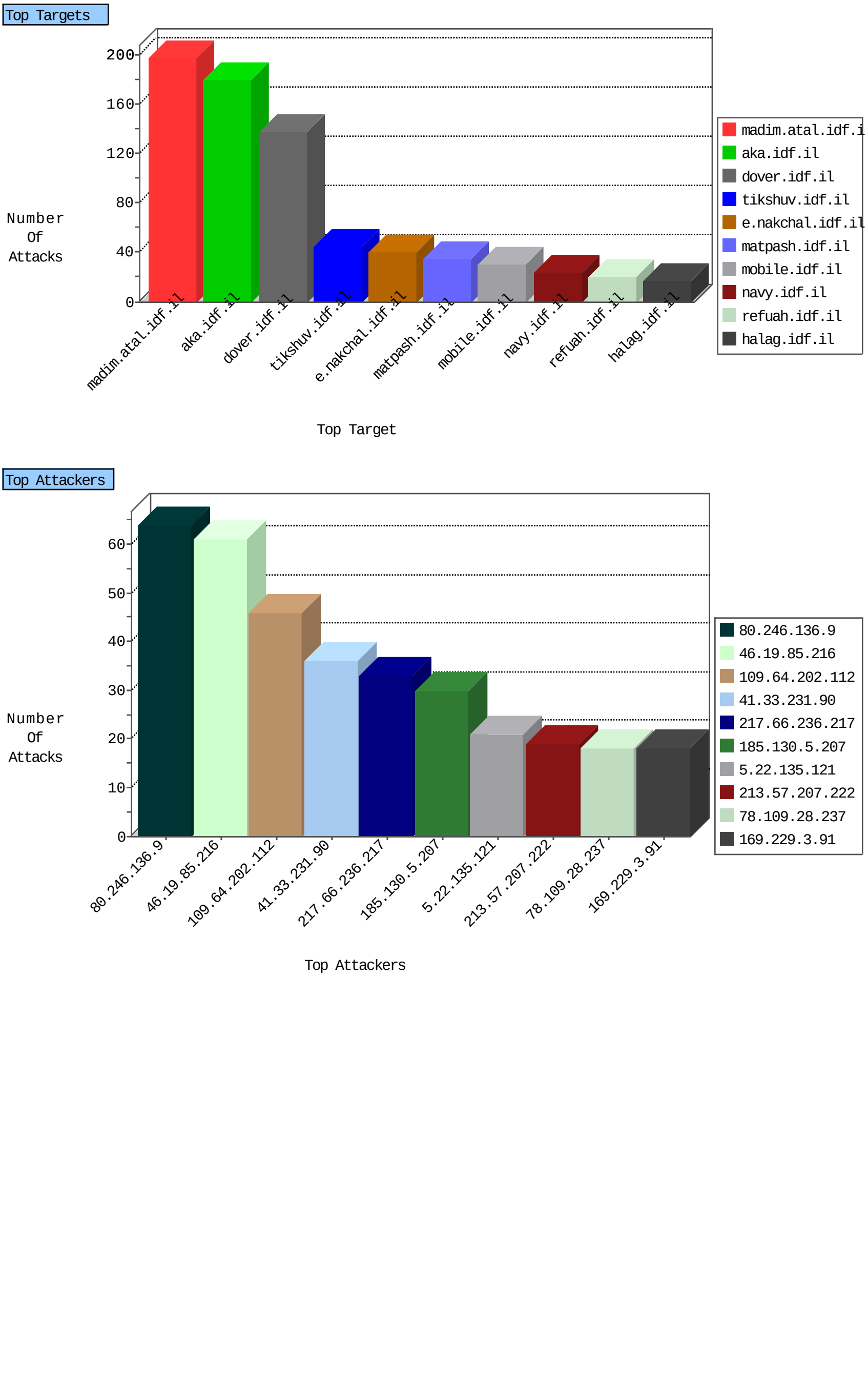
02-06-2016-14:04:02 to 02-06-2016-15:04:02

IDF Under Attack Daily Report



02-06-2016-14:04:02 to 02-06-2016-15:04:02

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	2
66.249.93.184	Israel	147.237.72.166	aka.idf.il	HTTP-Misc-BadBlue-Dir-Trave-2	dest-reset	1
217.127.127.69	Spain	147.237.76.39	mobile.meitav.idf.il	Block_Udp_All_Nets	drop	1
115.230.124.164	China	147.237.77.216	dover.idf.il	block-sp-traf1	drop	1
185.130.5.174		147.237.76.176	test.ncore.idf.il	Block_Udp_All_Nets	drop	1
217.127.127.69	Spain	147.237.76.38	e.e.meitav.idf.il	Block_Udp_All_Nets	drop	1

