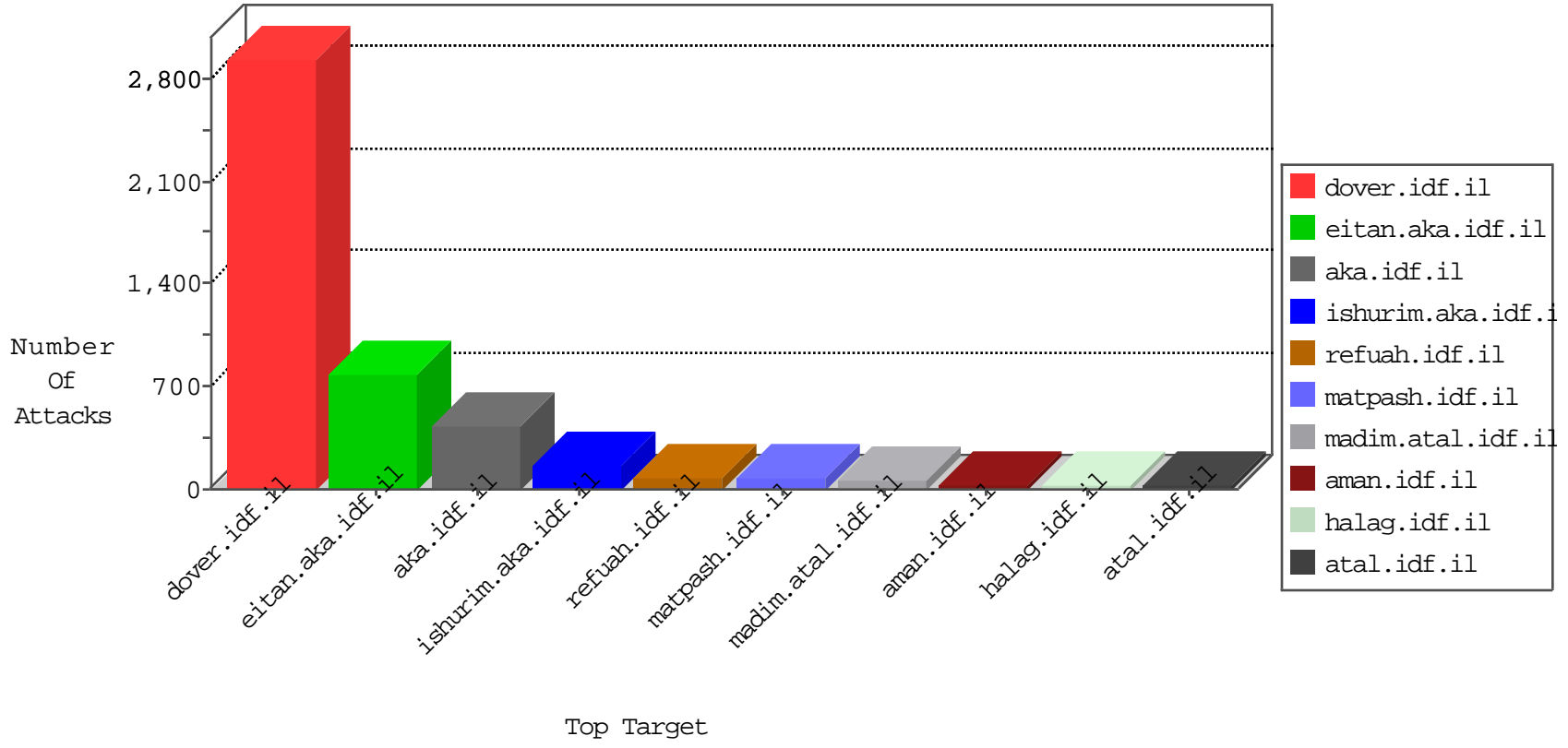


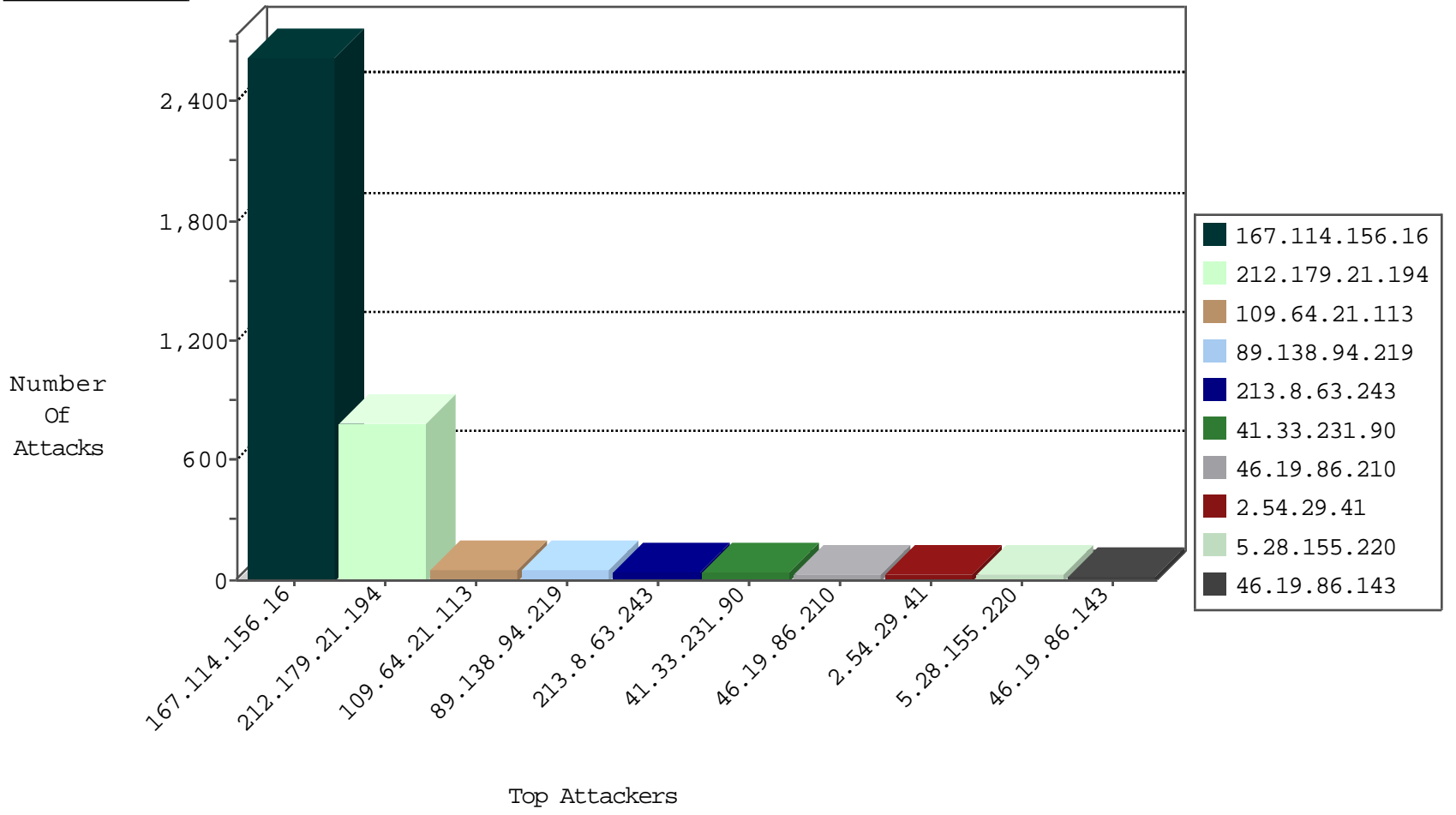
IDF Under Attack Daily Report



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	3607
79.176.206.162	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	6
94.123.202.49	Turkey	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	6
176.189.203.143	France	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	6
205.203.135.1	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
194.204.175.62	Poland	147.237.76.196	e.sviva.idf.il	Block_Ntp_All_Net	drop	1
194.204.175.62	Poland	147.237.76.197	e.himush.idf.il	Block_Ntp_All_Net	drop	1

12-08-2015-12:04:00 to 12-08-2015-13:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
------------------	------------------	----------------	------	-----------	---------------	-------

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	3
212.179.132.202	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	2
37.142.192.91	147.237.72.166	Israel	aka.idf.il	ET SCAN NMAP -sA (2)	2
94.230.86.151	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
85.130.217.215	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.179.180.180	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
210.50.197.154	147.237.8.45	Australia	e.eitan.idf.il	ET SCAN NMAP -sS window 4096	1
210.50.197.154	147.237.8.45	Australia	e.eitan.idf.il	ET SCAN NMAP -f -sS	1
185.112.102.211	147.237.8.50		e.tikshuv.idf.il	ET SCAN Potential SSH Scan	1
119.10.114.32	147.237.76.147	China	chimuch.aka.idf.il	ET SCAN NMAP -sS window 4096	1
93.173.240.94	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
84.176.149.40	147.237.77.216	Germany	dover.idf.il	portscan: TCP Distributed Portscan	1
78.193.2.8	147.237.0.15	France	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
212.106.82.120	147.237.77.176	Palestinian Territory, Occupied	matpash.idf.il	ET SCAN NMAP -sA (2)	1
5.102.254.161	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
210.50.197.154	147.237.8.45	Australia	e.eitan.idf.il	ET SCAN NMAP -sS window 2048	1
199.101.186.201	147.237.76.197	United States	e.himush.idf.il	ET SCAN NMAP -sS window 1024	1
192.114.91.232	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
176.12.139.82	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
109.64.21.113	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Checksum	Invalid checksum. Packet dropped.	drop	51
89.138.94.219	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	42
212.179.21.194	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	34
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	33
213.8.63.243	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid sequence number	monitor	30
46.19.86.210	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	28
2.54.29.41	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
46.19.86.190	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
79.181.4.118	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	21
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	20
5.29.230.12	Israel	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	16
213.8.63.243	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	13
77.30.180.65	Saudi Arabia	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
66.249.66.39	United States	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
77.125.93.217	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
