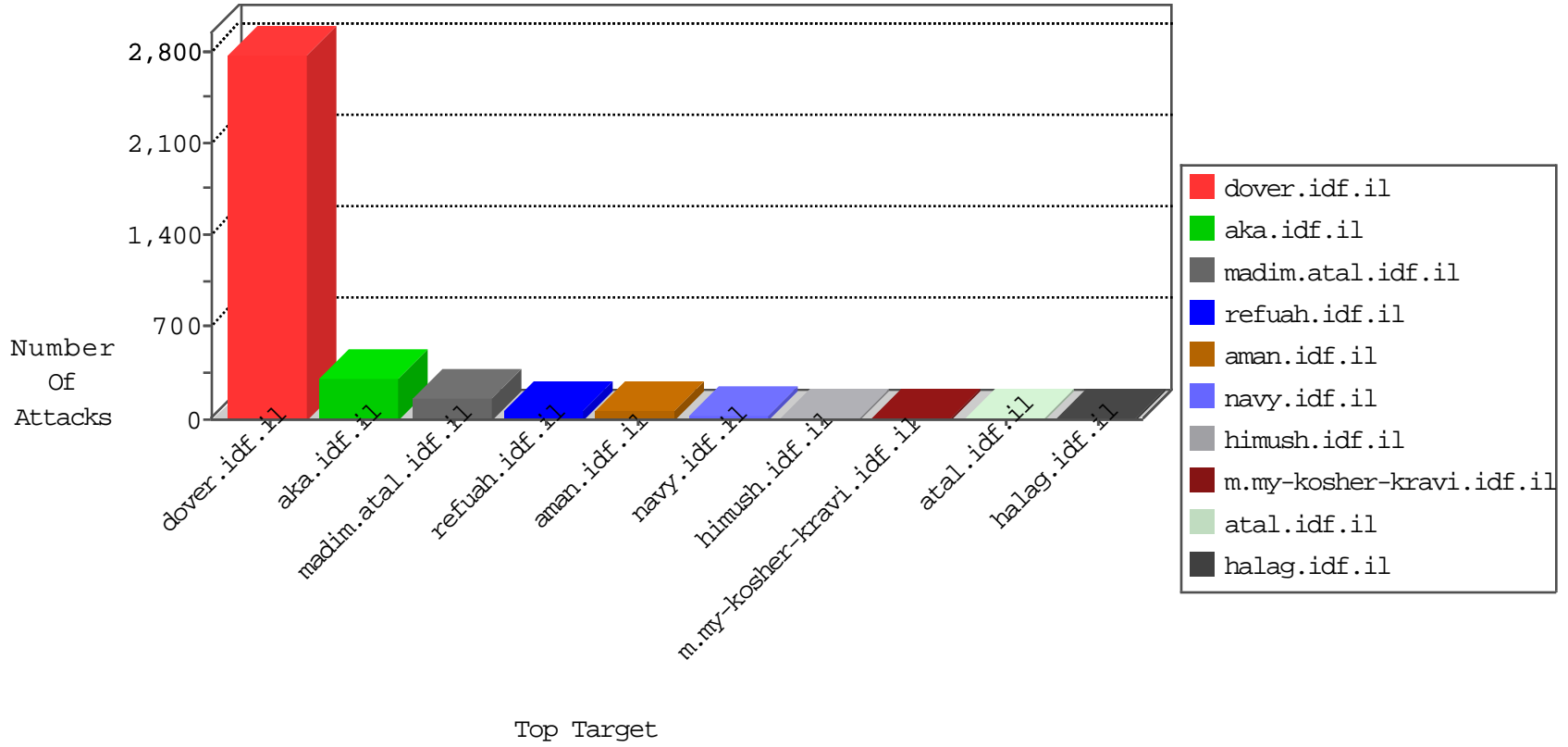


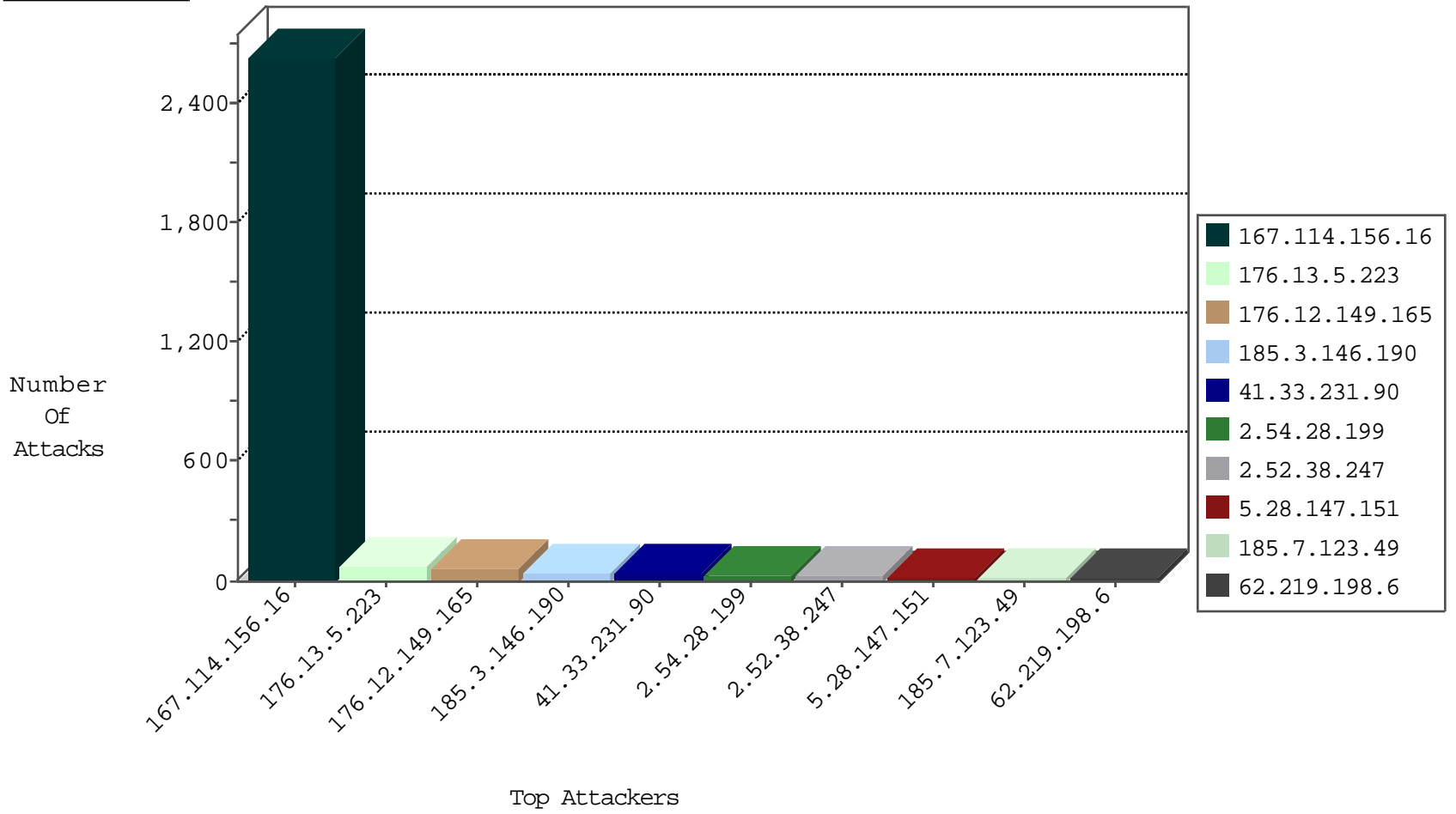
# IDF Under Attack Daily Report



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	3633
66.249.69.76	Israel	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	102
84.110.35.158	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	6
175.126.123.228	Korea, Republic of	147.237.76.38	e.e.meitav.idf.il	JLM_Under_Attack_Con_Tcp	drop	1
46.166.188.68	Netherlands	147.237.76.197	e.himush.idf.il	Block_Ntp_All_Net	drop	1
213.248.126.136	Europe	147.237.0.19	madim.atal.idf.il	Invalid TCP Flags	drop	1
46.166.188.68	Netherlands	147.237.76.198	e.yohalan.idf.il	Block_Ntp_All_Net	drop	1
115.230.124.164	China	147.237.77.216	dover.idf.il	block-sp-trafl	drop	1
62.90.174.63	Israel	147.237.76.34	yohalan.idf.il	Block_Udp_All_Nets	drop	1

## Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
91.12.70.251	Germany	147.237.72.166	aka.idf.il	C1000106: HTTP: majestic bot	Block	1
151.80.31.119	Italy	147.237.77.170	maarachot.idf.il	C228: HTTP: AhrefBot crawler	Block	1
194.114.146.227	Israel	147.237.77.216	dover.idf.il	C1000169: Block - dns poisoning (Clalit)	Permit	1

## Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	4
46.121.78.77	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
185.106.94.16	147.237.0.16		my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
39.81.84.46	147.237.0.15	China	kosher-kravi.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
183.61.109.189	147.237.72.217	China	e.idf.il	ET SCAN NMAP -sS window 1024	1
175.126.123.228	147.237.76.148	Korea, Republic of	ggcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
175.126.123.228	147.237.76.34	Korea, Republic of	yohalan.idf.il	ET SCAN Potential SSH Scan	1
175.126.123.228	147.237.0.200	Korea, Republic of	m4u.idf.il	ET SCAN Potential SSH Scan	1
209.126.116.147	147.237.76.34	United States	yohalan.idf.il	ET SCAN NMAP -sS window 1024	1
95.211.155.65	147.237.76.177	Netherlands	ncore.idf.il	ET SCAN Potential SSH Scan	1
89.163.140.142	147.237.0.34	Germany	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
190.36.168.200	147.237.0.15	Venezuela	kosher-kravi.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
66.249.66.1	147.237.72.166	United States	aka.idf.il	WEB-CGI redirect access	1
185.106.94.16	147.237.0.35		akaws.idf.il	ET SCAN NMAP -sS window 1024	1
43.229.53.89	147.237.0.17	Japan	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
183.61.109.189	147.237.72.217	China	e.idf.il	ET SCAN NMAP -sS window 4096	1
175.126.123.228	147.237.76.176	Korea, Republic of	test.ncore.idf.il	ET SCAN Potential SSH Scan	1
175.126.123.228	147.237.76.39	Korea, Republic of	mobile.meitav.idf.il	ET SCAN Potential SSH Scan	1
175.126.123.228	147.237.76.30	Korea, Republic of	himush.idf.il	ET SCAN Potential SSH Scan	1
