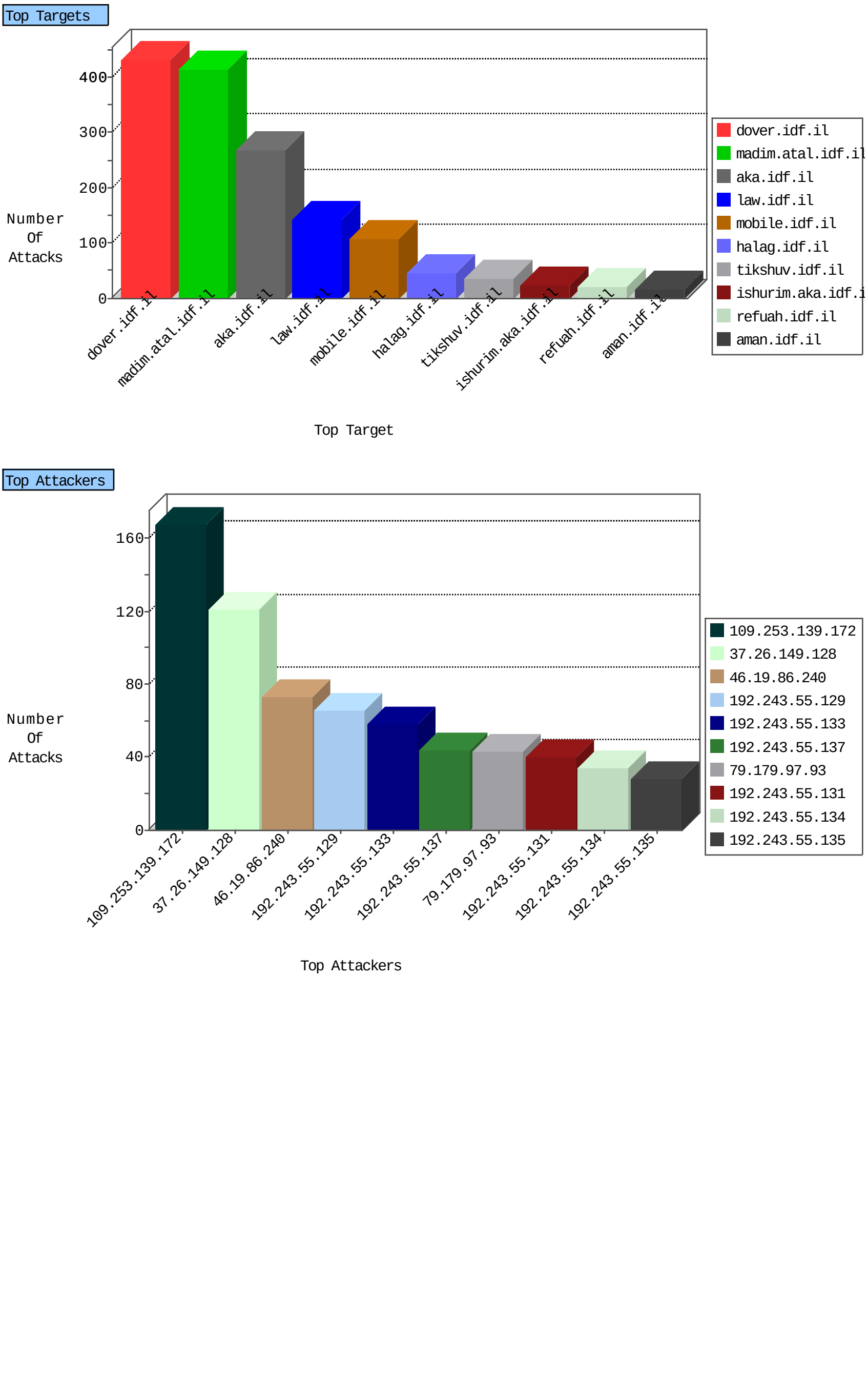
03-03-2016-12:04:05 to 03-03-2016-13:04:05

