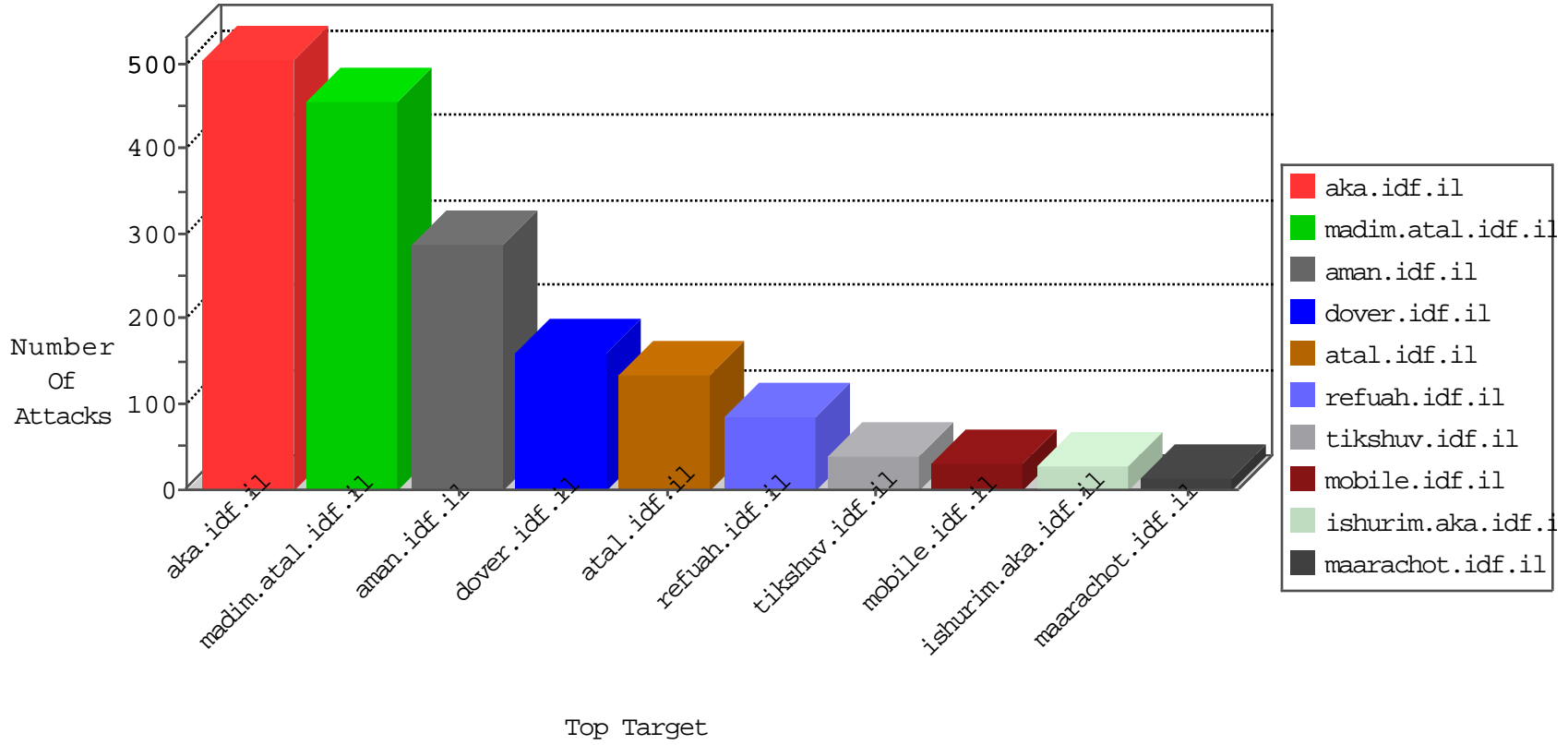


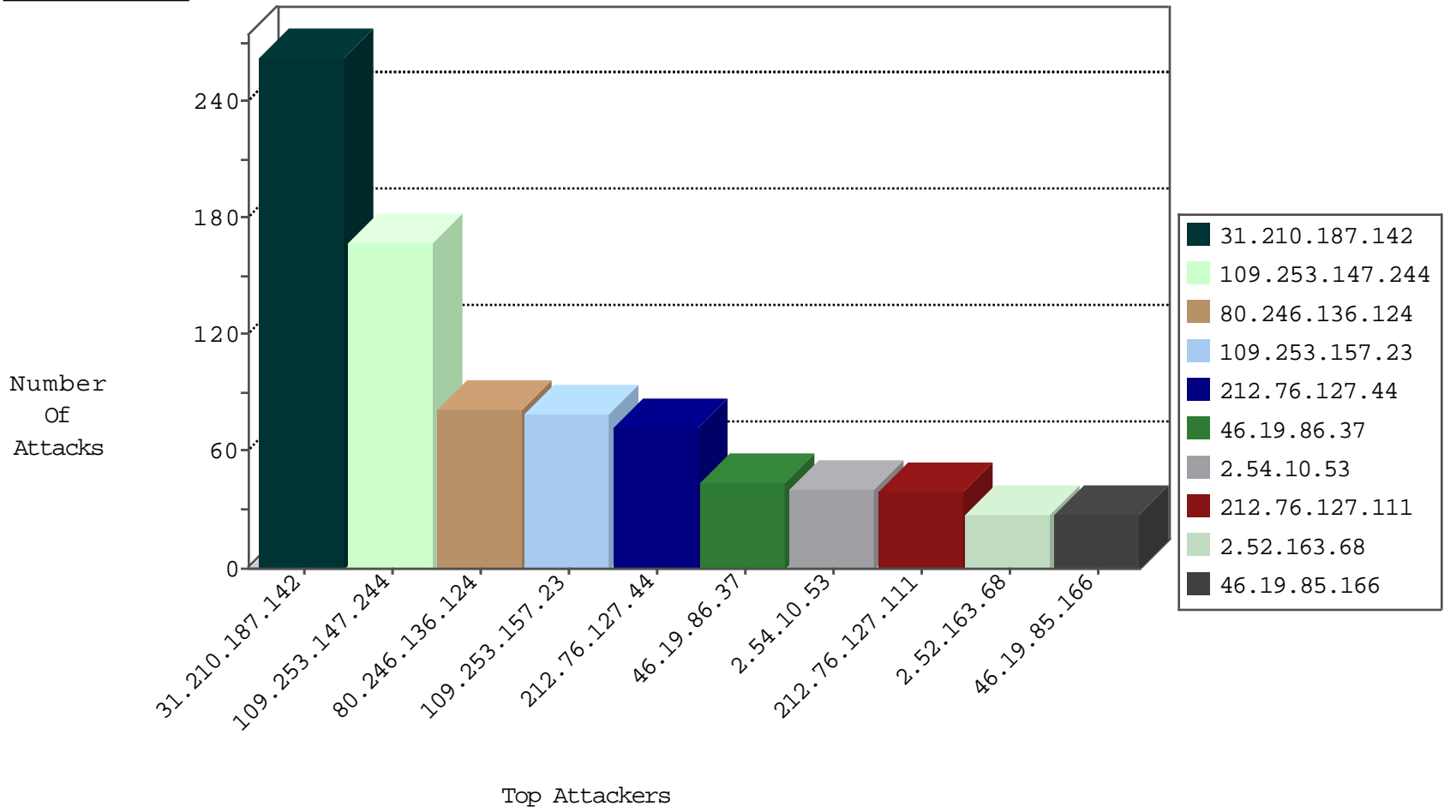
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
80.246.136.124	Israel	147.237.0.19	madim.atal.idf.il	Anomaly-TLS-renegotiation-Cl	dest-reset	399
147.236.238.250	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
198.20.70.114	United States	147.237.76.30	himush.idf.il	Block_Udp_All_Nets_Con_Limit	drop	3
115.239.228.10	China	147.237.76.202	e.halag.idf.il	JLM_Under_Attack_Con_Http	drop	2
146.185.239.100	Russian Federation	147.237.76.30	himush.idf.il	block-sp-trafl	drop	1

02-10-2016-10:04:04 to 02-10-2016-11:04:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.176.172.168	United States	147.237.77.216	dover.idf.il	C008: HTTP: Xenu UserAgent	Block	1
194.114.146.227	Israel	147.237.72.166	aka.idf.il	C169: Block - dns poisoning (Clalit)	Permit	1

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
97.88.205.32	147.237.77.233	United States	atal.idf.il	SQL Injection - Select From	2
212.235.103.211	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
114.112.90.54	147.237.0.19	China	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
93.173.146.2	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
85.65.244.76	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.117.110.165	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
2.52.6.144	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
194.114.146.227	147.237.72.166	Israel	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
87.68.248.12	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
82.205.122.157	147.237.77.216	Palestinian Territory, Occupied	dover.idf.il	portscan: TCP Distributed Portscan	1
2.52.175.118	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
212.76.127.44	Israel	147.237.77.233	atal.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	72
31.210.187.142	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	66
31.210.187.142	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	48
212.76.127.111	Israel	147.237.77.233	atal.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	39
31.210.187.142	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	37
31.210.187.142	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	35
31.210.187.142	Israel	147.237.72.156	aman.idf.il	SYN Attack		reject	26
212.179.102.167	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	24
2.52.163.68	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	21
176.13.6.1	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	20
46.19.86.216	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	19
31.210.187.142	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	alert	19
31.210.187.142	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	alert	13
46.19.86.226	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	13
46.19.85.152	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
2.54.10.53	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	11
46.19.86.192	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
5.29.40.43	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	9
46.19.85.166	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
31.210.187.142	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
