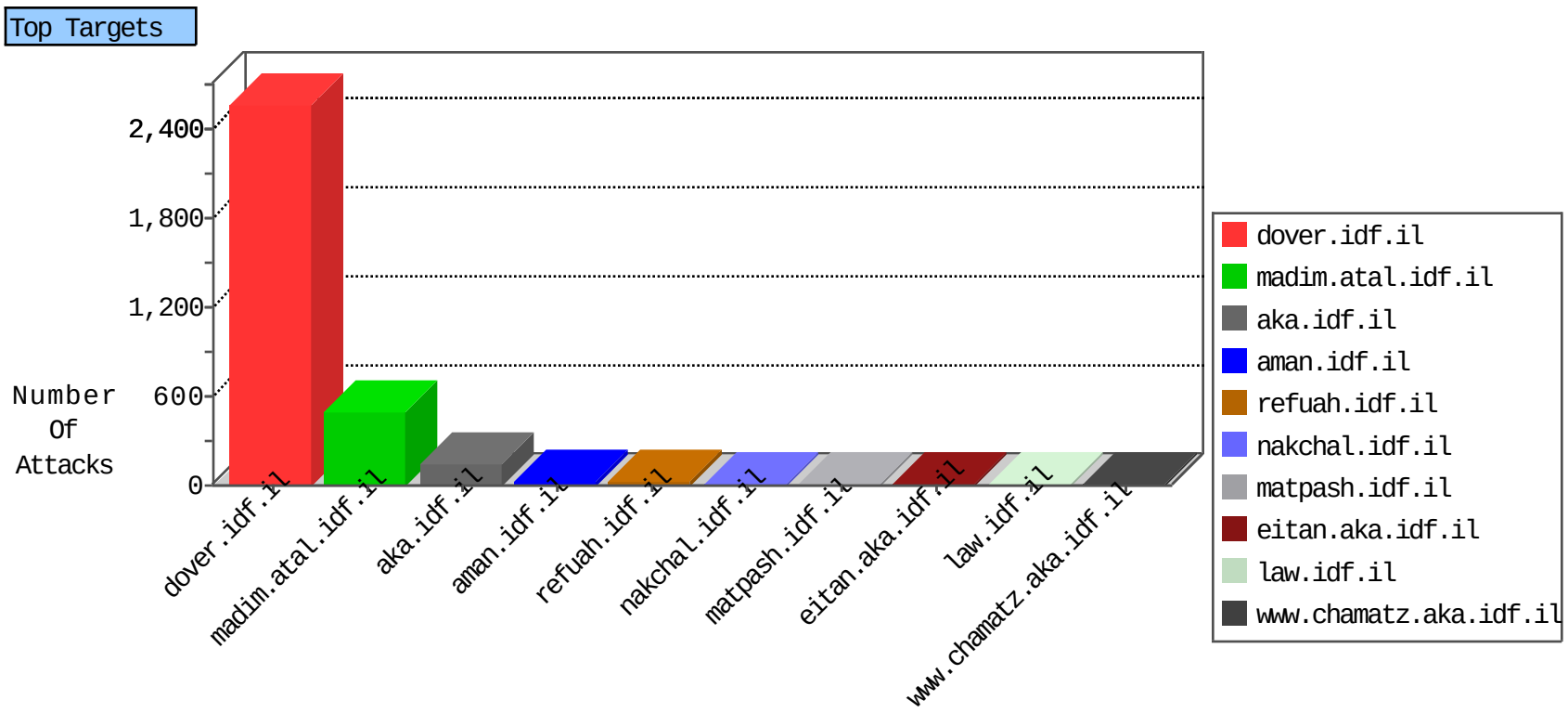
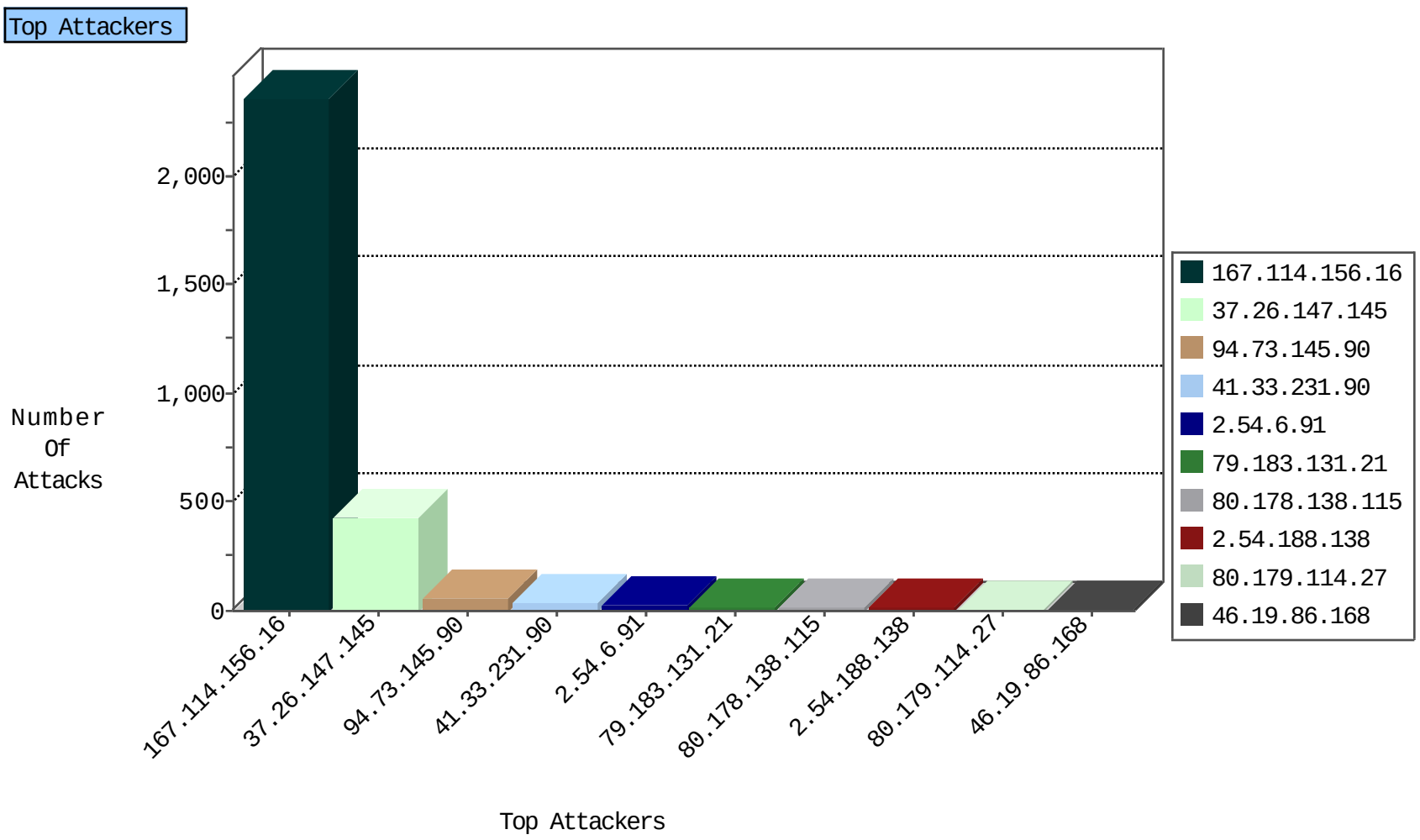
12-21-2015-07:04:05 to 12-21-2015-08:04:05

