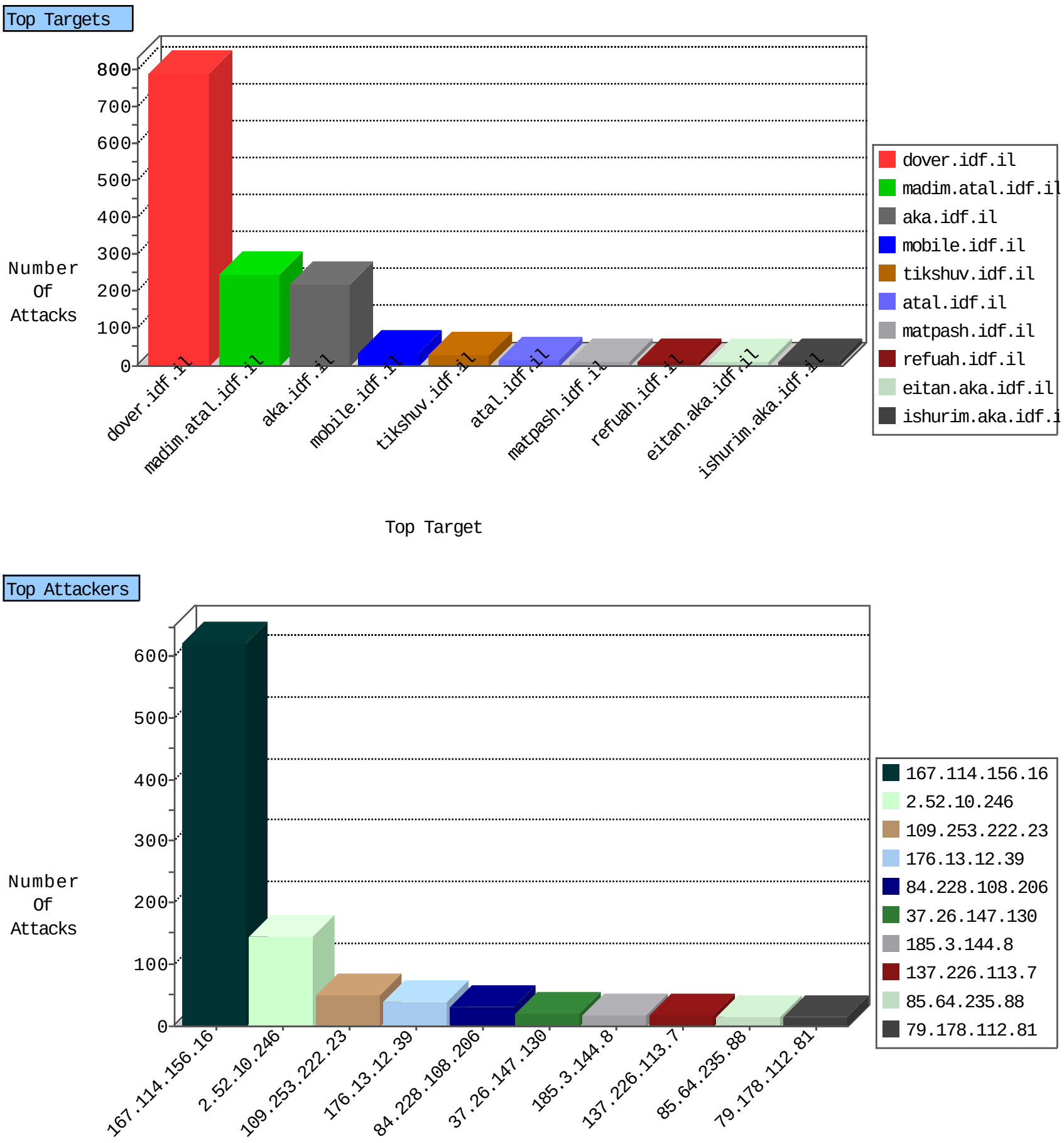
03-10-2016-21:04:02 to 03-10-2016-22:04:02

IDF Under Attack Daily Report



03-10-2016-21:04:02 to 03-10-2016-22:04:02

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	3001
82.145.221.141	Europe	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	5
81.218.65.210	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
119.93.47.186	Philippines	147.237.0.200	m4u.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
185.56.28.67	Netherlands	147.237.0.35	akaws.idf.il	Block_Ntp_All_Net	drop	1
185.56.28.67	Netherlands	147.237.76.197	e.himush.idf.il	Block_Ntp_All_Net	drop	1
185.56.28.67	Netherlands	147.237.76.201	e.atal.idf.il	Block_Ntp_All_Net	drop	1
185.56.28.67	Netherlands	147.237.77.233	atal.idf.il	Block_Ntp_All_Net	drop	1

