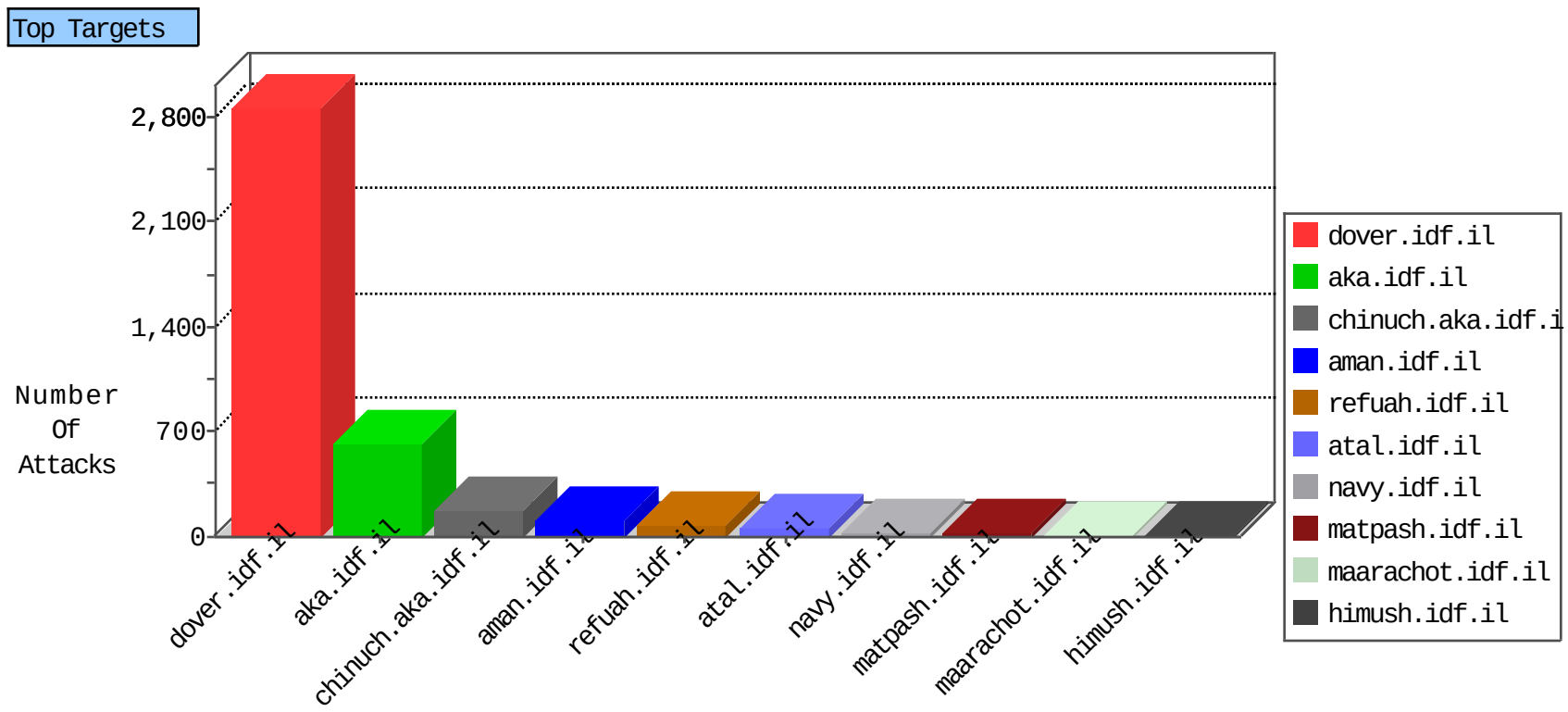
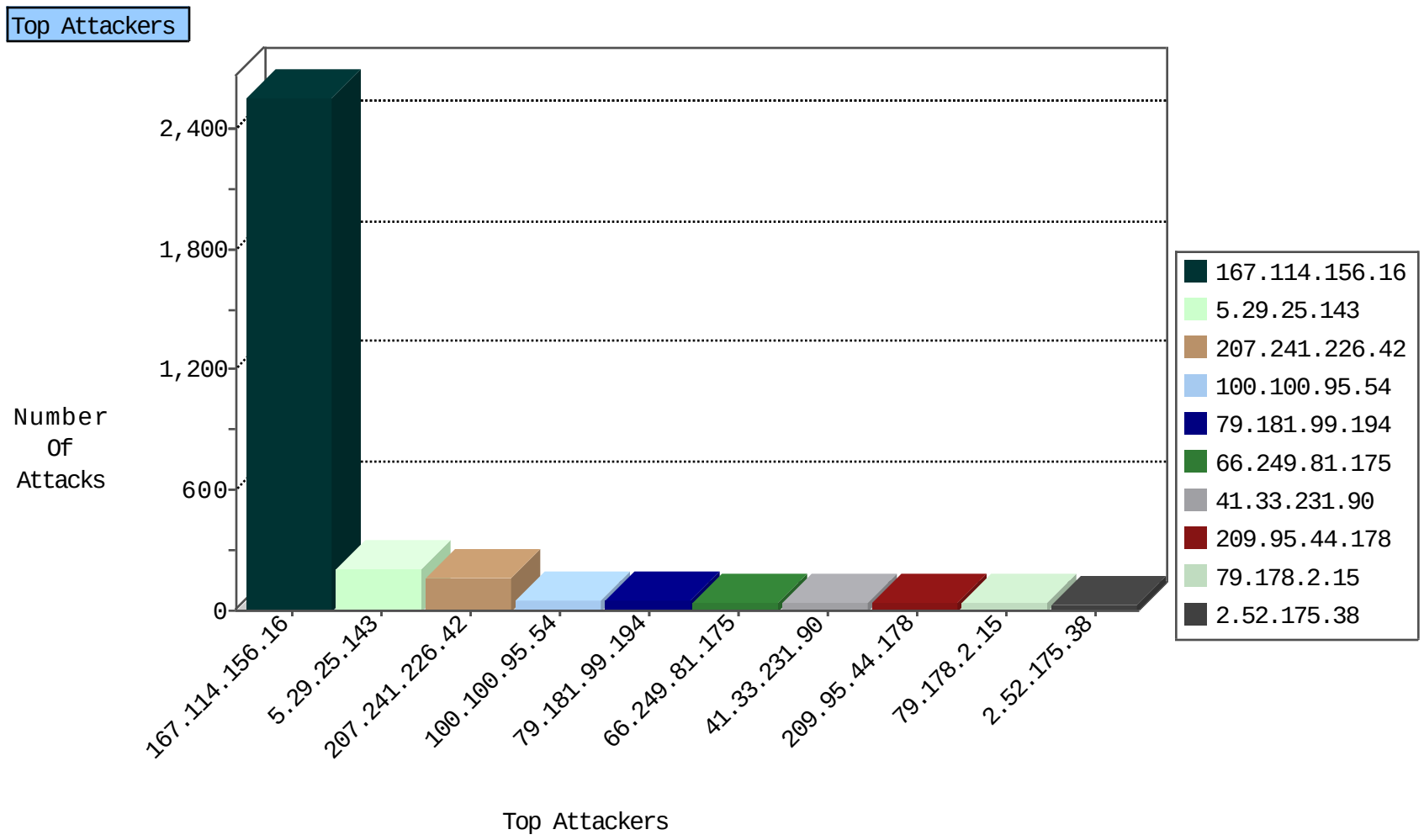
12-01-2015-22:04:08 to 12-01-2015-23:04:08

