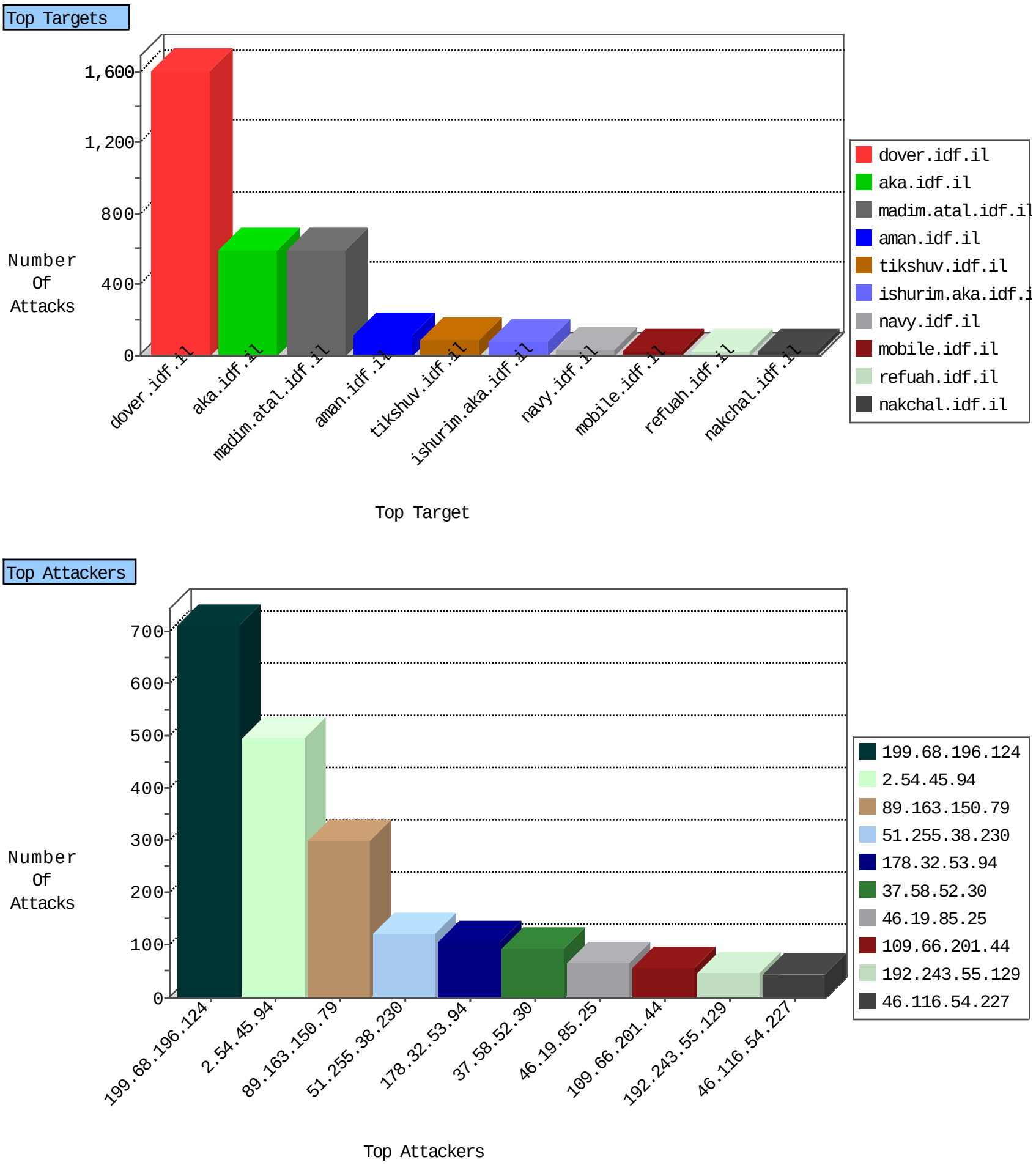
02-21-2016-16:04:08 to 02-21-2016-17:04:08