IDF Under Attack
Daily Report



03-03-2016-12:04:05 to 03-03-2016-13:04:05

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	108
81.218.241.26	Israel	147.237.72.156	aman.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	92
79.179.177.86	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	11
79.179.97.93	Israel	147.237.77.234	halag.idf.il	Invalid TCP Flags	drop	8
84.109.130.231	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	6
81.218.65.210	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
184.105.247.207	United States	147.237.77.234	halag.idf.il	Block_Udp_All_Nets	drop	1
123.180.204.101	China	147.237.76.177	ncore.idf.il	Block_Udp_All_Nets	drop	1
184.105.247.215	United States	147.237.77.226	www.chamatz.aka.idf.il	Block_Udp_All_Nets	drop	1
85.97.188.118	Turkey	147.237.76.176	test.ncore.idf.il	Block_Udp_All_Nets	drop	1
184.105.139.77	United States	147.237.77.212	e.dover.idf.il	Block_Udp_All_Nets	drop	1
192.243.55.131	Dominica	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1
85.97.188.118	Turkey	147.237.76.177	ncore.idf.il	Block_Udp_All_Nets	drop	1
184.105.139.117	United States	147.237.0.200	m4u.idf.il	Block_Udp_All_Nets	drop	1
202.58.137.76	Australia	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1
123.180.204.101	China	147.237.76.176	test.ncore.idf.il	Block_Udp_All_Nets	drop	1

03-03-2016-12:04:05 to 03-03-2016-13:04:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
5.29.150.215	Israel	147.237.0.34	tikshuv.idf.	C1000138: HTTP: prefix 1.01 in the URL	Block	9
46.117.104.113	Israel	147.237.0.34	tikshuv.idf.	C1000138: HTTP: prefix 1.01 in the URL	Block	5
123.126.113.154	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	5
192.118.12.102	Israel	147.237.0.34	tikshuv.idf.	C1000138: HTTP: prefix 1.01 in the URL	Block	4
144.76.29.66	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
62.219.227.250	Israel	147.237.0.34	tikshuv.idf.	C1000138: HTTP: prefix 1.01 in the URL	Block	2
195.154.187.115	France	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
66.249.93.121	United States	147.237.0.34	tikshuv.idf.	C1000138: HTTP: prefix 1.01 in the URL	Block	2
51.254.143.239	United Kingdom	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
66.249.93.117	Israel	147.237.0.34	tikshuv.idf.	C1000138: HTTP: prefix 1.01 in the URL	Block	1
106.38.241.106	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
66.249.93.121	Israel	147.237.0.34	tikshuv.idf.	C1000138: HTTP: prefix 1.01 in the URL	Block	1
123.126.113.80	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
89.216.115.6		147.237.77.216	dover.idf.il	17272: HTTP: Suspicious User-Agent (WindowsNT) With No Separating Space	Block	1

03-03-2016-12:04:05 to 03-03-2016-13:04:05

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
37.26.147.212	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
176.13.20.58	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
31.154.85.7	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
176.13.4.120	147.237.72.166	Israel	aka.idf.il	GPL SCAN myscan	1
5.28.135.74	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
132.70.66.12	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
132.64.217.47	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
98.119.105.221	147.237.77.74	United States	law.idf.il	ET SCAN NMAP -sS window 3072	1
84.111.5.241	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
218.246.0.97	147.237.8.50	China	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
79.181.134.157	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
209.126.116.147	147.237.8.46	United States	e.chinuch.idf.il	ET SCAN NMAP -sS window 1024	1
46.19.86.252	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
199.203.95.161	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
31.210.178.14	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
176.13.4.120	147.237.72.166	Israel	aka.idf.il	INDICATOR-SCAN myscan	1
31.154.8.70	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
149.88.85.247	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
132.70.66.9	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.253.211.193	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
94.230.86.116	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
218.246.0.97	147.237.76.39	China	mobile.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
84.110.36.136	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
213.244.88.90	147.237.77.216	Palestinian Territory, Occupied	dover.idf.il	portscan: TCP Distributed Portscan	1
79.178.59.113	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
208.80.155.214	147.237.76.86	United States	navy.idf.il	Tehila - Perl LWP with fake user agent	1

