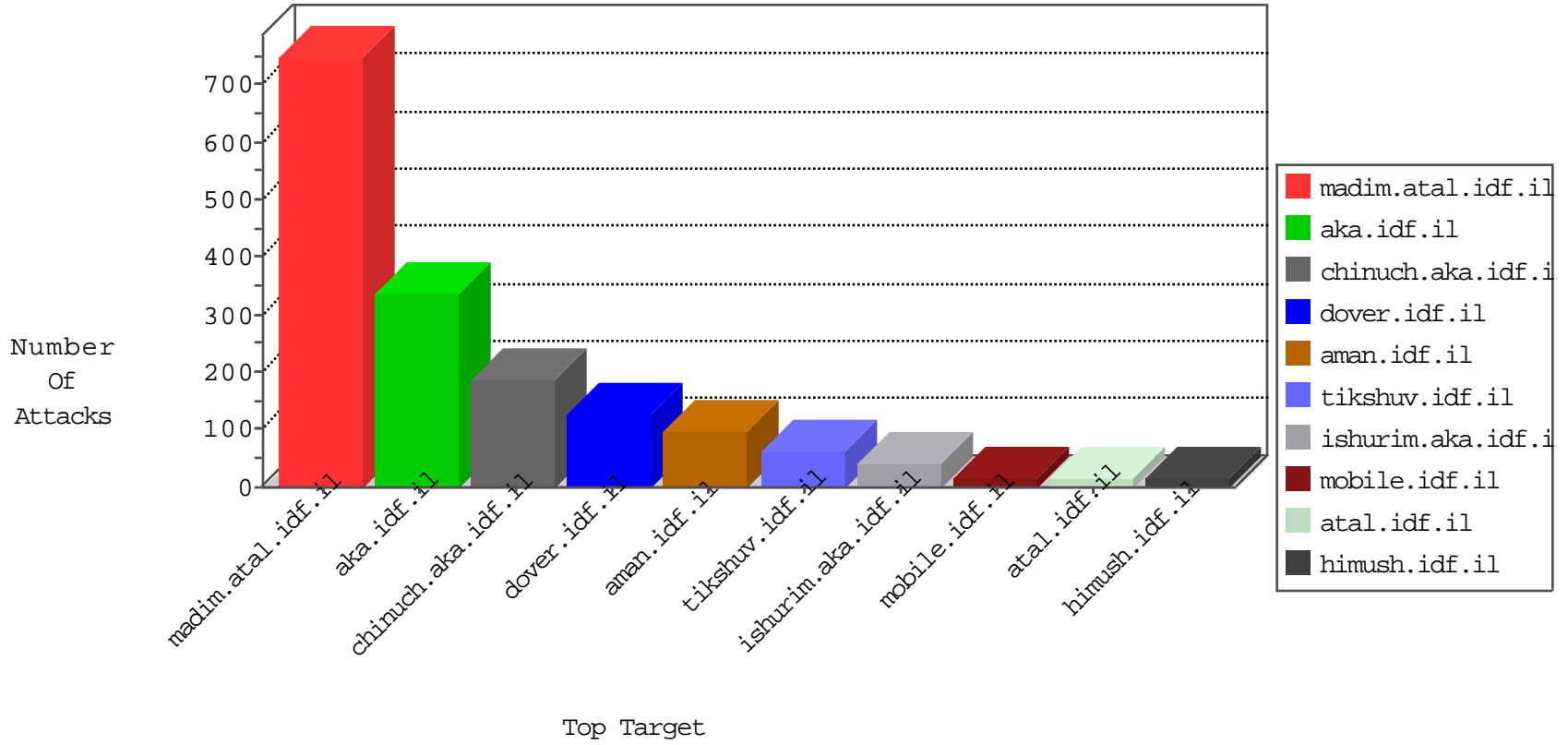


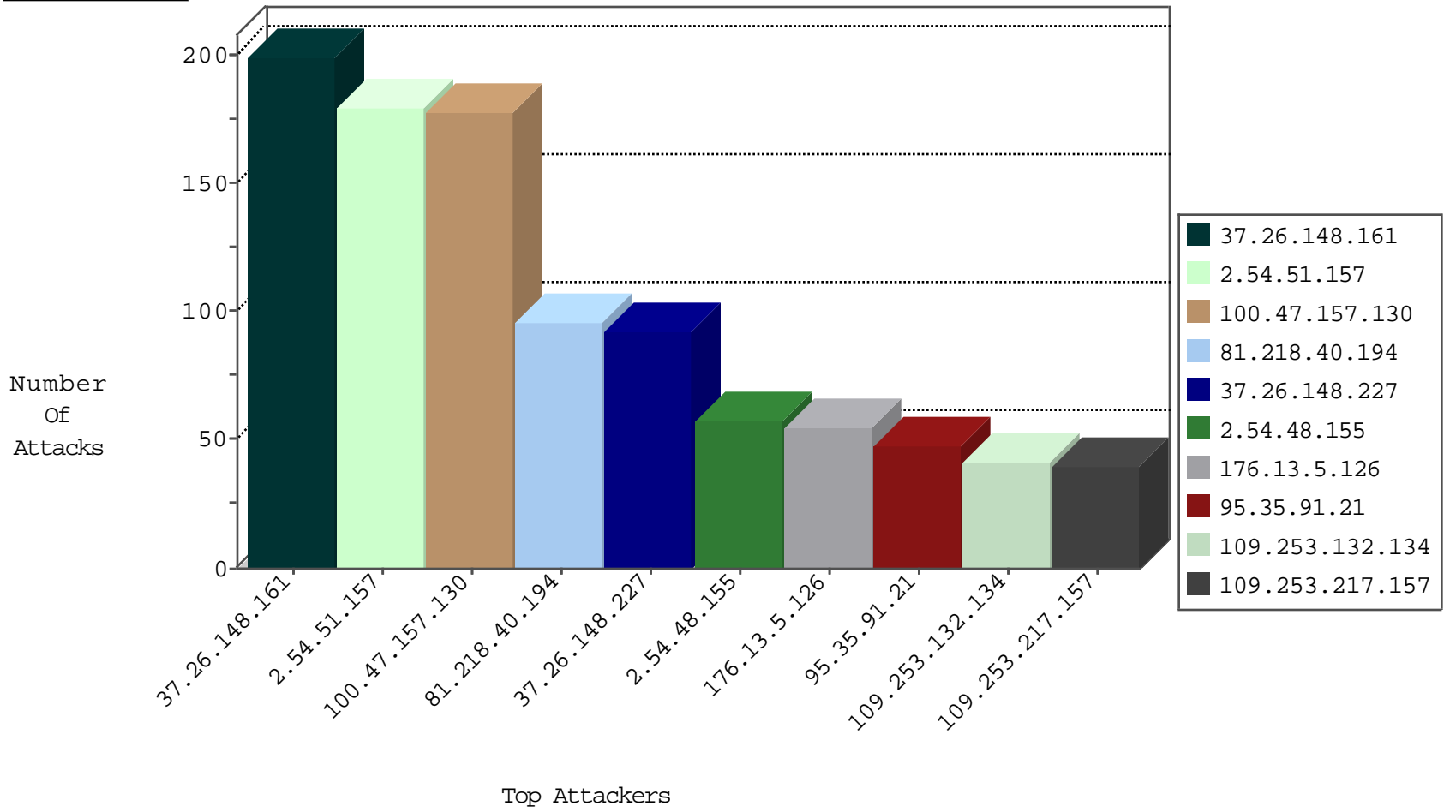
IDF Under Attack Daily Report



Top Targets



Top Attackers



Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
54.72.0.55	Ireland	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
185.94.111.1		147.237.76.197	e.himush.idf.il	Block_Udp_All_Nets	drop	1
45.63.8.39		147.237.76.148	ggcenter.aka.idf.il	Block_Ntp_All_Net	drop	1