02-06-2016-14:04:02 to 02-06-2016-15:04:02

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

02-06-2016-14:04:02 to 02-06-2016-15:04:02

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
108.45.93.68	147.237.77.216	United States	dover.idf.il	ET SCAN Potential SSH Scan	4
66.249.79.41	147.237.77.170	United States	maarachot.idf.il	ET SCAN NMAP -sA (2)	2
46.45.137.67	147.237.77.176	Turkey	matpash.idf.il	ET SCAN NMAP -sS window 1024	1
183.60.48.25	147.237.76.177	China	ncore.idf.il	ET SCAN Potential SSH Scan	1
151.11.201.3	147.237.8.24	Italy	e.lifestyle.idf.il	ET SCAN NMAP -sS window 4096	1
121.201.27.61	147.237.76.42	China	refuah.idf.il	ET SCAN Potential SSH Scan	1
109.235.254.181	147.237.77.212	Turkey	e.dover.idf.il	ET SCAN NMAP -sS window 2048	1
46.45.137.67	147.237.77.233	Turkey	atal.idf.il	ET SCAN NMAP -sS window 1024	1
46.45.137.67	147.237.77.121	Turkey	e.navy.idf.il	ET SCAN NMAP -sS window 1024	1
209.126.116.147	147.237.76.34	United States	yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
183.60.48.25	147.237.76.197	China	e.himush.idf.il	ET SCAN Potential SSH Scan	1
176.58.109.251	147.237.77.226	United Kingdom	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 1024	1
151.11.201.3	147.237.8.24	Italy	e.lifestyle.idf.il	ET SCAN NMAP -sS window 1024	1
109.235.254.181	147.237.77.212	Turkey	e.dover.idf.il	ET SCAN NMAP -sS window 4096	1
109.235.254.181	147.237.77.212	Turkey	e.dover.idf.il	ET SCAN NMAP -f -sS	1

02-06-2016-14:04:02 to 02-06-2016-15:04:02

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
185.130.5.207		147.237.0.34	tikshuv.idf.il	drop	SAM rule	drop	30
5.22.135.121	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	21
213.57.207.222	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	19
78.109.28.237	Ukraine	147.237.76.199	e.nakchal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	18
41.77.138.90	Egypt	147.237.76.199	e.nakchal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	15
217.66.236.217	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	11
217.66.236.217	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	11
217.66.236.217	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	11
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
107.6.123.226	Singapore	147.237.76.199	e.nakchal.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	7
46.19.85.129	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
66.249.81.149	United States	147.237.77.234	halag.idf.il	drop	First packet isn't SYN	drop	7
109.253.145.88	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.0	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
31.210.187.160	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
79.182.165.169	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
77.127.209.155	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.98	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
66.249.81.157	United States	147.237.77.234	halag.idf.il	drop	First packet isn't SYN	drop	6
31.154.150.60	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.98	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
79.183.66.38	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
185.3.147.205	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
79.183.225.197	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
217.132.138.94	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
66.249.65.125	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
81.218.117.20	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
46.19.85.231	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
79.182.135.23	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
46.19.85.117	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
46.19.86.198	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.249.64.203	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
82.80.181.167	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
81.169.237.146	Germany	147.237.76.38	e.e.meitav.idf.il	drop	SAM rule	drop	3
46.19.85.26	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.27	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
66.249.81.153	United States	147.237.77.234	halag.idf.il	drop	First packet isn't SYN	drop	3
2.52.187.165	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.117	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
46.19.86.18	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
84.228.114.21	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.182.50.59	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.78	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.183.29.233	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
130.193.37.16	Russian Federation	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.64.57.240	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.20	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