03-03-2016-12:04:05 to 03-03-2016-13:04:05

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
109.253.146.128	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
79.179.97.93	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	22
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	20
46.19.86.186	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	15
2.52.130.43	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	15
2.54.44.75	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
176.13.22.57	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
79.179.97.93	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	alert	12
192.243.55.133	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	11
192.243.55.129	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	10
192.243.55.133	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	10
37.26.147.199	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
192.243.55.137	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	9
46.19.85.26	Israel	147.237.77.216	dover.idf.il	drop	SAM rule	drop	9
192.243.55.133	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	9
192.243.55.129	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	9
192.243.55.135	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	8
62.90.193.162	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	8
192.243.55.134	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	8
192.243.55.129	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	8
192.243.55.134	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	8
46.19.85.26	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
192.243.55.133	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
192.243.55.131	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
46.32.214.239	Palestinian Territory, Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
192.243.55.131	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
208.69.40.101	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
192.243.55.129	Dominica	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	7
192.243.55.136	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	6
192.243.55.137	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
192.243.55.129	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
46.19.86.105	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
5.22.131.75	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
172.56.30.39	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.180.51.91	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.177.29.132	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
81.218.163.254	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.183.132.104	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
192.243.55.129	Dominica	147.237.77.74	law.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
192.243.55.137	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
192.243.55.137	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
176.13.9.123	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
157.55.39.58	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
192.243.55.133	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence		monitor	6
46.19.86.219	Israel	147.237.77.243	mobile.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
176.13.11.53	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
192.243.55.137	Dominica	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	5
192.243.55.129	Dominica	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
192.243.55.134	Dominica	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
192.243.55.136	Dominica	147.237.77.74	law.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5