02-10-2016-13:04:05 to 02-10-2016-14:04:05

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
174.37.194.144	147.237.77.227	United States	e.hamaz.idf.il	ET SCAN NMAP -sA (2)	3
59.45.79.117	147.237.72.14	China	dover.idf.il(old)	ET SCAN Potential SSH Scan	1
174.37.194.144	147.237.77.212	United States	e.dover.idf.il	ET SCAN NMAP -sA (2)	1
46.116.52.13	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
95.86.102.8	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
37.142.196.78	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
85.173.180.206	147.237.77.227	Russian Federation	e.hamaz.idf.il	ET SCAN Potential SSH Scan	1
2.54.51.215	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
85.64.21.43	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.181.119.170	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
218.246.0.97	147.237.72.217	China	e.idf.il	ET SCAN NMAP -sS window 1024	1
79.178.35.122	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
59.45.79.117	147.237.77.233	China	atal.idf.il	ET SCAN Potential SSH Scan	1
176.106.46.74	147.237.77.216	Palestinian Territory, Occupied	dover.idf.il	portscan: TCP Distributed Portscan	1
59.45.79.117	147.237.76.31	China	nakchal.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.8.46	China	e.chinuch.idf.il	ET SCAN Potential SSH Scan	1
95.86.106.128	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.19.86.107	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
85.173.180.206	147.237.77.234	Russian Federation	halag.idf.il	ET SCAN Potential SSH Scan	1
2.54.149.107	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
85.173.180.206	147.237.77.212	Russian Federation	e.dover.idf.il	ET SCAN Potential SSH Scan	1
84.94.184.120	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.180.250.198	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
217.194.203.100	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.177.51.241	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
188.120.151.249	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
59.45.79.117	147.237.76.197	China	e.himush.idf.il	ET SCAN Potential SSH Scan	1
174.37.194.144	147.237.77.235	United States	sviva.idf.il	ET SCAN NMAP -sA (2)	1

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
81.218.40.194	Israel	147.237.76.147	chinuch.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	96
100.47.157.130	United States	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	86
100.47.157.130	United States	147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	85
82.166.140.117	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	27
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	22
157.55.39.32	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
157.55.39.107	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
62.0.200.169	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
128.12.253.5	United States	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	7
46.19.86.181	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
109.67.237.89	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.64.0.213	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
94.230.93.211	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.183.61.79	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.25.60	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.237	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.178.117.37	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
84.85.32.6	Netherlands	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
79.181.48.173	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
94.230.93.220	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.28	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
94.230.93.131	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.26.149.229	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.26.147.187	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
84.109.112.133	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
94.230.93.185	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
188.120.148.137	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.143.169.119	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.142.64.2	Israel	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
82.80.196.44	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
46.19.86.59	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
91.200.12.106	Ukraine	147.237.77.216	dover.idf.il	drop	SAM rule	drop	4
95.199.9.219	Sweden	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
89.138.228.203	Israel	147.237.77.170	maarachot.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
91.200.12.106	Ukraine	147.237.76.31	nakchal.idf.il	drop	SAM rule	drop	4
94.230.93.140	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.142.64.2	Israel	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
85.130.132.159	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
5.29.170.191	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
46.19.86.130	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
84.228.21.28	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.23.24	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.133	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
40.77.167.40	United States	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.26.149.213	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

