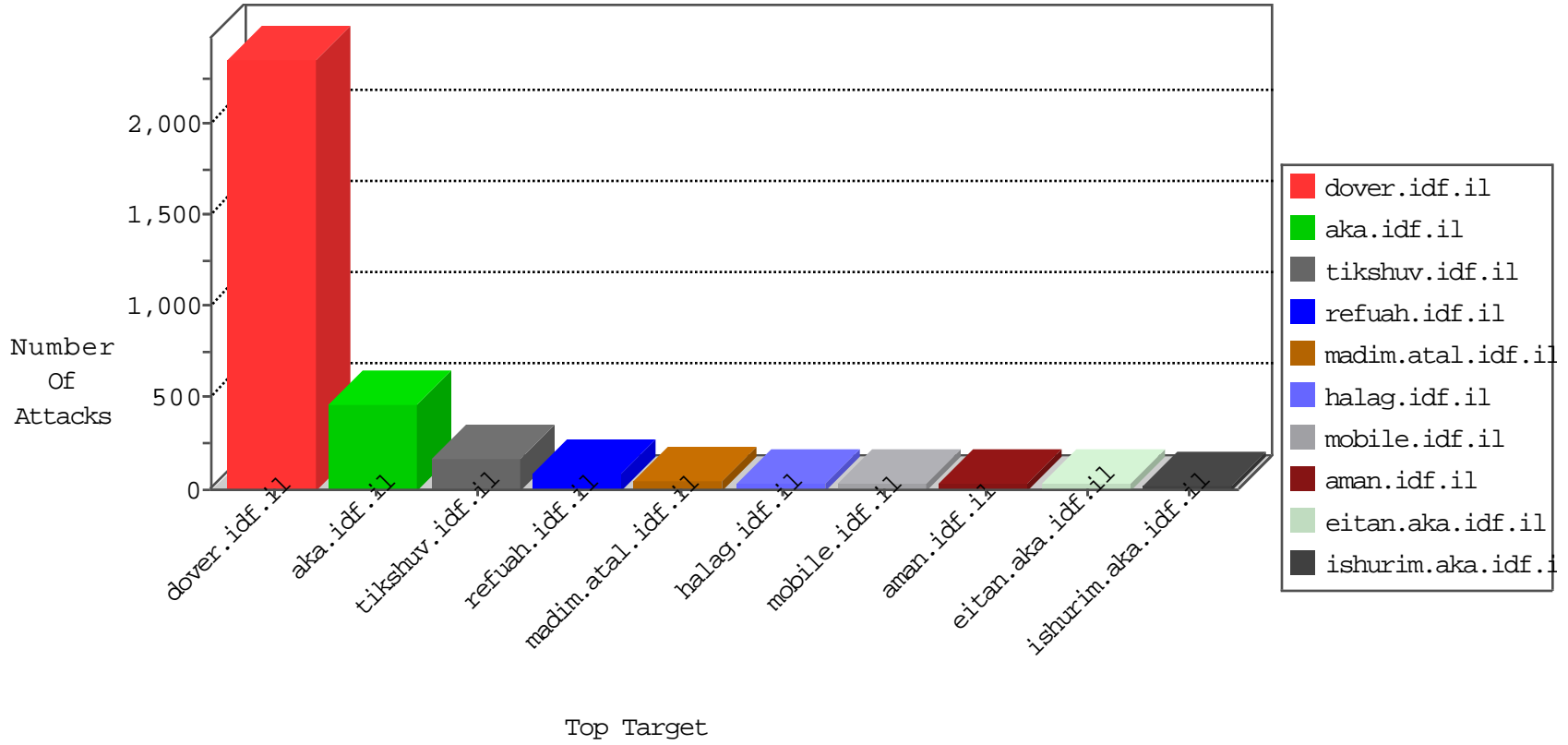


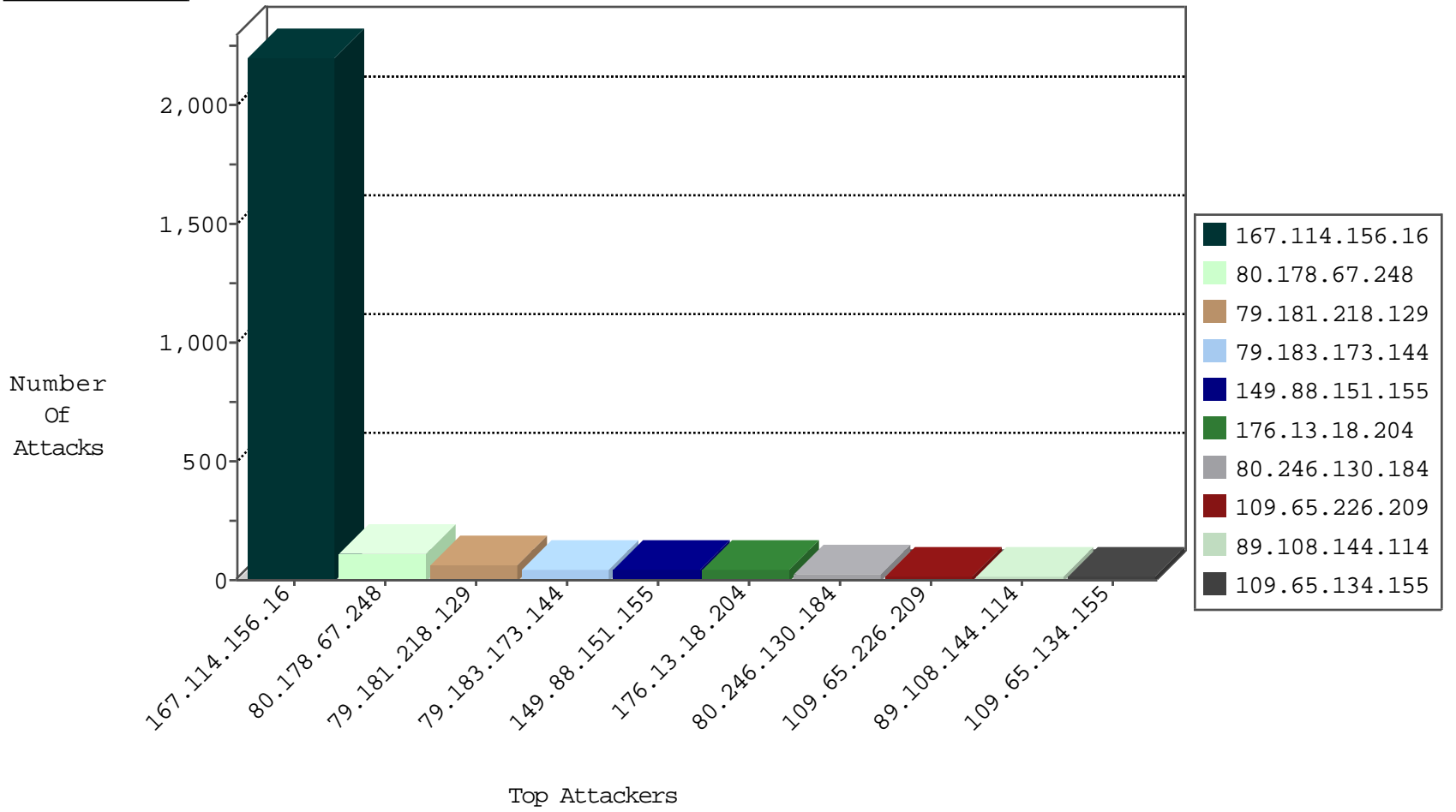
# IDF Under Attack Daily Report



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	3250
192.117.9.90	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	5
81.218.65.210	Israel	147.237.0.34	tikshuv.idf.il	Block_Udp_All_Nets	drop	3
81.218.65.210	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	3
10.33.252.254		147.237.77.216	dover.idf.il	SYN Flood out of context	drop	2
82.145.218.194	Europe	147.237.77.216	dover.idf.il	Block_Ip_Web_In	drop	1
41.130.6.65	Egypt	147.237.77.176	matpash.idf.il	TCP handshake violation, first packet not syn	drop	1
85.159.216.41	Jordan	147.237.77.216	dover.idf.il	TCP handshake violation, first packet not syn	drop	1

## Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
93.173.1.173	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	9
199.203.64.137	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
79.181.209.158	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	8
85.158.138.19	Germany	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	5
85.158.139.227	United Kingdom	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	3
84.111.13.67	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
136.243.5.215	Germany	147.237.77.216	dover.idf.il	C1000074: HTTP: majestic bot	Block	2
46.19.86.108	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
46.116.170.68	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	2
80.178.67.248	Israel	147.237.0.34	tikshuv.idf.il	C1000138: HTTP: prefix 1.01 in the URL	Block	1
106.120.173.159	China	147.237.77.233	atal.idf.il	C1000071: HTTP: User Agent Sogou+web+spider	Block	1

## Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
156.184.49.210	147.237.77.216		dover.idf.il	ET SCAN NMAP -sA (2)	5
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	2
212.143.79.186	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.116.19.95	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
46.19.85.218	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
98.119.105.221	147.237.76.148	United States	ggcenter.aka.idf.il	ET SCAN NMAP -sS window 2048	1
41.67.94.95	147.237.77.216	Egypt	dover.idf.il	portscan: TCP Distributed Portscan	1
94.102.48.194	147.237.77.19	Netherlands	law-forum.idf.il	ET SCAN NMAP -sS window 1024	1
5.160.14.250	147.237.0.17	Iran, Islamic Republic of	m.my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
93.189.26.18	147.237.76.34	Austria	yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
5.29.100.153	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
84.111.161.233	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
2.54.134.144	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
84.109.225.21	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
218.246.0.97	147.237.77.176	China	matpash.idf.il	ET SCAN NMAP -sS window 1024	1
82.166.214.228	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
213.57.254.225	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
62.90.100.214	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.19.86.204	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
