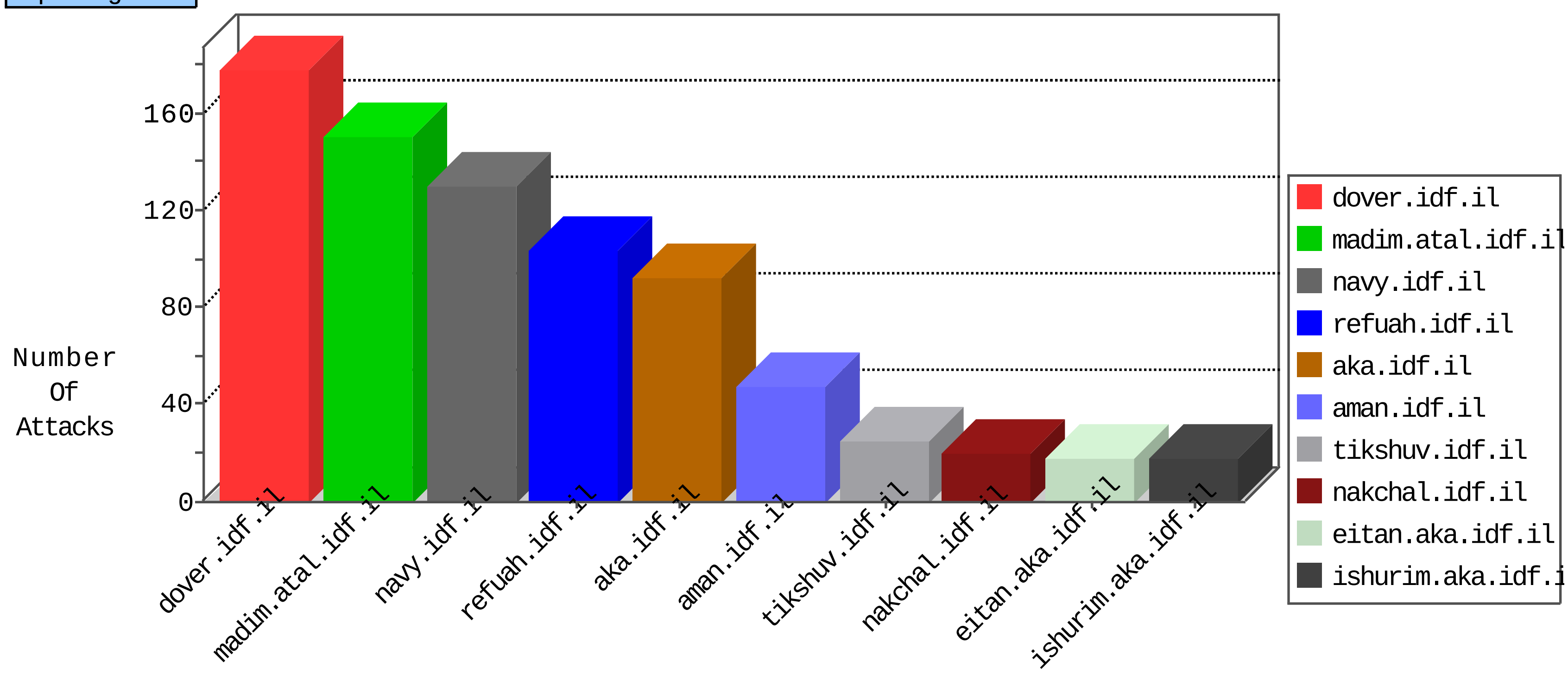
09-07-2016-15:04:06 to 09-07-2016-16:04:06

