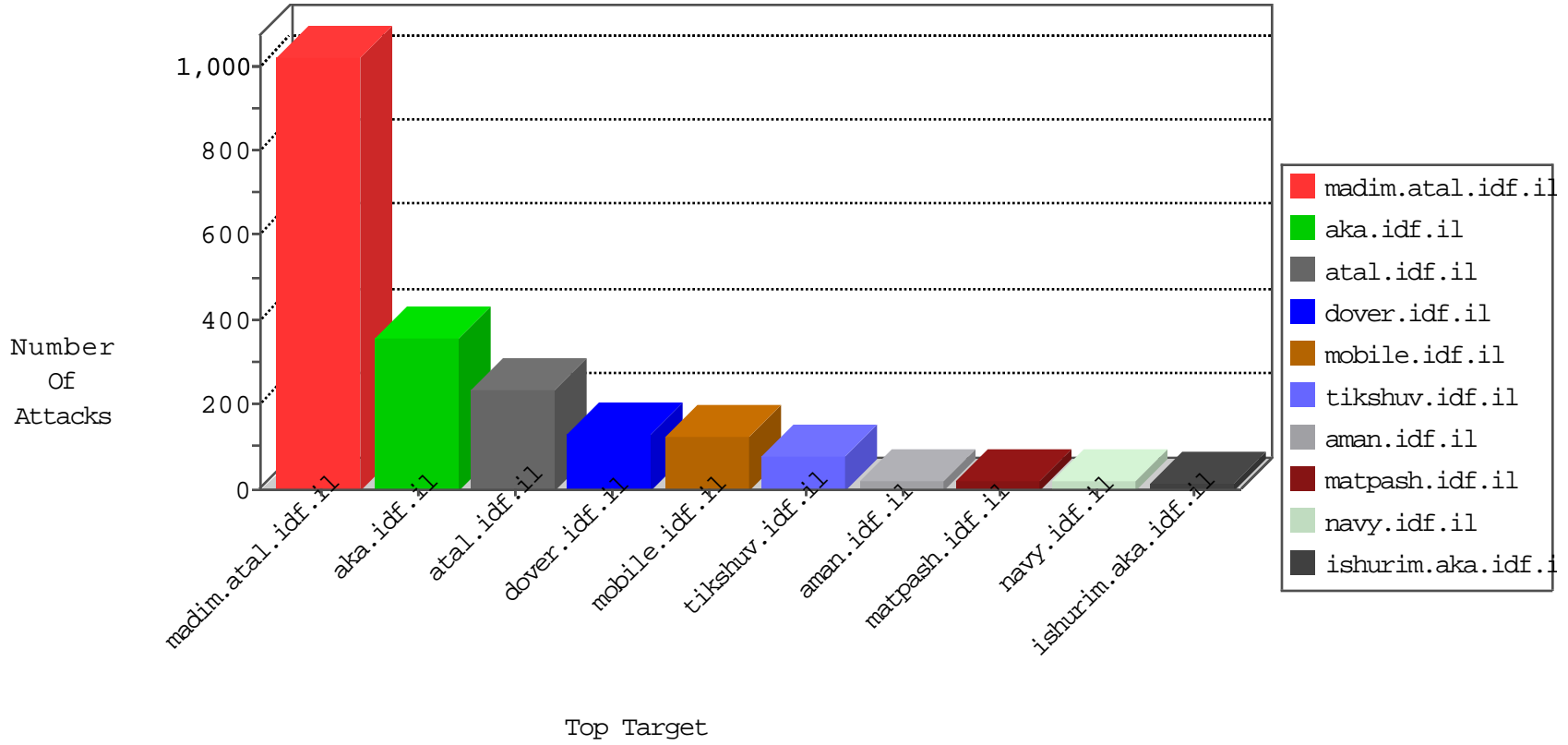


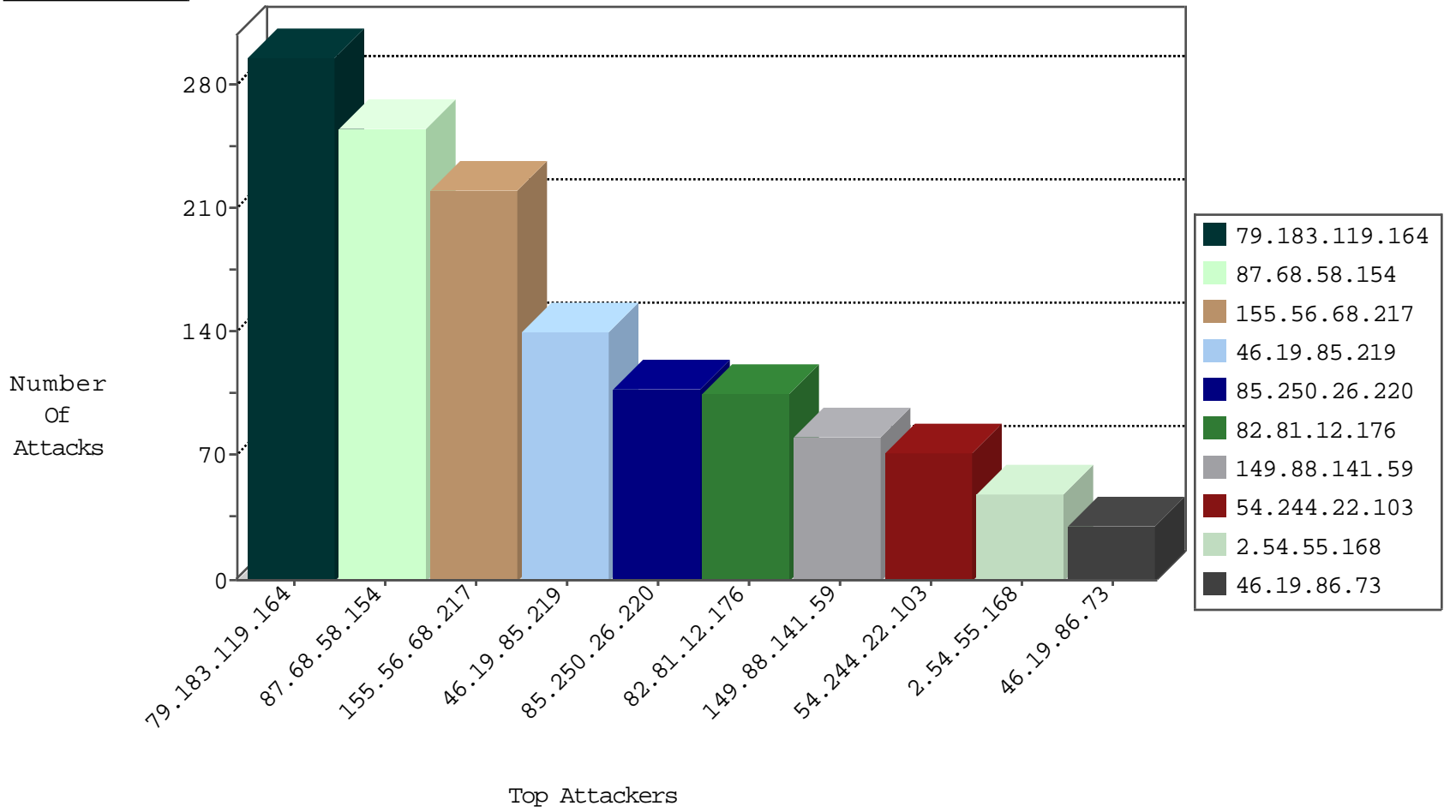
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
82.81.12.176	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	105
204.42.253.2	United States	147.237.76.199	e.nakchal.idf.il	Block_Ntp_All_Net	drop	2
0.0.0.0		147.237.77.216	dover.idf.il	HTTP_Page_Flood_Attack	forward	2
123.151.149.222	China	147.237.76.44	e.refuah.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
204.42.253.2	United States	147.237.76.200	eitan.aka.idf.il	Block_Ntp_All_Net	drop	2
204.42.253.2	United States	147.237.76.201	e.atal.idf.il	Block_Ntp_All_Net	drop	2
204.42.253.2	United States	147.237.76.198	e.yohalan.idf.il	Block_Ntp_All_Net	drop	2
204.42.253.2	United States	147.237.76.202	e.halag.idf.il	Block_Ntp_All_Net	drop	2
115.239.228.10	China	147.237.0.15	kosher-kravi.idf.il	Frk_Under_Attack_Con_Http	drop	2
185.130.5.201		147.237.76.202	e.halag.idf.il	Block_Udp_All_Nets	drop	1
115.239.228.10	China	147.237.0.15	kosher-kravi.idf.il	Frk_Purple_Con_Limit_Http	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
106.38.241.106	China	147.237.77.176	matpash.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
41.33.231.90	147.237.77.216	Egypt	dover.idf.il	Tehila - Perl LWP with fake user agent	9
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	3
199.191.56.188	147.237.77.205	United States	prisha.idf.il	ET SCAN NMAP -sS window 3072	1
199.191.56.188	147.237.77.205	United States	prisha.idf.il	ET SCAN NMAP -f -sS	1
168.62.238.153	147.237.0.15	United States	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
113.59.33.61	147.237.76.39	China	mobile.meitav.idf.i	ET SCAN NMAP -sS window 1024	1
101.75.211.247	147.237.0.34	China	tikshuv.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
218.246.0.97	147.237.8.24	China	e.lifestyle.idf.il	ET SCAN NMAP -sS window 1024	1
199.191.56.188	147.237.77.205	United States	prisha.idf.il	ET SCAN NMAP -sS window 2048	1
113.59.33.61	147.237.76.39	China	mobile.meitav.idf.i	ET SCAN NMAP -sS window 2048	1
113.59.33.61	147.237.76.39	China	mobile.meitav.idf.i	ET SCAN NMAP -f -sS	1
218.246.0.97	147.237.77.234	China	halag.idf.il	ET SCAN NMAP -sS window 1024	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
155.56.68.217	Germany	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	220
54.244.22.103	United States	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	72
2.54.32.248	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	25
46.19.86.73	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
213.151.32.163	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
2.54.128.178	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
107.167.108.218	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	18
37.26.146.240	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
141.8.132.112	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
2.52.12.201	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
80.179.31.209	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	9
82.102.169.113	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
