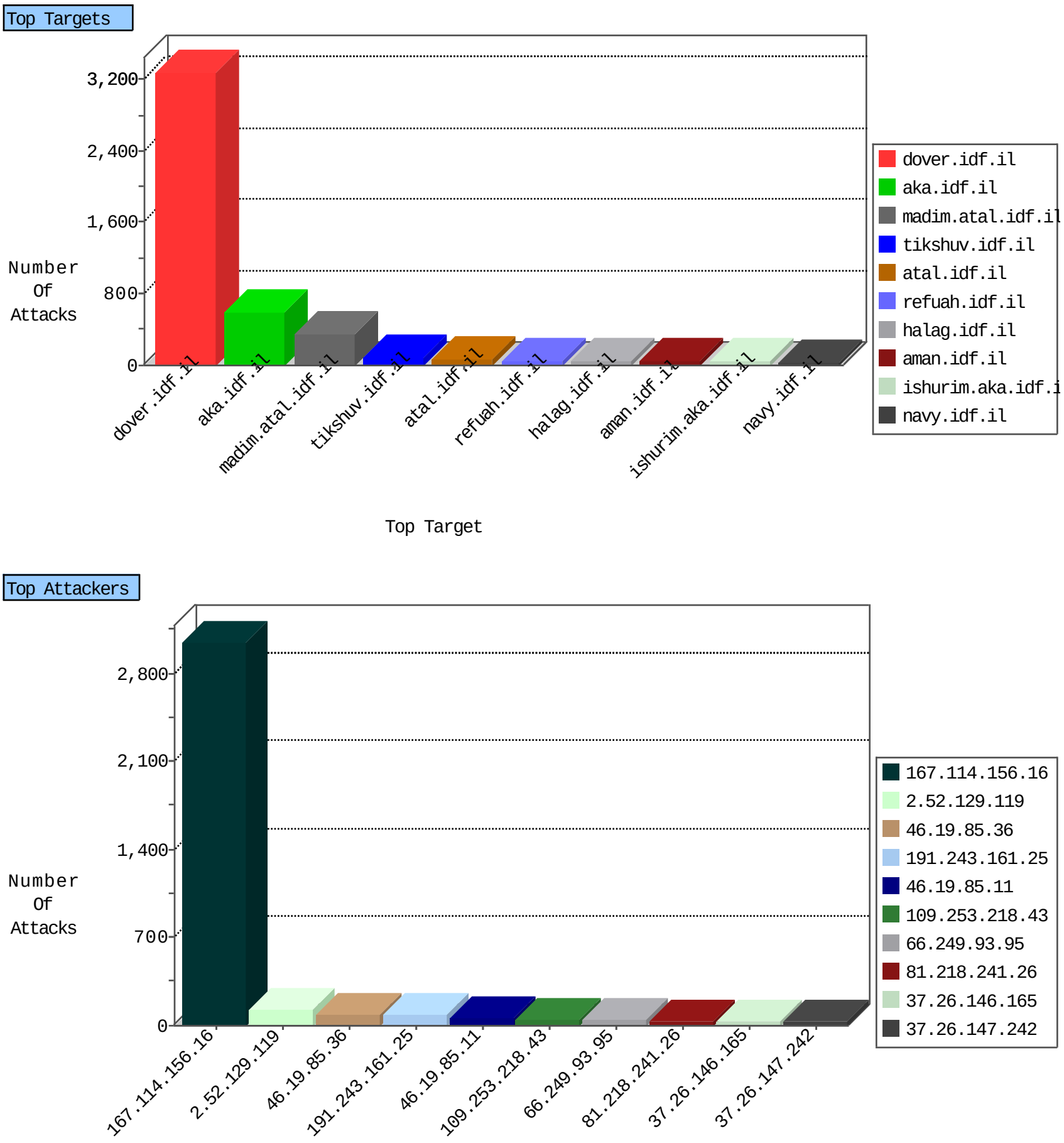
03-14-2016-18:04:08 to 03-14-2016-19:04:08

IDF Under Attack Daily Report



03-14-2016-18:04:08 to 03-14-2016-19:04:08

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	3797
81.218.241.26	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	198
81.218.65.210	Israel	147.237.0.34	tikshuv.idf.il	Block_Udp_All_Nets	drop	3
66.249.75.223	Israel	147.237.77.170	maarachot.idf.il	TCP handshake violation, first packet not syn	drop	1

03-14-2016-18:04:08 to 03-14-2016-19:04:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.121.153.250	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	23
84.94.47.122	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	12
213.151.37.164	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	9
5.29.213.64	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
109.67.131.45	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
62.210.107.201	France	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	4
69.30.215.122	United States	147.237.72.166	aka.idf.il	C1000074: HTTP: majestic bot	Block	3
109.64.59.4	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
5.22.135.129	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
69.30.215.122	United States	147.237.76.86	navy.idf.il	C1000074: HTTP: majestic bot	Block	2
69.30.215.122	United States	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
149.88.200.71	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
84.108.204.4	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
207.46.13.69	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
157.55.39.122	United States	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1