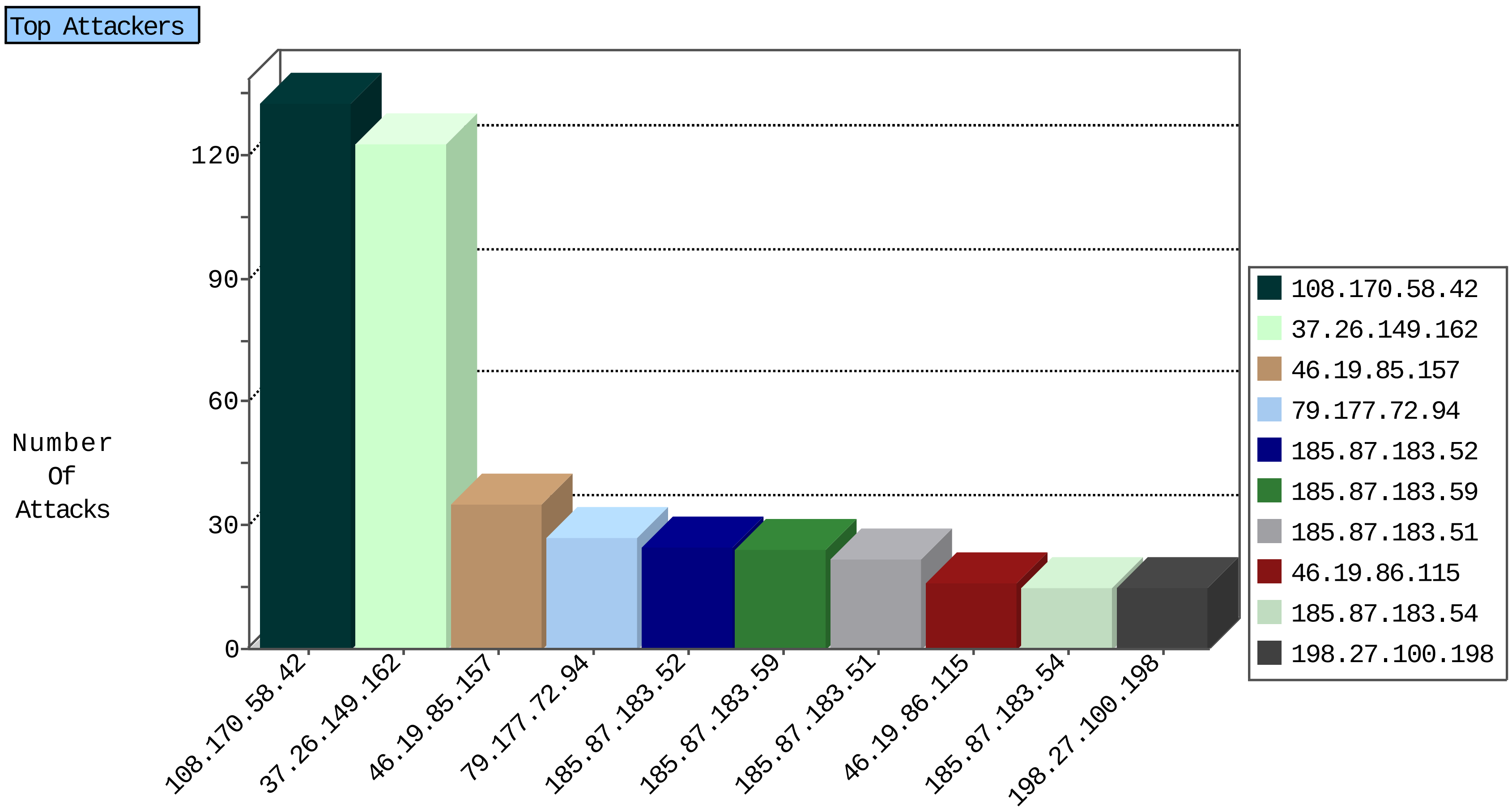
IDF Under Attack
Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

09-07-2016-15:04:06 to 09-07-2016-16:04:06

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.66.148.108	Israel	147.237.72.156	aman.idf.il	Black List	drop	5
109.65.125.134	Israel	147.237.77.216	dover.idf.il	Black List	drop	4
79.177.112.107	Israel	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	2
71.6.216.35	United States	147.237.76.39	mobile.meitav.idf.il	Black List	drop	1
109.66.148.108	Israel	147.237.77.216	dover.idf.il	Black List	drop	1
71.6.216.54	United States	147.237.76.30	himush.idf.il	Black List	drop	1
89.248.174.4	Netherlands	147.237.76.176	test.ncore.idf.il	Black List	drop	1
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
123.59.59.52	China	147.237.77.74	law.idf.il	block-sp-traf1	forward	1
71.6.216.58	United States	147.237.76.34	yohalan.idf.il	Black List	drop	1
66.240.192.138	United States	147.237.76.30	himush.idf.il	Black List	drop	1
71.6.216.60	United States	147.237.76.148	gqcenter.aka.idf.il	Black List	drop	1