46.19.86.78	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.86.211	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.64.212.66	Israel	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	6
5.28.177.93	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
62.0.197.205	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
37.26.147.180	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
37.26.147.180	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	5
82.102.169.113	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
2.54.141.237	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
37.26.147.180	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	5
37.26.147.180	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	5
79.183.55.105	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
37.247.36.102	Netherlands	147.237.76.44	e.refuah.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	4
5.22.135.215	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
141.8.183.16	Russian Federation	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	4
109.186.14.128	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence		monitor	4
82.166.247.138	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
85.250.26.220	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	3
109.253.135.47	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
185.3.147.164	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
62.90.235.170	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.178.161.185	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
188.120.148.163	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
37.26.146.217	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
85.64.147.130	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
5.29.242.115	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
109.65.134.103	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.179.124.160	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.253.223.34	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.7	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
2.54.32.189	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.66.224.117	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
176.12.160.2	Israel	147.237.77.243	mobile.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
87.68.58.154	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	213
79.183.119.164	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	146
79.183.119.164	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	110
85.250.26.220	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	81
149.88.141.59	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	80
46.19.85.219	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	74
46.19.85.219	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	66
87.68.58.154	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	42
79.183.119.164	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (403) in Session from 79.183.119.164	Block	39
2.54.55.168	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	37
37.26.146.139	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	30
85.250.26.220	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	24
