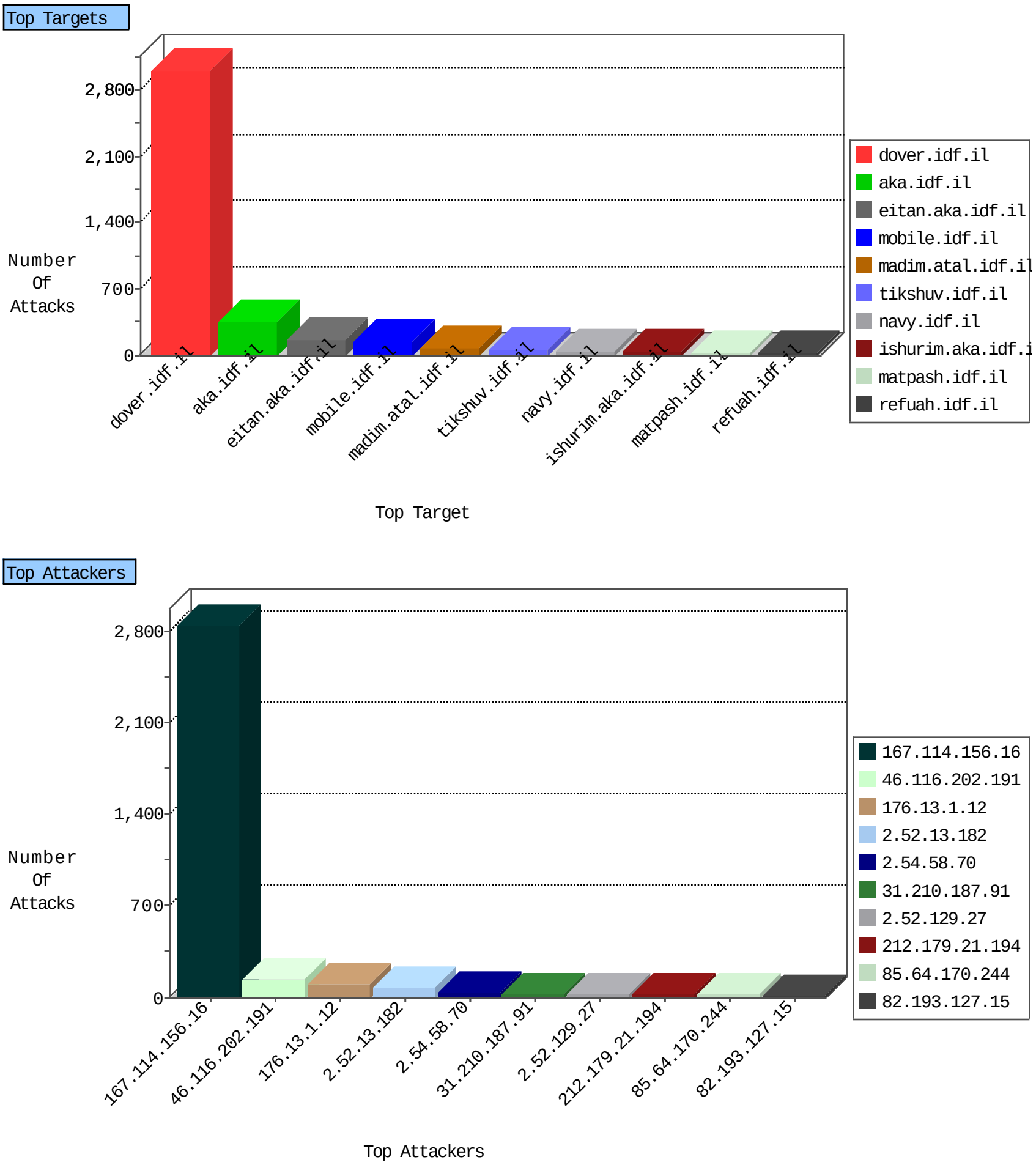
03-14-2016-16:04:02 to 03-14-2016-17:04:02

IDF Under Attack
Daily Report



03-14-2016-16:04:02 to 03-14-2016-17:04:02

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	3428
79.182.177.6	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
123.249.25.14	China	147.237.0.19	madim.atal.idf.il	JLM_Under_Attack_Con_Tcp	drop	2
0.0.0.0		147.237.77.216	dover.idf.il	HTTP Page Flood Attack	drop	2
219.232.243.28	China	147.237.76.34	yohalan.idf.il	Invalid L4 Header Length	drop	1