03-10-2016-21:04:02 to 03-10-2016-22:04:02

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
132.72.228.215	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
185.3.144.8	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	7
123.126.113.154	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	5
38.87.46.138	United States	147.237.77.216	dover.idf.il	C1000008: HTTP: Xenu UserAgent	Block	1
123.126.113.80	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
192.168.1.159		147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	1
66.249.79.234	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
106.38.241.106	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
176.104.37.122	Ukraine	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	1
106.120.173.102	China	147.237.76.42	refuah.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1

03-10-2016-21:04:02 to 03-10-2016-22:04:02

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
95.86.127.108	147.237.77.233	Israel	atal.idf.il	ET DOS Large amount of TCP ZeroWindow - Possible Nkiller2 DDos attack	8
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
173.166.65.97	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
66.249.93.32	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
112.54.83.98	147.237.0.35	China	akaws.idf.il	ET SCAN Potential SSH Scan	1
112.54.83.98	147.237.0.16	China	my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
104.215.89.20	147.237.77.226	United States	www.chamatz.aka.idf.il	ET SCAN NMAP -f -sS	1
93.113.125.12	147.237.77.235	Romania	sviva.idf.il	ET SCAN NMAP -sS window 1024	1
202.71.25.29	147.237.72.166	India	aka.idf.il	ET SCAN NMAP -sS window 2048	1
112.54.83.98	147.237.0.33	China	idf.il	ET SCAN Potential SSH Scan	1
104.215.89.20	147.237.77.226	United States	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 2048	1
202.71.25.29	147.237.72.166	India	aka.idf.il	ET SCAN NMAP -sS window 4096	1
202.71.25.29	147.237.72.166	India	aka.idf.il	ET SCAN NMAP -f -sS	1
180.97.106.162	147.237.77.212	China	e.dover.idf.il	ET SCAN Potential SSH Scan	1

03-10-2016-21:04:02 to 03-10-2016-22:04:02

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
109.253.222.23	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	51
79.178.112.81	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	14
81.4.163.106	Cyprus	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
87.68.243.37	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
176.13.13.209	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
213.57.240.123	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
84.109.76.32	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
46.19.86.191	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.85.209	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
5.102.254.50	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
79.178.4.147	Israel	147.237.77.176	matpash.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.253.201.81	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
158.69.112.86	United States	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
109.67.136.218	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
87.71.127.148	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.177.226.12	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.52.16.86	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
188.120.154.9	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.86.81	Israel	147.237.76.147	chinuch.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
109.65.248.31	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
37.26.148.155	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
46.120.150.126	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
85.64.123.234	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
85.64.235.88	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
212.34.12.94	Jordan	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
5.22.129.233	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
37.46.39.127	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
137.226.113.7	Germany	147.237.76.196	e.sviva.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	3
2.54.158.96	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
178.255.215.87	France	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
176.13.0.60	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
77.126.9.241	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
85.64.235.88	Israel	147.237.77.243	mobile.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
137.226.113.7	Germany	147.237.76.197	e.himush.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	3
109.67.36.145	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.183.178.155	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
149.78.27.155	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.177.13.243	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
185.3.144.8	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
2.52.150.231	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
46.19.85.230	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
79.180.15.182	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
87.71.102.100	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
185.3.147.169	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
137.226.113.7	Germany	147.237.77.176	matpash.idf.il	drop	SAM rule	drop	3
46.19.86.253	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
172.56.13.81	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3

03-10-2016-21:04:02 to 03-10-2016-22:04:02

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
80.230.38.149	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
185.27.105.148	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