149.78.183.136	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.19.85.170	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
98.119.105.221	147.237.76.148	United States	ggcenter.aka.idf.il	ET SCAN NMAP -f -sS	1
5.160.14.250	147.237.0.35	Iran, Islamic Republic of	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
93.189.26.18	147.237.76.44	Austria	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	1
5.102.216.217	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
87.69.86.186	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
2.54.173.196	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
84.110.109.87	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
2.52.146.65	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
84.108.245.37	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
218.246.0.97	147.237.77.170	China	maarachot.idf.il	ET SCAN NMAP -sS window 1024	1
80.246.139.49	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1

## Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
80.178.67.248	Israel	147.237.0.34	tikshuv.idf.il	drop	First packet isn't SYN	drop	109
79.181.218.129	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	67
149.88.151.155	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	42
176.13.18.204	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	30
80.246.130.184	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	26
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	19
176.13.10.161	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
109.65.134.155	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
79.182.21.197	Israel	147.237.0.34	tikshuv.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
109.65.226.209	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	12
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack		reject	11
37.26.149.231	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
79.181.123.7	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
108.61.123.86	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	8
89.108.144.114	Lebanon	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
89.108.144.114	Lebanon	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	7
37.26.147.144	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.46	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.67.49.231	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
176.13.18.204	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
87.70.39.137	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.183.193.120	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
109.65.226.209	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
192.116.231.161	Israel	147.237.77.170	maarachot.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.218	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.85.102	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
176.13.0.217	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
192.115.177.202	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
37.26.148.232	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
84.108.103.220	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
