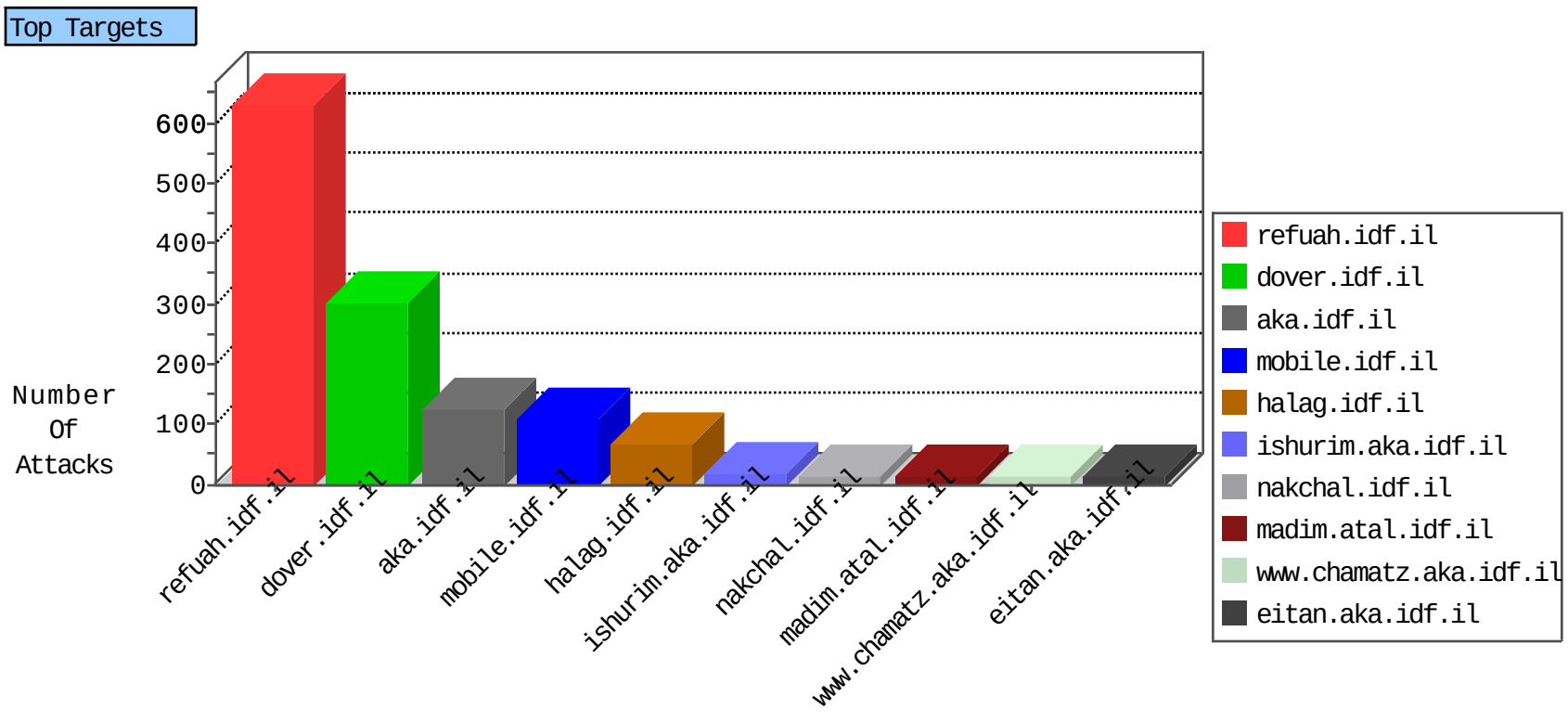
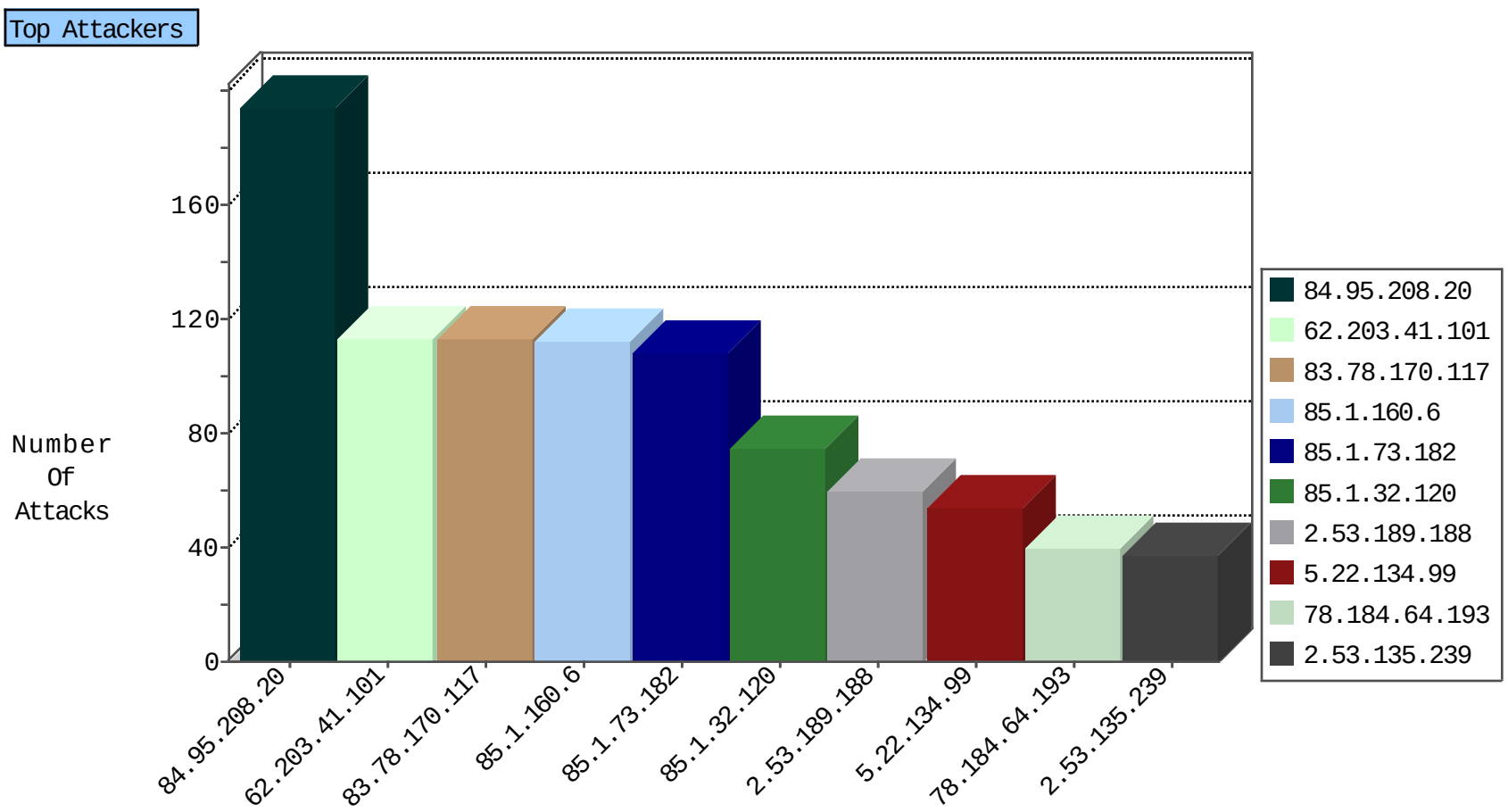
10-02-2016-13:04:01 to 10-02-2016-14:04:01