03-10-2016-21:04:02 to 03-10-2016-22:04:02

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.52.10.246	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	146
176.13.12.39	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	40
84.228.108.206	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	30
37.26.147.130	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	20
37.77.49.3	Iraq	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/error.htm	Block	4
37.26.147.167	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
85.64.123.234	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.54.162.59	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
73.22.155.10	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/	Block	2
109.64.22.85	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
83.244.5.162	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Malformed URL ·[[#30]]ß»”“\ok¬¸pˆ3Œ[[#6]]$qtÚÞ][[#2]]‰ ‰Ո¶]]e[[#17ת¿ž¸]]q lœwÊq`‰¸e[[#18ɔƴ´•±‡w¨'±ʊʁ]]#29[[]]#22[[l²ƒdf:¶Ðd]]#14[[p^•œÛ³zʊ¿×ƴž"	Block	1
82.80.196.44	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
109.253.200.197	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/mailbox.aspx	None	1
46.120.167.95	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/chinuch/general/default.asp	None	1
84.108.104.201	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/sip_storage/files/9/2479.jpg	Block	1
83.244.5.162	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Illegal Byte Code Character in Header Value	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english/1113-2.stm" target="_blank	Block	1
184.164.147.20	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/admin	Block	1
85.64.235.88	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
83.244.5.162	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Multiple Untraceable SSL Sessions from 83.244.5.162 (Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE))	None	1
83.130.105.203	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/console/core/doc_mgr/mce_src=	Block	1
149.88.71.234	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
66.249.64.51	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/8/2368.jpg	Block	1
84.228.12.27	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
5.29.101.156	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
83.244.5.162	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Illegal Byte Code Character in Method ÄJ®2b_º.üå"9kQ´4R)Ù¶/½ä·sÄ[[#17]]¦e(»°[[#19]]¨ÒíøÂZI[[#25]]Eñ7 röª`˜•xl¼ðÆ'ìá~puC[[#30]]–	Block	1
196.112.88.110		147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
37.26.148.168	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
85.65.185.40	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	PHP Attempt	Block	1
83.244.5.162	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	NULL Character in Method ÄJ®2b_º.üå"9kQ´4R)Ù¶/½ä·sÄ[[#17]]¦e(»°[[#19]]¨ÒíøÂZI[[#25]]Eñ7 röª`˜•xl¼ðÆ'ìá~puC[[#30]]–	Block	1
83.244.5.162	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Abnormally Long Header Line request header name	Block	1
66.249.64.56	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/layoutdev.css	Block	1
31.168.217.136	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
83.244.5.162	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Illegal Byte Code Character in URL ·[[#30]]ß»”“\ok¬¸pˆ 3Œ[[#6]]$qtÚÞ][[#2]]‰[[#22]][[#29]]'±ʊʁw¨‡±•´ɔʏq lœwÊq`‰¸ e[[#18]]¸ž¿ת[[#17]]¶Ʊ¿×ƴž"‰ת Û³zœ•^[[p#14d]]Ðfdƒ²l:¶	Block	1
79.181.184.83	Israel	147.237.76.31	nakchal.idf.il	PHP Attempt	Block	1
207.46.13.100	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/	Block	1
87.71.102.100	Israel	147.237.72.166	aka.idf.il	Unauthorized Method POST for www.aka.idf.il/main/sachar/faq.aspx	Block	1
83.244.5.162	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
83.244.5.162	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Abnormally Long Request request version	Block	1
180.76.15.29	China	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/994-9182-he/refuah.aspx	Block	1
66.249.64.61	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	1
37.26.146.231	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
83.244.5.162	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Illegal HTTP Version õÜ[[#25]]Ë»º™'ŽðW[[#6]]]SPŽ_WßÖ„*C![[#21]]PÍïÐ–?þ8ö‹:ôm•Ó þûÎä‰Œ[[#29]]ø[[#15]]×Heåf[[#15]]H#âàKYŸsHÎÁ[[#26]]l	Block	1
79.181.184.83	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to nakhal.idf.il/xmlrpc.php	Block	1
207.225.131.141	United States	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
38.81.65.42	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/robots.txt	Block	1
83.244.5.162	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Unknown HTTP Request Method ÄJ®2b_º.üå"9kQ´4R)Ù¶/½ä·sÄ[[#17]]¦e(»°[[#19]]¨ÒíøÂZI[[#25]]Eñ7 röª`˜•xl¼ðÆ'ìá~puC[[#30]]–	Block	1
83.244.5.162	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	Illegal Byte Code Character in Header Name Ó[[#21]]Z[[#19]][[#7]]Ô{ÛžRÖ.[[#16]]‡“™¸[[#3]]»[[#31]]xupOóòJ Ê-ÐŽí	Block	1
184.164.147.20	United States	147.237.77.216	dover.idf.il	Admin Blocking	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 68.180.228.112	Block	1

03-10-2016-21:04:02 to 03-10-2016-22:04:02