94.230.86.233	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
2.52.140.123	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
149.78.219.8	Israel	147.237.72.167	ishurim.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
85.158.138.19	Germany	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
176.13.1.60	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
37.46.39.66	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
2.54.50.22	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
66.249.93.250	Israel	147.237.76.202	e.halag.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	4
2.54.181.206	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
176.13.1.60	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
89.108.144.114	Lebanon	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	4
37.46.41.207	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
94.188.248.70	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
207.46.13.87	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
31.154.25.42	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
65.55.210.251	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
79.181.35.208	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
84.95.252.179	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
176.13.18.204	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	3

## Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
79.183.173.144	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	46
41.67.94.95	Egypt	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	5
2.52.146.36	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
37.26.148.232	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
176.13.17.208	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
2.54.16.43	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/hinuch	Block	2
197.166.75.148	Egypt	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	2
46.117.128.153	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/mainsachar	Block	2
37.26.149.231	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
80.246.139.18	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
37.26.146.211	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	2
41.67.94.95	Egypt	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	2
109.64.238.244	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in URL from 109.64.238.244	Block	1
83.130.104.122	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/https://www.idf.il/	Block	1
192.115.177.202	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$cphSachar\$ct183 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
66.249.69.84	Israel	147.237.77.74	law.idf.il	Illegal Parameter Encoding searchText in www.law.idf.il/275-he/patzar.aspx	None	1
149.88.151.155	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
87.69.99.191	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Open Mode	None	1
212.76.102.16	Israel	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	1
46.19.85.218	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
109.65.190.36	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/sip_storage/files/8/1668.doc	Block	1