175.126.123.228	147.237.0.17	Korea, Republic of	m.my-kosher-kravi.idf.il	ET SCAN Potential SSH Scan	1
209.126.116.147	147.237.0.35	United States	akaws.idf.il	ET SCAN NMAP -sS window 1024	1
89.163.140.142	147.237.76.147	Germany	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
194.114.146.227	147.237.77.216	Israel	dover.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
81.169.251.74	147.237.76.44	Germany	e.refuah.idf.il	ET SCAN NMAP -sS window 1024	1
185.106.94.16	147.237.76.201		e.atal.idf.il	ET SCAN Potential SSH Scan	1

## Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
185.3.146.190	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	23
185.3.146.190	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	alert	20
2.52.38.247	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	18
93.172.162.216	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	13
188.120.148.239	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
185.7.123.49	Palestinian Territory Occupied	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	9
94.230.86.230	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	9
46.19.86.34	Israel	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
5.28.147.151	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
185.7.123.49	Palestinian Territory Occupied	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
37.26.146.217	Israel	147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	7
5.28.147.151	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	7
37.26.146.217	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	7
2.54.28.199	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
2.54.28.199	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
188.122.254.208	Russian Federation	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
66.249.78.130	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.28.199	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
109.66.151.147	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
109.160.131.112	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
77.125.132.7	Israel	147.237.76.30	himush.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
2.54.28.199	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid sequence number	monitor	6
85.65.26.119	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	6
167.114.156.16	Canada	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	6
2.54.28.199	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
85.65.26.119	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
62.219.198.6	Israel	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
46.19.86.91	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
89.139.7.240	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	alert	5
46.19.86.167	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