IDF Under Attack Daily Report



Top Target



Top Attackers

10-02-2016-13:04:01 to 10-02-2016-14:04:01

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
130.0.177.12	Italy	147.237.77.74	law.idf.il	L4 Source or Dest Port Zero	drop	1
177.192.181.98	Brazil	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
66.240.236.119	United States	147.237.76.201	e.atal.idf.i	Black List	drop	1

10-02-2016-13:04:01 to 10-02-2016-14:04:01

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
220.181.125.23	China	147.237.77.233	atal.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Permit	1

10-02-2016-13:04:01 to 10-02-2016-14:04:01

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
185.110.132.201	147.237.76.44	Ukraine	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
58.218.200.137	147.237.76.197	China	e.himush.idf.il	ET SCAN Potential SSH Scan	1
185.110.132.201	147.237.72.156	Ukraine	aman.idf.il	ET SCAN Potential SSH Scan	1
31.220.3.199	147.237.76.44	Belize	e.refuah.idf.il	ET SCAN Potential SSH Scan	1
180.213.5.205	147.237.72.217	China	e.idf.il	ET SCAN NMAP -sS window 1024	1
14.152.59.11	147.237.76.38	China	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
176.47.61.54	147.237.77.216	Saudi Arabia	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
163.172.169.150	147.237.76.199	United Kingdom	e.nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
154.16.199.48	147.237.76.31	United States	nakchal.idf.il	ET SCAN Potential SSH Scan	1
94.102.48.194	147.237.77.243	Netherlands	mobile.idf.il	ET SCAN NMAP -sS window 1024	1
195.9.190.142	147.237.8.14	Russian Federation	e.orchot.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
78.26.169.218	147.237.76.31	Ukraine	nakchal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
185.110.132.201	147.237.77.227	Ukraine	e.hamaz.idf.il	ET SCAN Potential SSH Scan	1
58.218.200.137	147.237.76.199	China	e.nakchal.idf.il	ET SCAN Potential SSH Scan	1
185.110.132.201	147.237.76.30	Ukraine	himush.idf.il	ET SCAN Potential SSH Scan	1
58.218.200.137	147.237.76.148	China	gqcenter.aka.idf.i	ET SCAN Potential SSH Scan	1
185.110.132.201	147.237.0.34	Ukraine	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
31.220.3.199	147.237.76.34	Belize	yohalan.idf.il	ET SCAN Potential SSH Scan	1
178.76.195.202	147.237.76.86	Russian Federation	navy.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
14.152.59.11	147.237.8.46	China	e.chinuch.idf.il	ET SCAN NMAP -sS window 1024	1
163.172.169.150	147.237.76.200	United Kingdom	eitan.aka.idf.il	ET SCAN NMAP -sS window 1024	1
154.16.199.48	147.237.76.148	United States	gqcenter.aka.idf.i	ET SCAN Potential SSH Scan	1
125.65.82.44	147.237.76.86	China	navy.idf.il	ET SCAN NMAP -sS window 1024	1
208.100.26.228	147.237.76.198	United States	e.yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
94.102.48.194	147.237.77.216	Netherlands	dover.idf.il	ET SCAN NMAP -sS window 1024	1
192.223.94.47	147.237.77.170	Bolivia	maarachot.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
66.249.93.217	147.237.77.176	Europe	matpash.idf.il	ET SCAN NMAP -sA (2)	1

10-02-2016-13:04:01 to 10-02-2016-14:04:01

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
2.53.189.188	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	60
5.22.134.99	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	Invalid ACK number	monitor	52
78.184.64.193	Turkey	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	40
223.24.103.117	Thailand	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
2.53.135.239	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	29
83.78.170.117	Switzerland	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	27
62.203.41.101	Switzerland	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	27
85.1.160.6	Switzerland	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	26
62.203.41.101	Switzerland	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	26
83.78.170.117	Switzerland	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	26
85.1.160.6	Switzerland	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	25
85.1.73.182	Switzerland	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	23
85.1.73.182	Switzerland	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	22
62.203.41.101	Switzerland	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	22
83.78.170.117	Switzerland	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	22
85.1.73.182	Switzerland	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	22
85.1.160.6	Switzerland	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	22
85.1.73.182	Switzerland	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	21
62.203.41.101	Switzerland	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	20
83.78.170.117	Switzerland	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	20
85.1.160.6	Switzerland	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	20
85.1.73.182	Switzerland	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	20
85.1.160.6	Switzerland	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	19
82.145.222.192	Europe	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	19
62.203.41.101	Switzerland	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	18
83.78.170.117	Switzerland	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	18
85.1.32.120	Switzerland	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	15
85.1.32.120	Switzerland	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different sequence	alert	15
85.1.32.120	Switzerland	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different sequence	monitor	15
85.1.32.120	Switzerland	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	15
85.1.32.120	Switzerland	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	14
101.127.180.93	Singapore	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	14
109.235.254.148	Turkey	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	14
109.253.194.6	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	13
62.219.47.166	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	12
86.92.217.235	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
109.253.194.6	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
46.43.87.189	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
52.3.127.144	United States	147.237.72.166	aka.idf.il	drop	SAM rule	drop	9
109.253.194.6	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
79.178.206.182	Israel	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	7
2.53.135.239	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	7
93.172.205.208	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	7
46.19.85.62	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
109.201.154.139	Netherlands	147.237.77.227	e.hamaz.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	6
5.29.88.187	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	monitor	6
46.117.113.111	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.62	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
109.253.194.6	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	monitor	6
112.124.124.227	China	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5

