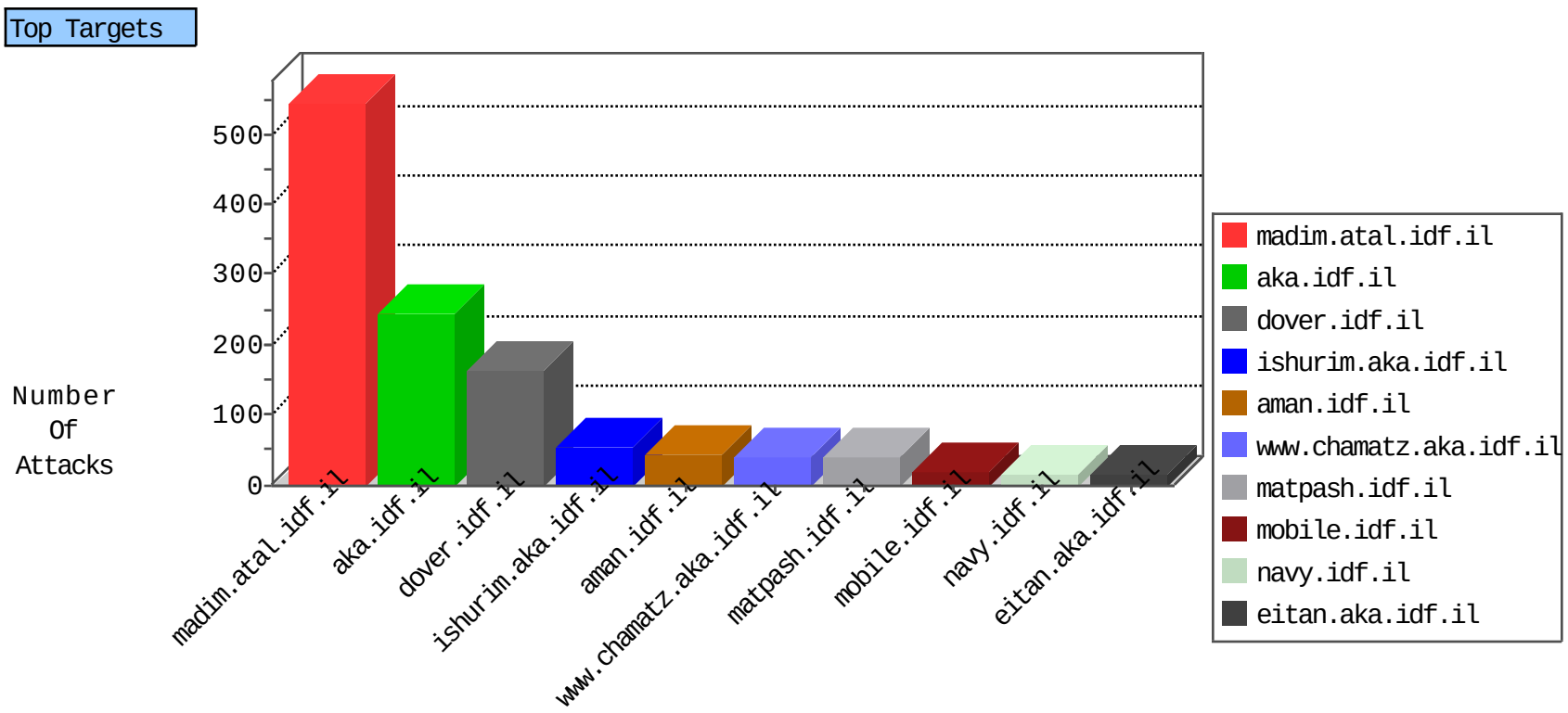
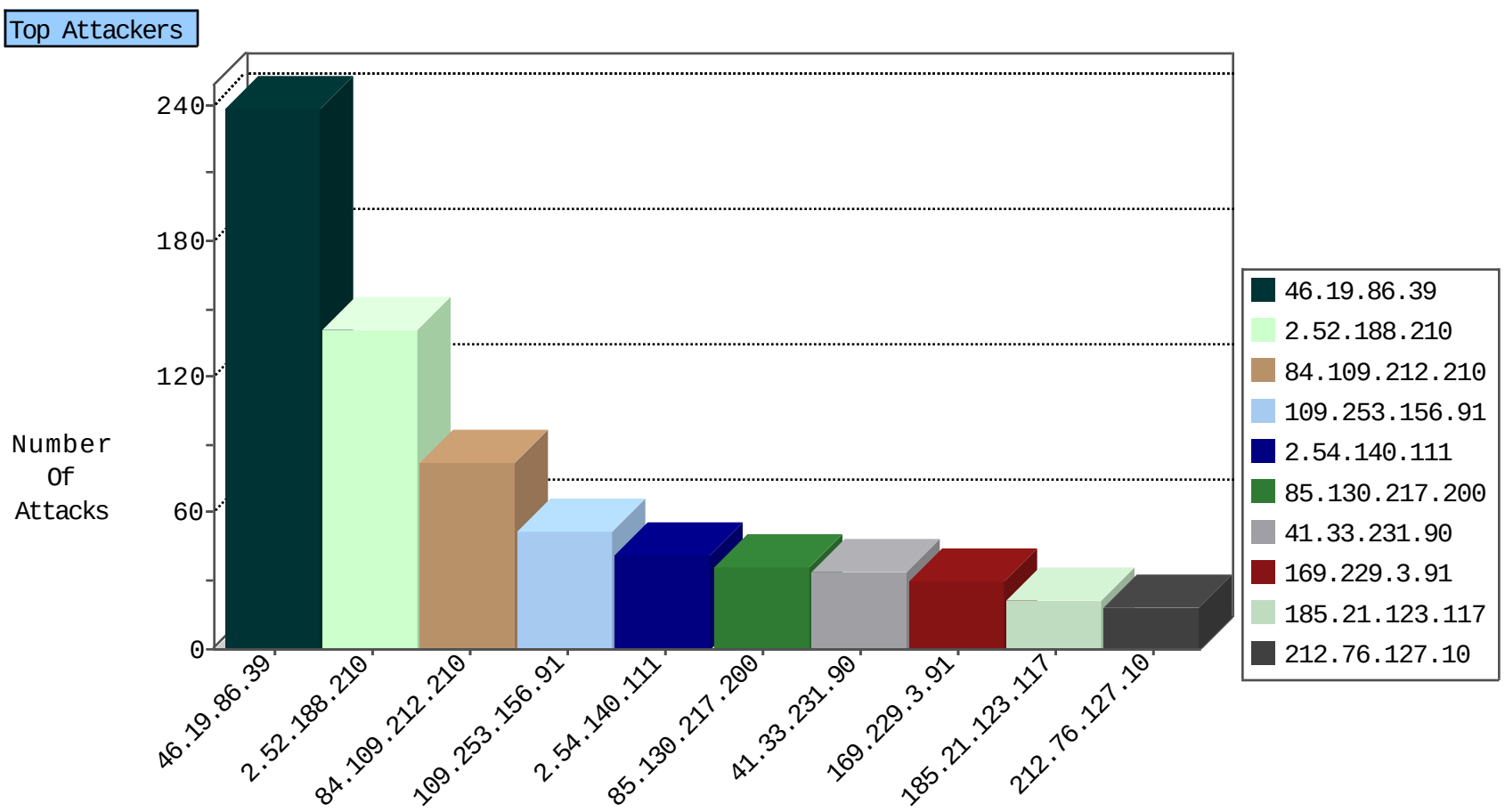
02-05-2016-11:04:00 to 02-05-2016-12:04:00