5.102.254.192	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.86.102	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
89.139.7.240	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.125	Israel	147.237.72.166	aka.idf.il	drop	SAM rule	drop	5
5.28.155.172	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
5.28.155.172	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
199.30.25.112	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
66.249.78.137	United States	147.237.76.86	navy.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	4
79.182.50.153	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
85.64.244.210	Israel	147.237.77.226	www.chamatz.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
84.228.161.108	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	4
85.64.39.143	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
5.28.147.151	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
5.28.147.151	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	4
79.183.127.158	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
79.181.105.24	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.46.39.17	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
79.177.168.72	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
167.114.156.16	Canada	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3

## Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.5.223	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	78
176.12.149.165	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	60
62.219.198.6	Israel	147.237.77.234	halag.idf.il	Multiple Unauthorized URL Access from 62.219.198.6	Block	7
176.13.19.180	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	6
176.12.139.71	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	4
46.19.86.212	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.22.158	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
84.108.50.107	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
176.13.6.40	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
185.32.179.41	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	3
107.178.194.87	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	2
79.181.138.25	Israel	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to www.eitan.aka.idf.il/xmlrpc.php	Block	2
79.177.36.104	Israel	147.237.76.42	refuah.idf.il	Parameter Type Violation ctl00\$ContentPlaceHolder1\$txtLastName in www.refua.atal.idf.il/1518-he/refuah.aspx	Block	2
176.228.128.6	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	2
79.181.138.25	Israel	147.237.76.42	refuah.idf.il	Distributed PHP Attempt	Block	2
46.19.85.202	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
79.181.138.25	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on www.refua.atal.idf.il/xmlrpc.php	Block	2
