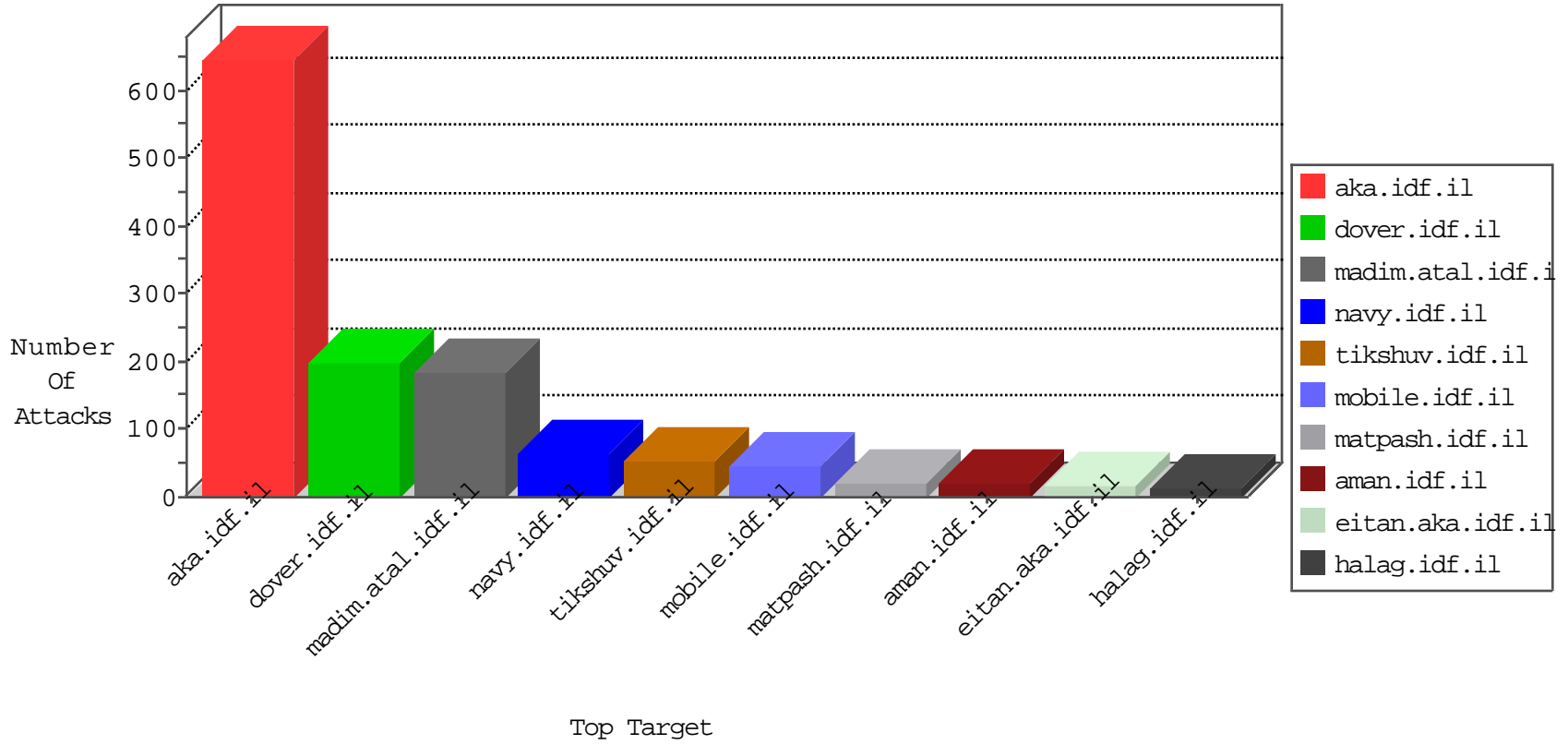


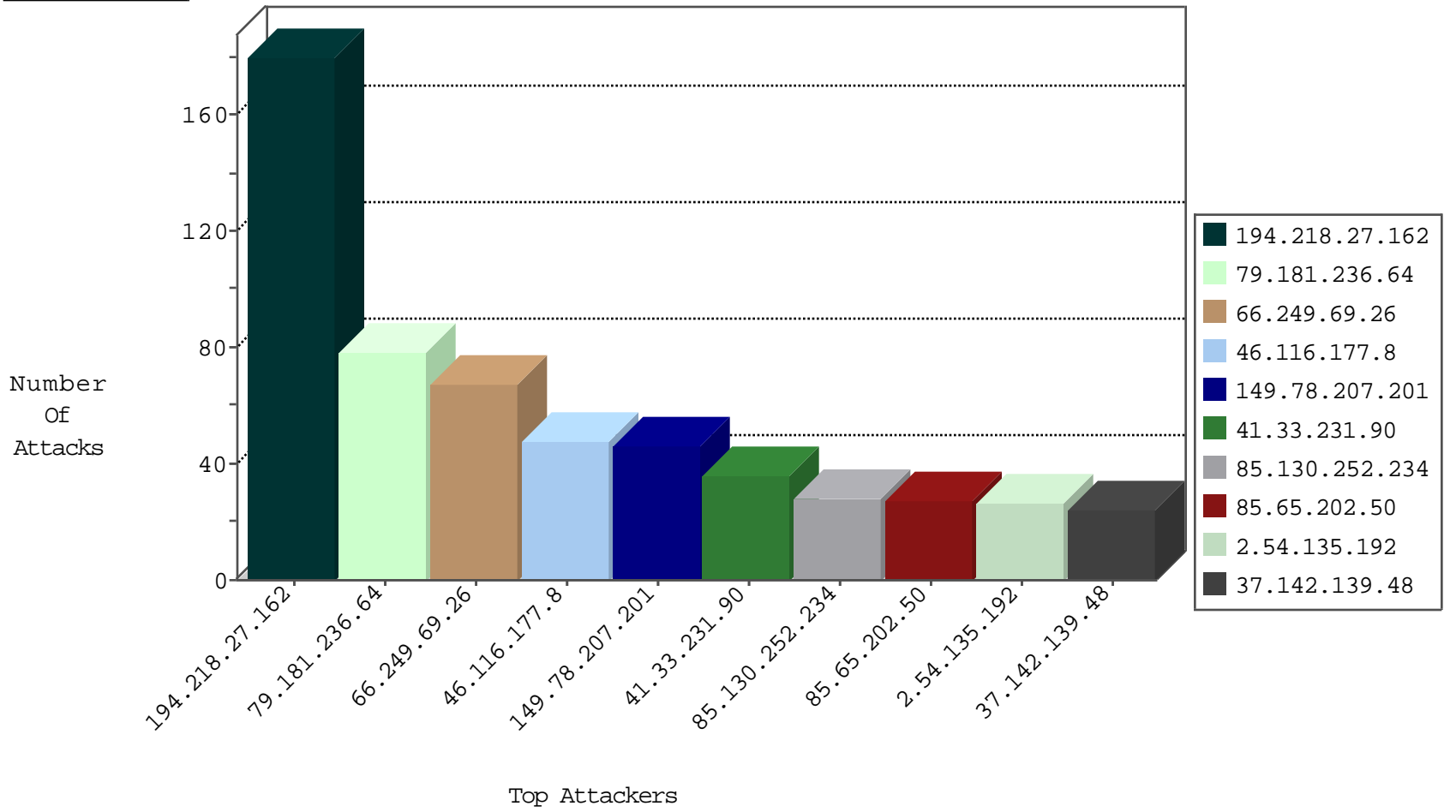
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
82.145.208.241	Europe	147.237.77.176	matpash.idf.il	Block_Tp_Web_In	drop	12
212.179.54.237	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
185.35.62.110	Switzerland	147.237.76.38	e.e.meitav.idf.il	Block_Ntp_All_Net	drop	1
91.121.151.223	France	147.237.77.227	e.hamaz.idf.il	Block_Udp_All_Nets	drop	1
185.35.62.220	Switzerland	147.237.76.148	ggcenter.aka.idf.il	Block_Ntp_All_Net	drop	1
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1
185.35.62.23	Switzerland	147.237.77.179	e.mazi.idf.il	Block_Ntp_All_Net	drop	1
185.35.62.251	Switzerland	147.237.0.33	idf.il	Block_Ntp_All_Net	drop	1
66.240.236.119	United States	147.237.77.235	sviva.idf.il	Block_Udp_All_Nets	drop	1
185.35.62.28	Switzerland	147.237.76.198	e.yohalan.idf.il	Block_Ntp_All_Net	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.117.144.55	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	16
79.179.12.74	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	11
87.70.31.140	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
46.120.91.150	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
106.120.173.124	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	4
199.30.24.43	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
66.249.64.180	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	3
217.132.16.228	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
51.254.130.60	United Kingdom	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Block	2
51.254.130.60	United Kingdom	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
66.249.64.185	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
207.46.13.147	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
54.82.8.196	147.237.77.176	United States	matpash.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	3
202.79.243.160	147.237.77.216	Japan	dover.idf.il	Tehila - Perl LWP with fake user agent	2
78.229.100.85	147.237.77.216	France	dover.idf.il	ET SCAN NMAP -sA (2)	2
66.102.9.28	147.237.72.167	United States	ishurim.aka.idf.il	ET SCAN NMAP -sA (2)	2
50.60.153.98	147.237.76.147	United States	chimuch.aka.idf.il	ET SCAN Potential SSH Scan	1
2.54.156.67	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
183.82.106.200	147.237.76.86	India	navy.idf.il	ET SCAN NMAP -sS window 2048	1
176.13.3.179	147.237.72.166	Israel	aka.idf.il	ET SCAN NMAP -f -sS	1
95.220.130.49	147.237.76.31	Russian Federation	nakchal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
45.32.88.244	147.237.77.243		mobile.idf.il	ET SCAN NMAP -sS window 3072	1
198.20.69.74	147.237.76.202	United States	e.halag.idf.il	ET DROP Dshield Block Listed Source	1
189.78.139.185	147.237.76.30	Brazil	himush.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
183.82.106.200	147.237.76.86	India	navy.idf.il	ET SCAN NMAP -f -sS	1
149.88.214.253	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
87.69.229.27	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
194.218.27.162	Sweden	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	120
194.218.27.162	Sweden	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	60
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
85.130.252.234	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
109.253.128.231	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
185.3.146.66	Israel	147.237.76.200	eitan.aka.idf.	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
46.19.85.14	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
46.19.86.111	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
77.127.209.155	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