109.253.157.44	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
109.253.132.182	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.85.166	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	9
109.65.153.32	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.86.192	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
46.19.86.181	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
2.54.10.53	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
2.54.10.53	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
192.0.80.128	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	7
2.54.159.200	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
2.54.10.53	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	7
2.52.6.144	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
2.54.10.53	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
46.19.85.66	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	6
149.78.161.211	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
77.125.141.253	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.54.159	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.253.218.173	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.143.111	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.11.204	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.64.193.167	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
46.19.85.11	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
79.181.217.210	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
5.102.254.217	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
77.126.88.140	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
81.218.66.107	Israel	147.237.77.170	maarachot.idf.il	drop	First packet isn't SYN	drop	6
2.54.31.18	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
62.219.35.93	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
31.210.187.142	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	5

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.253.147.244	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	134
109.253.157.23	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	79
80.246.136.124	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	49
46.19.86.37	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	44
109.253.147.244	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	30
85.64.14.41	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	25
2.54.189.75	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 2.54.189.75	Block	19
185.32.179.112	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	18
80.246.136.57	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	12
2.54.20.119	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	10
87.68.245.161	Israel	147.237.0.34	tikshuv.idf.il	Too Many of the Same Response Code (404) in Session from 87.68.245.161	Block	9
37.26.148.154	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	8
80.246.130.23	Israel	147.237.76.42	refuah.idf.il	Suspicious Response Code	Block	3
176.13.21.42	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.54.166.229	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.253.147.244	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (403)	Block	3
