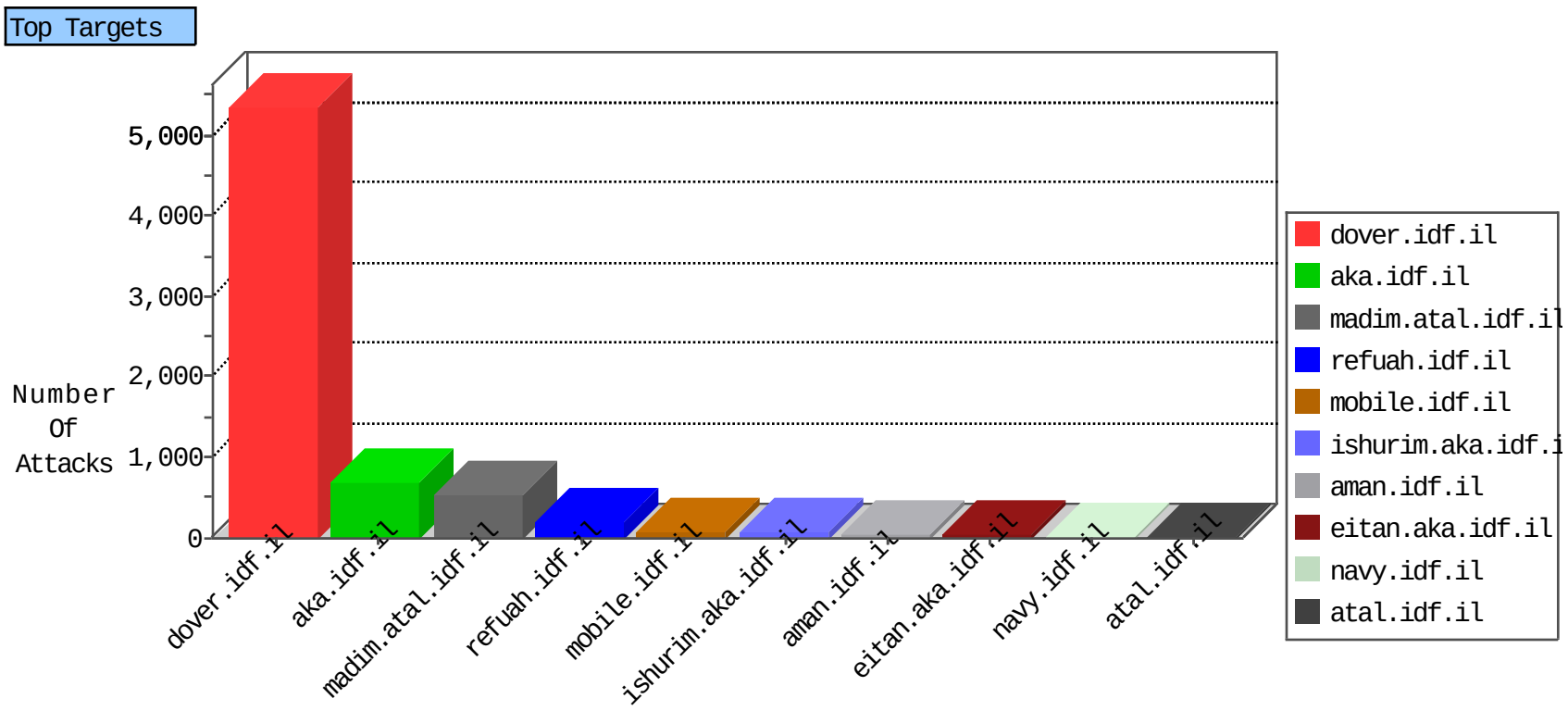
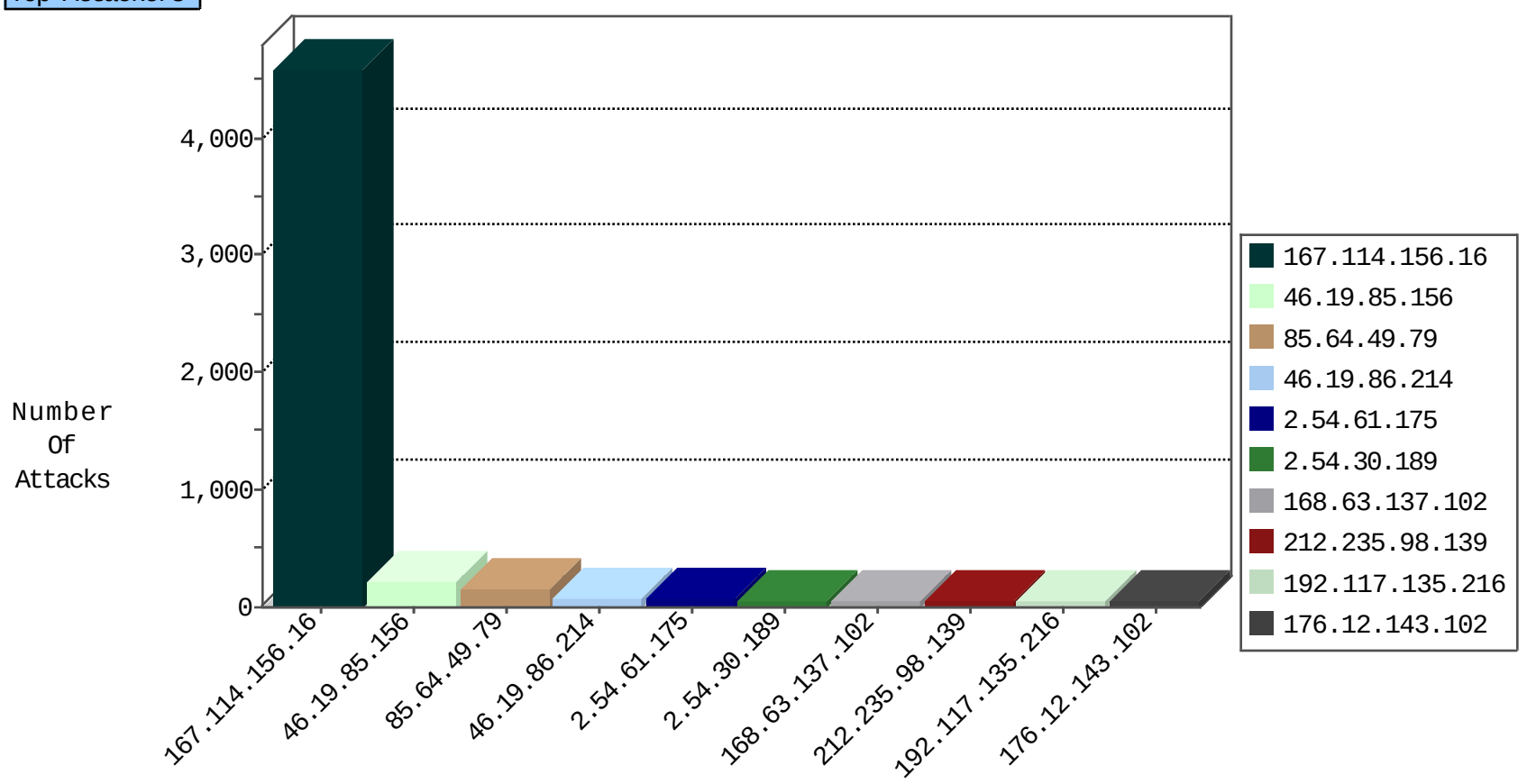
11-23-2015-10:04:08 to 11-23-2015-11:04:08

