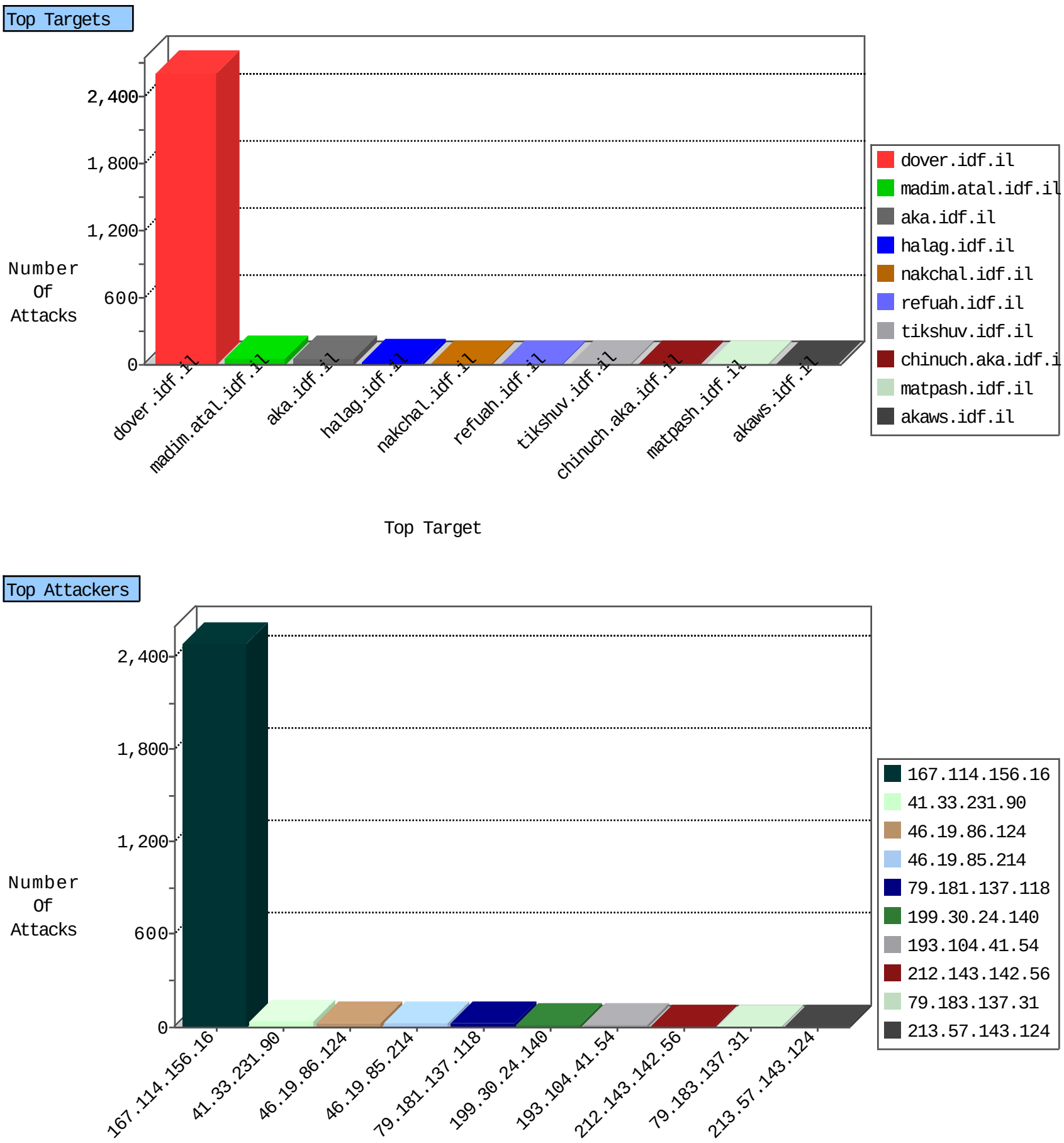
12-11-2015-01:04:46 to 12-11-2015-02:04:46

IDF Under Attack
Daily Report



12-11-2015-01:04:46 to 12-11-2015-02:04:46

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	3393
87.98.237.189	Poland	147.237.76.147	chinuch.aka.idf.il	Block_Ntp_All_Net	drop	1
158.69.199.64	United States	147.237.76.148	ggcenter.aka.idf.il	Block_Ntp_All_Net	drop	1