09-07-2016-15:04:06 to 09-07-2016-16:04:06

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
198.27.100.198	Canada	147.237.77.216	dover.idf.il	C1000026: HTTP: Access to - index.php?option=com_jce	Permit	6
106.38.241.105	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	2
198.27.100.198	Canada	147.237.77.216	dover.idf.il	22280: HTTP: Joomla Object Injection Vulnerability	Block	1

09-07-2016-15:04:06 to 09-07-2016-16:04:06

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
62.210.113.73	147.237.77.74	France	law.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	2
62.210.124.129	147.237.77.74	France	law.idf.il	ET WEB_SERVER Fake Googlebot UA 1 Inbound	2
93.172.202.134	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
2.229.35.234	147.237.0.19	Italy	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
84.109.231.152	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
80.246.133.98	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.177.29.169	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
212.71.253.43	147.237.0.16	United Kingdom	my-kosher-kravi.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
208.100.26.228	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sS window 1024	1
46.19.85.70	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	portscan: TCP Distributed Portscan	1
31.154.81.20	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
185.27.105.66	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
2.229.35.234	147.237.76.31	Italy	nakchal.idf.il	ET SCAN Potential SSH Scan	1
93.174.93.46	147.237.76.197	Netherlands	e.himush.idf.il	ET SCAN NMAP -sS window 1024	1
2.229.35.234	147.237.0.34	Italy	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
89.138.192.203	147.237.76.86	Israel	navy.idf.il	ET SCAN NMAP -sA (2)	1
2.229.35.234	147.237.0.16	Italy	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
84.108.8.104	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.181.251.72	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
208.100.26.228	147.237.77.212	United States	e.dover.idf.il	ET SCAN NMAP -sS window 1024	1
62.90.243.221	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
195.88.208.193	147.237.76.176	Russian Federation	test.ncore.idf.il	ET SCAN NMAP -sS window 1024	1
31.168.165.94	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
188.120.154.234	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
5.22.134.207	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
95.86.123.100	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
2.229.35.234	147.237.8.14	Italy	e.orchot.idf.il	ET SCAN Potential SSH Scan	1

09-07-2016-15:04:06 to 09-07-2016-16:04:06

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
79.177.72.94	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	20
108.170.58.42	United States	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	18
108.170.58.42	United States	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	18
108.170.58.42	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	18
108.170.58.42	United States	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	18
108.170.58.42	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	18
108.170.58.42	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	15
46.19.86.115	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	14
108.170.58.42	United States	147.237.76.39	mobile.meitav.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	14
108.170.58.42	United States	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	14
212.179.21.194	Israel	147.237.76.197	e.himush.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	13
46.19.85.157	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
46.19.85.157	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
77.126.46.236	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
81.218.163.92	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.86.72	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.157	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
79.176.98.65	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
185.87.183.52	Iran, Islamic Republic of	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	6
2.53.185.112	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	6
2.53.15.247	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	6
46.19.85.157	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
193.43.246.250	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
185.87.183.52	Iran, Islamic Republic of	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
185.87.183.59	Iran, Islamic Republic of	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	5
185.87.183.54	Iran, Islamic Republic of	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
37.76.210.53	Palestinian Territory Occupied	147.237.77.176	matpash.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
46.19.86.92	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
185.87.183.59	Iran, Islamic Republic of	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
192.116.128.90	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
176.13.21.19	Israel	147.237.77.234	halag.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
46.19.86.92	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
185.87.183.52	Iran, Islamic Republic of	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	5
185.87.183.59	Iran, Islamic Republic of	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	5
46.19.86.75	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
185.87.183.51	Iran, Islamic Republic of	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	5
192.116.128.90	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
109.66.198.163	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	5
185.87.183.59	Iran, Islamic Republic of	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	5
46.19.86.195	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
185.87.183.51	Iran, Islamic Republic of	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	5
185.87.183.52	Iran, Islamic Republic of	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	5
46.19.85.67	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	4
185.87.183.51	Iran, Islamic Republic of	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	4
2.53.9.147	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
84.108.27.188	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
185.87.183.51	Iran, Islamic Republic of	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	4
212.179.93.114	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
46.19.85.113	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
185.87.183.54	Iran, Islamic Republic of	147.237.76.86	navy.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	4

