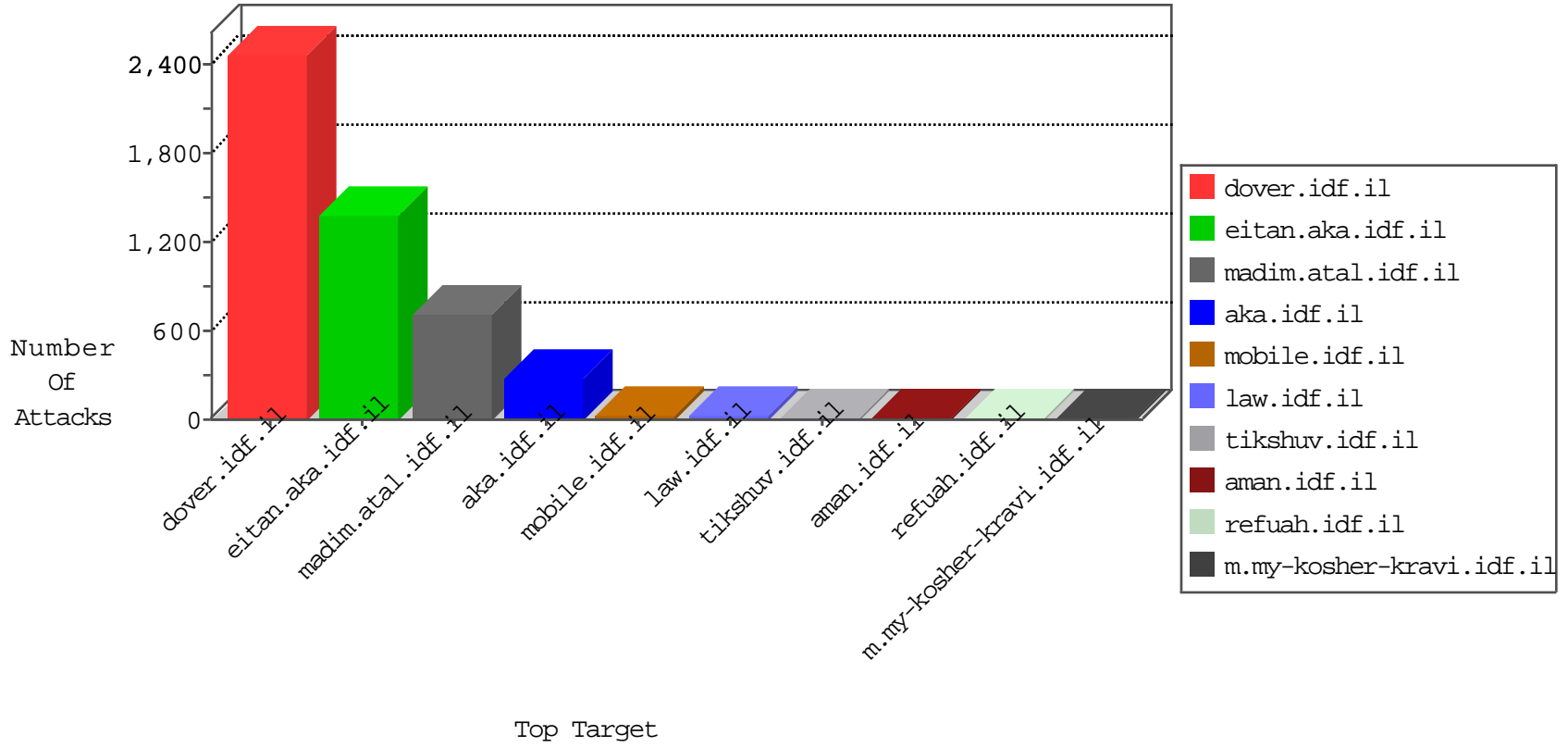


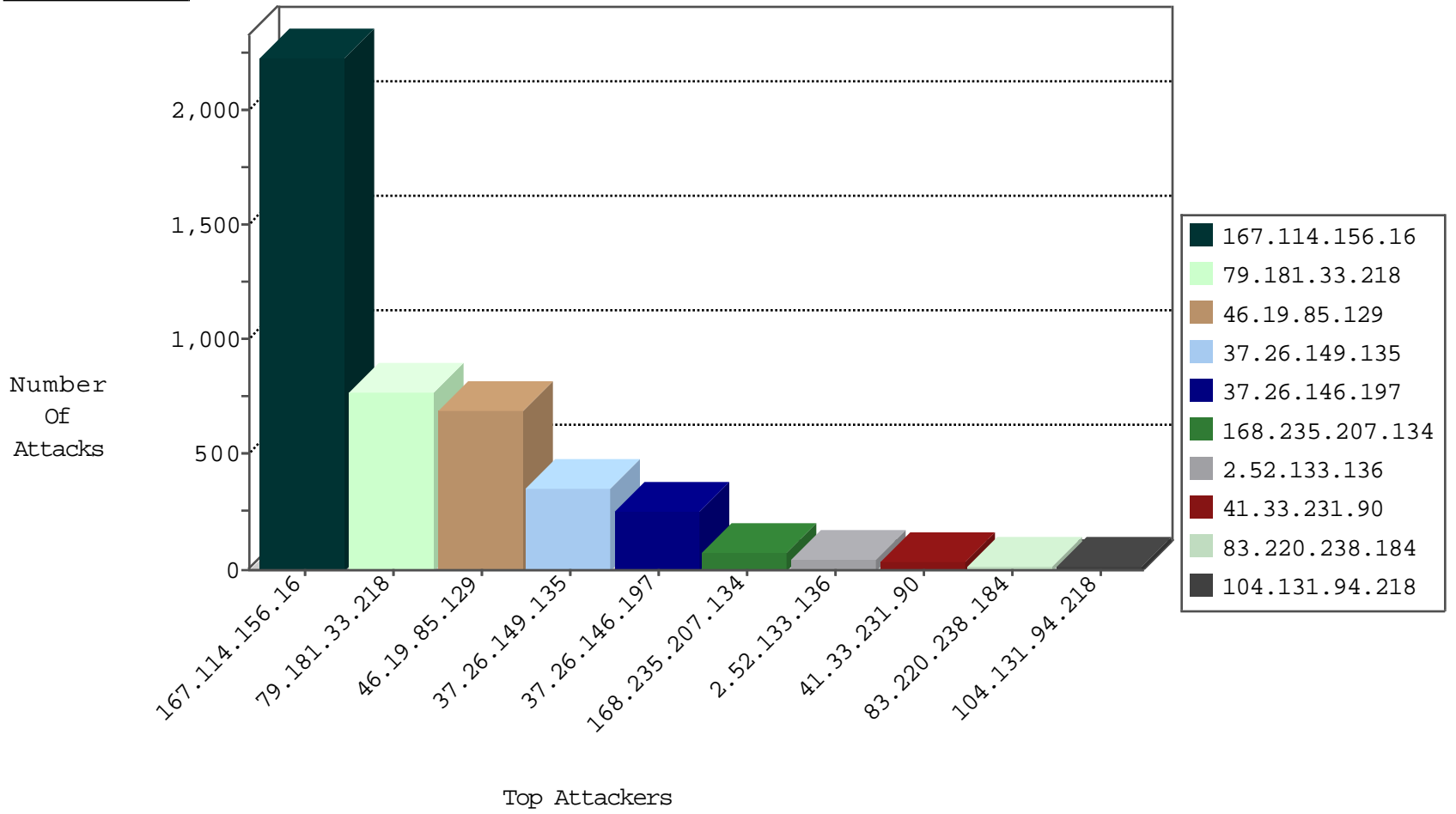
IDF Under Attack Daily Report



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	3461
66.249.78.146	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	305
66.249.78.254	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	105
168.235.207.134	United States	147.237.77.216	dover.idf.il	JLM_Dover_Con_Limit_Https	drop	28
168.235.207.134	United States	147.237.77.216	dover.idf.il	F_Dover_Under_Attack_Con_Http	drop	2
134.147.203.115	Germany	147.237.76.199	e.nakchal.idf.il	Block_Ntp_All_Net	drop	2
168.235.207.134	United States	147.237.77.216	dover.idf.il	F_Dover_Under_Attack_Con_Htps	drop	1

12-19-2015-19:04:07 to 12-19-2015-20:04:07

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	4
66.249.78.146	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
43.229.53.89	147.237.0.35	Japan	akaws.idf.il	ET SCAN Potential SSH Scan	1
147.27.11.143	147.237.77.19	Greece	law-forum.idf.il	ET SCAN NMAP -sS window 1024	1
115.182.17.13	147.237.0.16	China	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 4096	1
115.182.17.13	147.237.0.16	China	my-kosher-kravi.idf.il	ET SCAN NMAP -f -sS	1
94.102.60.89	147.237.72.217	Netherlands	e.idf.il	ET SCAN NMAP -sS window 1024	1
50.204.188.142	147.237.77.121	United States	e.navy.idf.il	ET SCAN NMAP -sS window 1024	1
43.229.53.89	147.237.0.17	Japan	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
147.27.11.143	147.237.77.19	Greece	law-forum.idf.il	ET SCAN NMAP -sS window 3072	1
119.146.221.68	147.237.76.42	China	refuah.idf.il	ET SCAN Potential SSH Scan	1
115.182.17.13	147.237.0.16	China	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 2048	1
111.255.53.152	147.237.0.33	Taiwan	idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
79.181.33.218	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	687
168.235.207.134	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	66
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
37.26.146.197	Israel	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	35
37.26.149.135	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	27
37.26.146.197	Israel	147.237.76.200	eitan.aka.idf.il	drop	First packet isn't SYN	drop	20
37.26.146.197	Israel	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	19
37.26.146.197	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	16
37.26.146.197	Israel	147.237.76.200	eitan.aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	11
83.220.238.184	Russian Federation	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	10
