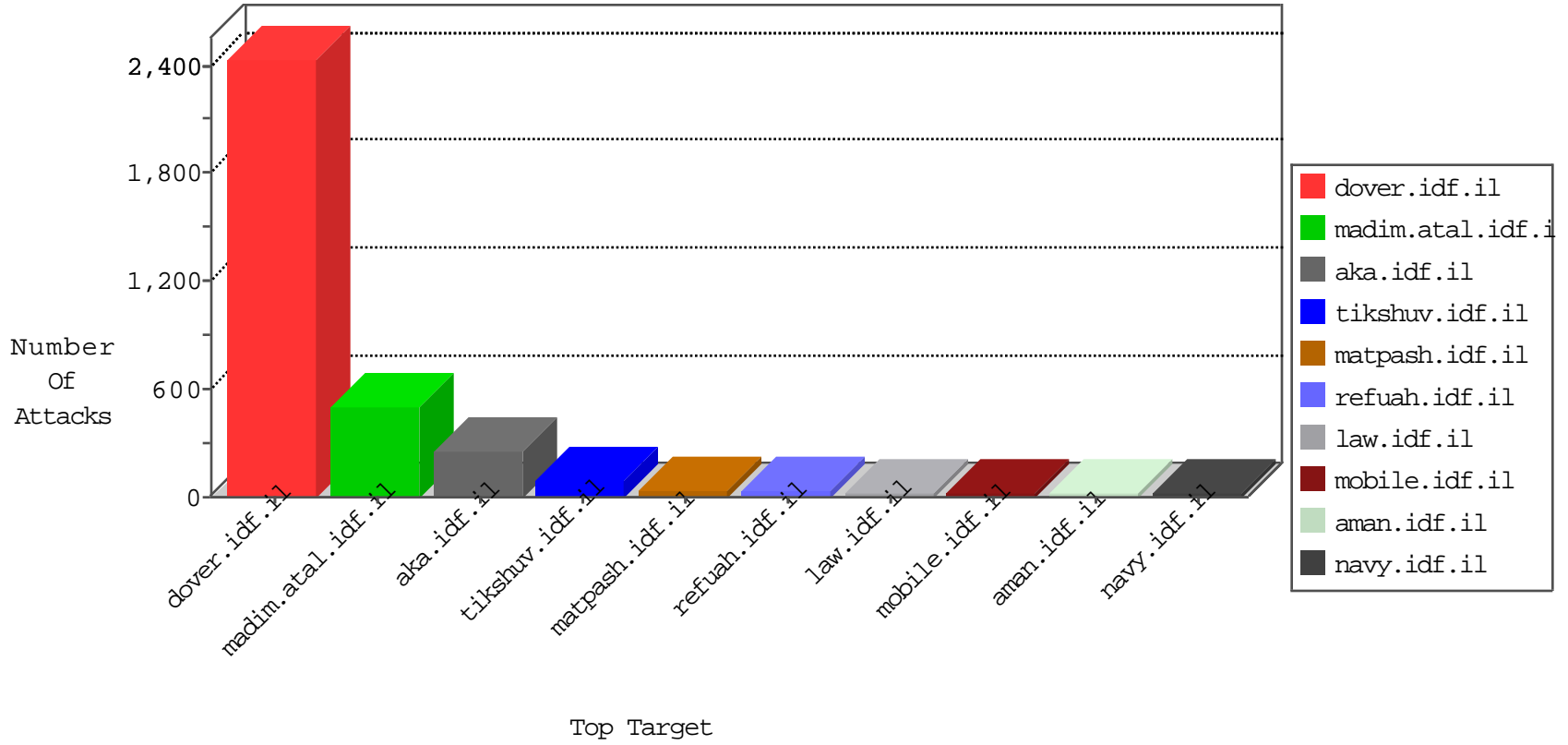


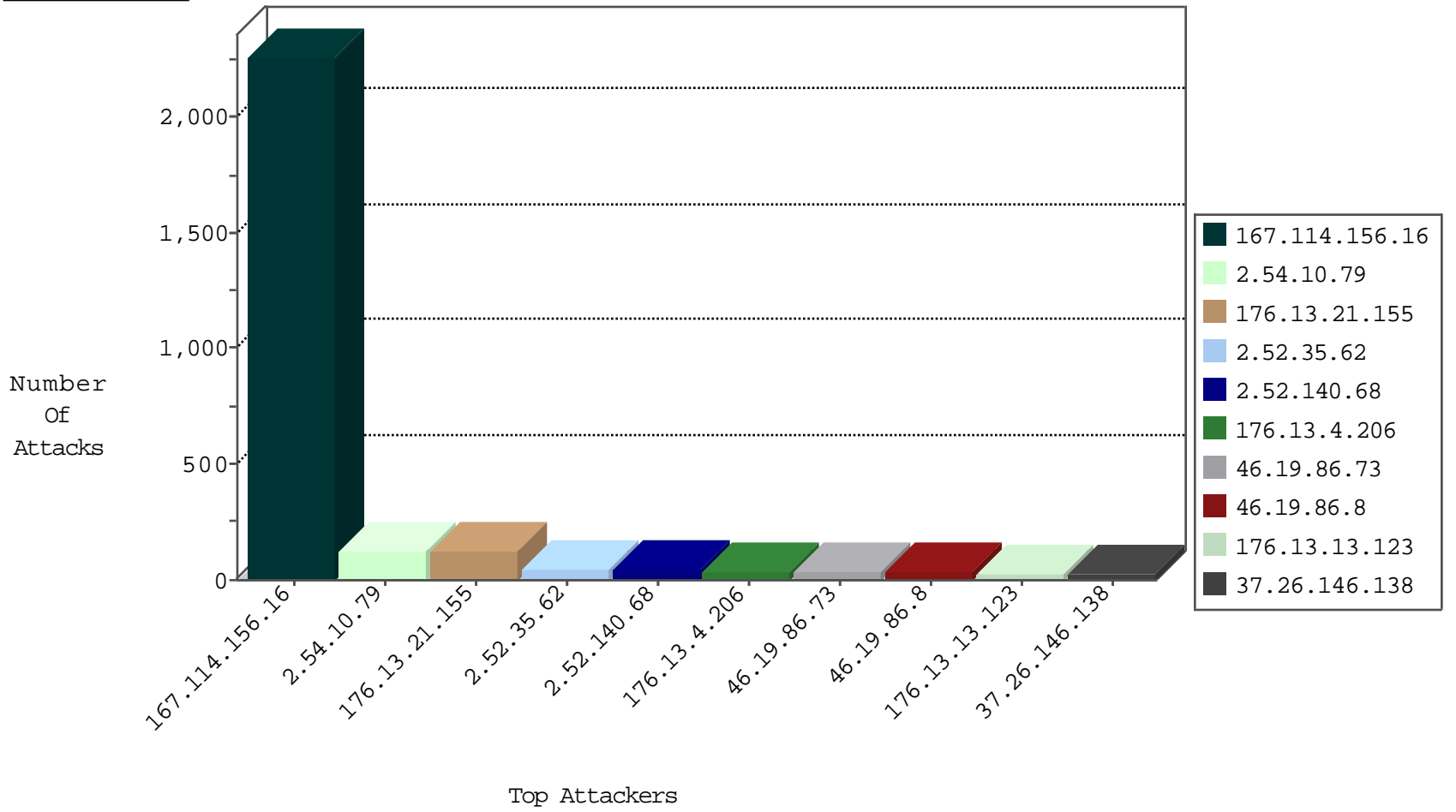
IDF Under Attack Daily Report



Top Targets



Top Attackers



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	3860
81.218.65.210	Israel	147.237.0.34	tikshuv.idf.il	Block_Udp_All_Nets	drop	6
107.167.108.62	United States	147.237.77.176	matpash.idf.il	Frk_Purple_Con_Limit_Http	drop	3
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	1
61.93.40.124	Hong Kong	147.237.76.39	mobile.meitav.idf.il	Block_Udp_All_Nets	drop	1
107.167.108.62	United States	147.237.77.176	matpash.idf.il	Frk_Under_Attack_Con_Http	drop	1
134.119.17.5	Germany	147.237.76.44	e.refuah.idf.il	Invalid L4 Header Length	drop	1