109.253.207.112	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	22
46.19.85.36	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	22
2.54.55.168	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	11
46.19.86.73	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	7
46.19.86.15	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
109.253.133.151	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/nekudot/index	Block	5
2.54.128.178	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	4
212.116.166.10	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/www.navy.idf.il	Block	3
5.102.254.131	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
46.19.85.61	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
46.19.86.89	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
46.19.86.151	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
185.32.179.206	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
72.9.148.10	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/994-8613-he/navy.aspx.aspx	Block	2
157.55.39.66	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	2
37.26.146.240	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
37.26.148.219	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
192.0.113.50	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
85.65.25.95	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
79.181.155.65	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
157.55.39.89	United States	147.237.76.200	eitan.aka.idf.il	Multiple Unauthorized URL Access from 157.55.39.89	Block	1
109.253.195.48	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
61.135.190.69	China	147.237.0.19	madim.atal.idf.i	Unauthorized URL Access to 147.237.0.19/	Block	1
212.76.112.188	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/&sa=u&ved=0ahukewjt5-ou6m7kahwffw8khzy9bmqfeggimaa&usg=afqjcnhcyyg7wlcq-yhd5_ammzoyodtwa	Block	1
31.154.94.28	Israel	147.237.76.86	navy.idf.il	Cookie Tampering on cookie __utma: Expected 104000134.1113191019.1450017655.1450017655.1450025453.2, Observed 104000134.1113191019.1450017655.1450025453.1454062941.3	None	1
176.13.7.134	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
79.183.161.167	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
2.54.26.13	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
61.135.190.200	China	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to 147.237.0.34/style/shared/reset.css	Block	1
109.65.36.190	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
85.65.74.148	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
37.142.64.52	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
194.90.15.61	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
5.22.135.243	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/favicon.ico	Block	1
157.55.39.114	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
109.253.200.124	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
61.135.190.69	China	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to 147.237.0.34/style/shared/layout.css	Block	1
87.69.100.185	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$cphSachar\$btnSubm in www.aka.idf.il/main/sachar/	None	1