104.131.94.218	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
2.52.133.136	Israel	147.237.72.166	aka.idf.il	SYN Attack		reject	10
2.52.133.136	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
5.22.134.85	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
2.52.133.136	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	9
2.52.133.136	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
77.127.221.216	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
2.52.133.136	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	8
79.183.233.76	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
46.19.86.250	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
109.67.58.20	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.253.157.234	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
94.230.86.138	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
213.57.141.126	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	5
37.26.146.197	Israel	147.237.76.200	eitan.aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	5
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
213.57.141.126	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	5
37.26.146.197	Israel	147.237.8.45	e.eitan.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
37.26.149.135	Israel	147.237.76.200	eitan.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
79.183.164.134	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
89.138.85.113	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
2.54.41.55	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
192.115.83.5	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.86.222	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
31.210.186.178	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
79.179.174.24	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	3
87.68.82.255	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
213.57.100.144	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
147.235.8.74	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
46.19.86.96	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.180.21.51	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.19.51	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
188.120.148.234	Israel	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
109.66.164.52	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
185.3.144.35	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
77.125.161.59	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
84.110.39.250	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.129	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 46.19.85.129	Block	404
37.26.149.135	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	317
46.19.85.129	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	157
37.26.146.197	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	136
46.19.85.129	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (403) in Session from 46.19.85.129	Block	136
79.181.33.218	Israel	147.237.76.200	eitan.aka.idf.il	Distributed Too Many of the Same Response Code (404)	Block	90
46.19.85.241	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	8
211.123.214.30	Japan	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 211.123.214.30	Block	3
2.52.38.166	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
85.64.76.118	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	3
204.13.200.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	2
46.120.212.177	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
84.94.38.200	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/main/giyus/authenticationsservice.aspx/getauthuser	Block	2
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	2
109.253.140.196	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	2
46.19.86.96	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in URL from 46.19.86.96	Block	2
149.88.66.67	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
37.26.147.205	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
149.78.59.239	Israel	147.237.72.156	aman.idf.il	Malformed URL	Block	1
68.180.230.224	United States	147.237.76.31	nakchal.idf.il	Parameter Type Violation PageNum in www.nakchal.idf.il/1111-he/nakchal.aspx	Block	1
61.135.190.197	China	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to 147.237.0.34/style/1.he/langstyle.css	Block	1
109.66.133.73	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/sachar/index	Block	1
89.76.82.40	Poland	147.237.77.176	matpash.idf.il	Admin Blocking	Block	1
46.117.148.230	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1462-he/atal.aspx	Block	1
176.13.12.45	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
79.183.227.26	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
40.77.167.73	United States	147.237.77.216	dover.idf.il	Multiple Fullwidth/Halfwidth Unicode Encoding on URL/Parameter(+) from 40.77.167.73	Block	1
149.88.228.158	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https://www.idf.il/	Block	1
5.22.131.107	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
