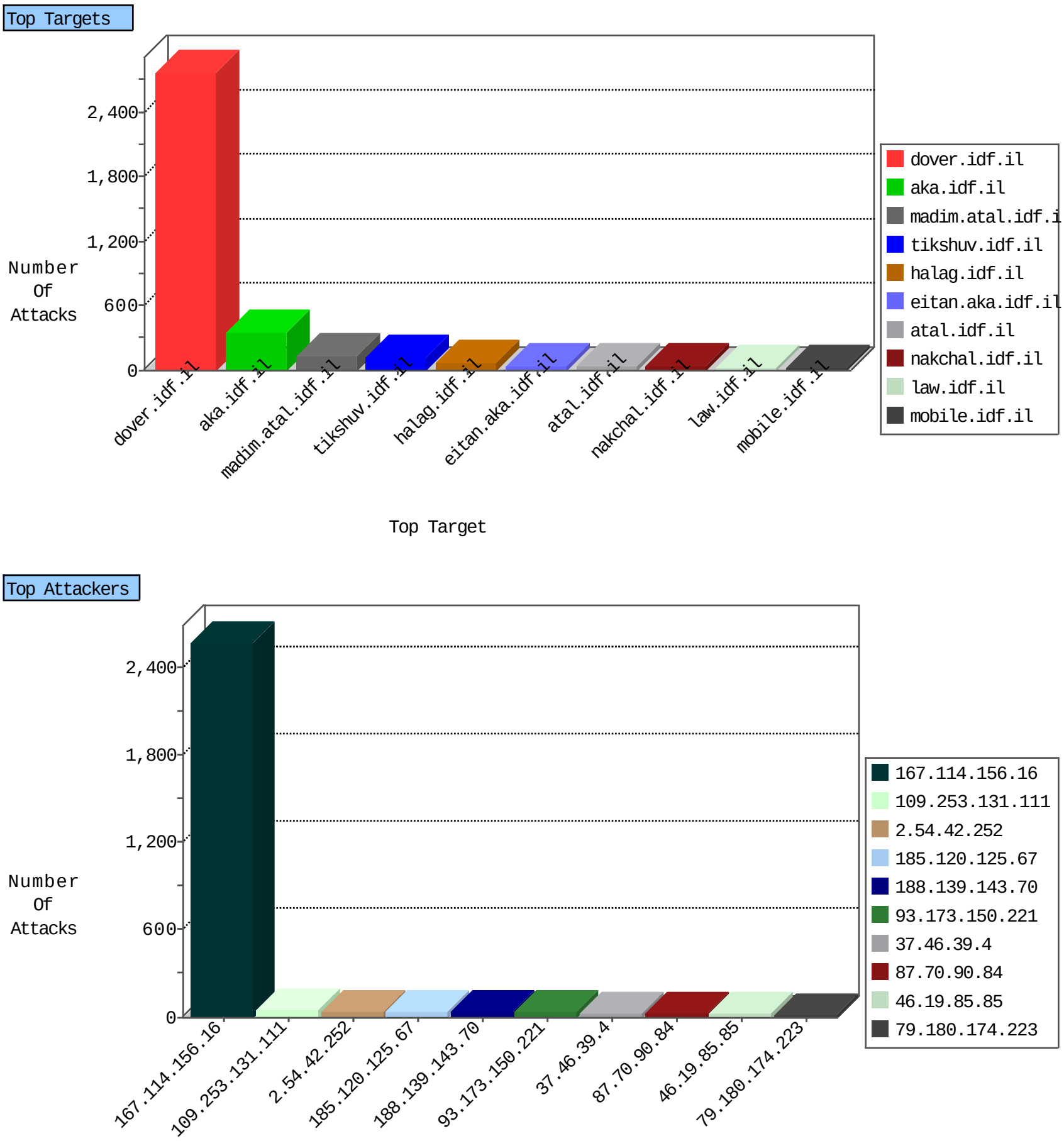
03-15-2016-20:04:05 to 03-15-2016-21:04:05

IDF Under Attack
Daily Report



03-15-2016-20:04:05 to 03-15-2016-21:04:05

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	3576
81.218.65.210	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
104.239.173.81		147.237.8.50	e.tikshuv.idf.il	Invalid L4 Header Length	drop	1
54.72.182.187	Ireland	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	1
89.248.160.138	Netherlands	147.237.8.50	e.tikshuv.idf.il	Block_Ntp_All_Net	drop	1
109.239.58.41	Germany	147.237.8.14	e.orchot.idf.il	Invalid TCP Flags	drop	1
66.249.78.146	Israel	147.237.72.166	aka.idf.il	HTTP-Misc-BadBlue-Dir-Trave-2	dest-reset	1
89.248.160.138	Netherlands	147.237.76.86	navy.idf.il	Block_Ntp_All_Net	drop	1
104.196.19.51	United States	147.237.76.44	e.refuah.idf.il	Invalid TCP Flags	drop	1
89.248.160.138	Netherlands	147.237.0.16	my-kosher-kravi.idf.il	Block_Ntp_All_Net	drop	1