IDF Under Attack Daily Report





12-21-2015-07:04:05 to 12-21-2015-08:04:05

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	3493
123.151.42.61	China	147.237.76.44	e.refuah.idf.il	Block_Udp_All_Nets_Con_Limit	drop	1
188.138.1.218	Germany	147.237.76.42	refuah.idf.il	Block_Udp_All_Nets	drop	1

12-21-2015-07:04:05 to 12-21-2015-08:04:05

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
188.165.15.160	France	147.237.72.156	aman.idf.il	C228: HTTP: AhrefBot crawler	Block	1
45.33.61.138		147.237.72.167	ishurim.aka.idf.il	C1000107: DDOS-Spoofed HTTP Packets	Block	1
106.38.241.147	China	147.237.77.216	dover.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1
123.126.113.154	China	147.237.77.216	dover.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1
187.122.224.78	Brazil	147.237.77.216	dover.idf.il	16643: HTTP: Protected File Access (/proc/self/environ)	Block	1

12-21-2015-07:04:05 to 12-21-2015-08:04:05

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
2.54.6.91	147.237.0.19	Israel	madim.atal.idf.il	POLICY-OTHER TCP packet with urgent flag attempt	16
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	3
66.249.78.146	147.237.72.166	United States	aka.idf.il	ET SCAN NMAP -sA (2)	2
218.108.132.58	147.237.76.38	China	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
166.63.122.229	147.237.77.235	United States	sviva.idf.il	ET SCAN NMAP -sS window 2048	1
128.199.41.249	147.237.77.216	Singapore	dover.idf.il	ET DROP Spamhaus DROP Listed Traffic Inbound	1
77.53.52.194	147.237.72.167	Sweden	ishurim.aka.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
46.19.86.14	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
31.19.116.8	147.237.77.61	Germany	e.cogat.idf.il	ET SCAN NMAP -sS window 1024	1
166.63.122.229	147.237.77.235	United States	sviva.idf.il	ET SCAN NMAP -f -sS	1
109.235.254.181	147.237.0.16	Turkey	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
37.26.147.145	147.237.0.19	Israel	madim.atal.idf.il	ET SCAN Possible SSL Brute Force attack or Site Crawl	1
24.232.114.214	147.237.0.19	Argentina	madim.atal.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1

