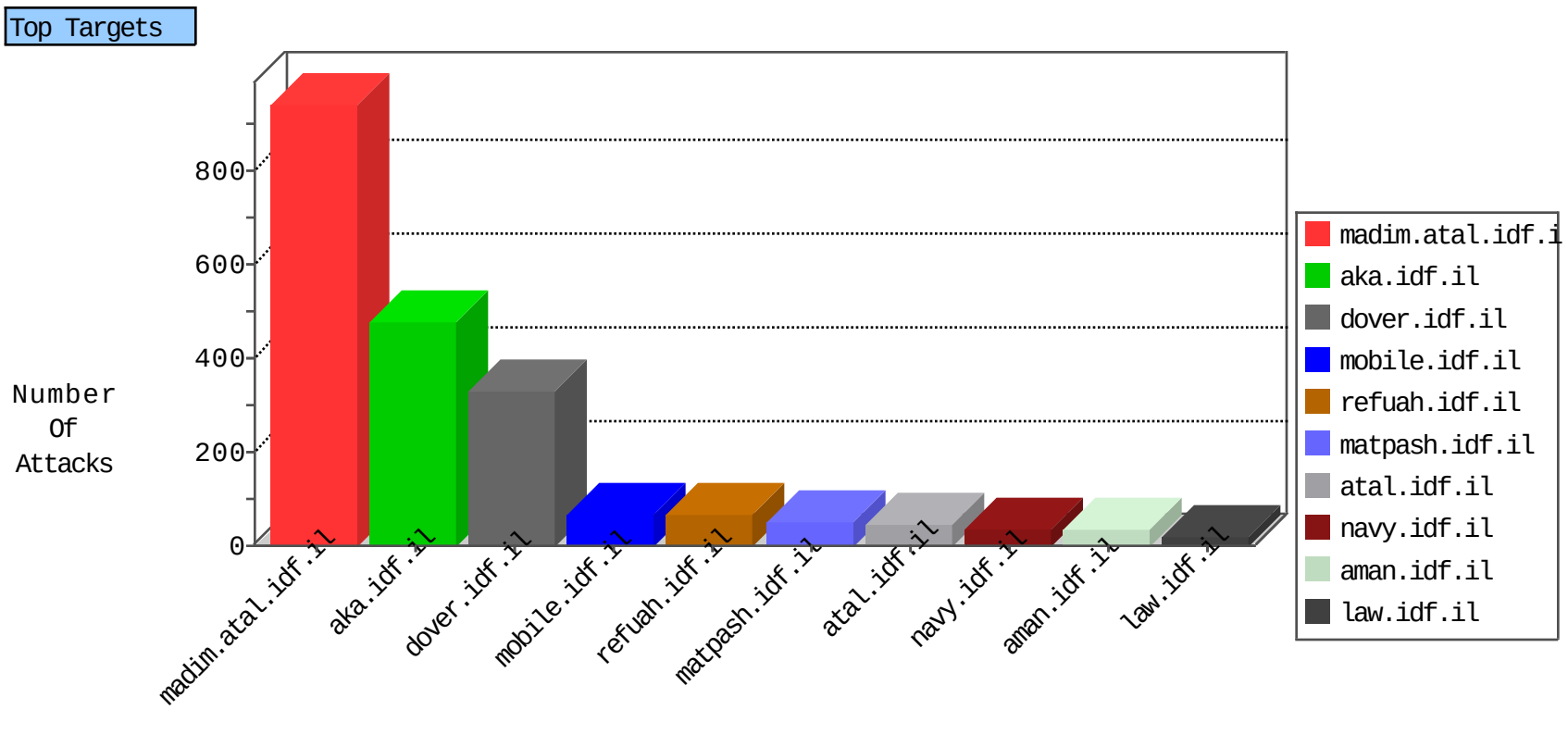
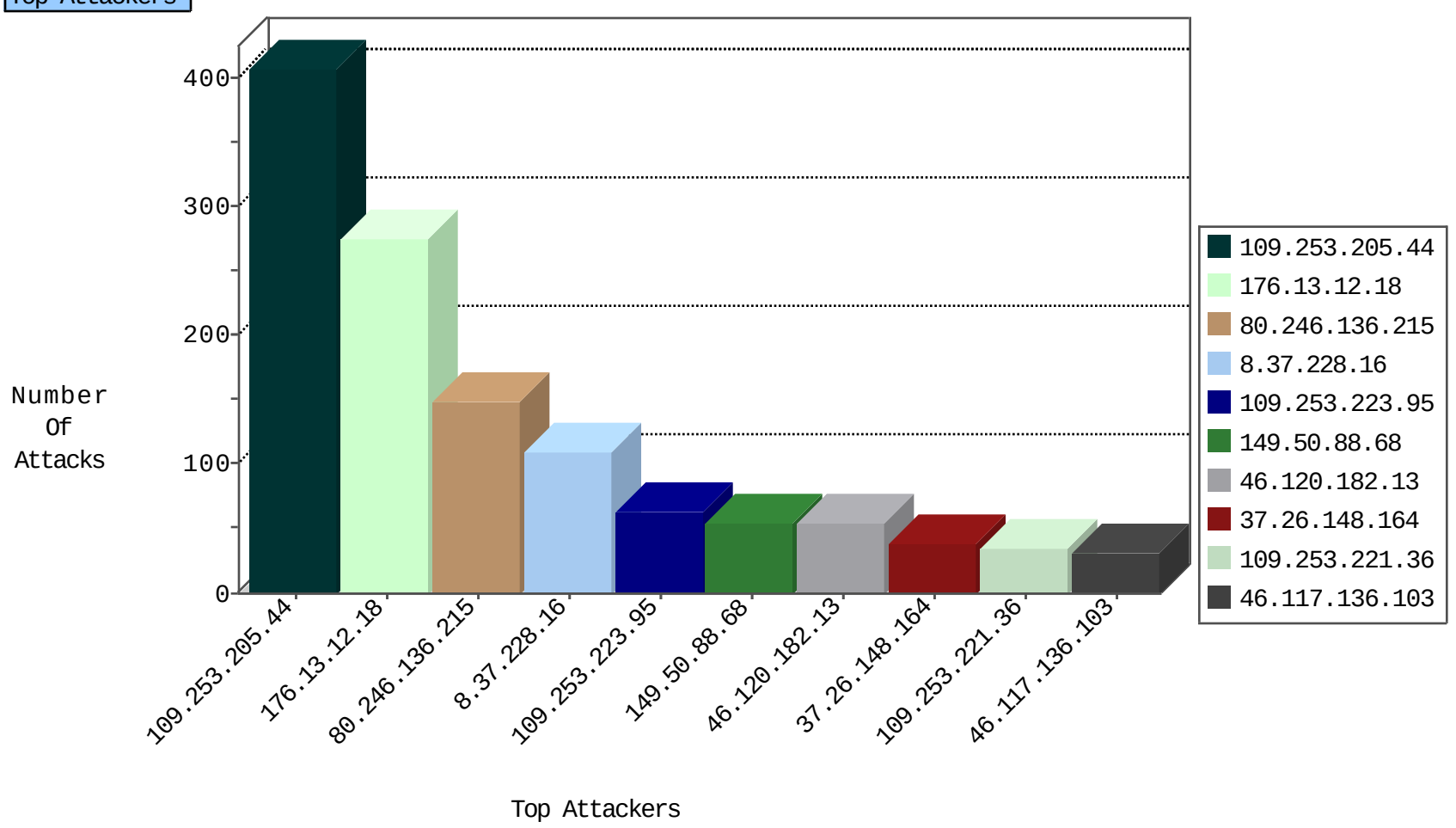
02-03-2016-18:04:04 to 02-03-2016-19:04:04