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
37.26.149.162	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	123
37.26.148.167	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	9
80.246.138.79	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	5
82.80.196.44	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	4
85.64.245.112	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	4
37.26.149.213	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
198.27.100.198	Canada	147.237.77.216	dover.idf.il	PHP Attempt	Block	4
46.19.86.107	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
176.13.2.221	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.253.134.119	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
79.181.8.173	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	3
109.253.228.225	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.245.15	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
198.27.100.198	Canada	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 198.27.100.198	Block	3
109.186.65.144	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/portalmiluim&yoterws=1&yoter_user=3715	Block	2
2.53.178.103	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
65.55.210.135	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
46.19.86.129	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	2
2.55.44.243	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
66.249.88.142	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
157.55.39.115	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
185.3.147.63	Israel	147.237.72.156	aman.idf.il	Distributed Suspicious Response Code	Block	2
2.55.190.95	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
157.55.39.115	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1283-16648-en/dover.asp	Block	1
77.139.111.179	France	147.237.77.216	dover.idf.il	Unknown HTTP Request Method [[#26]]@klµ9¦í=“Í3ú®¢!yçÃG”¶ÈÚ4»-ÔWÖDl7'•5%t[[#28]]±¢[-¹–Ž\} Ú•ëTÔa@´[[#0]] in URL ûp	Block	1
77.139.111.179	France	147.237.77.216	dover.idf.il	Abnormally Long Header Line request header name	Block	1
217.96.220.116	Poland	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	1
66.249.76.117	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
204.79.180.24	United States	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	1
85.64.32.96	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/9/	Block	1
79.177.112.107	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/shared/usercontrols/navmenu/mazi.idf.il	Block	1
185.89.217.226	Netherlands	147.237.76.86	navy.idf.il	URL is Above Root Directory www.navy.idf.il/../images/shared/home.png	Block	1
77.139.111.179	France	147.237.77.216	dover.idf.il	Illegal HTTP Version øb[[#12]]¶[[#26]]ªOŽ6ÿ[[#3]]bÊ‘îë[[#25]]Ûþ¨ó[[#24]][[#20]]!•è&åCª {wï•¦`Ô[[#24]]q•’F`×WÃ§Üq¯Y¥¾k°¥[[#6]]Éæ	Block	1
132.64.217.56	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1153-21991-he/	Block	1
89.237.65.66	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/yahash/sheelon.aspx	Block	1
71.6.135.131	United States	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to 147.237.77.226/robots.txt	Block	1
212.71.253.43	United Kingdom	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to /	Block	1
198.27.100.198	Canada	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/tmp/krd.php	Block	1
31.154.22.110	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/9/4629.jpg	Block	1
77.139.173.150	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/smalim/	Block	1
77.139.111.179	France	147.237.77.216	dover.idf.il	Abnormally Long Request method	Block	1
217.194.203.52	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.79.134	Israel	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/	Block	1
207.46.13.10	United States	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to tikshuv.idf.il/templates/sitemap/	Block	1
194.90.66.15	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/gius	Block	1
132.66.54.240	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/	Block	1
77.139.111.179	France	147.237.77.216	dover.idf.il	Malformed URL ûp	Block	1
93.172.151.103	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/kiosk/kiosk.aspx	Block	1
77.138.116.40	France	147.237.76.42	refuah.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtLastName in www.refua.atal.idf.il/1518-he/refuah.aspx	Block	1
212.235.56.185	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/	Block	1