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
2.54.3.159	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
95.86.109.39	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
212.179.185.50	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
81.218.65.218	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	6
2.52.34.102	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	4
66.249.93.242	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
66.249.93.244	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
2.54.168.51	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
31.31.73.93	Czech Republic	147.237.0.34	tikshuv.idf.il	C1000074: HTTP: majestic bot	Block	2
46.165.197.141	Germany	147.237.77.176	matpash.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
79.176.103.13	Israel	147.237.72.166	aka.idf.il	C1000008: HTTP: Xenu UserAgent	Block	1

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
37.8.23.71	147.237.77.176	Palestinian Territory, Occupied	matpash.idf.il	ET SCAN NMAP -sA (2)	15
84.110.32.186	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
82.81.193.82	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
71.217.126.12	147.237.76.86	United States	navy.idf.il	ET SCAN NMAP -sA (2)	1
46.116.19.176	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
220.178.78.138	147.237.8.28	China	e.mobile-ks.idf.il	ET SCAN NMAP -sS window 4096	1
31.154.159.210	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	1
167.114.156.16	147.237.77.216	Canada	dover.idf.il	portscan: TCP Distributed Portscan	1
94.102.48.194	147.237.76.196	Netherlands	e.sviva.idf.il	ET SCAN NMAP -sS window 1024	1
94.102.48.194	147.237.76.31	Netherlands	nakchal.idf.il	ET SCAN NMAP -sS window 1024	1
84.94.67.209	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
81.218.204.22	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
62.90.178.17	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
199.203.63.231	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
2.54.2.64	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
171.101.237.67	147.237.8.28	Thailand	e.mobile-ks.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
149.78.123.128	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
94.102.48.194	147.237.76.34	Netherlands	yohalan.idf.il	ET SCAN NMAP -sS window 1024	1