10-02-2016-13:04:01 to 10-02-2016-14:04:01

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
84.95.208.20	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	150
84.95.208.20	Israel	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	14
84.95.208.20	Israel	147.237.77.226	www.chamatz.aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	5
84.95.208.20	Israel	147.237.76.200	eitan.aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	5
79.183.71.213	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
79.177.170.47	Israel	147.237.76.31	nakchal.idf.il	Unauthorized HTTP Method	Block	4
5.11.43.181	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1133-19784-ar/idfgdover.aspx	Block	3
84.95.208.20	Israel	147.237.72.166	aka.idf.il	PHP Attempt	Block	3
79.177.170.47	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to nakhal.idf.il/sip_storage/files/2/	Block	3
72.37.140.45	Italy	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 72.37.140.45	Block	3
66.249.65.51	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.65.51	Block	2
212.179.41.221	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/authentication/index	Block	2
72.37.140.45	Italy	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/miluim/templates/inner.asp	Block	2
31.154.45.114	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
77.124.4.248	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
77.139.39.227	France	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/sachar	Block	2
5.11.43.181	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 5.11.43.181	Block	2
212.179.41.221	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
84.95.208.20	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 84.95.208.20	Block	2
169.229.3.91	United States	147.237.72.167	ishurim.aka.idf.il	Malformed URL	Block	1
169.229.3.91	United States	147.237.77.216	dover.idf.il	Multiple Abnormally Long Request from 169.229.3.91	Block	1
46.117.113.111	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
141.0.15.232	Norway	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/giyus/information.aspx	Block	1
77.139.240.226	France	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/home/default.aspx	Block	1
183.129.160.229	China	147.237.0.17	m.my-kosher-kravi.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
169.229.3.91	United States	147.237.72.167	ishurim.aka.idf.il	Unknown HTTP Request Method kúòÞ”[[#5]]#012!ôå½×QÃKI‰ „:[[#17]]ó;Mº‡¾„[[#12]]‹N’ûP³ÕSäÔ?½€ñ¨ in URL	Block	1
66.249.65.188	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-8919-he/refuah.aspx	Block	1
84.95.208.20	Israel	147.237.77.226	www.chamatz.aka.idf.il	PHP Attempt	Block	1
220.181.125.23	China	147.237.77.233	atal.idf.il	Multiple Unauthorized URL Access from 220.181.125.23	Block	1
80.246.136.150	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
169.229.3.91	United States	147.237.77.216	dover.idf.il	Multiple Illegal Byte Code Character in Method from 169.229.3.91	Block	1
66.102.9.5	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
169.229.3.91	United States	147.237.72.167	ishurim.aka.idf.il	Abnormally Long Request method	Block	1
183.129.160.229	China	147.237.0.19	madim.atal.idf.il	SSL Untraceable Connection - Open Mode	None	1
79.177.170.47	Israel	147.237.76.31	nakchal.idf.il	Multiple Unauthorized URL Access from 79.177.170.47	Block	1
169.229.3.91	United States	147.237.77.176	matpash.idf.il	Abnormally Long Request method	Block	1
66.249.69.232	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
37.142.102.236	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
85.65.160.59	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
220.181.125.23	China	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/994-he/atal.aspx	Block	1
82.80.222.116	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/894-ar	Block	1
77.138.180.7	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/ishurim	Block	1
169.229.3.91	United States	147.237.77.216	dover.idf.il	Unknown HTTP Request Method V:cZ©Åœ¥tÆ´¬}ÜÓÛ¼EÃEB[[#2]] in URL	Block	1
66.102.9.22	United States	147.237.72.166	aka.idf.il	Unauthorized Method POST for aka.idf.il/main/home/default.aspx	Block	1
169.229.3.91	United States	147.237.72.167	ishurim.aka.idf.il	Illegal Byte Code Character in Header Name	Block	1
183.129.160.229	China	147.237.0.19	madim.atal.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
169.229.3.91	United States	147.237.77.176	matpash.idf.il	Multiple Illegal Byte Code Character in Method from 169.229.3.91	Block	1
66.249.76.108	Israel	147.237.72.166	aka.idf.il	Unknown Parameter docI.. in www.aka.idf.il/main/giyus/general.aspx	None	1
46.116.60.185	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/404.aspx	Block	1
89.237.91.181	France	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar	Block	1

10-02-2016-13:04:01 to 10-02-2016-14:04:01