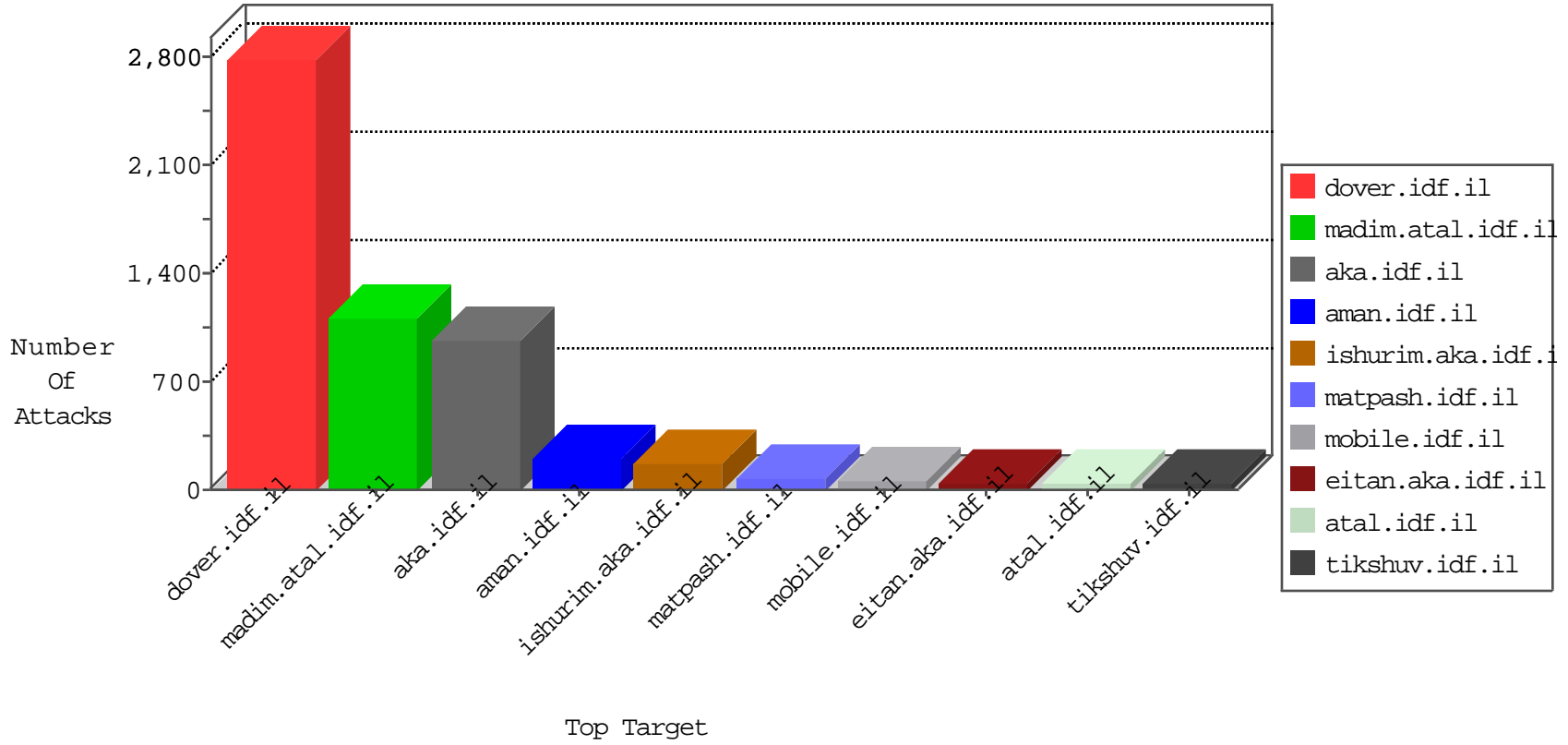


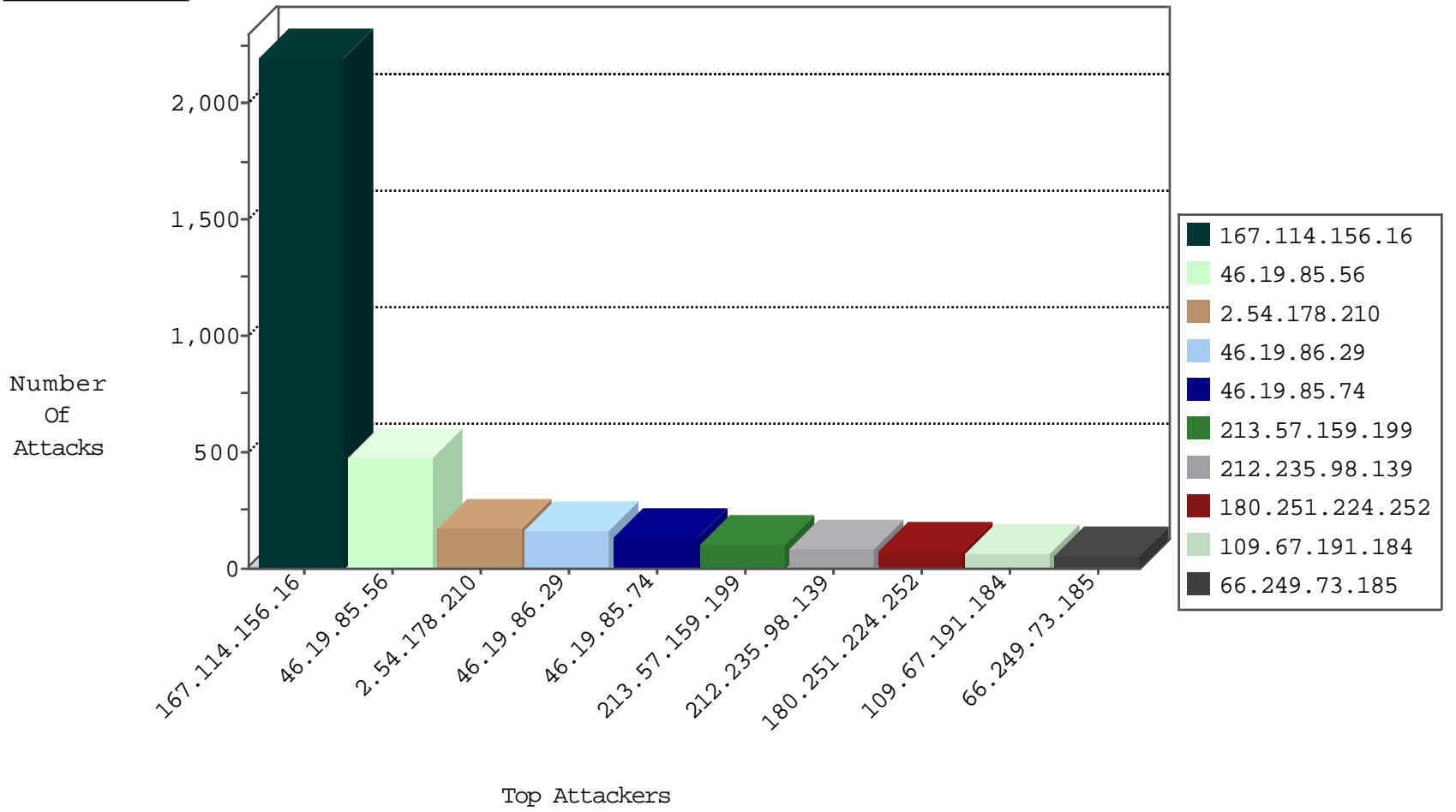
IDF Under Attack Daily Report



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	3327
198.240.128.75	United Kingdom	147.237.77.216	dover.idf.il	Anomaly-TLS-renegotiation-Cli	forward	148
92.232.155.105	United Kingdom	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
93.174.93.151	Netherlands	147.237.76.199	e.nakchal.idf.il	Block_Udp_All_Nets	drop	1
23.95.248.132	United States	147.237.76.201	e.atal.idf.il	Block_Ntp_All_Net	drop	1
149.78.56.233	Israel	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
194.114.146.227	Israel	147.237.77.74	law.idf.il	C1000004: HTTP: options method (Microsoft)	Block	6
188.106.241.59	Germany	147.237.72.166	aka.idf.il	C1000004: HTTP: options method (Microsoft)	Block	1
188.165.15.99	France	147.237.0.34	tikshuv.idf.il	C228: HTTP: AhrefBot crawler	Block	1
91.121.112.142	France	147.237.77.216	dover.idf.il	C1000106: HTTP: majestic bot	Block	1
123.126.113.80	China	147.237.72.166	aka.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
149.78.56.233	147.237.77.216	Israel	dover.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	3
66.249.66.1	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
62.38.250.31	147.237.77.121	Greece	e.navy.idf.il	ET SCAN NMAP -sS window 2048	1
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	1
58.60.184.225	147.237.76.200	China	eitan.aka.idf.il	ET SCAN Potential SSH Scan	1
46.19.85.191	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
125.91.120.136	147.237.0.34	China	tikshuv.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
37.46.39.84	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
118.69.135.26	147.237.76.197	Vietnam	e.himush.idf.il	ET SCAN Potential SSH Scan	1
31.63.243.41	147.237.77.216	Poland	dover.idf.il	ET SCAN Potential SSH Scan	1
118.69.135.26	147.237.76.42	Vietnam	refuah.idf.il	ET SCAN Potential SSH Scan	1
31.6.71.154	147.237.76.176	Poland	test.ncoore.idf.il	ET SCAN NMAP -sS window 1024	1
79.177.52.211	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
62.117.220.63	147.237.76.196	Spain	e.sviva.idf.il	ET SCAN NMAP -sS window 1024	1
199.101.186.178	147.237.76.200	United States	eitan.aka.idf.il	ET SCAN NMAP -sS window 4096	1
62.38.250.31	147.237.77.121	Greece	e.navy.idf.il	ET SCAN NMAP -f -sS	1
176.12.146.85	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.19.86.27	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
128.139.21.154	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
39.74.114.65	147.237.0.15	China	kosher-kravi.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
118.69.135.26	147.237.76.202	Vietnam	e.halag.idf.il	ET SCAN Potential SSH Scan	1
31.63.243.41	147.237.77.234	Poland	halag.idf.il	ET SCAN Potential SSH Scan	1
118.69.135.26	147.237.76.147	Vietnam	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
31.63.243.41	147.237.77.205	Poland	prisha.idf.il	ET SCAN Potential SSH Scan	1
118.69.135.26	147.237.76.38	Vietnam	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
66.249.66.61	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	1
62.219.124.47	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
46.19.85.74	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	128
212.235.98.139	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	85
66.249.73.185	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	50
213.57.53.217	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	49
180.251.224.252	Indonesia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	39
213.57.58.91	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	38