79.183.195.152	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
79.182.135.70	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
82.81.4.54	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	11
85.130.190.75	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
46.19.85.171	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
2.52.158.51	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
5.28.188.62	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.177.54.174	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
81.218.125.133	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.152	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.86.141	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.152	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.152	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
79.176.170.173	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
185.120.126.89		147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.65.75.113	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.171	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.152	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
85.130.190.75	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
31.210.187.136	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
5.102.254.50	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
66.249.64.163	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
207.46.13.70	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
46.121.211.156	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
80.178.13.182	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	4
192.115.83.5	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
5.22.130.69	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
37.142.139.48	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
84.109.7.80	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
79.183.171.236	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.180.1.113	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.66.28.45	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
31.168.201.140	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.181.117.72	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
87.68.65.167	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.65.126.186	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.180.105.81	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.177.205.95	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

02-28-2016-21:04:05 to 02-28-2016-22:04:05

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
84.109.165.19	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.67.163.227	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
196.23.22.4	South Africa	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.181.236.64	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	78
66.249.69.26	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.69.26	Block	64
46.116.177.8	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	48
2.54.135.192	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	25
85.65.202.50	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 85.65.202.50	Block	22
46.19.85.37	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	9
46.19.85.150	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
46.19.85.215	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
95.172.233.91	United Kingdom	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	6
85.65.202.50	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/5/	Block	5
149.78.207.201	Israel	147.237.72.166	aka.idf.il	Distributed Abnormally Long Request	Block	4
