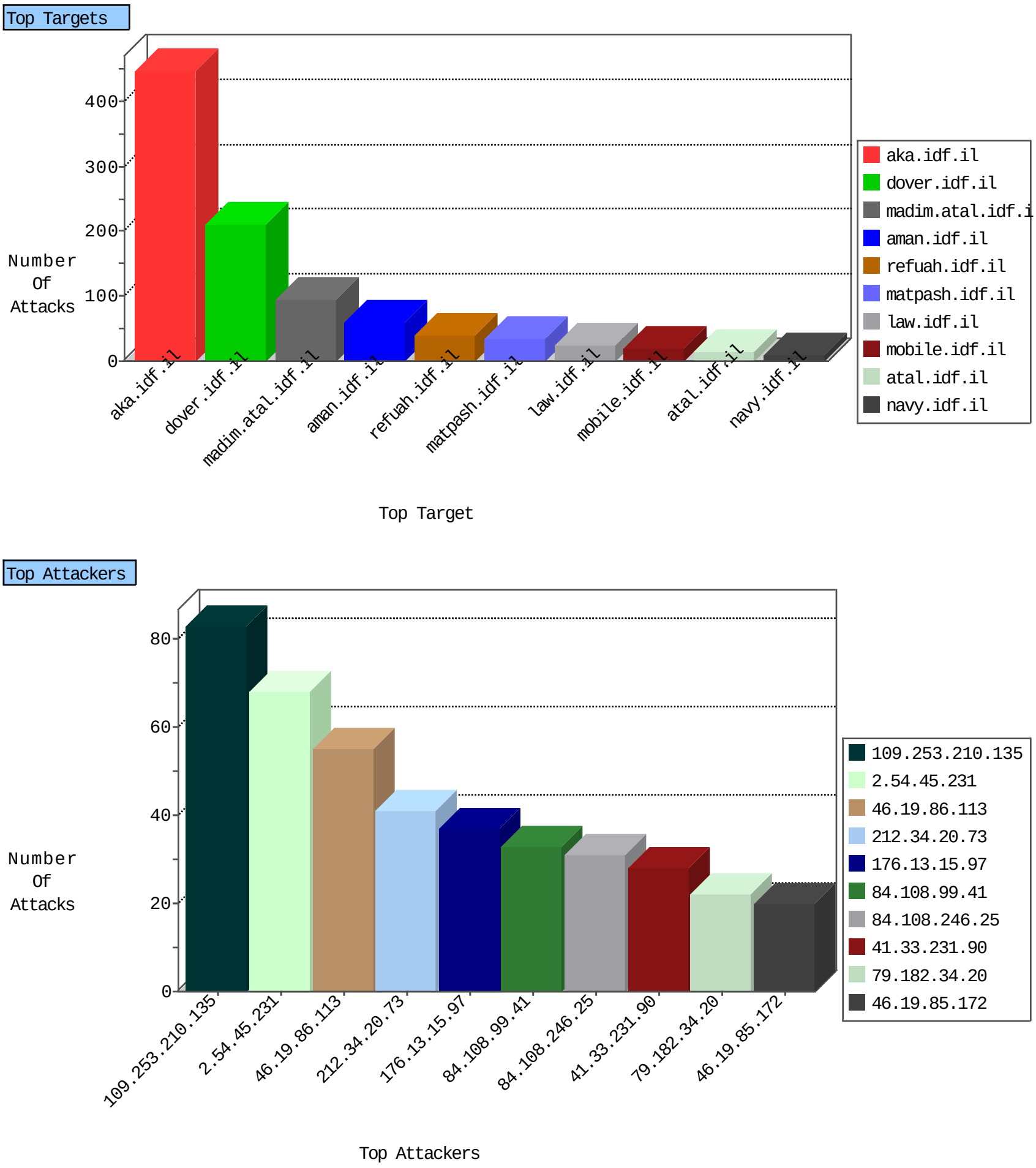
02-07-2016-15:04:09 to 02-07-2016-16:04:09