03-15-2016-20:04:05 to 03-15-2016-21:04:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.179.205.96	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	16
79.181.116.37	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	12
87.69.92.219	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	11
5.29.131.173	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
106.38.241.149	China	147.237.77.216	dover.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	8
5.29.70.72	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
85.64.131.110	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
213.8.145.99	Israel	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
37.26.149.232	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
96.47.2.10	United States	147.237.77.74	law.idf.il	5670: HTTP: SQL Injection (SELECT)	Block	4
79.183.192.171	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
217.132.110.134	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
149.78.57.192	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
104.197.218.202	United States	147.237.77.170	maarachot.idf.il	19813: HTTP: WordPress Theme Divi Directory Traversal Vulnerability	Block	1
106.38.241.106	China	147.237.72.166	aka.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1
177.185.192.77	Brazil	147.237.0.34	tikshuv.idf.il	6134: HTTP: SQL Injection Variable Declaration Evasion	Block	1

03-15-2016-20:04:05 to 03-15-2016-21:04:05

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
213.8.145.99	147.237.77.74	Israel	law.idf.il	SQL Injection - Select From	12
96.47.2.10	147.237.77.74	United States	law.idf.il	SQL Injection - Select From	6
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
177.185.192.77	147.237.0.34	Brazil	tikshuv.idf.il	SQL Injection - Select From	3
185.103.252.60	147.237.77.234		halag.idf.il	ET SCAN NMAP -sS window 1024	1
94.102.48.194	147.237.76.147	Netherlands	chinuch.aka.idf.il	ET SCAN NMAP -sS window 1024	1
185.103.252.60	147.237.77.216		dover.idf.il	ET SCAN Potential VNC Scan 5900-5920	1
59.45.79.117	147.237.77.234	China	halag.idf.il	ET SCAN Potential SSH Scan	1
185.72.179.221	147.237.77.233		atal.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.76.202	China	e.halag.idf.il	ET SCAN Potential SSH Scan	1
185.72.179.221	147.237.77.226		www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 1024	1
59.45.79.117	147.237.0.200	China	m4u.idf.il	ET SCAN Potential SSH Scan	1
185.72.179.221	147.237.77.179		e.mazi.idf.il	ET SCAN Potential SSH Scan	1
218.246.0.97	147.237.77.212	China	e.dover.idf.il	ET SCAN NMAP -sS window 1024	1
109.235.254.181	147.237.77.179	Turkey	e.mazi.idf.il	ET SCAN NMAP -sS window 3072	1
101.226.166.221	147.237.72.166	China	aka.idf.il	portscan: TCP Distributed Portscan	1
188.27.185.170	147.237.77.216	Romania	dover.idf.il	portscan: TCP Distributed Portscan	1
94.102.48.194	147.237.76.177	Netherlands	ncore.idf.il	ET SCAN NMAP -sS window 1024	1
185.103.252.60	147.237.77.226		www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 1024	1
77.126.169.158	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
185.92.72.82	147.237.72.166		aka.idf.il	ET SCAN NMAP -sS window 1024	1
59.45.79.117	147.237.77.19	China	law-forum.idf.il	ET SCAN Potential SSH Scan	1
185.72.179.221	147.237.77.227		e.hamaz.idf.il	ET SCAN Potential SSH Scan	1
59.45.79.117	147.237.76.198	China	e.yohalan.idf.il	ET SCAN Potential SSH Scan	1
185.72.179.221	147.237.77.205		prisha.idf.il	ET SCAN Potential SSH Scan	1
37.46.39.217	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
185.72.179.221	147.237.77.176		matpash.idf.il	ET SCAN NMAP -sS window 1024	1
218.246.0.97	147.237.77.235	China	sviva.idf.il	ET SCAN NMAP -sS window 1024	1
109.235.254.181	147.237.77.179	Turkey	e.mazi.idf.il	ET SCAN NMAP -sS window 4096	1
218.246.0.97	147.237.77.121	China	e.navy.idf.il	ET SCAN NMAP -sS window 1024	1
109.65.162.145	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1

