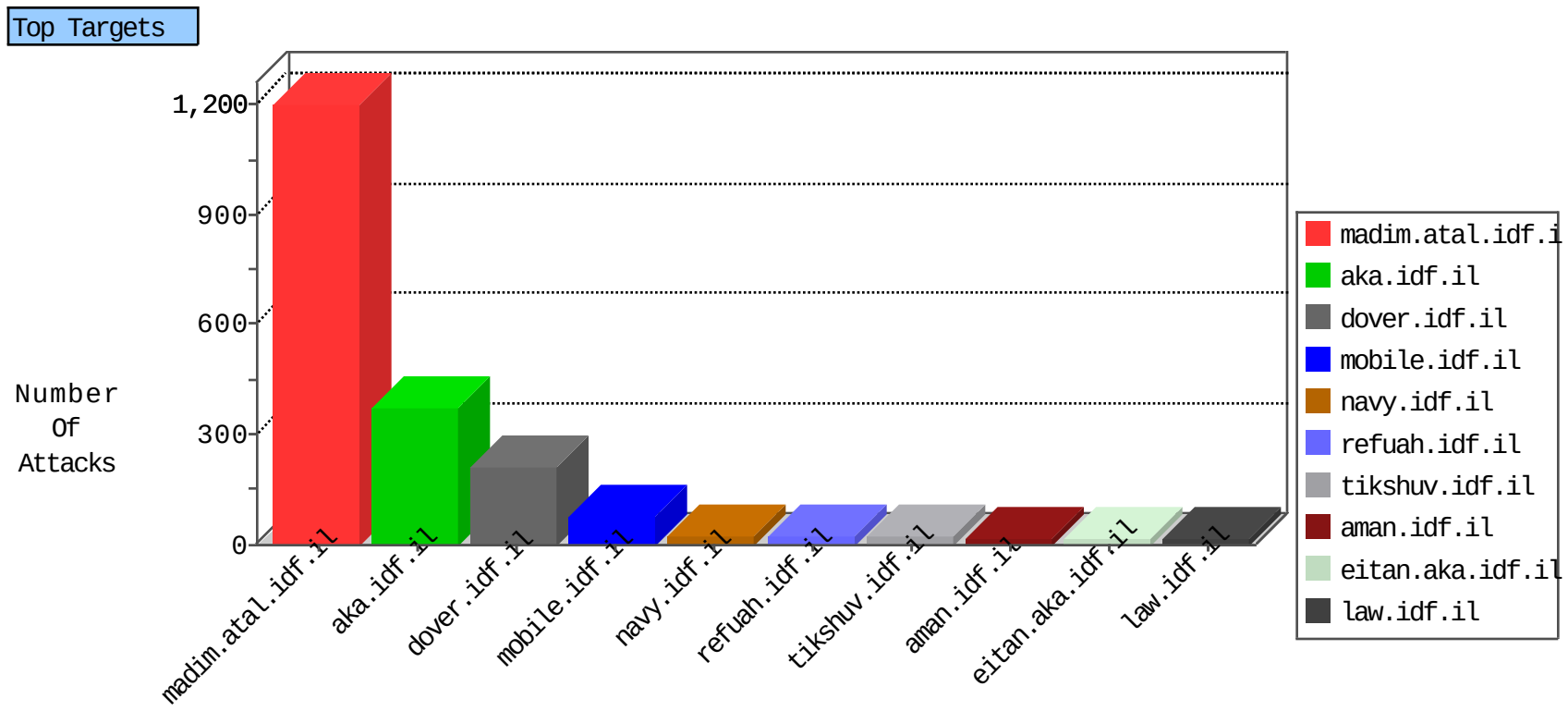
02-04-2016-11:04:03 to 02-04-2016-12:04:03