03-03-2016-12:04:05 to 03-03-2016-13:04:05

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.253.139.172	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	168
37.26.149.128	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	116
46.19.86.240	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	73
37.26.149.248	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	18
2.52.7.223	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation Password in mobile.idf.il/sachar/login	Block	6
94.159.170.199	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
79.182.59.15	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
176.13.15.37	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	5
62.219.236.190	Israel	147.237.77.176	matpash.idf.il	Distributed Unauthorized URL Access on www.cogat.idf.il/templates/shared/usercontrols/promotioncube/	Block	5
2.52.161.59	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	5
46.19.86.186	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	4
176.13.22.57	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	4
46.19.86.97	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	4
109.253.146.128	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	4
185.32.179.10	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
195.154.173.103	France	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/mazi	Block	3
66.249.66.184	United States	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 66.249.66.184	Block	2
79.180.61.36	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	2
31.154.34.246	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
46.119.127.64	Ukraine	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/mazi/	Block	2
46.19.86.105	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
176.13.9.104	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
79.179.97.93	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
185.32.179.136	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
140.123.101.42	Taiwan	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/aman	Block	1
77.126.221.196	Israel	147.237.77.216	dover.idf.il	Illegal Byte Code Character in URL (%#,•˛[[#21]]&[[!#30‡˙¥!{y]]|w•ת˛+o•«˜=«•ל ;[sכi»%f'•(•[[#18]]hא″¼ÿ˛t'פ	Block	1
91.108.88.200	Germany	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/shared/usercontrols/headerupper/	Block	1
77.126.221.196	Israel	147.237.77.216	dover.idf.il	Abnormally Long Request method	Block	1
46.19.86.131	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/reset.css	Block	1
194.72.238.241	United Kingdom	147.237.77.216	dover.idf.il	Unauthorized URL Access to /	Block	1
79.182.164.122	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
77.126.221.196	Israel	147.237.77.216	dover.idf.il	NULL Character in Header Name at Kº^O6[[#29]]˜&…-[[#23]][[#12]]Çôà/ýŽ–MË[Ð[[#22]]Aël3K–^·[»[[#23]]èªÈÁ Ú[[#6]]~[[#21]][[#22]]B{Ž»Íw&ÎµË[[#26]]ž3~[[#18]][[#23]]Ö@TXóÿJ?w– ²^µ'ÃÑ P#012ª;ðï[[#18]]{ØW3èQê‘57gÁ[[#18]]í¸ÙÂ[[#1]]-r[[#31]][[#11]]¹‘TÚ&=²ýÖ¡ #012ZaeÐnèðOIÈ@Ê[[#5]]¿éÏK`#011¾É”[[#19]] æ"ê8¦ÇåCœ•Ø]" Ä [[#22]][[#14]]Š?ä[[#17]]Ç–D®d5,u+çÆ[[#30]]'+[[#0]]Å†% •ÄrJ•±bNÄ[[#0]][[#26]]E.tŽ“ãG[[#14]]•Qô[[#16]]óFÚgÙ[[#20]].1/rvhy¦‹wSÚ £•Å§W•¢‡wK#012THÝ[[#18]]¼ÂÌaßLFúãK¸U»Â[[#26]][[#27]][[#31]]iÄpùd’á_¦ ûzâ®pÑ(âð[[#7]]	Block	1
5.22.131.75	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
77.126.221.196	Israel	147.237.77.216	dover.idf.il	Illegal Byte Code Character in Method “ü„•ÉSA[[#29]]A–O´pé]]~€˜[[#16]]³[[#17]][[#19]]tZÛJË¡wBßØæl•ñ‹À<÷Åi# 012òòpMÇ•#Ò·¹I#012[[#4]]½	Block	1
109.64.1.124	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//res#012 ources/images/innerpage/goback.gif	Block	1
80.246.136.203	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
79.179.177.86	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/undefined	Block	1
40.77.167.77	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/	Block	1
192.115.130.253	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/valtam	Block	1
157.55.39.67	United States	147.237.72.166	aka.idf.il	Unknown Parameter 136cd360 in www.aka.idf.il/main/home/default.aspx	None	1
77.126.221.196	Israel	147.237.77.216	dover.idf.il	Illegal HTTP Version ý©hølŸ[[#1]]ŽÜÁÌ–DaßÁ,¾¼¹¾:ÿx‡˜,ƒ†_âÈ[[#27]]ùl[[#4]]u"é¾ÌS[[#24]]•×ñ[[#30]]ºrÑ<¤28QýñÆR[[#12]]+ñÖÐ•'Ô‰ n¸-W[[#25]]ü	Block	1
77.126.221.196	Israel	147.237.77.216	dover.idf.il	Distributed Malformed URL	Block	1
194.90.128.185	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 194.90.128.185	Block	1
79.183.37.219	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/main/sachar/forgotpassword.aspx	None	1
77.126.221.196	Israel	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
17.142.156.109	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/apple-app-site-association	Block	1
77.126.221.196	Israel	147.237.77.216	dover.idf.il	Illegal Byte Code Character in Parameter Name W·iŒ7xÚ•rƒƒ|cX¸8[[ז#16p]]Ÿפ¸ 9t²¨,sÜ¸hœ[[#5]]&Ak–„[[˜"#31&g˙x,(d•j˛2"pÿ]]61#[[Ù]]ך[[71#]], in (%#,•˛ [sכi»%f'•(•[[#18]]hא″¼ÿ˛t'לפ+•o«˜=«•˛ך•w|‡˙¥!{y]]#30[[!&]]#21[[	Block	1
109.64.1.124	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in URL from 109.64.1.124	Block	1
82.166.182.145	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/templates/shared/usercontrols/promotioncube/	Block	1
192.243.55.129	Dominica	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-he	Block	1

03-03-2016-12:04:05 to 03-03-2016-13:04:05