IDF Under Attack Daily Report

Top Targets



Top Attackers



02-03-2016-18:04:04 to 02-03-2016-19:04:04

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.67.120.189	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	6
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	4
8.37.228.16	Anonymous Proxy	147.237.77.216	dover.idf.il	F_Dover_Under_Attack_Con_Http	drop	2
31.168.198.173	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1
41.141.73.85	Morocco	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
31.168.198.173	Israel	147.237.77.212	e.dover.idf.il	Block_Udp_All_Nets	drop	1

02-03-2016-18:04:04 to 02-03-2016-19:04:04

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
51.254.130.58	United Kingdom	147.237.72.166	aka.idf.il	C106: HTTP: majestic bot	Block	1
188.165.15.192	France	147.237.77.233	atal.idf.il	C228: HTTP: AhrefBot crawler	Block	1

02-03-2016-18:04:04 to 02-03-2016-19:04:04

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	3
79.181.154.160	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	2
5.29.76.119	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
89.139.175.211	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
149.88.106.167	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
86.183.10.100	147.237.72.166	United Kingdom	aka.idf.il	portscan: TCP Distributed Portscan	1
131.109.147.105	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
84.228.245.118	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
109.64.35.23	147.237.0.19	Israel	madim.atal.idf.il	ET SCAN NMAP -sA (2)	1
99.226.116.158	147.237.77.216	Canada	dover.idf.il	portscan: TCP Distributed Portscan	1
79.180.70.210	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
89.248.174.81	147.237.77.234	Netherlands	halag.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
77.126.68.76	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
89.248.174.81	147.237.77.61	Netherlands	e.cogat.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
31.10.41.114	147.237.77.216	United Kingdom	dover.idf.il	portscan: TCP Distributed Portscan	1
89.248.174.81	147.237.76.196	Netherlands	e.sviva.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
217.132.136.179	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
5.29.110.125	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
89.248.174.81	147.237.0.17	Netherlands	m.my-kosher-kravi.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
149.88.216.20	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
89.138.171.21	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
149.50.85.16	147.237.77.216	United States	dover.idf.il	portscan: TCP Distributed Portscan	1
85.64.20.11	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.66.22.236	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
84.108.5.79	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
104.168.133.63	147.237.76.34	United States	yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
79.181.124.236	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
93.172.21.194	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
79.178.161.213	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
89.248.174.81	147.237.77.233	Netherlands	atal.idf.il	ET SCAN NMAP -sS window 1024	1
46.117.158.34	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
89.248.174.81	147.237.76.198	Netherlands	e.yohalan.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
218.246.0.97	147.237.0.16	China	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
5.102.216.140	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
89.248.174.81	147.237.76.177	Netherlands	ncore.idf.il	ET SCAN Potential VNC Scan 5900-5920	1

02-03-2016-18:04:04 to 02-03-2016-19:04:04

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
8.37.228.16	Anonymous Proxy	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	60
149.50.88.68	United States	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	54
8.37.228.16	Anonymous Proxy	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	47
37.26.148.164	Israel	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	39
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	30
46.116.210.29	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	25
79.177.205.138	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	20
46.19.85.248	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	17
52.7.46.16	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	17
2.54.187.164	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
85.130.246.163	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
85.130.222.91	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
109.66.97.88	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
85.130.171.55	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.117.136.103	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
5.102.254.73	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
185.120.125.1		147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
80.246.137.107	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
46.117.136.103	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
89.139.226.81	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
79.183.226.118	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.253.198.146	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
74.6.254.127	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	6
2.54.38.23	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
87.68.78.43	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
95.90.237.101	Germany	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	6
46.19.85.121	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
31.10.41.114	United Kingdom	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid sequence number	monitor	5
54.173.9.10	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	5
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	5
46.19.85.186	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
31.10.41.114	United Kingdom	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	5
31.210.188.119	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
41.141.73.85	Morocco	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Checksum	Invalid checksum. Packet dropped.	drop	4
37.46.39.162	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
37.26.147.244	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		alert	4
46.19.85.230	Israel	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
37.26.147.244	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence		monitor	4
192.243.55.134	Dominica	147.237.0.15	kosher-kravi.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
95.86.95.106	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
46.19.85.230	Israel	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
77.125.93.45	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
46.117.136.103	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
54.241.198.78	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
192.243.55.134	Dominica	147.237.0.15	kosher-kravi.idf.i	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
46.19.85.84	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
80.230.37.98	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.64.146.246	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