03-14-2016-18:04:08 to 03-14-2016-19:04:08

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
66.249.93.95	147.237.77.233	United States	atal.idf.il	ET SCAN NMAP -sA (2)	44
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
80.178.148.59	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
218.246.0.97	147.237.76.177	China	ncore.idf.il	ET SCAN NMAP -sS window 1024	1
193.105.134.220	147.237.76.86	Sweden	navy.idf.il	ET SCAN NMAP -sS window 1024	1
46.19.85.175	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
185.72.179.221	147.237.76.42		refuah.idf.il	ET SCAN NMAP -sS window 1024	1
13.75.88.135	147.237.76.202	United States	e.halag.idf.il	ET SCAN NMAP -sS window 1024	1
154.16.138.35	147.237.77.212	Mauritius	e.dover.idf.il	ET SCAN NMAP -f -sS	1
149.78.105.92	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
94.102.48.194	147.237.77.176	Netherlands	matpash.idf.il	ET SCAN NMAP -sS window 1024	1
93.189.26.18	147.237.77.61	Austria	e.cogat.idf.il	ET SCAN NMAP -sS window 1024	1
81.218.241.26	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
218.246.0.97	147.237.76.196	China	e.sviva.idf.il	ET SCAN NMAP -sS window 1024	1
74.208.238.221	147.237.0.15	United States	kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
62.219.167.198	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
185.120.125.20	147.237.72.166		aka.idf.il	portscan: TCP Distributed Portscan	1
40.121.136.51	147.237.76.176	United States	test.ncore.idf.il	ET SCAN NMAP -sS window 1024	1
154.16.138.35	147.237.77.212	Mauritius	e.dover.idf.il	ET SCAN NMAP -sS window 2048	1
149.88.123.252	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
109.67.103.109	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
93.189.26.18	147.237.77.226	Austria	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 1024	1
85.130.252.25	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

03-14-2016-18:04:08 to 03-14-2016-19:04:08

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	81
191.243.161.25	Brazil	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	33
191.243.161.25	Brazil	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	33
89.139.190.247	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	30
109.65.66.98	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	27
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	20
176.13.10.163	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
81.218.241.26	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	18
79.182.190.163	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
84.94.47.122	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	17
191.243.161.25	Brazil	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	15
46.19.86.201	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
176.13.16.247	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
37.26.148.245	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
5.102.252.92	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
46.19.85.128	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
109.67.119.172	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	11
46.19.86.105	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
37.26.146.165	Israel	147.237.72.167	ishurim.aka.idf.i	drop	First packet isn't SYN	drop	9
149.50.24.36	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	8
212.179.214.113	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
185.32.179.114	Israel	147.237.72.166	aka.idf.il	SYN Attack		reject	7
212.179.214.113	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
37.26.146.165	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
87.71.30.109	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.67.127.178	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
87.68.245.68	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
149.50.24.36	United States	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
79.176.107.147	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.46.38.40	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
109.65.101.59	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.176.237.247	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.64.183.141	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
207.46.13.53	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
5.22.135.149	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
141.8.132.112	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
188.120.154.135	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
46.19.85.200	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
176.13.18.174	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.65.138.67	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
217.132.22.4	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.177.159.184	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
37.26.146.165	Israel	147.237.72.167	ishurim.aka.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
185.13.195.199	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
195.171.188.162	United Kingdom	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid sequence number	monitor	6
178.63.105.85	Germany	147.237.77.179	e.mazi.idf.il	drop	SAM rule	drop	6
132.3.53.81	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
85.65.209.50	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5

03-14-2016-18:04:08 to 03-14-2016-19:04:08

Attacker Address	Attacker Country	Target Address	Site	**Signature**	Message	Device Action	Count
195.171.188.162	United Kingdom	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid sequence number	monitor	5