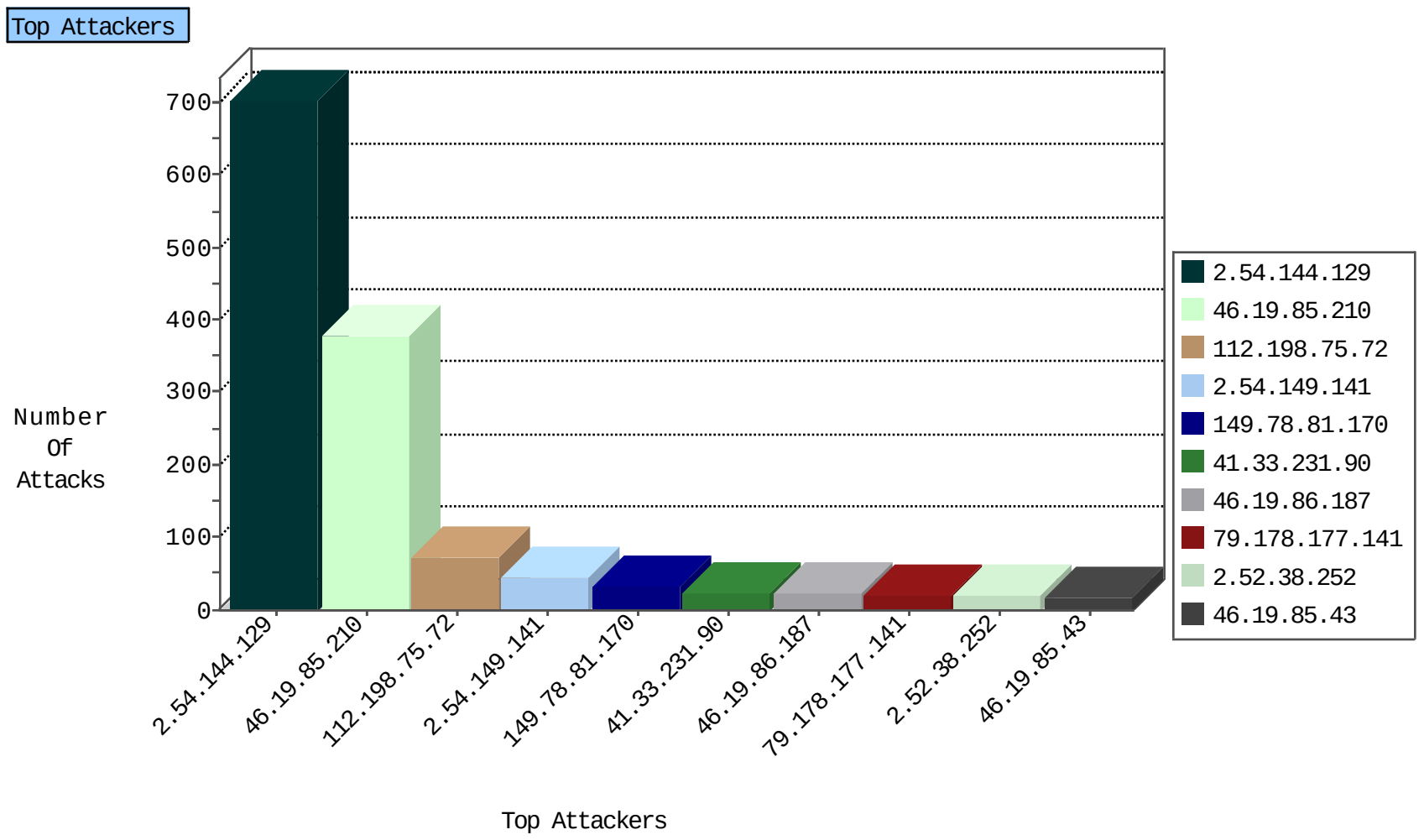
IDF Under Attack Daily Report

Top Targets



Top Target

Top Attackers



Top Attackers

02-04-2016-11:04:03 to 02-04-2016-12:04:03

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
130.190.65.20	France	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	4
79.176.4.158	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
113.171.23.126	Vietnam	147.237.77.233	atal.idf.il	Frk_Under_Attack_Con_Tcp	drop	2
115.230.124.164	China	147.237.0.34	tikshuv.idf.il	Frk_Under_Attack_Con_Tcp	drop	2
82.81.37.46	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	2
115.230.124.164	China	147.237.77.216	dover.idf.il	block-sp-traf1	drop	1
110.9.17.57	Korea, Republic of	147.237.76.86	navy.idf.il	Block_Udp_All_Nets	drop	1
64.246.161.42	United States	147.237.0.15	kosher-kravi.idf.il	block-sp-traf1	drop	1
212.179.73.146	Israel	147.237.77.176	matpash.idf.il	Block_Udp_All_Nets	drop	1
212.179.73.146	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1