84.94.56.72	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/giyus/www.navy.idf.il	Block	1
66.249.75.16	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/2/size100x0/2802.jpg	Block	1
37.26.149.192	Israel	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
157.55.39.49	United States	147.237.0.16	my-kosher-kravi.idf.il	Unauthorized URL Access to www.my-kosher-kravi.idf.il/	Block	1
87.70.60.114	Israel	147.237.72.156	aman.idf.il	Distributed Unauthorized URL Access on www.aman.idf.il/https://www.aman.idf.il/	Block	1
80.178.191.219	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized Method for Known URL on www.aka.idf.il/main/sachar/	Block	1
213.8.204.18	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$TochenPlaceHolder\$btnAtudaBack in www.aka.idf.il/main/giyus/atuda/asmachta.aspx	None	1
185.120.126.34		147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/sachar	Block	1
109.67.239.141	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
5.29.151.76	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
84.108.168.159	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/https://www.aman.idf.il/	Block	1
207.46.13.65	United States	147.237.0.34	tikshuv.idf.il	Parameter Type Violation catId in www.tikshuv.idf.il/site/contactus.aspx	Block	1
73.182.247.27	United States	147.237.77.216	dover.idf.il	NULL Character in Method	Block	1
157.55.39.193	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
87.71.5.136	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
80.246.130.184	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
213.254.241.7	United Kingdom	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$btnSearch in www.aka.idf.il/main/sachar/default.aspx	None	1
187.188.111.60	Mexico	147.237.0.17	m.my-kosher-kravi.idf.il	Unauthorized URL Access to 147.237.0.17/index.php	Block	1
66.249.64.131	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
118.193.163.150	China	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/shared/usercontrols/headerupper/	Block	1
31.154.175.79	Israel	147.237.77.234	halag.idf.il	Distributed Unauthorized URL Access on 147.237.77.234/images/shared/bullet1.gif	Block	1
85.65.191.205	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ct100\$ct100\$cphMain\$TochenPlaceHolder\$btnAtudaPrint in www.aka.idf.il/main/giyus/atuda/asmachta.aspx	None	1
78.154.170.2	Ukraine	147.237.72.166	aka.idf.il	Unknown Parameter amp;pagenum in www.aka.idf.il/iturim/asp/displayallsoldiers.asp	None	1
207.46.13.172	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/robots.txt	Block	1
176.13.8.192	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
109.64.238.244	Israel	147.237.72.166	aka.idf.il	Illegal Byte Code Character in URL /main/kapatz//res#012ources/images/innerpage/goback.gif	Block	1
216.218.207.138	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/1294-he/www.idf.il	Block	1
187.188.111.60	Mexico	147.237.0.19	madim.atal.idf.il	Unauthorized URL Access to 147.237.0.19/index.php	Block	1
66.249.65.174	Israel	147.237.77.233	atal.idf.il	Unauthorized URL Access to 147.237.77.233/1133-he/atal.aspx	Block	1