03-14-2016-16:04:02 to 03-14-2016-17:04:02

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.176.103.6	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	20
207.232.36.181	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	7
79.181.102.181	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
82.193.127.15	Ukraine	147.237.77.74	law.idf.il	C1000074: HTTP: majestic bot	Block	4
37.26.149.175	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
66.249.93.125	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
82.193.127.15	Ukraine	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Block	4
66.249.93.117	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	3
82.193.127.15	Ukraine	147.237.0.34	tikshuv.idf.il	C1000074: HTTP: majestic bot	Block	3
82.193.127.15	Ukraine	147.237.76.86	navy.idf.il	C1000074: HTTP: majestic bot	Block	3
82.193.127.15	Ukraine	147.237.77.226	www.chamatz.aka.idf.il	C1000074: HTTP: majestic bot	Block	2
109.253.195.247	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
82.193.127.15	Ukraine	147.237.77.170	maarachot.idf.il	C1000074: HTTP: majestic bot	Block	2
82.193.127.15	Ukraine	147.237.77.176	matpash.idf.il	C1000074: HTTP: majestic bot	Block	2
37.26.149.195	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
82.193.127.15	Ukraine	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
69.30.198.178	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
46.19.86.87	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
66.249.93.121	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1

03-14-2016-16:04:02 to 03-14-2016-17:04:02

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
212.179.21.194	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	2
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	2
109.226.45.141	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
109.65.243.121	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
93.172.228.251	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.120.97.101	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
5.22.129.93	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
218.246.0.97	147.237.72.156	China	aman.idf.il	ET SCAN NMAP -sS window 1024	1
193.105.134.220	147.237.77.212	Sweden	e.dover.idf.il	ET SCAN NMAP -sS window 1024	1
123.249.25.14	147.237.0.15	China	kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
109.67.146.31	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
94.102.48.194	147.237.76.44	Netherlands	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	1
84.109.230.105	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.19.85.164	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
218.246.0.97	147.237.0.16	China	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
185.127.10.35	147.237.77.216		dover.idf.il	portscan: TCP Distributed Portscan	1

03-14-2016-16:04:02 to 03-14-2016-17:04:02

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
46.116.202.191	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	138
176.13.1.12	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	93
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	80
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack		reject	33
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	33
31.210.187.91	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	28
2.52.13.182	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	22
178.2.8.170	Germany	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	21
212.179.21.194	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	20
85.64.170.244	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	14
2.52.13.182	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	14
2.52.13.182	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	14
85.64.170.244	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	14
2.52.13.182	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	14
176.13.23.199	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	13
2.52.13.182	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	13
46.19.85.1	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
37.26.146.183	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
212.179.21.194	Israel	147.237.76.176	test.ncore.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
31.210.187.91	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	alert	7
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
79.127.43.231	Iran, Islamic Republic of	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
79.182.193.172	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
95.35.89.203	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.179	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
5.22.130.70	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.52.129.27	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.144	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
79.127.43.231	Iran, Islamic Republic of	147.237.77.176	matpash.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
212.235.43.215	Israel	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	6
176.13.8.125	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.137.207	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
5.102.254.171	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
82.166.244.149	Israel	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
178.63.105.85	Germany	147.237.76.177	ncore.idf.il	drop	SAM rule	drop	4
46.19.85.210	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
46.19.85.76	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
5.102.123.185	Palestinian Territory, Occupied	147.237.77.176	matpash.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
46.19.85.76	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
185.3.147.238	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
37.26.148.199	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.66.49.123	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
192.114.23.211	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
213.57.72.229	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
31.168.69.107	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.86.75	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
91.135.102.190	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.176.161.89	Israel	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
176.13.14.36	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3