02-04-2016-11:04:03 to 02-04-2016-12:04:03

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
52.26.202.58	United States	147.237.77.74	law.idf.il	22280: HTTP: Joomla Object Injection Vulnerability	Block	1
89.216.115.6		147.237.77.216	dover.idf.i	17272: HTTP: Suspicious User-Agent (WindowsNT) With No Separating Space	Block	1
163.172.13.119	United Kingdom	147.237.77.216	dover.idf.i	C106: HTTP: majestic bot	Block	1

02-04-2016-11:04:03 to 02-04-2016-12:04:03

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
94.230.93.140	147.237.72.156	Israel	aman.idf.il	ET SCAN NMAP -sA (2)	2
212.179.21.194	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	2
59.45.79.117	147.237.77.74	China	law.idf.il	ET SCAN Potential SSH Scan	1
176.13.16.16	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
59.45.79.117	147.237.0.34	China	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
128.139.19.182	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.19.85.250	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
114.112.90.54	147.237.77.170	China	maarachot.idf.il	ET SCAN NMAP -sS window 1024	1
109.66.206.35	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
218.246.0.97	147.237.76.202	China	e.halag.idf.il	ET SCAN NMAP -sS window 1024	1
213.8.90.204	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
82.166.247.138	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
209.126.116.147	147.237.0.19	United States	madim.atal.idf.il	ET SCAN NMAP -sS window 1024	1
66.249.78.96	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sA (2)	1
185.27.105.73	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
62.90.235.151	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
179.43.141.234	147.237.76.39	Switzerland	mobile.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
59.45.79.117	147.237.8.46	China	e.chinuch.idf.il	ET SCAN Potential SSH Scan	1
132.73.199.179	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.19.86.171	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
125.212.232.144	147.237.77.235	Vietnam	sviva.idf.il	ET SCAN NMAP -sS window 1024	1
113.171.23.126	147.237.77.227	Vietnam	e.hamaz.idf.il	ET SCAN Potential SSH Scan	1
222.165.225.59	147.237.77.212	Indonesia	e.dover.idf.il	ET SCAN NMAP -sS window 3072	1
109.64.135.92	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
213.8.240.83	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
89.139.171.249	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
81.180.66.34	147.237.72.166	Moldova, Republic of	aka.idf.il	portscan: TCP Distributed Portscan	1
195.160.242.40	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
66.249.64.50	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	1
179.43.141.234	147.237.77.170	Switzerland	maarachot.idf.il	ET SCAN NMAP -sS window 1024	1

02-04-2016-11:04:03 to 02-04-2016-12:04:03

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	24
217.194.193.245	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
112.198.75.72	Philippines	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	17
2.54.57.132	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	14
46.117.116.155	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	13
109.64.56.64	Israel	147.237.76.200	eitan.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
141.0.12.85	Norway	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	10
81.218.141.178	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.85.43	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
176.13.16.76	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
2.54.130.100	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
37.26.148.144	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
2.54.159.91	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
2.54.48.176	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.28	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.85.28	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
176.13.20.125	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.62	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.43	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
2.54.159.91	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.250	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
37.46.39.137	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
213.57.119.122	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.250	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
217.132.5.126	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.94	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.181.174.62	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.215	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	5
84.108.119.196	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
2.52.38.252	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
149.78.235.82	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	4
2.52.38.252	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	4
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
2.54.58.67	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
84.108.119.196	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
212.179.212.111	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
199.203.215.1	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
2.54.58.67	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
2.52.38.252	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
46.19.86.75	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
2.52.38.252	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
80.246.138.137	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
81.218.57.61	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
37.46.39.137	Israel	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
37.26.148.219	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
82.166.77.241	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
37.46.38.3	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
79.177.21.232	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
62.219.253.242	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