12-21-2015-07:04:05 to 12-21-2015-08:04:05

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
94.73.145.90	Turkey	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	47
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	34
79.183.131.21	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
192.0.81.17	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	9
2.54.188.138	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	8
80.179.114.27	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
80.246.130.2	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	8
46.19.85.53	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	6
41.33.232.66	Egypt	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	5
144.131.136.120	Australia	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
2.54.6.91	Israel	147.237.0.19	madim.atal.idf.i	drop	First packet isn't SYN	drop	4
54.244.22.103	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	4
46.19.86.168	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
46.19.85.234	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
84.95.209.133	Israel	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	4
31.210.186.155	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	Invalid ACK number	monitor	4
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
2.54.188.138	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	4
54.151.42.39	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	4
94.73.145.90	Turkey	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	alert	4
46.19.85.234	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	4
2.54.185.56	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
147.235.8.68	Israel	147.237.72.156	aman.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	3
37.26.147.145	Israel	147.237.0.19	madim.atal.idf.i	Bad TCP sequence		alert	3
192.0.99.128	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	3
79.180.177.83	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
46.19.85.123	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
185.27.105.106	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
2.52.18.175	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	3
37.26.147.145	Israel	147.237.0.19	madim.atal.idf.i	Bad TCP sequence		monitor	3
66.102.9.2	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
66.102.9.24	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
37.26.149.175	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
80.178.138.115	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
2.54.191.210	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	3
2.52.161.52	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
80.178.138.115	Israel	147.237.77.74	law.idf.il	Bad TCP sequence	Invalid ACK number	monitor	3
147.235.8.68	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
46.19.86.126	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
192.0.81.57	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	2
46.19.86.41	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
79.177.103.40	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
208.115.113.89	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	2
68.180.229.239	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
50.18.94.121	United States	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	2
46.19.86.126	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	2
80.179.114.27	Israel	147.237.76.31	nakchal.idf.il	Bad TCP sequence	Invalid ACK number	alert	2
2.54.6.91	Israel	147.237.0.19	madim.atal.idf.i	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
212.25.69.22	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	2
80.178.138.115	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2

12-21-2015-07:04:05 to 12-21-2015-08:04:05

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
37.26.147.145	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (404) in Session from 37.26.147.145	Block	244
37.26.147.145	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	124
37.26.147.145	Israel	147.237.0.19	madim.atal.idf.i	Too Many of the Same Response Code (403) in Session from 37.26.147.145	Block	55
46.19.85.218	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	9
46.19.85.78	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	7
46.19.86.205	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
176.13.1.3	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
204.13.200.200	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	2
109.65.49.172	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
109.253.130.28	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
2.54.6.91	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
149.88.181.4	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$cb14120721 in www.aka.idf.il/main/sachar/payslips.aspx	None	2
87.69.110.9	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
185.32.179.142	Israel	147.237.72.166	aka.idf.il	SSL Untraceable Connection - Open Mode	None	1
68.180.229.239	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
46.19.86.164	Israel	147.237.77.243	mobile.idf.il	Unauthorized URL Access to mobile.idf.il/sachar/index	Block	1
109.201.152.237	Netherlands	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
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	1
82.80.130.117	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
66.249.66.136	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/layoutdev.css	Block	1
157.55.39.30	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to 147.237.77.176/robots.txt	Block	1
46.19.85.174	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
2.54.2.12	Israel	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	1
212.143.110.33	Israel	147.237.72.166	aka.idf.il	Unknown Parameter __VIEWSTATEENCRYPTED in www.aka.idf.il/main/sachar/declarationexplanation.aspx	None	1
91.106.36.165	Iraq	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/arr/	Block	1
188.138.9.49	Germany	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
79.178.137.98	Israel	147.237.77.74	law.idf.il	Unauthorized URL Access to www.mag.idf.il/images/1.he/infocenteritem/	Block	1
107.178.194.83	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
84.228.143.245	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
207.46.13.83	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to navy.idf.il/main/drushim/misrot.aspx	Block	1
158.69.197.249	United States	147.237.77.216	dover.idf.il	PHP Attempt	Block	1
66.249.66.191	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/style/shared/nav.css	Block	1
109.65.182.59	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.19.85.197	Israel	147.237.76.42	refuah.idf.il	Malformed URL	Block	1
212.143.110.33	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$cphSachar$employmentStatus in www.aka.idf.il/main/sachar/payslips.aspx	None	1
93.173.128.203	Israel	147.237.72.166	aka.idf.il	Multiple Illegal Byte Code Character in URL from 93.173.128.203	Block	1
192.115.177.202	Israel	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/sip_storage/files/9/4629.jpg	Block	1
79.179.183.139	Israel	147.237.72.166	aka.idf.il	Unauthorized Method HEAD for www.aka.idf.il/main/sachar/	Block	1
46.121.206.225	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to www.aka.idf.il/mains/sachar	Block	1
149.50.72.109	United States	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
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	1
37.26.148.229	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	1
85.64.162.159	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
207.46.13.117	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	1
158.69.197.249	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/magmi/web/magmi.php	Block	1
66.249.78.234	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/main/giyus/general.aspx	Block	1
109.65.212.194	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
46.19.85.197	Israel	147.237.76.42	refuah.idf.il	Unknown HTTP Request Method 5 in URL	Block	1
2.54.165.104	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
94.73.145.90	Turkey	147.237.72.166	aka.idf.il	MSSQL Data Retrieval with Implicit Conversion Errors	None	1

12-21-2015-07:04:05 to 12-21-2015-08:04:05