66.249.66.15	United States	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 66.249.66.15	Block	4
149.78.207.201	Israel	147.237.72.166	aka.idf.il	Distributed Illegal HTTP Version	Block	4
149.78.207.201	Israel	147.237.72.166	aka.idf.il	Distributed Unknown HTTP Request Method	Block	4
149.78.207.201	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in Header Name	Block	4
149.78.207.201	Israel	147.237.72.166	aka.idf.il	Distributed Malformed URL	Block	4
149.78.207.201	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in Method	Block	4
149.78.207.201	Israel	147.237.72.166	aka.idf.il	Distributed Abnormally Long Header Line	Block	3
149.78.207.201	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	3
208.115.111.72	United States	147.237.76.86	navy.idf.il	Distributed Unauthorized URL Access on navy.idf.il/giyus/forum/asp/showforum.asp	Block	3
94.230.86.212	Israel	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to madim.atal.idf.il/shared/ajax/updatesmakatgauntity.aspx	Block	3
66.249.69.26	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
149.78.207.201	Israel	147.237.72.166	aka.idf.il	Distributed Malformed HTTP Header Line	Block	3
149.78.207.201	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in Header Value	Block	3
109.67.163.227	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
66.249.66.69	United States	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 66.249.66.69	Block	2
149.78.207.201	Israel	147.237.72.166	aka.idf.il	Distributed NULL Character in Header Name	Block	2
204.152.209.103	United States	147.237.76.42	refuah.idf.il	Multiple Unauthorized URL Access from 204.152.209.103	Block	2
37.142.139.48	Israel	147.237.72.166	aka.idf.il	Distributed Unknown HTTP Request Method	Block	2
2.52.153.163	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
164.138.119.31	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 164.138.119.31	Block	2
37.142.139.48	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in Method	Block	2
66.249.78.87	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Untraceable SSL Sessions: Unknown Server Certificate	None	2
37.142.139.48	Israel	147.237.72.166	aka.idf.il	Distributed Malformed URL	Block	2
37.142.139.48	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	2
66.249.78.94	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Untraceable SSL Sessions: Unknown Server Certificate	None	2
66.249.66.21	United States	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 66.249.66.21	Block	2
2.54.146.118	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
37.142.139.48	Israel	147.237.72.166	aka.idf.il	Distributed Abnormally Long Request	Block	2
66.102.7.131	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
87.70.21.4	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/main/giyus/controls/atuda/	Block	2
46.19.85.78	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$TochenPlaceholder\$ct113\$ct101\$ct103\$cb1Question\$35 in www.aka.idf.il/main/giyus/questionnaire.aspx	None	1
79.179.17.89	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
37.142.139.48	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
82.166.22.37	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/	Block	1
67.19.79.218	United States	147.237.76.30	himush.idf.il	Distributed Unauthorized URL Access on /robots.txt	Block	1
157.55.39.67	United States	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/modiin/sip_storage/files/5/68625	Block	1
5.29.183.179	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/markiveysachar.aspx	None	1
80.178.13.182	Israel	147.237.72.166	aka.idf.il	Multiple NULL Character in Method from 80.178.13.182	Block	1
66.102.7.254	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1