IDF Under Attack Daily Report



02-07-2016-15:04:09 to 02-07-2016-16:04:09

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
81.218.241.26	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	126
113.199.101.23	Korea, Republic of	147.237.76.196	e.sviva.idf.il	Block_Udp_All_Nets	drop	3
222.208.62.106	China	147.237.72.166	aka.idf.il	Invalid TCP Flags	drop	1

02-07-2016-15:04:09 to 02-07-2016-16:04:09

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count

02-07-2016-15:04:09 to 02-07-2016-16:04:09

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
31.168.145.213	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
217.132.47.221	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
5.102.206.203	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
207.232.12.150	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
2.54.147.107	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.67.59.206	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
109.65.54.83	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
91.201.236.114	147.237.77.61	Ukraine	e.cogat.idf.il	ET SCAN NMAP -sS window 1024	1
84.109.113.177	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.177.27.43	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
31.168.189.29	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
31.168.101.163	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
213.151.35.216	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
5.29.6.89	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	1
109.66.101.103	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
107.182.27.248	147.237.0.33	United States	idf.il	ET SCAN NMAP -sS window 1024	1
89.248.168.218	147.237.77.74	Netherlands	law.idf.il	ET SCAN Potential SSH Scan	1
79.181.116.118	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
37.142.149.46	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

02-07-2016-15:04:09 to 02-07-2016-16:04:09

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
2.54.45.231	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	66
46.19.86.113	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	55
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	28
80.178.200.51	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.86.20	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
46.19.86.203	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
79.177.202.240	Israel	147.237.0.19	madim.atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	9
82.80.71.2	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
79.182.151.196	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
80.246.136.226	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	8
80.246.136.226	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	8
79.182.34.20	Israel	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	8
46.19.85.205	Israel	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
77.126.167.10	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.26.147.252	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.181.44	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.253.197.169	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
37.46.39.136	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
79.182.135.22	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
62.219.159.53	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.52.134.196	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.172	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.86.235	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
109.253.197.169	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
46.19.85.172	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
46.19.85.172	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
79.182.34.20	Israel	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
109.64.39.60	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
79.182.34.20	Israel	147.237.77.74	law.idf.il	Bad TCP sequence		monitor	5
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
176.13.2.47	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	5
2.54.157.40	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
46.19.86.235	Israel	147.237.77.243	mobile.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
193.171.202.150	Austria	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
85.65.22.205	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
46.19.85.172	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
31.210.186.66	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.85.169	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
80.246.136.210	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
46.121.124.255	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
109.66.138.144	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.109	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
193.43.246.250	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
31.168.116.14	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.183.12.12	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.64.201.181	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
79.181.57.27	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
84.228.233.253	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
62.219.208.243	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.20.248	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