5.28.155.220	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	11
37.26.148.215	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
185.120.125.19		147.237.72.166	aka.idf.il	drop	SAM rule	drop	9
109.65.81.196	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
41.47.71.45	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
46.19.85.4	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
62.0.117.233	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
5.29.201.150	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	8
5.29.201.150	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
185.3.144.137	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
79.177.135.144	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.85.4	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
149.78.154.69	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
46.19.86.250	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
109.64.147.102	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
66.249.93.234	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
81.218.44.254	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
89.135.240.233	Hungary	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	6
5.28.155.220	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
79.178.30.102	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
31.168.11.194	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.180.117.187	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.160.96	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
5.28.155.220	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
176.12.140.24	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.52.191.213	Israel	147.237.76.30	himush.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
109.66.199.212	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
105.94.136.2	Egypt	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
89.138.94.219	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	5
82.166.98.13	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
185.120.125.55		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
82.80.154.209	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
91.98.103.46	Iran, Islamic Republic of	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
176.12.138.191	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	5
82.80.154.209	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
212.179.21.194	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	742
46.19.86.143	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	22
176.12.142.60	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	13
176.13.18.89	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	13
138.134.102.15	Israel	147.237.77.234	halag.idf.il	Multiple Unauthorized URL Access from 138.134.102.15	Block	8
89.138.70.50	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 89.138.70.50	Block	7
46.19.85.84	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	5
208.115.113.88	United States	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 208.115.113.88	Block	4
46.19.85.213	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
132.72.33.84	Israel	147.237.72.167	ishurim.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	3
41.230.14.223	Tunisia	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 41.230.14.223	Block	3
