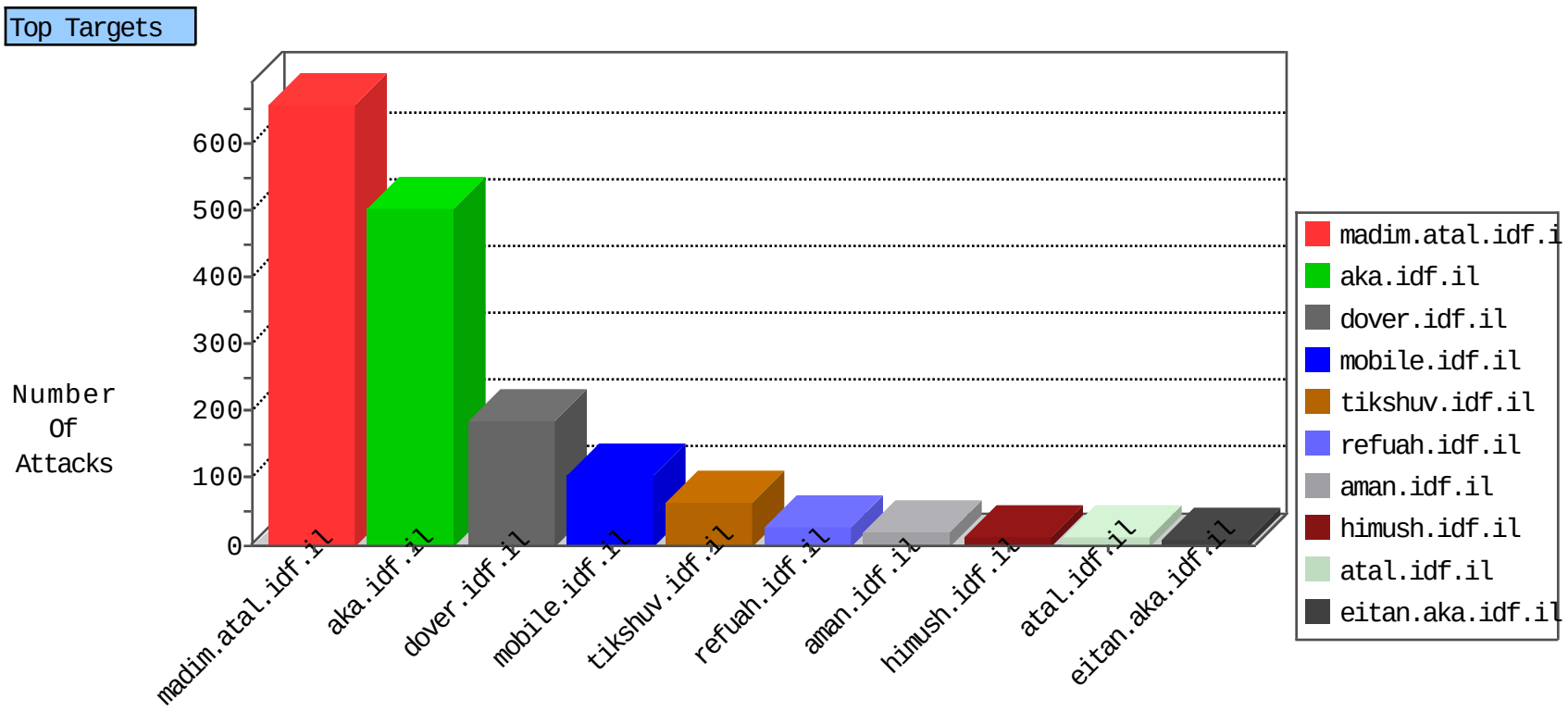
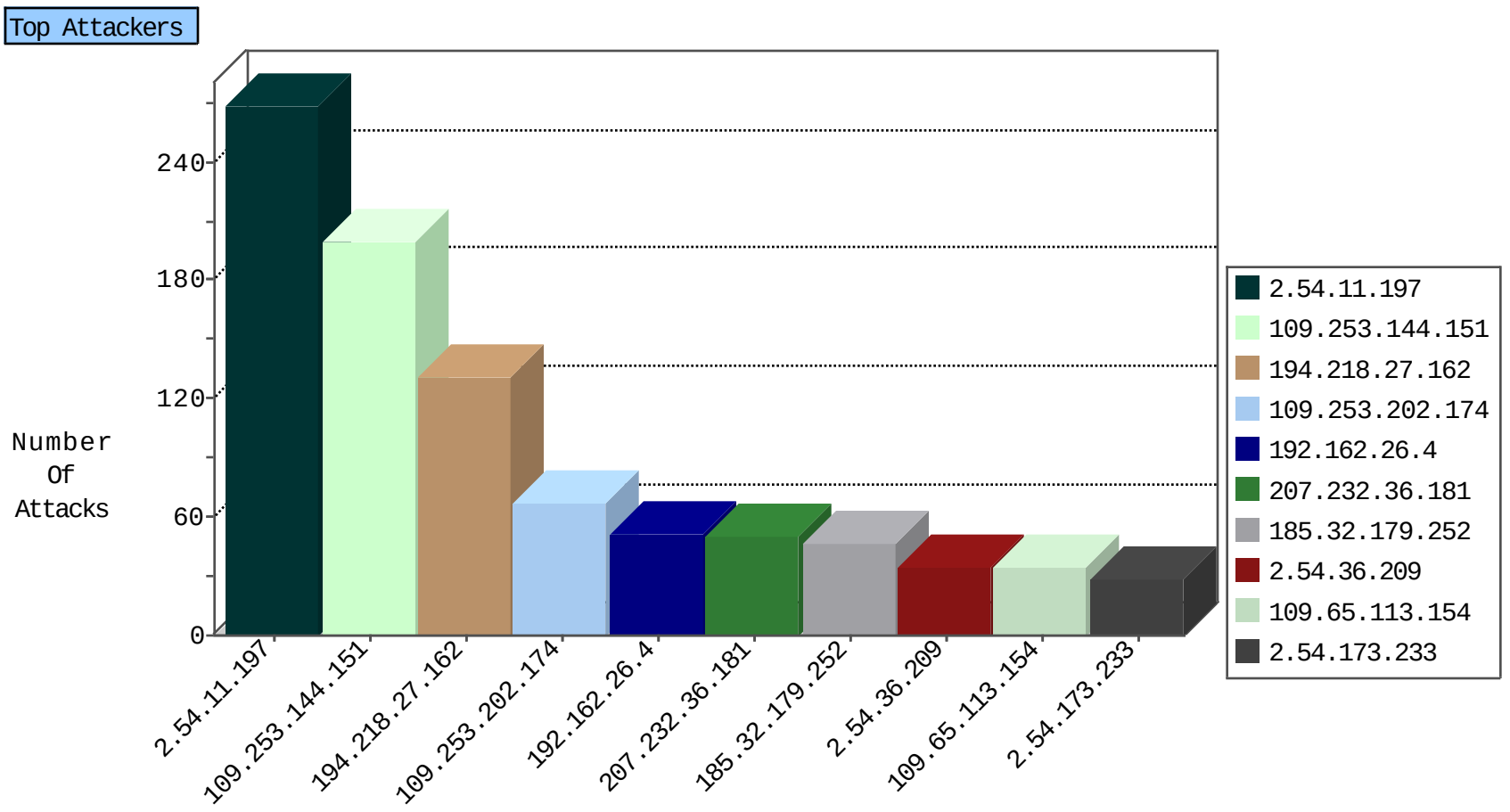
03-02-2016-12:04:00 to 03-02-2016-13:04:00