109.67.5.254	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/gyus/general.aspx	Block	2
62.219.198.6	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to www.logistics.atal.idf.il/sip_storage/files/1/size338x0/1531.jpg	Block	2
176.13.23.26	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	2
79.181.138.25	Israel	147.237.76.200	eitan.aka.idf.il	Distributed PHP Attempt	Block	2
73.148.91.22	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/https://twitter.com/	Block	2
176.13.22.5	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Distributed Illegal Parameter Encoding	None	2
212.199.66.195	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to aka.idf.il/main/	Block	2
79.176.148.227	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
195.154.146.225	France	147.237.77.216	dover.idf.il	Distributed Illegal HTTP Version	Block	1
46.19.86.114	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.78.140	Israel	147.237.0.34	tikshuv.idf.il	Multiple Unauthorized URL Access from 66.249.78.140	Block	1
176.228.36.5	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
37.26.149.183	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
84.108.156.37	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
2.54.172.222	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.66.1	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
176.13.9.162	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.166.190.167	Netherlands	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
149.88.76.218	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
79.177.198.89	Israel	147.237.77.226	www.chamatz.aka.idf.il	Unauthorized URL Access to www.chamatz.aka.idf.il/xmlrpc.php	Block	1
208.115.113.89	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/article/	Block	1
41.96.80.55	Algeria	147.237.77.74	law.idf.il	PHP Attempt	Block	1
89.139.7.240	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
77.127.196.170	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
188.120.148.239	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	1
66.249.66.32	Israel	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
176.13.22.5	Israel	147.237.0.17	m.my-kosher-kravi.idf.il	Illegal Byte Code Character in Parameter Value at 46 for m.my-kosher-kravi.idf.il/ajax/createcaptchainage.aspx	Block	1
14.192.210.196	Malaysia	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	1
81.17.31.222	Switzerland	147.237.76.147	chinuch.aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
212.199.107.106	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
64.71.32.32	United States	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on refua.atal.idf.il/old/wp-admin/	Block	1
2.54.28.199	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
79.180.212.4	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1