IDF Under Attack Daily Report

Top Targets



Top Attackers



12-01-2015-22:04:08 to 12-01-2015-23:04:08

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	3453
183.89.121.30	Thailand	147.237.76.202	e.halag.idf.il	JLM_Purple_Con_Limit_Http	drop	1

12-01-2015-22:04:08 to 12-01-2015-23:04:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
41.96.104.129	Algeria	147.237.77.216	dover.idf.il	13444: HTTP: WhatWeb User-Agent Header	Block	2

12-01-2015-22:04:08 to 12-01-2015-23:04:08

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
66.249.81.175	147.237.77.233	United States	atal.idf.il	ET SCAN NMAP -sA (2)	4
66.249.66.61	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
134.191.232.72	147.237.77.170	Israel	maarachot.idf.il	ET SCAN NMAP -sA (2)	2
79.176.132.215	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.174.70.237	147.237.76.42	Russian Federation	refuah.idf.il	ET SCAN Potential SSH Scan	1
198.20.69.74	147.237.76.177	United States	ncore.idf.il	ET DROP Dshield Block Listed Source	1
173.65.67.76	147.237.76.42	United States	refuah.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.72.14	China	dover.idf.il(old)	ET SCAN Potential SSH Scan	1
173.65.67.76	147.237.76.38	United States	e.e.meitav.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.0.19	China	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
173.65.67.76	147.237.76.31	United States	nakchal.idf.il	ET SCAN Potential SSH Scan	1
50.204.188.142	147.237.77.121	United States	e.navy.idf.il	ET SCAN NMAP -f -sS	1
94.102.48.195	147.237.76.30	Netherlands	himush.idf.il	ET SCAN NMAP -sS window 1024	1
31.6.71.154	147.237.0.16	Poland	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
87.68.84.68	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.177.37.241	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.174.70.237	147.237.77.227	Russian Federation	e.hamaz.idf.il	ET SCAN Potential SSH Scan	1
209.126.116.147	147.237.0.16	United States	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
185.106.94.91	147.237.76.38		e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
59.45.79.117	147.237.76.86	China	navy.idf.il	ET SCAN Potential SSH Scan	1
173.65.67.76	147.237.76.39	United States	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.0.200	China	m4u.idf.il	ET SCAN Potential SSH Scan	1
173.65.67.76	147.237.76.34	United States	yohalan.idf.il	ET SCAN Potential SSH Scan	1
50.204.188.142	147.237.77.121	United States	e.navy.idf.il	ET SCAN NMAP -sS window 2048	1
37.142.161.215	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
87.68.248.205	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.178.129.52	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1