02-06-2016-14:04:02 to 02-06-2016-15:04:02

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
80.246.136.9	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	64
46.19.85.216	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	61
109.64.202.112	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	46
46.19.86.84	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
192.243.55.131	Dominica	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.243.55.131	Block	4
46.19.86.0	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/nekudot/index	Block	3
46.19.86.18	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.85.82	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
85.64.1.97	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.8.220	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
192.243.55.138	Dominica	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.243.55.138	Block	2
5.29.93.171	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
216.104.160.77	United States	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 216.104.160.77	Block	2
84.108.182.222	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
2.52.33.231	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
151.227.25.244	United Kingdom	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-en/idfgdover.aspx	Block	2
5.28.153.215	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$35 in aka.idf.il/main/giyus/questionnaire.aspx	None	2
169.229.3.91	United States	147.237.0.34	tikshuv.idf.il	Illegal Byte Code Character in URL [[#24]]\9Â?iâ€	Block	1
41.236.204.17	Egypt	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/xmlrpc.php	Block	1
77.125.84.234	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
169.229.3.91	United States	147.237.77.19	law-forum.idf.il	Abnormally Long Request method	Block	1
157.55.39.100	United States	147.237.72.166	aka.idf.il	Unknown Parameter catid in aka.idf.il/main/smalim/faq.aspx	None	1
86.1.38.174	United Kingdom	147.237.77.74	law.idf.il	PHP Attempt	Block	1
176.58.109.251	United Kingdom	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to /	Block	1
62.90.167.180	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl38$ctl01$ctl03$cblQuestion$1 in www.aka.idf.il/main/giyus/questionnaire.aspx	None	1
169.229.3.91	United States	147.237.0.34	tikshuv.idf.il	Malformed URL [[#24]]\9Â?iâ€	Block	1
41.236.204.17	Egypt	147.237.77.170	maarachot.idf.il	PHP Attempt	Block	1
109.66.155.78	Israel	147.237.76.42	refuah.idf.il	Parameter Type Violation searchText in www.refua.atal.idf.il/1653-he/refuah.aspx	Block	1
192.243.55.138	Dominica	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/general.aspx?catid=58566&docid=35740	Block	1
169.229.3.91	United States	147.237.77.19	law-forum.idf.il	Illegal Byte Code Character in Method gÃ©1iÂ˜[[#22]]ÃŽÂ–Ã’cÃ’ÃŽ >`wy5'.Ã,[Â™Ã”6[[#12]] Ã‹ÂŽÂ•Ã¡Â‹Â?0S-vpm[[#27]]Ã¡Ã¥ÂžÃ¦f[[#14]]yfÃ,	Block	1
157.55.39.192	United States	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/	Block	1
5.29.187.130	Israel	147.237.76.86	navy.idf.il	PHP Attempt	Block	1
86.1.38.174	United Kingdom	147.237.77.74	law.idf.il	Unauthorized URL Access to www.law.idf.il/xmlrpc.php	Block	1
216.104.160.77	United States	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/wp-admin/	Block	1
184.105.247.196	United States	147.237.72.167	ishurim.aka.idf.il	Unauthorized URL Access to 147.237.72.167/	Block	1
66.249.65.88	Israel	147.237.76.200	eitan.aka.idf.il	Unknown Parameter tab in eitan.aka.idf.il/938-he/eitan.aspx	None	1
41.236.204.17	Egypt	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/xmlrpc.php	Block	1
169.229.3.91	United States	147.237.0.34	tikshuv.idf.il	Unknown HTTP Request Method ÂŒcÃ‘Â¤sÂœ.[Ã‡ Â¢I[[#25]]$zÂ¼[[#24]]Â„Ã‘SÃ¿[[#6]][[#8]]Â„9HÂ³Ã©1Â–Â¼[[#5]]Ã€J in URL [[#24]]\9Â?iâ€	Block	1
149.202.74.134	Germany	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/aman	Block	1
207.46.13.188	United States	147.237.72.166	aka.idf.il	Unknown Parameter catid in aka.idf.il/main/rabanut/general.aspx	None	1
169.229.3.91	United States	147.237.77.19	law-forum.idf.il	Illegal Byte Code Character in URL	Block	1
169.229.3.91	United States	147.237.0.34	tikshuv.idf.il	Abnormally Long Request method	Block	1
5.29.187.130	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/xmlrpc.php	Block	1
87.69.37.243	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$btnAtudaPrint in www.aka.idf.il/main/giyus/atuda/asmachta.aspx	None	1
185.3.147.205	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/apple-touch-icon-precomposed.png	Block	1
66.249.78.223	Israel	147.237.77.243	mobile.idf.il	Distributed Unauthorized URL Access on mobile.idf.il/nekudot/index	Block	1
169.229.3.91	United States	147.237.76.200	eitan.aka.idf.il	Illegal Byte Code Character in Method	Block	1
84.109.235.14	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl38$ctl01$ctl03$cblQuestion$6 in www.aka.idf.il/main/giyus/questionnaire.aspx	None	1
212.143.159.163	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$71 in aka.idf.il/main/giyus/questionnaire.aspx	None	1
169.229.3.91	United States	147.237.77.19	law-forum.idf.il	Unknown HTTP Request Method gÃ©1iÂ˜[[#22]]ÃŽÂ–Ã’cÃ’ ŽÃ>`wy5'.Ã,[Â™Ã”6[[#12]] Ã‹ÂŽÂ•Ã¡Â‹Â?0S-vpm[[#27]]Ã¡Ã¥ÂžÃ¦f[[#14]]yfÃ, in URL	Block	1

02-06-2016-14:04:02 to 02-06-2016-15:04:02