213.57.159.199	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	36
213.57.159.199	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	36
213.57.159.199	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	36
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
180.251.224.252	Indonesia	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	31
80.179.9.7	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
66.249.66.61	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	28
212.179.28.34	Israel	147.237.0.16	my-kosher-kravi.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	28
213.57.206.242	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	27
46.117.134.30	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
213.57.155.171	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	24
81.144.132.166	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
213.57.177.48	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	22
213.57.177.48	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	22
79.177.52.211	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	19
213.57.224.248	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	18
66.249.81.218	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
80.179.9.115	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
46.19.85.191	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	18
213.57.224.248	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	18
100.100.6.215		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	17
100.100.82.225		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
109.67.135.63	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	16
77.125.125.254	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
79.180.165.155	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
176.12.149.144	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	14
134.191.232.71	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	14
213.57.213.218	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	14
100.100.23.213		147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	12
100.100.28.123		147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	12
213.57.213.218	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	12
46.19.86.220	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
100.100.36.211		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	12
2.52.128.114	Israel	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	12
176.12.149.144	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	12
83.130.116.251	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	11
83.130.116.251	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
213.57.42.77	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	11
46.19.86.30	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
100.100.11.14		147.237.72.167	ishurim.aka.idf.il	drop	First packet isn't SYN	drop	10
95.35.207.14	Israel	147.237.77.212	e.dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	9
149.78.39.73	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
31.210.179.16	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
85.130.230.252	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.56	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	272
46.19.85.56	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	110
46.19.85.56	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (403) in Session from 46.19.85.56	Block	100
46.19.86.29	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	97
2.54.178.210	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	92
2.54.178.210	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	84