149.78.59.239	Israel	147.237.72.156	aman.idf.il	Abnormally Long Header Line request header name	Block	1
66.249.78.97	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/rights/asp/info.asp	Block	1
107.178.194.83	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
54.153.33.233	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
176.12.139.128	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
85.64.135.211	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
77.125.72.253	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
149.78.59.239	Israel	147.237.72.156	aman.idf.il	NULL Character in Header Name at wAžc[[#26]]A?[[#19]]Af A+[[#28]]&A AYZ9{iA, oKQ=A\$[[#27]]0A?@[[#30]]&uA?A~A,, 7hAf A?TUUA'7A~A,, [[#30]]A" [[#16]]A...A~aA~A; •OA%=Af[[#22]]A%A•A~A?A~ A@A"A; A+~A"A"AS[[#21]]>\$AeA; A~ASoA°A A+~A?A~Y[[#28]] [[#0]]A~A+ A~OA"A" A" (A•A~A~L?4A, A~KA~A~[[#4]]A,, [[#12]]Ae: AŠA~A~ [[#25]]A?-8B)AŠA' A?A°A» jKA?5Až#8PnA¶dA@_A, A~A~aA~O[[#4]]A~ +Mi){AeA~[[#17]]DÄfO a0AšVÄ'm##[[#21]]A@6	Block	1
61.135.190.198	China	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to 147.237.0.19/	Block	1
213.57.43.123	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/himush/site/he/himush.asp	Block	1
109.186.31.177	Israel	147.237.76.42	refuah.idf.il	Parameter Type Violation ct100\$ContentPlaceHolder1\$aptchaText in www.refua.atal.idf.il/1518-he/refuah.aspx	Block	1
89.76.82.40	Poland	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/administrator	Block	1
188.209.109.244	Romania	147.237.77.74	law.idf.il	PHP Attempt	Block	1
46.19.85.41	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
149.88.238.126	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
5.28.136.233	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
149.78.59.239	Israel	147.237.72.156	aman.idf.il	Illegal Byte Code Character in Header Name wAžc[[#26]]A?[[#19]]Af A+[[#28]]&A AYZ9{iA, oKQ=A\$[[#27]]0A?@[[#30]]&uA?A~A,, 7hAf A?TUUA'7A~A,, [[#30]]A" [[#16]]A...A~aA~A; •OA%=Af[[#22]]A%A•A~A?A~ A@A"A; A+~A"A"AS[[#21]]>\$AeA; A~ASoA°A A+~A?A~Y[[#28]] [[#0]]A~A+ A~OA"A" A" (A•A~A~L?4A, A~KA~A~[[#4]]A,, [[#12]]Ae: AŠA~A~ [[#25]]A?-8B)AŠA' A?A°A» jKA?5Až#8PnA¶dA@_A, A~A~aA~O[[#4]]A~ +Mi){AeA~[[#17]]DÄfO a0AšVÄ'm##[[#21]]A@6	Block	1
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/	Block	1
61.135.190.69	China	147.237.0.34	tikshuv.idf.il	Unauthorized URL Access to 147.237.0.34/style/1.he/op/youtube/movie_control.css	Block	1
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	1
46.19.86.4	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1