02-03-2016-18:04:04 to 02-03-2016-19:04:04

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.253.205.44	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	233
109.253.205.44	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	139
176.13.12.18	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	136
80.246.136.215	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	104
176.13.12.18	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	86
109.253.223.95	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	63
80.246.136.215	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (404)	Block	45
176.13.12.18	Israel	147.237.0.19	madim.atal.idf.il	Suspicious Response Code	Block	39
109.253.205.44	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (403)	Block	36
109.253.221.36	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	35
176.13.12.18	Israel	147.237.0.19	madim.atal.idf.il	Distributed Too Many of the Same Response Code (403)	Block	14
46.120.182.13	Israel	147.237.72.166	aka.idf.il	Multiple Abnormally Long Request from 46.120.182.13	Block	7
46.120.182.13	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in Method from 46.120.182.13	Block	7
46.120.182.13	Israel	147.237.72.166	aka.idf.il	Multiple Unknown HTTP Request Method from 46.120.182.13	Block	6
2.54.0.102	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation Email in mobile.idf.il/sachar/createaccount	Block	4
46.120.182.13	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in Header Name from 46.120.182.13	Block	4
46.120.182.13	Israel	147.237.72.166	aka.idf.il	Multiple Malformed URL from 46.120.182.13	Block	4
46.120.182.13	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in URL from 46.120.182.13	Block	3
46.19.86.128	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.54.187.164	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
46.120.182.13	Israel	147.237.72.166	aka.idf.il	Multiple Illegal HTTP Version from 46.120.182.13	Block	3
109.253.209.37	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
87.69.86.219	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 87.69.86.219	Block	3
37.26.149.161	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$38 in aka.idf.il/main/giyus/questionnaire.aspx	None	2
87.69.86.219	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/giyus/	Block	2
46.120.182.13	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	2
80.246.137.107	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
109.66.97.88	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
37.26.148.145	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$96 in aka.idf.il/main/giyus/questionnaire.aspx	None	2
81.218.22.216	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/about:blank	Block	2
46.120.182.13	Israel	147.237.72.166	aka.idf.il	Multiple Malformed HTTP Header Line from 46.120.182.13	Block	2
85.65.109.195	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$61 in aka.idf.il/main/giyus/questionnaire.aspx	None	2
2.54.145.148	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
46.120.182.13	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in Header Value from 46.120.182.13	Block	2
46.120.182.13	Israel	147.237.72.166	aka.idf.il	Multiple NULL Character in Header Name from 46.120.182.13	Block	2
46.120.182.13	Israel	147.237.72.166	aka.idf.il	Multiple Abnormally Long Header Line from 46.120.182.13	Block	2
46.117.158.34	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$23 in aka.idf.il/main/giyus/questionnaire.aspx	None	1
85.250.103.22	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl02$ctl03$txtField in aka.idf.il/main/giyus/questionnaire.aspx	None	1
213.57.174.150	Israel	147.237.77.233	atal.idf.il	Parameter Type Violation search in www.atal.idf.il/1437-he/atal.aspx	Block	1
2.54.156.85	Israel	147.237.72.166	aka.idf.il	Double URL Encoding - parameter: search in www.aka.idf.il/main/giyus/pniothandler1.asmx/search	Block	1
66.249.66.37	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-14463-he/dover.aspx	Block	1
109.253.212.1	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$23 in aka.idf.il/main/giyus/questionnaire.aspx	None	1
46.120.182.13	Israel	147.237.72.166	aka.idf.il	Too Many Headers per Request - 28 Headers	Block	1
109.226.15.119	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$38 in aka.idf.il/main/giyus/questionnaire.aspx	None	1
192.243.55.132	Dominica	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/404.aspx	Block	1
79.178.165.67	Israel	147.237.76.31	nakchal.idf.il	Distributed Suspicious Response Code	Block	1
89.248.174.4	Netherlands	147.237.72.167	ishurim.aka.idf.il	Unauthorized URL Access to 147.237.72.167/	Block	1
37.26.148.145	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$23 in aka.idf.il/main/giyus/questionnaire.aspx	None	1
5.29.60.149	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl02$ctl03$txtField in aka.idf.il/main/giyus/questionnaire.aspx	None	1
66.249.78.159	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	1

02-03-2016-18:04:04 to 02-03-2016-19:04:04