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	38
176.13.13.123	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	27
79.182.190.163	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
109.253.132.168	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	15
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	12
185.120.125.42		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	11
194.31.58.8	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
85.130.223.17	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
62.0.251.1	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	8
85.130.223.17	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
46.19.85.76	Israel	147.237.76.31	nakchal.idf.il	drop	First packet isn't SYN	drop	7
185.32.179.110	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
37.26.149.206	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.165	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
149.78.227.36	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
109.67.9.108	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
185.32.179.110	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.253.192.126	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.108	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
62.0.200.163	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
2.54.4.80	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack		reject	5
46.19.85.165	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
2.54.4.80	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
185.3.147.167	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
2.54.4.80	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	5
185.32.179.110	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	5
2.54.4.80	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
46.210.240.196	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	5
2.54.4.80	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
46.19.85.181	Israel	147.237.0.34	tikshuv.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
82.80.63.203	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
185.32.179.110	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
62.0.251.1	Israel	147.237.77.226	www.chamatz.aka.idf.il	drop	First packet isn't SYN	drop	4
195.200.205.2	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
82.81.30.208	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
46.19.85.172	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
2.54.172.205	Israel	147.237.77.216	dover.idf.il	SYN Attack		reject	4
2.54.172.205	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
79.180.153.121	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
192.117.49.194	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
62.90.235.190	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.67.246.239	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
77.127.84.229	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
185.120.125.42		147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.54.32.6	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
31.210.187.177	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.198	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	3
81.218.139.152	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
2.54.10.79	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	123
176.13.21.155	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	120
2.52.35.62	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	44
176.13.4.206	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	37
46.19.86.73	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	34
46.19.86.8	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	33
2.52.140.68	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	31
37.26.146.138	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	25
2.52.168.104	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	23
185.120.126.74		147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	14
109.253.223.5	Israel	147.237.77.243	mobile.idf.il	Distributed Parameter Type Violation on mobile.idf.il/sachar/changepassword parameter CurrentPassword	Block	4
213.251.182.103	France	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/0/size220x0/3410.jpg.src	Block	3
176.13.6.101	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
61.5.70.36	Indonesia	147.237.77.74	law.idf.il	Parameter Type Violation PageNum in www.law.idf.il/285-he/patzar.aspx	Block	2
212.25.102.63	Israel	147.237.77.74	law.idf.il	Parameter Type Violation ? in www.mag.idf.il/163-he/patzar.aspx	Block	2
27.159.192.115	China	147.237.77.216	dover.idf.il	PHP Attempt	Block	2
27.159.192.115	China	147.237.77.74	law.idf.il	Distributed PHP Attempt	Block	2
212.76.122.243	Israel	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 212.76.122.243	Block	2
79.182.57.210	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	2
194.90.240.253	Israel	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 194.90.240.253	Block	2
46.19.85.134	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
37.26.146.240	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
83.110.231.168	United Arab Emirates	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
79.178.144.63	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/himush/site/he/himush.asp	Block	1
5.102.254.191	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
169.229.3.91	United States	147.237.0.34	tikshuv.idf.il	Unknown HTTP Request Method [[#16]]µý+iJ[[#2]]ÔjûW in URL *[[#17]]x+{h[[#0]]}[[#30]]3[[#4]]x[[#8]]1#[[#5]]• '[[#2#]]µ	Block	1
169.229.3.91	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Illegal Byte Code Character in URL	Block	1
128.52.128.105	United States	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/71929-he/ctl00_ucsidebar_rptcategories_ctl00_spcode tails_rptsubcategories_ctl00_innerlevelcontainer	Block	1
37.26.149.206	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
169.229.3.91	United States	147.237.72.167	ishurim.aka.idf.il	Illegal Byte Code Character in Method	Block	1
79.180.150.131	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00\$ctl00\$cphMain\$cphSachar\$ctl187 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
169.229.3.91	United States	147.237.0.34	tikshuv.idf.il	Illegal Byte Code Character in URL *[[#17]]x+{h[[#0]]}[[#30]]3[[#4]]x[[#8]]1#[[#5]]• '[[#2#]]µ	Block	1
66.249.78.51	Israel	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to 147.237.77.170/robots.txt	Block	1
195.200.205.66	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/scripts/css3pie.htc	Block	1
157.55.39.117	United States	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/templates/departmentslobby/departmentslobby.aspx	Block	1
37.26.148.136	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
176.13.21.97	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
83.110.231.168	United Arab Emirates	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/xmlrpc.php	Block	1
79.178.179.208	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in URL	Block	1
169.229.3.91	United States	147.237.72.166	aka.idf.il	Multiple Abnormally Long Request from 169.229.3.91	Block	1
169.229.3.91	United States	147.237.0.17	m.my-kosher-kravi.idf.il	Multiple Illegal Byte Code Character in Method from 169.229.3.91	Block	1
61.5.70.36	Indonesia	147.237.77.74	law.idf.il	Parameter Type Violation PageNum in www.mag.idf.il/487-he/patzar.aspx	Block	1
141.212.122.145	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to 147.237.77.176/	Block	1
37.46.39.158	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to www.refua.atal.idf.il/1345-he/refuah.aspx	Block	1
194.6.255.4	Qatar	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/894-ar	Block	1
27.159.192.115	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/xmlrpc.php	Block	1
169.229.3.91	United States	147.237.77.216	dover.idf.il	Abnormally Long Request method	Block	1
169.229.3.91	United States	147.237.0.34	tikshuv.idf.il	Illegal HTTP Version	Block	1
68.180.230.189	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1395-en/dover.aspx	Block	1
46.19.86.121	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1