03-15-2016-20:04:05 to 03-15-2016-21:04:05

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
185.120.125.67		147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	38
93.173.150.221	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	35
46.19.85.85	Israel	147.237.76.31	nakchal.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	24
156.169.192.178		147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	19
46.19.86.234	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
212.76.110.148	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
46.19.85.6	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	18
188.139.143.70	Syrian Arab Republic	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	18
188.139.143.70	Syrian Arab Republic	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	18
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	18
2.54.162.86	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
37.46.39.217	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
87.71.29.93	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
87.69.92.254	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
46.19.85.61	Israel	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	9
46.19.86.69	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.116.56.236	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	8
79.180.174.223	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence		monitor	8
2.54.144.4	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
61.2.161.213	India	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
77.126.51.114	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.176.28	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.26.149.244	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
79.181.135.68	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.58	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.42.252	Israel	147.237.0.19	madim.atal.idf.i	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
79.183.172.78	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.53.19.20	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
176.13.1.10	Israel	147.237.0.19	madim.atal.idf.i	Bad TCP sequence	Invalid ACK number	monitor	6
192.114.105.254	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	5
80.241.219.45	Germany	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
2.52.165.139	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
46.19.86.116	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
50.101.170.111	Canada	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Checksum	Invalid checksum. Packet dropped.	drop	5
46.19.85.61	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
37.46.39.4	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
79.180.174.223	Israel	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
46.117.245.151	Israel	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
46.121.146.104	Israel	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
109.253.129.181	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
213.8.204.44	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
61.2.161.213	India	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
2.54.39.157	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
178.63.105.85	Germany	147.237.77.179	e.mazi.idf.il	drop	SAM rule	drop	4
31.154.190.15	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	4
98.19.222.133	United States	147.237.76.42	refuah.idf.il	drop	SAM rule	drop	4
79.180.174.223	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
37.46.39.4	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
79.180.174.223	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
109.253.131.111	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	53
2.54.42.252	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	34
37.46.39.4	Israel	147.237.0.34	tikshuv.idf.il	Automated Vulnerability Scanning V1	Block	22
109.253.140.90	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
79.179.26.247	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	5
79.181.202.210	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
2.52.131.174	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
104.162.149.104	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	3
109.67.26.57	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
87.70.90.84	Israel	147.237.72.166	aka.idf.il	Multiple NULL Character in Method from 87.70.90.84	Block	2
192.241.184.243	United States	147.237.76.31	nakchal.idf.il	Multiple Unauthorized URL Access from 192.241.184.243	Block	2
142.76.1.62	Canada	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 142.76.1.62	Block	2
87.70.90.84	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in Method from 87.70.90.84	Block	2
5.28.172.45	Israel	147.237.77.170	maarachot.idf.il	Unauthorized HTTP Method	Block	2
80.246.133.6	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
134.191.232.70	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
87.70.90.84	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
95.86.117.31	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 95.86.117.31	Block	2
5.29.51.154	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
2.52.20.154	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
87.70.90.84	Israel	147.237.72.166	aka.idf.il	Multiple Abnormally Long Request from 87.70.90.84	Block	1
2.54.143.250	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
134.191.232.72	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
87.70.90.84	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in Header Name	Block	1
95.86.117.31	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/pniotfindanswer.aspx&sa=u&ved=0ahukewis1z-up8plahwb_ywkhu7cdwuqjbaifw&usg=afqjcnhitw6sqodmeneoj2dvwbdz6bt4qa	Block	1
66.249.78.248	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/0/size100x0/3250.jpg	Block	1
87.70.90.84	Israel	147.237.72.166	aka.idf.il	Illegal HTTP Version	Block	1
5.29.236.123	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl69 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
85.65.116.235	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
134.191.232.68	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
87.70.90.84	Israel	147.237.72.166	aka.idf.il	Unknown HTTP Request Method ö[[#27]]#[[#18]][[#23]]>ˆw[[#12]][[#12]]wóÇĬqÕc`®Ë[[#25]]‹ko‘ [r[[#12]]55„5°˜g[[#0]]UÐš in URL ~p•m¸›[[#18]]•goe\z[[#19]]、[[#31]]+"Ê«\wp[[#6]]½[[#14]]×"#mj•`”-¸i2!z+•、„\¥•q[[#19]]}sf}ก•0¦2x0‰″[[#12]]}ak[[#23]]ƒm‹˜y„[[#27]]œd¡"²f·]]#21[[-″s’.]]#26[[‘]]#21[[	Block	1
77.75.76.160	Czech Republic	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/page/3/	Block	1
38.111.147.84	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-he	Block	1
87.70.90.84	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in Header Name from 87.70.90.84	Block	1
5.28.172.45	Israel	147.237.77.170	maarachot.idf.il	Multiple Unauthorized URL Access from 5.28.172.45	Block	1
87.70.90.84	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in Header Value	Block	1
79.183.185.125	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
66.249.79.162	Israel	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/	Block	1
87.70.90.84	Israel	147.237.72.166	aka.idf.il	Multiple Unknown HTTP Request Method from 87.70.90.84	Block	1
87.70.90.84	Israel	147.237.72.166	aka.idf.il	Malformed HTTP Header Line 1	Block	1
31.154.190.15	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
192.241.184.243	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to www.nakhal.idf.il/templates/shared/usercontrols/headerupper/	Block	1
134.191.232.69	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
87.70.90.84	Israel	147.237.72.166	aka.idf.il	Abnormally Long Header Line request header name	Block	1
2.54.4.46	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	1
87.70.102.246	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/nekudot/index	Block	1
46.19.86.58	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
142.76.1.62	Canada	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-he	Block	1
87.70.90.84	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in Method ö[[#27]]#[[#18]][[#23]]>ˆw[[#12]][[#12]]wóÇĬqÕc`®Ë[[#25]]‹ko‘ [r[[#12]]55„5°˜g[[#0]]UÐš	Block	1