12-11-2015-01:04:46 to 12-11-2015-02:04:46

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
106.38.241.106	China	147.237.72.166	aka.idf.il	C103: HTTP: User Agent Sogou+web+spider	Block	1

12-11-2015-01:04:46 to 12-11-2015-02:04:46

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	5
64.233.172.201	147.237.0.34	United States	tikshuv.idf.il	ET SCAN NMAP -sA (2)	2
193.104.41.54	147.237.76.86	Moldova, Republic of	navy.idf.il	ET SCAN Potential SSH Scan	1
193.104.41.54	147.237.72.217	Moldova, Republic of	e.idf.il	ET SCAN Potential SSH Scan	1
193.104.41.54	147.237.8.27	Moldova, Republic of	e.madim.atal.idf.il	ET SCAN Potential SSH Scan	1
193.104.41.54	147.237.0.35	Moldova, Republic of	akaws.idf.il	ET SCAN Potential SSH Scan	1
187.161.61.98	147.237.0.35	Mexico	akaws.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
104.131.178.83	147.237.0.16	United States	my-kosher-kravi.idf.il	SERVER-APACHE Apache mod_ssl non-SSL connection to SSL port denial of service attempt	1
218.108.132.58	147.237.0.16	China	my-kosher-kravi.idf.il	ET SCAN NMAP -sS window 1024	1
193.104.41.54	147.237.77.212	Moldova, Republic of	e.dover.idf.il	ET SCAN Potential SSH Scan	1
12.139.41.189	147.237.76.38	United States	e.e.meitav.idf.il	ET SCAN NMAP -sS window 1024	1
193.104.41.54	147.237.76.148	Moldova, Republic of	gqcenter.aka.idf.il	ET SCAN Potential SSH Scan	1
193.104.41.54	147.237.76.31	Moldova, Republic of	nakchal.idf.il	ET SCAN Potential SSH Scan	1
193.104.41.54	147.237.72.14	Moldova, Republic of	dover.idf.il(old)	ET SCAN Potential SSH Scan	1
193.104.41.54	147.237.8.14	Moldova, Republic of	e.orchot.idf.il	ET SCAN Potential SSH Scan	1
193.104.41.54	147.237.0.34	Moldova, Republic of	tikshuv.idf.il	ET SCAN Potential SSH Scan	1
187.161.61.98	147.237.0.15	Mexico	kosher-kravi.idf.il	ET SCAN Behavioral Unusually fast inbound Telnet Connections, Potential Scan or Brute Force	1
94.75.220.155	147.237.76.201	Netherlands	e.atal.idf.il	ET SCAN NMAP -sS window 1024	1
61.244.49.137	147.237.77.61	Hong Kong	e.cogat.idf.il	ET SCAN NMAP -sS window 1024	1
193.104.41.54	147.237.77.176	Moldova, Republic of	matpash.idf.il	ET SCAN Potential SSH Scan	1

12-11-2015-01:04:46 to 12-11-2015-02:04:46

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
199.30.24.140	United States	147.237.77.234	halag.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
46.19.85.214	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	12
46.19.85.214	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	12
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
46.121.85.185	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	6
46.19.85.84	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
109.66.49.180	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
79.183.137.31	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	4
79.183.199.215	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
109.64.213.43	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	3
213.57.143.124	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	alert	3
213.57.143.124	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	3
79.183.137.31	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
167.88.12.213	United States	147.237.76.198	e.yohalan.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	2
2.54.15.57	Israel	147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	2
46.19.85.58	Israel	147.237.0.34	tikshuv.idf.il	Bad TCP sequence	Invalid ACK number	monitor	2
68.180.229.121	United States	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
207.46.13.49	United States	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	2
128.232.110.28	United Kingdom	147.237.76.34	yohalan.idf.il	drop		drop	2
84.109.3.6	Israel	147.237.77.170	maarachot.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	2
141.212.122.68	United States	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
213.57.89.62	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
42.156.136.53	China	147.237.76.31	nakchal.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	1
141.212.122.105	United States	147.237.8.14	e.orchot.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
89.138.79.138	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
207.46.13.17	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
141.212.122.123	United States	147.237.77.178	e.matpash.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.122.69	United States	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
213.57.89.62	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
176.12.145.193	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	1
141.212.122.113	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
37.142.154.38	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
141.212.122.124	United States	147.237.77.178	e.matpash.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.122.77	United States	147.237.0.35	akaws.idf.il	drop		drop	1
84.108.162.214	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	1
188.138.17.205	France	147.237.76.196	e.sviva.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.122.114	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
71.209.223.190	United States	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
208.115.113.89	United States	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
141.212.122.125	United States	147.237.76.196	e.sviva.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.122.78	United States	147.237.0.35	akaws.idf.il	drop		drop	1
84.108.162.214	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	1
141.212.122.121	United States	147.237.76.176	test.ncore.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1
42.156.136.53	China	147.237.76.31	nakchal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	1
141.212.122.126	United States	147.237.76.196	e.sviva.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
141.212.122.104	United States	147.237.8.14	e.orchot.idf.il	Geo-location enforcement	Geo-location inbound enforcement	drop	1
204.13.200.200	United States	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	1
141.212.122.122	United States	147.237.76.176	test.ncore.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	1