37.26.147.173	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.86.56	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
37.26.147.187	Israel	147.237.77.216	dover.idf.il	Parameter Type Violation SearchText in www.idf.il/1065-he/dover.aspx	Block	2
2.52.153.162	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
46.19.85.87	Israel	147.237.76.31	nakchal.idf.il	Abnormally Long Request method	Block	1
185.32.179.228	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1362	Block	1
157.55.39.201	United States	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/sachar/	Block	1
79.177.151.89	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/sachar/default.aspx	Block	1
149.78.59.15	Israel	147.237.77.216	dover.idf.il	Illegal URL Path Encoding 0x'0%2xYxε)E+AYaAY[[#21]]4xx*%px' A2dA%[[#0]][[#16]][[#21]][[#14]]4x?x*aA~æ t:Â æe"Â>AY [[#15]]A?A~[[#11]]ox~[[#30]]xøw7A-ÂFrâ,,ç@0A¶9g[[#14]]\k\$Â;x™ [[#3]]xøA?A¶x±v0%tx ljA %x?Aµ[[#16]]yfaYÂ³~[[#18]]Ö.xfjxøu<xžAž x,afA«vA'z0%A%[[#18]][[#1]]r1A"lA æ™[[#11]]	Block	1
149.78.59.15	Israel	147.237.77.216	dover.idf.il	Abnormally Long Header Line request header name	Block	1
207.46.13.142	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/	Block	1
109.67.22.226	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
176.13.6.1	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
2.54.31.18	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
149.78.59.15	Israel	147.237.77.216	dover.idf.il	Too Many Headers per Request - 43 Headers	Block	1
149.78.59.15	Israel	147.237.77.216	dover.idf.il	Illegal Byte Code Character in Header Value	Block	1
68.180.229.239	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/undefined/	Block	1
216.218.206.68	United States	147.237.0.17	m.my-kosher-kravi .idf.il	Distributed Unauthorized URL Access on 147.237.0.17/	Block	1
46.19.85.87	Israel	147.237.76.31	nakchal.idf.il	Malformed URL	Block	1
192.115.21.197	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
87.68.245.161	Israel	147.237.0.34	tikshuv.idf.il	Too Many 404: Response Code per Session	Block	1
2.54.189.75	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/m	Block	1
169.229.3.91	United States	147.237.76.42	refuah.idf.il	Abnormally Long Request method	Block	1
79.177.196.49	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
149.78.59.15	Israel	147.237.77.216	dover.idf.il	Malformed HTTP Header Line 2	Block	1
149.78.59.15	Israel	147.237.77.216	dover.idf.il	Distributed Abnormally Long Request	Block	1
62.219.192.39	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
212.179.21.194	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
109.253.142.147	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
2.54.156.238	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
150.70.173.40	Japan	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
80.246.133.178	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/gious	Block	1
68.180.230.29	United States	147.237.77.176	matpash.idf.il	Parameter Type Violation PageNum in www.cogat.idf.il/2065-he/cogat.aspx	Block	1
217.194.197.154	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1