02-10-2016-13:04:05 to 02-10-2016-14:04:05

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
79.176.200.240	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.66.143.128	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
94.230.93.236	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
94.230.93.169	Israel	147.237.0.34	tikshuv.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
37.26.148.161	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	113
2.54.51.157	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	94
37.26.148.227	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	82
2.54.51.157	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	82
37.26.148.161	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	77
2.54.48.155	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	57
176.13.5.126	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	50
95.35.91.21	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	48
109.253.132.134	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	41
109.253.217.157	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	40
109.253.192.231	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	19
37.26.148.227	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	10
37.26.148.161	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (403) in Session from 37.26.148.161	Block	8
46.117.160.233	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for aka.idf.il/	Block	6
176.13.5.126	Israel	147.237.0.19	madim.atal.idf.il	Parameter Type Violation ct100\$ContentPlaceholder1\$txtCity in madim.atal.idf.il/mobile/1088-he/meretz.aspx	Block	5
46.117.160.233	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/sip_storage/files/9/	Block	3
2.52.39.86	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.17.165	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.5.96	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.12.59	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
84.108.124.64	Israel	147.237.76.42	refuah.idf.il	Parameter Type Violation ct100\$ContentPlaceholder1\$txtFirstName in www.refua.atal.idf.il/1518-he/refuah.aspx	Block	2
109.66.158.36	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
169.229.3.91	United States	147.237.76.39	mobile.meitav.idf.il	Illegal Byte Code Character in Method <?A%?A/fBUA% zUÃ_xÃµÃ³Ã@Ã?ÃsqwÃ&Ã?P[[#2]]	Block	1
79.178.198.210	Israel	147.237.77.216	dover.idf.il	Multiple Fullwidth/Halfwidth Unicode Encoding on URL/Parameter(+) from 79.178.198.210	Block	1
210.245.25.229	Vietnam	147.237.77.216	dover.idf.il	Distributed Parameter Type Violation on www.idf.il/1395-en/dover.aspx parameter PageNum	Block	1
169.229.3.91	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Multiple Illegal Byte Code Character in Method from 169.229.3.91	Block	1
109.253.130.155	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
37.26.147.197	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
83.166.235.5	Russian Federation	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/	Block	1
169.229.3.91	United States	147.237.77.226	www.chamatz.aka.idf.il	Illegal Byte Code Character in Method ÅªÅªfwÅ²U[[#17]]Åª T3Y[[#8]]Åª^4[[#20]]Åª ÅªNawÅª,ÅªÅª4ÅªÅª Åª?Åª~Åª&Åª?^LÅª³1[[#12]]Åª;[[#2]]Åª,[[#14]]Åª³\D[[#29]]Åªž[[#0]]Åª-	Block	1
169.229.3.91	United States	147.237.76.30	himush.idf.il	Multiple Illegal Byte Code Character in Method from 169.229.3.91	Block	1
66.249.78.170	Israel	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to www.eitan.aka.idf.il/1105-en/contactus.aspx	Block	1
186.202.153.33	Brazil	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
141.212.122.177	United States	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to 147.237.76.200/	Block	1
173.252.90.82	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/https://twitter.com/	Block	1
91.231.192.149	Israel	147.237.72.167	ishurim.aka.idf.il	Multiple Untraceable SSL Sessions from 91.231.192.149 (Unknown SSL Session)	None	1
79.182.33.176	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$TochenPlaceholder\$ct113\$ct101\$ct103\$cbQuesti on\$42 in aka.idf.il/main/giyus/questionnaire.aspx	None	1
169.229.3.91	United States	147.237.76.39	mobile.meitav.idf.il	Malformed URL	Block	1
211.62.81.204	Korea, Republic of	147.237.77.74	law.idf.il	Parameter Type Violation pos in www.law.idf.il/261-7234-en/patzar.aspx	Block	1
169.229.3.91	United States	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in Method from 169.229.3.91	Block	1
169.229.3.91	United States	147.237.77.226	www.chamatz.aka.idf.il	Illegal Byte Code Character in URL	Block	1
169.229.3.91	United States	147.237.76.30	himush.idf.il	NULL Character in Method [[#1]]K*ÃªÃªÃª•[[#0]]Åª-TÃª[[#3]]Åª† Åª+[[#25]]*5[[#23]]Åª?	Block	1
66.249.93.32	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/favicon.ico	Block	1
186.202.153.33	Brazil	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/wp-login.php	Block	1
157.55.39.39	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1787-he/dover.aspx	Block	1
174.37.194.144	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to /	Block	1
91.231.192.149	Israel	147.237.72.167	ishurim.aka.idf.il	SSL Untraceable Connection - Unknown SSL Session	None	1
80.179.223.31	Israel	147.237.77.176	matpash.idf.il	Distributed Unauthorized URL Access on www.cogat.idf.il/sip_storage/files/9/4629.jpg	Block	1
169.229.3.91	United States	147.237.76.39	mobile.meitav.idf.il	Unknown HTTP Request Method <A%?A/fBUA% zUÃ_xÃµÃ³Ã@Ã?ÃsqwÃ&Ã?P[[#2]] in URL	Block	1
46.120.107.127	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/https://www.aman.idf.il/	Block	1