02-04-2016-11:04:03 to 02-04-2016-12:04:03

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.54.144.129	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	416
2.54.144.129	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	228
46.19.85.210	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	194
46.19.85.210	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	114
46.19.85.210	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (403)	Block	70
2.54.149.141	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	44
2.54.144.129	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (403)	Block	36
2.54.144.129	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (403) in Session from 2.54.144.129	Block	24
46.19.86.187	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	22
149.78.81.170	Israel	147.237.77.243	mobile.idf.il	Multiple Unauthorized URL Access from 149.78.81.170	Block	19
109.253.213.170	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	18
149.78.81.170	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/categorytemplates/listchilddocuments/1362	Block	15
109.65.124.25	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	12
79.183.36.161	Israel	147.237.0.34	tikshuv.idf.il	Distributed Too Many of the Same Response Code (404)	Block	10
216.72.40.185	Israel	147.237.0.34	tikshuv.idf.il	Too Many of the Same Response Code (404) in Session from 216.72.40.185	Block	5
147.251.43.64	Czech Republic	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 147.251.43.64	Block	5
112.198.75.72	Philippines	147.237.72.166	aka.idf.il	Multiple Abnormally Long Request from 112.198.75.72	Block	4
112.198.75.72	Philippines	147.237.72.166	aka.idf.il	Multiple Unknown HTTP Request Method from 112.198.75.72	Block	4
79.178.177.141	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in Method	Block	4
112.198.75.72	Philippines	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in Method from 112.198.75.72	Block	4
112.198.75.72	Philippines	147.237.72.166	aka.idf.il	Multiple Malformed URL from 112.198.75.72	Block	3
112.198.75.72	Philippines	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in Header Name from 112.198.75.72	Block	3
46.19.85.43	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
109.253.197.163	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
112.198.75.72	Philippines	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in URL from 112.198.75.72	Block	3
62.0.10.250	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 62.0.10.250	Block	3
112.198.75.72	Philippines	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in Header Value from 112.198.75.72	Block	3
2.54.138.165	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
109.253.128.205	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
79.178.177.141	Israel	147.237.72.166	aka.idf.il	Distributed Abnormally Long Request	Block	2
84.229.150.146	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
112.198.75.72	Philippines	147.237.72.166	aka.idf.il	Multiple NULL Character in Header Name from 112.198.75.72	Block	2
79.178.177.141	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in Header Name	Block	2
2.54.130.100	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
46.19.85.239	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
79.178.177.141	Israel	147.237.72.166	aka.idf.il	Distributed NULL Character in Method	Block	2
109.253.202.246	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
112.198.75.72	Philippines	147.237.72.166	aka.idf.il	Multiple Illegal HTTP Version from 112.198.75.72	Block	2
79.178.177.141	Israel	147.237.72.166	aka.idf.il	Distributed Unknown HTTP Request Method	Block	2
79.178.177.141	Israel	147.237.72.166	aka.idf.il	Distributed Malformed HTTP Header Line	Block	2
112.198.75.72	Philippines	147.237.72.166	aka.idf.il	Multiple Malformed HTTP Header Line from 112.198.75.72	Block	2
176.13.4.215	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
112.198.75.72	Philippines	147.237.72.166	aka.idf.il	Multiple Abnormally Long Header Line from 112.198.75.72	Block	2
37.26.146.247	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
79.178.177.141	Israel	147.237.72.166	aka.idf.il	Distributed Malformed URL	Block	2
77.127.205.52	Israel	147.237.76.86	navy.idf.il	PHP Attempt	Block	1
97.74.215.183	United States	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to eitan.aka.idf.il/test/wp-admin/	Block	1
212.25.84.200	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/894-en/idfgdover.aspx	Block	1
84.109.192.142	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$2 in aka.idf.il/main/giyus/questionnaire.aspx	None	1
176.13.16.76	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1

02-04-2016-11:04:03 to 02-04-2016-12:04:03