IDF Under Attack
Daily Report



02-21-2016-16:04:08 to 02-21-2016-17:04:08

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
199.68.196.124	United States	147.237.77.216	dover.idf.il	DOS-Apache-httpd-apr2-BO	dest-reset	603
89.163.150.79	Germany	147.237.77.216	dover.idf.il	DOS-Apache-httpd-apr2-BO	dest-reset	300
207.232.36.181	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	253
178.32.53.94	United Kingdom	147.237.77.216	dover.idf.il	DOS-Apache-httpd-apr2-BO	dest-reset	185
81.218.241.25	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	153
207.232.36.181	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	148
89.163.150.79	Germany	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	88
178.32.53.94	United Kingdom	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	25
199.229.243.161	United States	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	17
109.65.112.60	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	14
89.163.150.79	Germany	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	9
178.32.53.94	United Kingdom	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	7
77.222.205.193	Norway	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	4
37.58.52.30	Germany	147.237.77.216	dover.idf.il	F_Dover_Under_Attack_Con_Http	drop	2
199.68.196.124	United States	147.237.77.216	dover.idf.il	F_Dover_Under_Attack_Con_Http	drop	2
134.147.203.115	Germany	147.237.76.44	e.refuah.idf.il	Block_Ntp_All_Net	drop	2
51.255.38.230	United Kingdom	147.237.77.216	dover.idf.il	F_Dover_Under_Attack_Con_Http	drop	2
134.147.203.115	Germany	147.237.76.197	e.himush.idf.il	Block_Ntp_All_Net	drop	2
192.243.55.129	Dominica	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	1

02-21-2016-16:04:08 to 02-21-2016-17:04:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
136.243.103.156	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
136.243.103.156	Germany	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Block	2
157.55.39.97	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
40.77.167.71	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
66.249.66.184	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1

02-21-2016-16:04:08 to 02-21-2016-17:04:08

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
77.127.87.157	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
66.212.177.166	147.237.8.46	Canada	e.chinuch.idf.il	ET SCAN NMAP -sS window 1024	1
198.20.69.74	147.237.76.202	United States	e.halag.idf.il	ET DROP Dshield Block Listed Source	1
46.19.85.100	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
185.3.144.98	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
109.67.147.179	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
94.102.48.193	147.237.76.38	Netherlands	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
82.102.169.113	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.178.149.125	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.177.29.83	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
74.201.85.87	147.237.77.179	United States	e.mazi.idf.il	ET SCAN Potential SSH Scan	1
212.199.144.158	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
62.90.11.134	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	1
149.78.31.60	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
109.66.59.137	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
93.173.59.73	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.181.219.227	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.178.125.223	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1

02-21-2016-16:04:08 to 02-21-2016-17:04:08

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
199.68.196.124	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	603
89.163.150.79	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	259
51.255.38.230	United Kingdom	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	120
37.58.52.30	Germany	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	93
178.32.53.94	United Kingdom	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	79
199.68.196.124	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	30
213.8.240.168	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	16
128.234.174.105	Romania	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	16
62.219.117.88	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
5.28.182.237	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
69.31.51.99	Anonymous Proxy	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	14
46.19.85.200	Israel	147.237.76.31	nakchal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
192.243.55.129	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
81.218.241.25	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	10
192.243.55.129	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	9
192.243.55.137	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	8
192.243.55.129	Dominica	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	8
109.66.152.131	Israel	147.237.72.167	ishurim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
192.243.55.129	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
128.234.174.105	Romania	147.237.77.216	dover.idf.il	Streaming Engine: TCP SYN Modified Retransmission	Data received before SYN was acknowledged. Stripping all packet data.	drop	7
31.168.196.210	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
84.108.90.253	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
81.218.106.146	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.232	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
79.180.2.98	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.176.211.12	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.249	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
84.108.90.253	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
84.228.87.176	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
41.238.5.123	Egypt	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
109.64.146.61	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
185.3.147.145	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
192.243.55.129	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	6
109.67.68.63	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.48	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.176.183.130	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
31.210.186.46	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
212.179.223.120	Israel	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid sequence number	monitor	5
31.210.187.31	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
192.243.55.129	Dominica	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
64.246.187.42	United States	147.237.76.86	navy.idf.il	Header Rejection	header rejection pattern found in request	monitor	4
89.139.141.12	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
5.102.242.98	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
185.120.125.24		147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	4
79.183.202.210	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.27.70	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