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
46.19.86.124	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	28
79.181.137.118	Israel	147.237.0.19	madim.atal.idf.il	Distributed Suspicious Response Code	Block	24
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
66.249.69.8	Israel	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to www.chinuch.aka.idf.il/404.htm	Block	2
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
66.33.212.131	United States	147.237.77.233	atal.idf.il	Multiple Unauthorized URL Access from 66.33.212.131	Block	2
84.111.12.156	Israel	147.237.72.166	aka.idf.il	Suspicious Response Code_Custom_Temporary	Block	2
79.182.168.41	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	2
93.160.60.22	Denmark	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/newsite/english	Block	1
46.148.18.122	Lithuania	147.237.76.147	chinuch.aka.idf.il	Unauthorized URL Access to 147.237.76.147/rom-0	Block	1
207.46.13.152	United States	147.237.72.166	aka.idf.il	Unknown Parameter catid in aka.idf.il/iturim/asp/results.asp	None	1
83.94.112.226	Denmark	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
217.132.32.207	Israel	147.237.76.31	nakchal.idf.il	PHP Attempt	Block	1
66.249.64.143	Israel	147.237.72.166	aka.idf.il	Distributed Unauthorized URL Access on 147.237.72.166/main/giyus/general.aspx	Block	1
37.142.231.35	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
157.55.39.119	United States	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to 147.237.76.31/robots.txt	Block	1
104.131.178.83	United States	147.237.0.15	kosher-kravi.idf.il	Unauthorized URL Access to /	Block	1
66.249.75.38	Israel	147.237.76.200	eitan.aka.idf.il	Unauthorized URL Access to www.eitan.aka.idf.il/templates/shared/usercontrols/navmenu/mazi.idf.il	Block	1
208.184.112.74	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22461-he/dover.aspx.	Block	1
107.178.194.87	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
84.108.241.42	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
217.132.32.207	Israel	147.237.76.31	nakchal.idf.il	Unauthorized URL Access to nakhal.idf.il/xmlrpc.php	Block	1
66.249.64.233	Israel	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/error.htm	Block	1
40.77.167.30	United States	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/navy/ official website	Block	1
176.12.145.193	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/1518-he/refuah.aspx	Block	1
104.236.94.195		147.237.76.39	mobile.meitav.idf.il	Unauthorized URL Access to /	Block	1
68.180.228.112	United States	147.237.77.216	dover.idf.il	Parameter Type Violation PageNum in www.idf.il/1393-en/dover.aspx	Block	1
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	1
66.33.212.131	United States	147.237.77.233	atal.idf.il	Unauthorized URL Access to atal.idf.il/wp-admin/	Block	1
109.65.160.235	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
66.249.64.235	Israel	147.237.77.216	dover.idf.il	Unauthorized URL Access to 147.237.77.216/1133-17805-he/dover.aspx	Block	1
46.19.85.55	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	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
104.236.94.195		147.237.76.42	refuah.idf.il	Unauthorized Method HEAD for /	Block	1
208.184.112.75	United States	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/1133-22638-he/dover.aspx.	Block	1
66.249.64.13	Israel	147.237.72.166	aka.idf.il	Unauthorized URL Access to 147.237.72.166/giyus/forum/asp/showforum.asp	Block	1
109.67.172.112	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
85.250.197.103	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: sigalgs DoS Attack	None	1
66.249.65.118	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/8/2378.jpg	Block	1
207.46.13.49	United States	147.237.72.166	aka.idf.il	Distributed Suspicious Response Code_Custom_Temporary	Block	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
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
157.55.39.48	United States	147.237.77.170	maarachot.idf.il	Unauthorized URL Access to maarachot.idf.il/pdf/files/9/110539.pdf,	Block	1

12-11-2015-01:04:46 to 12-11-2015-02:04:46