IDF Under Attack Daily Report

Top Targets



Top Attackers



11-23-2015-10:04:08 to 11-23-2015-11:04:08

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	TCP handshake violation, first packet not syn	drop	3214
167.114.156.16	Canada	147.237.77.216	dover.idf.il	DOS-Tool-SwitchbladG	dest-reset	986
212.143.3.44	Israel	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	15
79.177.80.237	Israel	147.237.77.216	dover.idf.il	Block_Udp_All_Nets	drop	6
31.168.240.21	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
66.249.67.67	United States	147.237.77.74	law.idf.il	TCP handshake violation, first packet not syn	drop	2
27.77.165.48	Vietnam	147.237.76.202	e.halag.idf.il	Block_Udp_All_Nets	drop	1
93.81.206.14	Russian Federation	147.237.76.31	nakchal.idf.il	Block_Udp_All_Nets	drop	1
185.32.179.13	Israel	147.237.77.216	dover.idf.il	SYN Flood unverified cookie	drop	1
114.80.122.91	China	147.237.76.196	e.sviva.idf.il	Block_Ntp_All_Net	drop	1

11-23-2015-10:04:08 to 11-23-2015-11:04:08

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
91.228.248.251	Israel	147.237.76.42	refuah.idf.il	C1000004: HTTP: options method (Microsoft)	Block	15
212.179.21.194	Israel	147.237.77.170	maarachot.idf.il	C1000004: HTTP: options method (Microsoft)	Block	4
2.54.165.84	Israel	147.237.76.42	refuah.idf.il	C1000004: HTTP: options method (Microsoft)	Block	4
212.235.62.200	Israel	147.237.77.216	dover.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
194.90.209.69	Israel	147.237.76.31	nakchal.idf.il	C1000004: HTTP: options method (Microsoft)	Block	2
151.80.31.139	Italy	147.237.77.233	atal.idf.il	C228: HTTP: AhrefBot crawler	Block	1
167.114.156.16	Canada	147.237.77.216	dover.idf.il	8262: HTTP: Slowloris DoS Tool	Block	1
66.240.213.93	United States	147.237.76.38	e.e.meitav.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1
188.165.15.127	France	147.237.77.170	maarachot.idf.il	C228: HTTP: AhrefBot crawler	Block	1
66.240.213.93	United States	147.237.76.39	mobile.meitav.idf.il	13840: TLS: OpenSSL Heartbeat Packet	Block	1
188.165.15.227	France	147.237.77.176	matpash.idf.il	C228: HTTP: AhrefBot crawler	Block	1

11-23-2015-10:04:08 to 11-23-2015-11:04:08

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	1
82.81.35.65	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
182.234.66.93	147.237.0.33	Taiwan	idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
79.182.105.26	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
176.12.140.52	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
62.0.53.15	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
117.45.238.188	147.237.0.34	China	tikshuv.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
46.117.123.149	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
90.44.93.107	147.237.77.176	France	matpash.idf.il	ET SCAN Potential SSH Scan	1
46.19.86.24	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
90.44.93.107	147.237.76.196	France	e.sviva.idf.il	ET SCAN Potential SSH Scan	1
37.26.147.212	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
90.44.93.107	147.237.76.147	France	chinuch.aka.idf.il	ET SCAN Potential SSH Scan	1
5.102.255.78	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
85.93.0.15	147.237.77.226	Germany	www.chamatz.aka.idf.il	ET SCAN NMAP -sS window 1024	1
212.143.3.44	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
82.117.208.243	147.237.77.235		sviva.idf.il	ET SCAN NMAP -sS window 1024	1
194.114.146.227	147.237.72.166	Israel	aka.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
79.182.121.125	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
176.13.22.108	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
79.181.175.75	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
176.12.138.177	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
46.121.96.87	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
90.44.93.107	147.237.77.178	France	e.matpash.idf.il	ET SCAN Potential SSH Scan	1
46.19.86.129	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
90.44.93.107	147.237.76.197	France	e.himush.idf.il	ET SCAN Potential SSH Scan	1
46.19.85.175	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
90.44.93.107	147.237.76.148	France	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
31.184.242.17	147.237.77.216	Russian Federation	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
90.44.93.107	147.237.76.31	France	nakchal.idf.il	ET SCAN Potential SSH Scan	1
2.54.183.146	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
212.143.56.219	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
85.64.135.239	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1