IDF Under Attack Daily Report

Top Targets



Top Attackers



02-05-2016-11:04:00 to 02-05-2016-12:04:00

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
66.249.78.146	Israel	147.237.72.166	aka.idf.il	TCP handshake violation, first packet not syn	drop	721
66.249.78.79	Israel	147.237.77.233	atal.idf.il	TCP handshake violation, first packet not syn	drop	716
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	10
37.8.86.185	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	6
79.180.52.13	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	6
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
104.207.128.23	United States	147.237.76.198	e.yohalan.idf.i	Block_Ntp_All_Net	drop	1
85.25.43.94	Germany	147.237.76.196	e.sviva.idf.il	Block_Udp_All_Nets	drop	1

02-05-2016-11:04:00 to 02-05-2016-12:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
86.193.37.134	France	147.237.72.166	aka.idf.il	C008: HTTP: Xenu UserAgent	Block	1
123.126.113.154	China	147.237.77.216	dover.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1

02-05-2016-11:04:00 to 02-05-2016-12:04:00

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
46.148.22.26	147.237.0.19	Lithuania	madim.atal.idf.il	ET SCAN Potential SSH Scan	1
125.212.232.144	147.237.77.205	Vietnam	prisha.idf.il	ET SCAN NMAP -sS window 4096	1
125.212.232.144	147.237.77.205	Vietnam	prisha.idf.il	ET SCAN NMAP -f -sS	1
93.104.213.84	147.237.8.45	Germany	e.eitan.idf.il	ET SCAN NMAP -sS window 1024	1
46.148.22.26	147.237.77.178	Lithuania	e.matpash.idf.il	ET SCAN Potential SSH Scan	1
46.148.22.26	147.237.76.177	Lithuania	ncore.idf.il	ET SCAN Potential SSH Scan	1
46.148.22.26	147.237.76.148	Lithuania	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
46.148.22.26	147.237.76.31	Lithuania	nakchal.idf.il	ET SCAN Potential SSH Scan	1
187.252.145.28	147.237.76.34	Mexico	yohalan.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
125.212.232.144	147.237.77.205	Vietnam	prisha.idf.il	ET SCAN NMAP -sS window 2048	1
104.214.148.178	147.237.77.205	United States	prisha.idf.il	ET SCAN NMAP -sS window 1024	1
91.201.236.114	147.237.8.24	Ukraine	e.lifestyle.idf.il	ET SCAN NMAP -sS window 1024	1
46.148.22.26	147.237.77.226	Lithuania	www.chamatz.aka.idf.il	ET SCAN Potential SSH Scan	1
46.148.22.26	147.237.77.61	Lithuania	e.cogat.idf.il	ET SCAN Potential SSH Scan	1
46.148.22.26	147.237.76.176	Lithuania	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
216.58.29.110	147.237.76.31	Canada	nakchal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
46.148.22.26	147.237.76.86	Lithuania	navy.idf.il	ET SCAN Potential SSH Scan	1
189.218.208.228	147.237.76.34	Mexico	yohalan.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1

02-05-2016-11:04:00 to 02-05-2016-12:04:00

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
85.130.217.200	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	34
185.21.123.117	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	21
212.76.127.10	Israel	147.237.77.226	www.chamatz.aka.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	18
31.168.149.92	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid sequence number	monitor	12
66.249.78.170	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
46.19.85.68	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
2.54.140.111	Israel	147.237.72.166	aka.idf.il	SYN Attack		reject	9
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
2.52.133.254	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
212.76.127.44	Israel	147.237.77.226	www.chamatz.aka.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	9
212.76.127.111	Israel	147.237.77.226	www.chamatz.aka.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	9
2.54.140.111	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
2.54.140.111	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	8
2.54.140.111	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
46.19.85.163	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
2.54.140.111	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
46.19.85.163	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
81.199.120.138	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
2.54.140.111	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
84.94.155.121	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
80.246.136.17	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
46.19.85.140	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
84.228.5.101	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.22	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
79.176.168.197	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.140	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.22	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
54.244.22.103	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	6
2.54.58.123	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
5.28.178.193	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.137	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	5
94.230.86.215	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
84.111.36.36	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	5
82.80.17.163	Israel	147.237.72.166	aka.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
31.210.188.32	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
94.230.86.189	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
66.249.65.122	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
46.19.85.255	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
31.210.187.124	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
212.179.215.152	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.1	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.183.52.37	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.159	Israel	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
87.68.149.229	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	3
109.253.159.252	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
212.76.127.219	Israel	147.237.77.226	www.chamatz.aka.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	3
77.127.217.211	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
212.179.215.152	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
82.80.17.163	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	3