IDF Under Attack Daily Report

Top Targets



Top Attackers



03-02-2016-12:04:00 to 03-02-2016-13:04:00

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
207.232.36.181	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	412
81.218.56.245	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	2
184.105.247.227	United States	147.237.77.243	mobile.idf.il	Block_Udp_All_Nets	drop	1
192.99.63.194	Canada	147.237.76.147	chinuch.aka.idf.il	Block_Ntp_All_Net	drop	1
185.94.111.1		147.237.8.24	e.lifestyle.idf.il	Block_Udp_All_Nets	drop	1
104.148.100.2	United States	147.237.0.35	akaws.idf.il	Block_Udp_All_Nets	drop	1
185.94.111.1		147.237.76.38	e.e.meitav.idf.il	Block_Udp_All_Nets	drop	1
164.132.54.194	Italy	147.237.77.19	law-forum.idf.il	Block_Ntp_All_Net	drop	1
185.94.111.1		147.237.76.44	e.refuah.idf.il	Block_Udp_All_Nets	drop	1
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1

03-02-2016-12:04:00 to 03-02-2016-13:04:00

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.179.128.52	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	12
46.19.86.193	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	9
147.236.31.231	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	7
46.117.233.31	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
79.176.80.248	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
147.234.241.19	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
51.255.65.85	United Kingdom	147.237.77.233	atal.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
192.116.55.245	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
51.255.65.28	United Kingdom	147.237.77.233	atal.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
51.255.65.31	United Kingdom	147.237.77.233	atal.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1
123.126.113.80	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
31.3.74.26	Denmark	147.237.77.216	dover.idf.il	C1000008: HTTP: Xenu UserAgent	Block	1
51.255.65.43	United Kingdom	147.237.77.233	atal.idf.il	C1000146: HTTP: AhrefBot crawler	Block	1

03-02-2016-12:04:00 to 03-02-2016-13:04:00

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
109.235.254.181	147.237.8.46	Turkey	e.chinuch.idf.il	ET SCAN NMAP -sS window 1024	1
109.67.123.106	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
85.64.242.247	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
82.166.16.174	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
218.246.0.97	147.237.8.46	China	e.chinuch.idf.il	ET SCAN NMAP -sS window 1024	1
82.80.196.44	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
209.126.116.147	147.237.76.177	United States	ncore.idf.il	ET SCAN NMAP -sS window 1024	1
66.249.93.103	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
193.105.134.220	147.237.0.34	Sweden	tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
62.219.144.41	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
192.198.151.44	147.237.77.216	Europe	dover.idf.il	portscan: TCP Distributed Portscan	1
5.29.185.180	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
185.120.125.1	147.237.77.216		dover.idf.il	portscan: TCP Distributed Portscan	1
109.81.209.151	147.237.77.216	Czech Republic	dover.idf.il	portscan: TCP Distributed Portscan	1
91.201.236.114	147.237.0.19	Ukraine	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
84.108.116.182	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
82.81.21.68	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
213.151.47.45	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
81.218.153.166	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
199.203.62.54	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
66.249.78.146	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	1
193.105.134.220	147.237.0.16	Sweden	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
37.26.147.227	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
187.58.224.213	147.237.72.166	Brazil	aka.idf.il	ET SCAN NMAP -sS window 4096	1