11-23-2015-10:04:08 to 11-23-2015-11:04:08

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	drop	First packet isn't SYN	drop	4096
85.64.49.79	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	143
2.54.30.189	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	60
168.63.137.102	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	56
212.235.98.139	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	55
192.117.135.216	Israel	147.237.72.167	ishurim.aka.idf.i	Streaming Engine: TCP Segment Limit Enforcement	TCP segment out of maximum allowed sequence. Packet dropped.	drop	48
38.111.147.88	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	37
93.157.81.75	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	36
208.115.111.73	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	35
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	32
100.100.90.184		147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
23.27.220.43	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	24
100.100.63.240		147.237.72.156	aman.idf.il	drop	First packet isn't SYN	drop	22
216.185.58.45	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	22
100.100.72.181		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	20
100.100.90.184		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	18
2.54.29.246	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	18
94.230.93.178	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
46.19.85.129	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	16
37.26.148.153	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	15
46.117.163.202	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	15
149.78.156.149	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	13
46.19.85.232	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	12
185.32.179.148	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	12
185.32.179.148	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	12
100.100.102.140		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	12
46.19.85.187	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
193.43.246.250	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
185.32.179.148	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	11
46.166.190.152	Netherlands	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	11
66.249.64.233	United States	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	10
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
66.249.93.192	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	10
185.32.179.13	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
94.230.93.181	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
37.26.146.167	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
77.125.123.70	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
46.120.128.68	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	9
94.230.93.162	Israel	147.237.77.216	dover.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
77.125.163.167	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
46.19.86.114	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	8
149.78.156.149	Israel	147.237.77.233	atal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
2.54.62.178	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
46.19.85.132	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
100.100.73.179		147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	7
185.32.179.148	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	7
46.19.86.233	Israel	147.237.72.167	ishurim.aka.idf.i	Bad TCP sequence	Invalid ACK number	monitor	7
62.0.207.1	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
193.43.245.250	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	7
46.19.85.241	Israel	147.237.76.86	navy.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.85.156	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	128
46.19.85.156	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	90
46.19.86.214	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	72
2.54.61.175	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	64
176.12.143.102	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	51
176.13.22.147	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	32
46.19.86.203	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	27
176.13.22.252	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	17
41.34.22.190	Egypt	147.237.72.166	aka.idf.il	Multiple Unauthorized URL Access from 41.34.22.190	Block	17
176.13.9.83	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	10
37.26.148.164	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	9
82.80.230.200	Israel	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 82.80.230.200	Block	9
2.54.61.175	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	8
38.111.147.88	United States	147.237.77.216	dover.idf.il	Distributed Suspicious Response Code	Block	7
176.13.21.22	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
46.19.86.113	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	3
77.103.134.195	United Kingdom	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
176.13.19.248	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
46.19.86.244	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
79.178.128.167	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in URL from 79.178.128.167	Block	2
93.157.81.75	Israel	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to www.eitan.aka.idf.il/templates/opmissingperson/opmissingperson.in.aspx	Block	2
107.178.194.79	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	2
79.179.145.90	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/ufi/reaction/	Block	2
2.54.33.152	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
107.178.194.83	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	2
176.12.144.48	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
81.218.174.225	Israel	147.237.77.176	matpash.idf.il	Distributed Unauthorized URL Access on www.cogat.idf.il/sip_storage/files/9/4629.jpg	Block	2
79.182.16.72	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/894-he	Block	2
208.184.112.74	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	2
66.249.64.3	Israel	147.237.77.176	matpash.idf.il	Multiple Unauthorized URL Access from 66.249.64.3	Block	2
199.16.156.124	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/sip_storage/files/8/size220x0/15148.jpg	Block	2
109.65.205.96	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
176.12.151.90	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
79.183.149.153	Israel	147.237.72.166	aka.idf.il	Parameter Read Only Violation in www.aka.idf.il/main/sachar/registrationwizard/register.aspx	None	2
105.154.75.29	Morocco	147.237.77.216	dover.idf.il	Untraceable SSL Sessions: Open Mode	None	1
68.180.230.224	United States	147.237.76.31	nakchal.idf.il	Parameter Type Violation PageNum in www.nakhal.idf.il/1111-he/nakhal.aspx	Block	1
204.13.200.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
84.108.65.155	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/main/scripts/css3pie.htc	Block	1
66.249.64.131	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
176.12.137.200	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
2.52.3.153	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
80.246.139.188	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
46.19.85.148	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
109.67.212.72	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/nekudot/index	Block	1
213.57.108.248	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/sip_storage/files/	Block	1
66.249.79.6	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/robots.txt	Block	1
190.17.182.236	Argentina	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/aman	Block	1
31.168.138.81	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$ctl39 in www.aka.idf.il/main/sachar/payslips.aspx	None	1
66.249.64.13	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
176.13.9.7	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1