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.52.129.119	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	126
46.19.85.36	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	90
46.19.85.11	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	62
109.253.218.43	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	48
212.199.57.195	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	9
2.54.162.234	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	7
37.26.147.242	Israel	147.237.72.166	aka.idf.il	Multiple Unknown HTTP Request Method from 37.26.147.242	Block	4
37.26.147.242	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in Method from 37.26.147.242	Block	3
2.54.39.224	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
213.57.140.129	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
37.26.147.242	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in URL from 37.26.147.242	Block	2
37.26.147.242	Israel	147.237.72.166	aka.idf.il	Multiple Malformed URL from 37.26.147.242	Block	2
176.13.13.140	Israel	147.237.0.17	m.my-kosher-kravi .idf.il	Multiple Illegal Parameter Encoding from 176.13.13.140	None	2
37.26.148.239	Israel	147.237.72.156	aman.idf.il	Untraceable SSL Sessions: Open Mode	None	2
176.13.15.137	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
66.249.65.115	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/shared/clientscripts/sa_swfobject.js	Block	1
37.26.147.242	Israel	147.237.72.166	aka.idf.il	Malformed URL [[ᴅ_'#29:u]]¸+[[8#]]₪ˈ—λ1=Š}y]]62#[[hᴐ‘7nu+zß•yÊ	Block	1
109.66.48.100	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
37.26.147.242	Israel	147.237.72.166	aka.idf.il	Abnormally Long Header Line request header name	Block	1
93.172.190.172	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https:/www.idf.il/	Block	1
89.138.228.189	Israel	147.237.76.42	refuah.idf.il	Distributed PHP Attempt	Block	1
37.26.147.242	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
197.115.74.47	Algeria	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/ar/'	Block	1
132.3.53.81	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
79.182.109.62	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
37.26.147.242	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in Query String on ,8+xjp”ɔr¸qe*[[#31]]v„ ×[[#0]]s’µv2Œ×[[#19]]ʃ ‰3Û••ûx-n=!·_zÛɲ4[[×#15[[©₪]]#27ɾ]] '!qb"j a×9₹ b[[ʋ#15´-k]]ᴐ[[62#]]ɲʏı¸Êλx”””¸tא%•ıt¸»¸'—^ɣ¨½¹]]82#[[„d bplº®¦[[#24]][[#14]][[#26]]ÞÊ‚t'	Block	1
109.64.52.163	Israel	147.237.77.233	atal.idf.il	Distributed PHP Attempt	Block	1
66.249.64.13	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/robots.txt	Block	1
37.26.148.239	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
5.30.165.138	United Arab Emirates	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
89.138.228.189	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/xmlrpc.php	Block	1
1.32.71.38	Malaysia	147.237.77.74	law.idf.il	PHP Attempt	Block	1
83.110.18.104	United Arab Emirates	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	1
37.26.147.242	Israel	147.237.72.166	aka.idf.il	NULL Character in Header Name at ªÞ2!&Âl²¿7Ëé[[#4]]÷dó¢[[#24]]ê&¦¤¦_S„v!gš¸ºD[[#28]]•Èo–ªÿ HµwNGŸ ëBÔS÷H¦[[[#2]]•PŒy;¨Ë‰BÑÜÐKºH[[#2]][çõBë[[#28]]MŠâ…•¾[[#6]]Ïèá×[[#11]]˜SknÛÆD[[#15]]œNOMy©Àf_C«öEo[[#7]]£¥ÚD[[#19]]*µn•N¦[[#7]]Ä =¹[[#18]]°¬Œ[[#6]]•\9@%n\±iýo[[#5]]ÕM[[#17]]•”bwÌPë-2[[#30]]&D[[#1]]„t¬[[#0]]•y-^P£aÖqlž#011”ÇÉ[[#16]]Š•(_[[#21]]•ë/rL)…[[#26]]¡•{[[# 25]][[#4]]~€2P#012•›¥]š'ñ£TRpoIñr»[[#6]]äÿ6êÁ=ÿu[[#22]]¸[[#7]]•›“$ €[[#0]][[#19]]³Hƒ&¼§qÍYü«É[[#11]]Á™—[[#17]][[#15]]á	Block	1
176.13.18.174	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
66.249.65.118	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/shared/clientscripts/jquery.plugins/jquery.scrollfollow.js	Block	1
37.26.147.242	Israel	147.237.72.166	aka.idf.il	Multiple Abnormally Long Header Line from 37.26.147.242	Block	1
109.67.119.172	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
37.26.147.242	Israel	147.237.72.166	aka.idf.il	Abnormally Long Request method	Block	1
94.230.95.82	Israel	147.237.76.42	refuah.idf.il	Distributed PHP Attempt	Block	1
89.138.228.189	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/xmlrpc.php	Block	1
37.26.148.133	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
197.239.5.27	Uganda	147.237.77.216	dover.idf.il	SSL Untraceable Connection - Open Mode	None	1
149.88.228.69	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
80.72.9.5	Sweden	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1497	Block	1
66.249.64.131	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/sip_storage/files/3/69383.pdf	Block	1
37.26.147.242	Israel	147.237.72.166	aka.idf.il	Illegal HTTP Version	Block	1
109.64.52.163	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to www.atal.idf.il/xmlrpc.php	Block	1
37.142.210.54	Israel	147.237.77.233	atal.idf.il	Distributed Unauthorized URL Access on 147.237.77.233/1134-he/atal.aspx	Block	1
217.69.133.243	Russian Federation	147.237.72.166	aka.idf.il	Unknown Parameter sidescroll in aka.idf.il/giyus/leshakot/	None	1