02-05-2016-11:04:00 to 02-05-2016-12:04:00

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.86.39	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	135
46.19.86.39	Israel	147.237.0.19	madim.atal.idf.il	Too Many of the Same Response Code (404) in Session from 46.19.86.39	Block	103
2.52.188.210	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	90
84.109.212.210	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	82
109.253.156.91	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	52
2.52.188.210	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	51
5.22.131.51	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
109.253.135.7	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	4
79.181.22.248	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/controls/atuda/Â	Block	3
213.251.182.103	France	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/0/size220x0/3410.jpg.src	Block	3
79.181.101.85	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.54.28.197	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
84.228.15.52	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/modiin/undefined	Block	3
217.132.152.111	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
85.64.217.92	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
101.200.204.198	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/atom	Block	2
182.92.7.12	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/rss/	Block	2
192.243.55.138	Dominica	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/giyus/kadatz	Block	2
192.243.55.138	Dominica	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.243.55.138	Block	2
2.54.128.170	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
109.253.140.116	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
84.109.126.100	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
192.243.55.135	Dominica	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 192.243.55.135	Block	2
101.200.204.113	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/feed	Block	2
169.229.3.91	United States	147.237.77.233	atal.idf.il	Illegal HTTP Version	Block	1
169.229.3.91	United States	147.237.77.176	matpash.idf.il	Abnormally Long Request method	Block	1
213.8.24.68	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1134-he/atal.aspx	Block	1
66.249.78.95	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-he/dover.aspx	Block	1
192.243.55.132	Dominica	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/eitan/pratim/pirteyerua	Block	1
46.19.86.61	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl02$ctl03$txtField in aka.idf.il/main/giyus/questionnaire.aspx	None	1
169.229.3.91	United States	147.237.77.235	sviva.idf.il	Multiple Abnormally Long Request from 169.229.3.91	Block	1
94.230.86.215	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$39 in aka.idf.il/main/giyus/questionnaire.aspx	None	1
218.25.89.100	China	147.237.0.17	m.my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.17/adminmanager!login	Block	1
169.229.3.91	United States	147.237.77.233	atal.idf.il	Illegal Byte Code Character in Header Name aÂ?Ã«EÃš[[#2]]Âµ*Â-Ãƒ Ã«xejÃŒ	Block	1
169.229.3.91	United States	147.237.76.42	refuah.idf.il	Illegal Byte Code Character in Header Value	Block	1
77.127.217.211	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/guyus	Block	1
192.243.55.137	Dominica	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/general.aspx?catid=58339&docid=68498	Block	1
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.64.233	Block	1
5.29.145.209	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
169.229.3.91	United States	147.237.77.233	atal.idf.il	Malformed URL Â¼{s[[#7]]×,Â¬yÃ·Â¨+â€˜[[#12]]$Âœ×ƒx×¢$â€ ºÂ·×¦â,¬Æ’	Block	1
85.65.200.154	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/sip_storage/files/8/1668.doc	Block	1
169.229.3.91	United States	147.237.77.176	matpash.idf.il	Illegal Byte Code Character in Method Ã”j[[#31]]VÃ?ÃšÃ‘ a[[#17]]TTZ+Â•Ã Â©Â£:Âº[[#12]]Â”Â¨K	Block	1
66.249.78.96	Israel	147.237.77.74	law.idf.il	Distributed Illegal Parameter Encoding	None	1
192.243.55.133	Dominica	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/giyus/kadatz	Block	1
128.232.110.28	United Kingdom	147.237.77.176	matpash.idf.il	Unauthorized URL Access to 147.237.77.176/	Block	1
94.230.86.215	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$82 in aka.idf.il/main/giyus/questionnaire.aspx	None	1
46.19.86.172	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
169.229.3.91	United States	147.237.77.235	sviva.idf.il	Multiple Illegal Byte Code Character in Header Name from 169.229.3.91	Block	1
84.110.35.243	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/https:/www.idf.il/	Block	1
218.25.89.100	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/adminmanager!login	Block	1

02-05-2016-11:04:00 to 02-05-2016-12:04:00