12-01-2015-22:04:08 to 12-01-2015-23:04:08

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
5.29.25.143	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	94
100.100.95.54		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	50
79.181.99.194	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	50
66.249.81.175	United States	147.237.77.233	atal.idf.il	drop	First packet isn't SYN	drop	39
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
209.95.44.178	United States	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	36
100.100.77.33		147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	22
79.172.193.32	Hungary	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	14
79.181.182.125	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	14
79.178.2.15	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
100.100.119.234		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
100.100.89.239		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	12
185.120.126.35		147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.85.12	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
100.100.108.24		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	8
66.249.67.155	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
79.178.2.15	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
37.58.75.46	Netherlands	147.237.76.39	mobile.meitav.idf.i	drop	SAM rule	drop	6
46.19.85.237	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
100.100.74.185		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
37.58.75.46	Netherlands	147.237.76.42	refuah.idf.il	drop	SAM rule	drop	6
79.183.26.105	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.180.189.183	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
37.26.146.237	Israel	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
46.19.85.147	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
213.57.138.223	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	6
46.19.85.147	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
79.178.144.34	Israel	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
213.57.138.223	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
31.168.92.94	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
46.19.85.48	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
37.58.75.46	Netherlands	147.237.76.30	himush.idf.il	drop	SAM rule	drop	6
79.178.201.88	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
100.100.95.54		147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	6
77.125.98.99	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
213.57.138.223	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
85.250.74.163	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
46.19.85.48	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
79.178.2.15	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	5
46.19.85.48	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
79.178.2.15	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	5
94.230.86.252	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.86.48	Israel	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	5
46.19.85.46	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
79.178.2.15	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
2.52.54.181	Israel	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	5
2.52.175.38	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
79.178.2.15	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
46.19.86.238	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.85.210	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
2.52.175.38	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
207.241.226.42	United States	147.237.76.147	chinuch.aka.idf.il	Multiple Unauthorized URL Access from 207.241.226.42	Block	162
5.29.25.143	Israel	147.237.72.166	aka.idf.il	Automated Vulnerability Scanning	Block	108
85.64.89.98	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 85.64.89.98	Block	7
87.68.17.163	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/8/	Block	5
176.12.150.115	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtAreaRemarks in m.my-kosher-kravi.idf.il/templates/training/training.aspx	Block	4
46.19.86.45	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
54.94.178.193	Brazil	147.237.77.176	matpash.idf.il	Distributed PHP Attempt	Block	3
46.19.85.147	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
217.132.22.215	Israel	147.237.77.216	dover.idf.il	Parameter Type Violation SearchText in www.idf.il/1065-he/dover.aspx	Block	2
164.138.114.45	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/geneal.aspx	Block	2
54.244.22.103	United States	147.237.76.147	chinuch.aka.idf.il	Suspicious Response Code_Custom_Temporary	Block	2
79.178.98.98	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	2
176.13.10.23	Israel	147.237.0.19	madim.atal.idf.il	Suspicious Response Code	Block	2
79.180.39.44	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/controls/atuda/Â	Block	2
73.212.124.204	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/aman	Block	2
204.13.200.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	2
2.54.29.166	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/modiin/resources/images/favicon/favicon.png	Block	2
79.183.26.105	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
54.94.178.193	Brazil	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/index.php	Block	2
87.68.166.104	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	2
37.142.202.22	Israel	147.237.77.176	matpash.idf.il	Distributed Unauthorized URL Access on www.cogat.idf.il/xmlrpc.php	Block	1
85.65.176.168	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$btnAtudaBack in www.aka.idf.il/main/giyus/atuda/asmachta.aspx	None	1
66.249.75.102	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/navy/navy/terms.aspx	Block	1
142.0.132.44	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1523-en/shared/usercontrols/headerupper/	Block	1
5.28.172.180	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
84.108.46.127	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
207.241.226.42	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
79.182.11.227	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
185.120.125.45		147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
52.29.95.104	United States	147.237.76.42	refuah.idf.il	PHP Attempt	Block	1
95.86.114.127	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/	Block	1
46.19.85.46	Israel	147.237.77.216	dover.idf.il	Malformed URL _pk_id.20.8afc=292f111f6ea0efbf.1438797224.2.1438809722.1438797224.;	Block	1
86.104.162.55	Romania	147.237.76.147	chinuch.aka.idf.il	PHP Attempt	Block	1
8.37.70.135	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1153-he/dover.aspx&usg=alkjrhjalmcbsy_9t1mu54hs87p6yh0t4w	Block	1
84.228.67.44	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//resources/images/innerpage/goback.gif	Block	1
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	1
66.249.66.75	Israel	147.237.72.166	aka.idf.il	Unknown Parameter hc_location in www.aka.idf.il/main/giyus/general.aspx	None	1
157.55.39.17	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 157.55.39.17	Block	1
2.54.179.95	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
80.246.136.102	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
197.38.114.43	Egypt	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/xmlrpc.php	Block	1
109.67.149.250	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.19.86.233	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
87.69.55.159	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/registrationwizard/step2.aspx	Block	1
180.76.15.139	China	147.237.72.156	aman.idf.il	Unauthorized URL Access to list.ips.gov.il/list5.htm	Block	1
66.249.81.212	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/aman	Block	1
176.12.150.115	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
40.77.167.14	United States	147.237.76.147	chinuch.aka.idf.il	Multiple Unauthorized URL Access from 40.77.167.14	Block	1
85.65.200.220	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
217.132.54.93	Israel	147.237.77.226	www.chamatz.aka.idf.il	Distributed PHP Attempt	Block	1