03-14-2016-16:04:02 to 03-14-2016-17:04:02

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

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.54.58.70	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	38
2.52.129.27	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	27
176.13.1.12	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	7
132.76.50.5	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	6
2.54.11.180	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.1.10	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
192.115.177.202	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/scripts/css3pie.htc	Block	3
80.246.139.203	Israel	147.237.0.19	madim.atal.idf.il	Suspicious Response Code	Block	3
46.19.85.1	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	3
176.13.8.125	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
72.9.148.10	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/994-8613-he/navy.aspx.aspx	Block	2
157.55.39.189	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
5.102.254.133	Israel	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	2
66.86.116.247	United States	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
176.228.62.25	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar/undefined	Block	2
85.64.218.245	Israel	147.237.76.147	chinuch.aka.idf.i	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	2
109.253.207.6	Israel	147.237.77.243	mobile.idf.il	Parameter Type Violation Password in mobile.idf.il/sachar/login	Block	2
5.102.254.133	Israel	147.237.77.170	maarachot.idf.il	Distributed PHP Attempt	Block	1
109.64.188.204	Israel	147.237.76.31	nakchal.idf.il	Distributed PHP Attempt	Block	1
79.179.56.214	Israel	147.237.72.166	aka.idf.il	Unknown HTTP Request Method ¹[[#31]]•µþ›* in URL nү ¨Þž[[#3]][[#3]][[#3]]–´[[#2]]•~™9ᴛ=',Ýoa[[#22]]„x″Ýo,b,¯:¹.p|½[[02#]]′0: w¼)‰j‥[[#27]]ˆ.[[#30]]…ᴛb—א!z[[#24]]′k˙‘¯y‡a¨2ᴵıû±±|kק	Block	1
79.179.56.214	Israel	147.237.72.166	aka.idf.il	Abnormally Long Header Line request header name	Block	1
213.57.194.251	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
87.71.29.15	Israel	147.237.72.166	aka.idf.il	Unknown Parameter docId in www.aka.idf.il/main/sachar/faq.aspx	None	1
66.249.69.32	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/robots.txt	Block	1
79.183.33.78	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/xmlrpc.php	Block	1
79.183.33.78	Israel	147.237.76.42	refuah.idf.il	Distributed PHP Attempt	Block	1
31.210.186.234	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$btnAtudaPrint in www.aka.idf.il/main/giyus/atuda/asmachta.aspx	None	1
109.253.219.83	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/mailbox.aspx	None	1
5.29.214.156	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
94.230.95.82	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on www.aka.idf.il/xmlrpc.php	Block	1
79.179.56.214	Israel	147.237.72.166	aka.idf.il	Illegal HTTP Version	Block	1
83.45.98.133	Spain	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
199.16.156.125	United States	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 199.16.156.125	Block	1
46.117.96.54	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/https:/www.aman.idf.il/	Block	1
79.183.33.78	Israel	147.237.77.170	maarachot.idf.il	Distributed Unauthorized URL Access on maarachot.idf.il/xmlrpc.php	Block	1
5.102.254.133	Israel	147.237.77.170	maarachot.idf.il	Distributed Unauthorized URL Access on maarachot.idf.il/xmlrpc.php	Block	1
109.64.188.204	Israel	147.237.76.31	nakchal.idf.il	Distributed Unauthorized URL Access on www.nakhal.idf.il/xmlrpc.php	Block	1
79.183.33.78	Israel	147.237.72.166	aka.idf.il	Distributed PHP Attempt	Block	1
79.179.56.214	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in Method	Block	1
213.151.53.59	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/home/default.aspx	Block	1
2.54.36.237	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
93.113.154.56	Romania	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	1
79.183.131.195	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
68.180.230.189	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1779-he/dover.aspx	Block	1
176.13.23.199	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
79.183.33.78	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/xmlrpc.php	Block	1
37.26.148.161	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	1
94.230.95.82	Israel	147.237.77.170	maarachot.idf.il	Distributed PHP Attempt	Block	1
79.179.56.214	Israel	147.237.72.166	aka.idf.il	Malformed URL nү¨Þž[[#3]][[#3]][[#3]]–´[[#2]]•~™9ᴛ=',Ýoa[[#22]]„x″Ýo,b,×ƒ קk|±±ûᴵız[[#24]]′k˙‘¯y‡a¨2!א—bᴛ…]]w¼)‰j‥[[#27]]ˆ.[[#30:0′]]#20[[½|¹p.¯	Block	1
2.52.13.182	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1

03-14-2016-16:04:02 to 03-14-2016-17:04:02