208.184.112.75	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	2
66.249.66.16	Israel	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	2
5.29.83.178	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
212.199.69.213	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	2
78.72.132.232	Sweden	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	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	2
78.72.132.232	Sweden	147.237.77.176	matpash.idf.il	Distributed Unauthorized URL Access on www.cogat.idf.il/xmlrpc.php	Block	2
176.13.11.116	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Multiple Illegal Parameter Encoding from 176.13.11.116	None	2
176.10.104.240	Switzerland	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	2
208.184.112.75	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	2
176.12.136.71	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
109.65.216.140	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
176.13.7.154	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
79.180.119.242	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.78.18	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1471-he/atal.aspx	Block	1
185.45.52.143	Belgium	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/6/4616.jpg	Block	1
41.230.14.223	Tunisia	147.237.72.166	aka.idf.il	Unknown Parameter C@ID in www.aka.idf.il/giyus/qanda/	None	1
107.178.194.87	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
176.12.138.191	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
85.65.204.39	Israel	147.237.76.42	refuah.idf.il	Parameter Type Violation ct100\$ContentPlaceholder1\$txtLastName in www.refua.atal.idf.il/1518-he/refuah.aspx	Block	1
2.54.3.46	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
80.246.136.168	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.19.85.234	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
149.78.227.155	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/requestpayslipexplanation.aspx	None	1
114.98.241.142	China	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/1570-ar/idfg.aspx/trackback/	Block	1
207.46.13.141	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	1
46.19.85.60	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
37.26.146.242	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
92.99.252.189	United Arab Emirates	147.237.77.216	dover.idf.il	Multiple Fullwidth/Halfwidth Unicode Encoding on URL/Parameter(+) from 92.99.252.189	Block	1
66.249.66.34	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/sip_storage/files/6/63076.pdf	Block	1
176.13.11.116	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Illegal Parameter Encoding rnd in m.my-kosher-kravi.idf.il/ajax/createcaptchaimage.aspx	None	1
46.19.86.165	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
173.252.121.119	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
2.54.128.181	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
82.80.154.209	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.19.85.223	Israel	147.237.77.216	dover.idf.il	Abnormally Long Request request version	Block	1
79.181.62.223	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
212.106.82.120	Palestinian Territory Occupied	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 212.106.82.120	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/english/history/entebbel.stm<p rel=	Block	1