02-07-2016-15:04:09 to 02-07-2016-16:04:09

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.253.210.135	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 109.253.210.135	Block	83
176.13.15.97	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	36
84.108.99.41	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	33
212.34.20.73	Jordan	147.237.77.176	matpash.idf.il	Multiple Unknown HTTP Request Method from 212.34.20.73	Block	9
212.34.20.73	Jordan	147.237.77.176	matpash.idf.il	Multiple Malformed URL from 212.34.20.73	Block	9
212.199.177.18	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	7
192.115.248.2	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	5
212.34.20.73	Jordan	147.237.77.176	matpash.idf.il	Multiple Illegal HTTP Version from 212.34.20.73	Block	5
212.34.20.73	Jordan	147.237.77.216	dover.idf.il	Multiple Malformed URL from 212.34.20.73	Block	4
212.34.20.73	Jordan	147.237.77.216	dover.idf.il	Multiple Unknown HTTP Request Method from 212.34.20.73	Block	4
212.34.20.73	Jordan	147.237.77.176	matpash.idf.il	Multiple Abnormally Long Request from 212.34.20.73	Block	4
82.80.196.44	Israel	147.237.72.156	aman.idf.il	Distributed Unauthorized HTTP Method	Block	4
109.253.136.189	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
109.253.205.58	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.2.45	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
46.19.86.236	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
5.22.131.125	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$76 in aka.idf.il/main/giyus/questionnaire.aspx	None	2
213.8.204.11	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized Method for Known URL from 213.8.204.11	Block	2
84.108.246.25	Israel	147.237.72.156	aman.idf.il	Multiple Illegal Byte Code Character in Header Name from 84.108.246.25	Block	2
84.108.246.25	Israel	147.237.72.156	aman.idf.il	Multiple Malformed URL from 84.108.246.25	Block	2
84.108.246.25	Israel	147.237.72.156	aman.idf.il	Multiple Illegal Byte Code Character in Header Value from 84.108.246.25	Block	2
109.64.112.43	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/undefined	Block	2
84.108.246.25	Israel	147.237.72.156	aman.idf.il	Multiple NULL Character in Header Name from 84.108.246.25	Block	2
46.19.86.78	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
84.108.246.25	Israel	147.237.72.156	aman.idf.il	Multiple Illegal Byte Code Character in Method from 84.108.246.25	Block	2
84.108.246.25	Israel	147.237.72.156	aman.idf.il	Multiple Unknown HTTP Request Method from 84.108.246.25	Block	2
37.26.147.161	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
84.108.246.25	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	2
84.108.246.25	Israel	147.237.72.156	aman.idf.il	Multiple Abnormally Long Request from 84.108.246.25	Block	2
84.108.246.25	Israel	147.237.72.156	aman.idf.il	Abnormally Long Header Line request header name	Block	1
37.26.149.150	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$67 in aka.idf.il/main/giyus/questionnaire.aspx	None	1
141.212.122.81	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Unauthorized URL Access to /x	Block	1
79.181.225.169	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
85.64.229.107	Israel	147.237.72.166	aka.idf.il	Unauthorized Method OPTIONS for www.aka.idf.il/	Block	1
84.108.246.25	Israel	147.237.72.156	aman.idf.il	Multiple Illegal HTTP Version from 84.108.246.25	Block	1
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/	Block	1
212.34.20.73	Jordan	147.237.77.176	matpash.idf.il	Illegal HTTP Version like Gecko) Chrome/47.0.2526.111 Safari/537.36	Block	1
176.13.2.47	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
84.108.246.25	Israel	147.237.72.156	aman.idf.il	Illegal URL Path Encoding ÂšsÃ?Ã»×¢nm[[#2]]×¤cÃšÂ¡Â izâ,¬ÃŠwÂ?×' #×¢Âš%Â¿8×,-Â?(â€¡[[#18]]yÖ¼Â?[[#5]][[#14]]ÂŒâ€ _	Block	1
46.19.86.27	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_CLIENT_HELLO)	None	1
109.66.168.124	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl38$ctl01$ctl03$cblQuestion$6 in www.aka.idf.il/main/giyus/questionnaire.aspx	None	1
82.80.196.44	Israel	147.237.72.156	aman.idf.il	Multiple Unauthorized URL Access from 82.80.196.44	Block	1
79.177.202.240	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 79.177.202.240	Block	1
84.108.246.25	Israel	147.237.72.156	aman.idf.il	NULL Character in Method Â‰ÃŸQÃ”RÂœ[[#15]]Ã?W[[#24]]Ã–Â‰[[#21]]Ã¼Ã¡[[#8]][[#31]][[#0]]ÂŒ	Block	1
66.249.74.104	Israel	147.237.77.170	maarachot.idf.il	Multiple Unauthorized URL Access from 66.249.74.104	Block	1
185.28.191.30	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-ar	Block	1
84.108.246.25	Israel	147.237.72.156	aman.idf.il	Abnormally Long Request request version	Block	1
37.60.44.122	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/0/68860.pdf&sa=u&ved=0ahukewiorjjg4oxkahxmxhokhz35bx04chawcaowaq&sig2=yzn9okwzws7q0wpzz4u2pg&usg=afqjcne_tcpgl_7mhotfqvemddrbsf6zua	Block	1
149.88.36.60	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
79.183.12.12	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$tfasimSignAll in www.aka.idf.il/main/sachar/payslips.aspx	None	1

02-07-2016-15:04:09 to 02-07-2016-16:04:09