109.67.191.184	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	65
46.19.86.29	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	65
176.12.143.89	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	54
2.54.9.83	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	36
85.250.237.81	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	32
185.32.179.103	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	26
80.246.136.11	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	23
2.54.8.150	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	21
79.181.120.41	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	19
77.127.255.29	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ufi/reaction/	Block	15
176.13.1.38	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
85.250.45.37	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ufi/reaction/	Block	6
46.19.85.228	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
66.249.66.61	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.249.66.61	Block	5
66.169.22.22	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 66.169.22.22	Block	5
176.13.10.209	Israel	147.237.77.243	mobile.idf.il	Distributed Parameter Type Violation on mobile.idf.il/sachar/changepassword parameter NewPassword	Block	5
77.125.95.229	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ufi/reaction/	Block	4
176.13.10.209	Israel	147.237.77.243	mobile.idf.il	Distributed Parameter Type Violation on mobile.idf.il/sachar/login parameter Password	Block	4
213.151.35.218	Israel	147.237.77.243	mobile.idf.il	Distributed Parameter Type Violation on mobile.idf.il/sachar/login parameter Password	Block	4
176.12.140.2	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation Password in mobile.idf.il/sachar/login	Block	4
176.12.150.41	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
66.249.66.61	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	3
176.13.1.110	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.186.185.197	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ufi/reaction/	Block	3
84.228.19.253	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/ufi/reaction/	Block	3
37.26.149.139	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.85.121	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
37.142.162.164	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
105.158.120.60	Morocco	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/arr/	Block	2
77.125.104.49	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
212.25.102.57	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
66.249.64.177	Israel	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	2
85.65.46.57	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ufi/reaction/	Block	2
79.176.110.252	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ufi/reaction/	Block	2
149.78.167.26	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/https://www.aka.idf.il/	Block	2
79.179.181.153	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 79.179.181.153	Block	2
185.32.179.74	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
208.184.112.74	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	2
84.228.227.73	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
5.29.118.210	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/ufi/reaction/	Block	2
176.13.6.175	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
37.142.64.107	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
107.178.194.87	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
80.246.136.95	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1