02-21-2016-16:04:08 to 02-21-2016-17:04:08

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.54.45.94	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	499
109.66.201.44	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	57
46.19.85.25	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	52
46.19.86.51	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	29
85.64.191.131	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 85.64.191.131	Block	17
213.8.204.55	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	17
46.19.85.25	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	15
85.64.191.131	Israel	147.237.72.166	aka.idf.il	PHP Attempt	Block	10
46.19.86.42	Israel	147.237.76.42	refuah.idf.il	Parameter Type Violation ctl00$ContentPlaceHolder1$txtLastName in www.refua.atal.idf.il/1518-he/refuah.aspx	Block	5
212.199.236.231	Israel	147.237.72.167	ishurim.aka.idf.i	Too Many of the Same Response Code (404) in Session from 212.199.236.231	Block	5
87.68.69.150	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 87.68.69.150	Block	4
46.116.54.227	Israel	147.237.72.156	aman.idf.il	Multiple Unknown HTTP Request Method from 46.116.54.227	Block	4
85.64.191.131	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/ajax/updatestatus.php	Block	4
62.219.117.88	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 62.219.117.88	Block	4
46.116.54.227	Israel	147.237.72.156	aman.idf.il	Multiple Malformed URL from 46.116.54.227	Block	4
46.116.54.227	Israel	147.237.72.156	aman.idf.il	Multiple Illegal Byte Code Character in Method from 46.116.54.227	Block	3
84.109.132.138	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 84.109.132.138	Block	3
87.68.69.150	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1362	Block	3
46.116.54.227	Israel	147.237.72.156	aman.idf.il	Multiple Abnormally Long Request from 46.116.54.227	Block	3
176.13.6.77	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1152	Block	2
37.142.246.25	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 37.142.246.25	Block	2
77.127.210.79	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/ajax/updatestatus.php	Block	2
197.32.152.186	Egypt	147.237.77.216	dover.idf.il	PHP Attempt	Block	2
46.116.54.227	Israel	147.237.72.156	aman.idf.il	Multiple NULL Character in Header Name from 46.116.54.227	Block	2
31.168.207.252	Israel	147.237.72.167	ishurim.aka.idf.i	Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	2
79.179.161.13	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/https:/www.aman.idf.il/	Block	2
46.121.232.50	Israel	147.237.72.156	aman.idf.il	Too Many Cookies in a Request - 101 cookies	Block	2
176.13.20.204	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	2
212.179.21.194	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	2
37.142.246.25	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/ajax/updatestatus.php	Block	2
197.32.152.186	Egypt	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/xmlrpc.php	Block	2
66.249.78.254	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	2
81.218.105.2	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	2
207.46.13.193	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	2
141.8.132.112	Russian Federation	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	2
79.182.51.12	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	2
80.246.133.97	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/giyus/main/	Block	2
149.88.6.116	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	2
46.116.54.227	Israel	147.237.72.156	aman.idf.il	Multiple Abnormally Long Header Line from 46.116.54.227	Block	2
81.218.106.146	Israel	147.237.72.167	ishurim.aka.idf.i	Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	2
77.127.210.79	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	2
87.68.144.81	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$67 in www.aka.idf.il/main/giyus/questionnaire.aspx	None	2
85.64.191.131	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	2
46.116.54.227	Israel	147.237.72.156	aman.idf.il	Illegal Byte Code Character in Header Value	Block	2
207.46.13.42	United States	147.237.72.166	aka.idf.il	Unknown Parameter d6369898 in www.aka.idf.il/main/home/default.aspx	None	2
81.218.241.25	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 81.218.241.25	Block	2
176.13.5.188	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	2
212.76.122.117	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1038-he/dover.aspx&sa=u&ved=0ahukewifz53_g4nlahwc8nikhzxhd68qfggkmae&usg=afqjcnepjiaix3qorrzujiwlvwkx6xrmsw	Block	2
37.142.246.25	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	2
77.127.210.79	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 77.127.210.79	Block	2

02-21-2016-16:04:08 to 02-21-2016-17:04:08