03-02-2016-12:04:00 to 03-02-2016-13:04:00

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
194.218.27.162	Sweden	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	84
194.218.27.162	Sweden	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	44
185.32.179.252	Israel	147.237.77.243	mobile.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	23
5.22.135.136	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
109.253.131.74	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
176.13.3.212	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
87.71.110.38	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	12
62.0.200.166	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	10
2.54.173.233	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
213.244.118.251	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
212.179.218.166	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	7
109.253.203.74	Israel	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
109.253.203.74	Israel	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
176.13.16.59	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.3.102	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
46.19.86.193	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
2.54.148.237	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.183	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
62.0.200.166	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
46.19.86.193	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.197	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
87.71.43.23	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
84.110.36.155	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.67.172.35	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.6	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.197	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
185.27.106.70	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.173.233	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.234	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
46.19.85.183	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
212.179.218.166	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
89.138.83.19	Israel	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
82.80.196.44	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
2.54.173.233	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
82.166.130.213	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
2.54.173.233	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	4
79.183.175.146	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
46.19.85.234	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
195.60.232.57	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
2.54.173.233	Israel	147.237.77.216	dover.idf.il	SYN Attack		reject	4
213.244.118.251	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
79.183.175.146	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
2.52.32.175	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
79.180.251.139	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
5.22.129.244	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
37.46.38.217	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
46.19.86.243	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.178.48.1	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.205	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.54.11.197	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	269
109.253.144.151	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	200
109.253.202.174	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	67
2.54.36.209	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	35
109.65.113.154	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	34
176.13.6.110	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	18
46.19.86.115	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	12
66.249.66.25	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 66.249.66.25	Block	12
185.32.179.252	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	7
46.121.123.29	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 46.121.123.29	Block	5
109.253.131.74	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	4
192.162.26.4	Spain	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in Method from 192.162.26.4	Block	4
2.54.54.107	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	4
185.32.179.252	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
192.162.26.4	Spain	147.237.72.166	aka.idf.il	Multiple Unknown HTTP Request Method from 192.162.26.4	Block	3
2.54.142.80	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1362	Block	3
176.13.10.60	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
192.162.26.4	Spain	147.237.72.166	aka.idf.il	Multiple Malformed URL from 192.162.26.4	Block	3
192.162.26.4	Spain	147.237.72.166	aka.idf.il	Multiple Abnormally Long Request from 192.162.26.4	Block	3
46.19.85.25	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
2.52.2.99	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
79.176.81.128	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 79.176.81.128	Block	3
192.162.26.4	Spain	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in Header Name from 192.162.26.4	Block	3
2.54.142.80	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 2.54.142.80	Block	3
131.253.25.229	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	3
82.213.48.43	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/6/4616.jpg	Block	2
192.162.26.4	Spain	147.237.72.166	aka.idf.il	Multiple Malformed HTTP Header Line from 192.162.26.4	Block	2
192.162.26.4	Spain	147.237.72.166	aka.idf.il	Multiple Abnormally Long Header Line from 192.162.26.4	Block	2
176.13.16.59	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
109.253.194.132	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
176.13.19.151	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
192.162.26.4	Spain	147.237.72.166	aka.idf.il	Multiple NULL Character in Header Name from 192.162.26.4	Block	2
94.199.151.22	United Kingdom	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 94.199.151.22	Block	2
176.13.3.212	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
192.162.26.4	Spain	147.237.72.166	aka.idf.il	Multiple NULL Character in Method from 192.162.26.4	Block	2
79.176.81.128	Israel	147.237.72.166	aka.idf.il	PHP Attempt	Block	2
105.106.175.182	Algeria	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	2
80.246.139.193	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
192.162.26.4	Spain	147.237.72.166	aka.idf.il	Multiple Illegal HTTP Version from 192.162.26.4	Block	2
169.229.3.91	United States	147.237.76.42	refuah.idf.il	Multiple NULL Character in Url from 169.229.3.91	Block	1
66.249.66.176	United States	147.237.77.74	law.idf.il	Unauthorized URL Access to 147.237.77.74/robots.txt	Block	1
192.162.26.4	Spain	147.237.72.166	aka.idf.il	Malformed URL [[Ɔ#2[[£]]#0ˆ©s]]11#[[9j]zf]]Ɔ€[[42#]]°ɲp|xŸ[[#31]]d¸[[#7]]~:®',¼¥¸qא–¾'xf¼v•€ע³צ068[[•#26:»¯Ž]]¦£¸t.!Ÿ[[#6]]—ח5@Û•••ɳŸ|q#cʊצ¸[[03#]]'דצו¨•'[[03#]]—′¸6210#×[[42#]]os§ע′pŒ¹Ú¯q¨pÝ¸q'']]#15[[ת~…'@c¸©)ı•Üižy┐¯a¿ɳ<Šfž±Œon››]]#16[[]]#6[[·ʊ¥[[[#17]]	Block	1
207.46.13.22	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 207.46.13.22	Block	1
62.219.35.179	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/templates/templatecontrols/generic/	Block	1
192.162.26.4	Spain	147.237.72.166	aka.idf.il	Illegal Byte Code Character in Header Name k¬[[#17]],§JgWñ[[#2]]víÓ§·†2_[[#29]]…zmv¶•¶"uI7ÌxIŽ¥<DS[[#17]]+´ÝEd?E,[[#22]]k4J±§æ87Ù*%[[#12]]½w[[#23]]Z#011Â\Ø–¤bËniÜÉæº ï,[[#3]]BN%\wQ{ç[[#18]]i°[[#18]]=bôŽõc_	Block	1
37.142.64.11	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl55 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
88.249.31.184	Turkey	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/arr/	Block	1
169.229.3.91	United States	147.237.77.234	halag.idf.il	Multiple Unknown HTTP Request Method from 169.229.3.91	Block	1
79.176.81.128	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/ajax/updatestatus.php	Block	1
66.249.66.37	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1065-he/dover.aspx	Block	1